rekt

WHITE PAPER

00 TABLE OF CONTENTS

01 DATE OF NOTIFICATION

2025-07-15

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 Not applicable

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.

07 Warning

This summary should be read as an introduction to the crypto-asset white paper. Any decision by a prospective holder to acquire this crypto-asset should be based on the content of the full white paper and not solely on this summary.

No public offering of this crypto-asset has been made by the issuer in the European Union or elsewhere. This white paper has been prepared for the purpose of transparency and compliance with Regulation (EU) 2023/1114 (MiCA) in connection with a potential admission to trading on a crypto-asset exchange platform.

This document does not constitute an offer or solicitation to purchase financial instruments. Any such offer or solicitation may only be made by means of a prospectus or other offer documents in accordance with 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

$REKT is a digital token created for cultural and community engagement. It does not provide any ownership, profit-sharing, voting rights, or access to products or services. Holding the token does not give the purchaser any legal or financial rights over the issuer or any affiliated project. There are no obligations on the part of the issuer towards holders of $REKT. The token cannot be redeemed, exchanged for goods or services by the issuer, or used to claim any benefits. Its purpose is symbolic — to represent alignment with the REKT brand and community. There are no procedures for exercising rights, as no rights are conferred by holding the token. Similarly, there are no mechanisms by which rights or obligations could be modified, as none are established in the first place.

09 Not applicable

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

There was no public offering of $REKT within the European Union. $REKT was distributed for free via airdrops to early supporters of the REKT ecosystem, including holders of Rektguy NFTs and purchasers of Rekt Drinks. No subscription fees were charged, and there were no target amounts, price tiers, or subscription periods. There was no fundraising, ICO, or sale event associated with this distribution. The total token supply was pre-defined and capped. No discounted purchase prices or phased offering mechanics were applied, and the token was not offered through any crypto-asset service provider. $REKT was not admitted to trading on any EU-registered trading platform. It is, however, accessible via decentralised exchanges that are publicly available on blockchains such as Ethereum, Base, and Solana. These listings were not arranged by the issuer.

Part I – Information on risks

I.1 Offer-Related Risks

There was no public offer of $REKT in the European Union. However, the general risks associated with informal distribution via airdrop include price volatility upon market listing. There was no firm placement, underwriter, or EU-based marketing. Any perception of value by recipients is driven solely by market dynamics.

I.2 Issuer-Related Risks

The issuer, Golden Pothos Foundation (Cayman Islands), is not regulated in the EU and is not subject to EU investor protection regimes. As a Cayman foundation, it is subject to Cayman law but may not offer the same degree of transparency or legal recourse available in EU jurisdictions. There are no financial obligations, ongoing business activities, or legal commitments tied to the token.

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.

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.

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

$REKT is a speculative digital asset with no intrinsic value or utility. Key risks include extreme price volatility, potential illiquidity, vulnerability to market manipulation, and reliance on third-party infrastructure (e.g., decentralised exchanges). There are no backing assets, redemption rights, or technical safeguards protecting token holders. Token value is driven by narrative, cultural momentum, and market sentiment alone.

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

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

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

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

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

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

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

I.4 Project Implementation-Related Risks

There is no formal project implementation roadmap associated with $REKT. It is not tied to future deliverables, milestones, or product developments. Any perceived alignment with the REKT brand or ecosystem is informal and non-binding. Risks include the discontinuation of community interest, lack of issuer engagement, and the failure of associated brand projects to maintain relevance or visibility.

I.5 Technology-Related Risks

$REKT is built on Ethereum and bridged to other chains using LayerZero's OFT standard. Risks include smart contract vulnerabilities (on Ethereum or bridge contracts), chain outages or failures, and reliance on third-party infrastructure. Although no upgradeable logic exists, external exploits or changes in base-layer protocol behaviour may affect token availability, functionality, or security.

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 circumstances, 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 an 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

No formal mitigation measures are in place. The token is immutable and has no administrative privileges, upgrade capabilities, or governance. Security relies on the robustness of the Ethereum network and LayerZero bridging infrastructure. Holders are advised to take precautions such as using hardware wallets, avoiding phishing scams, and understanding the risks of interacting with decentralised platforms.

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

A.1 Name

Golden Pothos Foundation

A.2 Legal Form

N/A (see LEI below)

A.3 Registered Address

N/A (see LEI below)

A.4 Head Office

N/A (see LEI below)

A.5 Registration Date

2024-07-18

A.6 Legal Entity Identifier

254900R3KG5GAA2E1127

A.7 Another Identifier Required Pursuant to Applicable National Law

N/A (see LEI)

A.8 Contact Telephone Number

+1 345-749-9601

A.9 E-mail Address

gkennedy@leewardmanagement.ky

A.10 Response Time (Days)

30

A.11 Parent Company

N/A (see LEI)

A.12 Members of the Management Body

Full Name	Business Address	Function
Glenn Kennedy	Golden Pothos Foundation c/o Leeward Management Limited Suite 3119, 9 Forum Lane, Camana Bay PO Box 144, George Town Grand Cayman KY1-9006 Cayman Islands	Director

A.13 Business Activity

Technology

- Purpose/strategy/vision - To build the world's first culturally-driven crypto brand through memes, community, and decentralised brand equity.

- Products/services - Rekt creates viral consumer products, digital collectibles, and engagement experiences tied to crypto culture.
- Markets served - Rekt serves a global audience across Web3, digital art, and online consumer markets in the US, EU, and Asia.
- Outlook - Rekt aims to expand its ecosystem across new product verticals, retail partnerships, and crypto-native loyalty models.

A.14 Parent Company Business Activity

N/A

A.15 Newly Established

true

A.16 Financial Condition for the past three Years

N/A

A.17 Financial Condition Since Registration

N/A

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

N/A - see B.1

B.3 Legal Form

N/A - see B.1

B.4 Registered Address

N/A - see B.1

B.5 Head Office

N/A - see B.1

B.6 Registration Date

N/A - see B.1

B.7 Legal Entity Identifier

N/A - see B.1

B.8 Another Identifier Required Pursuant to Applicable National Law

N/A - see B.1

B.9 Parent Company

N/A - see B.1

B.10 Members of the Management Body

N/A - see B.1

B.11 Business Activity

N/A - see B.1

B.12 Parent Company Business Activity

N/A - see B.1

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

N/A

C.2 Legal Form

N/A

C.3 Registered Address

N/A

C.4 Head Office

N/A

C.5 Registration Date

N/A

C.6 Legal Entity Identifier

N/A

C.7 Another Identifier Required Pursuant to Applicable National Law

N/A

C.8 Parent Company

N/A

C.9 Reason for Crypto-Asset White Paper Preparation

N/A

C.10 Members of the Management Body

N/A

C.11 Operator Business Activity

N/A

C.12 Parent Company Business Activity

N/A

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

N/A

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

N/A

D. Part D - Information about the crypto-asset project

D.1 Crypto-Asset Project Name

Rekt

D.2 Crypto-Assets Name

Rekt

D.3 Abbreviation

$REKT

D.4 Crypto-Asset Project Description

$REKT is a memecoin issued as a symbol of community alignment and internet culture. It has no utility, governance, or financial rights. The token is purely speculative and not tied to any roadmap or product.

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

Full Name	Business Address	Function
Glenn Kennedy	Golden Pothos Foundation c/o Leeward Management Limited Suite 3119, 9 Forum Lane, Camana Bay PO Box 144, George Town Grand Cayman KY1-9006 Cayman Islands	Director
Ovie Faruq	Rekt Brands Inc, 1207 Delaware Ave, Ste 4069, Wilmington, 19206, DE	Contributor

D.6 Utility Token Classification

false

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

N/A

D.8 Plans for the Token

Rekt aims to expand its ecosystem across new product verticals, retail partnerships, and crypto-native loyalty models

D.9 Resource Allocation

N/A

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

N/A (no token sale or offering)

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

ATTR

E.2 Reasons for Public Offer or Admission to Trading

No funds are being raised and no public offering is being made; admission to trading is sought solely to enable secondary market access and improve token liquidity.

E.3 Fundraising Target

N/A - No funds are being raised and no public offer is being made

E.4 Minimum Subscription Goals

N/A - No funds are being raised and no public offer is being made

E.5 Maximum Subscription Goal

N/A - No funds are being raised and no public offer is being made

E.6 Oversubscription Acceptance

N/A - No funds are being raised and no public offer is being made

E.7 Oversubscription Allocation

N/A - No funds are being raised and no public offer is being made

E.8 Issue Price

N/A - No funds are being raised and no public offer is being made

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

N/A - No funds are being raised and no public offer is being made

E.10 Subscription Fee

N/A - No funds are being raised and no public offer is being made

E.11 Offer Price Determination Method

N/A - No funds are being raised and no public offer is being made

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

420,690,000,000,000

E.13 Targeted Holders

ALL

E.14 Holder Restrictions

No restrictions.

E.15 Reimbursement Notice

N/A - No funds are being raised and no public offer is being made

E.16 Refund Mechanism

N/A - No funds are being raised and no public offer is being made

E.17 Refund Timeline

N/A - No funds are being raised and no public offer is being made

E.18 Offer Phases

N/A - No funds are being raised and no public offer is being made

E.19 Early Purchase Discount

N/A - No funds are being raised and no public offer is being made

E.20 Time-Limited Offer

false

E.21 Subscription Period Beginning

N/A - No funds are being raised and no public offer is being made

E.22 Subscription Period End

N/A - No funds are being raised and no public offer is being made

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

N/A - No funds are being raised and no public offer is being made

E.24 Payment Methods for Crypto-Asset Purchase

N/A - No funds are being raised and no public offer is being made

E.25 Value Transfer Methods for Reimbursement

N/A - No funds are being raised and no public offer is being made

E.26 Right of Withdrawal

N/A - No funds are being raised and no public offer is being made

E.27 Transfer of Purchased Crypto-Assets

N/A - No funds are being raised and no public offer is being made

E.28 Transfer Time Schedule

N/A - No funds are being raised and no public offer is being made

E.29 Purchaser's Technical Requirements

N/A - No funds are being raised and no public offer is being made

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

N/A - No funds are being raised and no public offer is being made

E.31 CASP identifier

N/A - No funds are being raised and no public offer is being made

E.32 Placement Form

N/A - No funds are being raised and no public offer is being made

E.33 Trading Platforms name

Kraken

E.34 Trading Platforms Market Identifier Code (MIC)

PGTP

E.35 Trading Platforms Access

Investors can access $REKT on compliant EU trading platforms (e.g., Kraken EU) by creating and verifying a platform account, completing required KYC/AML checks, and depositing funds via supported payment methods or crypto wallets.

E.36 Involved Costs

Accessing and trading $REKT on centralised platforms such as Kraken may involve certain costs. These can include trading fees (typically ranging from 0.10% to 0.40%), deposit and withdrawal fees (which vary by payment method and currency), and potential spreads applied to instant buy/sell transactions. Additional charges may apply depending on the user's chosen subscription tier or funding method. Users should refer to the applicable trading platform's published fee schedule for up-to-date information.

E.37 Offer Expenses

N/A - No funds are being raised and no public offer is being made

E.38 Conflicts of Interest

No known conflicts of interest exist between the issuer, its management, or affiliated parties in relation to the admission of $REKT to trading. No individual involved in this process receives preferential treatment, access, or financial incentives outside of publicly disclosed holdings and existing contractual relationships.

E.39 Applicable Law

N/A - No funds are being raised and no public offer is being made

E.40 Competent Court

N/A - No funds are being raised and no public offer is being made

F. Part F - Information about the crypto-assets

F.1 Crypto-Asset Type

Fungible crypto-asset issued on a public blockchain (ERC-20 standard), not classified as an asset-referenced token (ART), e-money token (EMT), or utility token.

F.2 Crypto-Asset Functionality

$REKT has no built-in functionality. It does not grant access to any service, platform, or product, and confers no governance, ownership, or utility rights. It is purely symbolic and operates as a memecoin.

F.3 Planned Application of Functionalities

N/A

F.4 Type of white paper

OTHR

F.5 The type of submission

NEWT

F.6 Crypto-Asset Characteristics

$REKT is a fungible, freely transferable ERC-20 token with a fixed total supply. It has no utility, governance, or financial rights attached. It does not provide access to any product or service and carries no redemption, yield, or voting features. The token is purely symbolic and operates as a memecoin representing cultural alignment and online community participation.

F.7 Commercial name or trading name

Rekt

F.8 Website of the issuer

https://rektcoin.com

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

2025-08-18 (Note, no public offering, only admission to trading)

F.10 Publication date

2025-07-22

F.11 Any other services provided by the issuer

N/A

F.12 Identifier of operator of the trading platform

PGTP

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

ISO 24165 Digital Token Identifier

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

ISO 24165 FFG DTI

F.16 Voluntary data flag

true

F.17 Personal data flag

true

F.18 LEI eligibility

true

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, Iceland, Liechtenstein, Norway

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

G.1 Purchaser Rights and Obligations

No rights or obligations

G.2 Exercise of Rights and Obligation

No rights or obligations

G.3 Conditions for Modifications of Rights and Obligations

No rights or obligations

G.4 Future Public Offers

No future public offering planned

G.5 Issuer Retained Crypto-Assets

3 - (USDC, USDT, REKT)

G.6 Utility Token Classification

false

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

N/A - the tokens have no utility

G.8 Utility Tokens Redemption

N/A - the tokens have no utility

G.9 Non-Trading Request

true

G.10 Crypto-Assets Purchase or Sale Modalities

N/A - admission sought

G.11 Crypto-Assets Transfer Restrictions

N/A - no restrictions

G.12 Supply Adjustment Protocols

false

G.13 Supply Adjustment Mechanisms

N/A

G.14 Token Value Protection Schemes

false

G.15 Token Value Protection Schemes Description

N/A - false

G.16 Compensation Schemes

false

G.17 Compensation Schemes Description

N/A - false

G.18 Applicable Law

The $REKT crypto-asset is issued by a legal entity incorporated in the Cayman Islands, and is therefore subject to the laws of the Cayman Islands. No public offering is being made in the European Union.

G.19 Competent Court

Any disputes arising in connection with the $REKT crypto-asset shall be subject to the exclusive jurisdiction of the courts of the Cayman Islands, without prejudice to applicable consumer protection laws in the jurisdiction of the token holder.

H. Part H – information on the underlying technology

H.1 Distributed ledger technology

Distributed Ledger Technology (DLT) refers to a decentralised network architecture where a shared database is maintained collectively by a network of participants (nodes), rather than a central authority. Every change to the ledger is recorded and agreed upon by consensus, which enhances transparency, security, and trustlessness.

Blockchain is a specific type of DLT where data is stored in linked blocks in chronological order. Each block contains transaction data and a cryptographic reference to the previous block, making it extremely difficult to alter past records without consensus from the network.

The Ethereum Blockchain

Ethereum is a decentralised, public blockchain that enables not only the transfer of value but also the execution of smart contracts—programs that run exactly as coded without downtime, fraud, or third-party interference. It was launched in 2015 and has since become the most widely used blockchain for decentralised applications (dApps), NFTs, and decentralised finance (DeFi).

Ethereum currently operates using a proof-of-stake (PoS) consensus mechanism, known as Ethereum 2.0 or "the Merge," which replaced the prior proof-of-work (PoW) system. Validators are selected to confirm transactions and add new blocks based on the amount of ETH they stake, making the network more energy-efficient and scalable.

The native token of Ethereum is Ether (ETH). It is used to:

- Pay for transaction and smart contract execution fees (called gas),
- Secure the network via staking,
- Interact with dApps and decentralised protocols.

Key Characteristics of Ethereum

- Smart Contract Functionality: Ethereum allows anyone to deploy programmable logic on-chain, enabling complex financial products, governance mechanisms, and game mechanics.
- Token Standards: Ethereum supports a wide range of token types, including ERC-20 (fungible tokens), ERC-721 (NFTs), and ERC-1155 (multi-token standard).
- Interoperability: Ethereum is compatible with thousands of wallets and apps across the crypto ecosystem.
- Transparency and Immutability: All transactions and smart contract logic are publicly visible and nearly impossible to tamper with once confirmed.
- Developer Ecosystem: With the largest developer community in crypto, Ethereum evolves rapidly and supports extensive tooling and infrastructure.

Further Information

For more technical and community information, see:

https://ethereum.org – official Ethereum portal

https://github.com/ethereum – official GitHub organisation

https://etherscan.io – blockchain explorer for Ethereum

H.2 Protocols and Technical Standards

ERC-20 token standard; LayerZero OFT v2 standard for omnichain compatibility. Supports interoperability across Ethereum, Base, Solana, and other supported chains.

H.3 Technology Used

Smart contract deployed on Ethereum. Additional smart contracts enable cross-chain transfers via LayerZero. Token holders manage custody via standard EVM-compatible wallets.

H.4 Consensus Mechanism

The Ethereum blockchain uses a proof-of-stake (PoS) consensus mechanism called Ethereum 2.0, introduced with "The Merge" in September 2022. This transition marked a shift from Ethereum's original proof-of-work model to a more energy-efficient and scalable architecture.

In Ethereum's PoS model, validators are selected to propose and attest to new blocks based on the amount of Ether (ETH) they have staked. A minimum of 32 ETH is required to operate a validator node. Validators are randomly chosen to propose new blocks and are rewarded for honest participation while penalised (slashed) for malicious or faulty behaviour.

Blocks are created in fixed intervals known as slots (~12 seconds), and organised into epochs (~6.4 minutes). A finality gadget known as Casper FFG (Friendly Finality Gadget) is used to reach consensus and finalise blocks, reducing the chance of chain reorganisations. Finality occurs when a supermajority of validators attest to the same chain history.

This PoS mechanism increases security, reduces environmental impact, and supports Ethereum's roadmap toward higher scalability via sharding and other upgrades.

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

H.5 Incentive Mechanisms and Applicable Fees

Ethereum's fee and incentive structure is designed to ensure the long-term sustainability and security of the network, encourage validator participation in the consensus mechanism, and provide a dynamic and market-driven approach to transaction pricing.

Ethereum uses a base fee + tip model introduced with EIP-1559, which replaced the prior auction-based system. Transaction fees are calculated as:

Total Fee = Base Fee + Priority Fee (Tip)

- The base fee is an algorithmically adjusted amount that reflects current network demand and is burned (permanently removed from circulation), reducing ETH supply.
- The priority fee (tip) is set by the user and paid to validators as an incentive for including the transaction in a block.

Smart contract execution also requires gas, a unit representing computational effort. Each operation has a defined gas cost, and users specify a gas limit and max fee per gas unit. If unused, the remaining gas is refunded.

Incentives for validators are structured around Ethereum's proof-of-stake mechanism, where validators stake 32 ETH to participate. They receive rewards in ETH for proposing and attesting to blocks, funded by a combination of:

- Priority fees from users,
- A small ETH issuance (new supply),
- MEV (Maximal Extractable Value) in some cases.

Validators are penalised for malicious behaviour or extended downtime via slashing or reduced rewards. This model incentivises honest participation and helps secure the Ethereum network.

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

H.6 Use of Distributed Ledger Technology

false

H.7 DLT Functionality Description

The Ethereum network does not rely on a single centralised entity; instead, it is operated by a global set of independent validators who participate in transaction validation and block production under the proof-of-stake consensus mechanism. Anyone meeting the minimum staking requirement (32 ETH) can run a validator node and contribute to Ethereum's operation. The network is sufficiently decentralised, with no single party able to control or alter its operation.

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

H.8 Audit

true

H.9 Audit Outcome

The Ethereum blockchain has undergone multiple independent audits by third-party organisations specialising in blockchain infrastructure and cybersecurity. Audits have been conducted across various components of the Ethereum ecosystem, including its core consensus upgrades and virtual machine (EVM).

Ahead of the Ethereum 2.0 upgrade ("The Merge"), critical components—such as the Beacon Chain, consensus clients (e.g. Prysm, Lighthouse, Teku, and Nimbus), and execution clients (e.g. Geth, Nethermind)—underwent formal audits by leading security firms including Trail of Bits, Sigma Prime, and Runtime Verification.

These audits assessed protocol implementation, consensus logic, validator operations, and network resilience. No critical vulnerabilities were found in the audited versions, and any medium-risk findings were addressed by the Ethereum developer community prior to deployment. These efforts reflect Ethereum's commitment to robust and peer-reviewed development.

A selection of public audit reports is available here:

https://github.com/ethereum/eth2.0-specs/tree/dev/audits

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

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

This disclosure is provided in accordance with the template referred to in the Annex to Commission Delegated Regulation (EU) 2025/422 specifying the content, methodologies, and presentation of sustainability indicators in relation to adverse impacts on the climate and other environment-related aspects under Regulation (EU) 2023/1114 (MiCA).

Following the Ethereum network's transition to proof-of-stake (known as "The Merge") in September 2022, Ethereum no longer relies on energy-intensive mining operations. The energy consumption of the network has been reduced by over 99.95%, replacing the previous proof-of-work model with a highly efficient validator-based system.

The adverse environmental impact of Ethereum is now comparatively low, with total estimated annual electricity consumption of approximately 2.6 GWh, equivalent to the energy footprint of a small office building. Emissions are limited to indirect scope 2 emissions, as validators are geographically distributed and use standard computing hardware. Many validators operate using renewable or low-carbon power sources.

Relevant data for the Ethereum network's sustainability indicators can be found here:

- https://www.carbon-ratings.com (Crypto Carbon Ratings Institute reports)
- https://ethereum.org/en/sustainability (Ethereum Foundation – Sustainability Overview)
- https://github.com/ethereum/eth2.0-specs (Consensus specifications and performance benchmarks)

General information	
S.1 Name *Name reported in field A.1*	Ethereum
S.2 Relevant legal entity identifier Identifier referred to in field A.2	N/A – Ethereum is not operated by a central legal entity. Core development is maintained by the Ethereum Foundation (LEI: 2549000V2YXYDJ9OB270)
S.3 Name of the crypto-asset Name of the crypto-asset, as reported in field D.2	Ether (ETH)
S.4 Consensus Mechanism The consensus mechanism, as reported in field H.4	Proof-of-Stake (Ethereum 2.0, post-Merge)
S.5 Incentive Mechanisms and Applicable Fees	Validators stake ETH to participate in consensus and receive rewards from priority fees and protocol issuance. Users pay variable

Incentive mechanisms to secure transactions and any fees applicable, as reported in field H.5	transaction fees calculated via EIP-1559 (base fee + priority tip).
S.6 Beginning of the period to which the disclosure relates	2024-01-01
S.7 End of the period to which the disclosure relates	2024-01-01
Mandatory key indicator on energy consumption	
S.8 Energy consumption Total amount of energy used for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions, expressed per calendar year	~2,600 MWh per year (or 2.6 GWh) for entire Ethereum network (2024 est.)
Sources and methodologies	
S.9 Energy consumption sources and Methodologies Sources and methodologies used in relation to the information reported in field S.8	Based on publicly available estimates from Crypto Carbon Ratings Institute (CCRI) and the Ethereum Foundation's post-Merge emissions report. The estimates are derived from the energy use of validator nodes, not mining hardware. Assumes ~6,000 active validators globally with average energy use of ~0.44 kWh/day per validator.

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

Supplementary key indicators on energy and GHG emissions	
S.10 Renewable energy consumption Share of energy used generated from renewable sources, expressed as a percentage of the total amount of energy used per calendar year, for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions.	Varies by validator; estimated 40–60% of validators run on renewable-powered infrastructure (source: CCRI, Ethereum Foundation surveys).
S.11 Energy intensity Average amount of energy used per validated transaction	Estimated at ~0.03 Wh per transaction (post-Merge)
S.12 Scope 1 DLT GHG emissions – Controlled	Negligible; Ethereum validators do not produce direct emissions.

Scope 1 GHG emissions per calendar year for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions	
S.13 Scope 2 DLT GHG emissions – Purchased Scope 2 GHG emissions, expressed in tCO2e per calendar year for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions	Estimated ~870 tCO_2e/year (2024 estimate from CCRI based on average energy mix)
S.14 GHG intensity Average GHG emissions (scope 1 and scope 2) per validated transaction	~0.00001 kg CO_2e per transaction
Sources and methodologies	
S.15 Key energy sources and methodologies Sources and methodologies used in relation to the information reported in fields S.10 and S.11	Energy source mix based on geographic distribution of validator nodes; methodology from CCRI and peer-reviewed models including Ethereum Foundation's own reporting.
S.16 Key GHG sources and methodologies Sources and methodologies used in relation to the information reported in fields S.12, S.13 and S.14	Scope 2 emissions calculated using location-based emissions factors from IEA and CCRI. Aggregated by estimated node distribution and energy mix.