Flux (FLUX)
White paper

In accordance with Title II of Regulation (EU) 2023/1114 (MiCA)

N	Field	Content
0	Table of content	

01	Date of notification	2025-06-26
02	Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114	This crypto-asset white paper has not been approved by any competent authority in any Member State of the European Union. The operator of the trading platform of the crypto-asset is solely responsible for the content of this crypto-asset white paper.
03	Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114	This crypto-asset white paper complies with Title II of Regulation (EU) 2023/1114 and, to the best of the knowledge of the management body, the information presented in the crypto-asset white paper is fair, clear and not misleading and the crypto-asset white paper makes no omission likely to affect its import.
04	Statement in accordance with Article 6(5), points (a), (b), (c) of Regulation (EU) 2023/1114	The crypto-asset referred to in this white paper may lose its value in part or in full, may not always be transferable and may not be liquid.
05	Statement in accordance with Article 6(5), point (d) of Regulation (EU) 2023/1114	False
06	Statement in accordance with Article 6(5), points (e) and (f) of Regulation (EU) 2023/1114	The crypto-asset referred to in this white paper is not covered by the investor compensation schemes under Directive 97/9/EC of the European Parliament and of the Council. 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 in accordance with Article 6(7), second subparagraph of Regulation (EU) 2023/1114	**Warning** This summary should be read as an introduction to the crypto-asset white paper. The prospective holder should base any decision to purchase this crypto-asset on the content of the crypto-asset white paper as a whole and not on the summary alone. The admission to trading 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	FLUX is a fungible token designed for use within the Flux ecosystem. Its utilities

<table>
<tr><td></td><td></td><td>include facilitating transactions by fee payments, as incentives for miners and node operators, and facilitating governance via the Flux DAO.

FLUX has a fixed maximum supply of 440 000 000 tokens distributed as follows:

<table><tr><th>Category</th><th>Amount</th></tr><tr><td>Parallel Assets*</td><td>47,2%</td></tr><tr><td>Liquidity Mining</td><td>47,5%</td></tr><tr><td>Exchange Liquidity</td><td>1,7%</td></tr><tr><td>Foundation</td><td>2,9%</td></tr><tr><td>Operational Allocation</td><td>0,7%</td></tr></table>
*Parallel assets on the FLUX crypto network are a feature that facilitates cross-chain interoperability. They are tokenized representations of FLUX that exist on multiple blockchain ecosystems.

FLUX tokens are freely transferable, in whole or in part, to third parties, and all associated usage rights and obligations follow the token upon transfer.</td></tr>
<tr><td>09</td><td>Information about the quality and quantity of goods or services to which the utility tokens give access and restrictions on the transferability</td><td>N/A</td></tr>
<tr><td>10</td><td>Key information about the offer to the public or admission to trading</td><td>Kraken seeks admission to trading of the FLUX token so as to be compliant with MiCA and in keeping with its mission to make available for trading to its clients a wide range of assets.</td></tr>
<tr><td colspan="3">Part I – Information on risks</td></tr>
<tr><td>I.1</td><td>Offer-Related Risks</td><td>General Risk Factors Associated with Crypto-Asset Offerings
The admission to trading of crypto-assets, including FLUX, is subject to general risks inherent to the broader cryptocurrency market.

Market Volatility
The value of FLUX may experience substantial fluctuations driven by investor sentiment, macroeconomic developments, and market conditions.</td></tr>
</table>

		Regulatory Risks Changes in legislation, applicable laws, compliance requirements or the implementation of new regulatory frameworks could affect the availability, trading, or use of such assets. **Security Risks** The risk of exploitation, hacking or security vulnerabilities of the underlying protocol and/or contracts of the token leading to a loss. **Reputational Risks** The potential for damage to an organization's credibility or public trust, which can negatively impact stakeholder confidence and overall business viability**.** **Technology Risks** The potential for losses or disruptions caused by failures related to the hardware and software in the underlying protocol the token is issued on. **Liquidity Risks** The ability to buy or sell the asset without significantly affecting its price can result in losses or the inability to exit a position when needed, especially during periods of market stress or low trading volume.
I.2	Issuer-Related Risks	**Financial Stability Risk** The financial condition of the issuer, including challenges in cash flow or profitability, may influence the project's ability to meet its objectives. If financial difficulties arise, they could impact the operations or sustainability of the issuer. **Competition and Business Environment** Flux operates in the web3 cloud computing sector, which is competitive and rapidly evolving. Competing platforms or new technologies could reduce Flux's market share or render its tools less unique. If Flux fails to continue innovating or to respond to competitive pressures, user adoption of its platform (and demand for FLUX) may not grow as projected, posing a risk to the token's utility value. **Legal and Regulatory Risks** Flux must comply with applicable laws and regulations (including those beyond crypto-specific laws, such as data protection and financial regulations). Any legal challenges, regulatory investigations, or compliance failures involving the company could disrupt operations or tarnish its reputation. **Internal Control and Governance Risks** The effectiveness of the issuer's internal controls and operational processes may impact the overall management of the project. Weaknesses in controls, governance and operations could impact the project's ability to meet its goals.

I.3	Crypto-Assets-related Risks	**Market Volatility** The crypto-asset market is subject to significant price volatility, which may affect the value of FLUX. Prices can fluctuate rapidly and unpredictably due to various factors, including market sentiment, economic indicators, technological developments, regulatory news, and macroeconomic trends. This high level of volatility may lead to sudden gains or losses and can impact the liquidity and tradability of the crypto-asset. **Liquidity** Liquidity refers to the ability to buy or sell a crypto-asset without causing significant price impact. FLUX may experience periods of low liquidity, meaning that it could be difficult to enter or exit positions at desired prices or volumes. Reduced liquidity may result from limited market participation, exchange restrictions, or broader market conditions. This can lead to increased price volatility, slippage, and difficulty in executing transactions. **Cybersecurity & Technology Risks** Risks arising from vulnerabilities in the blockchain technology used by the project or platforms. Example risks include smart contract exploits, compromise of platforms, forking scenarios, compromise of cryptographic algorithms. **Adoption Risks** The risk associated with the project not achieving its goals leading to lower than expected adoption and use within the ecosystem, the impact leading to a reduced utility and value proposition. **Custody & Ownership Risk** The risk related to the inadequate safekeeping and control of crypto-assets e.g. loss of private keys, custodian insolvency leading to a loss.
I.4	Project Implementation-Related Risks	**Development Delays or Shortfalls** The success of the Flux project is not guaranteed. There is a risk that the project's technical development or business objectives will not be achieved as planned. Delays or failures in building the cloud computing platform could reduce the utility and demand for FLUX **Adoption and Competition** Competition from other cloud computing platforms could adversely affect the project. If the project fails to meet milestones or usage targets, the utility of FLUX would diminish. **Scaling and Infrastructure:** As usage grows, Flux will need to scale its infrastructure. If the team fails to scale the technology appropriately, users might face poor performance or

		downtime. Any significant technical outages or data inaccuracies on the platform can erode user trust.
I.5	Technology-Related Risks	**Smart contract risks** FLUX uses smart contracts to facilitate automated transactions and processes. While these contracts enhance efficiency and decentralization, they also introduce specific technical risks. Vulnerabilities such as coding errors, design flaws, or security loopholes within the smart contract code may be exploited by malicious actors. Such exploits could result in the loss of assets, unauthorized access to sensitive information, or unintended and irreversible execution of transactions. **Blockchain Network Risks** FLUX operates on a public blockchain infrastructure, which is maintained by a decentralized network of participants. The functionality and reliability of the crypto-asset are dependent on the performance and security of the underlying blockchain. Risks may include network congestion, high transaction fees, delayed processing times, or, in extreme cases, outages and disruptions. Additionally, vulnerabilities or failures in the consensus mechanism, attacks on the network (e.g., 51% attacks), or protocol-level bugs could impact the operation and availability of FLUX. **Risk of Cryptographic Vulnerabilities** Technological advancements, such as quantum computing, could pose potential risks to cryptocurrencies. While this is a long-term and industry-wide risk; it is worth noting that if encryption standards were broken or significantly weakened, the security of all blockchain assets, including FLUX, would be at risk. This could potentially allow bad actors to forge signatures or otherwise manipulate the blockchain. **Privacy** Transactions involving FLUX are recorded on a public blockchain, where transaction data is transparent and permanently accessible. While public addresses do not directly reveal personal identities, transaction histories can be analyzed and, in some cases, linked to individuals through data aggregation or external information sources. This transparency may pose privacy concerns for users seeking confidentiality in their financial activity. Transaction data on public blockchains is not inherently private and could be subject to scrutiny by third parties, including regulators, analytics firms, or malicious actors.
I.6	Mitigation measures	**Reliance on Secure Infrastructure** Flux chose a reputable blockchain network (Ethereum) for FLUX. Ethereum has undergone extensive security audits across its core components to ensure security. While this does not guarantee safety, it means the foundational

		infrastructure is maintained by experienced entities and is subject to scrutiny from the wider blockchain community. **Open-Source Codebase** All core contracts and libraries are released under a permissive licence in a public repository. Anyone may audit or fork the code. Open sourcing boosts transparency and community-driven security. **Geographic Redundancy of Data-hosts** FluxNode operators must meet minimum bandwidth and uptime service level agreements. Geographically dispersed hosting means that regional outages do not interrupt FluxOS workloads network wide. **Bug-Bounty Program** The issuer operates a continuous bug-bounty scheme: external researchers can probe the smart contracts, back-end, and UI, then submit vulnerability reports for potential rewards. These vulnerabilities are then triaged and considered in Flux's broader bounty process. This incentivises rapid detection and resolution of critical issues. It must be stressed that, despite these mitigation efforts, risks remain. The measures above reduce the likelihood or impact of certain events but cannot remove risk entirely from FLUX or the Flux project. Token holders and users should remain prudent and aware of the residual risks described in this white paper.
Part A - Information about the offeror or the person seeking admission to trading		
A.1	Name	N/A
A.2	Legal form	N/A
A.3	Registered address	N/A
A.4	Head office	N/A
A.5	Registration Date	N/A
A.6	Legal entity identifier	N/A
A.7	Another identifier required pursuant to applicable national law	N/A
A.8	Contact telephone number	N/A
A.9	E-mail address	N/A

A.10	Response Time (Days)	N/A
A.11	Parent Company	N/A
A.12	Members of the Management body	N/A
A.13	Business Activity	N/A
A.14	Parent Company Business Activity	N/A
A.15	Newly Established	N/A
A.16	Financial condition for the past three years	N/A
A.17	Financial condition since registration	N/A
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	true
B.2	Name	InFlux Technologies Limited
B.3	Legal form	H0PO - Private Limited Company
B.4	Registered address	Formal House, 60 St. Georges Place, Cheltenham, Gloucestershire, England, GL50 3PN
B.5	Head office	N/A
B.6	Registration Date	2019-08-07
B.7	Legal entity identifier	Unknown
B.8	Another identifier required pursuant to applicable national law	Company number 12144906
B.9	Parent Company	N/A
B.10	Members of the Management body	

Full Name	Business Address	Function
Jeremy Anderson	Formal House, 60 St. Georges Place, Cheltenham, Gloucestershire,	Director

			England, GL50 3PN	
		Simon Timothy Jewell	Formal House, 60 St. Georges Place, Cheltenham, Gloucestershire, England, GL50 3PN	Director
		Daniel Keller	Formal House, 60 St. Georges Place, Cheltenham, Gloucestershire, England, GL50 3PN	Director
		Tadeas Kmenta	Formal House, 60 St. Georges Place, Cheltenham, Gloucestershire, England, GL50 3PN	Director
		Valter Silva	Formal House, 60 St. Georges Place, Cheltenham, Gloucestershire, England, GL50 3PN	Director

B.11	Business Activity	62090 - Other information technology service activities
B.12	Parent Company Business Activity	N/A
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	Payward Global Solutions LTD
C.2	Legal form	N/A
C.3	Registered address	N/A
C.4	Head office	N/A
C.5	Registration Date	2023-07-11
C.6	Legal entity identifier of the operator of the trading platform	9845003D98SCC2851458

<table>
<tr><td>C.7</td><td>Another identifier required pursuant to applicable national law</td><td>N/A</td></tr>
<tr><td>C.8</td><td>Parent Company</td><td>N/A</td></tr>
<tr><td>C.9</td><td>Reason for Crypto-Asset White Paper Preparation</td><td>Kraken seeks admission to trading of the FLUX token so as to be compliant with MiCA and in keeping with its mission to make available for trading to its clients a wide range of assets.</td></tr>
<tr><td>C.10</td><td>Members of the Management body</td><td>
<table>
<tr><th>Full Name</th><th>Business Address</th><th>Function</th></tr>
<tr><td>Shannon Kurtas</td><td>70 Sir John Rogerson's Quay, Dublin 2, Ireland</td><td>Board Member</td></tr>
<tr><td>Andrew Mulvenny</td><td>70 Sir John Rogerson's Quay, Dublin 2, Ireland</td><td>Board Member</td></tr>
<tr><td>Shane O'Brien</td><td>70 Sir John Rogerson's Quay, Dublin 2, Ireland</td><td>Board Member</td></tr>
<tr><td>Laura Walsh</td><td>70 Sir John Rogerson's Quay, Dublin 2, Ireland</td><td>Board Member</td></tr>
<tr><td>Michael Walsh</td><td>70 Sir John Rogerson's Quay, Dublin 2, Ireland</td><td>Board Member</td></tr>
</table>
</td></tr>
<tr><td>C.11</td><td>Operator Business Activity</td><td>PGSL is the operator of a Trading Platform for Crypto Assets, in accordance with Article 3(1)(18) of Regulation (EU) 2023/1114 (MiCA).</td></tr>
<tr><td>C.12</td><td>Parent Company Business Activity</td><td>Payward, Inc., a Delaware, USA corporation, is the parent company of a worldwide group of subsidiaries (the following paragraphs use the term "Payward" or "Payward Group" to refer to the group) collectively doing business as "Kraken." Payward's primary business is the operation of an online virtual asset platform that enables clients to buy and sell virtual assets on a spot basis, including the transfer of crypto-assets to and from external wallets.

Payward, through its various affiliates, offers a number of other services and products, including:
* A trading platform for futures contracts on virtual assets ("Kraken Derivatives");
* A platform for buying and selling NFTs;
* An over-the-counter ("OTC") desk;
* Extensions of margin to support spot trading of virtual assets;
* A benchmark administrator; and
* Staking services.</td></tr>
</table>

C.13	Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	N/A
C.14	Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	N/A
Part D- Information about the crypto-asset project		
D.1	Crypto-asset project name	Flux
D.2	Crypto-assets name	Flux Token
D.3	Abbreviation	FLUX
D.4	Crypto-asset project description	Flux is an open-source, decentralised cloud-infrastructure stack launched in 2018. At its core is a UTXO-based Layer-1 blockchain (fork of Zcash) secured by FluxHash proof-of-work. Flux offers a suite of services, including blockchain-as-a-service solutions, aiming to provide a decentralized alternative to traditional cloud providers. The platform operates through a network of FluxNodes, which are servers distributed globally, contributing to its computational resources.
D.5	Details of all natural or legal persons involved in the implementation of the crypto-asset project	The project is developed and issued by InFlux Technologies Limited, a Private Limited Company incorporated in the United Kingdom with a registered office located at Formal House, 60 St. Georges Place, Cheltenham, Gloucestershire, England, GL50 3PN. The core development team consists of the project's cofounders Daniel Keller, Tadeas Kmenta, and Parker Honeyman, who also serve as Chief Strategy Officer, Chief Information Officer, and Chief Operations Officer, respectively. Additionally, Davy Wittock is the project's, Chief Business Officer, Jeremy Anderson is the Chief Technical Officer, Tim Bukhe is Chief Legal Counsel, Alex Perritaz is Chief Compute Architect, and Darren Williams is Chief AI Officer.
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	Past milestones include the project launch in 2018 as ZelCash. In March 2021, Zelcash was hard-forked and rebranded as Flux. The token's maximum supply was raised to 440 million and the parallel-asset architecture was approved. Please refer to the project team website for any further information regarding future milestones.
D.9	Resource Allocation	2,9 % of the FLUX token supply is held by the Flux Foundation for core-development grants, ecosystem growth, marketing and community programs. Additionally, Flux's operational allocation makes up 0,7% of the token distribution. 50% of every block reward is issued to Proof-of-Work miners, while the other 50% is paid to FluxNode operating, which funds the servers that supply computing power, RAM, and storage to FloxOS users. This aims to ensure a sustainable incentive for miners and node operators.
D.10	Planned Use of Collected Funds or Crypto-Assets	N/A
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	Making secondary trading available to the consumers on the Kraken Trading platform in compliance with the MiCA regulatory framework
E.3	Fundraising Target	N/A
E.4	Minimum Subscription Goals	N/A
E.5	Maximum Subscription Goal	N/A
E.6	Oversubscription Acceptance	N/A
E.7	Oversubscription Allocation	N/A
E.8	Issue Price	N/A

E.9	Official currency or other crypto-assets determining the issue price	N/A
E.10	Subscription fee	N/A
E.11	Offer Price Determination Method	N/A
E.12	Total Number of Offered/Traded crypto-assets	440 000 000 tokens is the maximum supply
E.13	Targeted Holders	ALL
E.14	Holder restrictions	N/A
E.15	Reimbursement Notice	N/A
E.16	Refund Mechanism	N/A
E.17	Refund Timeline	N/A
E.18	Offer Phases	N/A
E.19	Early Purchase Discount	N/A
E.20	Time-limited offer	N/A
E.21	Subscription period beginning	N/A
E.22	Subscription period end	N/A
E.23	Safeguarding Arrangements for Offered Funds/crypto-assets	N/A
E.24	Payment Methods for crypto-asset Purchase	N/A
E.25	Value Transfer Methods for Reimbursement	N/A
E.26	Right of Withdrawal	N/A
E.27	Transfer of Purchased crypto-assets	N/A
E.28	Transfer Time Schedule	N/A

E.29	Purchaser's Technical Requirements	N/A
E.30	crypto-asset service provider (CASP) name	N/A
E.31	CASP identifier	N/A
E.32	Placement form	NTAV
E.33	Trading Platforms name	N/A
E.34	Trading Platforms Market Identifier Code (MIC)	N/A
E.35	Trading Platforms Access	N/A
E.36	Involved costs	N/A
E.37	Offer Expenses	N/A
E.38	Conflicts of Interest	All listings decisions made by Payward Global Solution Ltd are made independently by staff of the entity in line with internal policies. PGSL publishes a conflict of interest disclosure on its website advising of potential conflicts that may arise.
E.39	Applicable law	Any dispute relating to this white paper shall be governed by and construed and enforced in accordance with the laws of Ireland without regard to conflict of law rules or principles (whether of Ireland or any other jurisdiction) that would cause the application of the laws of any other jurisdiction, irrespective of whether FLUX tokens qualify as right or property under the applicable law.
E.40	Competent court	Any disputes or claims arising out of this white paper will be subject to the exclusive jurisdiction of the Irish courts.
Part F - Information about the crypto-assets		
F.1	Crypto-Asset Type	FLUX is classified as a crypto-asset other than an asset referenced token or e-money token under MiCA, (EU) 2023/1114.
F.2	Crypto-Asset Functionality	FLUX functions as the native token of the Flux network. FLUX serves multiple roles within the ecosystem. It acts as the utility token for transactions, incentivizes miners and node operators, and facilitates governance through the Flux decentralized autonomous organization (DAO).
F.3	Planned Application of Functionalities	N/A. All functionalities described in Flux’s roadmap are live.
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	FLUX allows holders to access platform services. FLUX facilitates transactions within the platform, incentivizes miners and node operators, and facilitates governance through the Flux decentralized autonomous organization (DAO).
F.7	Commercial name or trading name	InFlux Technologies Limited
F.8	Website of the issuer	https://runonflux.com/
F.9	Starting date of offer to the public or admission to trading	2018-07-31
F.10	Publication date	2025-07-24
F.11	Any other services provided by the issuer	N/A
F.12	Identifier of operator of the trading platform	PGSL
F.13	Language or languages of the white paper	English
F.14	Digital Token Identifier	Not available
F.15	Functionally Fungible Group Digital Token Identifier	N/A
F.16	Voluntary data flag	Mandatory
F.17	Personal data flag	true
F.18	LEI eligibility	N/A
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
Part G - Information on the rights and obligations attached to the crypto-assets		
G.1	Purchaser Rights and Obligations	**Right of Transfer**

		The holder can transfer the FLUX tokens to third parties. Upon transfer, all rights and obligations are transferred to the new holder. **Trading** If the FLUX token is listed on cryptocurrency exchanges, holders can trade their tokens there. **Access platform Services** Holders of FLUX may use the token to transact on the Flux platform, to receive incentive rewards, and to introduce and vote on governance proposals. **Obligations of FLUX Holders:** There are no mandatory obligations imposed on FLUX purchasers beyond the general terms of use of the platform.
G.2	Exercise of Rights and obligations	**Procedure to Exercise Rights** To use FLUX's utility rights, a holder typically needs to interact with the Flux platform: for instance, a holder connects a wallet that supports FLUX to the FluxOS Marketplace, selects a compute package and signs an on-chain transaction that transfers the quoted FLUX amount to the FluxOS smart-contract. To operate a node, the owner deposits the required collateral to a deterministic address generated by FluxNode software. To participate in on-chain governance, holders will delegate or lock FLUZ in a voting contract and sign a message indicating their choice.
G.3	Conditions for modifications of rights and obligations	The rights and obligations attached to FLUX as described in this white paper reflect information available at the time of issuance. This white paper is issued by Kraken and does not constitute a commitment or guarantee by Flux or any other party regarding future modifications. No promises, warranties, or assurances are made herein regarding future token functionality, and this section is provided solely for informational purposes.
G.4	Future Public Offers	The team has not announced any future public offers of FLUX.
G.5	Issuer Retained Crypto-Assets	12 760 000 FLUX or 2,9% is retained by the foundation.
G.6	Utility Token Classification	false
G.7	Key Features of Goods/Services of Utility Tokens	false
G.8	Utility Tokens Redemption	N/A
G.9	Non-Trading request	This white paper reflects a request to admit the token to trading.

G.10	Crypto-Assets purchase or sale modalities	N/A
G.11	Crypto-Assets Transfer Restrictions	Kraken may, in accordance with applicable laws and internal policies and terms, impose restrictions on buyers and sellers of these tokens.
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
G.16	Compensation Schemes	false
G.17	Compensation Schemes Description	N/A
G.18	Applicable law	Any dispute relating to this white paper shall be governed by and construed and enforced in accordance with the laws of Ireland without regard to conflict of law rules or principles (whether of Ireland or any other jurisdiction) that would cause the application of the laws of any other jurisdiction, irrespective of whether FLUX tokens qualify as right or property under the applicable law.
G.19	Competent court	Any disputes or claims arising out of this white paper will be subject to the exclusive jurisdiction of the Irish courts.
Part H – information on the underlying technology		
H.1	Distributed ledger technology	FLUX is implemented on two blockchains. **Ethereum** Ethereum is a public, permissionless Layer-1 blockchain that is EVM-compatible and reaches consensus through Proof-of-Stake (PoS). Validators stake ETH, propose/attest blocks roughly every 12 seconds and are subject to slashing for malicious behaviour. **Flux Mainnet (Native L1)** Flux's own UTXO-based Layer-1 chain has been live since 31 Jan 2018 (forked from Zcash). Flux Mainnet employs FluxHash (Equihash 125,4) Proof-of-Work, producing blocks every ~2 minutes. GPU miners secure the chain while > 11 000 collateralised FluxNodes run FluxOS to deliver decentralised compute, storage and edge-services.

H.2	Protocols and technical standards	Ethereum Blockchain Protocol + ERC-20: the FLUX token contract follows the ERC-20 standard on Ethereum, ensuring interoperability with wallets, DEXs and DeFi apps. Flux Mainnet layer Native FLUX resides on Flux Mainnet, a UTXO-based chain that forked from Zcash/Bitcoin. Transactions follow Bitcoin-style serialization and are timestamped in blocks produced with FluxHash (Equihash 125,4) Proof-of-Work an ASIC-resistant variant of Equihash designed for GPU mining. The protocol inherits Zcash's Sapling libraries for shielded addresses and uses peer-to-peer gossip plus compact block propagation for network messaging.
H.3	Technology Used	FLUX is held natively as a UTXO coin on Flux Mainnet and, via the non-custodial Fusion bridge in the Zelcore wallet, and as an ERC-20 token on Ethereum.
H.4	Consensus Mechanism	The FLUX token uses the existing ERC-20 fungible token standard on Ethereum and Flux mainnet it uses Proof-of-Work. Ethereum uses a Proof-of-Stake (PoS) consensus mechanism, where validators are selected based on ETH stake to propose and attest to new blocks. Transactions on Ethereum typically take 12 seconds, with strong decentralization and security guarantees. Flux Mainnet relies on FluxHash (Equihash 125-4) Proof-of-Work; GPU miners solve memory-intensive puzzles to produce a block about every 2 minutes, and the longest-chain rule anchors finality. Validator-like FluxNodes (collateralised servers) do not create blocks but supply redundant compute and store chain snapshots.
H.5	Incentive Mechanisms and Applicable Fees	FLUX relies on the existing incentive mechanisms and fee structures of the Ethereum network. Flux Mainnet layer: Proof-of-Work miners and collateralised FluxNodes share each block reward 50 / 50 (currently 37,5 native FLUX per side, halving every 2,5 yrs). Miners also collect transaction fees (≈ 0,0002 – 0,002 FLUX per tx). FluxNodes additionally earn parallel-asset payouts (7,5 units of every live parallel asset per block) and workload-hosting fees paid by FluxOS users.
H.6	Use of Distributed Ledger Technology	False
H.7	DLT Functionality Description	N/A
H.8	Audit	True
H.9	Audit outcome	15 July 2020; FLUX Token Audit (iosiro)

		The security audit revealed: 0 critical issues 0 high issues 0 medium issues 7 informational issues (all acknowledged) 13 December 2024; FLUX ERC-20 Audit (Cyberscope) The security audit revealed: 0 critical issues 0 high issues 0 medium issues 2 minor (acknowledged) 23 Dec 2024 – 3 Jan 2025; Schnorr-MultiSig Wallet Audit (Halborn) The security audit revealed: 0 critical issues 0 high issues 1 medium issue (fixed) 3 low issues (all acknowledged)
Part J - Information on the suitability indicators in relation to adverse impact on the climate and other environment-related adverse impacts		
S.1	Name	Payward Global Solutions Limited
S.2	Relevant legal entity identifier	9845003D98SCC2851458
S.3	Name of the crypto-asset	flux
S.4	Consensus Mechanism	flux is present on the following networks: Binance Smart Chain, Ethereum, Solana, Tron. Binance Smart Chain (BSC) uses a hybrid consensus mechanism called Proof of Staked Authority (PoSA), which combines elements of Delegated Proof of Stake (DPoS) and Proof of Authority (PoA). This method ensures fast block times and low fees while maintaining a level of decentralization and security. Core Components:

		1. Validators (so-called “Cabinet Members”): Validators on BSC are responsible for producing new blocks, validating transactions, and maintaining the network’s security. To become a validator, an entity must stake a significant amount of BNB (Binance Coin). Validators are selected through staking and voting by token holders. There are 21 active validators at any given time, rotating to ensure decentralization and security. 2. Delegators: Token holders who do not wish to run validator nodes can delegate their BNB tokens to validators. This delegation helps validators increase their stake and improves their chances of being selected to produce blocks. Delegators earn a share of the rewards that validators receive, incentivizing broad participation in network security. 3. Candidates: Candidates are nodes that have staked the required amount of BNB and are in the pool waiting to become validators. They are essentially potential validators who are not currently active but can be elected to the validator set through community voting. Candidates play a crucial role in ensuring there is always a sufficient pool of nodes ready to take on validation tasks, thus maintaining network resilience and decentralization. Consensus Process 4. Validator Selection: Validators are chosen based on the amount of BNB staked and votes received from delegators. The more BNB staked and votes received, the higher the chance of being selected to validate transactions and produce new blocks. The selection process involves both the current validators and the pool of candidates, ensuring a dynamic and secure rotation of nodes. 5. Block Production: The selected validators take turns producing blocks in a PoA-like manner, ensuring that blocks are generated quickly and efficiently. Validators validate transactions, add them to new blocks, and broadcast these blocks to the network. 6. Transaction Finality: BSC achieves fast block times of around 3 seconds and quick transaction finality. This is achieved through the efficient PoSA mechanism that allows validators to rapidly reach consensus. Security and Economic Incentives

		7. Staking: Validators are required to stake a substantial amount of BNB, which acts as collateral to ensure their honest behavior. This staked amount can be slashed if validators act maliciously. Staking incentivizes validators to act in the network's best interest to avoid losing their staked BNB. 8. Delegation and Rewards: Delegators earn rewards proportional to their stake in validators. This incentivizes them to choose reliable validators and participate in the network's security. Validators and delegators share transaction fees as rewards, which provides continuous economic incentives to maintain network security and performance. 9. Transaction Fees: BSC employs low transaction fees, paid in BNB, making it cost-effective for users. These fees are collected by validators as part of their rewards, further incentivizing them to validate transactions accurately and efficiently. The crypto-asset's Proof-of-Stake (PoS) consensus mechanism, introduced with The Merge in 2022, replaces mining with validator staking. Validators must stake at least 32 ETH every block a validator is randomly chosen to propose the next block. Once proposed the other validators verify the blocks integrity. The network operates on a slot and epoch system, where a new block is proposed every 12 seconds, and finalization occurs after two epochs (~12.8 minutes) using Casper-FFG. The Beacon Chain coordinates validators, while the fork-choice rule (LMD-GHOST) ensures the chain follows the heaviest accumulated validator votes. Validators earn rewards for proposing and verifying blocks, but face slashing for malicious behavior or inactivity. PoS aims to improve energy efficiency, security, and scalability, with future upgrades like Proto-Danksharding enhancing transaction efficiency. Solana uses a unique combination of Proof of History (PoH) and Proof of Stake (PoS) to achieve high throughput, low latency, and robust security.

		Core Concepts: 1. Proof of History (PoH): - Time-Stamped Transactions: PoH is a cryptographic technique that timestamps transactions, creating a historical record that proves that an event has occurred at a specific moment in time. - Verifiable Delay Function: PoH uses a Verifiable Delay Function (VDF) to generate a unique hash that includes the transaction and the time it was processed. This sequence of hashes provides a verifiable order of events, enabling the network to efficiently agree on the sequence of transactions. 2. Proof of Stake (PoS): - Validator Selection: Validators are chosen to produce new blocks based on the number of SOL tokens they have staked. The more tokens staked, the higher the chance of being selected to validate transactions and produce new blocks. - Delegation: Token holders can delegate their SOL tokens to validators, earning rewards proportional to their stake while enhancing the network's security. Consensus Process: 1. Transaction Validation: Transactions are broadcast to the network and collected by validators. Each transaction is validated to ensure it meets the network’s criteria, such as having correct signatures and sufficient funds. 2. PoH Sequence Generation: A validator generates a sequence of hashes using PoH, each containing a timestamp and the previous hash. This process creates a historical record of transactions, establishing a cryptographic clock for the network.

		3. Block Production: The network uses PoS to select a leader validator based on their stake. The leader is responsible for bundling the validated transactions into a block. The leader validator uses the PoH sequence to order transactions within the block, ensuring that all transactions are processed in the correct order. 4. Consensus and Finalization: Other validators verify the block produced by the leader validator. They check the correctness of the PoH sequence and validate the transactions within the block. Once the block is verified, it is added to the blockchain. Validators sign off on the block, and it is considered finalized. Security and Economic Incentives: 1. Incentives for Validators: - Block Rewards: Validators earn rewards for producing and validating blocks. These rewards are distributed in SOL tokens and are proportional to the validator's stake and performance. - Transaction Fees: Validators also earn transaction fees from the transactions included in the blocks they produce. These fees provide an additional incentive for validators to process transactions efficiently. 2. Security: - Staking: Validators must stake SOL tokens to participate in the consensus process. This staking acts as collateral, incentivizing validators to act honestly. If a validator behaves maliciously or fails to perform, they risk losing their staked tokens. - Delegated Staking: Token holders can delegate their SOL tokens to validators, enhancing network security and decentralization. Delegators share in the rewards and are incentivized to choose reliable validators. 3. Economic Penalties:

		Slashing: Validators can be penalized for malicious behavior, such as double-signing or producing invalid blocks. This penalty, known as slashing, results in the loss of a portion of the staked tokens, discouraging dishonest actions. The Tron blockchain operates on a Delegated Proof of Stake (DPoS) consensus mechanism, designed to improve scalability, transaction speed, and energy efficiency. Core Components: 1. Delegated Proof of Stake (DPoS): Tron uses DPoS, where token holders vote for a group of delegates known as Super Representatives (SRs)who are responsible for validating transactions and producing new blocks on the network. Token holders can vote for SRs based on their stake in the Tron network, and the top 27 SRs (or more, depending on the protocol version) are selected to participate in the block production process. SRs take turns producing blocks, which are added to the blockchain. This is done on a rotational basis to ensure decentralization and prevent control by a small group of validators. 2. Block Production: The Super Representatives generate new blocks and confirm transactions. The Tron blockchain achieves block finality quickly, with block production occurring every 3 seconds, making it highly efficient and capable of processing thousands of transactions per second. 3. Voting and Governance: Tron's DPoS system also allows token holders to vote on important network decisions, such as protocol upgrades and changes to the system's parameters. Voting power is proportional to the amount of TRX (Tron's native token) that a user holds and chooses to stake. This provides a governance system where the community can actively participate in decision-making.

		4. Super Representatives: The Super Representatives play a crucial role in maintaining the security and stability of the Tron blockchain. They are responsible for validating transactions, proposing new blocks, and ensuring the overall functionality of the network. Super Representatives are incentivized with block rewards (newly minted TRX tokens) and transaction feesfor their work.
S.5	Incentive Mechanisms and Applicable Fees	flux is present on the following networks: Binance Smart Chain, Ethereum, Solana, Tron. Binance Smart Chain (BSC) uses the Proof of Staked Authority (PoSA) consensus mechanism to ensure network security and incentivize participation from validators and delegators. Incentive Mechanisms 1. Validators: - Staking Rewards: Validators must stake a significant amount of BNB to participate in the consensus process. They earn rewards in the form of transaction fees and block rewards. - Selection Process: Validators are selected based on the amount of BNB staked and the votes received from delegators. The more BNB staked and votes received, the higher the chances of being selected to validate transactions and produce new blocks. 2. Delegators: - Delegated Staking: Token holders can delegate their BNB to validators. This delegation increases the validator's total stake and improves their chances of being selected to produce blocks. - Shared Rewards: Delegators earn a portion of the rewards that validators receive. This incentivizes token holders to participate in the network’s security and decentralization by choosing reliable validators.

		3. Candidates: Pool of Potential Validators: Candidates are nodes that have staked the required amount of BNB and are waiting to become active validators. They ensure that there is always a sufficient pool of nodes ready to take on validation tasks, maintaining network resilience. 4. Economic Security: - Slashing: Validators can be penalized for malicious behavior or failure to perform their duties. Penalties include slashing a portion of their staked tokens, ensuring that validators act in the best interest of the network. - Opportunity Cost: Staking requires validators and delegators to lock up their BNB tokens, providing an economic incentive to act honestly to avoid losing their staked assets. Fees on the Binance Smart Chain 1. Transaction Fees: - Low Fees: BSC is known for its low transaction fees compared to other blockchain networks. These fees are paid in BNB and are essential for maintaining network operations and compensating validators. - Dynamic Fee Structure: Transaction fees can vary based on network congestion and the complexity of the transactions. However, BSC ensures that fees remain significantly lower than those on the Ethereum mainnet. 2. Block Rewards: Incentivizing Validators: Validators earn block rewards in addition to transaction fees. These rewards are distributed to validators for their role in maintaining the network and processing transactions. 3. Cross-Chain Fees: Interoperability Costs: BSC supports cross-chain compatibility, allowing assets to be transferred between Binance Chain and Binance Smart Chain.

		These cross-chain operations incur minimal fees, facilitating seamless asset transfers and improving user experience. 4. Smart Contract Fees: Deploying and interacting with smart contracts on BSC involves paying fees based on the computational resources required. These fees are also paid in BNB and are designed to be cost-effective, encouraging developers to build on the BSC platform. The crypto-asset's PoS system secures transactions through validator incentives and economic penalties. Validators stake at least 32 ETH and earn rewards for proposing blocks, attesting to valid ones, and participating in sync committees. Rewards are paid in newly issued ETH and transaction fees. Under EIP-1559, transaction fees consist of a base fee, which is burned to reduce supply, and an optional priority fee (tip) paid to validators. Validators face slashing if they act maliciously and incur penalties for inactivity. This system aims to increase security by aligning incentives while making the crypto-asset's fee structure more predictable and deflationary during high network activity. Solana uses a combination of Proof of History (PoH) and Proof of Stake (PoS) to secure its network and validate transactions. Incentive Mechanisms: 1. Validators: - Staking Rewards: Validators are chosen based on the number of SOL tokens they have staked. They earn rewards for producing and validating

		blocks, which are distributed in SOL. The more tokens staked, the higher the chances of being selected to validate transactions and produce new blocks. - Transaction Fees: Validators earn a portion of the transaction fees paid by users for the transactions they include in the blocks. This provides an additional financial incentive for validators to process transactions efficiently and maintain the network's integrity. 2. Delegators: - Delegated Staking: Token holders who do not wish to run a validator node can delegate their SOL tokens to a validator. In return, delegators share in the rewards earned by the validators. This encourages widespread participation in securing the network and ensures decentralization. 3. Economic Security: - Slashing: Validators can be penalized for malicious behavior, such as producing invalid blocks or being frequently offline. This penalty, known as slashing, involves the loss of a portion of their staked tokens. Slashing deters dishonest actions and ensures that validators act in the best interest of the network. - Opportunity Cost: By staking SOL tokens, validators and delegators lock up their tokens, which could otherwise be used or sold. This opportunity cost incentivizes participants to act honestly to earn rewards and avoid penalties. Fees Applicable on the Solana Blockchain Transaction Fees: 1. Low and Predictable Fees: Solana is designed to handle a high throughput of transactions, which helps keep fees low and predictable. The average transaction fee on Solana is significantly lower compared to other blockchains like Ethereum. 2. Fee Structure:

		Fees are paid in SOL and are used to compensate validators for the resources they expend to process transactions. This includes computational power and network bandwidth. 3. Rent Fees: State Storage: Solana charges rent fees for storing data on the blockchain. These fees are designed to discourage inefficient use of state storage and encourage developers to clean up unused state. Rent fees help maintain the efficiency and performance of the network. 4. Smart Contract Fees: Execution Costs: Similar to transaction fees, fees for deploying and interacting with smart contracts on Solana are based on the computational resources required. This ensures that users are charged proportionally for the resources they consume. The Tron blockchain uses a Delegated Proof of Stake (DPoS) consensus mechanism to secure its network and incentivize participation. Incentive Mechanism: 1. Super Representatives (SRs) Rewards: - Block Rewards: Super Representatives (SRs), who are elected by TRX holders, are rewarded for producing blocks. Each block they produce comes with a block reward in the form of TRX tokens. - Transaction Fees: In addition to block rewards, SRs receive transaction fees for validating transactions and including them in blocks. This ensures they are incentivized to process transactions efficiently. 2. Voting and Delegation: - TRX Staking: TRX holders can stake their tokens and vote for Super Representatives (SRs). When TRX holders vote, they delegate their voting

		power to SRs, which allows SRs to earn rewards in the form of newly minted TRX tokens. - Delegator Rewards: Token holders who delegate their votes to an SR can also receive a share of the rewards. This means delegators share in the block rewards and transaction fees that the SR earns. - Incentivizing Participation: The more tokens a user stakes, the more voting power they have, which encourages participation in governance and network security. 3. Incentive for SRs: SRs are also incentivized to maintain the health and performance of the network. Their reputation and continued election depend on their ability to produce blocks consistently and efficiently process transactions. Applicable Fees: 1. Transaction Fees: - Fee Calculation: Users must pay transaction fees to have their transactions processed. The transaction fee varies based on the complexity of the transaction and the network's current demand. This is paid in TRX tokens. Transaction - Fee Distribution: Transaction fees are distributed to Super Representatives (SRs), giving them an ongoing income to maintain and support the network. 2. Storage Fees: Tron charges storage fees for data storage on the blockchain. This includes storing smart contracts, tokens, and other data on the network. Users are required to pay these fees in TRX tokens to store data. 3. Energy and Bandwidth:

		Energy: Tron uses a resource model that allows users to access network resources like bandwidth and energy through staking. Users who stake their TRX tokens receive \energy
S.6	Beginning of the period to which the disclosure relates	2024-06-20
S.7	End of the period to which the disclosure relates	2025-06-20
S.8	Energy consumption	52.09916 kWh/a
S.9	Energy consumption sources and methodologies	The energy consumption of this asset is aggregated across multiple components: To determine the energy consumption of a token, the energy consumption of the network(s) binance_smart_chain, ethereum, solana, tron is calculated first. For the energy consumption of the token, a fraction of the energy consumption of the network is attributed to the token, which is determined based on the activity of the crypto-asset within the network. When calculating the energy consumption, the Functionally Fungible Group Digital Token Identifier (FFG DTI) is used - if available - to determine all implementations of the asset in scope. The mappings are updated regularly, based on data of the Digital Token Identifier Foundation. The information regarding the hardware used and the number of participants in the network is based on assumptions that are verified with best effort using empirical data. In general, participants are assumed to be largely economically rational. As a precautionary principle, we make assumptions on the conservative side when in doubt, i.e. making higher estimates for the adverse impacts.