Derive (DRV)
White paper

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

N	Field	Content	
0	Table of content

01	Date of notification	2025-06-19
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	DRV is a crypto-asset designed for use within the Derive platform ecosystem. It primarily serves governance and incentive functions in the project's decentralized protocol. Holders of DRV can stake their tokens to participate in protocol governance (influencing decisions on platform parameters and upgrades) and earn rewards for supporting the network. DRV was airdropped 1:1 to LYRA holders on Ethereum using a snapshot taken on May 8th, 2024. There was no dilution to eligible LYRA holders, with the same total supply of 1 000 000 000 DRV. All token holders have the right to transfer DRV tokens to third parties at their discretion, subject only to standard network fees and conditions. All associated usage rights and obligations follow the token upon transfer.
09	Information about the quality and quantity of goods or services to which the utility tokens give access and restrictions on the transferability	N/A
10	Key information about the offer to the public or admission to trading	Kraken seeks admission to trading of the DRV 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.

Part I – Information on risks		
I.1	Offer-Related Risks	**General Risk Factors Associated with Crypto-Asset Offerings** The admission to trading of crypto-assets, including DRV, is subject to general risks inherent to the broader cryptocurrency market. **Market Volatility** The value of DRV may experience substantial fluctuations driven by investor sentiment, macroeconomic developments, and market conditions. **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.
I.2	Issuer-Related Risks	**Operational and Financial Risk** The success of Derive and the value of DRV depend on the issuer's ability to continue developing and operating the platform. If the entity behind Derive or the core team faces financial difficulties, insufficient funding, or operational failures, the development and maintenance of the project could be jeopardized, adversely affecting DRV holders. **Legal and Regulatory Risk for Issuer** The issuer and affiliated entities may be subject to changing laws, government actions, or legal disputes in relevant jurisdictions. Any regulatory sanctions, lawsuits, or compliance failures involving the issuer could damage the project's reputation or limit the functionality and value of DRV. **Governance and Internal Control Risk** As Derive is governed by a DAO, there is a risk of ineffective decision-making or conflicts of interest within the governance process. Poor governance (for example, low community participation or dominance by a small group) or weaknesses in the issuer's internal controls could result in suboptimal decisions or security oversights, potentially harming the project's viability and the interests of DRV holders.

I.3	Crypto-Assets-related Risks	**Market Volatility** The crypto-asset market is subject to significant price volatility, which may affect the value of DRV. 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. DRV 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 Failures** There is a risk that certain promised or expected features are delayed or not delivered. Such delays or failures in delivering core features could directly impact the usefulness of DRV. If advanced capabilities or updates are not implemented on schedule or at all, it may reduce confidence in the project and thus affect DRV's value and demand. **Operational Dependencies** The implementation of the Derive platform relies on various components and partners: for instance, an off-chain orderbook system, oracle services for price feeds, and integrations with user wallets. Any failure or performance issue in one of these components (e.g., an oracle malfunction or wallet integration bug) could disrupt the platform's operation. This could hinder users from utilizing the platform or DRV as intended, thereby posing a risk to the project's success.

		Human Resources and Key Personnel The project's execution depends on the expertise and continuity of the development team and contributors. Loss of key team members or inability to attract and retain skilled personnel could slow down or compromise the implementation of the project. A diminished team capacity may result in project delays, reduced innovation, or quality issues in the protocol, which in turn pose a risk to the value and utility of DRV.
I.5	Technology-Related Risks	**Smart contract risks** DRV 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** DRV operates on Ethereum 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 DRV. For the Derive Layer-2, which relies on optimistic rollup technology, there are risks of downtime or failure of the sequencer, delays in fraud proof submission, or other issues that might affect the timely finalization of Layer-2 transactions. In extreme cases, vulnerabilities in the rollup protocol could result in loss or theft of funds on the Layer-2. **Risk of Cryptographic Vulnerabilities** Technological advancements, such as quantum computing, could pose potential risks to cryptocurrencies. **Privacy** Transactions involving DRV 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. Participants should be

		aware that 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	**Code Audits** The Derive project has subjected its smart contracts to third-party security audits prior to launch. These audits help identify and address vulnerabilities, thereby reducing (though not eliminating) the risk of smart contract failures. **Insurance Fund** The platform's design includes an on-chain insurance fund that accumulates a portion of trading fees to cover unexpected losses or shortfalls. This fund could mitigate the impact on users in case of certain adverse events (for example, to partially compensate for losses in a hack or insolvency of a liquidity pool), though it may not cover all possible losses. **Gradual Decentralization and Governance** The project employs a DAO governance model, which spreads decision-making power among DRV holders. This community oversight can act as a check on unilateral risky actions by any single party and allows for collective decision-making to address new risks.

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	Lyra Foundation
B.3	Legal form	Foundation
B.4	Registered address	PO Box 144, 3119 9 Forum Lane, Camana Bay, George Town, Grand Cayman KY1- 9006, Cayman Islands
B.5	Head office	N/A
B.6	Registration Date	Unknown
B.7	Legal entity identifier	Unknown
B.8	Another identifier required pursuant to applicable national law	Unknown
B.9	Parent Company	Unknown
B.10	Members of the Management body	Unknown
B.11	Business Activity	Unknown

B.12		
	Parent Company Business Activity	Unknown

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	11-07-2023
C.6	Legal entity identifier of the operator of the trading platform	9845003D98SCC2851458
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	Kraken seeks admission to trading of the DRV 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.

C.10	Members of the Management body			
		Full Name	**Business Address**	**Function**
		Shannon Kurtas	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Board Member
		Andrew Mulvenny	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Board Member
		Shane O'Brien	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Board Member
		Laura Walsh	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Board Member
		Michael Walsh	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Board Member
C.11	Operator Business Activity	PGSL is the operator of a Trading Platform for Crypto Assets, in accordance with Article 3(1)(18) of Regulation (EU) 2023/1114 (MiCA).		
C.12	Parent Company Business Activity	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.		

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	Derive
D.2	Crypto-assets name	Derive
D.3	Abbreviation	DRV
D.4	Crypto-asset project description	Derive is a decentralized derivatives protocol that enables on-chain trading of options, perpetual futures, and spot trading. The platform provides a composable ecosystem for advanced financial contracts, combining an automated market maker for options liquidity with an off-chain matcher for efficient trade execution. The Derive Chain is an Optimistic Rollup built using the OP Stack (settling on Ethereum). The project is governed by the Derive DAO, composed of DRV token holders who propose and vote on upgrades and parameter changes.

D.5	Details of all natural or legal persons involved in the implementation of the crypto-asset project	Lyra Technologies Corp: Development company leading the building and maintenance of the Derive protocol and platform. Incorporated in Panama The Lyra Foundation was set up as a not-for-profit legal entity whose mandate is to support Derive's (formerly Lyra's) decentralised growth on behalf of the DAO. The Lyra Foundation's address is PO Box 144, 3119 9 Forum Lane, Camana Bay, George Town, Grand Cayman KY1- 9006, Cayman Islands Core Development Team: Key project contributors include co-founders Michael Spain, Nick Forster, and Jake Fitzgerald, who oversee engineering, operations, and product development respectively. Derive DAO: The decentralized community of DRV token holders that governs the project's ongoing development and parameters.
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	The Derive project originated as Lyra in 2021, focusing on on-chain options AMMs. A community governance proposal to launch the new DRV token and expanded Derive platform was approved on 24 September 2024. The DRV token was subsequently launched on 15 January 2025, completing a 1:1 token migration for LYRA holders. Refer to the project team website for any further information regarding future milestones.
D.9	Resource Allocation	$6.3 million in private financing, raised across two rounds ($3.3 m seed/DAO round in July 2021 and $3 m strategic round in November 2022). 500 000 OP ecosystem-development tokens (Optimism Governance Fund, October 2024). In-protocol revenues (trading & gas fees) and the DAO's DRV treasury continue to fund ongoing development, audits, and liquidity-incentive programs.

D.10	Planned Use of Collected Funds or Crypto-Assets	Refer to the project team website for any further information regarding planned use of collected funds.

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	1 000 000 000 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 conflicts 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 DRV 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	DRV 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	DRV functions as the governance and incentive token within the Derive ecosystem. Holders of DRV can stake their tokens to participate in on-chain governance of the protocol. DRV also acts as a reward mechanism. Users are granted DRV tokens for contributing to the platform (for example, by providing liquidity or trading on the exchange, as part of weekly incentive programs).
F.3	Planned Application of Functionalities	All core functionalities 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	DRV allows holders to participate in governance, the incentive program, and transfer their tokens freely.
F.7	Commercial name or trading name	Lyra Foundation
F.8	Website of the issuer	https://www.derive.xyz/
F.9	Starting date of offer to the public or admission to trading	2025-01-15

F.10	Publication date	2025-07-17
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	**Rights of DRV Holders:** Holders of DRV are entitled to utilize the token within the Derive ecosystem as described. Holders can stake DRV for rewards and to participate in governance. **Obligations of DRV Holders:** There are no mandatory obligations imposed on DRV purchasers beyond the general terms of use of the platform. **Transferability and Trading:** Holders have the ability to transfer their DRV tokens to others (on-chain) or to trade them on available markets at will. Ownership of DRV carries with it the aforementioned access rights, and when a token is transferred, those rights pass to the new holder. The previous holder loses access once they no longer hold the token. This means all rights (which are usage rights) are fully transferable with the token.
G.2	Exercise of Rights and obligations	Procedure and conditions for the exercise of rights
G.3	Conditions for modifications of rights and obligations	The rights and obligations attached to DRV 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 Derive 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 project team has not indicated a planned future public offerings of DRV.
G.5	Issuer Retained Crypto-Assets	200 000 000 (20% of the maximum supply) DRV was allocated to the core team
G.6	Utility Token Classification	false

G.7	Key Features of Goods/Services of Utility Tokens	N/A
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 DRV 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	DRV is implemented on Ethereum and Derive. **Ethereum** Ethereum is a public, open-access blockchain that reaches consensus through Proof-of-Stake (PoS). **Derive Layer-2** DRV is also deployed on the Derive Chain, an EVM-compatible Layer-2 network built using optimistic rollup technology. The Derive Chain derives its security from Ethereum, transaction data from the Layer-2 is periodically published to Ethereum. This rollup design provides improved scalability and faster settlement for DRV transactions while relying on Ethereum's robust security for finality.
H.2	Protocols and technical standards	The DRV token is based on the Ethereum and Derive protocols, which utilize Distributed-Ledger Technology. These protocols provide the foundation for secure transactions and smart contracts. ERC20 Token Standard: The ERC20 standard is a technical protocol for issuing and managing tokens, ensuring that the DRV token is compatible with most wallets, exchanges, and decentralized applications (DApps).
H.3	Technology Used	The DRV token uses the existing ERC-20 fungible token standards on Ethereum and Derive Chain.
H.4	Consensus Mechanism	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.

		Derive Chain leverages optimistic rollups to scale Ethereum. DRV transactions are executed off-chain and submitted to Ethereum in batches, with finality usually taking 20-30 minutes. Transactions on the Derive Chain typically confirm in about 2 seconds.
H.5	Incentive Mechanisms and Applicable Fees	DRV relies on the existing incentive mechanisms and fee structures of the Ethereum blockchain. On the Derive Chain, users pay L2 gas (typically ETH) to the sequencer, which batches transactions to L1 and earns the sequencer fee spread.
H.6	Use of Distributed Ledger Technology	true
H.7	DLT Functionality Description	Ethereum is operated by a decentralized network of validators Derive Chain is an OP-Stack optimistic roll-up (Layer 2). Block production on the Derive Chain is performed by a single sequencer infrastructure run by Conduit, an independent roll-up-infrastructure provider engaged by Derive. Transaction data is periodically posted to Ethereum, and any invalid state transitions can be challenged with fraud proofs.
H.8	Audit	true
H.9	Audit outcome	Sigma Prime Smart-Contract Security Review v2.0 (Sep 2024) 25 issues (4 critical, 2 high). All critical & high issues resolved prior to report release Sigma Prime Smart-Contract Security Review v2.1 – Round 2 (Jan 2025) 10 issues (1 critical, 1 high). Both issues were closed or fully mitigated before mainnet deployment; no outstanding critical vulnerabilities
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	derive
S.4	Consensus Mechanism	derive is present on the following networks: Arbitrum, Base, Ethereum, Optimism.

Arbitrum is a Layer 2 solution on top of Ethereum that uses Optimistic Rollups to enhance scalability and reduce transaction costs. It assumes that transactions are valid by default and only verifies them if there's a challenge (optimistic).

Core Components:
- Sequencer: Orders transactions and creates batches for processing.
- Bridge: Facilitates asset transfers between Arbitrum and Ethereum.
- Fraud Proofs: Protect against invalid transactions through an interactive verification process.

Verification Process:

1. Transaction Submission: Users submit transactions to the Arbitrum Sequencer, which orders and batches them.
2. State Commitment: These batches are submitted to Ethereum with a state commitment.
3. Challenge Period: Validators have a specific period to challenge the state if they suspect fraud.
4. Dispute Resolution: If a challenge occurs, the dispute is resolved through an iterative process to identify the fraudulent transaction. The final operation is executed on Ethereum to determine the correct state.
5. Rollback and Penalties: If fraud is proven, the state is rolled back, and the dishonest party is penalized.

Security and Efficiency: The combination of the Sequencer, bridge, and interactive fraud proofs ensures that the system remains secure and efficient. By minimizing on-chain data and leveraging off-chain computations, Arbitrum can provide high throughput and low fees.

Base is a Layer-2 (L2) solution on Ethereum that was introduced by Coinbase and developed using Optimism's OP Stack. L2 transactions do not have their own consensus mechanism and are only validated by the execution clients. The so-called sequencer regularly bundles stacks of L2 transactions and publishes them on the L1 network, i.e. Ethereum. Ethereum's consensus mechanism (Proof-of-stake) thus indirectly secures all L2 transactions as soon as they are written to L1.

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 block's 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.

Optimism is a Layer 2 scaling solution for Ethereum that uses Optimistic Rollups to increase transaction throughput and reduce costs while inheriting the security of the Ethereum main chain.
Core Components:

1. Optimistic Rollups:
    - Rollup Blocks: Transactions are batched into rollup blocks and processed off-chain.
    - State Commitments: The state of these transactions is periodically committed to the Ethereum main chain.
2. Sequencers:
    - Transaction Ordering: Sequencers are responsible for ordering transactions and creating batches.
    - State Updates: Sequencers update the state of the rollup and submit these updates to the Ethereum main chain.
    - Block Production: They construct and execute Layer 2 blocks, which are then posted to Ethereum.
3. Fraud Proofs:
    - Assumption of Validity: Transactions are assumed to be valid by default.
    - Challenge Period: A specific time window during which anyone can challenge a transaction by submitting a fraud proof.
    - Dispute Resolution: If a transaction is challenged, an interactive verification game is played to determine its validity. If fraud is detected, the invalid state is rolled back, and the dishonest participant is penalized.

Consensus Process:
    1. Transaction Submission: Users submit transactions to the sequencer, which orders them into batches.
    2. Batch Processing: The sequencer processes these transactions off-chain, updating the Layer 2 state.
    3. State Commitment: The updated state and the batch of transactions are periodically committed to the Ethereum main chain. This is done by posting the state root (a cryptographic hash representing the state) and transaction data as call data on Ethereum.
    4. Fraud Proofs and Challenges: Once a batch is posted, there is a challenge period during which anyone can submit a fraud proof if they believe a transaction is invalid.

		- Interactive Verification: The dispute is resolved through an interactive verification game, which involves breaking down the transaction into smaller steps to identify the exact point of fraud. - Rollbacks and Penalties: If fraud is proven, the batch is rolled back, and the dishonest actor loses their staked collateral as a penalty. 5. Finality: After the challenge period, if no fraud proof is submitted, the batch is considered final. This means the transactions are accepted as valid, and the state updates are permanent.
S.5	Incentive Mechanisms and Applicable Fees	derive is present on the following networks: Arbitrum, Base, Ethereum, Optimism. Arbitrum One, a Layer 2 scaling solution for Ethereum, employs several incentive mechanisms to ensure the security and integrity of transactions on its network. The key mechanisms include: 1. Validators and Sequencers: - Sequencers are responsible for ordering transactions and creating batches that are processed off-chain. They play a critical role in maintaining the efficiency and throughput of the network. - Validators monitor the sequencers' actions and ensure that transactions are processed correctly. Validators verify the state transitions and ensure that no invalid transactions are included in the batches. 2. Fraud Proofs: - Assumption of Validity: Transactions processed off-chain are assumed to be valid. This allows for quick transaction finality and high throughput. - Challenge Period: There is a predefined period during which anyone can challenge the validity of a transaction by submitting a fraud proof. This mechanism acts as a deterrent against malicious behavior. - Dispute Resolution: If a challenge is raised, an interactive verification process is initiated to pinpoint the exact step where fraud occurred. If the challenge is valid, the fraudulent transaction is reverted, and the dishonest actor is penalized. 3. Economic Incentives: - Rewards for Honest Behavior: Participants in the network, such as validators and sequencers, are incentivized through rewards for performing their duties honestly and efficiently. These rewards come from transaction fees and potentially other protocol incentives. - Penalties for Malicious Behavior: Participants who engage in dishonest behavior or submit invalid transactions are penalized. This can include slashing of staked tokens or other forms of economic penalties, which serve to discourage malicious actions. Fees on the Arbitrum One Blockchain

1. Transaction Fees:
   - Layer 2 Fees: Users pay fees for transactions processed on the Layer 2 network. These fees are typically lower than Ethereum mainnet fees due to the reduced computational load on the main chain.
   - Arbitrum Transaction Fee: A fee is charged for each transaction processed by the sequencer.This fee covers the cost of processing the transaction and ensuring its inclusion in a batch.
2. L1 Data Fees:
   - Posting Batches to Ethereum: Periodically, the state updates from the Layer 2 transactions are posted to the Ethereum mainnet as call data. This involves a fee, known as the L1 data fee, which accounts for the gas required to publish these state updates on Ethereum.
   - Cost Sharing: Because transactions are batched, the fixed costs of posting state updates to Ethereum are spread across multiple transactions, making it more cost-effective for users.

Base is a Layer-2 (L2) solution on Ethereum that uses optimistic rollups provided by the OP Stack on which it was developed. Transactions on base are bundled by a, so called, sequencer and the result is regularly submitted as a Layer-1 (L1) transaction. This way many L2 transactions get combined into a single L1 transaction. This lowers the average transaction cost per transaction, because many L2 transactions together fund the transaction cost for the single L1 transaction. This creates incentives to use base rather than the L1, i.e. Ethereum, itself.
To get crypto-assets in and out of base, a special smart contract on Ethereum is used. Since there is no consensus mechanism on L2 an additional mechanism ensures that only existing funds can be withdrawn from L2. When a user wants to withdraw funds, that user needs to submit a withdrawal request on L1. If this request remains unchallenged for a period of time the funds can be withdrawn. During this time period any other user can submit a fault proof, which will start a dispute resolution process. This process is designed with economic incentives for correct behaviour.

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.

Optimism, an Ethereum Layer 2 scaling solution, uses Optimistic Rollups to increase transaction throughput and reduce costs while maintaining security and decentralization.

Incentive Mechanisms:
1. Sequencers:
   - Transaction Ordering: Sequencers are responsible for ordering and batching transactions off-chain. They play a critical role in maintaining the efficiency and speed of the network.
   - Economic Incentives: Sequencers earn transaction fees from users. These fees incentivize sequencers to process transactions quickly and accurately.
2. Validators and Fraud Proofs:
   - Assumption of Validity: In Optimistic Rollups, transactions are assumed to be valid by default. This allows for quick transaction finality.
   - Challenge Mechanism: Validators (or anyone) can challenge the validity of a transaction by submitting a fraud proof during a specified challenge period. This mechanism ensures that invalid transactions are detected and reverted.
   - Challenge Rewards: Successful challengers are rewarded for identifying and proving fraudulent transactions. This incentivizes participants to actively monitor the network for invalid transactions, thereby enhancing security.
3. Economic Penalties:
   - Fraud Proof Penalties: If a sequencer includes an invalid transaction and it is successfully challenged, they face economic penalties, such as losing a portion of their staked collateral. This discourages dishonest behavior.
   - Inactivity and Misbehavior: Validators and sequencers are also incentivized to remain active and behave correctly, as inactivity or misbehavior can lead to penalties and loss of rewards.

Fees Applicable on the Optimism Layer 2 Protocol:
1. Transaction Fees:
   - Layer 2 Transaction Fees: Users pay fees for transactions processed on the Layer 2 network. These fees are generally lower than Ethereum mainnet fees due to the reduced computational load on the main chain.
   - Cost Efficiency: By batching multiple transactions into a single batch, Optimism reduces the overall cost per transaction, making it more economical for users.

		2. L1 Data Fees:

		- Posting Batches to Ethereum: Periodically, the state updates from Layer 2 transactions are posted to the Ethereum mainnet as calldata. This involves a fee known as the L1 data fee, which covers the gas cost of publishing these state updates on Ethereum.
		    - Cost Sharing: The fixed costs of posting state updates to Ethereum are spread across multiple transactions within a batch, reducing the cost burden on individual transactions.
		3. Smart Contract Fees:
		    Execution Costs: Fees for deploying and interacting with smart contracts on Optimism are based on the computational resources required. This ensures that users are charged proportionally for the resources they consume.

S.6	Beginning of the period to which the disclosure relates	2024-05-28
S.7	End of the period to which the disclosure relates	2025-05-28
S.8	Energy consumption	13.52371 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) arbitrum, base, ethereum, optimism 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.