Cyber (CYBER)
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.

<table>
<tr><td colspan="3">Summary</td></tr>
<tr><td>07</td><td>Warning in accordance with Article 6(7), second subparagraph of Regulation (EU) 2023/1114</td><td>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.</td></tr>
<tr><td>08</td><td>Characteristics of the crypto-asset</td><td>CYBER is the native governance token of the Cyber Protocol, a decentralized social network infrastructure that allows users to own and control their digital identities, content, and social connections across Web3 applications.

CYBER has a maximum supply of 100 000 000 distributed as follows:

<table>
<tr><th>Category</th><th>Allocation</th></tr>
<tr><td>Private sale</td><td>25,12%</td></tr>
<tr><td>Team & advisors</td><td>15%</td></tr>
<tr><td>Community treasury</td><td>10,88%</td></tr>
<tr><td>Developer community</td><td>10%</td></tr>
<tr><td>Marketing</td><td>10%</td></tr>
<tr><td>Ecosystem partners</td><td>9%</td></tr>
<tr><td>Community rewards</td><td>9%</td></tr>
<tr><td>Early integration partners</td><td>5%</td></tr>
<tr><td>CoinList public sale</td><td>3%</td></tr>
<tr><td>Binance Launchpool</td><td>3%</td></tr>
</table>

CYBER 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>
</table>

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 CYBER 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 CYBER, is subject to general risks inherent to the broader cryptocurrency market. **Market Volatility** The value of CYBER 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	**Lack of Operating History** The Cyber project (and the Cyber Foundation as issuer) is relatively new and does not have a long track record. This means the management and technical team are operating a novel network without years of operational history, which

		could lead to unforeseen challenges. There is a risk that the Foundation or core team might not successfully execute the project's vision on time or on budget. **Key Personnel and Dependency on Core Team** The development of Cyber relies on a small number of key developers and leaders (the founding team and core engineers). The departure of one or more important team members, or any internal team issues, could adversely affect the project's progress and success. **Legal and Organizational Risk** The Cyber Foundation is based in the Cayman Islands, and changes in that jurisdiction's laws or its regulatory status could impact its ability to support the project. Additionally, as a foundation company, it is designed to eventually hand over governance to the community (CyberDAO); during this transition, there could be uncertainties in accountability. If the Foundation were to be dissolved or face legal action, it could disrupt project funding or operations. However, the decentralized nature of the network is intended to mitigate single-point failure risk.
I.3	Crypto-Assets-related Risks	**Market Volatility** The crypto-asset market is subject to significant price volatility, which may affect the value of CYBER. 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. CYBER 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. **Token Concentration Risk** A relatively small number of entities (such as the project team and early investors) hold a significant portion of the CYBER supply. For example, the team and private investors collectively were allocated around 40%+ of the total supply. If these major holders choose to sell their tokens, it could put downward pressure on the market price and reduce confidence. Moreover, large holders could potentially exert outsized influence on governance if they stake their tokens (though governance processes are one-token-one-vote, high concentration can skew decisions). **Governance Outcome Risk** While decentralized governance is a feature, there is a risk that governance decisions made by CYBER holders could negatively impact some stakeholders. For instance, proposals could pass that introduce unfavorable economic policies. If governance is dominated by a small group (due to the concentration mentioned), the broader community's interests might not always prevail.
I.4	Project Implementation-Related Risks	**Development Delays or Shortfalls** There is a risk that some of the planned features could be delayed or not fully achieved as scheduled. Technical challenges may slow development. Any significant delay in delivering promised functionality could affect community trust and the token's utility prospects. **Third-Party Dependency** Cyber relies on external technologies and partners such as the Optimism OP Stack and EigenLayer. If any of these third-party providers encounter problems or change their technology (for example, if EigenLayer's EigenDA is delayed or if Optimism's stack has a critical bug), the Cyber project may suffer setbacks. Dependence on LayerZero for bridging means that issues in LayerZero's protocol (security or performance) could hinder CYBER transfers across chains, impacting user experience. **Resource and Funding Risk** While the project has raised funds, sustained development requires continuous resources. If expenditures exceed budget or if additional funding is needed later, there is a risk the project might face a shortfall. Market conditions can impact the value of the treasury (which may be partly held in CYBER or other crypto), potentially reducing available funding if crypto prices drop significantly.

		Scaling and User Growth Risk Building a social network platform requires achieving network effects. There is a risk that even if the technology is delivered on time, the project might not scale to the level of mainstream usage due to user acquisition challenges. This is more of an adoption risk, but it also ties to implementation: features like account abstraction and low fees are meant to drive adoption. If they are not implemented effectively, the onboarding of non-crypto-savvy users could stall.
I.5	Technology-Related Risks	**Smart contract risks** CYBER 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** CYBER 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 CYBER. **Risk of Cryptographic Vulnerabilities** Technological advancements, such as quantum computing, could pose potential risks to cryptocurrencies. **Privacy** Transactions involving CYBER 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. **Cross-Chain Bridge Risks** CYBER is designed to be omnichain, using LayerZero's protocol to operate

		across multiple blockchains. Cross-chain bridges historically have been targets for attacks; an incident on the bridging infrastructure could cause a disparity in CYBER tokens across networks or loss of pegged tokens. For example, if the LayerZero messaging or the OFT Adapter/Controller contracts were compromised, CYBER tokens might be minted or unlocked incorrectly on a chain, affecting the token's value or supply integrity. Users bridging CYBER also face the risk of delays or failures in transfer due to technical issues. **Restaking and Consensus Risks** The Cyber network's security partly relies on Ethereum restaking via EigenLayer (Ethereum validators restaking ETH to secure Cyber). This novel security model carries risks: if Ethereum's validators or the restaking mechanism fail (e.g., a large portion of restaked ETH validators go offline or act maliciously), Cyber's security could be undermined. There is also slashing risk: malicious actions by Cyber's validators could lead to their staked ETH (restaked) being slashed, which in extreme cases could erode confidence in Cyber's validator set or reduce willingness to participate in validation. Additionally, any critical issue in the EigenLayer protocol could indirectly impact Cyber.
I.6	Mitigation measures	**Security Audit** All contracts that underpin CYBER's OFT implementation were subjected to extensive internal and external security audits in collaboration with LayerZero Labs and specialist audit teams prior to main-net deployment. Cyber itself has also undergone an audit by CertiK. This audit process helps identify and address potential vulnerabilities, thereby reducing the risk of smart contract failures or exploits. **Validator Slashing** Cyber's security stack (EigenDA data-availability and CyberDB storage AVS) imposes slashing on restaked-ETH validators or storage nodes that act maliciously or fail performance requirements, providing economic deterrence. **Community Governance** CYBER stakers govern protocol parameters on-chain via CyberDAO; this decentralised process lets the community adjust rewards, fees or and other things in response to emerging risks. **Open-Source Codebase** Core protocol and contract code is published in public repositories under the cyberconnect GitHub organisation, enabling continuous peer review and community-driven security contributions.
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	Cyber Foundation
B.3	Legal form	Foundation
B.4	Registered address	Not available
B.5	Head office	Unknown
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

<table>
<tr><td>C.6</td><td>Legal entity identifier of the operator of the trading platform</td><td>9845003D98SCC2851458</td></tr>
<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 CYBER 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</td></tr>
</table>

		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	Cyber
D.2	Crypto-assets name	Cyber

D.3	Abbreviation	CYBER
D.4	Crypto-asset project description	Cyber is a restaked Ethereum Layer-2 (L2) blockchain built with the Optimism OP Stack to serve Web3 social applications. The network leverages EigenLayer's EigenDA for data availability, giving it sub-cent transaction costs and high throughput for storing social-graph data. **Architecture highlights** • Native account abstraction (EIP-7560 smart-account EOAs with Passkey/WebAuthn login) enables seedless wallets and gas sponsorship for mainstream UX. • Dual-staking security: validators post both CYBER and restaked ETH; mis-behaviour is deterred by slashing. • A roadmap to a decentralised sequencer + verifier set further reduces censorship risk Cyber aligns with the Optimism Superchain, remaining fully EVM-compatible and inheriting Ethereum security. The native token CYBER powers governance (CyberDAO) and network staking, while the LayerZero OFT standard lets CYBER move across Ethereum, BNB Chain, Optimism, and Cyber L2. By combining EigenDA scalability, Ethereum-aligned security, and social-specific tooling, Cyber aims to provide censorship-resistant, user-owned social networks that match Web2 ease-of-use while granting Web3 sovereignty.
D.5	Details of all natural or legal persons involved in the implementation of the crypto-asset project	**Core Development Team** The project was founded by Wilson Wei, Ryan Li, Shiyu Zhang, and Zhimao Liu in 2021. Development and engineering are led by Cybertino Inc., the company behind the CyberConnect protocol, with a team of engineers and product developers. The Cyber Foundation (Cayman Islands) oversees governance structuring and legal compliance, providing a formal legal vehicle to support CyberDAO. **Key Partners and Service Providers** AltLayer (infrastructure partner) manages the rollup's technical deployment and operations, including the sequencer and upgrades. EigenLayer provides restaking infrastructure for Ethereum validators that enhance Cyber's security.

		Optimism Collective: Cyber aligns with the Optimism ecosystem and shares in the Superchain vision, contributing a portion of sequencer revenues back to the collective. Advisors: The project is backed by several investors (Animoca Brands, Multicoin Capital, Sky9 Capital, and others).
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** The CyberConnect protocol (the precursor to Cyber) launched in 2021, enabling decentralized social profiles and a social graph with over 50 integrated dApps by 2023. The CYBER token was introduced in mid-2023, with a public sale and initial exchange listings in Q2–Q3 2023. Throughout 2023, the team secured partnerships and prepared the Cyber network launch (e.g., integration of LayerZero for omnichain token capability and collaboration with Omni Network for cross-chain features). 2024 Roadmap: Stage 1 (Q2 2024): Cyber network testnet deployment and governance framework establishment (including on-chain voting and a Grants Council). Stage 2 (Q3 2024): Cyber Mainnet launch, featuring integration of EigenDA for scalable data availability and activation of the dual-stake security model (CYBER staking + ETH restaking) on a decentralized validator network. This stage introduced staking rewards for CYBER holders and full on-chain governance. Stage 3 (Q4 2024): Decentralization of the sequencer: Cyber began transitioning to a decentralized sequencer or participating in a shared sequencer network, reducing reliance on any single operator and enabling cross-chain interoperability for social dApps. Stage 4 (Q4 2024): Launch of CyberDB, the enshrined decentralized social data storage solution, completing the core social graph infrastructure and improving data availability for applications (with safeguards such as slashing for malfeasance in place). **Future Milestones** Refer to the official project roadmap on the Cyber website for any updates to

		future milestones.
D.9	Resource Allocation	The project has raised over USD 30 million Furthermore, several token pools are set aside for the project: 34% to Ecosystem Development 10.88% to a Community Treasury 9% to Community Rewards
D.10	Planned Use of Collected Funds or Crypto-Assets	To date, the project has raised over USD 30 million across a seed round, a Series A round, and the public token sale. These funds are dedicated to development, infrastructure, and ecosystem growth. A significant portion of the token supply has been set aside for community and ecosystem incentives (e.g., 34% to the Ecosystem Development, 10.88% to a Community Treasury and 9% to Community Rewards). The Community Treasury tokens are intended to fund future development, grants, and community initiatives via governance decisions. The Cyber Foundation, in coordination with CyberDAO, manages the project treasury and oversees expenditures such as protocol development costs, security audits, operational expenses, and marketing or ecosystem programs. The Ecosystem and Development pool is allocated as follows: 9 % Ecosystem Partners, 10 % Developer Community, 5 % Early-Integration Partners, and 10 % Marketing.
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	100 000 000
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 CYBER 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	CYBER 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	Governance: CYBER is a governance token for the Cyber ecosystem, staking CYBER enables participation in governance via CyberDAO. Staking & Security: CYBER is used to secure the Cyber network. Holders can stake CYBER with network validators (Active Validation Service operators) who run Cyber's sequencers, verifiers, and CyberDB nodes. In return, stakers earn rewards from network fees and revenue (including a share of sequencer revenue and fees from restaked ETH services).
F.3	Planned Application of Functionalities	Please refer to the project team's official channels for any planned application of functionalities.
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	CYBER allows holders to participate in governance, staking to secure the network, and transfer their tokens freely.
F.7	Commercial name or trading name	N/A
F.8	Website of the issuer	https://cyber.co/
F.9	Starting date of offer to the public or admission to trading	2023-08-15
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	349F5QPTN;R1DHBQJKZ;ZST44VTRK
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 CYBER Holders:** Holders of CYBER are entitled to stake the token to secure the network and participate in governance. **Obligations of CYBER Holders:** There are no mandatory obligations imposed on CYBER purchasers beyond the general terms of use of the platform. **Transferability and Trading:** Holders have the ability to transfer their CYBER tokens to others (on-chain) or to trade them on available markets at will. Ownership of CYBER 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	Transfers are executed via the standard ERC-20 functions on Ethereum, Cyber L2, or any supported chain bridged through the LayerZero OFT contracts. Governance rights are exercised by staking CYBER in the Cyber Vault or Staking Pool, which issues cCYBER or stCYBER; these derivatives are then used to submit or vote on CyberDAO proposals. Staking and reward claims are performed through the respective smart-contract calls, while unstaking requires a 7-day waiting period (unless the holder sells transferable cCYBER on a DEX). All actions are subject to normal network gas fees and the contracts' on-chain

		rules.
G.3	Conditions for modifications of rights and obligations	The rights and obligations attached to CYBER 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 Cyber 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	No future public offers of CYBER have been announced by the project team.
G.5	Issuer Retained Crypto-Assets	The team and advisors were allocated 15 000 000 or 15% of the maximum supply
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 CYBER 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	N/A
H.2	Protocols and technical standards	The CYBER token is based on the Cyber Network and the OP Mainnet protocol, which utilize Distributed-Ledger Technology. These protocols provide the foundation for secure transactions and smart contracts. The ERC-20 standard is a technical protocol for issuing and managing tokens, ensuring that the CYBER token is compatible with most wallets, exchanges, and

		decentralized applications (DApps).
H.3	Technology Used	The CYBER token uses the existing ERC-20 token standard on the Cyber Network and OP Mainnet.
H.4	Consensus Mechanism	Cyber leverages optimistic roll-up security: L2 blocks are sequenced ~every 2 seconds by AVS operators; batches are posted to Ethereum, where Ethereum PoS finality (~12 s per block, ~20–30 min challenge window) secures the roll-up. Restaked-ETH AVS validators can be slashed for fraud-proof failures or downtime. OP Mainnet leverages optimistic rollups to scale Ethereum. CYBER transactions are executed off-chain and submitted to Ethereum in batches, with finality usually taking 20-30 minutes. Transactions on OP Mainnet typically confirm in about 2 seconds.
H.5	Incentive Mechanisms and Applicable Fees	Cyber Network: Users pay L2 gas (currently denominated in ETH) that is captured by the sequencer; a fixed share of sequencer revenue is remitted to the Optimism Collective under Superchain rules. Staking rewards: CYBER stakers and restaked-ETH AVS operators receive protocol rewards and a portion of network fees. OP Mainnet: CYBER relies on the existing incentive mechanisms and fee structures of the OP Mainnet blockchain.
H.6	Use of Distributed Ledger Technology	false
H.7	DLT Functionality Description	N/A
H.8	Audit	true
H.9	Audit outcome	Q3 2022 CertiK (general audit) 0 critical 2 major (both mitigated) 2 medium (all resolved) 5 minor (all resolved) 9 informational (8 resolved, 1 acknowledged) Q3 2023 CertiK (cybergraph) 0 critical

		1 major (acknowledged) 1 medium (acknowledged) 1 minor (acknowledged) 2 informational (both acknowledged) Q3 2023 CertiK (Cyber token) 0 critical 1 major (acknowledged) 0 medium 0 minor 1 informational (acknowledged) Q3 2023 CertiK (general audit) 0 critical 5 major (all acknowledged) 4 medium (all resolved) 8 minor (1 resolved, 7 acknowledged) 6 informational (2 resolved, 2 partially resolved, 2 acknowledged) Q1 2024 CertiK (cybergraph) 0 critical 1 major (acknowledged) 0 medium 1 minor (acknowledged) 0 informational Q2 2024 CertiK (staking pool) 0 critical 1 major (acknowledged) 2 medium (all resolved) 6 minor (3 resolved, 3 acknowledged) 1 informational (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	cyber
S.4	Consensus Mechanism	cyber is present on the following networks: Binance Smart Chain, Cyber, Ethereum, Optimism.

		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. Cyber operates as a Layer 2 network built on the Ethereum ecosystem, utilizing the OP Stack from Optimism and integrating EigenDA for data availability. The network employs a decentralized sequencer and verifier architecture. 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. 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 calldata 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	cyber is present on the following networks: Binance Smart Chain, Cyber, Ethereum, Optimism. 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 native token, CYBER, serves multiple functions within the Cyber ecosystem. CYBER holders can participate in governance decisions, influencing protocol parameters and development directions. Staking CYBER tokens enables users to secure the network and earn rewards. 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	2024-06-20
S.7	End of the period to which the disclosure relates	2025-06-20
S.8	Energy consumption	1977.78924 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, cyber, 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.