LANDWOLF (WOLF)
WHITE PAPER

IN ACCORDANCE WITH
TITLE II OF REGULATION (EU) 2023/1114

N	FIELD	CONTENT
00	Table of content	01 – Date of notification 02 – Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114 03 – Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114 04 – Statement in accordance with Article 6(5), points (a), (b), (c) of Regulation (EU) 2023/1114 05 – Statement in accordance with Article 6(5), point (d) of Regulation (EU) 2023/1114 06 – Statement in accordance with Article 6(5), points (e) and (f) of Regulation (EU) 2023/1114 **SUMMARY** 07 – Warning in accordance with Article 6(7), second subparagraph of Regulation (EU) 2023/1114 08 – Characteristics of the crypto-asset 09 – Information about the quality and quantity of goods or services to which the utility token gives access and restrictions on transferability 10 – Key information about the offer to the public or admission to trading **PART I - INFORMATION ON RISKS** I.1 – Offer-Related Risks I.2 – Issuer-Related Risks I.3 – Crypto-Asset-related Risks I.4 – Project Implementation-Related Risks I.5 – Technology-Related Risks I.6 – Mitigation Measures

		PART A - INFORMATION ABOUT THE OFFERER OR THE PERSON SEEKING ADMISSION TO TRADING A.1 – Name A.2 – Legal Form A.3 – Registered address A.4 – Head office A.5 – Registration Date A.6 – Legal entity identifier A.7 – Another identifier required pursuant to applicable law A.8 – Contact telephone number A.9 – E-mail address A.10 – Response Time (Days) A.11 – Parent Company A.12 – Members of the Management Body A.13 – Business Activity A.14 – Parent Company Business Activity A.15 – Newly Established A.16 – Financial condition for the past three years A.17 – Financial condition since registration **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 **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 UP THE WHITE PAPER PURSUANT TO ARTICLE 6(1), SECOND SUBPARAGRAPH OF REGULATION (EU) 2023/1114** C.13 – Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114

		C.14 – Reasons for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114 **PART D - INFORMATION ABOUT THE CRYPTO-ASSET PROJECT** D.1 – Crypto-asset project name D.2 – Crypto-assets name D.3 – Abbreviation D.4 – Crypto-asset project description D.5 – Details of all natural or legal persons involved in the implementation of the crypto-asset project D.6 – Utility Token Classification D.7 – Key Features of Goods/Services for Utility Token Projects D.8 – Plans for the token D.9 – Resource Allocation D.10 – Planned Use of Collected Funds or Crypto-Assets **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 E.2 – Reasons for Public Offering or Admission to trading E.3 – Fundraising Target E.4 – Minimum Subscription Goals E.5 – Maximum Subscription Goals E.6 – Oversubscription Acceptance E.7 – Oversubscription Allocation E.8 – Issue Price E.9 – Official currency or any other crypto-assets determining the issue price E.10 – Subscription fee E.11 – Offer Price Determination Method E.12 – Total Number of Offered/Traded Crypto-Assets

		E.13 – Targeted Holders
		E.14 – Holder restrictions
		E.15 – Reimbursement notice
		E.16 – Refund Mechanism
		E.17 – Refund Timeline
		E.18 – Offer Phases
		E.19 – Early Purchase Discount
		E.20 – Time-limited offer
		E.21 – Subscription period beginning
		E.22 – Subscription period end
		E.23 – Safeguarding Arrangements for Offered Funds/Crypto-Assets
		E.24 – Payment Methods for Crypto-Asset Purchase
		E.25 – Value Transfer Methods for Reimbursement
		E.26 – Right of Withdrawal
		E.27 – Transfer of Purchased Crypto-Assets
		E.28 – Transfer Time Schedule
		E.29 – Purchaser's Technical Requirements
		E.30 – Crypto-asset service provider (CASP) name
		E.31 – CASP identifier
		E.32 – Placement form
		E.33 – Trading Platforms name
		E.34 – Trading Platforms Market Identifier Code (MIC)
		E.35 – Trading Platforms Access
		E.36 – Involved costs
		E.37 – Offer Expenses
		E.38 – Conflicts of Interest
		E.39 – Applicable Law
		E.40 – Competent court

		PART F - INFORMATION ABOUT THE CRYPTO-ASSETS F.1 – Crypto-Asset Type F.2 – Crypto-Asset Functionality F.3 – 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 F.5 – The type of submission F.6 – Crypto-Asset Characteristics F.7 – Commercial or trading name F.8 – Website of the issuer F.9 – Starting date of the offer to the public or admission to trading F.10 – Publication date F.11 – Any other services provided by the issuer F.12 – Identifier of the operator of the trading platform F.13 – Language or languages of the white paper F.14 – Digital Token Identifier Code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available F.15 – Functionally Fungible Group Digital Token Identifier, where available F.16 – Voluntary data flag F.17 – Personal data flag F.18 – LEI eligibility F.19 – Home Member State F.20 – Host Member States

		H.8 – Audit H.9 – Audit outcome **PART J - INFORMATION ON THE SUSTAINABILITY INDICATORS IN RELATION TO ADVERSE IMPACT ON THE CLIMATE AND OTHER ENVIRONMENT-RELATED ADVERSE IMPACTS** J.1 – Adverse impacts on climate and other environment-related adverse impacts **TABLE 1: MANDATORY INFORMATION ON PRINCIPAL ADVERSE IMPACTS ON THE CLIMATE AND OTHER ENVIRONMENTAL RELATED ADVERSE IMPACTS OF THE CONSENSUS MECHANISM** S.1 – Name S.2 – Relevant legal entity identifier S.3 – Name of the crypto-asset S.4 – Consensus Mechanism S.5 – Incentive Mechanisms and Applicable Fees S.6 – Beginning of the period to which disclosure relates S.7 – End of the period to which the disclosure relates S.8 – Energy consumption S.9 – Energy consumption sources and methodologies
01	Date of notification	This white paper was notified to the Malta Financial Services Authority on 2025-02-03
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 person seeking admission to trading 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 this 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	Not applicable
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.
	SUMMARY	
07	Warning in accordance with Article 6(7), second subparagraph of Regulation (EU) 2023/1114	This summary should be read as an introduction to the crypto-asset white paper. The prospective holder should base any decision to purchase this crypto-asset on the content of the crypto-asset white paper as a whole and not on the summary alone. The offer to the public of this crypto-asset does not constitute an offer or solicitation to purchase financial instruments and any such offer or solicitation can be made only by means of a prospectus or other offer documents pursuant to applicable national law. This crypto-asset white paper does not constitute a prospectus as referred to in Regulation (EU) 2017/1129 of the European Parliament and of the Council or any other offer document pursuant to Union or national law.
08	Characteristics of the crypto-asset	LandWolf tokens are crypto-assets other than EMTs and ARTs, which are available on the Ethereum blockchain. LandWolf tokens are fungible, and a total of 1,000,000,000,000 have already been issued. LandWolf tokens are a digital representation of value, and have no

		inherent rights attached. Further, LandWolf tokens have no intrinsic utility. Further, ownership of the contract has been renounced, meaning that no changes may be made.
09	Information about the quality and quantity of goods or services to which the utility token gives access and restrictions on transferability	Not applicable
10	Key information about the offer to the public or admission to trading	The issuance of LandWolf tokens has already been completed, and the tokens are currently listed on Gate.io. However, Dot Vision is seeking admission to trading on MiCA-compliant trading platforms.
Part I - Information on Risks		
I.1	Offer-Related Risks	The admission to trading of LandWolf tokens poses minimal risks when considering that all tokens have already been issued, and are currently in circulation. Since LandWolf tokens are not ARTs or EMTs, there are no reserves of assets, financial risks, or liabilities which need to be managed. The main risk to be considered is that trading platforms would not accept to list LandWolf tokens for internal reasons.
I.2	Issuer-Related Risks	Not applicable
I.3	Crypto-Asset-related Risks	**Market Volatility** Crypto-asset prices are highly susceptible to dramatic fluctuations influenced by various factors, including market sentiment, regulatory changes, technological advancements, and macroeconomic conditions. These fluctuations can result in significant financial gains or losses within short periods, making the market highly unpredictable and challenging for investors.

Liquidity Challenges
Some crypto-assets may suffer from limited liquidity, which can present difficulties when executing large trades without significantly impacting market prices. This lack of liquidity can lead to substantial financial losses, particularly during periods of rapid market movements when selling assets may become challenging or require accepting unfavorable prices.

Asset Security
Crypto-assets face unique security threats, including the risk of theft from exchanges or digital wallets, loss of private keys, and potential failures of custodial services. Since crypto transactions are generally irreversible, any security breach or mismanagement can result in the permanent loss of assets, emphasizing the importance of strong security measures and practices.

Smart Contract Vulnerabilities
Many crypto-assets rely on smart contracts to automate processes, but these contracts are not immune to risks. Bugs, coding errors, or vulnerabilities within the smart contract code can be exploited by malicious actors, potentially leading to asset loss, unauthorized data access, or unintended operational consequences.

Privacy Concerns
All transaction details on the Ethereum blockchain are permanently recorded and publicly accessible, which can potentially expose user activities. Although addresses are pseudonymous, the transparent and immutable nature of the blockchain allows for advanced forensic analysis and intelligence gathering. This level of transparency can make it possible to link blockchain addresses to real-world identities over time, compromising user privacy.

Regulatory Uncertainty
The regulatory environment surrounding crypto-assets is constantly evolving, which can directly impact their usage, valuation, and legal status. Changes in regulatory frameworks may introduce new requirements related to consumer protection, taxation, and anti-money

laundering compliance, creating uncertainty and potential challenges for investors and businesses operating in the crypto space.

Counterparty Risk
Engaging in agreements or storing crypto-assets on exchanges introduces counterparty risks, including the failure of the other party to fulfill their obligations. Investors may face potential losses due to factors such as insolvency, regulatory non-compliance, or fraudulent activities by counterparties, highlighting the need for careful due diligence when engaging with third parties.

Reputational Concerns
Crypto-assets are often subject to reputational risks stemming from associations with illegal activities, high-profile security breaches, and technological failures. Such incidents can undermine trust in the broader crypto ecosystem, negatively affecting investor confidence and market value, thereby hindering widespread adoption and acceptance.

I.4	Project Implementation-Related Risks	The risks related to project implementation are minimal, since the issuance has already been completed. As per I.1, the main potential risk is based on trading platforms opting not to list LandWolf tokens for internal reasons. Further, it is possible that potential marketing deals may fall through.
I.5	Technology-Related Risks	**Private Key Management** The security of crypto-assets heavily depends on the effective management of private keys, which serve as the only means to access and control digital funds. Losing a private key or engaging in poor security practices, such as sharing or storing keys insecurely, can result in the irreversible loss of assets. Additionally, theft or unauthorized access to private keys can lead to the complete loss of funds, emphasizing the importance of secure key storage solutions like hardware wallets and multi-signature schemes. **Transaction Finality**

Blockchain transactions achieve finality probabilistically, meaning their security increases as more blocks are confirmed. However, theoretical risks of transaction reversals exist, particularly in cases of blockchain reorganizations or consensus attacks. Furthermore, transactions sent to incorrect or unintended addresses are typically irreversible, making it crucial for users to double-check addresses and transaction details before execution.

Scalability Issues

As blockchain networks experience increased adoption and usage, scalability challenges can arise. A higher number of transactions can lead to network congestion, resulting in increased transaction fees, slower confirmation times, and reduced usability. Solutions such as layer-2 scaling technologies and blockchain sharding are being explored to address these concerns, but scalability remains a fundamental challenge for widespread adoption.

Network Sustainability

For a blockchain network to remain sustainable, it must maintain sufficient transaction volume to ensure economic viability. This volume is necessary to incentivize validators or miners, support network security, and sustain overall operations. If transaction activity declines significantly, the network may face economic challenges, leading to protocol changes or, in extreme cases, network obsolescence due to a lack of participants and security contributors.

Cybersecurity Threats

Blockchain networks are vulnerable to various cybersecurity threats that can compromise their operations and data integrity. Potential attacks include 51% attacks, where a single entity gains majority control over the network, Sybil attacks, where attackers create multiple fake identities to manipulate the network, and DDoS attacks, which can overwhelm nodes and disrupt network functionality. Mitigating these threats requires robust security protocols and decentralized network structures.

Consensus Failures

Issues with a blockchain's consensus mechanism can lead to serious disruptions such as network forks, operational halts, and a loss of trust among participants. Forks can result in duplicate transactions or diverging ledger states, causing confusion and potential financial losses. Ensuring a well-designed consensus algorithm and timely upgrades is essential to maintaining network stability and integrity.

Protocol Vulnerabilities

Undetected bugs and flaws within a blockchain's core protocol code pose significant risks, including network disruption, balance manipulation, and potential exploits by malicious actors. Continuous code audits, rigorous testing, and the implementation of bug bounty programs help identify and mitigate such vulnerabilities before they can be exploited.

Smart Contract Risks

Smart contracts, while offering automation and efficiency, introduce risks stemming from coding flaws, misconfigurations, and unintended logic vulnerabilities. Exploitable weaknesses in smart contracts can lead to asset loss, unauthorized access to sensitive data, and broader network vulnerabilities. Thorough audits and security best practices are essential to minimize these risks.

Infrastructure Dependencies

Blockchain networks depend on various underlying infrastructures such as internet connectivity, cloud services, and hardware systems, which may themselves be susceptible to attacks, outages, or external interference. Any disruption in these critical dependencies can compromise the accessibility and reliability of blockchain services, emphasizing the need for decentralized and resilient infrastructure solutions.

Technological Obsolescence

As technology evolves, blockchain systems face the risk of becoming obsolete. Emerging innovations, such as quantum computing, could potentially break current cryptographic

encryption standards, rendering blockchain networks insecure. To remain resilient, continuous advancements in cryptographic techniques and blockchain protocols must be pursued to address evolving threats.

Governance Challenges
The decentralized nature of blockchain networks can present governance challenges, particularly when it comes to decision-making and issue resolution. Ineffective governance models may result in delays in addressing critical network concerns, instability, and even centralization of power among a small group of stakeholders. Transparent, inclusive, and well-structured governance frameworks are necessary to support long-term sustainability.

Data Integrity
Maintaining the integrity of blockchain data is critical to its reliability and trustworthiness. Bugs, errors, or malicious tampering with transaction data can undermine the accuracy and consistency of the ledger, potentially leading to financial and operational risks. Mechanisms such as data verification, redundancy, and integrity checks are essential to safeguarding the blockchain against corruption.

Third-Party Risks
The reliance on external service providers, such as cryptocurrency exchanges, wallet providers, and custodial services, introduces additional layers of risk. These third parties may be susceptible to security breaches, operational failures, and regulatory non-compliance, which could impact users' assets and overall market stability. Due diligence and choosing reputable service providers are essential to mitigating such risks.

I.6	Mitigation Measures	**Smart Contract Vulnerabilities** The LandWolf token contract has been audited and found not to pose any critical, high, or medium risks. The LandWolf tokens contract is open source, and anyone can consult it. Since all LandWolf tokens have been issued, and the ownership of the contract has been renounced, Dot Vision Limited cannot prevent any risks related to smart contract

<table>
<tr>
<td colspan="3">vulnerabilities in relation to services provided by third-parties.

Regulatory Uncertainty
Dot Vision Limited stays abreast with all legal and regulatory updates, and continuously works to ensure compliance of LandWolf tokens with any applicable laws and regulations.

Blockchain Related Risks
While noting that all blockchain face risks, LandWolf tokens have been built on the Ethereum blockchain, which is recognised for its reputation, security, and resilience. Considering that there are over 1,000,000 validators on Ethereum, risks related to consensus failures and cybersecurity threats are minimal.

Risks Related to Project Implementation and Admission to Trading
While Dot Vision Limited can in no way guarantee the listing of LandWolf tokens on particular platforms, it will ensure that all necessary actions are taken to ensure listing on targeted platforms, while maintaining the highest level of integrity and professionality.</td>
</tr>
<tr>
<td colspan="3" align="center">**Part A - Information about the offerer or the person seeking admission to trading**</td>
</tr>
<tr>
<td>A.1</td>
<td>Name</td>
<td>Dot Vision Limited</td>
</tr>
<tr>
<td>A.2</td>
<td>Legal Form</td>
<td>Private limited liability company registered under the laws of Malta</td>
</tr>
<tr>
<td>A.3</td>
<td>Registered address</td>
<td>MK Business Centre, 115A, Floor 2, Valley Road, BKR9022, Birkirkara, Malta</td>
</tr>
<tr>
<td>A.4</td>
<td>Head office</td>
<td>MK Business Centre, 115A, Floor 2, Valley Road, BKR9022, Birkirkara, Malta</td>
</tr>
<tr>
<td>A.5</td>
<td>Registration Date</td>
<td>2023-05-03</td>
</tr>
<tr>
<td>A.6</td>
<td>Legal entity identifier</td>
<td>Not available</td>
</tr>
</table>

A.7	Another identifier required pursuant to applicable law	Maltese Company Number C105164
A.8	Contact telephone number	+385 97 678 1308
A.9	E-mail address	landwolf@dotvision.io
A.10	Response Time (Days)	7 days
A.11	Parent Company	Not applicable
A.12	Members of the Management Body	**Mr Sasa Dordevic** Managing Director Professional address: MK Business Centre, 115A, Floor 2, Valley Road, Birkirkara, Malta **Dr Matteo Alessandro** Director Professional address: 6, Level 2, Office 1, Triq is-Suq, Floriana, Malta.
A.13	Business Activity	Dot Vision Limited offers digital services related to distributed ledger technology and other traditional technologies. Services include bespoke development and consultancy related to distributed ledger technology. Dot Vision Limited operates globally, with a focus in the European Union.
A.14	Parent Company Business Activity	Not applicable
A.15	Newly Established	Yes
A.16	Financial condition for the past three years	Dot Vision Limited was formally incorporated on May 3, 2023

A.17	Financial condition since registration	Dot Vision Limited started its activities on May 3, 2023. The share capital of Dot Vision Limited is EUR 1,200. As of 31 December 2024, the company has a balance sheet total of approximately EUR 50,000 with no debt, had a turnover of approximately EUR 100,000 in 2024, and made a profit of approximately EUR 50,000 in 2024.
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	No
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 up the white paper pursuant to Article 6(1), second subparagraph of Regulation (EU) 2023/1114		
C.13	Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	MK Fintech Partners Limited, a company registered under the Laws of Malta bearing company registration number C94602, with registered address at MK Buildings, 115A, Level 0, Valley Road, Birkirkara, BKR9024, Malta, and formally incorporated on February 11, 2020.
C.14	Reasons for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	MK Fintech Partners Limited acts as a consultancy firm for Dot Vision Limited, and has been tasked with ensuring the compliance of this white paper with Regulation (EU) 2023/1114.
Part D - Information about the crypto-asset project		
D.1	Crypto-asset project name	LandWolf

D.2	Crypto-assets name	LandWolf Token
D.3	Abbreviation	WOLF
D.4	Crypto-asset project description	The issuer of Land Wolf tokens is Dot Vision Limited, a company registered in Malta. All LandWolf tokens have already been issued, with a total supply of 1,000,000,000,000. The project is completely community-driven, aiming to immortalise the art of Matt Furie's LandWolf art, which is the namesake of the crypto-asset project and the tokens. The plan is to ensure the longevity of Furie's work long term, working on digitally archiving his work and also creating the LandWolf project. This actively promotes Furie's work to future generations, and creates a legacy around its impact; essentially making it accessible and relevant to all.
D.5	Details of all natural or legal persons involved in the implementation of the crypto-asset project	<table><tr><td>**Management Body**</td><td>Sasa Dordevic - MK Business Centre, 115A, Floor 2, Valley Road, Birkirkara, Malta Dr Matteo Alessandro - 6, Level 2, Office 1, Triq is-Suq, Floriana, Malta.</td></tr><tr><td>**Legal and Consultancy**</td><td>MK Fintech Partners Limited - MK Buildings, 115A, Floor 0, Valley Road, Birkirkara, Malta</td></tr></table>
D.6	Utility Token Classification	No
D.7	Key Features of Goods/Services for Utility Token Projects	Not applicable
D.8	Plans for the token	Since all LandWolf tokens have already been issued, and having already been listed on Gate.io, Dot Vision Limited now seeks to admit LandWolf tokens to trading on several

		MiCA-compliant trading platforms, to increase the project's market cap and increase ease of access. It is also the aim to market the LandWolf tokens through a variety of channels, including the sponsorship of major football teams in Europe.
D.9	Resource Allocation	The project is funded through a community-funded and community-managed treasury. As of date, the folllowing financial resources have been allocated: ● **Art:** Approximately EUR 100,000 ● **Marketing:** Approximately EUR 500,000 ● **Consultancy and other services:** Approximately EUR 400,000
D.10	Planned Use of Collected Funds or Crypto-Assets	Not applicable
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 Offering or Admission to trading	It is the aim of the project to be compliant with all applicable laws and regulations, while increasing accessibility to LandWolf tokens, and increasing their value. As such, Dot Vision Limited is seeking to admit LandWolf tokens to trading so as to be able to have a wider reach within the EU, while ensuring legal compliance.
E.3	Fundraising Target	Not applicable
E.4	Minimum Subscription Goals	Not applicable
E.5	Maximum Subscription Goals	Not applicable
E.6	Oversubscription Acceptance	Not applicable
E.7	Oversubscription Allocation	Not applicable

E.8	Issue Price	Not applicable
E.9	Official currency or any other crypto-assets determining the issue price	Not applicable
E.10	Subscription fee	Not applicable
E.11	Offer Price Determination Method	Not applicable
E.12	Total Number of Offered/Traded Crypto-Assets	1,000,000,000,000
E.13	Targeted Holders	The project is targeted to all types of holders, and no restrictions are being applied other than those applied by relevant laws and regulations.
E.14	Holder restrictions	None
E.15	Reimbursement notice	Not applicable
E.16	Refund Mechanism	Not applicable
E.17	Refund Timeline	Not applicable
E.18	Offer Phases	Not applicable
E.19	Early Purchase Discount	Not applicable
E.20	Time-limited offer	Not applicable
E.21	Subscription period beginning	Not applicable

E.22	Subscription period end	Not applicable
E.23	Safeguarding Arrangements for Offered Funds/Crypto-Assets	Not applicable
E.24	Payment Methods for Crypto-Asset Purchase	Not applicable
E.25	Value Transfer Methods for Reimbursement	Not applicable
E.26	Right of Withdrawal	Not applicable
E.27	Transfer of Purchased Crypto-Assets	Not applicable
E.28	Transfer Time Schedule	Not applicable
E.29	Purchaser's Technical Requirements	The purchase of LandWolf tokens from EU-regulated trading platforms will be available to all users of such trading platforms. Most trading and exchange services offered by regulated crypto-asset service providers are open to retail holders, and may be subject to the compliance requirements of the respective providers. Further, holders of LandWolf tokens must have Ethereum blockchain compatible wallets which may be self-custodial or managed by a third-party.
E.30	Crypto-asset service provider (CASP) name	Not applicable
E.31	CASP identifier	Not applicable
E.32	Placement form	NTAV

E.33	Trading Platforms name		
		Trading Name	**Legal Entity Name**
		Coinbase	Coinbase Germany GmbH (Germany)
			Coinbase Europe Limited (Ireland)
		Binance	Binance France SAS (France)
			Bifinity UAB (Lithuania)
			Binance Spain S.L. (Spain)
			Binance Poland Spółka z Ograniczoną Odpowiedzialnością (Poland)
		Gate.io	Gate Technology Ltd. (Malta)
			Gate Global UAB (Lithuania)
		Kraken	Payward European Solutions Limited (Ireland, Belgium, Spain, and Italy)
			Coin Meester B.V. (France and Poland)
			Payward Continental Services Limited (Netherlands)
		HTX/Huobi Global	Safe Glory UAB (Lithuania)
		Bitstamp	Bitstamp Europe S.A. (Luxembourg, Netherlands, France, Spain, and Italy)

		Cex.io	CEX.IO EU VASP UAB (Lithuania)
		Bitpanda	Bitpanda GmbH (Austria, France, Spain, Italy, and Czech Republic)
		OKX	Okcoin Europe Ltd. (Malta)
		Gemini	Gemini Intergalactic EU Ltd. (Malta)
E.34	Trading Platforms Market Identifier Code (MIC)	Not available	

E.35	Trading Platforms Access		
		Platform Name	**Means of Access**
		Coinbase	www.coinbase.com
		Binance	www.binance.com
		Gate.io	www.gate.io
		Kraken	www.kraken.com
		HTX/Huobi Global	www.htx.com
		Bitstamp	www.bitstamp.net
		Cex.io	www.cex.io
		Bitpanda	www.bitpanda.com
		OKX	www.okx.com
		Gemini	www.gemini.com
E.36	Involved costs	The above trading platforms may have their own fee structures in place and holders are advised to familiarise themselves with the respective fee structure before accessing the trading platforms. Dot Vision Limited shall not charge any fees in this regard.	
E.37	Offer Expenses	Not applicable	
E.38	Conflicts of Interest	No conflicts of interest have been identified as of today in relation to the admission to trading of LandWolf tokens.	

E.39	Applicable Law	Malta
E.40	Competent court	Subject to the applicable law, any dispute arising out of or in connection with this white paper and all claims in connection to the LandWolf tokens shall be exclusively that of the Courts of Malta.
Part F - Information about the crypto-assets		
F.1	Crypto-Asset Type	LandWolf tokens are considered as crypto-assets other than EMTs and ARTs under Regulation (EU) 2023/1114. LandWolf tokens are not considered utility tokens. LandWolf tokens are fungible tokens, based on the ERC-20 token standard.
F.2	Crypto-Asset Functionality	LandWolf tokens have the inherent functionalities of ERC-20 tokens, mainly being transferred and stored on the Ethereum blockchain. No other functionalities are planned to be implemented.
F.3	Planned Application of Functionalities	All functionalities referred to in F.2 have already been applied since they are intrinsic to the tokens.
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	LandWolf tokens are crypto-assets other than EMTs and ARTs, which are available on the Ethereum blockchain, and are based on the ERC-20 token standard. LandWolf tokens are fungible, and a total of 1,000,000,000,000 have already been issued. LandWolf tokens are a digital representation of value, and have no inherent rights attached. Further, LandWolf tokens have no intrinsic utility. Further, ownership of the contract has been renounced,

		meaning that no changes may be made.
F.7	Commercial or trading name	LandWolf
F.8	Website of the issuer	www.landwolf.com
F.9	Starting date of the offer to the public or admission to trading	2025-03-03
F.10	Publication date	2025-03-03
F.11	Any other services provided by the issuer	Not applicable
F.12	Identifier of the operator of the trading platform	Not available
F.13	Language or languages of the white paper	English
F.14	Digital Token Identifier Code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available	Not available
F.15	Functionally Fungible Group Digital Token Identifier, where available	Not available

F.16	Voluntary data flag	Mandatory
F.17	Personal data flag	Yes
F.18	LEI eligibility	Eligible
F.19	Home Member State	Malta
F.20	Host Member States	Austria Belgium Bulgaria Croatia Cyprus Czech Republic Denmark Estonia Finland France Germany Greece Hungary Ireland Italy Latvia Lithuania Luxembourg Netherlands Poland Portugal Romania Slovakia

		Slovenia Spain Sweden
Part G - Information on the rights and obligations attached to the crypto-assets		
G.1	Purchaser Rights and Obligations	The LandWolf tokens do not have any inherent rights or obligations attached to them.
G.2	Exercise of Rights and obligations	LandWolf tokens, issued by Dot Vision Limited, are classified as crypto-assets under Regulation (EU) 2023/1114 and relevant laws, excluding ARTs and EMTs. According to these regulations, a crypto-asset is defined as "a digital representation of value or rights that can be electronically transferred and stored using distributed ledger technology or similar technologies." Ownership of LandWolf tokens grants holders only the rights explicitly outlined in this white paper and those established under Regulation (EU) 2023/1114 and applicable laws. No additional rights are conferred beyond these terms. LandWolf token holders acknowledge that transferring LandWolf tokens to another address results in the automatic assignment of ownership to the recipient of that address. Transactions involving LandWolf tokens are irreversible. Once tokens are sent to an address, holders accept the possibility of permanently losing access or claims to them. This may occur due to reasons such as (i) incorrect address entry, making it impossible to identify the recipient, (ii) loss or lack of access to the private key associated with the address, (iii) transfer to an entity unwilling to return the tokens, or (iv) transfer to an entity requiring identity verification or other actions before returning the tokens. Dot Vision Limited bears no responsibility to track, verify, or determine the ownership of LandWolf token balances unless explicitly required by applicable laws.

		Holding LandWolf tokens will not result in: (i) the creation of any lien upon any property, asset, or revenue of Dot Vision Limited; or (ii) the creation of any shareholding or ownership interest in Dot Vision Limited. By holding, using, or accessing LandWolf tokens, holders confirm and guarantee that: • They comply with the terms outlined in this white paper and applicable laws. • They are at least 18 years of age. • They will not use LandWolf tokens for any illegal purposes, including but not limited to illicit gambling, money laundering, fraud, extortion, ransomware, financing of terrorism, violent activities, or prohibited market practices. LandWolf token holders use and hold their tokens solely for their own account and are not considered as nominees or agents of Dot Vision Limited unless explicitly agreed upon in writing by Dot Vision Limited. Holders are fully informed that Dot Vision Limited, along with its affiliates, officers, directors, agents, employees, and suppliers, holds liability only as expressly stated under applicable laws and this white paper. Specifically, Dot Vision Limited assumes no responsibility for (i) the use of LandWolf tokens; (ii) costs associated with acquiring replacement goods or services resulting from any purchases, transactions, or communications involving LandWolf tokens; or (iii) unauthorised access to or modification of token holders' data or transactions. To the maximum extent permitted by applicable laws, Dot Vision Limited disclaims all warranties, whether express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose. Furthermore, Dot Vision Limited shall not be liable for any damages resulting from the use of LandWolf tokens, including but not limited to direct, indirect, incidental, punitive, or consequential damages.
G.3	Conditions for modifications of	As provided by Article 12 of Regulation (EU) 2023/1114, any significant new factor, material

	rights and obligations	mistake, or material inaccuracy that is capable of affecting the assessment of the crypto-assers will be described in a modified version of this white paper, notified to the competent authorities, and published on the issuer's website.
G.4	Future Public Offers	None
G.5	Issuer Retained Crypto-Assets	None
G.6	Utility Token Classification	No
G.7	Key Features of Goods/Services of Utility Tokens	Not applicable
G.8	Utility Tokens Redemption	Not applicable
G.9	Non-Trading request	Sought
G.10	Crypto-Assets purchase or sale modalities	Not applicable
G.11	Crypto-Assets Transfer Restrictions	Not applicable
G.12	Supply Adjustment Protocols	No
G.13	Supply Adjustment Mechanisms	Not applicable
G.14	Token Value Protection Schemes	No

G.15	Token Value Protection Schemes Description	Not applicable
G.16	Compensation Schemes	No
G.17	Compensation Schemes Description	Not applicable
G.18	Applicable law	Malta
G.19	Competent Court	Subject to the applicable law, any dispute arising out of or in connection with this white paper and all claims in connection to the LandWolf tokens shall be exclusively that of the Courts of Malta.
	Part H - Information on the underlying technology	
H.1	Distributed ledger technology	**Overview of Distributed Ledger Technology (DLT)** Distributed Ledger Technology (DLT) is a decentralised and distributed system that enables multiple participants to collectively manage and verify a shared database without relying on a central authority. Unlike traditional database systems that depend on a single entity for maintaining consistency and security, DLT distributes control across a network of computers, known as nodes. These nodes validate and record changes through consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS), ensuring data integrity and agreement across the network. This decentralised model enhances security, improves system resilience, and promotes transparency, reducing the need for intermediaries while requiring participants to trust the network's underlying consensus rules. Common implementations of DLT include blockchain technology, as well as other frameworks such as directed acyclic graphs (DAGs), each offering unique advantages depending on the use case.

Blockchain as a Subset of DLT

Blockchain is one of the most widely recognised implementations of Distributed Ledger Technology (DLT), organising data into a continuously growing sequence of blocks. Each block contains transaction records and is cryptographically linked to the preceding block in chronological order, ensuring data integrity and security. Blockchain networks can operate in a decentralised manner across nodes, with each node maintaining an identical copy of the ledger and participating in transaction validation and synchronisation. Depending on the network type—public or private—the level of decentralisation and participation may vary.

Security within blockchain is achieved through cryptographic techniques, including hashing algorithms such as SHA-256 or Keccak-256, and consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS), making it nearly impossible to alter stored data without revalidating all subsequent blocks and gaining majority network consensus. Transparency is another key feature of blockchain technology, as transaction details are typically accessible to all participants in public blockchains. Once recorded and confirmed, transactions become virtually immutable due to the cryptographic safeguards in place, ensuring data permanence and resistance to unauthorised modifications.

The Ethereum Blockchain
Introduction
Ethereum is a second-generation, open-source blockchain platform that transformed the cryptocurrency space by introducing programmable smart contracts and decentralised applications (dApps). Conceived by Vitalik Buterin and a group of co-founders in 2013 and officially launched on July 30, 2015, Ethereum was designed to expand blockchain technology beyond basic financial transactions. It has since become a foundational element of the decentralised web, providing developers with a robust infrastructure for building blockchain-based solutions.

At its core, Ethereum functions as a decentralised global network powered by its native cryptocurrency, Ether (ETH). The Ethereum Virtual Machine (EVM) acts as a runtime

environment for smart contracts, enabling the execution of complex, self-executing agreements without intermediaries. This functionality has spurred the growth of decentralised finance (DeFi), non-fungible tokens (NFTs), and numerous other blockchain applications.

On September 15, 2022, Ethereum completed a major upgrade known as The Merge, transitioning from a Proof-of-Work (PoW) to a Proof-of-Stake (PoS) consensus mechanism. This transition reduced Ethereum's energy consumption by approximately 99.95%, addressing environmental concerns and laying the foundation for improved network scalability and security. The Ethereum ecosystem continues to evolve with ongoing developments, including sharding and layer-2 scaling solutions such as rollups, which aim to enhance transaction throughput and accommodate an expanding user base.

Ethereum's Native Token
Ether (ETH) is the native cryptocurrency of the Ethereum blockchain and acts as the fuel that powers its ecosystem. ETH is required to pay for gas fees, which facilitate transactions and smart contract execution. With Ethereum's transition to a Proof-of-Stake (PoS) consensus mechanism, ETH gained an additional utility—staking. Validators can lock up their ETH to contribute to network security and consensus, earning rewards in return. This staking model enhances network security and provides ETH holders with an opportunity to earn rewards, though it also introduces potential penalties for improper validator behavior.

Within the broader Ethereum ecosystem, ETH is essential for deploying smart contracts, interacting with decentralised applications (dApps), and enabling complex financial operations within decentralised finance (DeFi). It serves as a medium of exchange, a store of value, and a critical component in various protocols, including lending, borrowing, and liquidity provision.

Ethereum, as of January 2025, operates under the Proof-of-Stake (PoS) consensus mechanism, following its transition from Proof-of-Work (PoW) in September 2022 through an upgrade known as The Merge. This event fundamentally changed Ethereum's consensus model,

drastically reducing energy consumption and improving network sustainability, while setting the stage for further enhancements such as sharding and Layer-2 scaling solutions.

Multi-Layer Architecture
Ethereum has a layered architecture that consists of multiple components working together to facilitate decentralised applications (dApps) and smart contract execution. At its core, the execution layer (Layer 1) handles transaction processing, smart contract execution via the Ethereum Virtual Machine (EVM), and consensus through Proof of Stake (PoS). This layer also includes state management and networking protocols for peer-to-peer communication. Ethereum's data availability layer ensures efficient storage and accessibility of blockchain data using Merkle Patricia Trees and transaction tries to maintain account balances and smart contract storage. The consensus and networking layer secures the network through node communication, gossip protocols, and validator-based PoS consensus.

On top of the base layer, Ethereum supports an application layer, where smart contracts, dApps, wallets, and user interfaces operate to provide usability and accessibility. To address scalability challenges, Ethereum integrates Layer 2 solutions, such as rollups (Optimistic and ZK-Rollups), state channels, and sidechains like Polygon, which help improve transaction throughput and reduce costs. This multi-layered architecture ensures Ethereum's scalability, security, and transparency while supporting a growing ecosystem of decentralised applications

Smart Contracts and Native Asset Capabilities
Ethereum smart contracts are self-executing programs that run on the Ethereum blockchain, enabling automated, trustless transactions and operations without intermediaries. These contracts are written in high-level programming languages such as Solidity and Vyper, and they are executed by the Ethereum Virtual Machine (EVM), which ensures consistent behavior across all nodes in the network. Smart contracts define the rules and logic of decentralised applications (dApps), automating complex processes such as financial transactions, token issuance, and governance. Once deployed on the blockchain, smart contracts are immutable

and tamper-proof, meaning they cannot be altered, ensuring transparency and security. Their ability to interact with other contracts allows for composability, enabling the development of complex ecosystems like decentralised finance (DeFi) and non-fungible tokens (NFTs).

Ethereum's native asset capability is another key feature that supports the seamless creation and transfer of digital assets. The network's primary currency, Ether (ETH), serves as both a medium of exchange and a means to pay for transaction fees (gas) required to execute smart contracts. Additionally, Ethereum's ERC standards, such as ERC-20 for fungible tokens and ERC-721 for non-fungible tokens (NFTs), provide a framework for creating and managing digital assets on the blockchain. These standards have enabled a vast ecosystem of decentralised applications, from tokenised financial instruments to digital collectibles and gaming assets. Through smart contracts and its native asset functionality, Ethereum has become the foundation for a diverse range of blockchain-based applications, offering flexibility and programmability unmatched by traditional financial systems.

Ethereum's Monetary Policy
Ethereum's monetary policy is designed to balance network security, incentivise participation, and manage token supply. Unlike Bitcoin's fixed supply cap, Ethereum adopts a flexible approach that has evolved over time. A significant change occurred with the transition from Proof-of-Work (PoW) to Proof-of-Stake (PoS) in September 2022, known as "The Merge," which reduced the issuance rate of new ETH by approximately 90%. In the PoS system, new ETH is issued as rewards to validators who stake their tokens to secure the network. The issuance rate is influenced by the total amount of ETH staked and the number of active validators, with a decreasing rate of issuance as the total staked ETH increases.

Fee Burning Mechanism and Supply Dynamics
Another crucial component of Ethereum's monetary policy is the fee-burning mechanism introduced by EIP-1559 in August 2021. This upgrade implemented a base fee for transactions that is burned, effectively removing ETH from circulation. The interplay between issuance through staking rewards and burning through transaction fees can lead to periods of deflation

when network activity is high, potentially reducing the overall ETH supply. The current structure ensures that, at most, the total supply inflates by about 1.5% per year, assuming 100% of the current supply is staked with zero burn. However, in practice, supply dynamics fluctuate between inflationary and deflationary depending on network activity. This flexibility allows Ethereum to adjust to changing network conditions and demand, introducing uncertainty in long-term supply projections.

Ongoing Discussions
As of January 2025, Ethereum's monetary policy continues to be a topic of debate within the community. Proposals to further refine the issuance rate and manage the growth of the staking pool are being discussed, aiming to balance network security, decentralisation, and Ethereum's function as a form of money. The ongoing evolution of Ethereum's monetary policy reflects its commitment to adapting to the needs of its growing ecosystem while striving to maintain economic stability and security.

Ethereum's Governance Model
Ethereum operates with an informal, off-chain governance system that emphasises community participation and consensus. Unlike some blockchain projects that utilise on-chain voting or formal governance structures, Ethereum's decision-making process is decentralised and relies on discussions among developers, feedback from the community, and implementation by core development teams.

Ethereum Improvement Proposals (EIPs)
The primary method for proposing changes to the Ethereum protocol is through Ethereum Improvement Proposals (EIPs). Any community member can submit an EIP, detailing potential modifications or additions to the network. These proposals undergo extensive discussion and review in various forums, including Ethereum All Core Developers calls, ETHMagicians, Discord, and GitHub. While this open process fosters diverse input and dialogue, it can also result in slower decision-making compared to more centralised systems. The implementation of approved changes is ultimately carried out by client teams responsible for developing and

		maintaining the core Ethereum software. This approach aims to balance the need for expert oversight with the principles of decentralisation, though it has faced criticism for potentially concentrating power among a small group of core developers. Despite these challenges, Ethereum's governance model continues to evolve, striving to maintain transparency, inclusivity, and alignment with the network's decentralised ethos. *Further Information and Links* (All links validated as of January 20, 2025) ● https://ethereum.org/en/ provides overall information about the Ethereum blockchain, such as technology, roadmap, white paper, and latest updates. ○ https://ethereum.org/en/developers/ is the official hub for those developing on the Ethereum blockchain, and provides resources such as tutorials and technical documentation. ○ https://ethereum.org/en/developers/docs/ is the official documentation of the Ethereum blockchain, offering resources to help understand and use Ethereum's technology
H.2	Protocols and technical standards	The LandWolf tokens were developed using the Solidity programming language and OpenZeppelin ERC Token Standard Libraries, primarily the ERC-20 standard. The token contract may be found at: https://etherscan.io/token/0x67466be17df832165f8c80a5a120ccc652bd7e69#code **Solidity Programming Language** Solidity is a high-level, statically typed, contract-oriented programming language designed for developing smart contracts that run on the Ethereum Virtual Machine (EVM). Its syntax is influenced by languages such as C++, Python, and JavaScript, making it accessible to developers with diverse programming backgrounds. Solidity supports complex features including inheritance, libraries, and user-defined types, enabling the creation of sophisticated decentralised applications (dApps).

Compatibility with EVM-Based Blockchains
Beyond Ethereum, Solidity is compatible with other EVM-based blockchains, allowing developers to deploy smart contracts across various platforms without significant modifications. This compatibility facilitates interoperability and leverages existing developer expertise, promoting a broader adoption of blockchain technology.

Security Features
While Solidity provides robust features for smart contract development, it is essential for developers to implement best practices and conduct thorough testing to ensure security and reliability in decentralised applications.

ERC-20 Token Standard
The ERC-20 token standard, introduced by Fabian Vogelsteller in November 2015, has become the cornerstone of fungible token creation on the Ethereum blockchain. This technical specification defines a set of rules and functions that Ethereum-based tokens must adhere to, ensuring interoperability and compatibility across the ecosystem. By providing a standardised framework, ERC-20 has significantly simplified the process of creating and deploying tokens, allowing developers to focus on innovative applications rather than grappling with compatibility issues.

Core Functions of ERC-20
At its core, the ERC-20 standard mandates six essential functions that every compliant token must implement:

- totalSupply(): Returns the total supply of the token.
- balanceOf(address _owner): Provides the account balance of the owner's account.
- transfer(address _to, uint256 _value): Transfers a number of tokens directly from the message sender to another address.
- transferFrom(address _from, address _to, uint256 _value): Transfers tokens from a

specified address.

- approve(address _spender, uint256 _value): Allows a spender to withdraw a set number of tokens from a specified account.
- allowance(address _owner, address _spender): Returns the number of tokens a spender is allowed to withdraw from the owner's account.

These functions enable basic operations such as checking token balances, transferring tokens between addresses, and allowing third-party spending. Additionally, optional functions like name(), symbol(), and decimals() provide descriptive information about the token. This uniformity has fostered a vibrant ecosystem of decentralised applications (dApps), exchanges, and wallets that can seamlessly interact with any ERC-20 token, driving the growth of decentralised finance (DeFi) and other blockchain-based innovations.

OpenZeppelin's ERC Token Standard Libraries
OpenZeppelin offers a comprehensive suite of libraries for implementing Ethereum Request for Comments (ERC) token standards, providing developers with secure and efficient tools to create compliant tokens. These libraries include implementations for popular standards such as ERC-20 for fungible tokens and ERC-721 for non-fungible tokens (NFTs). OpenZeppelin's ERC libraries are extensively audited, battle-tested, and optimised for gas efficiency, ensuring that developers can focus on building their specific token features rather than reinventing the wheel for basic functionalities. Additionally, these libraries often include optional extensions like pausable and burnable tokens, providing enhanced flexibility and security features. By leveraging OpenZeppelin's ERC libraries, developers can significantly reduce the risk of vulnerabilities and ensure compatibility with the broader Ethereum ecosystem, making them an essential tool for secure and standardised token development.

OpenZeppelin Standards and Interfaces Utilised
Apart from the main ERC-20 he LandWolf tokens also make use of the following OpenZeppelin standards and interfaces:

		- IERC5267 - IERC20Permit - IERC20Errors - IERC721Errors - IERC1155Errors - IERC20 - IERC20Metadata - Ownable
H.3	Technology Used	The technology allowing for the holding, storing, and transferring crypto-assets is based on the Ethereum blockchain, and has been outlined throughout this section.
H.4	Consensus Mechanism	**Proof-of-Stake Consensus** In Ethereum's PoS system, validators replace miners as the primary actors securing the network. Validators are participants who have staked at least 32 ETH as collateral to earn the right to propose and validate new blocks. Validator Selection and Block Proposal The PoS mechanism randomly selects validators to propose new blocks. For each slot (12 seconds), one validator is chosen as the block proposer. Simultaneously, a committee of validators is selected to attest to the proposed block's validity. **Block Validation Process** 1. The selected validator proposes a new block. 2. Other validators in the network receive and verify the block. 3. If the majority of validators agree on the block's validity, it is added to the blockchain. 4. The block proposer and attestors receive rewards in ETH for their participation. **Security and Finality** Ethereum's PoS implements a concept called "finality" to ensure the immutability of

transactions:

1. Checkpoints occur at the start of each epoch (32 slots or about 6.4 minutes).
2. When two consecutive checkpoints receive votes from at least 66% of the total staked ETH, the earlier checkpoint becomes finalised.

This finality mechanism makes it extremely costly and difficult for attackers to alter the blockchain, as they would need to control a significant portion of the staked ETH.

Staking and Rewards
Validators earn rewards for their participation in the consensus process. The current annual staking yield ranges from approximately 2.23% to 4%. This incentive structure encourages honest behavior and network participation.

Slashing
To maintain network integrity, Ethereum implements a penalty system called slashing. Validators who act maliciously or fail to perform their duties can have a portion of their staked ETH destroyed, ensuring that there are economic consequences for harmful behavior.

In conclusion, Ethereum's PoS consensus mechanism has significantly enhanced the network's efficiency, security, and scalability while drastically reducing its environmental impact. As the Ethereum ecosystem continues to evolve, this consensus mechanism forms the foundation for future improvements and innovations in the platform.

H.5	Incentive Mechanisms and Applicable Fees	**Ethereum's Fee Structure and EIP-1559** Ethereum employs a gas system to price computational operations, where each transaction or smart contract execution requires a specific amount of gas, paid in ETH. The total transaction fee is determined by multiplying the gas used by the gas price, denominated in gwei (1 billionth of an ETH). With the implementation of EIP-1559 in August 2021, Ethereum introduced a more predictable fee structure comprising a base fee and an optional priority fee (tip). The base fee adjusts dynamically based on network congestion and is burned, effectively

		removing it from circulation, while the priority fee allows users to incentivise faster transaction processing. This mechanism aims to stabilise gas prices and introduces a deflationary aspect to ETH's supply. **Ethereum's Incentive Structure and Proof-of-Stake** Following Ethereum's transition to a Proof-of-Stake (PoS) consensus mechanism, validators are responsible for securing the network by proposing and attesting to blocks. Validators earn rewards from both newly issued ETH (consensus layer rewards) and transaction fees (execution layer rewards). The system is designed to encourage honest participation by rewarding validators for their contributions and penalising malicious actions through slashing, where a portion of the validator's staked ETH is forfeited for protocol violations. This economic model aligns validators' interests with the overall health and security of the Ethereum network, promoting decentralisation and robust participation in the consensus process.
H.6	Use of Distributed Ledger Technology	No, DLT not operated by the issuer or a third-party acting on the issuer's behalf
H.7	DLT Functionality Description	Not applicable
H.8	Audit	Yes
H.9	Audit outcome	**LandWolf Token Contract** The LandWolf Contract underwent an audit focusing on the contract's security, compliance, and potential vulnerabilities, which was published on April 26, 2024. The audit was undertaken by SolidProof.io, which is a brand of the officially registered company MAKE Network GmbH, based in Germany. The full audit report may be found at: https://github.com/solidproof/Projects/blob/main/2024/Landwolf%200x67/SmartContract_Audit_Solidproof_Landwolf0x67.pdf

The scope of the audit focused on reviewing the provided Solidity code to identify risks such as unauthorised access, logical inconsistencies, and security loopholes. The assessment was limited to the contract files explicitly provided by the project team, ensuring a thorough evaluation of the codebase while excluding integrations with external services. The audit methodology involved a combination of manual code reviews and automated security analysis to uncover vulnerabilities and ensure adherence to industry best practices. Manual checks were conducted line-by-line to identify potential weaknesses, while automated tools were used to detect common patterns of vulnerabilities such as reentrancy, integer overflows, and access control flaws.

The audit outcomes indicated a strong security posture, with no critical, high, or medium-risk issues identified in the contract. A single low-risk issue related to the use of a floating Solidity pragma version was noted, recommending the adoption of a fixed version to avoid potential compiler-related issues. Additionally, an informational finding highlighted missing NatSpec documentation, which would enhance the clarity and maintainability of the contract.

Ownership of the contract was renounced, eliminating the possibility of centralised control, and key functions such as token minting, burning, and blacklisting were disabled to prevent misuse. The report concluded that the contract is non-upgradable, ensuring immutability post-deployment, and recommended best practices such as multi-signature wallets and governance mechanisms to enhance decentralisation and security further.

OpenZeppelin ERC-20 Contract
OpenZeppelin's ERC20 implementation has undergone formal verification to ensure its correctness and security. CertiK, a leading blockchain security firm, conducted a formal verification of OpenZeppelin's ERC20 reference implementation as of version 4.7.3. They verified 38 security properties and confirmed that all were satisfied, indicating a high level of assurance in the implementation's reliability.

Ethereum Blockchain

		The Ethereum blockchain as a whole has not been audited in the same way a traditional software project might be. However, various components of Ethereum, such as its core protocol upgrades, client implementations, and smart contracts deployed on the network, have undergone extensive security audits by different organisations. Key aspects of Ethereum that have been audited include: 1. **Ethereum 2.0 (Consensus Layer) Audits:** The transition to Ethereum's Proof-of-Stake (PoS) consensus mechanism, known as The Merge, was subjected to multiple security audits by firms such as Sigma Prime and Trail of Bits. These audits focused on vulnerabilities in the new consensus mechanism, staking, and validator operations. 2. **Ethereum Client Implementations:** Major Ethereum clients (such as Geth, Prysm, and Besu) have undergone security reviews and testing to ensure compliance with protocol specifications and to identify potential vulnerabilities. 3. **Ethereum Improvement Proposals (EIPs) Security Reviews:** Significant protocol changes introduced through EIPs (such as EIP-1559 and EIP-4844) are reviewed for security implications before implementation. 4. **Bug Bounty Programs:** The Ethereum Foundation operates bug bounty programs to incentivise researchers and developers to discover and report vulnerabilities in the protocol. While these targeted audits enhance Ethereum's security, a comprehensive, single audit of the entire Ethereum blockchain would be impractical due to the network's decentralised and constantly evolving nature. Security in Ethereum is instead achieved through continuous review, community vigilance, and layered security mechanisms.
Part J - Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts		
J.1	Adverse impacts on climate	Dot Vision Limited, as the issuer of crypto-assets excluding EMTs and ARTs, provides insights

	and other environment-related adverse impacts	into the principal adverse impacts of the consensus mechanism used for validating LandWolf token transactions and ensuring the integrity of the distributed ledger. These insights focus on the environmental impacts, particularly those related to climate change. The data presented covers the period from April 15, 2024, to December 31, 2024, with estimated projections provided for the period from January 1, 2024, to December 31, 2024. Transaction validation and ledger maintenance for LandWolf tokens have resulted in an estimated total energy consumption of 6,512.891 kilowatt-hours (kWh) annually. Furthermore, the energy required to validate a single LandWolf token transaction is estimated at 0.013177241 kWh per transaction. For further details on the consensus mechanism and its impact on climate and environmental factors, please refer to Section H of this document. Additionally, Table 1 provides the required information regarding the principal adverse effects of the consensus mechanism on climate and other environmental aspects.

Table 1: Mandatory information on principal adverse impacts on the climate and other environmental related adverse impacts of the consensus mechanism

N	Field	Content
S.1	Name	Dot Vision Limited
S.2	Relevant legal entity identifier	Maltese Company Number C105164
S.3	Name of the crypto-asset	LandWolf Token
S.4	Consensus Mechanism	Proof of Stake as per H.4
S.5	Incentive Mechanisms and Applicable Fees	As per H.5
S.6	Beginning of the period to which disclosure relates	2024-01-01
S.7	End of the period to which the disclosure relates	2024-12-31
Mandatory key indicator on energy consumption		
S.8	Energy consumption	6512.891 kWh

		Sources and methodologies
S.9	Energy consumption sources and methodologies	The sources for information related to energy consumption are as follows: ● **Etherscan.io:** Transaction amounts in disclosure period ● **Crypto Carbon Ratings Institute (CCRI):** Annualised electricity consumption for the Ethereum blockchain ○ https://indices.carbon-ratings.com/ The methodology used in calculating the energy consumption related to the LandWolf token is based on the methodology proposed by CCRI in the white papers titled *Methodologies to calculate sustainability indicators for the EU Markets in Crypto Assets (MiCA) regulation (2024)* and *Accounting for carbon emissions caused by cryptocurrency and token systems (2021, updated 2023)*. Since the LandWolf token had its first transaction on April 15, 2024, the data from that date until the end of 2024 was used, and then aggregated to cover the whole period. In the same period, the Ethereum blockchain had a total of 330,487,921 transactions, of which 359,128 were related to the LandWolf token. Therefore, LandWolf tokens contributed 0.109% of all transactions on the Ethereum blockchain within the period. This percentage of transactions is then applied to the whole number of transactions which Ethereum had in 2024, which is that of 454,836,639. As such, it is being assumed that over 2024, had LandWolf tokens been available for the whole year, then they would have contributed to a total of 494,253 transactions (rounded up). Considering that according to CCRI's indices, Ethereum's annualised energy consumption is that of 5,993,491.9 kWh. Thus, applying the percentage of 0.109% to this figure, it leaves us with the calculated figure of 6512.891 kWh for the year.