NAORIS PROTOCOL WHITEPAPER

00 Table of content

01 DATE OF NOTIFICATION

2025-09-02

COMPLIANCE STATEMENTS

02 This crypto-asset white paper has not been approved by any competent authority in any Member State of the European Union. The offeror of the crypto-asset is solely responsible for the content of this crypto-asset white paper.

03 This crypto-asset white paper complies with Title II of Regulation (EU) 2023/1114 and, to the best of the knowledge of the management body, the information presented in the crypto-asset white paper is fair, clear and not misleading and the crypto-asset white paper makes no omission likely to affect its import.

04 The crypto-asset referred to in this white paper may lose its value in part or in full, may not always be transferable and may not be liquid.

05 The utility token referred to in this white paper may not be exchangeable against the good or service promised in the crypto-asset white paper, especially in the case of a failure or discontinuation of the crypto-asset project.

06 The crypto-asset referred to in this white paper is not covered by the investor compensation schemes under Directive 97/9/EC of the European Parliament and of the Council.

The crypto-asset referred to in this white paper is not covered by the deposit guarantee schemes under Directive 2014/49/EU of the European Parliament and of the Council.

SUMMARY

07 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 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 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 or any other offer document pursuant to Union or national law.

08 Characteristics of the crypto-asset

The $NAORIS token is a utility crypto asset central to the Naoris Protocol, a decentralized cybersecurity ecosystem. It facilitates access to a range of blockchain-based services designed to improve digital trust, data integrity, and network security. The token underpins a global, quantum-resistant cybersecurity mesh powered by decentralized swarm AI and advanced cryptographic technologies.

09 Utility Token Rights and Transfer Restrictions

Rights and Obligations of Purchasers

Purchasers of $NAORIS tokens gain the **right to access and participate in services within the Naoris Protocol ecosystem**, including:

- Running or interacting with decentralized security or trust services;
- Participating in governance mechanisms;

- Potentially earning rewards for contributing to network security, integrity validation, or compliance assurance tasks.

Purchasers **do not gain equity, profit rights, or ownership** in Naoris Protocol. The token is strictly utility-focused and does not represent an investment contract.

Exercise of Rights

Users can exercise their rights by:

- Using tokens to pay for services offered by the protocol;
- Possibly staking tokens to support network operations or validation processes;
- Engaging with various dApps and services built on the Naoris infrastructure.

To exercise these rights, users typically need a compatible wallet and access to the Naoris Protocol network.

Modification of Rights and Conditions

The terms associated with the use of $NAORIS tokens may be modified through **protocol updates or community governance decisions**, especially if on-chain governance mechanisms are introduced. All changes would need to follow predefined processes ensuring transparency and user awareness.

Access to Goods and Services

As a **utility token**, $NAORIS provides access to high-integrity digital infrastructure, including:

- Quantum-resistant cybersecurity services;
- Compliance and threat detection automation;
- Decentralized identity and data sovereignty systems.

The quantity and quality of services accessed via tokens depend on usage levels, token holdings, and network participation.

Transferability

There are **no technical restrictions on transferability** of $NAORIS tokens within the protocol's own ecosystem or on public blockchains. However, users must comply with jurisdictional laws, and tokens may be subject to KYC/AML restrictions when interacting with regulated services or exchanges.

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

Total offer amount	*24,000,000 x $0.125*
Total number of tokens to be offered to the public	*24,000,000*
Subscription period	*From 20/05/2025 to 30/06/2025*
Minimum and maximum subscription amount	*Minimum: 800* *Maximum: 8,000,000*
Issue price	*USD $0.125*
Subscription fees (if any)	*None*
Target holders of tokens	*Web3 participants and general public*
Description of offer phases	*Public Sale: we offer our early users to buy the token at a fixed price*
CASP responsible for placing the token (if any)	*N/A*
Form of placement	*Tokensoft Platform*
Admission to trading	*ZBX*

PART I – INFORMATION ON RISKS

I.1 Offer-Related Risks

The listing and trading of Naoris Protocol's tokens involve risks stemming from market fluctuations, regulatory uncertainties, and evolving trading conditions. Token prices can be subject to market volatility based on various factors, including investor sentiment, macroeconomic shifts, institutional participation, and speculative trends. While Naoris Protocol aims to maintain robust liquidity, unforeseen events, such as regulatory developments, exchange listing changes, or systemic economic instability, could influence market access or trading dynamics. Furthermore, changing legal and compliance frameworks may introduce new restrictions on trading or using Naoris tokens within specific jurisdictions, potentially affecting overall market availability.

I.2 Issuer-Related Risks

Regulatory Compliance Risks

Naoris Protocol operates within the rapidly evolving global landscape of digital asset regulation. As such, the issuer may face risks related to:

- Non-compliance with jurisdiction-specific crypto regulations (e.g., MiCA in the EU, SEC regulations in the U.S.);
- Potential classification disputes (e.g., utility vs. security);
- Delays or costs in obtaining necessary licenses;
- Risk of market access restrictions in specific countries due to non-alignment with local compliance frameworks.

These risks may result in **sanctions, delistings, project delays, or token utility restrictions**, all of which can affect the protocol's adoption and token value.

Financial Risks

Although the issuer is engaged in an innovation-driven ecosystem, it remains exposed to:

- **Liquidity constraints**, especially during development phases or in down markets;
- Dependence on **funding from token sales or private investment rounds**;
- Cost-intensive R&D and infrastructure requirements, which may outpace revenue generation in the early stages;
- Exposure to crypto market volatility, which can impact treasury reserves and operational runway.

Failure to maintain financial health may hinder the timely deployment of services or compromise network security and functionality.

Business and Industry Risks

Naoris Protocol operates in the **blockchain cybersecurity and data integrity sector**, which is:

- **Highly competitive**, with constant technological innovation and emerging rivals;
- **Heavily reliant on adoption**, requiring both technical robustness and user trust;
- Dependent on **interoperability with other networks and infrastructure**, which may face technical or governance limitations.

Additionally, success depends on the protocol's ability to scale user adoption, retain developer support, and keep pace with emerging quantum and AI technologies.

Legal Risks

The issuer may be subject to:

- Unclear legal treatment of decentralized autonomous structures;
- Cross-border liabilities due to the international nature of token distribution;

- Risk of intellectual property disputes or legal claims regarding technology usage or branding.

Unfavorable legal developments could impair token usability, limit platform growth, or expose the issuer to costly litigation.

Internal Control and Operational Risks

As a decentralized and innovation-focused organization, the issuer faces:

- Risks related to **internal governance, auditing, and financial reporting**, particularly in early or pre-commercial phases;
- Potential **dependency on a small core development team**, exposing the protocol to personnel and key knowledge risks;
- Risks from software bugs, smart contract vulnerabilities, or operational mismanagement.

A failure in internal controls may lead to financial losses, security breaches, or reputational damage.

Reputational Risks

Reputation is critical for trust-driven platforms like Naoris Protocol. Risks include:

- **Security incidents** (e.g., protocol exploits, validator collusion);
- **Associations with illicit activity,** especially if on-chain activity is not well-governed;
- **Delays in roadmap delivery**, missed milestones, or breakdowns in community communication;
- Misinformation or negative media coverage impacting token credibility.

A compromised reputation can reduce user trust, slow adoption, and adversely affect token liquidity and utility.

Environmental, Social, and Governance (ESG) Risks

Although the protocol promotes secure and ethical technology use, ESG-related risks may include:

- **Environmental concerns** if the protocol relies on energy-intensive consensus mechanisms;
- **Social equity concerns** related to global token distribution or governance influence;
- **Governance transparency**, especially if decisions are concentrated among early stakeholders or the issuer.

Failure to meet ESG expectations may lead to reduced institutional support and broader reputational risks.

I.3 Crypto-Assets-related Risks

Naoris Protocol's token operates without a central issuer, offering a decentralized architecture but simultaneously facing a range of risks. Market dynamics may cause significant price volatility, influenced by factors such as overall sentiment, economic indicators, and individual market participants. Although the token is planned for broad availability on multiple exchanges and trading platforms, unexpected policy changes, macroeconomic disruptions, or regulatory clampdowns could adversely affect liquidity. On the user side, individuals who choose to self-custody must guard private keys diligently, as losing them typically results in irretrievable funds.

Moreover, storing tokens on centralized entities introduces additional hazards – such as hacks, insolvency, or other forms of counterparty exposure.

Beyond these market and custodial aspects, the regulatory environment is equally crucial. Governmental guidelines can shift rapidly and differ widely across jurisdictions, potentially restricting the token's tradability or imposing particular tax implications that impact user decisions.

Despite these uncertainties, Naoris Protocol aspires to maintain a resilient ecosystem by focusing on secure, low-latency validation and an adaptable governance framework – objectives designed to weather both technical and legal uncertainties over the long term.

I.4 Project Implementation-Related Risks

Naoris Protocol operates as a decentralized, open-source blockchain without a central issuer, yet certain factors can influence its growth and adoption. While Naoris Protocol's dPoSec consensus provides sub-10ms finality and helps mitigate scalability pressures, rising transaction volumes could still present challenges in extreme market conditions.

Security risks are lower compared to systems reliant on complex smart contracts, but software bugs, network vulnerabilities, and evolving cyberattack methods remain possibilities. Long term, the onset of quantum computing may call for further refinement of Naoris Protocol's cryptographic methods, even though it has been designed with post-quantum resilience in mind.

Market volatility can also affect liquidity and investor sentiment. Despite these challenges, Naoris Protocol's focus on rapid settlement, robust security, and decentralized validation positions it as a strong contender for secure, scalable blockchain solutions in various industries.

I.5 Technology-Related Risks

Private Key Management Risk

Naoris Protocol's security model depends on maintaining strict control over private keys, which authorize transactions within the network. If a user's private keys – or related login credentials – are lost, stolen, or poorly secured, the resulting compromise can lead to permanent and irreversible loss of tokens or other assets.

Settlement and Transaction Finality

Though Naoris Protocol employs a near-instant finality mechanism through its Distributed Proof of Security (dPoSec), the concept of definitive settlement remains theoretically probabilistic. In rare circumstances – such as unforeseen forks or unusual consensus failures – transactions could be reversed, or divergent versions of the ledger might briefly persist. Typically, once a transaction has been validated, it cannot be undone or cancelled, and crypto-assets sent to an incorrect address are irretrievable.

Potential Bugs in Core Protocol Code

Despite continuous testing and code audits, there is always a possibility that undiscovered bugs or security gaps remain in Naoris Protocol's underlying software. Exploitable vulnerabilities may disrupt network operations or compromise account balances. Regular code reviews, structured bug bounty programs, and community-driven oversight help mitigate and respond to these risks quickly.

Smart Contract Security

Although Naoris Protocol is not primarily focused on complex smart contract execution, any integrated or future implementation of automated on-chain logic can be susceptible to coding errors or vulnerabilities. Such flaws may allow attackers to trigger unintended behaviors—ranging from unauthorized transactions to broader systemic disruptions—highlighting the importance of thorough audits and robust development practices.

Anonymity and Privacy

By nature, blockchain transactions leave immutable, transparent records. While Naoris Protocol addresses quantum security, linking an address to real-world data can expose users to spam, phishing, or other targeted attacks. Participants who handle sensitive information must employ proper privacy safeguards and consider off-chain mixing or similar solutions to maintain confidentiality.

Third-Party Dependencies

Although Naoris Protocol supports decentralized self-custody, users often rely on exchanges, wallet services, or other third-party platforms for storage and trading. These external services are vulnerable to hacks, internal failures, or policy restrictions, which may result in the unauthorized loss or freezing of crypto-assets. Operators and users alike must remain vigilant about the risks posed by these external entities.

I.6 Mitigation Measures

Naoris Protocol encourages users to implement strong private key custody, including secure backups and hardware wallets, to reduce the risk of theft or loss. Incorporating multi-factor authentication, rotating addresses, and performing regular audits of smart contracts or on-chain code can further mitigate issues like unauthorized access, transaction errors, and protocol bugs. In parallel, the network's decentralized governance and transparent code reviews help swiftly identify and resolve potential vulnerabilities, while privacy-friendly solutions, such as address rotation and off-chain data handling, minimize exposure of sensitive information.

When working with third parties – such as exchanges and custodians – users should diversify their asset storage, scrutinize each service provider's security practices, and consider obtaining relevant insurance or SLA-based protections. By combining these measures with continuous code audits and conservative operational procedures, Naoris Protocol and its participants can significantly reduce common blockchain-related risks, preserving both trust and integrity across the network.

PART A – INFORMATION ABOUT THE OFFEROR OR THE PERSON SEEKING ADMISSION TO TRADING

A.1 Name

NDSE Cyber Ltd

A.2 Legal form

Company Limited by Shares, ELF Code 98A8, Country of Formation: Bahamas

A.3 Registered address

Suite 2 C, One Sandyport Plaza, West Bay Street, Nassau, Bahamas

A.4 Head office

Albany Financial Center, Suite 502, South Ocean Boulevard, Nassau, Bahamas SP-63158

A.5 Registration Date

2021-08-04

A.7 Another identifier required pursuant to applicable national law

Company registration number 207328 B

A.8 Contact telephone number

David Carvalho, CEO: +351 911 148 512

João Ferreira Santos, Head of Compliance: +351 916 31 20 25

A.9 E-mail address

David Carvalho: david@naoris.com

João Ferreira Santos: joaosantos@naoris.com

A.10 Response Time (Days)

005 (days)

A.12 Members of the Management Body

David Carvalho – CEO – Albany Financial Center, Suite 502, Nassau, Bahamas SP-63158

A.13 Business Activity

Purpose / Strategy / Vision

Naoris Protocol's vision is to transform cybersecurity and digital trust by pioneering a decentralized and quantum-resistant security framework. Its strategy centers on creating a global, resilient, and incorruptible digital ecosystem where every connected device contributes to a secure, compliant, and intelligent mesh network. By issuing the $NAORIS utility token, the protocol aims to incentivize network participation, enable access to advanced security services, and foster trust across digital environments.

Products / Services

Naoris Protocol delivers a suite of blockchain-based digital integrity and cybersecurity services, including:

- **Decentralized Cybersecurity Mesh:** A distributed security framework that protects networks against threats without centralized points of failure.
- **Quantum-Resistant Blockchain Infrastructure:** Security solutions designed to withstand current and future quantum computing threats.
- **Swarm AI-Driven Trust & Compliance:** Automated compliance, data validation, and trust scoring powered by decentralized artificial intelligence.

- **Decentralized Proof of Trust & Data Sovereignty Tools:** Real-time trust assessment and local data validation services, enabling privacy-by-design.

The $NAORIS token is used to **access, power, and secure these services** across the network.

Markets Served

Naoris Protocol serves a **global market** with emphasis on:

- **Highly regulated industries** (e.g., finance, healthcare, government);
- **Data-sensitive sectors** (e.g., supply chain, legal, education);
- **Technology-forward ecosystems** (e.g., smart cities, IoT networks, blockchain applications).

Its technology is applicable across **multinational enterprises, critical infrastructure providers, and digital service platforms.**

Milestones Reached

- Development of the first decentralized cybersecurity mesh;
- Integration of quantum-resistant consensus mechanisms;
- Implementation of Decentralized Proof of Trust and Swarm AI;
- Strong recognition and alignment with key enterprise needs for compliance, data integrity, and threat mitigation.

Outlook

Naoris Protocol is poised to become a foundational infrastructure layer for secure digital transformation worldwide. With rising threats in cybersecurity and the advent of quantum computing, its vision and product-market fit are strongly aligned with future global demands. As adoption grows and the token economy expands, the project expects to see increased usage of the $NAORIS token,

deeper integrations across industries, and new layers of decentralized governance and scalability.

A.14 Parent Company Business Activity

Where applicable, business or professional activity of the parent company, including principal activities and principal markets.

A.15 Newly Established

False

A. 16 Financial Condition for the past three Years

Over the past three financial years (2022–2024) the Company operated in a deliberate investment phase: approximately **$5 million of annual operating expenses** were incurred to build the core technology platform and deliver multiple proof-of-concept deployments with government and enterprise counterparties. During this period the business was effectively pre-revenue and therefore reported operating losses consistent with its development strategy.

To fund this phase the Company **raised an aggregate $34 million** of capital. After funding cumulative operating spend of roughly $15 million over 2022–2024 (excluding any non-cash items), the remaining cash resources have provided a substantial liquidity buffer and runway to support commercialisation. The successful proof-of-concept projects have de-risked the technology and established reference customers, positioning the Company to transition from development to revenue generation.

Beginning in **2025** the Company is converting these pilots into contracted deployments and expects to **achieve profitability during the 2025 financial year** as recurring revenues begin to exceed the stable cost base. Accordingly, the financial condition of the Company has strengthened: it retains significant cash from the $34 million raised, maintains a relatively low fixed cost structure

(~$5 million per annum), and now enters a scaling phase in which prior R&D investment is anticipated to translate into sustainable positive earnings.

PART D – INFORMATION ABOUT THE CRYPTO-ASSET PROJECT

D.1 Crypto-asset project name

Naoris Protocol

D.2 Crypto-assets name

$NAORIS

D.3 Abbreviation

$NAORIS

D.4 Crypto-asset project description

Naoris Protocol is a next-generation blockchain designed to function as a decentralized cybersecurity layer, converting every connected device into an active validator that continuously monitors network integrity. By employing Distributed Proof of Security (dPoSec) and post-quantum cryptographic techniques, Naoris offers near-instant settlement while significantly reducing single points of failure. This architecture enables real-time threat mitigation and more reliable operation across diverse infrastructures.

In contrast to traditional blockchains reliant on energy-intensive mining or staking, Naoris's design focuses on continuous trust validation at the device level. Through dPoSec, compromised or malicious devices are identified and quarantined swiftly, preserving the network's resilience. This approach provides a secure, low-latency foundation for digital ecosystems seeking robust protection against evolving threats.

D.5 Details of persons involved in the implementation

David Carvalho	CEO
Sumit Chauhan	CTO

Guy Davies	CMO
David Holtzman	CSO
Scott MacAndrew	CFO
Youssef El Maddarssi	Global Head of Business Development
Kjell Grandhagen	Advisor
Knut Grandhagen	Advisor
Umeir Zulkufli	Advisor
Calum James	Advisor

D.6 Utility Token Classification

True

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

Naoris Protocol introduces its native token as the essential medium for accessing and maintaining decentralized cybersecurity services in a machine-to-machine ecosystem. Every network operation – ranging from basic transactions to advanced validation checks – consumes a small amount of the token, guaranteeing that participating devices contribute consistently and honestly to the network's security. Because the protocol's trust mesh design requires continuous, automated interactions between devices, the token serves as the binding "fuel", ensuring these operations can only occur if the token is spent. Thus, the token underpins all activity within Naoris: no transaction or validation process can take place without it.

D.8 Plans for the token

Naoris Protocol envisions its token serving as "gas fee" within a broader ecosystem of decentralized security services. When users or devices submit operations, whether basic transactions or specialized calls related to threat detection and response, they pay fees in Naoris tokens. These fees incentivize

validator devices to maintain honest and robust participation. Specifically, each transaction consumes a small amount of token "gas," ensuring that only authentic and properly authenticated actions are processed.

Over time, this approach not only sustains network integrity and operational efficiency but also bolsters the token's utility across multiple verticals, such as finance, supply chain, and other critical infrastructure use cases, where quantum-resistant security and low-latency transactions are paramount.

PART E – INFORMATION ABOUT THE ADMISSION TO TRADING

E.1 Public Offering or Admission to trading

ATTR

E.2 Reasons for Public Offer or Admission to trading

Naoris Protocol is committed to meeting high standards of regulatory compliance and industry best practices in every jurisdiction where it operates. We aim to align with applicable guidelines, maintain transparent governance structures, and proactively address evolving legal requirements. By ensuring robust compliance measures – whether through ongoing audits, clear disclosures, or adherence to recognized frameworks – Naoris Protocol seeks to foster trust among users, enterprises, and regulatory bodies alike.

In pursuing these objectives, Naoris Protocol aspires to create a secure, future-proof environment that supports responsible innovation while safeguarding market integrity and user interests. Our focus on continuous improvement and open collaboration with stakeholders underscores the importance of adhering to regulations, thereby offering a stable foundation for broad adoption and long-term success.

E.3 Fundraising Target

3 million USD

E.4 Minimum Subscription Goals

100 USD

E.5 Maximum Subscription Goal

1 million USD

E.6 Oversubscription Acceptance

Not applicable

E.7 Oversubscription Allocation

Not applicable

E.8 Issue Price

0.125 USD

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

US Dollars.

E.10 Subscription Fee

Not applicable

E.11 Offer Price Determination Method

Not applicable

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

24 millions

E.13 Targeted Holders

Crypto and technology enthusiast, web3 investors, high net worth individuals.

E.14 Holder Restrictions

Not applicable

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

Early private backers entered two private rounds at $0.04 and $0.08 when Naoris was still pre-testnet. The steep discount compensated them for taking the highest technical and execution risk.

Today's public buyers join a very different project, one already running on a public testnet with 3-plus million users, so the risk premium (and discount) no longer applies.

To keep the launch orderly, those private-sale tokens remain locked for 4-6 months, preventing early investors from immediately selling into the public market.

E.20 Time-Limited Offer

40 days.

E.21 Subscription Period Beginning

20/05/2025

E.22 Subscription Period End

30/06/2025

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

Not applicable

E.24 Payment Methods for Crypto-Asset Purchase

Bitcoin, Ethereum, USDT and USDC.

E.25 Value Transfer Methods for Reimbursement

Not applicable

E.26 Right of Withdrawal

Not applicable

E.27 Transfer of Purchased Crypto-Assets

Holders will be able to claim their tokens at launch.

E.28 Transfer Time Schedule

31/07/2025, 12pm UTC

E.29 Purchaser's Technical Requirements

Purchaser needs to own or create a wallet such as Metamask, Rabby, to purchase the tokens and ability to perform an online KYC, ability to e-sign a Token Purchase Agreement and execute the payment transaction.

E.33 Trading Platforms name

ZBX.

E.35 Trading Platforms Access

Investors can access the platform: https://www.zbx.com/

E.36 Involved Costs

2 500€ which is the MSFA payment to submit the whitepaper. Either than that, none.

E.38 Conflicts of Interest

None.

E.39 Applicable law

The law applicable to the admission to trading shall be determined in accordance with the relevant jurisdiction of the trading platform(s).

E.40 Competent court

Magistrate Court Bahamas

PART F – INFORMATION ABOUT THE CRYPTO-ASSETS

F.1 Crypto-Asset Type

Utility token

F.2 Crypto-Asset Functionality

The $NAORIS token functions as the heartbeat of the entire Naoris Protocol, underpinning every layer of its decentralized cybersecurity mesh. Beyond a simple unit of account, the token unlocks day-to-day access to the platform's expanding catalogue of services; ranging from secure data-sovereignty tools and post-quantum wallet operations to advanced Swarm-AI threat-mitigation modules. Whenever a user deploys an application, calls an API, or spins up a node, $NAORIS is the medium that settles the associated network fees and bandwidth costs, ensuring that value flows seamlessly, and transparently, between participants.

On the infrastructure side, each validator and edge device must stake $NAORIS to participate in the Distributed Proof-of-Security (dPoSec) consensus. Staking aligns incentives: well-behaved nodes earn additional tokens for validating peers

and reporting real-time cyber-trust metrics, while malicious or non-performing nodes risk losing their stake. This creates a self-regulating, “always-on” trust layer that continually hardens as more devices join the mesh. Tokens released as block rewards and service payments circulate back to operators, developers, and end-users, fueling a device-to-device, machine-economy loop where increased adoption directly amplifies token demand.

Because every attestation, threat-mitigation event, and post-quantum transaction is immutably recorded on-chain, $NAORIS also serves as a cryptographic proof that systems and processes have been validated over time, creating a verifiable audit trail for enterprises and regulators alike.

F.3 Planned Application of Functionalities

Core functionalities are planned to go live at mainnet launch. Certain staking, access, and governance to follow in phased deployments.

F.4 Type of white paper

OTHR

F.5 The type of submission

NEWT

F.6 Crypto-Asset Characteristics

General Information

- **Name:** $NAORIS
- **Type:** Utility Token
- **Project:** Naoris Protocol
- **Standard:** ERC-20 (or other applicable blockchain standard, pending confirmation)

- **Digital Token Identifier (DTI)**: To be assigned under ISO 24165 once registered
- **Functionality Activation:** Core functionalities are planned to go live with the protocol's mainnet launch (date to be confirmed by the issuer). Certain staking, access, and governance features may follow in phased deployments.

Classification for EU Crypto-Asset Register

As defined under Regulation (EU) 2023/1114, the $NAORIS token qualifies as a **utility token**. It **does not confer ownership rights, voting rights in the issuer company, or a claim on profits**, and is designed exclusively to provide access to specific services and features within the Naoris Protocol.

Token Functionality

The $NAORIS token enables:

- **Access to Protocol Services:** Used to pay for services such as threat detection, compliance assurance, data integrity validation, and decentralized cybersecurity operations;
- **Network Participation:** May be used in staking mechanisms or node participation schemes where applicable, contributing to the protocol's decentralized cybersecurity mesh;
- **Incentivization and Rewards:** May be used to reward participants who contribute computational or validation services, or uphold data trust and compliance standards;
- **Governance (future functionality):** Potential use in protocol governance decisions is expected in later development stages.

Planned Rollout of Functionalities

- **Beta/Testnet Phase:** Limited service access for early users and developers (Q2 – Q3 2025, tentative);

- **Mainnet Launch:** Full access to token-based services (expected late 2025);
- **Governance & Staking Launch:** Planned in subsequent phases post-mainnet, subject to ecosystem readiness and community input.

F.7 Commercial name or trading name

Naoris Protocol

F.8 Website of the issuer

https://www.naorisprotocol.com/

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

2025/10/01

F.10 Publication date

2025/09/30

F.13 Language or languages of the white paper

English

F.19 Home Member State

Malta, it's the first authority we reach in the EU

F.20 Host Member States

All EU/EEA countries

PART G – INFORMATION ON THE RIGHTS AND OBLIGATIONS ATTACHED TO THE CRYPTO-ASSETS

G.1 Purchaser Rights and Obligations

Purchasers of $NAORIS tokens gain access to the Naoris Protocol ecosystem services. The tokens grant the right to:

- Access and use protocol services;
- Participate in network validation activities (where applicable);
- Engage in future governance mechanisms (when implemented);
- Transfer tokens freely subject to applicable regulations.

Purchasers are obligated to:

- Comply with all applicable laws and regulations;
- Secure their private keys and wallet access;
- Use the protocol services in accordance with terms of use;
- Not engage in any activities that could harm the protocol or its participants.

G.2 Exercise of Rights and obligations

Token holders exercise their rights by:

- Connecting compatible wallets to the Naoris Protocol;
- Paying for services using $NAORIS tokens;
- Participating in network activities as they become available;
- Following protocol-specific procedures for each service type.

G.3 Conditions for modifications of rights and obligations

Rights and obligations may be modified through:

- Protocol governance decisions (once governance is implemented);
- Technical upgrades required for security or functionality;
- Regulatory requirements in applicable jurisdictions;
- Community consensus following transparent procedures.

All modifications will be communicated to token holders with reasonable notice.

G.6 Utility Token Classification

True

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

The $NAORIS token provides access to:

- **High Quality:** Enterprise-grade cybersecurity services with quantum-resistant encryption;
- **Automated & Scalable:** Millisecond threat detection and mitigation;
- **Compliance by Design:** Automated regulatory compliance services;
- **Quantity:** Access levels determined by token holdings and network fees.

G.8 Utility Tokens Redemption

$NAORIS tokens are redeemed automatically when:

- Paying for protocol services;
- Executing transactions on the network;
- Accessing advanced features;
- Participating in validation activities.

G.11 Crypto-Assets Transfer Restrictions

There are no technical restrictions on token transfers within the protocol. However:

- Regulatory compliance (KYC/AML) may apply on certain platforms;
- Jurisdictional limitations may restrict access in some countries;
- Smart contract restrictions may apply for specific functions (e.g., staking lock-ups).

G.12 Supply Adjustment Protocols

No

G.14 Token Value Protection Schemes

No

G.18 Applicable Law

The applicable law shall be determined based on the jurisdiction of token usage and relevant regulatory frameworks.

G.19 Competent Court

Disputes shall be subject to the jurisdiction of competent courts as determined by applicable law and the specific circumstances of each case.

PART H – INFORMATION ON THE UNDERLYING TECHNOLOGY

H.1 Distributed ledger technology

Naoris Protocol is a next-generation, post-quantum distributed ledger designed for secure, efficient, and ultra-fast transaction processing – serving as a decentralized security layer for virtually any type of system or network. At its core is the Distributed Proof of Security (dPoSec) mechanism, which achieves consensus in about 10 milliseconds, continuously verifying the integrity of every connected device in real time. Each device acts as a validator, removing single points of failure and ensuring robust decentralization.

To remain resilient against advanced quantum-computing threats, Naoris Protocol employs specialized post-quantum cryptographic algorithms (such as CRYSTALS-Dilithium) aligned with NIST standards. This approach delivers near-instant confirmation for transactions while automatically detecting and isolating malicious behavior across the network. By operating as a universal "trust mesh," Naoris Protocol can integrate seamlessly into existing infrastructures – be they industrial, governmental, or consumer-based – reinforcing them with a zero-trust security model that prioritizes resilience and reliability.

H.2 Protocols and technical standards

Naoris Protocol is a post-quantum distributed ledger designed to operate as a decentralized security layer. All connected devices act as validator nodes,

removing single points of failure. Transactions typically finalize within ~10ms, delivering near-instant throughput without relying on classical Proof-of-Work (PoW) or Proof-of-Stake (PoS) paradigms.

Consensus Mechanism – Distributed Proof of Security (dPoSec)

Naoris Protocol employs dPoSec, a consensus model in which network participants continuously assess each device's trust status in real time. Rather than mining or staking, devices validate and propagate state changes collaboratively, ensuring:

- **Sub-10ms finality** for transactions, thanks to a lightweight, deterministic voting round;
- **Adaptive Security**, as malicious behavior is rapidly flagged and quarantined;
- **High Scalability**, since adding more devices expands validation capacity instead of congesting the network;
- **No Resource-Intensive Mining**: Removing energy-intensive computations reduces both costs and centralization risks.

Token Standard

Naoris Protocol's native token conforms to the **ERC-20** standard, facilitating broad interoperability with existing toolkits and exchanges.

- **Device-Validated Transactions:** Each transaction is confirmed by multiple devices, leveraging post-quantum signatures to ensure authenticity.
- **Hierarchical Addressing:** The protocol supports hierarchical key derivation for flexible account management and enhanced security practices.

Post-Quantum Cryptography Standards

Naoris Protocol incorporates cryptographic primitives aligned with **NIST**, **NATO**, and **ETSI** post-quantum guidelines:

- **Dilithium-based Signatures:** Resilient to attacks from future quantum computers, preserving long-term transaction integrity;
- **Quantum-Resistant Hashing:** Ensures tamper-proof data structures that remain secure even under large-scale quantum capabilities.

Security & Cryptography Highlights

- **No Single Point of Failure:** Each device monitors all others, reinforcing security consensus;
- **Immutability:** The ledger's tamper-evident design uses quantum-safe hashing and block references;
- **Future-Proof:** As new PQ algorithms emerge, Naoris Protocol's modular design allows for cryptographic updates without compromising the integrity of historical records.

H3. Technology Used

Naoris Protocol is a high-speed, decentralized blockchain built around its Distributed Proof of Security (dPoSec) mechanism, achieving sub-10 ms transaction finality without relying on mining or staking. The network supports a range of tools to facilitate secure, post-quantum-ready operations. Users can employ standard ERC-20-compatible wallets for token handling, while hardware wallet integrations (e.g., Ledger, Trezor) provide enhanced security for private key storage.

Interoperability is addressed through modular bridging components and dedicated APIs/SDKs, enabling seamless connectivity with other chains and existing IT infrastructures. With its minimal transaction costs, advanced cryptography, and rapid finality, Naoris Protocol stands out as a robust solution

for organizations seeking secure and efficient on-chain validation—particularly in contexts where reliable, real-time protection against ever-evolving cyber threats is essential.

H4. Consensus Mechanism

Naoris Protocol employs Distributed Proof of Security (dPoSec), a consensus algorithm designed to maintain both high throughput and robust protection against cyber threats. Instead of selecting validators based on staking or computational resources, Naoris Protocol treats every connected device as a validator node, evaluating trust status in real time. This approach results in:

- **Sub-10ms finality:** Consensus is reached in milliseconds, as devices collectively confirm transactions without waiting for block confirmations;
- **Randomized Selection:** Each device's role is determined through a lightweight, verifiable random process at short intervals, ensuring no single entity can monopolize block creation;
- **Energy Efficiency:** dPoSec requires minimal computational overhead, eliminating the high energy demands associated with proof-of-work or continuously active staking;
- **Resilience and Security:** Through continuous trust checks on each device, malicious or compromised nodes are quickly detected and isolated, preserving the ledger's integrity.

By relying on cryptographically secure randomness and rigorous real-time validation rather than large stakes or mining power, dPoSec upholds Naoris Protocol's mission of providing a decentralized, post-quantum-ready environment that is both highly scalable and sustainable.

H5. Incentive Mechanisms and Applicable Fees

Naoris Protocol's **incentive and fee structure** is designed to reward continuous, real-time validation while ensuring minimal friction for users:

1. **Device-Based Rewards**

- **Validator Participation:** Instead of staking tokens or performing mining, every connected device that meets validation criteria is eligible for periodic rewards. A small portion of each transaction fee is pooled and allocated to these devices, reflecting the continuous security services they provide.
- **Trust Score and Bonus Incentives:** Devices maintaining high accuracy and consistent uptime earn additional bonuses, enhancing overall network reliability. Malicious or offline devices receive reduced or zero rewards, encouraging honest behavior.

2. **Transaction Fees**

- **Lightweight Fee Model:** The baseline transaction fee at less than a cent, aiming to accommodate frequent validation checks that occur in near-real time.
- **Proportional to Complexity:** While most transfers incur a minimal fee, more complex operations (e.g., multi-signature verifications or large data payloads) may requires lightly higher fees to reflect additional computation.
- **Fee Distribution:** Collected fees are distributed among active validator devices and a sustainability reserve, ensuring the protocol can fund ongoing development and potential network upgrades.

H6. Use of Distributed Ledger Technology

No. DLT not operated by the issuer or a third-party acting on the issuer's behalf.

H7. DLT Functionality Description

The Naoris Protocol does not rely on a single entity but is rather operated by all nodes participating in transaction validation and block generation. The network is sufficiently decentralized so that there is no central party operating the system. Anyone is open to operate a node and contribute to Naoris Protocol's operation.

H8. Audit

Yes

H9. Outcome

The Naoris Protocol has undergone independent audits by third-party organizations specializing in software and blockchain technology. The most recent, and therefore relevant for the current code base, was conducted in 2025 by Hashlock, a cybersecurity firm.

J. INFORMATION ON THE SUSTAINABILITY INDICATORS IN RELATION TO ADVERSE IMPACT ON THE CLIMATE AND OTHER ENVIRONMENT-RELATED ADVERSE IMPACTS

J.1 Mandatory information on principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism

General Information	
S.1 Name	NDSE Cyber Ltd
S.2 Relevant legal entity identifier	Company registration number 207328 B
S.3 Name of the crypto-asset	$Naoris
S.4 Consensus Mechanism	Distributed Proof of Security (dPoSec) Naoris turns every staked device into a validator + watchdog. Randomly chosen nodes propose blocks, and any one of them can invoke a “rationality clause” to halt finality and force a broader vote if something looks off; honest nodes earn rewards, malicious ones are slashed . The engine layers Proofs of Availability, Integrity and Evidence onto PoS-BFT, so

	the mesh audits itself in real time while still achieving rapid, low-fee finality .
S.5 Incentive Mechanisms and Applicable Fees	● **Device-first validator economy (dPoSec).** Every phone, server or IoT sensor that runs the lightweight Naoris agent can join the validator pool. To participate, the device (or its operator) stakes $NAORIS; good behaviour earns continuous block-rewards and service fees, while downtime or malicious activity triggers slashing. This “machine-to-machine” loop turns the network’s attack surface into its defence surface, because each device is financially motivated to police every other device in real time. ● **Sub-cent transaction fees.** Thanks to the dPoSec consensus and Layer-2 architecture, normal on-chain actions—post-quantum signatures, threat attestations, data writes—settle for **well under $0.01 per transaction**, keeping Naoris

	usable for everything from micro-payments to high-frequency device telemetry. The protocol is engineered to operate at "near-zero" or even "zero-fee" cost when network utilisation is high. ● **Reward recycling and slashing.** A portion of each micro-fee flows back to honest validators as block incentives; another slice funds the Swarm-AI security treasury, ensuring constant model updates. If a validator submits fraudulent data or stays offline, the protocol automatically burns part of its stake, redistributing the remainder to the validators that exposed the fault. ● **Delegated staking for non-technical holders.** Token-holders who don't want to run hardware can delegate their $NAORIS to community validator pools. They share in the same reward stream, increasing decentralisation while lowering the capital threshold to earn yield.

S.6 Beginning of the period to which the disclosure relates	2025/07/31
S.7 End of the period to which the disclosure relates	None.
Mandatory key indicator on energy consumption	
S.8 Energy consumption	dPoSec's agent leverages idle CPU cycles on host devices—phones, servers, or IoT sensors; so consensus duties never exceed ≈ 0.1 % of available processing power. At this level the workload is effectively absorbed by the device's normal power-management envelope; no additional wattage is drawn beyond its baseline consumption. All node classes share this footprint. Full Nodes maintain the ledger, standby nodes stake and await selection, active Validators are randomly promoted for one round of block work, and High-Security Nodes perform a final audit. Each role runs the same constant-time attest-and-vote routine, keeping energy use flat across promotions. Precise figures will be published after main-net launch, but lab tests confirm dPoSec delivers its security guarantees with negligible incremental power demand.
S.9 Energy consumption sources and Methodologies	Energy consumption estimates based on theoretical calculations of device validation requirements.

	Actual measurements will be conducted post-mainnet launch using industry-standard monitoring tools.

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

Naoris Protocol's dPoSec consensus mechanism represents a significant advancement in energy-efficient blockchain technology. Unlike traditional Proof-of-Work systems, dPoSec requires minimal computational resources, as it relies on lightweight trust validation rather than energy-intensive mining. The protocol's design prioritizes sustainability while maintaining security and performance, aligning with global environmental goals and ESG standards.