Net3 Whitepaper

The Third-Generation Private Communication Network Infrastructure

September 2, 2024

V0.1

www.net3.org
hi@net3.org

Abstract – In 2023, the global market size for private communication networks was approximately $54 billion. According to authoritative forecast reports, the global private communication network market is expected to reach $103.69 billion by 2029, with a compound annual growth rate (CAGR) of 17.2%. We are optimistic that the private communication network sector represents a significant growth market.

The development of traditional private communication network technologies is relatively mature; however, there are still practical challenges between service providers and consumers. These challenges include reduced network speeds, high performance requirements for servers, incompatibility with all applications, security vulnerabilities, high operational costs, the need for a certain level of technical expertise, and the risk of being blocked by local internet service providers. Therefore, we believe that continuous technological innovation is essential to address these real-world issues and improve the usability of private communication networks.

As blockchain technology matures, Web3 has seen widespread adoption. Through its inherent economic model, Web3 connects everyone, fundamentally transforming the mechanism of value distribution. In this new paradigm, every individual becomes a service provider, and everyone can benefit economically from the services they contribute.

Amid the wave of Web3 development, DePIN (Decentralized Physical Infrastructure Network) has started to emerge. DePIN refers to the use of crypto-economic protocols to deploy real-world physical infrastructure and hardware networks. By leveraging token-based incentive mechanisms, it encourages participants to collaboratively build physical infrastructure networks. This presents a disruptive innovation with the potential to address the shortcomings of existing private communication networks.

Net3 will become the industry's first private communication network provider to adopt the DePIN model, continuously exploring cutting-edge technologies in this field. Therefore, we proudly define Net3 as the third-generation infrastructure for private communication networks.

Contents

I. Introduction

This document provides an overview of Net3's architecture, applications, network features, tokenomics, and development plans. In the future, we will offer more detailed content, particularly focusing on consensus and governance mechanisms. It is important to note that our architecture is holistic, with all applications and components working together in a modular, integrated manner to ensure seamless collaboration.

The remainder of this document is structured around three core sections. First, we will introduce and discuss the fundamental theoretical basis of the Net3 Private network, including its essential foundational applications and potential use cases, while providing guidance for developers on how to leverage the platform. Second, we will delve into the relevant concepts surrounding the Net3 blockchain and its validation implementation. Finally, we will outline our development roadmap, offering initial insights and exploring future directions, with a commitment to ongoing improvement and innovation.

II. Net3 Private Communication Network

A. Overview

The Net3 private communication network is built on its own public blockchain, incorporating a consensus mechanism, smart contracts, and a token economic model. Net3 has designed a solution tailored for the AI era, supporting cross-regional information flow and third-party application deployment. By leveraging its advanced networking protocols and network scheduling algorithms, Net3 addresses the challenge of network Private protection with extremely low costs and high efficiency.

The development of the Net3 private communication network will be structured around four key milestones: the Net3 Beacon Network, the Net3 Protocol Private Network, the Net3 Telecom Private Network, and the Net3 Interstellar Private Network. Each of these milestones represents a significant step in advancing the network's capabilities, progressively enhancing Private, scalability, and global reach.

In the first phase, Net3 will focus on building a private communication network at the software protocol layer. Subsequent phases will expand to the Net3 proprietary telecom Private network and the Net3 interstellar connectivity Private network, progressively enhancing the scope and capabilities of the network.

B. Core Products

Currently, Net3 has designed eight core foundational products. In addition, we offer a standard software development kit (SDK) that supports the deployment of any third-party applications, enabling seamless integration and fostering a robust ecosystem of Private-focused solutions.

B1.Net3 Core

Net3 Core functions as a central server, responsible for managing the blockchain network, bandwidth network, encryption keys, network changes, and access policy modifications. It maintains connections with all nodes within the Net3 network. Net3 Core is part of the control plane rather than the data plane, meaning it does not relay traffic between machines, thereby avoiding becoming a performance bottleneck.

B2.Net3 Link

Net3 Link is the core networking protocol of the Net3 private communication network. To maximize compatibility across various networking protocols, the current Net3 networking module integrates several mainstream protocols, including WireGuard, SSL-VPN, L2TP, OpenVPN, and SST. Additionally, Net3 Link has the ability to dynamically schedule multiple protocols in real-time, ensuring high availability for global private connections.

B3.Net3 Web

Net3 Web is the private network service interface created by the Net3 management console. It natively supports end-to-end encryption and security control policies, while also bridging the Net3 blockchain network. With Net3 Web, users can facilitate private information exchange and interact with digital assets securely.

B4. Net3 Waf

Net3 Waf provides near-zero-cost access protection services for hundreds of millions of enterprise applications globally. It can dynamically reroute user requests to the nearest service node based on real-time analysis of network traffic, node connections, load conditions, proximity to users, and response times. This ensures service continuity by preventing outages caused by malicious attacks, enhancing overall network resilience.

B5.Net3 Edge

Net3 Edge is a relay edge service for connecting network devices, operating as a globally self-healing Anycast network. It provides stable connectivity for both the Net3 blockchain network and the distributed bandwidth network, ensuring reliable performance and seamless integration across the global network infrastructure.

B6.Net3 SDK

Net3 SDK supports third-party development, enabling the rapid deployment of their solutions. It provides a P2P SDK for developers of various applications, such as games and video platforms, allowing seamless integration into their apps. This ensures a continuous and stable connection between the application and its end users, eliminating concerns about network quality and global scalability.

B7.Net3 TPN

Net3 TPN, or Net3 Telecom Private Network, enables network connections for smart devices, including call handling and SMS services, without the need for any third-party intermediaries. This ensures secure and private Telecoms while maintaining full control over the communication infrastructure.

B8.Net3 IPN

Net3 IPN, or Net3 Interstellar Private Network, is a global, high-capacity, low-latency interstellar Private communication system. It provides high-speed private internet services across the globe and into space, ensuring secure and efficient connectivity for users regardless of their location, even in extraterrestrial environments.

C. Network Features

The Net3 network elevates Private and security to a new level while being more affordable and user-

friendly. It combines cutting-edge technologies and innovative protocols to deliver enhanced Private protection, making secure communication more accessible and efficient for users worldwide.

C1. Decentralized Mesh Network

Net3 operates on countless decentralized physical devices across the globe, with each node seamlessly interconnected. Unlike the traditional hub-and-spoke model, the mesh network connects nodes directly to one another, facilitating enhanced redundancy, fault tolerance, and multiple data paths for load balancing. This architecture ensures a more resilient and efficient network, capable of adapting to changing conditions while maintaining high performance and security.

- Strong resistance to node failures, highly scalable, with reduced latency and more balanced traffic distribution.
- Direct connections reduce latency and optimize application performance.
- No single point of failure; even if individual nodes fail, the network continues to operate smoothly.
- Increased Private by making data tracking and analysis more difficult.
- New nodes can be flexibly added without affecting overall performance.
- High efficiency in resource sharing and processing between nodes.

C2.End-to-End Encryption

The Net3 private communication network utilizes popular end-to-end encryption (E2EE) technology, ensuring that no middleman can decrypt messages during transmission. This maximizes the protection of personal Private data from interception or decryption.

End-to-end encryption (E2EE) is a method of encoding messages sent from one endpoint to another. E2EE ensures that data encrypted at the sender's end can only be decrypted by the intended recipient. As a result, messages remain hidden throughout their transmission via intermediary servers, making them inaccessible to network service providers, internet service providers (ISPs), or any third parties.

End-to-end encryption (E2EE) works through the following steps:

- Key Generation: The system using end-to-end encryption generates a pair of encryption keys: a public key and a private key. The public keys are shared between the sender and the receiver, while each party keeps their own private key.
- Encryption: When the sender sends a message, the end-to-end encryption algorithm uses the receiver’s public key to encrypt the message. Only the receiver can decrypt the message using their private key.
- Transmission: During the transmission process, even if the encrypted message is intercepted, it is virtually impossible for the interceptor to understand the content. Without the receiver’s private key, the interceptor cannot decrypt the message.
- Decryption: Once the receiver receives the encrypted message, their private key decrypts the message, making the content readable.

C3. Network Penetration

People often experience communication failures due to certain "unknown issues." For example, when traveling in a specific country and attempting to access websites like OpenAI, Google, or Steam, connections may fail. However, access to other international websites, such as Yahoo, might still be possible.

The Net3 network, with its globally distributed nodes, can resolve 99% of such network access issues, including:

- Unstable connections to gaming servers.
- Blocked access to certain services.
- Slow network connections.

Net3 provides a robust solution to these challenges by ensuring reliable and secure access to online services, overcoming regional restrictions, and improving overall connection quality.

C4. Free Usage

Thanks to Net3's advanced blockchain-based economic model, the Net3 network is freely accessible to everyone, including but not limited to:

- Individual consumers.
- Application developers.
- Enterprise users.

This open access allows a wide range of users to leverage the network's Private, security, and efficiency

benefits without financial barriers, promoting broader adoption and innovation.

C5. Earning Tokens

The Net3 network allows volunteers from communities worldwide to contribute their idle servers, as well as computers and smart devices, as node servers within the Net3 distributed bandwidth network. This not only maximizes the utilization of idle resources but also enables participants to earn Net3 token rewards through traffic mining after connecting to the Net3 network.

From the consumer's perspective, by using Net3 services, they can become part of the network's consensus and earn Net3 token rewards, including those using the service for free. This incentivizes both resource contribution and service usage, fostering a sustainable and decentralized ecosystem.

C6. Cross-Platform Support

Net3 services are supported across all platforms, including the following clients:

- Linux Client.
- Windows Client.
- Mac Client.
- Android Client.
- iOS Client.
- Chrome Client.

This wide range of platform support ensures that users can seamlessly access Net3's private communication services on virtually any device, enhancing flexibility and accessibility.

C7. AI Algorithm Optimization

The Net3 network integrates AI algorithms and features a scalable, guided, multimodal large language model (LLM). With AI algorithm optimization, the Net3 network possesses the following capabilities:

- Optimal routing scheduling algorithms based on real-time global network conditions.
- Automatic link optimization tailored to the specific structure of each network detected.
- Automatic network adjustments based on cost, bandwidth, and quality to improve network efficiency.
- ChatGPT-like services, reducing the learning curve for users and simplifying network usage.

This AI-enhanced infrastructure ensures smarter, more efficient, and user-friendly network management.

C8. Post-quantum Cryptography

Post-quantum cryptography is a powerful field of computer science that aims to use existing computer technologies to crack quantum encryption algorithms on quantum computers, thus protecting data security. The development of this technology arose in response to quantum encryption algorithms, which leverage quantum computers for data encryption, using sufficiently long keys to safeguard Private and ensure secure communication free from eavesdropping threats. However, if one masters post-quantum algorithms, they could potentially break quantum encryption, compromising data security.

The National Institute of Standards and Technology (NIST) has been actively seeking new algorithms capable of resisting attacks from quantum computers. Since opening the submission process in 2016, NIST has narrowed down the pool to four finalists and three alternate algorithms. These new algorithms employ techniques designed to withstand attacks from quantum computers using Shor's algorithm.

The four post-quantum algorithms that have made it to the finals for NIST's post-quantum encryption standard (Crystals-Kyber, CRYSTALS-DILITHIUM, FALCON, and SPHINCS+) serve two primary purposes:

- General encryption to protect information exchanged over public networks.
- Digital signatures for authentication purposes.

These algorithms represent a major step forward in protecting against the potential threats posed by quantum computing.

NIST provides all of the (candidate) algorithms on its website for reference if needed, and Net3 will integrate post-quantum cryptography at the appropriate time. This forward-looking approach ensures that Net3 remains at the forefront of security advancements, preparing to safeguard data against potential quantum computing threats as the technology evolves.

- https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-

standardization/round-3-submissions

D. Core Technologies and Principles

The Net3 team brings extensive experience in the field of network communications, particularly excelling in algorithms, protocols, and architecture. Our expertise in these areas positions us at the forefront of the industry, ensuring that we consistently deliver cutting-edge solutions and innovations.

D1. Algorithm

- Provides the best routing scheduling algorithm available on the market.
- Deploys Anycast protocol globally, with full control over the entire foundational Anycast network.
- Automatically adjusts link conditions based on cost, bandwidth, and quality.
- Reduces the initial impact of DDoS attacks through distributed traffic and adjustable scheduling mechanisms.

These features ensure optimal network performance, resilience, and security in dynamic environments.

D2. Protocol

- Developed a high-performance Layer 2 encapsulation protocol in-house.
- Capable of operating within any IP network.
- Proprietary high-performance Net3 Link networking protocol.
- Configurable access policies tailored to different political environments across global regions.

These capabilities enable Net3 to offer highly adaptable, secure, and efficient network solutions regardless of the underlying infrastructure or geopolitical context.

D3. Technical Architecture

- High scalability for smart devices, with each extended function strongly tied to the borderless network.
- Seamless integration of each value-added service with the main network, creating a frictionless modular experience.
- Networks are differentiated as either collaborative or SDK-created through a tagging system.
- Networks created via the SDK can still interact with Net3 main network services for business or data exchanges.
- Modular support is available for developers to deeply customize solutions based on different scenarios.

These features ensure that Net3 provides flexible, scalable, and integrated solutions for diverse use cases, enabling smooth interactions across various platforms and environments.

E. Technical Advancements and Challenges

Through the points discussed above, we demonstrate a natural advantage in algorithms and protocols. The key challenges in the algorithm space lie in the need for substantial network operation data, peer-to-peer network data, and a deep understanding of machine learning algorithms for effective training.

On the protocol side, challenges involve cross-platform compatibility and performance optimization, requiring a deep knowledge of infrastructure to develop a new high-performance cross-platform protocol. We have nearly completed this work, and our performance significantly surpasses mainstream proxy protocols.

Once we train a high-quality switching algorithm through deep learning on this data, it will be integrated with large language models (LLM) to create an automated optimization solution, offering network-specific adaptations based on the detected structure of each network.

From an architectural perspective, Net3 Edge is unprecedented in the industry. If we position Net3 Edge as a source-distinguishing solution that doesn't participate in decryption, the difficulty lies in the substantial modifications required to the Linux kernel to support native relaying. Competing products lack this feature; their "nodes" either decrypt traffic within the network or operate with a simplistic, unfocused forwarding model that can't distinguish between sources and destinations, nor can they provide commercial metrics and segmentation.

Moreover, the architecture for smart devices is unparalleled in similar products. The complexity here lies in integrating devices into user networks while

reusing the same relay controller, requiring distinction between different modules within the relay to provide services on the business platform. This level of modular control and service differentiation is a challenge that competitors have yet to address.

III. Net3 Blockchain

A. Overview

The Net3 network is built on its own public blockchain, which includes a consensus mechanism, smart contracts, and a token-based economy. These components form the backbone of Net3's decentralized infrastructure, ensuring secure, transparent, and incentivized operations within the network. This architecture enables efficient resource sharing and user participation, while fostering innovation through its robust economic model.

B. Smart Contracts

Smart contracts are programs stored on the blockchain that execute when predetermined conditions are met. They are typically used to automatically enforce agreements so that all participants can immediately verify the outcome without intermediaries, saving time and resources. Smart contracts can also automate workflows by triggering the next action when conditions are satisfied.

The Net3 network incorporates several smart contracts, including:

- Base Protocol.
- Accounts.
- Token Issuance.
- Transactions.
- PoW Algorithm.
- PoS Algorithm.
- Supplier Identity.
- Consumer Identity.
- Validator Identity.
- Communication Protocol.
- Programmable Communication SDK.
- Epoch.
- Governance (Gov).
- …

These smart contracts automate various functions within the Net3 ecosystem, streamlining operations and ensuring the smooth functioning of the decentralized network.

C. Blockchain Wallet

A blockchain wallet is a digital storage solution for cryptocurrencies, allowing users to store, manage, and transact their digital assets. Unlike traditional wallets that hold physical cash, a blockchain wallet doesn't store actual coins or tokens. Instead, it stores the private and public keys associated with a user's cryptocurrency holdings. These keys enable users to access and control their funds on the blockchain.

Blockchain wallets operate on the principles of blockchain technology, which is a decentralized and distributed ledger system. When a user creates a blockchain wallet, they are assigned a unique address on the blockchain, used for sending and receiving cryptocurrency.

Key features of a blockchain wallet include:

- Receiving Crypto Assets: When a user requests funds, they share their blockchain wallet address with the sender. The sender uses their private key to digitally sign the transaction and broadcasts it to the blockchain network. Once verified, the transaction is recorded on the blockchain, updating the recipient's wallet balance.
- Sending Crypto Assets: To send funds from a blockchain wallet, the user specifies the recipient's address and the amount. The user then signs the transaction with their private key. The transaction is broadcast to the network, verified by miners, and added to the blockchain.

This system ensures that users can securely manage their digital assets and perform transactions in a decentralized environment, without the need for intermediaries.

D. Blockchain Explorer

A blockchain explorer (also known as a block explorer) is a software application that allows users to retrieve, visualize, and view metrics related to blockchain networks. It provides crucial information about cryptocurrency transactions, such as transaction history, wallet balances, transaction fees, and more.

Key features of a blockchain explorer include:

- Transaction History: Users can view the

transaction history for any given wallet address, including details about sent and received transactions.

- Block Analysis: It offers detailed information about each block, such as the timestamp, block size, miner information, and the transactions included within that block.
- Real-time Tracking: The explorer allows users to track blocks and transactions in real time, offering up-to-date data on when transactions are broadcast and confirmed.

This tool is essential for gaining insights into the workings of a blockchain, ensuring transparency and traceability of cryptocurrency transactions.

E. Roles

In the Net3 network, there are three primary roles: Suppliers, Consumers, and Validators. These roles form the core foundation for the smooth operation of the Net3 network, ensuring its functionality and efficiency. The distribution of Net3 token rewards is allocated among these three roles.

These roles work together to maintain the decentralized ecosystem, with token rewards acting as incentives for participation and contribution.

E1. Supplier

Suppliers are volunteers from around the world who provide bandwidth servers or other smart network devices, continually expanding the boundaries of the Net3 distributed bandwidth network. Suppliers are the core of the Net3 distributed Private edge network. During the operation of the Net3 network, suppliers are rewarded with Net3 network tokens for their contributions.

By offering resources, they help ensure the scalability, Private, and efficiency of the network, making them a crucial part of its decentralized infrastructure.

E2. Consumer

Consumers in the Net3 network are not real-world individuals; rather, they can be any type of endpoint, such as Linux, Windows, macOS, iPhone, Android, and other devices. Consumers are the bandwidth users within the Net3 distributed Private network, responsible for proving the genuine flow of bandwidth. During the operation of the Net3 network, consumers also receive Net3 token rewards for their participation in validating and utilizing network bandwidth, contributing to the overall functionality of the decentralized system.

E3. Validator

Validators are volunteers from around the world who operate Net3 blockchain nodes, playing a crucial role in maintaining the decentralized nature of the Net3 network. We encourage everyone to run a Net3 blockchain node and participate in the governance of the Net3 blockchain network. During the operation of the Net3 network, validators are rewarded with Net3 tokens for their contributions, ensuring the integrity and security of the network while actively participating in its decentralized governance.

F. Consensus Mechanism

The Net3 network's consensus mechanism is composed of both Proof of Work (PoW) and Proof of Stake (PoS) mechanisms. These two consensus models work together to ensure the security, efficiency, and decentralization of the network.

By combining PoW and PoS, the Net3 network balances energy consumption, security, and fairness in its token reward distribution.

F1. Proof of Work (PoW)

Proof of Work (PoW) is an economic mechanism designed to counteract service and resource abuse, such as denial-of-service (DoS) attacks. It typically requires users to perform computationally intensive tasks, where the solution can be quickly verified by the service provider. The time, hardware, and energy consumed act as collateral, ensuring that the services and resources are being utilized by legitimate needs. Bitcoin is a classic example of PoW.

In the Net3 network, PoW can be abstracted as network traffic mining, where traffic is the core, quantifiable metric within the system. We conceptualize the flow of network traffic as part of the consensus process, which involves Suppliers,

Consumers, and Validators. Suppliers provide network bandwidth, consumers use the traffic, and validators are responsible for recording the transaction information on the blockchain.

This PoW-based model in Net3 ensures that the resources provided by suppliers and the traffic consumed by users are validated and securely recorded through a decentralized consensus process, creating a balanced and efficient network economy.

F2. Proof of Stake (PoS)

Proof of Stake (PoS) is a blockchain consensus algorithm where blocks are produced and approved by randomly selected validators. Validators "stake" native network tokens by locking them within the blockchain. The more tokens a validator stakes, the greater their chances of being selected to validate transactions and produce new blocks. In return, validators earn rewards based on their staked tokens, incentivizing them to secure and verify the network. Ethereum is a classic example of PoS in action.

In the Net3 network's staking process, token holders stake a certain amount of tokens to assist validators in verifying transactions and producing blocks. In return for their participation, stakers receive token rewards, promoting both network security and user engagement through a decentralized reward system.

G. Token Allocation

The Net3 Token is the sole governance token of the Net3 network, with a total supply of 102.4 billion tokens.

The token distribution is as follows:

- Community Foundation: 6% of the total supply, amounting to 6,144,000,000 tokens.
- Team: 5% of the total supply, amounting to 5,120,000,000 tokens.
- Fundraising: 6% of the total supply, amounting to 6,144,000,000 tokens.
- PoW & PoS Output: 83% of the total supply, amounting to 84,992,000,000 tokens.

incentivizing participants in both PoW and PoS processes while providing necessary allocations for team operations, fundraising, and foundation activities.

IV. Roadmap

The journey from concept design to product implementation for Net3 requires meticulous planning, as building the third-generation private communication network infrastructure is a challenging endeavor. We will achieve this ambitious goal through four phases of dedicated effort. Step by step, we aim to provide free access to the Net3 private communication network for everyone worldwide, while helping users reclaim their network Private sovereignty.

A. Phase 1 - Beacon Network

In this phase, the primary focus is on collecting and clustering global foundational network operation data. After being processed through AI training, these data sets will provide scientific support for the foundational construction of the Net3 network, core network development, networking protocols, scheduling algorithms, bandwidth server deployment, and blockchain node deployment. This data-driven approach ensures that the network infrastructure is built on a solid, optimized foundation.

B. Phase 2 - Protocol Private Network

The key focus of this phase is the development of the Net3 core network, addressing data Private and flow through the software protocol layer. The core products must not only meet current market demands but also lay the technical groundwork for the next stages of development. This ensures that the Net3 network is both scalable and adaptable to future advancements in Private and communication technologies.

C. Phase 3 - Telecom Private Network

This phase, known as the Net3 Telecom Private Network, focuses on the construction of physical infrastructure for the Net3 telecom Private network. It includes the development of the telecom core network, transmission network, access network, and the integration of the Net3 core network.

With the Net3 client, users can directly connect to the Net3 telecom Private network, providing a direct replacement for traditional telecom operators. By

rebuilding the Private communication network at the physical layer, Net3 addresses and resolves various real-world issues that traditional Private networks face at the protocol layer, offering a more secure, private, and efficient solution.

D. Phase 4 - Interstellar Private Network

This phase, known as the Net3 Interstellar Private Network, focuses on developing and implementing a satellite constellation leasing plan, ground terminal development and integration, private transmission protocols for space-to-ground communication, ground station development and integration, scheduling system development, and further integration with the Net3 core network.

The Net3 Interstellar Private Network represents a low-orbit satellite-based private internet initiative that transcends the geographic limitations of traditional telecom networks. It aims to provide internet services anytime, anywhere, particularly in remote regions, oceans, high altitudes, space, and conflict zones. This phase ensures that Net3 can deliver secure, private communication even in the most challenging and isolated environments.

V. Audit Rules

We believe that any product should be issued with respect for the laws and regulations of each country. To comply with global legal frameworks and ensure the stable operation of Net3, the Net3 community will continuously refine its content filtering rules for inappropriate information.

In your region, if you use Net3 to engage in illegal or non-compliant activities, your communication will be automatically terminated.

Regarding Private, we only record real-time activities based on publicly defined rules, and we do not log your communication directions or content. Please rest assured that your Private is respected. At the same time, we appreciate your understanding of our efforts to manage such inappropriate behavior.

We will continuously update and publish detailed audit rules through the community. Please stay tuned to our official website for the latest information. Thank you.

VI. Statement on Compliance with Regional Administrative Regulations

This project is a non-profit research initiative under the Net3 Foundation. For the legal and compliant implementation of our products, we may provide specialized versions based on local administrative regulations.

We aim to maintain open communication channels with the governments of the regions where the project is implemented and sincerely hope to receive their support.

If the government or administrative bodies of the project's implementation region believe that this project is unsuitable for their area, we kindly request that they contact us (the Net3 project team) to discuss any concerns in accordance with local laws, regulations, or special circumstances.

We are fully committed to collaborating and cooperating to the greatest extent possible. If there are any requirements or questions, please feel free to contact us via the email address below.

Thank you for your understanding and support.

VII. Anti-Abuse Policy

Anyone can use the Net3 distributed bandwidth network to hide their IP address. It is expected that most users will utilize this feature for legitimate purposes. However, some may abuse this functionality for illicit activities such as fraud, child exploitation, money laundering, and other illegal actions. To combat such misuse, Net3 has established the following anti-abuse policy:

- Monitoring and Detection: We will deploy advanced systems to detect suspicious activity or patterns that suggest misuse of the network, while maintaining user Private in compliance with our Private policy.
- Reporting Mechanisms: Users and partners are encouraged to report any observed illegal activity within the network. Net3 will promptly investigate any reported cases of abuse.
- Automatic Termination: If illegal activities are detected, the user's connection will be automatically terminated to prevent further misuse.

- Collaboration with Authorities: Net3 is committed to cooperating with local and international authorities to address serious legal violations, while balancing the protection of user Private and security.
- Preventive Measures: We will continuously update our abuse detection systems and improve policies to prevent the use of the network for harmful activities.

By implementing this anti-abuse policy, Net3 aims to ensure that the network remains a safe and secure space for all users while upholding the principles of Private and freedom.

VIII. Terms and Concepts

This document outlines several key components and concepts relevant to the Net3 network and its operation:

- ACL (Access Control List): Uses rules from Net3 policy files to manage system access. You can filter traffic using ACLs and enhance security by controlling who can access specific resources.
- Tags: Allow you to assign an identity to a device (distinct from human users). Tags can be used in access rules to restrict access based on device identity.
- Management Console: The central hub for viewing and managing the Net3 network. You can manage nodes, users, permissions, and settings like key expiration. It also notifies you of available Net3 client updates for your devices.
- CLI (Command Line Interface): A powerful command set, included with Net3 installations on Linux, macOS, and Windows, offering capabilities beyond GUI applications.
- Devices: Any entity, physical or virtual, that sends, receives, or processes data on the Net3 network, excluding users.
- Device Key: A unique public/private key pair assigned to a specific device. Multiple users can use a device key, but each device has only one key. A combination of a user and a device key represents a unique node.
- Key Expiration: Refers to the end of the validity period for encryption keys. Expired keys can no longer encrypt or decrypt data or authenticate a device on the Net3 network. Net3 automatically handles key expiration and renewal. You can disable key expiration for long-term devices from the management console.
- Network Topology: The arrangement of nodes within a network, illustrating their interconnections. Examples include star, bus, mesh, and hybrid topologies. Traditional VPNs use a hub-and-spoke topology, routing all traffic through a central gateway. Net3 uses a mesh topology, where each machine communicates directly with others using NAT traversal.
- Firewall: Restricts network traffic between points. Firewalls can be hardware- or software-based. Net3 includes a built-in firewall governed by domain-specific access rules.
- Identity Provider: A method of user authentication on Net3. Examples include Google, Microsoft, Binance, and Wallet Connect. Net3 may rely on these or other providers for user verification.
- NAT: A method for connecting nodes across barriers like firewalls or network address translation (NAT) devices. NAT traversal enables communication between devices that would otherwise be blocked.
- Tunnel: A secure, encapsulated connection between points in a network, allowing users, nodes, or resources to communicate securely over a public network.
- WireGuard: A modern, lightweight protocol that uses advanced encryption techniques for fast and secure connections.
- Blockchain: A decentralized distributed ledger technology that records transactions and information in a growing chain of blocks. It ensures data security and transparency, maintained by computers worldwide rather than a central authority.
- Mining: The process of verifying blockchain transactions and creating new cryptocurrency units.
- Web3: The third generation of internet technology, also known as the decentralized internet, which returns power to users through ownership using blockchain, cryptocurrencies, and NFTs.
- Staking: The process of locking your cryptocurrency in a specific wallet address on the

blockchain to participate in network operations and transaction validation, earning rewards in return. From a user experience perspective, staking is similar to depositing money in a bank and earning interest, though the sources of income differ.

- NIST: The National Institute of Standards and Technology (NIST) is part of the U.S. Department of Commerce. It conducts research in physics, biology, engineering, and measurement techniques, and provides standards, reference data, and related services with a high reputation internationally.

This collection of components and definitions forms the foundational understanding needed to effectively use and manage the Net3 network and its associated technologies.

IX. Open Source Code

- Core components are released under the GPLv2 license.
- Other projects are licensed under MIT, BSD, Apache 2.0, or GPL.
- The source code is hosted on GitHub.

These licensing models ensure open-source access while maintaining flexibility for contributors and users. Each project within the Net3 ecosystem follows a specific licensing agreement that governs how the code can be used, modified, and distributed.

X. Community and Communication

- Website：https://net3.org
- Github：https://github.com/net3org
- Twitter：https://twitter.com/net3org
- Telegram：https://t.me/net3org
- Youtube：https://youtube.com/net3org
- e-mail：hi@net3.org

XI. Version Update Statement

This whitepaper is intended only as a high-level overview of Net3 products. Due to certain reasons, we are currently unable to disclose the technical details of the related products. A more detailed version will be released prior to the launch of the testnet.

This project follows an established technical roadmap and milestones, but unforeseen issues may arise that could result in changes or delays. Based on real-world circumstances, we will update the whitepaper accordingly. Please stay tuned for the latest updates. Thank you for your understanding and continued attention.