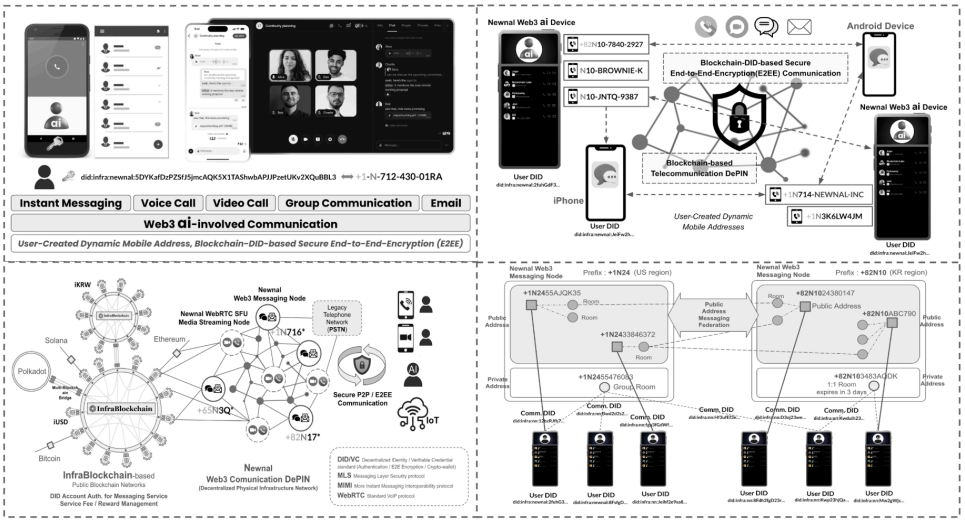
Web3 ai **Newnal** - Technology 3

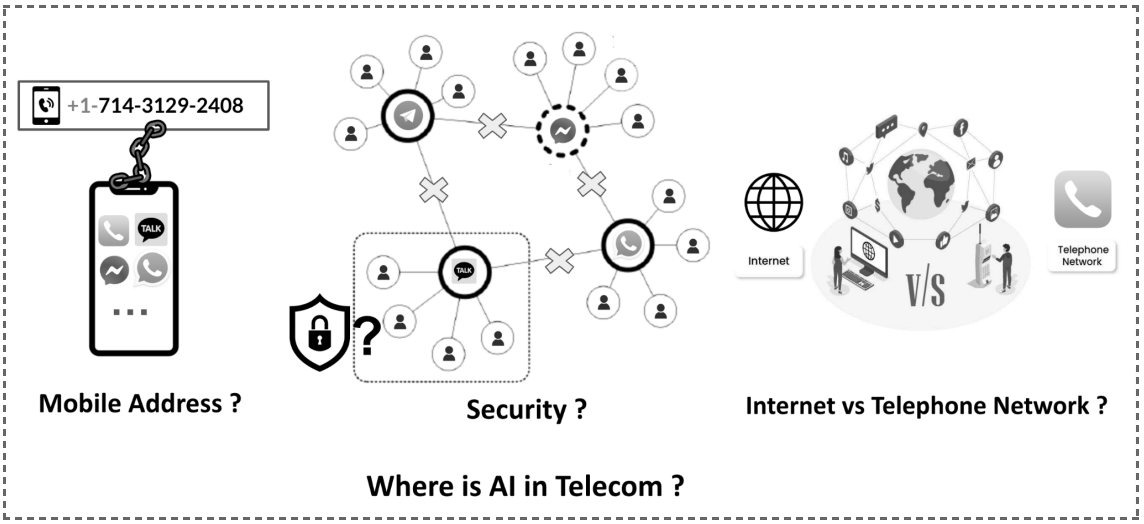
Web3 Telecom

Next-generation secure communication protocol including AI-involved calls.



Telecommunication has a long history beginning with the advent of modern communication technology in the late 19th century. Bell's Telephone (1876), the beginning of voice calls, and Marconi's wireless Telegraph (1896), the beginning of text message technology, laid the foundation for modern telecommunication technology. In the 20th century, with the invention of computers and the Internet, all communication technologies were digitized and later developed into the current high-speed communication system through the development of optical cable technology and cellular technology. Instant messaging, voice calls, and video calls are the main functions of mobile devices, allowing anyone to communicate in real time anywhere in the world with a mobile phone. Telecommunication technology, which has made such great developments, is still moving toward new innovations in the Web3 ai paradigm, not staying in the present.

Limitations of Web 2.0 Communication

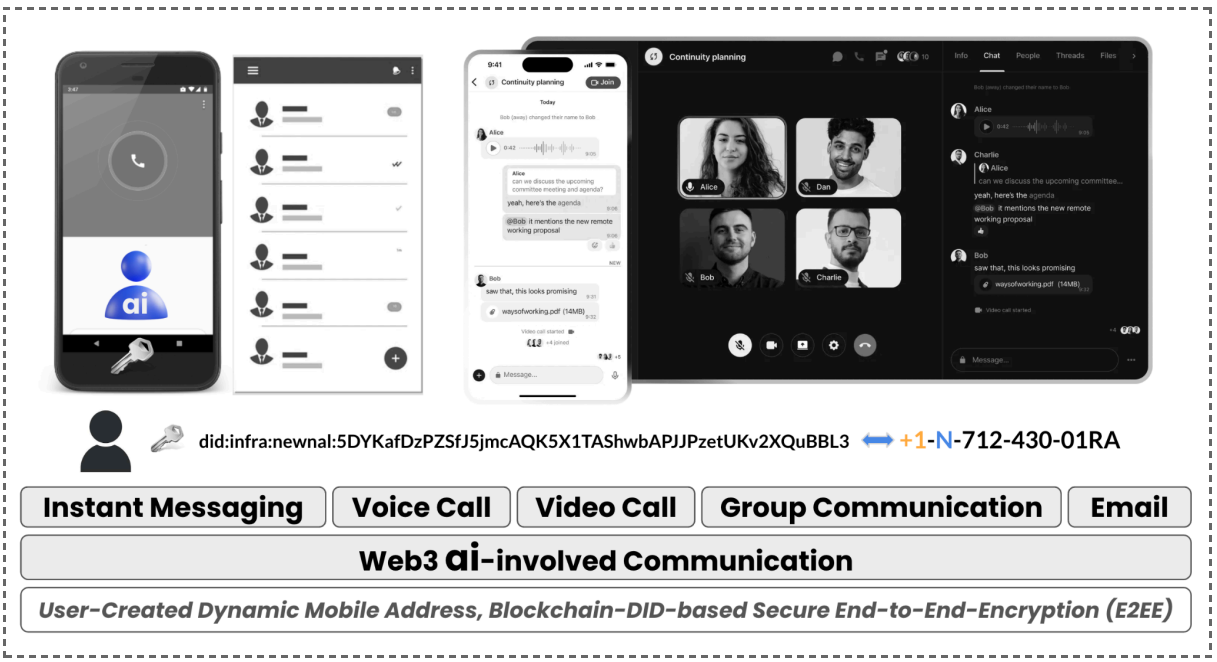


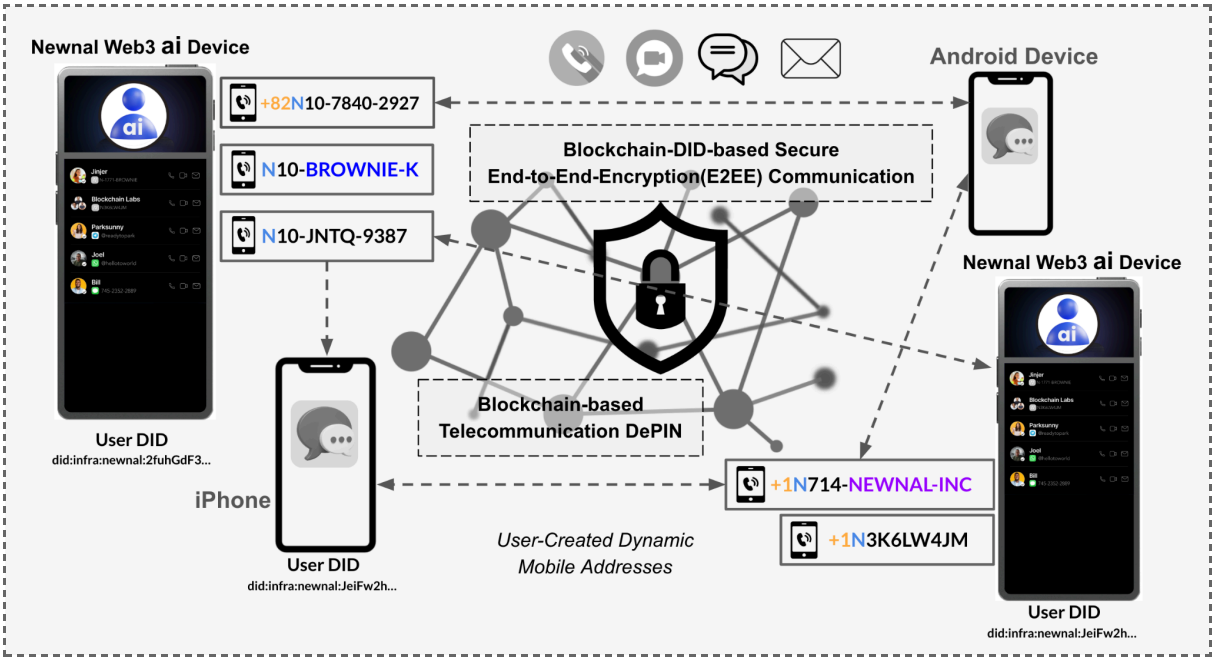
There are various problems in the current Web 2.0 communication paradigm. Only one phone number is connected to each mobile device, and in general, the user maintains the same phone number for a long time. If the phone number is leaked, the phone number owner would be exposed to serious risks such as spam advertisements, smishing, voice phishing, and personal information theft. The existing phone number system does not have an authentication function in itself for the phone number owner, so secure real time mutual authentication is impossible, resulting in many problems.

In addition, centralized messaging platforms such as Telegram and Facebook Messenger always pose a serious risk to privacy as personal messages are stored on the platform's central servers, allowing private personal data to be leaked from inside the platform. DNS (Domain Name Service) and e-mail system are designed to operate as decentralized distributed systems based on standard Internet protocols and to enable interoperability between systems. However, instant messaging platforms, which are currently mainstream communication methods, do not have a standard protocol that can provide interoperability and are designed and operated in a centralized and siloed manner that does not allow interworking user accounts and message transmission between separate platforms.

The traditional Telephone Network, which provides phone number-based SMS and voice calls provided through existing telecom carriers, can be completely replaced through VoIP technology through Internet data networks by using web standard technology such as WebRTC. And, the explosive growth of Generative AI technology has yet to find a real use case that can give users direct utility in the Telecom field and is not being used in earnest.

Newnal Web3 Telecom





Newnal Web3 Telecom technology is a next-generation secure communication technology based on the Web3 ai paradigm leveraging blockchain technology and personalized AI technology that overcome the limitations of Web 2.0 paradigm communication technology.

Users can create a blockchain-based ID (DID(Decentralized Identifiers)/VC(Verifiable Credentials) technology-based *Web3 ai-ID*) that can be generated from user devices without relying on a central server platform and use it as a communication ID. DIDs are mapped to *Newnal Mobile Addresses* in a format that is easy for humans to identify and remember. Unlike phone numbers allocated through telecom carriers, users can generate many

communication blockchain IDs (DIDs) as they want, so they can set and use different phone numbers (Newnal Mobile Address) for each communication peer. For example, each user's family, friends, and co-worker can communicate by connecting to different addresses, and mobile addresses exposed to couriers or used in online second-hand markets can be temporarily generated and discarded after using them.

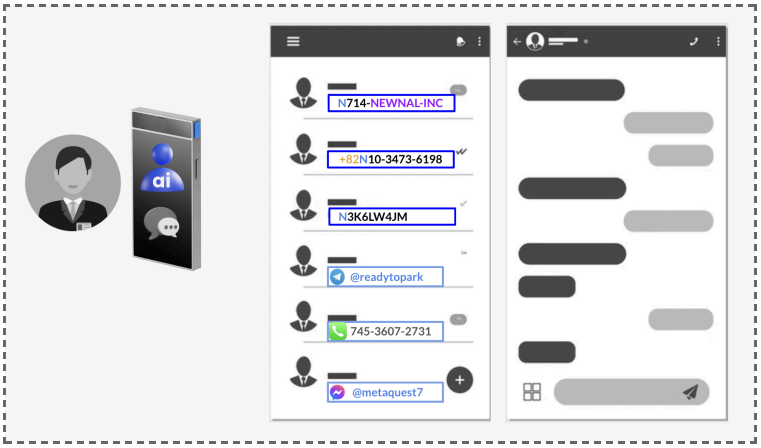
Newnal Mobile Address is mapped to a blockchain-based DID that can provide user authentication and P2P secure communication features and can be easily identified and remembered by humans, similar to the existing phone number system. The address format consists of [*country code* + N + (*user-selectable numbers/Uppercase character code*)].

All text messaging, voice, and video calls between user devices are processed through end-to-end encryption(E2EE)-based cryptographic encryption technology between users' blockchain IDs, enabling P2P communication that maintains complete security between users. Unlike phone numbers and ID/passwords, DIDs of the user and counter-party using asymmetric key encryption technology can create a secure message channel (via Diffie-Hellman key exchange, Double Ratcheting, and Ratchet Tree) that allows complete secret communication and mutual authentication through secure channels without an intermediary such as central servers. Messages exchanged between users are not exposed to central servers and networks, and complete security is maintained. Even in the user device, communication cryptographic keys are generated and managed through the hardware security module, so that personal message information encrypted and stored in the device is not leaked even through digital forensics. For the voice and video call, DID-based user authentication and E2EE encryption technology are implemented on top of WebRTC(Web Real-Time Communication) protocol, so users' real-time audio video streaming data is not exposed at all on media streaming servers and networks. For group communication involving more than three users(or AIs), the MLS (Messaging Layer Security) standard secure messaging protocol based on *Ratchet Tree* technology, which was recently developed as an Internet standard, is implemented. Even in the case of secret

group communication involving more than thousands of people who are difficult to implement on existing messaging platforms, the communication content works in a way that is not exposed to the central server at all.

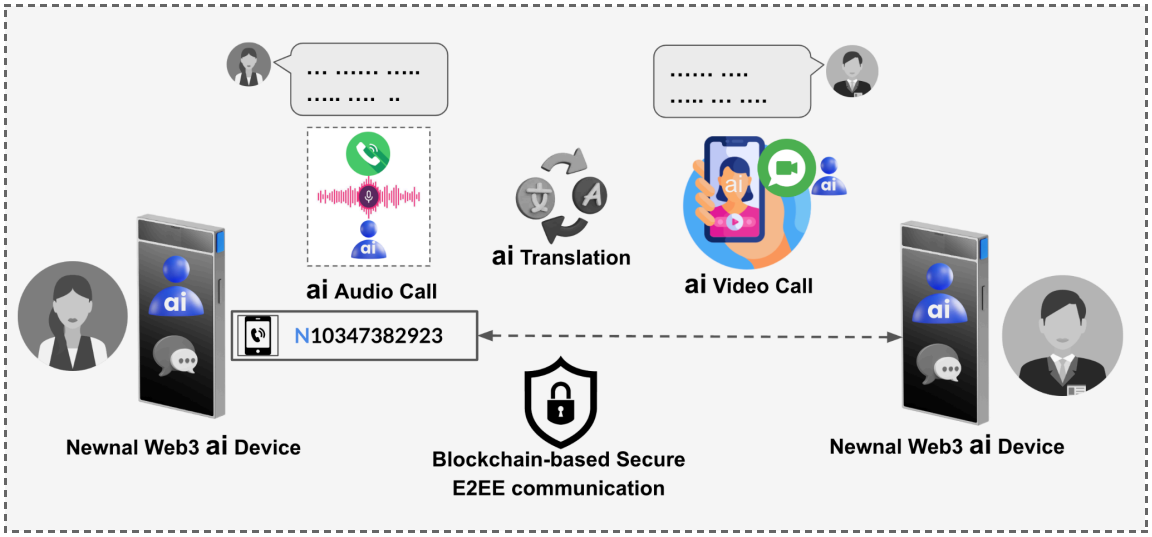
The identity of the communication peer (person, AI) can also be accurately identified through the Web3 ai blockchain ID to protect users from spam, phishing, and deepfake calls. Through authentication using blockchain-based DID/VC technology, the identity of the communication peer can be authenticated in real time without the help of a central server-based platform.

Appless Messaging Service built upon Newnal Web3 Telecom



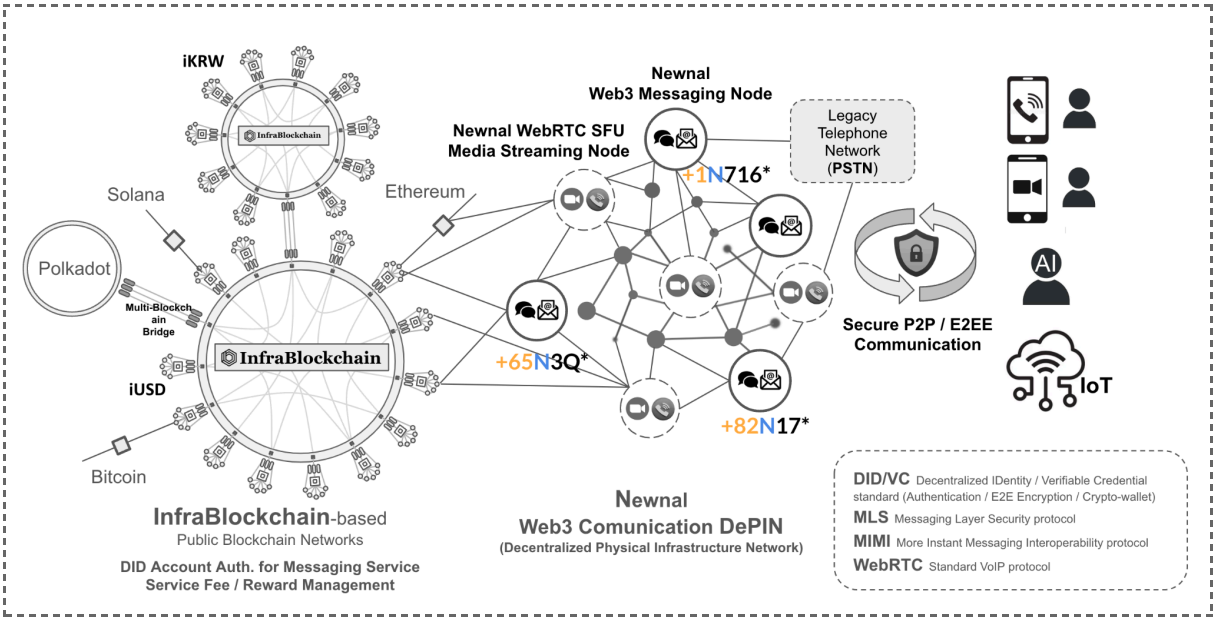
Digital Market Act (DMA) regulations currently in effect in Europe are also widely applied to the field of instant messaging. Existing big tech instant messaging platforms are phased in regulations that force them to work with other heterogeneous messaging platforms, allowing messaging service users to freely make text messaging, voice and video calls in a way that is not dependent on specific platform applications, the similar way the email system works. Internet standard protocols are being developed to implement this technically. Following the TLS(Transport Layer Security) standard protocol, a 1:1 secure server-to-client communication protocol used for HTTPS, the **MLS** (Messaging Layer Security) secure messaging standard used in multilateral messaging environments, such as existing instant messaging apps, has been developed as the Internet standard security messaging protocol. In addition, **MIMI** (More Instant Messaging Interoperability) standard is being developed to provide interoperability between messaging platform servers. Through networks that operate based on standard messaging protocols such as MLS and MIMI, we can implement “Appless Messaging Service” in which text messaging and voice/video calls can be made by linking and integrating all existing messaging platform services with one blockchain-based user account without being dependent on a specific messaging app.

Newnal Web3 ai Communication : AI-involved Call and Messaging



An AI agent (*Newnal Web3 ai Agent*) can participate in the Newnal Web3 Telecom network to perform text messaging, voice calls, and video calls on behalf of the user. Newnal Web3 ai Agent is a personalized AI agent, ***a****nother-****i***, that collects and learns each user's personal data, performs reasoning and natural language generation based on user personal data, and performs actions for the user. A Web3 ai agent can authenticate connected peers (people or other AI agents) through DIDs, and can make a call with the other party on behalf of the user by referring to the PKG(Personal Knowledge Graph) database in which the user's personal data is stored. The ai agent can control sensitive personal information not to be leaked in the call or message content depending on the connected peer's identity. The ai agent may present appropriate information or actions to the user depending on the content of the conversation between users, and in communication that requires various languages, it can provide real-time translation services to the user to support the user's communication activities. Newnal Web3 ai agent is driven by AI agent engine based on **(AG)²** (AI Action Graph Generation model), a personalized AI model trained to perform optimized AI behavior based on personal information, and performs RAG(Retrieve Augmented Generation) based on the personal data-stored *PKG* database leveraging open LLM models. Through generative audio/video AI models, voice audio streams and 'talking-face' video streams that look similar to the user are generated in real time to perform a call service through the WebRTC protocol.

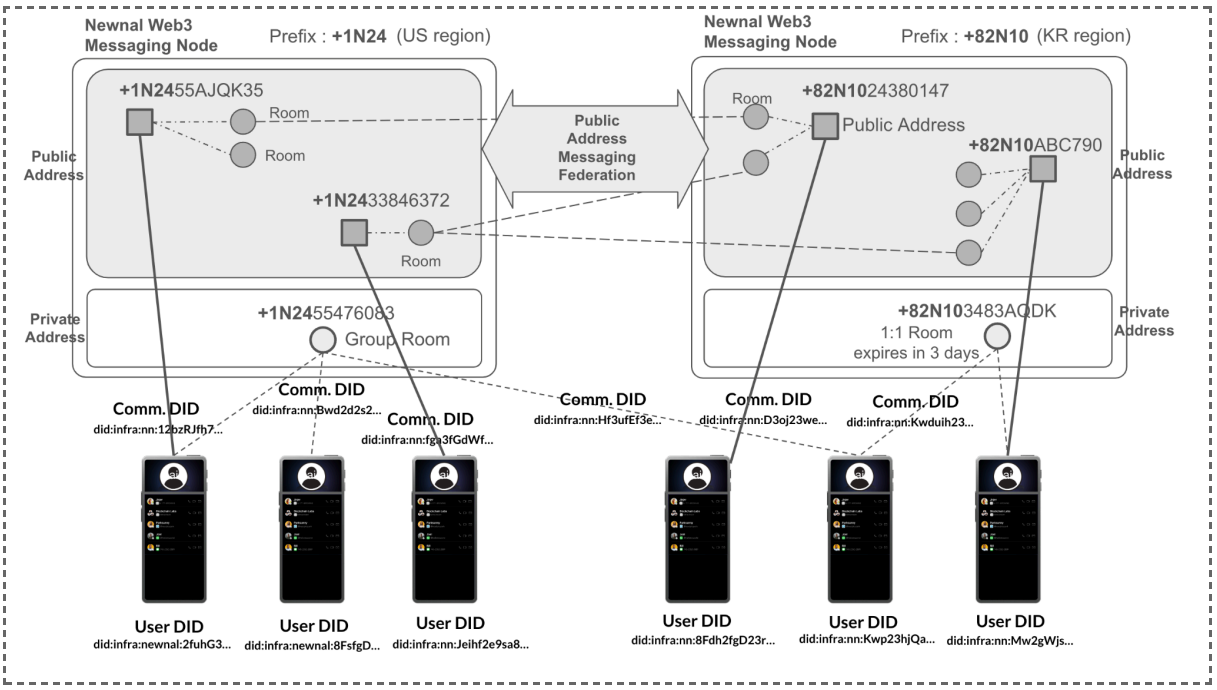
Newnal Web3 Telecom DePIN Architecture



Newnal Web3 Telecom network is a blockchain-based **DePIN** (Decentralized Physical Infrastructure Network) in which communication infrastructure nodes operate in a decentralized setup. ***Newnal Web3 Messaging Node*** and ***Newnal WebRTC Media Streaming Node*** (WebRTC SFU Node) are required to implement the *Newnal Web3 Telecom Network*. Anyone can operate these Telecom Infrastructure nodes through their own computing equipment using open-source node implementations. Existing Web 2.0 messaging/call service infrastructure is operated by telecom carriers and big-tech platform companies exclusively providing infrastructure, but Newnal Web3 Telecom allows anyone to participate as a communication infrastructure node operator using their computing equipment and earn revenue from infrastructure operations. Even by registering an individual's idle laptop equipment as a *Media Streaming Node*, encrypted streaming of voice/video calls occurring near the user equipment can be mediated without personal data exposure and certain profits can be compensated from the blockchain network. DePIN Supervisor nodes authorized to monitor whether DePIN nodes are operating normally may periodically perform a public test suite for each node to verify whether Web3 Telecom Infra nodes are operating correctly, approve compensation for registered DePIN nodes, or apply penalties for malfunctions on the blockchain. Blockchain ID-based accounts of Web3 Telecom network users are managed through blockchain, and mutual authentication between users is performed in real time without a central server during connection between users and message transmission. The cost of using the Web3 Telecom infrastructure by network users and compensation for DePIN infrastructure node participants are also settled as legal currency-based stable tokens through InfraBlockchain, a public multi-blockchain network without virtual currency. The Web3 Telecom network extends to existing cryptocurrency-based public blockchains such as Ethereum, allowing the blockchain wallet services of those blockchains to be used as

Web3 Telecom messaging/call clients, and settling the cost of using the Web3 Telecom infrastructure can be processed as the cryptocurrency on the public blockchain.

Decentralized Interoperable Newnal Web3 Messaging Nodes



The Newnal Web3 Messaging Node acts as a message relay node that is assigned a prefix of the *Newnal Mobile Address*, handles connection processing and encrypted message delivery between user DIDs associated with the allocated Newnal Address prefix. Since the Messaging Node processes only messages encrypted with P2P-based E2EE between user DIDs, the user's personal message content cannot be exposed to the Messaging Node server at all. The Messaging Node is distributed by country region because it is assigned a prefix of *Newnal Mobile Address* starting with the country code. It is designed to handle the processing load for messaging and calls occurring in the country's region, so that messaging nodes can be distributed region by region so that the network can operate efficiently. *Newnal Mobile Address* is divided into Private Address issued for private 1:1 or group messaging, and Public Address that can be used as a public address, like an existing phone number or ID of instant messaging services. Private Address is used as the Room ID of the private message channel and is accessible only to connected users after mutual authentication. All messages relayed by the Messaging Node and stored on user devices are managed based on the MLS encryption message standard. In order to relay messages between *Public Addresses* existing in multiple *Messaging Nodes*, Newnal Messaging Nodes implement the interoperability interface between messaging nodes based on the MIMI protocol.

Patents

[USPTO] US-19/104055

ELECTRONIC DEVICE AND METHOD PROVIDING SECRET MESSENGER FUNCTION THROUGH END TO END ENCRYPTION BASED ON BLOCKCHAIN DID TECHNOLOGY

[WIPO/PCT] WO/2024/048838

ELECTRONIC DEVICE AND METHOD PROVIDING SECRET MESSENGER FUNCTION THROUGH END TO END ENCRYPTION BASED ON BLOCKCHAIN DID TECHNOLOGY

[USPTO] US-19/059751

METHOD AND DEVICE FOR BUILDING DECENTRALIZED SECURE COMMUNICATION INFRASTRUCTURE NETWORK BASED ON BLOCKCHAIN AND DID TECHNOLOGY