

DRAFT FOR OPEN COMMUNITY REVIEW AND SUBJECT TO CHANGE

# **Nubit: The Next-Generation Consumer Network**

**Bridging Web2 and Web3 for the Internet of Tomorrow**



The Nubit Team  
Aug 22, 2024

DRAFT FOR OPEN COMMUNITY REVIEW AND SUBJECT TO CHANGE

**Legal Disclaimer**

Nothing in this white paper constitutes legal, financial, business, or tax advice and you should consult your own legal, financial, tax or other professional adviser before engaging in any activity in connection herewith. Neither Riema Labs nor any of its employees are liable for any kind of direct or indirect damage that you may suffer in connection with accessing this white paper.

© 2024 Riema Labs. All Rights Reserved.

# The Nubit Lite Paper

## Introduction

Web3 holds immense promise, but it's far from realizing its full potential. While technology has advanced rapidly, the gap between what's possible and what's accessible remains significant. Most consumer applications struggle to make the leap from Web2 to Web3 because the transition is anything but straightforward. The technical complexity of blockchain development, coupled with the lack of compatibility between Web2 and Web3 technologies, makes it difficult for teams to successfully migrate and scale their applications.

In addition to these technical challenges, existing blockchain infrastructure often imposes high costs on projects, such as staking requirements and expensive gas fees. These costs create a "rent-seeking" environment that's particularly tough on startups, raising the barrier to entry. Moreover, security requirements in Web3 are far more stringent than in Web2, as every interaction involves handling digital assets and financial transactions. This forces projects to invest significant resources not only in adapting to the new technology but also in maintaining the security of their systems, further complicating the transition.

At Nubit, we believe in a future where the boundaries between Web2 and Web3 disappear, giving rise to a new era of interconnected applications and ecosystems. This vision drives us to break down barriers and push the limits of what's possible in the rapidly evolving Web3 space.

Before unrolling our proposal, let us take a detour and look into WeChat, one of the most successful cases in Web2. As one of the world's largest mobile apps with over a billion active users, WeChat created a powerful ecosystem by integrating users, social features, payment interfaces, and Mini Apps. As shown in Figure 1, WeChat users enjoy a unified experience where they can easily switch between social interactions, explore thousands of Mini Programs, and manage their finances—all within one app. The WeChat wallet not only facilitates payments and services but also serves as a central hub for managing assets. This entire ecosystem is underpinned by Tencent Cloud, which ensures high availability and data security, thereby enhancing user experience.

However, WeChat's success goes way beyond a collection of powerful features. The true game-changer lies in the Weixin DevTools—a development toolkit that drastically lowers the barrier for developers to create Mini Programs. This toolkit abstracts away the complexities of payment integration, security concerns, and other underlying implementation details, offering developers a unified interface that allows them to focus solely on building the core logic of their applications. Performance, security, and all the intricate backend details are seamlessly handled by the Weixin DevTools, enabling developers to bring high-quality mini-programs with little effort.

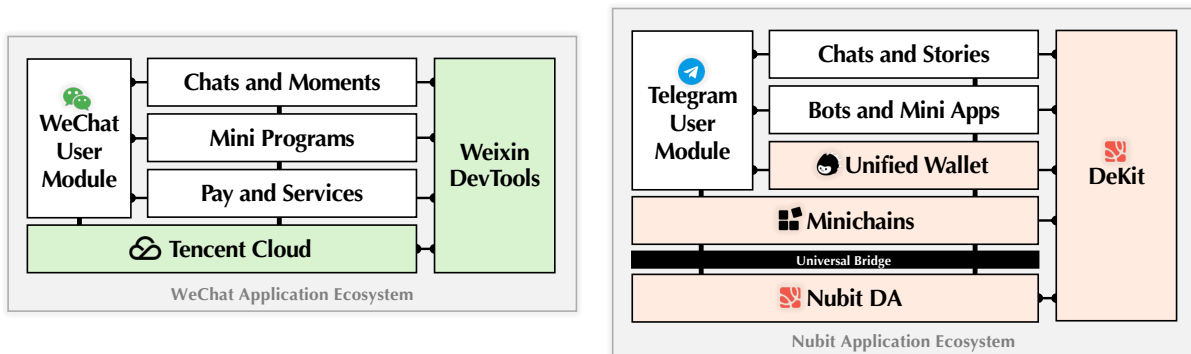


Figure 1: Comparison of WeChat and Nubit Application Ecosystems.

This approach, proven successful in the traditional Web2, can be equally transformative in the Web3 domain. Like WeChat, Telegram also boasts a billion-strong user base with its own rich ecosystem of social features like Chats, Stories, and thousands of Mini Apps that enhance its functionality. To fully harness the potential of the Telegram ecosystem and leverage the decentralized, trustless nature of blockchains, it's essential to take this model a step further by transitioning these applications to Web3.

As shown in Figure 1, in this Web3 architecture, a Unified Wallet Interface that supports multiple blockchains would serve as the payment system. Additionally, Mini Apps would need to evolve into Web3 applications, connected to various blockchains through the Unified Wallet, allowing users to interact with decentralized finance smoothly. To guarantee data availability, sharing, and security across these components, a secure and scalable DA layer is also essential.

Most importantly, just as WeChat's Weixin DevTools made Web2 development accessible, Web3 requires an easy-to-use Blockchain Integration SDK. This SDK would make the complexity of blockchain 'invisible' to developers, allowing them to build Web3 applications with the same ease as Web2 apps. Moreover, this SDK makes the applications built on it more secure by simplifying the development process, which allows for better auditing compared to complex implementations.

**Our Solution.** Let's start by considering Figure 2, which illustrates the core components of our solution. At the forefront is the **Unified Wallet** (e.g., Tomo, OKX, etc.), the primary gateway for Web2 users into the Web3 world. This wallet is designed to be intuitive and accessible, supporting multiple chains—including Bitcoin, Solana, EVM, TON, and more—ensuring that users can manage their digital assets across different networks all within Telegram. The wallet is secure and non-custodial, offering a seamless entry point that's crucial for onboarding the next wave of Web3 users.

Once users are integrated through the Unified Wallet, developers still face two significant challenges: the high costs associated with network usage, such as gas fees, and the limited flexibility of general-purpose blockchains, which may not support the specific features or optimizations needed for their applications. These constraints can hinder an app's performance, security, and overall user experience.

To address these, we introduce **Minichains**—dedicated, customizable chains that are tailored to the application's unique requirements. Minichains enable developers to create applications without being constrained by the general-purpose nature of traditional blockchains. Importantly, these Minichains can ultimately settle on major Layer 1 networks such as Ethereum, Bitcoin, Solana, or TON, ensuring security and interoperability within the broader blockchain ecosystem.

Minichain offers developers the flexibility to create a sustainable revenue model through user activity. By operating on their own Minichains, applications can directly engage users, who, in turn, can gain ownership stakes within the ecosystem. This fosters a deeper symbiotic connection between the app and its users, promoting loyalty and extending the app's lifecycle. Unlike traditional models where the application's success primarily benefits the underlying Layer-1, the Minichain approach ensures that the value created stays within the app's ecosystem.

However, the rise of numerous Minichains can lead to fragmentation, causing liquidity challenges and inconsistent user experiences. To mitigate these issues, we provide the **Universal Bridge**, which enables smooth transitions between interconnected Minichains, allowing users to navigate these chains as if they were part of a unified platform. The Universal Bridge offers two solutions: traditional cross-chain bridges, functioning similarly to cross-rollup bridges, and a more advanced option—direct data sharing through **Nubit DA**. Nubit DA provides a Shared Data Availability layer across Minichains, enabling efficient and secure state-sharing, ensuring that data remains consistent and accessible across the entire ecosystem.

These components—Unified Wallet, Minichains, Universal Bridge, and Nubit DA—form a comprehensive solution addressing the full spectrum of challenges in the Web3 space. Yet, while this system is highly functional, the complexity of its underlying technology can be daunting, and ensuring that these components operate securely in an optimized, integrated manner is a significant challenge. This is where the **Decentralization Kit (DeKit)** and **Minichain-as-a-Service (MaaS)** become not just essential, but the most critical elements of our entire solution.

Drawing from the success of WeChat’s Weixin DevTools, we recognize the need to simplify the development process. Just as Weixin DevTools made Web2 development accessible, our **DeKit** abstracts away the complexities of blockchain, allowing developers to build Web3 applications with the same ease as Web2. DeKit is pivotal in two ways:

- ▶ **Web2 to Web3 Integration:** DeKit makes it straightforward for Web2 developers to integrate decentralized features into their Telegram apps without deep blockchain expertise. This enables traditional Web2 applications to seamlessly transition into the Web3 ecosystem, opening up new possibilities for user engagement and functionality.
- ▶ **Web3 to Web2 Expansion:** Conversely, DeKit also serves as a gateway for existing Web3 applications to tap into the vast user base of Web2. It provides tools that enable Web3 apps to interact with familiar Web2 interfaces and services, allowing decentralized applications to extend their reach and onboard new users who may not yet be familiar with blockchain technologies.

However, managing and scaling a minichain is inherently complex. To simplify this process, Nubit offers **Minichain-as-a-Service (MaaS)**, enabling developers to deploy and manage their Minichains with ease. What was once a complex and daunting task is transformed into an accessible and efficient process, allowing developers to focus on what they do best—building and scaling great applications.

By integrating these elements, Nubit offers an ecosystem solution—what we call **The Matrix**—empowering Web2 platforms such as Telegram to fully harness the potential of Web3 and drive the next generation of decentralized applications. In what follows, we briefly highlight the insight and core features of Nubit’s ecosystem solution.

## Overview

The success of **The Matrix** hinges on several key components that collectively bring its vision to life, ensuring seamless interaction, scalability, and ease of use within the Minichain ecosystem.

### Unified Wallet

A seamless and secure wallet experience is crucial for onboarding Web2 users into Web3. The Unified Wallet (e.g., Tomo) supports multiple blockchains, including Bitcoin, Solana, Ethereum, and Ton, all integrated directly into Telegram. This non-custodial wallet ensures that users have full control over their assets while offering a consistent, user-friendly interface.

In addition, the Unified Wallet supports social login, significantly lowering the barrier to entry for new users. By leveraging familiar sign-in methods like Google, Apple, Facebook, X (Twitter), GitHub, and Discord, the wallet transforms the onboarding process, making it more intuitive and accessible. Users can access Web3 using just their social media handles, simplifying the traditionally complex process of setting up and managing blockchain wallets.

Moreover, the Unified wallet includes onramp/offramp functionality, allowing users to easily deposit and withdraw funds, further streamlining the process of entering and exiting the blockchain ecosystem. The ultimate goal is to create an experience so seamless that users are unaware they



**Figure 2:** Overview of The Matrix.

are unaware they

are interacting with blockchain technology. The Unified Wallet thus serves as the gateway for Web2 users transitioning into the Web3 space.

## Universal Bridge

The ability and efficiency to communicate across different Minichains is critical. The Universal Bridge is designed to facilitate this communication, making cross-chain transactions efficient and secure.

Traditional cross-chain transactions often face challenges due to their asynchronous nature, leading to risks such as incomplete or failed transactions.

Nubit addresses this with a **shared sequencing protocol** for all Minichains that allows for synchronous cross-chain messaging, enabling atomic transactions across multiple chains. This means that complex operations, such as cross-Minichain arbitrage or flash loans, can be executed with confidence, knowing that all parts of the transaction will be completed as intended.

The Universal Bridge not only simplifies these interactions but also ensures that developers can build more sophisticated applications without worrying about the intricacies of cross-Minichain coordination. It enables gas fee interoperability, allowing users to seamlessly use gas fees across different Minichains. It also facilitates the smooth movement of users within the ecosystem, effectively creating a shared user base across applications. Additionally, the enhanced atomic composability enabled by the Universal Bridge allows different applications to securely integrate their functions, fostering greater innovation and flexibility within the network.

To further optimize these cross-chain interactions, the Universal Bridge leverages **Nubit DA** for direct data sharing, providing a shared data availability layer that ensures consistency across the entire Minichain ecosystem.

## Nubit DA

As the number of Minichains grows, so does the need for a robust data availability solution. Nubit DA is designed to meet this need, providing a scalable and trustless layer that ensures the security and efficiency of data across all Minichains.

Traditional Layer-1 blockchains often struggle to handle the sheer volume of data generated by multiple chains, but Nubit DA, powered by Bitcoin, offers a solution that scales with the ecosystem.

By leveraging Bitcoin's unmatched security, Nubit DA ensures that data remains accessible and consistent across the entire Minichain ecosystem. This shared state capability not only enhances the security of individual chains but also enables smoother interactions and data exchange between them.

Nubit DA comprises the following components:

- ▶ **Validators** These nodes operate using a consensus algorithm rooted in Practical Byzantine Fault Tolerance (Tendermint) and are tasked with proposing blocks and verifying the integrity of blocks and transactions.
- ▶ **Full Storage Node** After receiving block data from validators, these nodes are entrusted with the reliable storage of all data. The integrity and availability of stored data are critical, especially given the risks of malicious activities such as data withholding or tampering. To mitigate these risks, Data Availability Sampling (DAS) requests from light clients are employed to verify data availability, ensuring the system's resilience against such threats.
- ▶ **Light Client** Light clients obtain block headers broadcasted by validators, which include data commitments. Based on these commitments, they may randomly initiate requests to full storage nodes to verify data availability.

## Decentralization Kit (DeKit)

Whether you're a Web2 developer transitioning into Web3 or a seasoned blockchain developer, DeKit allows developers to launch and scale their Minichains quickly, without worrying about the underlying technical complexities. In particular, DeKit is built on a Model-View-Controller (MVC) architecture, a widely used design pattern in software development. MVC divides an application into three interconnected components—Model, View, and Controller—allowing developers to separate the internal representations of information from the ways that information is presented and accepted by the user. This separation of concerns is crucial because it simplifies development, testing, and maintenance, making the overall process more efficient.

By adopting this familiar and proven structure, DeKit makes it easier for developers to transition into Web3 development, especially those coming from a Web2 background where MVC is commonly used in frameworks like WeChat Mini Programs. With this architecture, developers can effectively manage various aspects of their Minichain applications:

- ▶ **Model (Ledger Management)** The Model layer represents the ledger, where all on-chain data is stored and managed. Developers can perform common operations like updating account balances, transferring assets, or querying transaction histories through simple API calls.
- ▶ **View (User Interface)** The View layer is responsible for what users see and interact with. Nubit provides tools that integrate seamlessly with existing Web2 technologies, enabling developers to create user interfaces that interact directly with Minichain and Telegram wallets without requiring specialized blockchain knowledge.
- ▶ **Controller (Smart Contract Logic)** The Controller layer handles the business logic of the application. Developers can use Nubit's pre-built smart contracts (e.g., Fungible tokens, Non-fungible tokens, airdrop) or customize them as needed, all through easy-to-use APIs.

## Minichain-as-a-Service

Minichain-as-a-Service (MaaS) leverages DeKit to empower developers with the ability to create and manage Minichains that are tailored to their specific applications. Through configurations provided by DeKit, Minichains are automatically generated, each with a minimal runtime optimized to support a single Mini App. This approach ensures that the chain's resources are focused entirely on maximizing the performance, security, and user experience of that particular application, without the bloat of unnecessary functionalities.

MaaS simplifies the traditionally complex process of blockchain deployment, offering a no-code dashboard that allows developers to configure their Minichains effortlessly. Whether it's adjusting sequencers, gas limits, or middleware solutions, the process is designed to be accessible even to non-technical users. This ease of use democratizes blockchain development, enabling a broader range of developers to build powerful, custom blockchain solutions without needing deep expertise in blockchain technology.

In addition to these essential infrastructure services, such as RPC services, state verification, and chain explorers—critical for maintaining the integrity and performance of Minichains—MaaS significantly reduces the operational overhead typically associated with managing a blockchain network. These tools allow developers to focus on innovation rather than the complexities of infrastructure management.

More importantly, MaaS offers a comprehensive ecosystem solution that spans the entire spectrum of blockchain needs, from foundational infrastructure to user engagement. Integrated services like the Unified Wallet, Universal Bridge, and Nubit DA are seamlessly embedded into each Minichain, creating a fully interconnected environment that enhances interoperability, data availability, and user experience across the ecosystem.

## Conclusion

At Nubit, we see the future of digital ecosystems as one where the barriers between Web2 and Web3 no longer exist. Our vision is to bridge this gap by offering a comprehensive ecosystem solution that simplifies the transition and unlocks the full potential of decentralized applications.

The core of our approach includes components like the Unified Wallet, Minichains, Universal Bridge, and Nubit DA, each designed to address key challenges in the Web3 space. While these tools are powerful, their integration and security present complex challenges. This is where Decentralization Kit (DeKit) and Minichain-as-a-Service (MaaS) become indispensable.

DeKit abstracts the complexities of blockchain, enabling developers to build Web3 applications with the ease and familiarity of Web2. It offers a familiar Model-View-Controller (MVC) architecture, making it intuitive for developers to manage their Minichains without needing to delve into blockchain intricacies. Complementing DeKit, Minichain-as-a-Service automates the creation and management of Minichains, ensuring each one is optimized for performance and security. With a no-code dashboard for easy customization, MaaS empowers developers to focus on innovation, while Nubit handles the underlying infrastructure.

Together, these components form The Matrix—a unified ecosystem solution that enables Web2 platforms like Telegram to fully embrace Web3, driving the next generation of decentralized applications and paving the way for the Internet of tomorrow.