SuiMail  
**Decentralized, Secure, Private, and Spam-Free Mailing on the Sui Blockchain.**TEAM ALPHA.SUI  
hello.teamalphadotsui@gmail.com  
  
Version 1.0 | May 2025.  
  


**1. Abstract** Today’s Email communication infrastructure is dominated by centralized platforms that extract user data, monetize attention, and control access to personal inboxes. Users have no ownership over their messages, are constantly exposed to unsolicited content, and lack transparency in how their data is stored, used, or shared. Meanwhile, most Web3 solutions focus on finance and infrastructure, leaving real-world user applications like messaging largely untouched.  
 At it's core **SuiMail** addresses this gap by introducing a decentralized, wallet-native communication protocol that prioritizes **DATA OWNERSHIP**, not just **PRIVACY**. Built on the Sui Blockchain, every message is treated as an on-chain object owned and controlled by the recipient. Messages are encrypted by the sender, stored via decentralized blob storage (Walrus), and economically filtered through a " **PAY-TO-SEND MODEL**" allowing users to get rewarded for receiving relevant messages and block spam with economic cost.  
 To onboard everyday users, SuiMail integrates zkLogin for frictionless Web2-style access and SUINS to resolve wallet identities into human-readable names.   
 From DAOs and protocols to individual users, SuiMail provides a transparent, censorship-resistant communication layer that returns control of messaging back to those it belongs to **"THE USERS"..  
  
By restoring control to the inbox owner and offering economic incentives for receiving targeted communications, SuiMail aims to become the default communication layer in a decentralized internet.**

**2. Introduction** In today’s digital communication landscape, tech giants dominate messaging infrastructure, amassing and monetizing vast amounts of user data with little transparency or accountability. Every interaction **emails, notifications, subscriptions** is filtered through centralized systems that **prioritize profit over privacy**. Users rarely own the messages they receive or send. Instead, their data is harvested, resold, and algorithmically optimized for attention extraction. This exploitation of personal communication data poses deep ethical, security, and systemic risks, yet remains the norm in both consumer and enterprise communications.  
 While Web3 has introduced groundbreaking solutions in finance, governance, and decentralized infrastructure, one critical sector remains largely untouched**: messaging**. Existing attempts to decentralize communication are either clunky, lack real-world usability, or fail to provide enterprise-grade reliability and trust models. The result is a major gap between decentralized ideals and the real-world standards of communication platforms used by institutions and individuals alike.  
 **SuiMail** aims to close this gap by reimagining messaging through a "**data ownership-first architecture"** built on the Sui Blockchain. Unlike conventional platforms, messages in SuiMail are treated as user-owned on-chain objects, cryptographically encrypted, economically filtered, and completely resistant to centralized control or censorship. Leveraging Sui’s low-latency, object-centric model, zkLogin for seamless onboarding, and SUINS for human-readable wallet identities, SuiMail introduces a secure, wallet-native communication protocol that balances privacy, usability, and scalability.  
 Decentralized storage, powered by Walrus, ensures messages and files are accessible and persistent without relying on centralized servers. Whether for DAOs, protocols, or regular users, SuiMail offers a high-integrity communication layer that aligns with the Confidentiality, Integrity, and Availability (CIA) triad.  
 In an era where data sovereignty is more urgent than ever, SuiMail provides a bridge between the trustless ethos of Web3 and the functional demands of modern communication empowering users to truly own their inbox.

**3. Problem Statement**

**i) Centralized Control and Data Ownership:**  
 Traditional email platforms are largely controlled by centralized service providers, not by the users. Major services collect vast amounts of personal data from location and device identifiers to calendar events and shopping information to improve features and target advertising.   
 In practice, free email accounts come at the hidden “cost” of user data. As one privacy expert observes, a mainstream email account is free only because **“you don’t pay it with money, but with data”**. Crucially, users have little insight or consent over this data harvesting. There is minimal transparency or regulatory enforcement for email tracking, so all of the content, metadata (who you email and when), and usage patterns are essentially under the provider’s control. **In short, users do not truly own their messages or metadata on today’s email systems, centralized platforms do**.

**ii) Economic Value and Lack of User Compensation:**  
 The data extracted from users’ communications is economically very valuable to tech and advertising companies, but users see none of that value. Researchers note that platforms **“collect personal information without compensation to the user”** effectively imposing a **take-it-or-leave-it deal in exchange for “free” services**.   
 In a fair market, users would be able to sell their data or be paid for it. Instead, all the surplus value (from targeted ads and analytics) goes to the platform. For example, detailed profiles built from email and related data are highly attractive to advertisers and can be sold at high prices. Users currently have no mechanism to recover any of this value: **they are simply not paid or rewarded for the data generated by their everyday communications**.

**iii) Email Spam and Productivity Loss:** Volume of Spam: A significant fraction of email traffic is unsolicited. Studies estimate that roughly 45–85% of all emails sent each day are spam. This unwanted volume floods users’ inboxes and makes finding legitimate messages harder.  
  
 Time Wasted: Employees with moderately busy inboxes waste many work hours on spam. For example, **workers who receive 30–60 external emails per day spend roughly 11 hours per year just sorting and deleting spam**; **those with 60–100 emails per day lose about 18 hours per year** (over two full workdays) to spam management.  
  
 Economic Cost:These inefficiencies translate into real money. Nucleus Research calculates that spam costs employers on average about \*\*\$1,934 per employee per year\*\* in lost productivity.  
 Together, these numbers paint a clear picture: email spam causes massive productivity losses and fuels information overload. Users are inundated with junk mail, which clogs inboxes and creates frustration, distraction, and burnout. The sheer volume of unwanted messages is a chronic pain point with \*\*no reward or compensation\*\* for the time users spend sorting through it.  
  
  
**iv) Security and Trust Concerns** Users lack confidence that traditional email is secure enough for sensitive or high-value information. By default, popular email services do not enable end-to-end encryption, so messages can be read or intercepted by intermediate servers or eavesdroppers. Human errors compound this risk: for example, **the UK Information Commissioner’s Office reports that emails sent to the wrong recipient are the leading cause of reported data breaches**. Researchers have even found that an estimated 4–10% of internet traffic is vulnerable to interception.  
 On top of these vulnerabilities, email is a prime vector for attacks. In one recent survey, 94% of organizations reported falling victim to email-based phishing attacks in the past year. Account takeover and malware often start with a malicious email link or attachment. In fact, over half of affected companies reported having to cease operations following a breach initiated through an internal email incident. Together these facts contribute to a pervasive lack of trust: users and businesses are wary of sending confidential data via email, knowing that privacy is limited and threats (phishing, spoofing, ransomware) are commonplace.

**v) Gap in Web3 Communication Protocols:**  
 The shortcomings of Web2 email are especially glaring given the rapid evolution of Web3 in other domains. While the blockchain space has delivered DeFi platforms, NFT marketplaces, and decentralized organizations, **secure decentralized communication is still undeveloped at enterprise scale.** There is currently no widely-adopted, enterprise-grade protocol for Web3-native email or messaging.   
(Existing projects are still early-stage.) As developers acknowledge: **“There is no purpose-built communication protocol that supports…end-to-end encrypted communication between Web3 identities.”**In other words, despite the innovation in wallets and smart contracts, the ecosystem lacks a true Web3 version of email. Users and organizations in blockchain communities must still rely on legacy email or proprietary chat apps to communicate, forfeiting the benefits of decentralization (ownership, privacy, trustless security) in the process.  
  
**Toward a Decentralized Email (SuiMail)**  
 The net result of these problems is clear: email users are disenfranchised and exposed. To fill this gap, SuiMail is being developed as a Web3-native email solution. It is designed to restore data ownership (by anchoring messages and metadata on a blockchain) and enhance privacy/security (via cryptographic controls) for users.   
 **By tackling data ownership, compensation, spam, and security together, SuiMail aims to solve the core problems of traditional email and deliver a truly user-centric communication protocol.**

**4. Proposed Solution: SuiMail:** SuiMail reimagines email as a decentralized, wallet-native messaging layer built on the Sui Blockchain. By leveraging Sui’s object-centric architecture, each user owns and controls their inbox as an on-chain object, enabling programmable, user-defined communication rules.  
 To prevent spam and introduce sender accountability, SuiMail implements a Pay-to-Send mechanism. Users can define a fee that must be paid before a message is delivered, turning spam into a potential revenue stream and allowing users to set economic thresholds for who can reach them.  
 Message content is stored off-chain using Walrus, a decentralized verifiable storage protocol. Anchored on-chain through Merkle proofs, this ensures trustless data integrity while minimizing on-chain storage costs.  
 Additionally, SuiMail introduces whitelist and blacklist controls, allowing users to explicitly permit or block certain wallet addresses, enabling highly customizable communication policies.  
 **By combining on-chain ownership, economic-based permissions, and verifiable off-chain storage, SuiMail provides a secure, scalable, and user-sovereign alternative to traditional messaging systems, optimized for Web3 ecosystems**.  
  
  
**5. Architecture & Technical Design** SuiMail is architected as a modular, scalable protocol that combines the strengths of the Sui Blockchain, decentralized storage, and optional backend services. It prioritizes privacy, efficiency, and extensibility to support seamless Web3-native messaging.

**Message Objects & Storage** Each message is represented on-chain as a "**Sui Object"**, storing metadata such as sender, recipient, timestamp, and status.  
 The message payload is encrypted server-side, and the resulting encrypted blob is stored off-chain on **Walrus**, a decentralized storage layer optimized for immutability and scalability.  
 SuiMail stores only encrypted payload hashes on Walrus, with access controlled via sender/recipient wallets.

**Ownership & Privacy**  
 Messages are tied to wallet identities. **While encryption is currently server-side**, messages remain protected during storage and delivery.  
 A future upgrade will shift toward client-side encryption, ensuring full zero-knowledge privacy.  
Only the intended recipient has permission to decrypt message data, enforced through wallet-based access control.

**Gas Optimization**Built on **Sui’s parallel execution engine**, SuiMail enables low-latency and cost-efficient microtransactions.  
 Offloading encrypted payloads to Walrus reduces on-chain congestion and ensures scalable message handling.

**Frontend (Client Application)**   
- Web-based, responsive application (with mobile support planned).  
 Key features:  
 - Wallet authentication, message signing.

- Identity resolution via Suins (human-readable names).

- Inbox, outbox, pay-to-send fee settings.

- Whitelist/blacklist address management.

- Identity management interface for name settings and profile control.

- Client-side caching of frequently accessed metadata to improve performance.

**Backend Services ( Off-Chain Layer)**  
 Server-side encryption: Message payloads are encrypted in the backend before off-chain storage.  
 Real-time notifications: Event-based backend pushes alerts to web clients when new messages arrive.  
 Hybrid storage architecture: Uses both decentralized storage (Walrus) and centralized databases (e.g., MongoDB) for managing:  
 - User-defined namespaces (NS)  
 - Wallet addresses  
 - Pay-to-send fee rules  
 - Whitelisted/blacklisted senders  
 - Auth token versions for secure session management.

**6. Use Cases {SuiMail in Action}**  
 Let's explore the real-world applications of SuiMail, showcasing how it transforms communication across Web3-native and traditional environments. These use cases illustrate how SuiMail introduces privacy, control, and monetization to messaging, ushering in a new era of secure, decentralized, and incentive-driven communication.  
  
**Secure Wallet-to-Wallet Communication:**  
 SuiMail enables verifiable, encrypted messaging between blockchain wallets. This allows for secure, tamper-proof communication without relying on off-chain platforms.  
Example:  
A DAO could notify members about urgent proposals or voting deadlines directly through **SuiMail** instead of Discord or email.  
  
**Spam-Proof Business Communication:**  
 Businesses, builders, and individuals can set a fee to receive messages. This **"pay-to-send" model** ensures that only senders who truly need to reach the recipient will pay to do so.  
Example:  
A DeFi auditor offers consultation services and sets a 0.5 SUI message fee. Startups can pay to pitch collaborations or request audits, eliminating spam and saving time.  
  
**User-Owned Messaging for Communities:{future plans}**  
 Projects can integrate SuiMail into their dApps to offer in-platform, user-to-user messaging, without needing centralized tools like Discord or Slack.  
Example:  
An NFT marketplace embeds SuiMail to let collectors and creators message each other privately after a trade, all within the app.  
  
**Cross-Chain Notifications & Alerts:**  
 SuiMail supports notifications from multiple chains and systems. Users receive identity-verified alerts from dApps, exchanges, or protocols they interact with.  
Example:  
A user receives a SuiMail alert that their staking position on a DeFi app is about to be liquidated, giving them a chance to act in time.  
  
**KOL Inbox Monetization:**  
 Key Opinion Leaders (KOLs) can charge access fees or require verification to be messaged, like a premium DM feature. This lets creators control attention and monetize access to their inboxes.  
Example:  
A Sui-based game founder sets a 1 SUI message fee for proposals and invites. Only serious offers make it through, and their inbox becomes a source of passive income.  
  
**Earning from Spam (Pay-to-Send):**  
 Users can monetize spam. Senders who want to reach inboxes must pay a fee, and recipients earn when they receive messages from non-whitelisted sources.  
Example:  
A wallet user receives a cold pitch from a new token project. Because of pay-to-send, the user earns 0.25 SUI for simply receiving the message.  
  
**Marketing Campaigns with Verified Reach:**  
 Projects can pay to reach users who’ve opted in to receive campaign messages. The audience earns rewards for attention, creating a fairer advertising ecosystem.  
Example:  
A cross-chain bridge launches and pays 5,000 SUI to target 10,000 engaged users on SuiMail. Those who open or click the message earn SUI, while the project gets warm leads.

**7. Roadmap** The primary goal of SuiMail is to redefine digital communication by enabling secure, spam-proof, and wallet-native messaging for both Web3 and traditional users. Our strategy begins with a lean MVP and testnet validation, then moves through integration, monetization, and eventual ecosystem-wide adoption.  
 We aim to build the future of wallet-to-wallet communication—starting from foundational tools and expanding toward powerful real-world use cases for DAOs, KOLs, DeFi protocols, NFT communities, and more.  
  
**Q2 2025:**  
- MVP Development   
- Testnet Deployment.  
  
**Q3 2025:**  
- Beta Launch  
- Initial traction and community onboarding.  
  
**Q3–Q4 2025:**  
- User Growth Phase  
- Integration with dApps and Web3 projects.  
  
**Q4 2025+:**  
- Mainnet Expansion  
- Pay-to-send monetization,  
- Cross-chain alerts,  
- KOL inboxes & campaigns.  
 This roadmap aligns with our current plan to establish SuiMail as the go-to protocol for secure, wallet-native communication, prioritizing utility, privacy, and creator-first monetization from the ground up.  
  
  
**8. Team {**Meet the Founders and the Team**}** SuiMail is proudly built by **Team Alpha** a passionate group of college students with a shared belief in the power of blockchain to solve real-world problems. Though we're still in school, our drive, technical skills, and vision for the future of decentralized communication push us to build at the level of global innovators.  
 What started as a campus collaboration by the **SUI ON CAMPUS INITIATIVE** has grown into a mission to redefine messaging in the Web3 space, enabling secure, wallet-to-wallet communication while giving users ownership, control, and new ways to earn through messaging.  
 Despite juggling classes, assignments, and personal growth, we’ve assembled a talented cross-functional team of developers, designers, and strategists. Each of us brings unique strengths to the table, from smart contract development and cybersecurity to user experience, community building, and brand design.  
  
**"We’re building SuiMail not just for the ecosystem, but also to prove that student-led teams can launch impactful, production-grade Web3 products".....**

In the following section, you’ll get to know the minds behind SuiMail, their areas of expertise, and their roles in bringing this vision to life.

**Abdulwahab Salisu  
Team Lead & Co-Founder**  
 Abdulwahab is a cybersecurity student and operations strategist driving the architectural vision of SuiMail. With a strong background in network defense and product coordination, he ensures SuiMail stays secure, scalable, and aligned with user needs. His leadership blends deep technical insight with efficient team coordination, keeping Team Alpha focused and agile.  
  
**Oladipo Evangel  
Technical Lead** Oladipo is the core blockchain engineer behind SuiMail’s smart contracts. With \the Move programming language and protocol design, he’s building the logic that powers our secure wallet-to-wallet interactions. His work ensures our systems are robust, auditable, and future-proof for cross-chain utility.  
  
**Abdulwaliy Jamiu  
UI/UX Designer**  
 Jamiu is responsible for shaping the user experience of SuiMail. He crafts clean, intuitive interfaces that ensure seamless message delivery, inbox navigation, and dApp integration. His design philosophy prioritizes both user comfort and Web3 accessibility.  
  
**Abundant Joel  
Brand Designer**  
 Abundant is the visual storyteller behind the SuiMail identity. From logo systems to brand tone and campaign assets, he translates complex blockchain concepts into bold, memorable visuals, making SuiMail recognizable across platforms.

**Abdulwahab Abdullahi  
Front-End Developer** Abdulwahab specializes in crafting fast, scalable interfaces with native Sui wallet support. His focus is performance and responsiveness, ensuring SuiMail runs smoothly across browsers and devices, with secure wallet-based authentication at its core.  
  
**Sarah Terwase  
Front-End / Move Developer**  
 Sarah bridges the front-end with Move smart contracts. Her hybrid skillset allows her to rapidly prototype and connect on-chain logic with user-facing components. She plays a vital role in syncing UI with blockchain actions like message signing and identity verification.  
  
**Ukanah Dean  
Full-Stack & Backend Developer**  
 Dean manages our off-chain infrastructure, including user metadata, message indexing, and external APIs. He’s the architect behind, our backend system that ensures low-latency performance and secure message storage.  
  
**Gyang Solomon  
Graphic Designer**  
 Solomon works closely with Brand and Community leads to produce stunning visuals, from social media assets to decks, infographics, and campaign media. Every design is aligned with SuiMail’s vision of clarity, professionalism, and decentralization.  
  
**Abdullahi Sofiyullah  
Community Manager**  
 Abdullahi is the voice of SuiMail across Web3. They lead growth campaigns, engage early adopters, and coordinate collaborations with other protocols, communities, and influencers, ensuring SuiMail has real traction from day one.  
  
 At SuiMail, we’re learning, building, and growing together. We're proof that a committed student team can dream big, build fast, and create something meaningful for the future of Web3.  
 Together, Team Alpha represents a rare blend of technical expertise, creative force, and operational excellence**. We're not just building a product,we're defining a new category in communication.** SuiMail is the future of messaging, and this team is the engine driving it forward.

**9. Governance & Community**  
 SuiMail envisions a decentralized future where the community actively shapes the protocol’s evolution and success. To achieve this, we plan to implement the following governance and engagement strategies:  
**- Community-Driven Governance:** Governance will progressively shift to a decentralized model, empowering users, developers, and stakeholders to propose, discuss, and vote on protocol upgrades, fee structures, and feature rollouts.  
**- Incentivized Participation:** Community members will be rewarded for activities like testing, bug reporting, marketing efforts, and moderation, creating a vibrant, engaged user base.  
**- Ambassador & Working Groups**: Establishing ambassador programs and focused working groups to advocate for SuiMail across regions and use cases, while providing structured feedback loops.  
**- Educational Initiatives:** Hosting webinars, workshops, and content campaigns to onboard users from both Web2 and Web3 backgrounds, ensuring inclusivity and awareness.  
**- Feedback Channels:** Maintaining transparent communication via platforms like Whatsapp, Telegram, X and other platforms for continuous dialogue and community input.  
 Through these efforts, SuiMail aims to foster a user-first, censorship-resistant messaging ecosystem guided by its global community.

**10. Legal Disclaimer** This whitepaper is provided for informational purposes only and does not constitute legal, financial, investment, or professional advice of any kind.  
 SuiMail is currently under active development, and the features, architecture, and roadmap outlined in this document are subject to change. No part of this document should be interpreted as a commitment, guarantee, or legally binding obligation by the SuiMail team or its contributors.  
 Engaging with or building on the SuiMail protocol involves risks inherent in emerging technologies, including but not limited to technical issues, regulatory developments, and market volatility.  
 Readers are encouraged to conduct their own research and consult appropriate professionals before making any decisions related to the project or its ecosystem.

**11. References**

1. Sui Blockchain Whitepaper – [[https://docs.sui.io](https://docs.sui.io)](https://docs.sui.io%5d(https//docs.sui.io))  
 Official documentation for the Sui blockchain, covering its architecture, object-centric model, and Move language.  
  
2. Move Language Documentation – [[https://move-language.github.io/move](https://move-language.github.io/move)](https://move-language.github.io/move%5D(https://move-language.github.io/move))

Technical guide to the Move smart contract language used on Sui and other chains.

3. XMTP Protocol – [[https://xmtp.org](https://xmtp.org)](https://xmtp.org%5d(https//xmtp.org))

A protocol for secure, wallet-to-wallet messaging; informed concepts like wallet communication and decentralized inboxes.

4. EPNS / Push Protocol – [[https://push.org](https://push.org)](https://push.org%5d(https//push.org))  
 A decentralized notification protocol inspiring our cross-chain alerts and opt-in messaging.

5. Walrus Key Management (Fictional/Internal Concept) – Used as internal inspiration for secure user metadata handling off-chain.

6. Sui Ecosystem Projects & Developer Blogs – [[https://sui.io/ecosystem](https://sui.io/ecosystem)](https://sui.io/ecosystem%5D(https://sui.io/ecosystem))  
 For benchmarking integration strategies and understanding best practices across current dApps and tooling.

7. Product-Led Startup Roadmaps (Generic/Startup Templates) – Used to guide the roadmap format, including MVP → Beta → Ecosystem growth trajectory.