

Krown Technologies Unveils BLOQ Talk, a Trust-First Web3 Messenger Built for the Post-Quantum Era

Launching October 1 on iOS and Android, BLOQ Talk combines Cipher Lock, AI scam defense, Liveproof verification, Trust Passport and trust-gated communities

MONROE, LA, UNITED STATES,

September 16, 2026 /

EINPresswire.com/ -- [Krown](#)

[Technologies Inc.](#) today announced the upcoming public launch of [BLOQ Talk](#), a security-first messaging platform designed for an era in which artificial intelligence, digital assets, impersonation attacks and future quantum computing are rapidly changing what it means to communicate securely online.

BLOQ Talk will launch globally on the Apple App Store and Google Play on October 1, 2026.

The platform was built around a simple premise: protecting the contents of a conversation is no longer enough. Users also need stronger ways to determine whether the person, community, device, wallet, link and identity on the other side of that conversation can be trusted.

BLOQ Talk combines private messaging with a broader trust architecture spanning post-quantum encryption, identity verification, scam detection, behavioral reputation, Web3 verification, deepfake-resistant human checks and trust-gated communities.



Bloq Talk Logo 2



Krown Wordmark Stacked Logo

“Messaging has evolved far beyond sending text from one phone to another, but the trust model behind most messaging has barely changed,” said James Stephens, Founder of Krown Technologies Inc. “Encryption can protect what somebody says. It cannot, by itself, tell you whether the person saying it is real. BLOQ Talk was built to address both problems — protecting the conversation while giving users substantially stronger signals about who they are communicating with.”

Cipher Lock: Encryption Built for Today — and the Post-Quantum Future

At the foundation of BLOQ Talk is Cipher Lock, Krown's post-quantum end-to-end encryption architecture.

Rather than treating post-quantum security as a future upgrade, Cipher Lock was designed into BLOQ Talk's private communications architecture from the beginning.

Its security model includes:

- Hybrid post-quantum key establishment. Cipher Lock combines the NIST-standardized ML-KEM-768 algorithm with classical X25519 key exchange in a hybrid handshake, creating defense-in-depth against both current cryptographic attacks and future quantum threats.
- Post-quantum device identity. Device key bundles are authenticated using ML-DSA-65, allowing users to verify cryptographic identity with a digital-signature scheme designed for the post-quantum era.
- Authenticated end-to-end encryption. Derived session keys protect messages using AES-256-GCM, providing both confidentiality and tamper detection.
- Group Cipher Lock. Sender-key encryption extends protected communications beyond one-to-one conversations and into group messaging.
- Safety-code verification. Users can verify contacts through QR-based safety codes and retain a persistent verification indicator once cryptographic identities have been confirmed.
- Post-quantum protection at rest. Stored encrypted content can be protected through an additional hybrid ML-KEM-768 and X25519 envelope around AES-256-GCM data keys.
- Cryptographic agility. Cipher Lock artifacts carry version information so algorithms and security parameters can evolve as standards and cryptographic research advance.

Under the architecture, Krown's servers handle public cryptographic material and encrypted content without possessing the session keys required to read private conversations.



BloqTalk Usage on a phone

The result is an architecture intended not only to protect conversations against today's attacks, but also to reduce exposure to so-called "harvest now, decrypt later" strategies in which encrypted data is collected today in anticipation of more powerful future computing systems.

Encryption Protects the Conversation. BLOQ Talk Adds the Trust Layer.

Krown describes post-quantum encryption as the foundation of BLOQ Talk.

Trust is the product built on top of it.

BLOQ Shield

- BLOQ Shield is the platform's always-on security and anti-abuse layer.
- Shield is designed to identify and respond to phishing links, impersonation attempts, suspicious domains, wallet-drainer patterns, spam and other malicious behavior before it reaches the user.
- Community operators also receive AI-assisted moderation tools for detecting abuse at scale.

And BLOQ Talk begins with an unusually restrictive privacy posture:

- Strangers cannot simply cold-DM or cold-call users by default.
- Unknown users must first pass through connection and trust controls, reducing one of the most common entry points for social-engineering attacks.

Liveproof

- Encryption cannot stop someone from using an AI-generated face or cloned voice during a call.
- BLOQ Talk's Liveproof system adds a human-verification mechanism designed specifically for that problem.

Two trusted people can establish a private verification word or phrase that exists only inside their encrypted relationship. Krown does not receive or store that secret in readable form.

During a suspicious call — particularly one involving money, credentials or another consequential request — a user can ask the other person to provide their Liveproof verification.

The feature is designed to make AI-assisted impersonation and deepfake fraud substantially harder by introducing a piece of shared human knowledge that is separate from a person's publicly available voice, face or online content.

Trust Passport and BLOQ Score

- Every BLOQ Talk user can build a Trust Passport: a portable record of identity verification, account history, community standing, recognition and other trust signals.
- Its companion BLOQ Score gives communities and users a dynamic indication of account trust.
- Unlike a simple follower count or popularity score, BLOQ Score is designed around identity,

behavior, contribution and standing.

-That score can then become functional.

-A Circle or BLOQ can require a minimum score before somebody enters, posts links, speaks in a live room or accesses a protected community.

Communities That Decide Who Gets Through the Door

BLOQ Talk introduces a configurable trust-gating system for communities.

Instead of treating every community as either “public” or “private,” owners can establish rules based on signals such as:

BLOQ Score, verified identity, invitation status, wallet ownership, NFT ownership, verified NFT profile pictures, manual approval or other trust requirements.

That creates a fundamentally different model for founders, creators, project teams, investors, developers and Web3 communities that routinely face impersonators, bots and fraudulent accounts.

Users can participate in BLOQs, Circles and verified Channels, while organizations and community operators control who can enter and what different trust levels are permitted to do.

Encrypted Voice, Video and Live Community Communication

BLOQ Talk extends private communication beyond text.

The platform includes encrypted one-to-one voice and video calling, incoming-call notifications, picture-in-picture support and call history.

Community communication expands further through live audio and video Rooms, including speaker and listener roles, raise-hand controls, event recording options and AI-generated recaps for users who miss live conversations.

Lifeline: Recovery Without Handing Krown the Keys

Account recovery presents one of the hardest tradeoffs in private communications: recovery systems that are convenient can also become security weaknesses.

BLOQ Talk's Lifeline feature is designed around trusted guardians.

Users can designate people they trust, and a configurable quorum of those guardians can participate in account recovery if a device is lost.

The recovery model can include both threshold approval and a veto window, providing a path back into an account without requiring Krown to become the custodian of a user's private encryption keys.

Web3 Features Without Abandoning the Safety Model

BLOQ Talk was built specifically for Web3 communities, but the platform's Web3 features sit behind the same trust and security architecture as the rest of the application.

Users can link wallets across supported blockchain networks, prove ownership without surrendering private keys, display verified NFT profile pictures, enter token- or NFT-gated communities, send crypto-related tips and participate in other blockchain-enabled experiences.

Wallet verification is based on cryptographic signatures and read-only blockchain verification.

BLOQ Talk never asks users to provide a wallet seed phrase or private key.

The platform also integrates with the broader KROWN ecosystem.

Everything Users Expect From a Modern Messenger

BLOQ Talk's security architecture does not replace the usability expected from a modern communications platform.

The application includes private chats, group messaging, communities, Channels, Stories, emoji reactions, GIFs, stickers, polls, checklists, disappearing messages, view-once media, voice notes, HD media, file sharing and translation capabilities.

BLOQ Talk also includes the native @bloq Assistant, bringing AI assistance directly into the application for functions such as conversation summaries, smart replies, translation and other messaging workflows.

The application is designed mobile-first for iOS and Android, with complementary web functionality.

Built for Creators, Projects and Communities

BLOQ Talk also introduces creator and community monetization tools, including paid memberships, tips, Circle Boosts, ticketed events and creator-oriented commerce capabilities.

A dedicated Creator Hub provides visibility into community activity and earnings, while trust gates give operators greater control over who participates.

That combination is intended to create a creator economy in which monetization and identity are supported by the same trust infrastructure used throughout the platform.

“Security should feel like a superpower, not like a security exercise,” Stephens said. “Cipher Lock, Shield, Liveproof, Lifeline and Trust Passport are designed to operate around the conversation instead of getting in its way. What the user should experience is a fast, beautiful messenger where a verification mark or green shield actually means something.”

A Different Model for Messaging

BLOQ Talk enters a market dominated by communications platforms built primarily around reach, convenience and network size.

Krown is taking a different approach.

BLOQ Talk is being built around trusted communication.

That means:

- post-quantum encryption instead of waiting for quantum migration;
- connection requests instead of unrestricted cold DMs;
- verified identity instead of usernames alone;
- trust-gated communities instead of one-size-fits-all access;
- on-chain ownership verification instead of screenshots and claims;
- human Liveproof checks instead of assuming a face or voice is real;
- and a portable Trust Passport instead of leaving reputation trapped inside a single community.

The company believes those differences become increasingly important as AI-generated identities, automated scams, digital assets and increasingly sophisticated social-engineering attacks converge.

Availability

BLOQ Talk launches October 1, 2026, on the Apple App Store and Google Play.

Additional platform availability and rollout information will be published through:

bloqtalk.app

About BLOQ Talk

BLOQ Talk is a trust-first, Web3-native communications platform developed by Krown Technologies Inc. The platform combines post-quantum encrypted messaging, trust-gated

communities, AI-assisted scam defense, identity and reputation tools, encrypted voice and video communication, Web3 verification and creator features within a mobile-first messaging experience.

BLOQ Talk is designed around the principle that secure communication requires more than protecting the message — it requires helping users establish trust in the person, device and community behind it.

About Krown Technologies Inc.

Krown Technologies Inc. develops blockchain, cybersecurity, digital identity and Web3 technologies focused on secure digital interaction and next-generation decentralized infrastructure.

Media Contact

Krown Technologies Inc.
Peter Biggs
peter.biggs@krown.network
media@krown.network
bloqtalk.app

Cipher Lock is described as quantum-resistant rather than “unbreakable.” Its architecture uses standardized post-quantum cryptographic algorithms in combination with established classical cryptography and is designed to evolve as cryptographic standards and research advance. Liveproof is an additional human-verification safeguard designed to reduce impersonation risk and does not replace appropriate judgment when responding to financial, credential or other sensitive requests.

Peter Biggs
Krown Technologies Inc.
+ +1 6828950101
email us here
Visit us on social media:
LinkedIn
YouTube
X
Other

Legal Disclaimer:

EIN Presswire provides this news content "as is" without warranty of any kind. We do not accept any responsibility or liability for the accuracy, content, images, videos, licenses, completeness,

legality, or reliability of the information contained in this article. If you have any complaints or copyright issues related to this article, kindly contact the author above.

Peter Biggs

Krown Technologies Inc.

+ +1 6828950101

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[YouTube](#)

[X](#)

[Other](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/942849546>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.