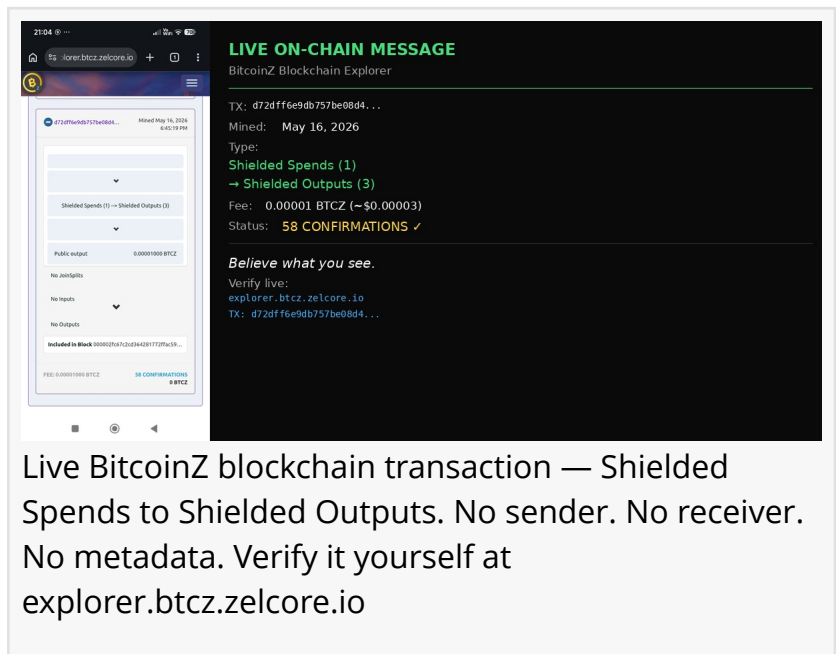


# Z-TEXT LLC: First Blockchain Messenger to Publish Its Threat Model

*Z-TEXT publishes full threat model and launches 7 ZEC bug bounty. First blockchain messenger with zero metadata and no phone number.*

SHERIDAN, WY, UNITED STATES, June 4, 2026 /EINPresswire.com/ -- Z-TEXT LLC, developer of the Z-TEXT privacy application — a blockchain-based messenger built on the [BitcoinZ](#) network — is publishing its threat model and launching a paid bug bounty program, disclosing known security limitations ahead of its public release.



Live BitcoinZ blockchain transaction — Shielded Spends to Shielded Outputs. No sender. No receiver. No metadata. Verify it yourself at [explorer.btcz.zelcore.io](#)

Z-TEXT is a 6-in-1 mobile application. It combines three tools — a shielded messenger, a password manager, and a crypto wallet — with three layers of privacy: zero metadata collection, zk-SNARKs zero-knowledge encryption, and post-quantum cryptographic protection. One single 24-word seed phrase generates and recovers everything. No phone number. No IP address. No central server. Ever. Messages are stored permanently on the BitcoinZ blockchain — eternal memory, at \$0.00003 per message.

“

Z-TEXT was built with no venture capital and no compromise. Publishing our limitations publicly is how we earn trust. Security scrutiny is our fuel.”

*Eric Pierrot, Founder, Z-TEXT LLC*

Privacy applications try to compete on features. Z-TEXT LLC is the first messenger to publish its full threat model at [z-text.com/docs/security](#) — June 2026. This public document lists exactly what Z-TEXT protects against — and its known limitations. Simultaneously, the company launched a paid bug bounty program, funding a 7 ZEC reward pool for security researchers — with up to 3 ZEC for a single critical

discovery.

Z-TEXT applies two independent encryption layers to every message. The first layer uses zk-

SNARKs shielded transactions on the BitcoinZ blockchain — hiding sender, receiver, amount, and content. The second layer applies AES-256-GCM contact key encryption. Both layers must be broken simultaneously to read a single message. Z-TEXT also implements ML-KEM-768 and ML-DSA-65 post-quantum cryptographic keys — designed to resist attacks from quantum computers.

Z-TEXT collects zero telemetry. No analytics. No crash reports. No phone number. No IP address. No server-side data storage. But your messages do not disappear. Your messages are stored permanently and immutably on the BitcoinZ blockchain — encrypted, invisible to the world, releasable only by your private keys. Forever.

Full threat model, known limitations, and bug bounty program: [z-text.com/docs/security](https://z-text.com/docs/security)

Z-TEXT LLC is a privacy technology company incorporated in Wyoming, United States. The company develops the Z-TEXT mobile application — available for Android and iOS — a blockchain-based private messenger built on the BitcoinZ network. Z-TEXT LLC is 100% self-funded with no venture capital.

eric pierrot

z-text llc

Contact@z-text.com

---

This press release can be viewed online at: <https://www.einpresswire.com/article/917360656>

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.