

Z-Text Bug Bounty Goes Live: 7 ZEC On-Chain to Anyone Who Breaks It

The zk-SNARKs blockchain messenger enters closed beta on five platforms and publishes a 7 ZEC bounty pool anyone can verify on-chain. zk means zero leaks.

SHERIDAN, WY, UNITED STATES, June 14, 2026 /EINPresswire.com/ -- Most privacy apps ask you to trust them. The Z-Text zk-SNARKs blockchain messenger asks you to attack it.

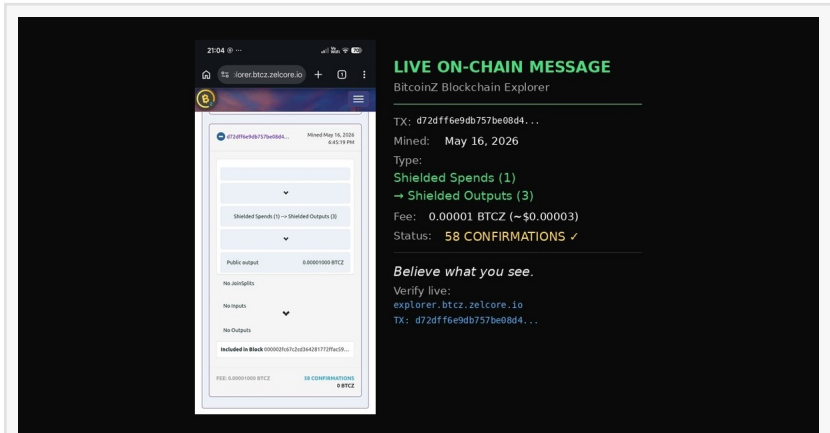
Z-Text, a zk-SNARKs blockchain messenger built on the BitcoinZ network, is now live in closed beta across five platforms at once:

Windows, Linux, Android, macOS, and iOS. Z-Text needs no phone number, no email, and no SIM, and is designed to collect zero metadata. Alongside the beta, Z-Text runs a live, paid bug bounty with a funded pool of 7 ZEC, and the bounty wallet address is published openly so anyone can verify it on-chain.

“

Privacy by promise is everywhere. Privacy by proof is rare. We published a 7 ZEC bounty and opened beta on five platforms because we would rather be attacked than trusted. Freedom cannot be free.”

*Eric Pierrot, founder, Z-Text
zk-SNARKs blockchain
messenger*



A live shielded message on the BitcoinZ blockchain, verifiable on-chain — Z-Text's proof that privacy can be checked, not just promised.

The message is simple. Break it, and get paid.

Why metadata is the real battleground

Most encrypted apps protect what you say. They do not protect who you talk to, or when. That residue is called metadata, and security experts have long warned it is enough. As former NSA general counsel Stewart Baker once put it, with enough metadata you do not really need the content at all.

This is the gap Z-Text was built to close. Standard

encrypted apps like Signal protect the content of your messages, but they still reveal who is talking to whom and when. The Z-Text zk-SNARKs blockchain messenger targets the metadata

itself, using zero-knowledge proofs to let a user prove the right to send or receive a message without revealing identity.

Three rules Z-Text plays by

Zero KYC. No phone number, no email, no SIM, no identity check. Nothing to collect, nothing to leak, nothing to sell.

Shielded digital identity. Your identity is a 24-word seed phrase you control, not an account on someone else's books. From it you can generate thousands of shielded identities.

Censorship-proof by design. Messages settle on the decentralized BitcoinZ blockchain, not on a company message server that can be seized or switched off.

Cryptography is not enough

All the cryptography in the world means nothing if the service behind it is centralized and authority-dependent. A company that depends on venture capital, advertising, or selling data has a master, and a master can be pressured or compelled. This is why Z-Text charges a small license fee instead of being free. When a service is free, the user is usually the product. Freedom cannot be free.

The field, scored honestly

Z-Text publishes where it leads and where it does not. Against SimpleX, Session, and Briar, Z-Text leads on five points no rival combines: post-quantum encryption on by default, message recovery from a single seed phrase, shielded payments, a built-in password manager, and all



Privacy as the Fifth Element — Z-Text carries censorship-resistant, on-chain messaging into the open



The Z-Text bird — a zk-SNARKs blockchain messenger built on BitcoinZ.

three tools in one app.

It also names its gaps. Z-Text has not yet completed an independent third-party security audit, while SimpleX and Session have. That is exactly why the bounty exists. The threat model and the full list of what Z-Text does not protect against, including ISP-level visibility and device compromise, are published openly on the [Z-Text security page](#).

The data behind the demand

The public already senses the problem. Research from Pew and others shows that 81% of US adults believe the data companies collect will be used in ways they find uncomfortable, and 52% of Americans have avoided a product or service over data-collection concerns. In the World Economic Forum's 2026 outlook, business leaders named the leak of personal data through new AI systems as their single biggest security concern.

Z-Text is a different bet, made in the open, with the bounty wallet on-chain for anyone to check.

About Z-Text

Z-Text is a zk-SNARKs blockchain messenger built on the BitcoinZ blockchain, live since September 10, 2017. Z-Text combines a shielded messenger, a password manager, and a crypto wallet in one app, with post-quantum protection, panic mode, and stealth mode. Z-Text requires no phone number, no email, and no SIM, and is designed to collect zero metadata. Learn more at z-text.com, read the full bug bounty and threat model at the Z-Text security page, and read about the blockchain it runs on at getbtcz.com.

eric pierrot

z-text llc

security@z-text.com

Visit us on social media:

[Other](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/919511632>

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.