

This is a copy of a conversation between ChatGPT &amp; Anonymous.

[Report conversation](#)

what do you know about zoscii

Here's what I found about **ZOSCII** (Zero Overhead Secure Code Information Interchange) — the project claims to deliver a radically different security paradigm:

### ✓ What ZOSCII claims to do

- ZOSCII says it enables **"zero encryption / zero ciphering"**, i.e. no traditional cryptographic key-based encryption. [zoscii.com](#) +1
- It uses **address-based indirection**: instead of encrypting data, it points into a shared reference file (ROM) via addresses, so the "data" is essentially a sequence of pointers. [Linksealln. +22](#)
- It claims to be **quantum-proof** because the attack surface is not computational complexity but combinatorial/indirection-based. [zoscii.com](#) +1
- It claims to allow **perfect deniability** (no visible encrypted blob or key, making it hard to prove a hidden payload exists). [zoscii.com](#)
- They propose use-cases: automotive security (relay/replay attack proof key fobs), IoT, blockchain/tamperproof storage, message queues. [zoscii.com](#)
- They also have a "snake-oil challenge": "Think it's snake-oil? Prove it by cracking a file encoded with ZOSCII, win 10 billion ZOSCII tokens." [zoscii.com](#) +1

### ⚠ Observations & caveats

- The core claim—"no encryption, no ciphering, yet 100% secure" via indirection—is **very bold** and deviates heavily from standard cryptographic practice.
- On the Hacker News thread, the method is described simply: storing addresses into data in a shared reference file rather than transforming the data. [news.ycombinato...](#)
- Because it's so unconventional, there's **very limited independent cryptographic peer review** (as far as I found) verifying claims such as "mathematically impossible to break."
- The "challenge" implies they expect scepticism: they invite people to break their scheme. That can be a positive sign (they're open) or a red flag (if no one has done it yet and it's marketed as "unbreakable").
- The token side: there is a token called ZOSCII COIN (symbol ZOSCII) listed on BSC with low liquidity/volume. [ApeSpace](#)
- Low liquidity and small holder count in the token suggest it might be very early stage or speculative.

### 🔍 My view / what to check

- If you're considering using it for security: ensure there is **peer-reviewed cryptanalysis** of the protocol. Unconventional claims require strong evidence.

- If you're looking at the token side: given low market cap and liquidity, be aware of **high risk** (volatility, limited adoption).
- If any project claims "100% secure" and "no encryption" it merits extra caution: cryptography is hard and many past "unbreakable" claims have been wrong.
- For practical deployment: check how the shared ROM (reference file) is managed, how addresses are kept secret, how integrity is ensured, how deniability truly works, how large the reference file must be, etc.
- If you're just exploring: this is a very interesting "alternative cryptography" experiment worth following — but I would treat it as speculative until matured.

If you like, I can check for **any academic papers** on ZOSCII or **independent security audits** to see whether its claims hold up. Would you like me to do that?

 Sources

can you find anything that claims it's fiction?

I couldn't locate any *definitive* published cryptographic analysis or formal peer-reviewed study that declares ZOSCII to be purely fictional, but there are **strong warning signs** and commentary from the crypto-community that classify it as likely "snake oil"-type cryptography. Here's a summary:

### ✓ Evidence in favour of scepticism

- The ZOSCII website itself states that critics like Bruce Schneier called it "snake-oil of the highest degree".  
zoscii.com +1
- The marketing claim is extremely bold: "ZERO encryption, ZERO ciphering, 100% secure" via address-based indirection. zoscii.com +1
- There is no readily found independent cryptanalysis (or publicly cited one) that verifies the core security claim.
- In cryptography, systems that claim to be "unbreakable" or "perfectly secure" without well-understood and widely vetted foundations are flagged as "snake oil". sajiebunty..+22
- The very existence of a "challenge" (decode this file & win tokens) suggests they expect sceptics — but also that the proof of concept has not been widely validated. zoscii.com +1

### ⚠ Why it doesn't necessarily mean "fiction"

- The system is publicly described (at least superficially) and claims open-source licensing (MIT) for some tools. zoscii.com +1
- They give a challenge with specific quantitative security figures (e.g.,  $\sim 10^{156}$  combinations) rather than purely vague marketing. zoscii.com
- "Fiction" would mean the system is entirely bogus or non-functional; scepticism alone does not prove it's non-functional — just that it lacks independent verification and may rely on unproven premises.

### 🔍 My assessment

Given the evidence, I lean toward treating ZOSCII as **high-risk** and **speculative** rather than fully credible for production security use. It exhibits many of the tell-tale markers of "crypto snake oil":

- Grand claims of unbreakability without sufficient peer-reviewed evidence
- Use of novel paradigm (address-based indirection) rather than well-tested cryptographic primitives
- Marketing that emphasises "zero encryption" in a field where encryption/key management is central and well-understood.

So while I wouldn't state unequivocally "it's pure fiction", I would say the **burden of proof is high**, and until validated by independent cryptographers the claims should be treated **very cautiously**.

---

If you like, I can dig into cryptography forums (e.g., sci.crypt, cryptography mailing lists) to see if anyone has attempted or published a technical critique of ZOSCII and found concrete flaws. Would you like me to do that?

   Sources

Message ChatGPT

 Attach

 Search

 Study

 Voice

ChatGPT can make mistakes. Check important info. See [Cookie Preferences](#).

### We use cookies

Some cookies are essential for this site to function and cannot be turned off. We also use cookies and collect and share device identifiers to help us understand how our service performs and is used, and to support our marketing efforts. Learn more in our [Cookie Policy](#). You can update your preferences at any time by clicking '[Manage Cookies](#)'.

Manage Cookies

Reject non-essential

Accept all