ensuro

Blockchain-based, licensed, (re)insurance.

Ensuro Risk Disclosure

Last Updated: April 09, 2025

By accessing or using Ensuro's services—including our website (ensuro.co), web-based application, or any affiliated interfaces—you acknowledge and agree to the inherent risks associated with cryptographic systems, blockchain-based financial protocols, and tokenized insurance-linked products. Ensuro Re, a regulated entity under the Bermuda Monetary Authority (BMA), operates these services under an Insurance General Business (IIGB) license and a Digital Asset Business Class M license. Before engaging in any transaction, you must carefully review and accept the following material risks:

1. Cryptographic and Blockchain Network Risks

Ensuro operates primarily on the Polygon blockchain, using smart contracts to underwrite insurance risks and manage capital. These systems are subject to:

- Ongoing technical evolution, including risks from quantum computing and cryptographic vulnerabilities.
- Potential software bugs or unexpected outcomes, despite external audits and adherence to rigorous security standards.
- Hacking risks that could compromise blockchain integrity or user assets.

2. Responsibility for Private Keys

Interactions with Ensuro, including eToken management, rely on public/private key cryptography:

- You are solely responsible for safeguarding your private keys and wallet credentials.
- Loss or compromise of your private keys will result in irrevocable loss of your digital assets (e.g., eTokens or stablecoins).
- Ensuro cannot recover lost keys or restore access to funds.

3. Decentralized Protocol Interactions

Ensuro may allocate eToken pool capital to decentralized finance (DeFi) protocols (e.g., Aave, Compound) to generate yield. These interactions carry:

- Smart contract vulnerabilities or exploits.
- Admin key risks, where protocol administrators could mismanage funds.
- Underlying asset liquidity risks, potentially affecting pool stability.
- Systemic DeFi risks, even with Ensuro's strict investment policies and use of well-audited, high-total-value-locked (TVL) protocols.

4. Insurance Underwriting and Credit Risk

As a decentralized (re)insurance platform, Ensuro assumes underwriting risks from partner risk modules:

- Risks are assessed and collateralized using actuarial models (e.g., 99.5% Value-at-Risk), but losses remain possible.
- Claim surges or mispriced risks could lead to partial or total loss of capital in eToken pools.
- Investors bear the financial impact of such losses, limited to their pool's assets.

5. Liquidity Risk

eToken and insurance pool liquidity depends on utilization rates and market conditions:

- Most capital is held in highly liquid stablecoins (e.g., USDC), but constraints may arise during high claim periods or market volatility.
- You may not be able to withdraw funds instantly, especially when pool capital is heavily utilized.

6. Smart Contract and Platform Risks

Despite multiple audits and rigorous testing, Ensuro's smart contracts and platform face:

- Potential unforeseen bugs or vulnerabilities to exploits.
- Downtime risks from frontend oracles, settlement layers, or partner integrations, which could disrupt access to capital, transaction execution, or policy resolution.

7. Platform Shutdown Risk

In extreme scenarios, such as force majeure, regulatory mandates, or catastrophic technical failures:

- The Ensuro protocol or services may become inaccessible.
- Contingency plans (e.g., multisig safeguards, disaster recovery strategies) exist, but immediate access cannot be guaranteed in all situations.

8. Regulatory Oversight and Jurisdictional Restrictions

Ensuro Re Ltd. is regulated by the BMA, but:

- Regulatory changes in Bermuda or globally could impact service availability, restrict investor onboarding, or necessitate structural changes.
- Services are unavailable to residents of restricted jurisdictions (e.g., Crimea, Cuba, Iran, North Korea, Syria, the United States) or regions under sanctions by the U.S., UK, or EU.

9. Cybersecurity Risks

Ensuro employs a multilayer cybersecurity framework and "security by design" principles, but:

- Threats like phishing, DDoS attacks, and smart contract exploits persist.
- You must follow best practices (e.g., secure wallet management, avoiding unverified channels) to mitigate these risks.

10. Data Handling Risks

Personal information is not stored on-chain:

- KYC/AML data is securely stored off-chain per privacy laws, but no system is entirely immune to breaches.

11. No Insurance Coverage

Ensuro does not provide insurance for:

- Digital asset losses, cyber theft, smart contract bugs, or DeFi protocol failures.
- You must factor this lack of coverage into your investment decisions.

12. Independent Evaluation Required

Ensuro does not offer financial recommendations:

- You must independently assess all risks, including legal and tax implications in your jurisdiction.
- Past performance is not indicative of future results.

Acknowledgment

By using Ensuro's services, you confirm your understanding of these risks, including those tied to future technological developments (e.g., quantum computing). This disclosure is provided in compliance with the Digital Asset Business (Client Disclosure) Rules 2018 and is available for download at ensuro.co/risksdisclosure. You will be required to acknowledge these risks prior to your first transaction via the Ensuro platform.

For further details, review our full Terms of Service at https://ensuro.co/Ensuro_ToS.pdf or contact us at info@ensuro.co.