WORM

A Privacy-Preserving, Cryptographically Scarce Token

Backed by ETH burn 🔥

The Problem

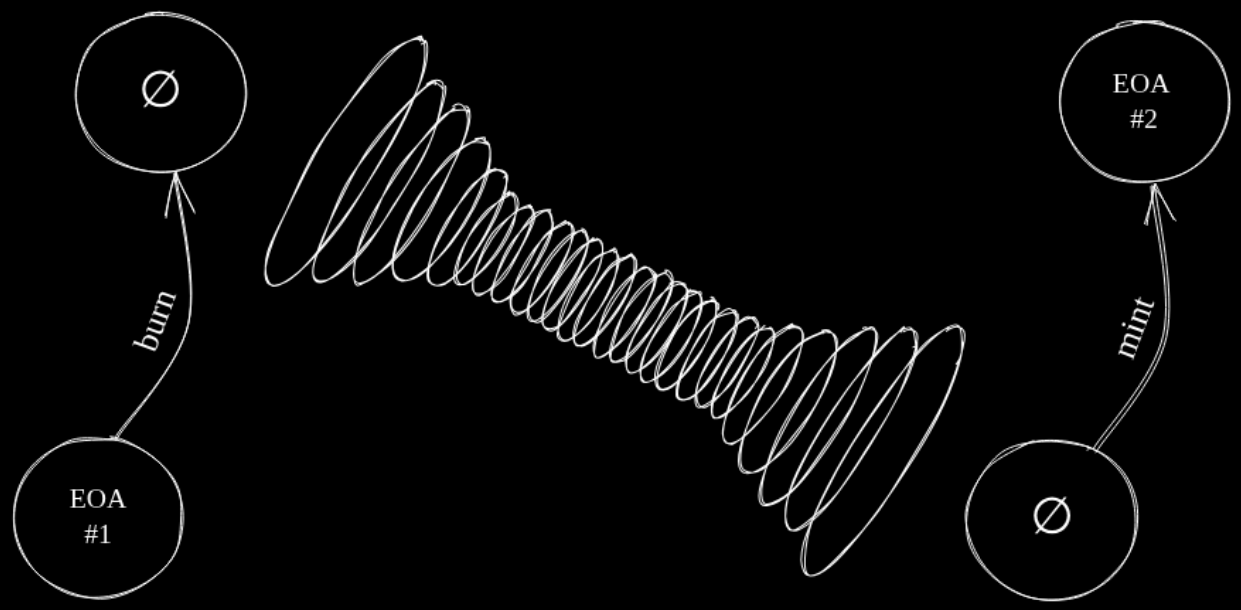
🎭 Privacy ≠ Invisibility 👻

- 🌪️ Tornado Cash users ***flagged*** despite ZK privacy
- 🚩 On-chain activity = signal
- 🥣 Mixing ≠ plausible deniability

Privacy without deniability is just surveillance-resistant!

EIP-7503 🕳️

1. Burn ETH (Privately! 😈)
2. Prove it 🧾
3. Get something back in return! 🖨️



Plausible Deniability

Deny you have ever participated in a privacy protocol!

0xbfda002fae4...	Transfer	8879368	3 days ago	0x0F19c76C...f795ac396	OUT	0x2402128E...03cEA6035	1 ETH	0.000021

🕵️ This is what an outsider sees:

- A perfectly normal looking transfer. 🤷
- To a perfectly normal looking Ethereum address. 👀
- Only you and the ZK circuit knows this is a burn-address! 🔥

WORM's implementation

WORM

- Burn ETH
- Get WORM

bitcoin

- Burn electricity ⚡
- Get BTC

🖨️ WORM Issuance

🪱 50 WORM / 30 min ⏳

WORM per user = (User's BETH) / (Total BETH) × 50

The Two-Token Model

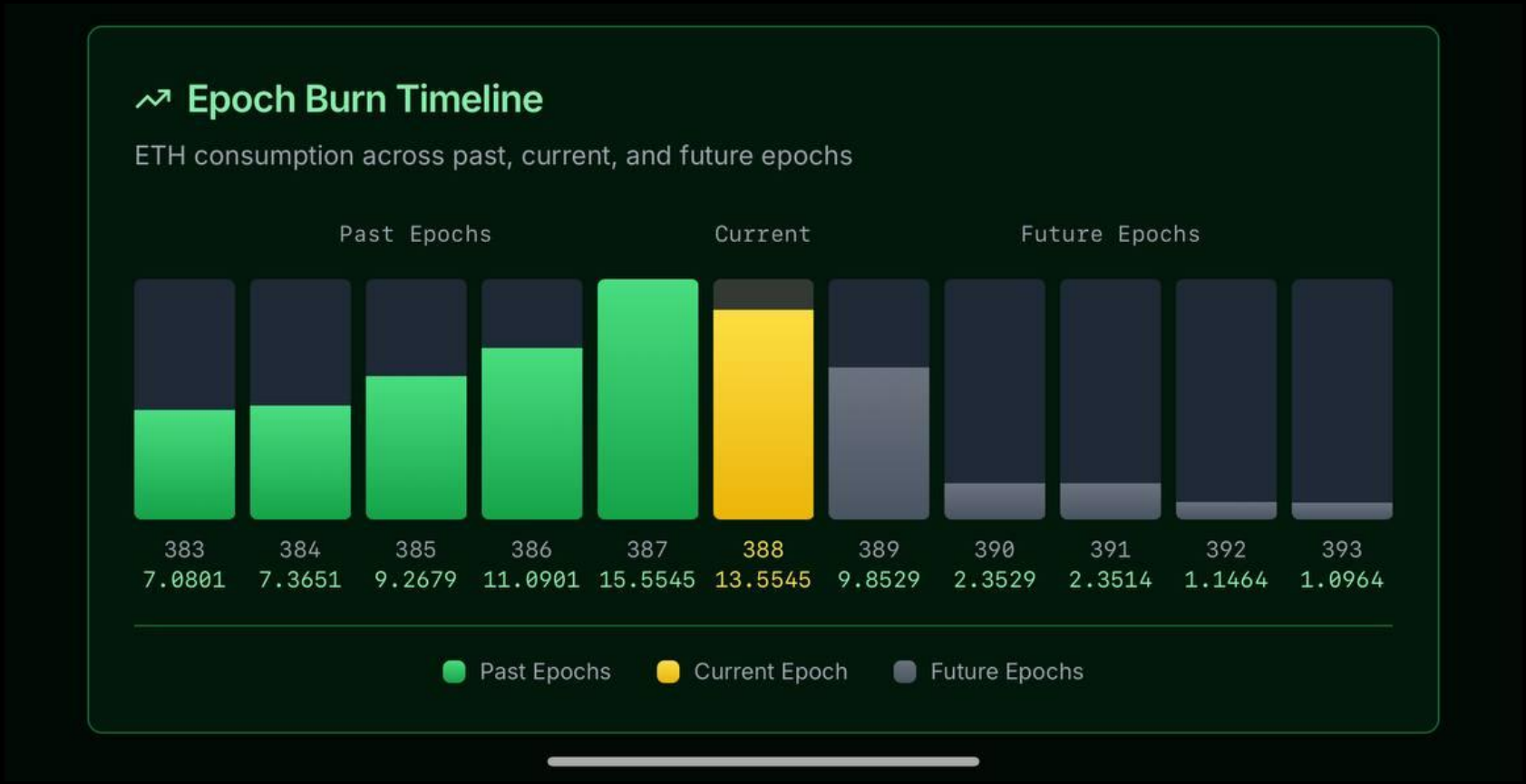
🔥 BETH – Burn Receipt

- 🧾 1 BETH = 1 ETH provably burned

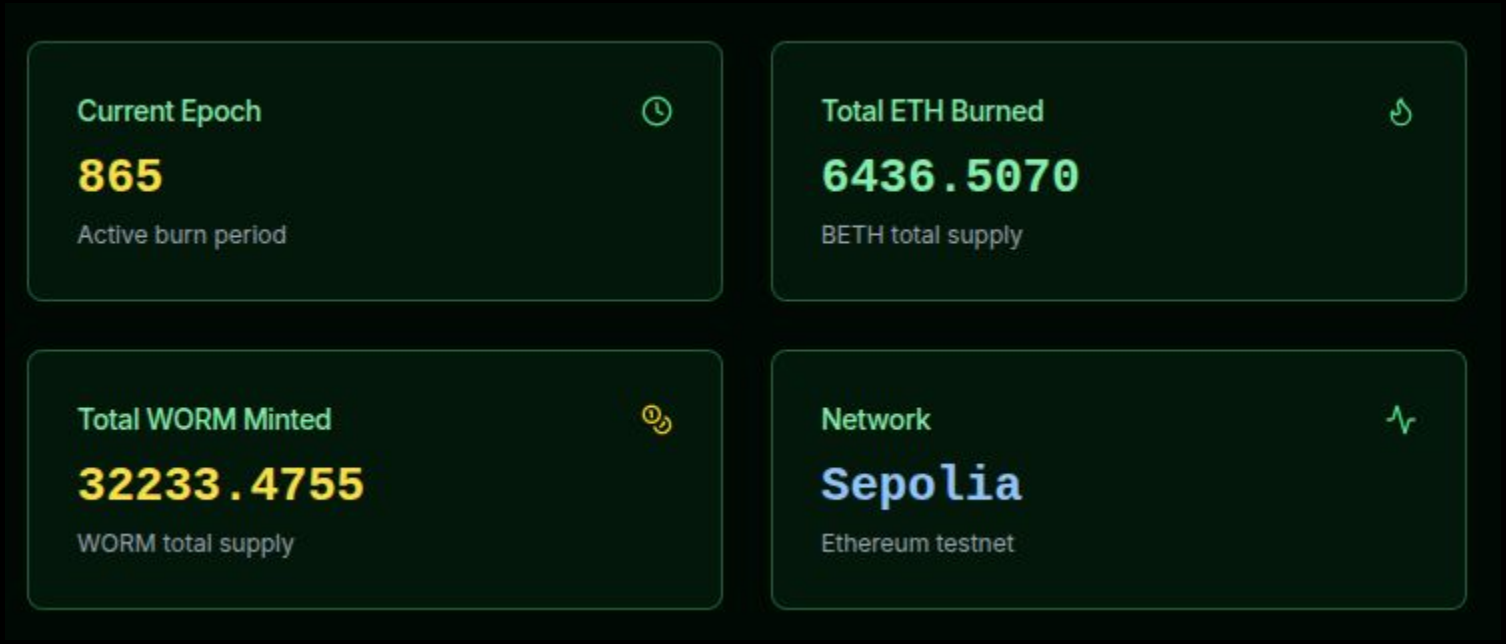
🪱 WORM – Scarce ERC-20 Token

- 🌱 50 minted / 30 min epoch

Lindwurm Testnet



Lindwurm Testnet



~40 real participants

Technology stack

- 🎭 **Circom + SnarkJS**
- 🔱 **Poseidon** hash function for burn-address generation
- 🌳 **Keccak** hash function for Merkle-Patricia-Trie proofs
- 🪨 **Solidity** verifier contracts
- 🦀 **Rust**-based ETH-burner and WORM-miner

Good and bad BETH are distinguishable

The good actor may provide a ZK proof that his burnt ETH is not associated with bad actors!

Comparison

	Tornado	Railgun	WORM
On-chain link	Yes	Yes	Receiver only
Sanctionable	Yes	Yes	Receiver only
Proof of innocence	No	Yes	Yes
Deposit fee	1,088,354	730,000	21,000 🌀
Withdrawal fee	301,233	> 500,000	303,000

🌀 Sending is just a plain transfer

Tokenomics (BETH)

ETH		BETH
1	:	1

Tokenomics (WORM)

Monero-style gradual decay with tail emission

Why?

- Provides a clear, predictable supply curve.
- Supports stable growth of the privacy ecosystem.
- Incentivizes long-term network participation.

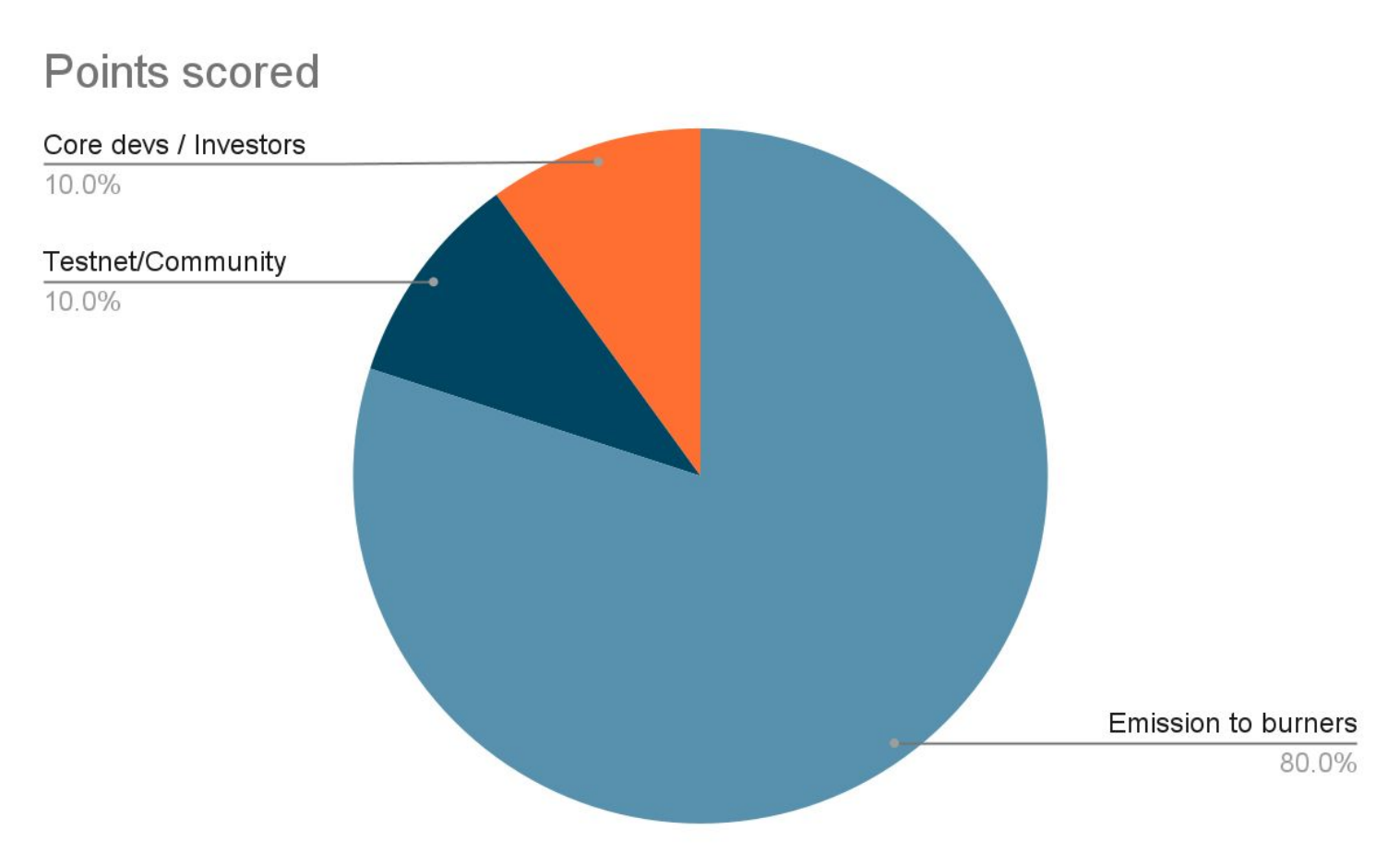
Tokenomics (WORM)

Year	Block Range	Avg Block Reward (WORM)	Annual Reward (WORM)
1	0 - 17,520	~37.0	37 × 17,520 = 647,000
2	17,521 - 35,040	~27.5	27.5 × 17,520 = 481,800
3	35,041 - 52,560	~20.5	20.5 × 17,520 = 359,160
4	52,561 - 70,080	~15.3	15.3 × 17,520 = 268,000
5	70,081 - 87,600	~11.4	11.4 × 17,520 = 199,700
6	87,601 - 105,120	5 (tail)	5 × 17,520 = 87,600
7	105,121 - 122,640	5	87,600
8	122,641 - 140,160	5	87,600
9	140,161 - 157,680	5	87,600
10	157,681 - 175,200	5	87,600

$$R(n) = \max\left((R_0 - R_{tail}) \times e^{-k \times n} + R_{tail},\ R_{tail}\right)$$

Proposed allocation

(% of total supply over 5 years)



Roadmap

Q3 2025

- Implementing the Proof-of-Burn circuits ✅
- Launching and finalizing the Lindwurm testnet ✅
- Auditing and freezing of Proof-of-Burn circuits ⏳
- Finalizing the tokenomics / raising fund ⏳

Q4 2025

- Launching WORM's second testnet ➡️SOON
- Performing trusted-setup ceremony ➡️SOON
- Building better UX + Bridge/DEX integrations ➡️SOON
- Mainnet preparation ➡️SOON
- Building a more sophisticated WORM-miner ➡️SOON

Q1 2026

🪱 MAINNET LAUNCH! 🥳

Team

Keyvan Kambakhsh

Cofounder | Protocol Architect

Core developer and architect of the WORM protocol, specializing in zero-knowledge cryptography and privacy-preserving systems.

GitHub

Shahriar Ebrahimi

Cofounder | Applied Cryptography

Applied Cryptographer, mostly focused on Zero-Knowledge Proofs and Multi-Party Computation.

GitHub

Zero Savvy Ltd - UK registered entity

Thanks!

#FreeRomanStorm