ProofChain Protocol

PROTOCOL PROVENANCE REGISTRY

Immutable audit provenance for smart contracts. Trust in Web3 should be verifiable, not assumed.

BLOCKCHAIN PROVENANCE · SEPOLIA TESTNET

THE TRUST DEFICIT

FRAGMENTATION

Audit reports are trapped in off-chain silos: PDFs, emails, and private systems. Verification is slow and manual.

OPAQUE HISTORY

No immutable record of protocol changes over time. It's impossible to verify if the "audited" code matches the "deployed" code.

ON-CHAIN PROVENANCE

ProofChain creates a **Decentralized Truth Layer** for security audits. By anchoring hashes on-chain, we bridge the gap between audit reports and live protocols.

- Immutable Audit Signatures
- Protocol Version Tracking
- Cryptographic Verification

VERIFICATION WORKFLOW

1. REGISTER

Protocol data anchored on-chain

2. COMMIT

Store Audit + Commit Hash

3. HASH

PDF hashed via keccak256

4. VERIFY

Instant VALID / INVALID result

Verification Logic:

$$\text{Status} = \begin{cases} \text{VALID} & \text{if} H_{local} = H_{chain} \\ \text{INVALID} & \text{otherwise} \end{cases}$$

SYSTEM CAPABILITIES

ON-CHAIN REGISTRY

Append-only ledger of all protocol identity and audit metadata on Sepolia.

PDF CRYPTO-VERIFY

Verify audit integrity by matching local PDF hashes with blockchain records.

VERSION TRACKING

Track audit history across multiple protocol upgrades and commit hashes.

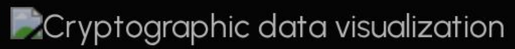
TECHNICAL STACK

BACKEND: SEPOLIA

Solidity smart contracts act as the source of truth. Zero database dependency ensures decentralization.

FRONTEND: NEXT.JS

Tailwind CSS + Ethers.js v6. Client-side Keccak256 hashing via browser crypto APIs.


Cryptographic data visualization

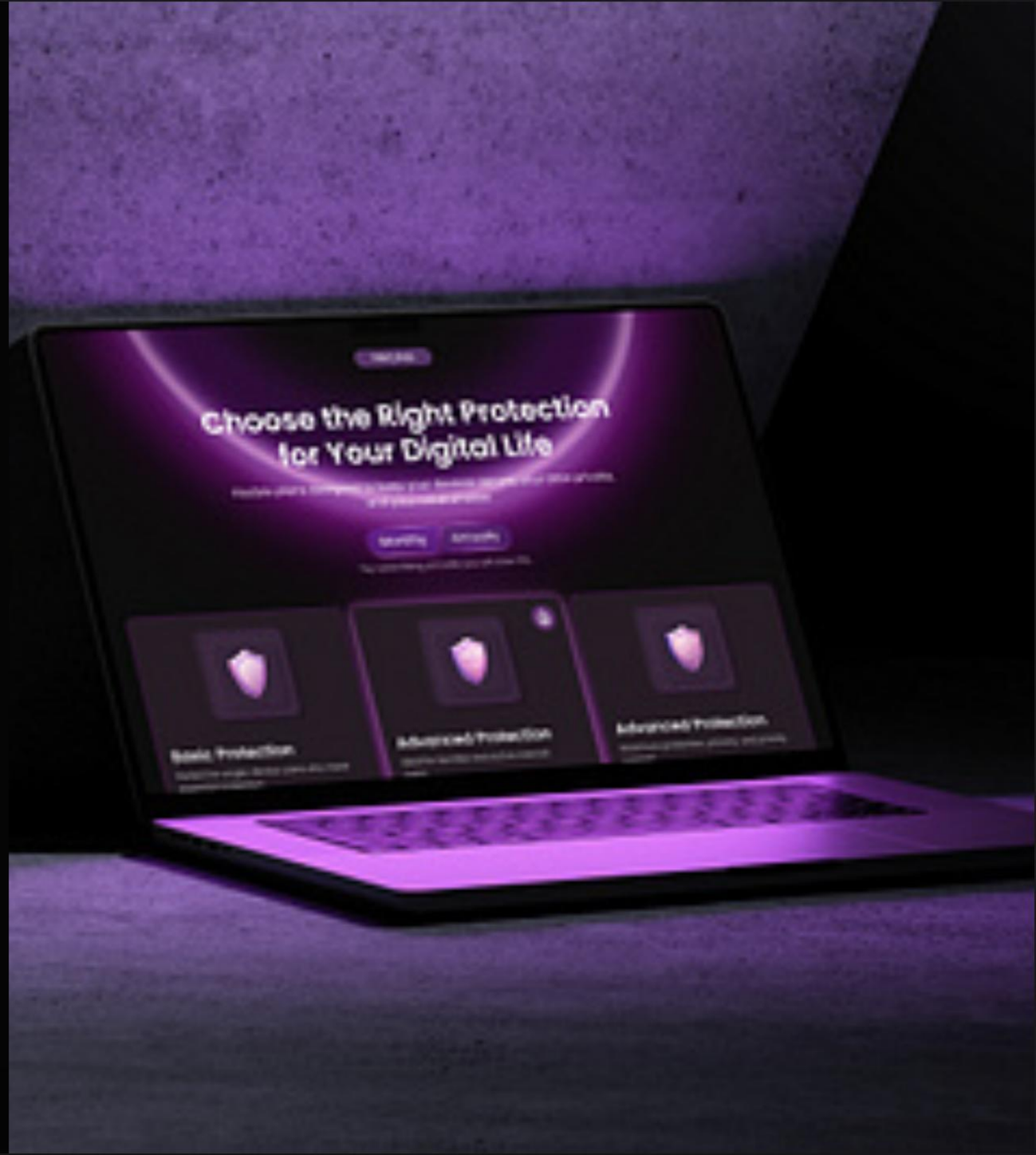
UX & INTERFACE

PROTOCOL EXPLORER

Users can browse a timeline view of audits and historical smart contract versions.

VERIFICATION PORTAL

A drag-and-drop interface that generates local hashes without uploading sensitive files.



ON-CHAIN DATA MODEL

100%

Audit Transparency

```
struct ProtocolRecord {
  string name;
  bytes32 auditHash;
  string commitHash;
  uint256 timestamp;
  address auditor;
}
```

"Immutable append-only registry ensures that audit history can never be rewritten or deleted by malicious actors."

IMPACT & ADOPTION

- **DeFi Protocols:** Publicly verify that a deployment matches its audited commit.
- **Compliance:** Immutable audit logs for regulatory reporting and KYC/AML protocols.
- **Insurance:** Accurate risk assessment based on verifiable audit history.

LIVE PERFORMANCE

Metric	Manual Process	ProofChain Registry
Verification Time	Hours / Days	~15 Seconds (Block Time)
Trust Source	Centralized (PDF Host)	Decentralized (Sepolia)
Audit Integrity	Tamperable	Cryptographically Immutable
Cost	Personnel Overhead	Minimal Gas Fee

A Protocol for Truth

“TRUST IN WEB3 SHOULD BE VERIFIABLE, NOT ASSUMED.”

ProofChain makes audit history immutable, transparent, and accessible to every participant in the ecosystem.

QUESTIONS?

Build the Future of On-Chain Trust

github.com/proofchain-registry

proofchain.io

@ProofChain


Abstract blockchain visual

IMAGE SOURCES

https://img.freepik.com/premium-vector/bright-purple-neon-shield-icon-cybersecurity-data-protection-digital-security-concept_894188-8379.jpg

Source: www.freepik.com

https://images.stockcake.com/public/b/e/0/be0b6e46-6cc0-40be-b94a-84b1fb8aab46_medium/digital-matrix-visualized-stockcake.jpg

Source: stockcake.com

https://cdn.dribbble.com/userupload/43787547/file/original-d20fb8cd3971c6637bbaa4e1bfda0234.jpg?resize=400x0

Source: dribbble.com

https://images.stockcake.com/public/9/2/e/92e499b8-06ac-4069-883b-19c3a519cc90_medium/digital-world-glow-stockcake.jpg

Source: stockcake.com

https://images.stockcake.com/public/8/e/7/8e782f0b-bf75-4a2e-81f4-8e785b4b156d/futuristic-blockchain-logo-stockcake.jpg

Source: stockcake.com