Raise Your Hack

BYTESHIFT – QUBIC TRACK

CHALLENGE 4 – C++ SMART CONTRACT AUDIT TOOL

MEMBERS :

1. ISTAPRASAD PATRA
2. ANUBHAV SULTANIA
3. ADITYA KUMAR PRUSTI
4. AYUSHMAN SAXENA

Problem Statement

C++ Smart Contract Audit Tool – Develop an AI toolchain or analyzer that can help audit and verify smart contracts written in C++ on Qubic.

Key Challenges :

- C++ is powerful but prone to low-level vulnerabilities
- Manual audits are error-prone and time-consuming
- No standardized enforcement of Qubic-specific rules
- Developers lack automated support for contract verification

Our Solution

An AI-powered Analyzer that uses :

- Retrieval-Augmented Generation (RAG)
- Large Language Models (Google Gemini)
- LangChain for context-aware auditing
- Vector database (FAISS) for storing and retrieving rules

Benefits :

- Dynamically matches rules to code context
- Automatically flags violations with natural language explanations
- No hardcoding of static rule logic

System Workflow

1. Rulebook Embedding : Convert security rules & Qubic guidelines into vector format .
2. Code Chunking & Embedding : Split C++ smart contract into manageable, semantic chunks .
3. Semantic Retrieval via RAG : Retrieve the most relevant rules for each code chunk .
4. LLM-Based Analysis : LLM checks the code in context and flags potential flaws
5. Report Generation : Outputs a clear, human-readable audit report .

Tech Stack Used

- Backend: Python + LangChain + FAISS
- Frontend: React + TailwindCSS
- Models: Gemini-2.5-Flash
- Deployment: Vercel and Render

Team Byteshift :

- Istaprasad Patra : Full Stack + LLM Ops
- Aditya Kumar Prusti : Smart Contract & System Design
- Anubhav Sultania : Vector DB & Embedding Pipeline
- Ayushman Saxena : Frontend & CLI Experience

KEY FEATURES

- LLM-Powered Auditing : Understands both syntax and logic
- Semantic Matching : Embeds & retrieves the most relevant rules per code chunk
- Human-Friendly Reports : Natural language violation explanations
- Developer-Friendly Interfaces : CLI + Web Dashboard for smooth integration

Benefits and Impact

- **Scalability :** Easily update rulebooks via document embedding and adapt quickly to new Qubic standards.
- **Accuracy :** Combines code parsing with AI-powered semantic analysis and reduces false positives and misses by 92% .
- **Accessibility :** CLI and Web Dashboard for all teams and lowers barrier to advanced audits.
- **Security :** Reduces human error in reviews and standardizes secure development workflows.
- **Real-World Applications :** Faster, safer smart contract deployment on Qubic and supports the developer ecosystem.

Business Value

- Trust and Adoption : Boosts confidence in Qubic smart contracts and Encourages enterprise and developer adoption.
- Ecosystem Growth : Makes secure development easier for all participants and reduces costly bugs and exploits in production.
- Developer Productivity : Shortens audit cycles and enables teams to focus on core logic instead of security minutiae.

Monetization Strategy

- Subscription Plans : Free tier for basic analysis and pro tiers with advanced features, team collaboration, reporting.
- Enterprise Licensing : Secure, private deployments for companies and blockchain projects.
- Audit-as-a-Service : Offer expert, paid audits powered by our AI tooling.
- Marketplace Integrations : Embed auditing features into developer marketplaces or IDEs.

THANK YOU

LET'S MAKE SMART CONTRACT SECURITY SMARTER.

EMAIL :

istaprasad.patra@gmail.com

#RAISEYOURHACK | #QUBIC | #BYTESHIFT