FATHOMS OF FUTURE

kurukshetra 2025™

The Battle of Brains

An International Techno - Management Fest

K! HACKS 2.0

ONLINE SUBMISSION

TEAM NAME: Tech Aspirants

COLLEGE: SRM Madurai College For Engineering And Technology

PROBLEM STATEMENT: Block Chain And Cyber Security

PROBLEM STATEMENT

K! HACKS 2.0

With the rise of block chain technology and its widespread adoption across industries, the security of decentralized networks, smart contracts, and decentralized applications (dApps) has become a pressing concern. Block chain's decentralized and immutable nature ensures a high level of security, but it is not immune to vulnerabilities, exploits, and attacks. Blockchain-based systems, such as decentralized finance (DEFI) applications and smart contracts, are frequently targeted by malicious actors.]

Common attack vectors include:

- The need for an automated, scalable, and efficient solution to continuously audit block chain systems for security threats and compliance has never been more critical.
- Smart contract vulnerabilities (e.g., reentrancy attacks, integer overflows, and improper access control).

SOLUTION

K! HACKS 2.0

Use python tools and libraries such as Py-Solc, Web3.py, and mythril to scan smart contracts for common vulnerabilities.

The solution will:

- Perform static analysis to detect known vulnerabilities such as reentrancy, overflow, and underflow
- Implement dynamic analysis by simulating smart contract execution to identify issues during runtime.
- Integrate with popular blockchain platforms like Ethereum, Binance Smart Chain, and others for smart contract analysis.

SOLUTION

K! HACKS 2.0

Technologies:

Web3.py for interacting with blockchain networks.Py-Solc for compiling Solidity contracts and checking for errors.Mythril for analyzing Ethereum smart contracts to detect security vulnerabilities.Slither for static analysis and security audits of Solidity code.Benefit: This automated scanning ensures that vulnerabilities are detected and fixed before smart contracts are deployed, reducing the risk of exploitation.

TECHNICAL REQUIREMENTS

K! HACKS 2.0

Automated block chain-based cybersecurity auditing tools play a crucial role in enhancing security and ensuring compliance with standards. Here are a few key technical requirements for these tools:

- **Smart Contract Analysis and Auditing**
- **Distributed Ledger Inspection**
- **Access Control and Permission Management**
- **Anomaly Detection and Threat Intelligence Integration**
- **Data Privacy and Confidentiality Checks**
- **Automated Compliance and Regulatory Reporting**
- **Scalability and Performance Optimization**
- **Integration with Blockchain Oracles**
- **Interoperability Across Multiple Blockchains**
- **Automated Risk Assessment and Vulnerability Scanning**

TARGET MARKET

K! HACKS 2.0

The target market for automated block chain-based cybersecurity auditing tools is diverse and spans several industries that are leveraging blockchain technology. Below are the key segments that would benefit from these tools:

- **Block chain Development and Smart Contract Teams**
- **Financial Institutions and DEFI Projects**
- **Enterprise Block chain Implementations**
- **Regulatory Authorities and Compliance Firms**
- **Block chain Service Providers (BAAS)**
- **Cryptocurrency and Digital Asset Investors**
- **Security and Penetration Testing Firms**
- **Legal and Forensic Experts**
- **Block chain Start ups and Entrepreneurs**
- **Academia and Research Institutions**

BUSINESS MODEL

K! HACKS 2.0

The business model for automated blockchain-based cybersecurity auditing tools can vary depending on the specific market segment, target audience, and value proposition. Below are some common business model approaches for these tools:

1.Subscription-Based Model
2. Pay-Per-Audit Model
3. Licensing Model
4. API or SaaS-Based Model
5. Consulting & Professional Services Model
6.Performance-Based Model
7. Education & Certification Model

TEAM DETAILS

K! HACKS 2.0

ROLE	NAME	STREAM/DEPT	YEAR	COLLEGE
Project Manager	Anandharaj G	**B Tech IT**	**2024 - 2025**	**SRM MCET**
Strategist	Keerthi Shivani M	**B Tech IT**	**2024 - 2025**	**SRM MCET**
Technical Architect	Manikandan K	**BE CSE (CS)**	**2024 - 2025**	**SRM MCET**
Presentation Specialist	Aditya A	**BE CSE (CS)**	**2024 - 2025**	**SRM MCET**