Smart Contract Auditing Companies

This document presents an in-depth overview of top-tier smart contract auditing companies in the blockchain ecosystem. Each profile includes core company information, service offerings, audit methodologies, tooling, client ecosystems, and contact details.

It aims to help founders, developers, and protocol operators choose the right security partner for their needs.
By comparing technical depth, methodology, and client experience, this guide provides clarity on leading audit providers.

By comparing technical depth, methodology, and client experience, this guide provides clarity on leading audit providers.

The landscape of blockchain security is rapidly evolving, making informed choices more critical than ever.
With billions of dollars at stake, selecting a reputable auditing partner can be the difference between project success and catastrophic loss.
This guide highlights not only technical expertise but also the unique strengths and specialties of each firm.
Readers will also gain insight into the latest trends in auditing methodologies and post-deployment monitoring.

---

1. CertiK

🏢 Company Overview

- **Founded:** December 2017 by professors from Yale University and Columbia University
- **Headquarters**: New York, NY, USA
- **Mission:** Secure the Web3 world by leveraging formal verification and AI-driven technology
- **Vision:** To become the default standard for blockchain security and enable mission-critical applications to scale safely and correctly
- **Positioning:** Industry leader in blockchain security, having audited over 4,800 projects and secured more than $530 billion in digital assets
- **Team Size:** 201-500 employees
- **Notable Investors:** Insight Partners, Sequoia, Tiger Global, Coatue Management, Lightspeed, Advent International, SoftBank, Hillhouse Capital, Goldman Sachs, Coinbase Ventures, Binance, and others

🛡️ Core Services

- **Smart Contract Auditing:** Combines manual code review, AI-powered static analysis, and formal verification to identify vulnerabilities

- **Security Consulting:** Advises on protocol architecture, governance risk, and secure design principles
- **Post-Audit Monitoring:** Skynet - a real-time risk engine for continuous surveillance and anomaly detection
- **Penetration Testing:** Simulated attacks on blockchain protocols, exchanges, wallets, and dApps
- **Bug Bounty Platform:** CertiKShield enables community-driven vulnerability reporting and rewards
- **Compliance & AML Services:** Assists projects with regulatory compliance and anti-money laundering frameworks

📊 Auditing Methodology

- **Hybrid Approach:** AI-enhanced automated tools combined with expert manual review
- **Tools:** Proprietary CertiK engine, Slither, Manticore, DeepSEA formal verification tools
- **Severity Levels:** Critical, Major, Medium, Minor, Informational
- **Patch Validation:** Reviews and validates fixes via GitHub before deployment

🎯 Roles and Responsibilities

- **Comprehensive Code Review**: Manual and AI-enhanced logic checks
- **Vulnerability Detection**: Detect exploits like reentrancy, logic flaws, and overflows
- **Formal Verification**: Mathematical validation of smart contract behavior

- **Security Consulting**: Guidance on secure protocol architecture and governance
- **Reporting & Remediation**: Actionable audit reports and remediation suggestions
- **Patch Validation**: Review fixes before deployment
- **Post-Audit Monitoring**: Automated surveillance via Skynet
- **Incident Response**: 24/7 monitoring and alerting of suspicious activity

🔐 Security Philosophy

- Emphasizes formal verification over trust assumptions to mathematically guarantee security properties
- Utilizes AI-enhanced behavioral anomaly detection for proactive risk management

📜 Sample Audit Reports

- PancakeSwap, ShibaSwap, Aave, dYdX, and many more available on CertiK's website

🌍 Clients & Ecosystem

- Major clients include Binance, Polygon, OKX, Terra, ApeCoin DAO, Multichain, Solana, and Binance Smart Chain projects

⚙️ Tooling & Infrastructure

- CertiK Skynet for real-time monitoring
- DeepSEA for formal verification
- CertiKShield bug bounty platform

📦 How to Request an Audit

- Website: certik.com
- Intake form: https://www.certik.com/request-audit

📚 Learning & Community

• YouTube, Blog, Exploits Library

📞 Contact Info

- Email: contact@certik.org
- Telegram: @certikorg

2. OpenZeppelin

🏢 Company Overview

- **Founded:** 2015
- **Mission:** Build secure, open-source infrastructure and tools for Ethereum and blockchain developers
- **Vision:** Empower builders with security-first tools and best practices to create reliable decentralized applications
- **Positioning:** Core contributor to Ethereum ecosystem; trusted by projects securing over $50 billion in assets
- **Team**: Distributed globally across North America, Europe, Asia, Latin America, and Oceania

🛡️ Core Services

- **Smart Contract Auditing:** Deep manual code reviews with expertise in Ethereum Virtual Machine (EVM) internals
- **Security Consulting:** Threat modeling, secure protocol design, and architecture reviews
- **Post-Audit Monitoring:** OpenZeppelin Defender platform providing relayers, sentinels, and automation tools to monitor and manage deployed contracts

- **Open-Source Libraries:** Industry-standard, audited Solidity contract libraries widely used for secure smart contract development

📊 Auditing Methodology

- **Manual-First Approach:** In-depth manual code review complemented by automated tools such as Slither, MythX, Echidna, and custom scripts
- **Formal Specifications:** Applied especially to upgradeable contracts and token standards to ensure correctness and security
- **Focus Areas:** Modular audits of upgradeable and standard contracts, with emphasis on EVM-specific vulnerabilities and best practices

🎯 Roles and Responsibilities

- **Comprehensive Code Review:** Modular audit of upgradable and standard contracts
- **Vulnerability Detection**: Deep scan for EVM-specific vulnerabilities
- **Formal Verification**: Applied to upgradeable proxies and token standards
- **Security Consulting**: In-depth threat modeling and architecture review
- **Reporting & Remediation**: GitHub-based feedback loop with clients
- **Patch Validation**: Secure fix validation by lead auditors
- **Post-Audit Monitoring**: Defender's Sentinel and Admin automation tools

- **Incident Response**: Direct consulting on post-deployment incidents

🔐 Security Philosophy

Emphasizes open-source transparency as a foundation for trust and security

Advocates for the Checks-Effects-Interactions pattern and modular, reusable contract design to minimize vulnerabilities

📜 Sample Audit Reports

Notable audits include Aave, Uniswap V3, and Compound

Reports and insights available at: [OpenZeppelin Security Audits]

🌍 Clients & Ecosystem

Trusted by leading organizations including the Ethereum Foundation, Arbitrum, Optimism, and Base (Coinbase)

Integral part of the Ethereum and Layer 2 ecosystems

⚙️ Tooling & Infrastructure

- **OpenZeppelin Contracts:** Widely used audited Solidity libraries for tokens, governance, and security patterns
- **OpenZeppelin Defender:** Security operations platform for monitoring, automation, and incident response
- **OpenZeppelin Wizard**: Tool to help developers generate secure smart contract templates

📦 How to Request an Audit

GitHub or the contact form on [openzeppelin.com]

📚 Learning & Community

- Active community forum, detailed blog posts, and comprehensive tutorials
- Contributors to Ethereum Request for Comments (ERC) standards and open-source security practices

📞 Contact Info

- **General inquiries:** contact@openzeppelin.com
- **Security issues:** security@openzeppelin.com

🔹 3. ConsenSys Diligence

🏢 Company Overview

- **Founded:** Part of ConsenSys (founded by Joseph Lubin, Ethereum co-founder)
- **Mission:** Strengthen Ethereum ecosystem via expert audits
- **Vision:** Formal security practices for decentralized systems
- **Positioning:** Ethereum-native auditors

🛡️ Core Services

- **Smart Contract Auditing:** Threat modeling, manual + symbolic analysis
- **Security Consulting:** Secure protocol workflows, multi-sig setup

📊 Audit Methodology

- Tools: Scribble, MythX, Diligence Fuzzing
- Focused on formal specs + logic correctness

🎯 Roles and Responsibilities

- **Comprehensive Code Review:** Manual + symbolic analysis of contract logic
- **Vulnerability Detection:** MEV, oracle, overflow bugs, and logic issues
- **Formal Verification:** With Scribble for behavior spec validation
- **Security Consulting:** Secure workflow, safe deployment design
- **Reporting & Remediation:** Detailed findings with remediation paths
- **Patch Validation:** Secondary verification cycles
- **Post-Audit Monitoring:** Optional fuzzing integrations
- **Incident Response:** Support during contract failure/exploit cases

🔐 Security Philosophy

- Developer-first security integration
- Push toward verifiable correctness

📜 Sample Audit Reports

- MakerDAO, Metamask, 1inch
- https://consensys.net/diligence/audits/

🌍 Clients & Ecosystem

- Ethereum mainnet protocols, L2s, DAOs

⚙️ Tooling & Infrastructure

- MythX, Scribble, Harvey

📦 How to Request an Audit

- https://consensys.net/diligence/audit-request

📚 Learning & Community

- Diligence Blog, Solidity Friday newsletters

📞 Contact Info

- audits@consensys.net

🔹 4. Trail of Bits

🏢 Company Overview

- **Founded:** 2012
- **Mission:** Secure mission-critical software (Web3, defense, enterprise)
- **Vision:** Blend formal methods with battle-tested security engineering
- **Positioning:** Elite security firm trusted by top DeFi protocols

🛡️ Core Services

- **Smart Contract Auditing:** Manual & symbolic execution + fuzzing
- **Security Consulting:** Secure compiler/toolchain design

📊 Audit Methodology

- Tools: Slither (they built it), Manticore, Echidna
- Advanced formal analysis + test generators

🎯 Roles and Responsibilities

- **Comprehensive Code Review:** Low-level audits, compiler checks
- **Vulnerability Detection:** Formal logic violations, state machine errors
- **Formal Verification:** With Slither, Echidna, and Manticore
- **Security Consulting:** Compiler/hardhat integrations and CI tooling
- **Reporting & Remediation:** Academic-grade reports and fixes
- **Patch Validation:** Regression test generators
- **Post-Audit Monitoring:** Optional support extensions
- **Incident Response:** Advanced exploit analysis during live attacks

🔐 Security Philosophy

- White-box by default
- Attack simulation focus

📜 Sample Audit Reports

- Compound, Balancer, Element Finance
- https://github.com/trailofbits/publications

🌍 Clients & Ecosystem

- Ethereum Foundation, OpenSea, Coinbase

⚙️ Tooling & Infrastructure

- Slither, Echidna, Manticore (open source)

📦 How to Request an Audit

- trailofbits.com

📚 Learning & Community

- GitHub, blog, whitepapers

📞 Contact Info

- info@trailofbits.com

🔹 5. Hacken

🏢 Company Overview

- **Founded:** 2017, Ukraine-based
- **Mission:** Web3 cybersecurity ecosystem
- **Vision:** End-to-end security infrastructure for DeFi, exchanges
- **Positioning:** Full-stack security (audit + bug bounty + KYC)

🛡️ Core Services

- **Smart Contract Auditing:** Manual + automated + test-driven
- **Security Consulting:** Exchange security, blockchain protocol audits
- **Post-Audit Monitoring:** Real-time threat detection, AML, bug bounty

📊 Audit Methodology

- OWASP-based risk classification
- Slither, Foundry, Hardhat testing

- Tools: HackenProof platform

🎯 Roles and Responsibilities

- **Comprehensive Code Review:** Both traditional and blockchain-native flaws
- **Vulnerability Detection:** Includes AML and exchange-specific checks
- **Formal Verification:** Selectively applied to critical protocols
- **Security Consulting:** KYC, bug bounty, and DeFi risk modeling
- **Reporting & Remediation:** OWASP-aligned reporting with patching guidance
- **Patch Validation:** Manual follow-up audit
- **Post-Audit Monitoring:** HackenProof and bug bounty sync
- **Incident Response:** Emergency coordination for breaches

🔐 Security Philosophy

- Proactive security lifecycle
- Bug bounty + public transparency

📜 Sample Audit Reports

- VeChain, Solana, 1inch, Avalanche projects

🌍 Clients & Ecosystem

- KuCoin, 1inch, Gate.io, MEXC

⚙️ Tooling & Infrastructure

- HackenProof, AML integrations

📦 How to Request an Audit

- hacken.io/security-audit

📚 Learning & Community

- Hacken Twitter, Blog, Proof of Hack reports

📞 Contact Info

- audit@hacken.io
- Telegram: @hacken_io

🔹 6. QuillAudits

🏢 Company Overview

- **Founded:** 2018, India-based
- **Mission:** Secure multi-chain Web3 ecosystems through scalable audits
- **Vision:** Democratize Web3 security across chains
- **Positioning:** Audited 1400+ projects across 20+ blockchains

🛡️ Core Services

- **Smart Contract Auditing:** Manual + static analysis, fuzzing, symbolic testing
- **Security Consulting:** Threat modeling, DAO governance

📊 Audit Methodology

- Multi-tool stack: Slither, MythX, Echidna
- Automated + manual hybrid audits

🎯 Roles and Responsibilities

- **Comprehensive Code Review:** Human-led inspection supported by static tools
- **Vulnerability Detection:** Covers over 20 blockchain ecosystems
- **Formal Verification:** Symbolic testing and fuzzing routines
- **Security Consulting:** DAO risk modeling and governance design
- **Reporting & Remediation:** Custom report + issue dashboard
- **Patch Validation:** Git-based fix evaluation
- **Post-Audit Monitoring:** QuillMonitor and alerting tools
- **Incident Response:** Telegram/Slack-based response team

🔐 Security Philosophy

- Emphasizes human review + chain-specific attack vectors

📜 Sample Audit Reports

- Polygon, Avalanche, Near ecosystem
- https://audits.quillhash.com/

🌍 Clients & Ecosystem

- Klaytn, XDC, Persistence, NFT marketplaces

⚙️ Tooling & Infrastructure

- QuillMonitor, fuzz testing framework

📦 How to Request an Audit

- https://audits.quillhash.com/#get-started

📚 Learning & Community

- Security blog, chain-specific insights

📞 Contact Info

- audits@quillhash.com
- Telegram: @quillhash

🔹 7. Hashlock

🏢 Company Overview

- **Founded:** 2021, Australia-based
- **Mission:** Deliver community-aligned, high-quality audits
- **Vision:** Promote safer dApp ecosystems through manual-first analysis
- **Positioning:** Trusted by leading DAOs and early-stage protocols

🛡️ Core Services

- **Smart Contract Auditing:** Manual line-by-line code inspection
- **Security Consulting:** Upgrade safety, modularization reviews

📊 Audit Methodology

- Manual-first with hardhat tests
- Clear audit logs + remediation checklist

🎯 Roles and Responsibilities

- **Comprehensive Code Review:** Manual-first review with test harness
- **Vulnerability Detection:** Thorough business logic validation
- **Formal Verification:** Not primary but included if requested

- **Security Consulting:** Modular dApp design & upgrade risk assessment
- **Reporting & Remediation:** Line-by-line audit logs
- **Patch Validation:** Follow-up re-audit with checklist
- **Post-Audit Monitoring:** Limited; referrals for external tools
- **Incident Response:** Early-stage mitigation advice

🔐 Security Philosophy

- Human-led deep dive, frequent re-audits

📜 Sample Audit Reports

- Frax DAO, Olympus Pro

🌍 Clients & Ecosystem

- Synthetix, Beanstalk, Velodrome

⚙️ Tooling & Infrastructure

- In-house static checker, custom simulators

📦 How to Request an Audit

- https://hashlock.com.au

📚 Learning & Community

- Blog, case studies, GitHub open reports

📞 Contact Info

- hello@hashlock.com.au

🔹 8. Cyfrin

🏢 Company Overview

- **Founded:** 2022
- **Mission:** Train and deploy the next generation of security experts
- **Vision:** Build the most developer-centric auditing company in Web3
- **Positioning:** Known for technical community presence and Foundry-native audits

🛡️ Core Services

- **Smart Contract Auditing:** Specialized in Solidity and Vyper audits
- **Security Education:** Web3 security bootcamps

📊 Audit Methodology

- Foundry-based testing stack, fuzzing, hardhat integration
- Community-driven bug discovery

🎯 Roles and Responsibilities

- **Comprehensive Code Review:** Foundry-native structured audits
- **Vulnerability Detection:** Includes fuzzing and invariant testing
- **Formal Verification:** Research-driven review where needed
- **Security Consulting:** Community-led mentoring and tooling feedback

- **Reporting & Remediation:** CLI-driven audit pipelines and docs
- **Patch Validation:** Integrated with CI/CD tooling
- **Post-Audit Monitoring:** Optional developer-side testing
- **Incident Response:** Discord-based incident escalation

🔐 Security Philosophy

- Community-first, education-focused

📜 Sample Audit Reports

- Chainlink, zkSync, Solmate

🌍 Clients & Ecosystem

- LayerZero, Scroll, StarkNet tools

⚙️ Tooling & Infrastructure

- SpeedRun audits, Audit Foundry

📦 How to Request an Audit

- https://cyfrin.io/contact

📚 Learning & Community

- YouTube, bootcamp repos, Discord

📞 Contact Info

- security@cyfrin.io

🔹 9. Spearbit

🏢 Company Overview

- **Founded:** 2021
- **Mission:** Connect world-class security researchers with high-value protocols
- **Vision:** Build a marketplace of top-tier audit talent
- **Positioning:** Audit DAO infrastructure; screened auditor network

🛡️ Core Services

- **Smart Contract Auditing:** Custom team-based audits
- **Security Consulting:** Protocol upgrade management, attack simulations

📊 Audit Methodology

- Researcher team formation + scope alignment
- Severity classification: Critical to Informational

🎯 Roles and Responsibilities

- **Comprehensive Code Review:** Multi-auditor scoped reviews
- **Vulnerability Detection:** Parallel validation by distributed researchers
- **Formal Verification:** Applied where protocol logic demands it

- **Security Consulting:** DAO upgrade safety, ecosystem coordination
- **Reporting & Remediation:** Collaborative remediation and audit chats
- **Patch Validation:** Managed re-review and certification
- **Post-Audit Monitoring:** Long-term audit DAO involvement
- **Incident Response:** Researcher-driven deep dives on active issues

🔐 Security Philosophy

- Research-first, distributed audits

📓 Sample Audit Reports

- Arbitrum DAO, NounsDAO

🌎 Clients & Ecosystem

- DAOs, L2s, Rollups

⚙️ Tooling & Infrastructure

- Audit coordination dashboards

📦 How to Request an Audit

- https://spearbit.com

📚 Learning & Community

- Twitter Spaces, open workshops

📞 Contact Info

- info@spearbit.com

🔹 10. SlowMist

🏢 Company Overview

- **Founded:** 2018, China-based
- **Mission:** Provide comprehensive blockchain security solutions
- **Vision:** Become the trusted global brand in blockchain security
- **Positioning:** Renowned in Asia for proactive attack-defense strategies and AML integrations

🛡️ Core Services

- **Smart Contract Auditing:** Manual vulnerability identification
- **Security Consulting:** Risk evaluation, best practice design
- **Post-Audit Monitoring:** Threat intelligence and AML compliance

📊 Audit Methodology

• Manual-first approach using proprietary static analysis tools
• OWASP and CVE-mapped classification
• Comprehensive simulation of attack vectors

🎯 Roles and Responsibilities

- **Comprehensive Code Review**: Rigorous manual audits
- **Vulnerability Detection**: Identifying both traditional and blockchain-specific risks
- **Formal Verification**: Mathematical validation when applicable
- **Security Consulting**: Targeted DeFi defense modeling
- **Reporting & Remediation**: Clear reporting and patch assistance
- **Patch Validation**: Confirm post-audit fixes

- **Post-Audit Monitoring**: Integrates AML and blacklist scanning
- **Incident Response**: Rapid forensic analysis during active exploits

🔐 Security Philosophy

- Attack simulation-led process
- Emphasis on cross-platform interoperability risks

📜 Sample Audit Reports

- EOS, VeChain, IOST
- https://slowmist.medium.com

🌍 Clients & Ecosystem

- Binance, OKEx, Huobi, Crypto.com

⚙️ Tooling & Infrastructure

- SlowMist Hacked database, AML solutions

📦 How to Request an Audit

- https://slowmist.com/en/contact.html

📚 Learning & Community

- Blog, research papers, WeChat channels

📞 Contact Info

- Email: contact@slowmist.com

🔹 11. Zellic

🏢 Company Overview

- **Founded:** 2021
- **Mission:** Bring cryptographic and protocol-level rigor to blockchain auditing
- **Vision:** Pioneer high-assurance audits for cutting-edge Web3 systems
- **Positioning:** Security research firm specializing in deep blockchain internals

🛡️ Core Services

- **Smart Contract Auditing:** Focused on cross-chain and zero-knowledge systems
- **Security Consulting:** Protocol architecture, cryptographic primitives

📊 Audit Methodology

• Research-driven reverse engineering
• Heavy use of fuzzing, mutation, and adversarial testing

🎯 Roles and Responsibilities

- **Comprehensive Code Review**: Emphasis on cryptographic correctness
- **Vulnerability Detection**: Research-grade deep bug discovery
- **Formal Verification**: If needed for protocol-level assurance
- **Security Consulting**: Cryptography + protocol-level modeling
- **Reporting & Remediation**: Research-style documentation and remediation planning

- **Patch Validation**: Highly targeted regression testing
- **Post-Audit Monitoring**: Optional R&D follow-ups
- **Incident Response**: Advanced exploit detection advisory

🔐 Security Philosophy

- Cryptography-first; assume all inputs are adversarial

📜 Sample Audit Reports

- LayerZero, Aptos, Mysten Labs

🌍 Clients & Ecosystem

- Aptos Labs, SushiSwap, Mysten, Wormhole

⚙️ Tooling & Infrastructure

- In-house fuzzing infrastructure

📦 How to Request an Audit

- https://zellic.io/contact

📚 Learning & Community

- Research publications, talks, technical blog

📞 Contact Info

- Email: hello@zellic.io

🔹 12. PeckShield

🏢 Company Overview

- **Founded:** 2018
- **Mission:** Defend the decentralized economy through security intelligence and audits
- **Vision:** Provide both reactive and proactive Web3 security
- **Positioning:** Major BSC and Ethereum auditor with DeFi-specific threat visibility

🛡️ Core Services

- **Smart Contract Auditing:** Manual and static/dynamic tools
- **Security Intelligence:** Real-time exploit monitoring (PeckShield Alert)
- **Post-Audit Monitoring:** Transaction threat alerts and blacklist tracking

📊 Audit Methodology

• Combines on-chain analysis and offline review
• Strong coverage of MEV, arbitrage, oracle, and flashloan attacks

🎯 Roles and Responsibilities

- **Comprehensive Code Review**: Logic flaw and system-level checks
- **Vulnerability Detection**: Specialized DeFi exploit scanning
- **Formal Verification**: In selected high-value protocols
- **Security Consulting**: Oracle risks, MEV, arbitrage protections
- **Reporting & Remediation**: Bilingual audit reports + remediation sessions

- **Patch Validation**: Issue re-verification
- **Post-Audit Monitoring**: PeckShield Alert bot monitoring
- **Incident Response**: Frontline incident updates & responses

🔐 Security Philosophy

- Blend auditing with real-time analytics
- Fast-response culture for on-chain attacks

📜 Sample Audit Reports

- Curve Finance, Euler, Tornado Cash

🌍 Clients & Ecosystem

- Binance, Tornado Cash, Curve, Sushi, Lido

⚙️ Tooling & Infrastructure

- PeckShield Alert, MEV scanner, Fork explorer

📦 How to Request an Audit

- https://peckshield.com/contact.html

📚 Learning & Community

- Twitter @peckshield, Medium blog

📞 Contact Info

- Email: info@peckshield.com

🔹 13. Quantstamp

🏢 Company Overview

- **Founded**: 2017
- **Mission**: Secure the future of smart contracts by building advanced security tools and protocols.
- **Vision**: A world where blockchain technology is trusted by all.
- **Positioning**: Leading blockchain security company dedicated to securing and auditing smart contracts. Canvas TemplatesCanvas Templates+1smartcontractaudits.com+1

🛡️ Core Services

- Smart Contract Auditing
- Security Monitoring
- Insurance Products Canvas Templates+4PitchBook+4Quantstamp: Securing the Future of Web3+4

📊 Audit Methodology

- Combines manual audits with automated security tools.
- Focuses on enhancing the safety and reliability of decentralized applications. TechData VC+1CompWorth+1PitchBook

🎯 Roles and Responsibilities

- Comprehensive code review for vulnerabilities.
- Security analysis and monitoring.
- Providing detailed audit reports and remediation guidance.The Cryptonomist+3TechData VC+3Hashlock+3

🔐 Security Philosophy

- Building trust in blockchain technology through rigorous security practices.Canvas Templates

📜 Sample Audit Reports

- Ethereum 2.0 clients: Prysm and Teku. Quantstamp: Securing the Future of Web3

🌍 Clients & Ecosystem

- Ethereum Foundation, Prysmatic Labs, ConsenSys.

⚙️ Tooling & Infrastructure

- Quantstamp Protocol
- Automated Security ToolsCompWorth+1TechData VC+1

📦 How to Request an Audit

- https://quantstamp.com/

📚 Learning & Community

- Twitter: @Quantstamp
- Blog: https://quantstamp.com/blog

📞 Contact Info

- Email: info@quantstamp.com

🔹 14. ChainSecurity

🏢 Company Overview

- **Founded**: 2017
- **Mission**: Enhance blockchain security through advanced smart contract audits.
- **Vision**: Provide reliable security solutions for decentralized applications.
- **Positioning**: Trusted by leading Web3 projects, central banks, and international corporations. docs.usdfi.com+8PitchBook+8smartcontractaudits.com+8Smart Contract Audits by ChainSecurity

🛡️ Core Services

- Smart Contract Auditing
- Security Analysis
- Formal VerificationCoinPedia Pro+6Hacken+6Coinweb+6

📊 Audit Methodology

- Utilizes tools like Securify for static analysis.
- Combines automated and manual review processes. Smart Contract Audits by ChainSecurity+1docs.usdfi.com+1

🎯 Roles and Responsibilities

- Identify and mitigate security vulnerabilities in smart contracts.
- Provide comprehensive audit reports with recommendations.

🔐 Security Philosophy

- Academic rigor combined with practical security solutions.

📜 Sample Audit Reports

- Various Ethereum-based projects and DeFi protocols.CB Insights+4web3index.com+4F6S+4

🌍 Clients & Ecosystem

- Ethereum Foundation, DeFi projects, central banks.Smart Contract Audits by ChainSecurity+3ornedo.com+3Quantstamp: Securing the Future of Web3+3

⚙️ Tooling & Infrastructure

- Securify
- Chaincode ScannerSmart Contract Audits by ChainSecurity+2smartcontractaudits.com+2docs.usdfi.com+2

📦 How to Request an Audit

- https://www.chainsecurity.com/

📚 Learning & Community

- Blog: https://www.chainsecurity.com/blog/Smart Contract Audits by ChainSecurity

📞 Contact Info

- Email: info@chainsecurity.com

why are so many hacks still happening?

1. Complexity of Code

Smart contracts aren't just simple scripts. They often handle intricate financial logic, interact with multiple protocols, and execute a series of automated transactions.

2. Unforeseen Attack Vectors

- Attackers develop new strategies, exploit novel techniques, and discover vulnerabilities that weren't even considered when an audit was performed.
- Auditors work with known vulnerabilities and best practices at the time of the audit, but if a new type of attack emerges later, the contract might still be at risk

3. Limitation of Auditing Tools

- While automated analysis tools like Slither, Mythril, and Echidna are essential for detecting common vulnerabilities (e.g., reentrancy, integer overflows, access control issues), they aren't a silver bullet.
- Many smart contract exploits involve logic bugs, complex multi-contract interactions, or dependencies that scanners struggle to analyze.

4 .Human Error

- Security audits rely on skilled professionals, but even the best experts can make mistakes.

- Complexity of Systems: Multi-chain protocols, cross-bridge interactions, and upgradeable contracts introduce layers of complexity

5. Dependency on External Systems

- Smart contracts rarely operate in isolation, they interact with oracles, third-party services, and cross-chain bridges**.**
- Hackers exploit weak points in APIs, wallets and external systems**.**
- A strong security approach is essential. Smart contract audits must combine strict access rules, private key protection and real-time monitoring to defend against all risks.
- Audits primarily focus on *on-chain code vulnerabilities* (e.g., reentrancy, integer overflows), but many modern hacks exploit off-chain weaknesses .