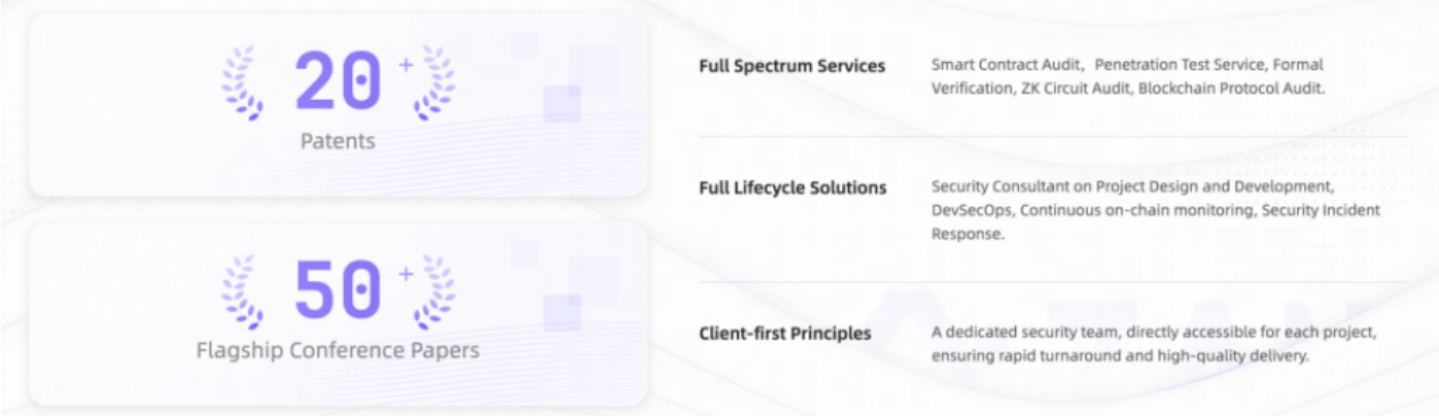
ZAN Expert Audit: Helping Web3 Projects Achieve Smart Contract Security from Development to Deployment



Hangzhou, Zhejiang Jul 13, 2026 (Issuewire.com) - A decentralized finance protocol is preparing for its highly anticipated mainnet launch. Developers are finalizing the core codebase, and liquidity providers have committed initial capital. Hours after deployment, an undetected reentrancy vulnerability allows external actors to drain the primary liquidity pool, turning a milestone launch into an immediate financial recovery operation. Smart contracts are immutable once deployed—vulnerabilities can lead to irreversible fund losses. This makes smart contract auditing a critical safeguard for Web3 projects to launch securely. ZAN—the Web3 technology brand under Ant Digital Technologies—offers professional smart contract auditing services covering penetration testing, AI auditing, static analysis, and formal verification, designed to identify structural risks and logical flaws throughout the entire development lifecycle, guiding projects from initial architecture design through mainnet deployment and ongoing operations.

Web3 Security Auditing: From Post-Development Code Review to Full-Lifecycle Security

Traditional Web3 security approaches typically treat auditing as a final checklist item before deployment. However, post-development code reviews frequently overlook fundamental architectural flaws that are difficult or costly to change later in the software development lifecycle. When security assessments are limited to completed smart contracts, systemic risks embedded during the design phase can persist into production, becoming the root cause of DeFi security incidents.

ZAN Expert Audit's contract auditing service provides financial-grade compliance assurance. The team holds 20 security patents and 50 top-tier security conference papers, backed by deep security research expertise.

Design Phase: Security consultants engage with development teams during initial architecture planning, providing security advisory services. This early intervention helps identify potential logical flaws and economic model risks, ensuring the protocol's structural foundation aligns with industry security best practices.

Development Phase: Continuous security is maintained through integrated DevSecOps toolchains and expert manual auditing. Automated testing tools scan the codebase upon code commits, instantly

detecting common contract vulnerabilities and standard attack vectors, helping developers quickly fix basic defects. Building on this foundation, the ZAN security expert team conducts deep manual code review, examining business logic and access controls line by line to identify complex logical vulnerabilities, economic model risks, and governance attack vectors that automated tools cannot easily cover, ensuring contracts meet security baseline requirements before entering the deployment process.

Post-Deployment Phase: Security requirements do not terminate at mainnet launch. When a project encounters a security attack incident, the ZAN security expert team can provide incident response services, rapidly analyzing attack vectors, assessing the scope of vulnerability impact, and assisting project teams in formulating emergency remediation plans and asset protection strategies, minimizing losses caused by security incidents.

Deployment Phase: ZAN provides end-to-end support from auditing to deployment. Audited contracts can be securely deployed to target chains via ZAN's 28+ chain RPC services (including Ethereum RPC, Solana RPC, Polygon RPC, Base RPC, BSC RPC, Arbitrum RPC, etc.), and enterprise customers can also choose Dedicated Node Service for exclusive node resources. All RPC endpoints provide sub-30ms response times and 99.9% SLA guarantees.

Dual-Engine Model: Professional Services and Automated Platform

Different stages of project growth and code complexity require different security assessment methodologies. ZAN Expert Audit operates through a dual-engine model, balancing customized human analysis with rapid automated screening.

The Professional Service track provides one-on-one engagement with dedicated security researchers, covering manual code review, penetration testing, formal verification, and ZK circuit auditing, focused on discovering complex logical vulnerabilities, economic manipulation vectors, and governance risks that automated scanners typically cannot detect. The Express Service leverages a SaaS-based automated platform for rapid evaluation of standard smart contracts, detecting security vulnerabilities, coding standards, compiler errors, gas optimizations, and logical issues, generating risk assessment reports within minutes to hours, supporting rapid iteration in agile development environments.

Structured Audit Process and Transparent Delivery

Effective security collaboration relies on clear operational methodology and reliable communication channels. ZAN Expert Audit follows a customer-first principle—each project can directly engage with a dedicated security team, ensuring rapid feedback and high-quality delivery. Security experts remain accountable throughout the evaluation process, ensuring technical queries receive precise responses and code remediation efforts receive consistent review.

Initial Audit Round: Comprehensive automated scanning, manual code review, and penetration testing are conducted, yielding a preliminary audit report and communicating findings.

Final Report Delivery: A detailed public or private audit report is published, outlining verified code status, remaining risk mitigation measures, and overall architectural security assessment. ZAN supports public audit report publication, enhancing a project's security transparency within the Web3 community.

Web3 Security: Smart Contract Auditing as the Foundation of Ecosystem Trust

In the Web3 environment, smart contract security auditing is a core requirement for establishing

ecosystem credibility. Through systematic audit services, decentralized applications build verified security baselines that facilitate regulatory compliance, build user confidence, and meet institutional capital requirements during due diligence. For more information, visit https://zan.top/home/expert-audit.

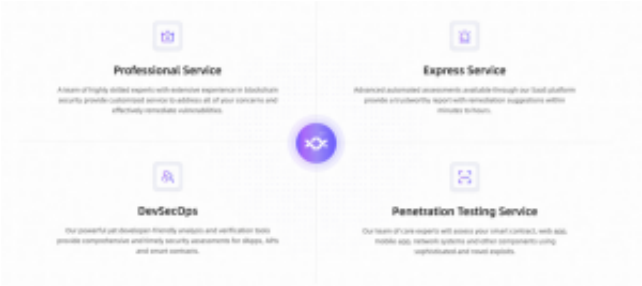
FAQ

Q: Which blockchains does ZAN's smart contract auditing support?

A: ZAN Expert Audit supports smart contract auditing on all major chains, including EVM chains such as Ethereum (Solidity/Vyper), BSC, Polygon, Arbitrum, Optimism, Base, zkSync Era, and Starknet, as well as non-EVM chains including Solana (Rust/Anchor), Sui, and Aptos (Move). After audit approval, contracts can be securely deployed via ZAN's 28+ chain RPC services and Dedicated Nodes. ZAN also offers complementary services including ZK Acceleration, Solana Trading Boost, and ZAN Identity.

Q: What is the audit timeline for ZAN Expert Audit?

A: Professional services typically complete within 1–4 weeks (depending on project scope), covering automated scanning, manual code review, penetration testing, and multiple rounds of remediation verification. Express Service, based on the SaaS platform, can generate risk assessment reports within minutes to hours.



Media Contact

ZAN

*********@zan.top

http://zan.top

Source : ZAN

See on IssueWire