How can blockchain technology build trust and secure confidence?

EY Blockchain Analyzer: Smart Contract and Token Review

EY
Building a better
working world

The better the question. The better the answer. The better the world works.

FAQs

EY Blockchain Analyzer: Smart Contract and Token Review (SC&TR) is a solution that aims to enhance confidence in blockchain-enabled transactions. By reviewing the underlining code of smart contracts, SC&TR helps identify common security vulnerabilities, validate the alignment of the code with business logic and improve code efficiency and quality.

What is a smart contract?

A smart contract is a self-executing computer program that automatically enforces the terms of an agreement between parties. It operates without the need for intermediaries and is built on blockchain technology, making it secure and transparent. Smart contracts can be used in a wide range of applications from financial transactions to supply chain management.

Why should smart contracts be reviewed?

Smart contracts must be reviewed to mitigate the risks of errors, vulnerabilities, and other issues that could compromise their security and functionality. By identifying potential risks and opportunities to improve the code, reviews help reduce the risks of costly mistakes, fraud and hacking attempts. Such reviews can help stakeholders assess that the smart contract operates as it has been designed, which is crucial for applications that involve sensitive data or high-value transactions.

What is Smart Contract and Token Review?

The SC&TR solution gives organizations the confidence to deploy and interact with smart contracts. It helps users to run hundreds of industry standard and custom testing scenarios, with detailed results around the purpose and logic of each test. Test results help users understand flaws and inconsistencies in the smart contract.

What type of blockchain do you support?

At EY, we believe that public blockchains are the only viable long-term option. We focus on the Ethereum Blockchain.

How does the Smart Contract and Token Review solution work?

When you submit your code, it is scanned, compiled with the relevant solidity compiler version, and sent through our testing engine. The testing engine uses static code analysis through both the source code and the solidity AST, and a customized Ethereum Virtual Machine (EVM) dynamically simulates various testing scenarios.

Who should use the Smart Contract and Token Review?

The solution is primarily used by EY client-serving professionals. It can also be used directly by the clients and any person or enterprise wanting to assess a smart contract (subject to EY's client acceptance process, as applicable). We also see interest from tech-savvy specialists, developers, auditors, compliance and risk teams.

Which security tests do you support?

The solution covers common security vulnerabilities such as underflow or overflow, unsafe changes to smart contract state, use of deprecated or unsafe keywords, short addresses and more. We continually update our list of security tests as we progress research and development. Within every engagement, automated reviews are complemented with manual expert reviews to ensure full coverage of the code.

What is functionality testing?

Our research and experience reveal that most smart contract exploits occur through unexpected behavior of the smart contract and manipulation of edge cases. Functionality testing aims to reduce that risk by verifying that a smart contract behaves as expected. The tool aims to test functionality by both reviewing the required syntax and simulating various scenarios that are part of the ERC-20 standard core functionality.

When should I use the Smart Contract and Token Review tool?

The SC&TR solution offers most benefits when used prior to deployment, as part of the development process or to validate code before deploying a contract to the Mainnet. Once deployed, a smart contract is immutable, meaning that, in most cases, bugs and vulnerabilities cannot be fixed.

Why are EY team's positioned so well to support the clients with smart contract reviews?

EY teams core business is to provide trust and confidence to business ecosystems. We do that in the assurance business but also across our consulting business. We have robust methodologies and standards in place to deliver the highest quality services to help stakeholders gain more trust in the technology they are using.

Continuing the conversation

If you would like to learn more about EY Blockchain Analyzer: Smart Contract and Token Review solution and how it can help your organization, please contact the team below.

Avner Geifman
Partner, SCR Solution Lead
avner.geifman@il.ey.com

Aminadav Glickshtein
Manager, Digital & Emerging Technologies, Blockchain Expert
aminadav.glickshtein@il.ey.com