

Smart Contract Security: a Practitioners' Perspective

Codebook of Interviews

Name	Description
Blockchain Platforms	
CITA	
EOS	
Ethereum	
Hyperchain	
Hyperledger Fabric	
WASM	
Experience with Smart Contract Development	Experience in Years
P1 - Experience	
P10 - Experience	
P11 - Experience	
P12 - Experience	
P13 - Experience	
P2 - Experience	
P3 - Experience	
P4 - Experience	
P5 - Experience	

Name	Description
P6 - Experience	
P7 - Experience	
P8 - Experience	
P9 - Experience	
Experience with Software Development	Experience in Years
P1 - Experience	
P10 - Experience	
P11 - Experience	
P12 - Experience	
P13 - Experience	
P2 - Experience	
P3 - Experience	
P4 - Experience	
P5 - Experience	
P6 - Experience	
P7 - Experience	
P8 - Experience	
P9 - Experience	
Smart Contract Development - Adoption Factors of Security Tools	The factors that affect the adoption of security tools
The tool covers a wide range of security issues.	

Name	Description
The tool does not cost much money.	
The tool generates understandable reports.	
The tool is actively maintained.	
The tool is easy to use.	
The tool is extensible.	
The tool is highly automated.	
The tool produces low false negatives.	
The tool produces low false positives.	
The tool runs fast.	
The tool supports multiple languages.	
Smart Contract Development - Competing Priorities	
Avoiding Bugs	
Costing Less Gas	
Easy to Use	
Protecting Privacy	
Securing against Malicious Attacks	
Supporting Features	
Smart Contract Development - Job Responsibility	
Design	

Name	Description
Management	
Programming	
Testing	
Smart Contract Development - Life Cycle Model	
Agile	
Iterative	
Waterfall	
Smart Contract Development - Programming Languages	
C++	
Go	
Java	
JavaScript	
LLL	
Mutan	
Serpent	
Solidity	
Vyper	
Smart Contract Development - Security Deterrents	The factors that deter practitioners from devoting efforts to security
Available security tools for smart contracts are not useful.	

Name	Description
In my team, it is more important to deliver features on time than to address smart contract security.	
It is easy to mitigate the negative impact of a security breach.	
It is unlikely that our smart contract will be attacked.	
My company does not have a formal process for smart contract security.	
My team does not have the budget to address smart contract security.	
Smart contract security is a burden on top of my main responsibilities.	
Smart contract security is not my responsibility.	
The smart contracts I develop are not prone to security attacks.	
Smart Contract Development - Security Knowledge Sources	Sources where practitioners acquire security knowledge
Blockchain Security Companies	
OpenZeppelin	
Quantstamp	
Latest News	
Vulnerability News	
Official Forums of Blockchain Platforms	
Ethereum Official Website	

Name	Description
Question and Answer Websites	
Reddit	
Stack Overflow	
Research Papers	
Smart Contract Development - Security Motivators	The factors that motivate practitioners to address security
Customers would lose money in case of a security breach.	
I care about my users' experience in security and privacy.	
I see software security as my responsibility.	
It is challenging to detect and trace attacks on smart contracts deployed to blockchains.	
My company is audited for smart contract security by an external entity.	
My company mandates security practices in smart contract development.	
My company would lose customers in case of a security breach.	
Security breaches would hurt my company's reputation.	
Software security is a shared responsibility by all those involved in the development lifecycle.	
Software security is in my company's culture.	

Name	Description
The deployed smart contracts are immutable.	
Smart Contract Development - Security Strategies	
Code Reuse from Reliable Sources	
Code Review	
Code Style Checking	
External Auditing	
Formal Verification	
Fuzzing	
Runtime Monitoring	
Security Testing	
Static Analysis	
Threat Assessment	
Vulnerability Scan	
Smart Contract Development - Security Tools	
Formal Verification	
Boogie	
Fuzzer	
Echidna	
ILF	
Mythril	
Oyente	

Name	Description
Reverse Engineering	
Security plugin in IDE	
Remix	
Slither	
SmartCheck	
Smart Contract Development - Stages	
Construction	
Deployment	
Design	
Maintenance	
Requirement	
Testing	
Smart Contract Security Issues	
Delegatecall Injection	
DoS	
Exception Disorder	
Integer Overflow and Underflow	
Memory Leak	
Reentrancy	
Transaction Ordering Dependence	
Upgradable Contract	