Ethereum

- 10-Minute Ethereum Orientation
- Ethereum in 30 minutes by Vitalik Buterin
- What happens when you send 1 DAI

Solidity

Language

- Solidity Documentation
- Solidity Cheatsheet
- All About Solidity
- Data Representation in Solidity
- Solidity Inline Assembly & Yul
- Data Representation in Solidity

Frameworks

- HardHat
- Foundry
    - How to Foundry with Brock Elmore
    - How to Foundry 2.0: Brock Elmore
    - How to test a smart contract function a million times
    - Solidity Coverage in VS Code with Foundry

Libraries

- OpenZeppelin Contracts

Best Practices

- Ethereum Smart Contract Security Best Practices
- Building Secure Smart Contracts by Crytic
- Nascent's Simple Security Toolkit
- Solidity DevSecOps Standard
- Secure Smart Contract Design Principles

EVM

- The EVM Handbook
- Ethereum in 30 minutes
- LearnEVM by 0xMacro
- EVM Deep Dives [Part 1] [Part 2] [Part 3] [Part 4] [Part 5] [Part 6]
- EVM: From Solidity to byte code, memory and storage
- Openzeppelin's Deconstructing a Solidity Contract Articles [Part 1] [Part 2] [Part 3] [Part 4] [Part 5] [Part 6]
- evm.codes
- Ethervm

Smart Contract Vulnerabilities

General

- Chapter 9 of Mastering Ethereum - smart-contracts-security
- Smart Contract Weakness Classification and Test Cases
- Smart Contract Security Verification Standard (SCSVS)
- Smart Contract Vulnerabilities
- Smart contract attack vectors
- SCV-List
- Secureum blog
    - Smart Contract Security 101
    - Security Pitfalls & Best Practices 101
    - Security Pitfalls & Best Practices 201
    - Audit Findings 101
    - Audit Findings 201
    - Audit Techniques & Tools 101

- Smart Contract Security
- SmartContracts-audit-checklist
- Web3 Security: Attack Types and Lessons Learned
- Ethereum Smart Contract Auditor's 2022 Rewind
- Blockchain Hacking Techniques of 2022 | Top 10
- Smart Contract Security in Solidity

Reentrancy

- A Historical Collection of Reentrancy Attacks
- Reentrancy Attacks on Smart Contracts Distilled
- Cross-Contract Reentrancy Attack
- Decoding $220K Read-only Reentrancy Exploit
- Cross-chain re-entrancy

DOS

- Uncovering Real-Life Examples of Denial of Service Attacks on Smart Contracts

Price Manipulation

- awesome-oracle-manipulation

Signature Malleability

- Signature Malleability PoC

Smart Contract Audit

- How to become a smart contract auditor by cmicel
- How to become Smart Contract Auditor and Bounty Hunter by officercia

Threat Modelling

- Threat Modelling for Smart Contracts: Best Step-by-Step Guide
- Threat Modelling Cheat Sheet
- Uniswap v4 - threat modeling for secure integration

Auditing Process

- The Auditing Process by Owen
- Video: Complete Smart Contract Auditing System by Owen
- The Audit Process by obront.eth
- Smart Contract Audit Methodology by Hacken
- Smart Contract Auditing Methodology Mind Map by QuillAudits
- Smart Contract Audit Methodology & Tips By DeFiHackLabs
- Smart Contract Auditing Heuristics
- Mindsets of Auditing by @BowTiedDravee
- Smart Contract Audit Methodology
- Becoming a web 3 security researcher - Balancing foundations and the attacker mindset

Auditing Tools

- Slither
    - Slitherin
    - Slither printers and modules
- Echidna
    - Fuzzing Workshop
- Solidity Visual Developer
- Signature Database
- codeslaw: search for verified smart contracts
- Solodit.xyz
- Query Storage Slot
- Bytegraph - smart contract analysis
- Bytecode Decompilation
- Pyrometer - bound analysis
- contract-diff.xyz
- Evm.storage
- Smart Contract VulnDB
- How to diff contracts against Etherscan verified code
- https://gptscan.github.io/

Fuzzing

- Solidity-fuzzing-boilerplate
- Invariant fuzzing testing

CTFs

- Damn Vulnerable DeFi
- Mr Steal Yo Crypto
- CTFProtocol
- Ethernaut
- Blocksec-ctfs

- CTF Blockchain Challenges
- Ghosts of epochs past
- QuillCTF
- Smart-contract-challenges from Morpho Labs
- OnlyPwner
- Secureum race

Domain Specific

Standards

- ERC-20: Token Standard
- ERC-721: Non-Fungible Token Standard
- ERC-1155: Multi Token Standard
- ERC-4626: Tokenized Vaults
- EIP-712: Typed structured data hashing and signing

Proxies

- yAcademy Proxies Research
- Check upgrade history
- Diamond Pattern
- Louper - The Ethereum Diamond Inspector

ERC20

- The Dangers of Token Integration
- Weird ERC20 Tokens
- Token Interaction Checklist
- ERC20 Misbehaviors

NFT

- Auditing Tips for NFT Projects
- NFT Best Practices - build safe

ERC1155

- Security Analysis of the ERC 1155 NFT Smart Contract

ERC4337

- A deep dive into the main components of ERC-4337: Account Abstraction Using Alt Mempool — [Part 1] [Part 2]
- ERC-4337 & Account Abstraction: A Comprehensive Overview
- Account Abstraction's Impact on Security and User Experience
- You Could Have Invented Account Abstraction
- Account Abstraction. Auditor’s View
- Security Audit Checklist for Account Abstraction Wallets

ERC4626

- Overview of the Inflation Attack
- Exploring ERC-4626: A Security Primer
- A Novel Defense Against ERC4626 Inflation Attacks
- Shared Vulnerabilities Between ERC-4626 Vaults and Vault-Like Contracts [P1] [P2] [P3]

DeFi

- Defi Mooc
- SoK: Decentralized Finance (DeFi)
- SoK: Decentralized Finance (DeFi) Attacks
- Uniswap V3 Development Book
- Programming DeFi: Uniswap V2 [Part 1] [Part 2] [Part 3] [Part 4]
- Defi Threat
- DeFi Security Summit 2022
- Security Pitfalls when Building with DeFi Money Legos
- Lending/Borrowing DeFi Attacks
- How its made: Euler v2
- Vulnerable Spots of Lending Protocols

AMM

- Typical vulnerabilities in AMM protocols

Uniswap V4

- Threats for UniswapV4 hooks

Staking

- Guidelines for Auditing Staking Protocols
- The staking algorithm of Sushiswap MasterChef and Synthetix

Oracle

- SoK: Oracles from the Ground Truth to Market Manipulation [paper] [video]
- How To Consume Chainlink Price Feeds Safely
- Chainlink Data Feeds, Security Researcher's Perspective
- 10 Security Pitfalls w/ integrating price oracles

Dao

- DAO Voting Vulnerabilities

Bridge

- SoK: Not Quite Water Under the Bridge: Review of Cross-Chain Bridge Hacks
- Setting Up A Bridge With Foundry
- A Visual Guide to Blockchain Bridge Security
- Crosschain Risk Framework

- Bridge Bug Tracker
- Cross-Chain Security with LayerZero Labs

Multichain

- Observations and tips for auditing protocols on multiple chains

L2

- Mental models for L1 and L2
- SoK: Validating Bridges as a Scaling Solution for Blockchains
- L2-security-framework

Layer Zero

- Secure integration with LayerZero
- LZ Checklist

Cryptography

- Ethereum Cryptography Basics
- Web3 Exploits | Signature Malleability
- Ethereum signatures for hackers and auditors 101
- ECDSA signature vulnerabilities

Merkle Tree

- Securely building and verifying Merkle Trees with Solidity and Javascript

PoC

- Proof of Concept (PoC) Guidelines and Rules
- How To Use Foundry To PoC Bug Leads [Part1] [Part2]
- DefiHackLabs
- Immunefi PoC Templates

Post-mortem

- rekt news
- Retrospective: Hacks in Web3
- Defillama Hacks Dashboard
- REKT Database

Audit Reports

- Blockchain Security Audit List
- code4rena
- Spearbit Public Portfolio
- Solodit.xyz
- How To Read Smart Contract Audit Reports

- https://ventral.digital/posts/2022/12/15/ethereum-smart-contract-auditors-2022-rewind/
- https://ventral.digital/posts/2024/1/19/ethereum-smart-contract-auditors-2023-rewind/

Writing Reports

- Tips from Trust

Newsletters & Blogs

- ventral.digital blog
- Blockchain Threat Intelligence
- Security Pills Newsletter
- Secureum
- Week in Ethereum News
- DeFiHackLabs's Substack

Awesome web3 security

- Introduction to smart contract security and hacking in Ethereum
- QuillAudit's SmartContract Auditor Roadmap
- AuditorsRoadmap
- Awesome-web3-Security
- Immunefi's Web3 Security Library
- DeFiHackLabs's web3 security collections
- How to Learn Web3 Security
- Smart contract auditor resource bank
- Web3 Project Security Practice Requirements
- Smart Contract Security: A Simple Checklist for Web3 Development
- matta.'s Ethereum security road-map

Things to tell your clients

- tincho's advice to be friends with your auditors
- Auditors: what do you ask developers?
- How to Prepare for a Smart Contract Audit
- The Rekt Test

Cairo

Starknet

- https://www.starknet.io/
- https://book.starknet.io/

Language study

- Moving from Solidity to Cairo

- Cairo Lang
- WTF Cairo
- Cairo Book

Example

- Cairo Example
- Openzeppelin

Security

- StarknetCC-CTF
- Starknet security challenges
- Damn vulnerable defi

Solana

Learning Maps:

sannykim/solsec: A collection of resources to study Solana smart contract security, auditing, and exploits.
https://learnblockchain.cn/maps/Solana

Docs

https://solana.com/zh/docs

Solana Secure Roaming Guide

A Hitchhiker's Guide to Solana Program Security

Learning Advice

https://x.com/0xcastle_chain/status/1851939543164813646

Courses:

Solana 的 60 天 - RareSkills

Developer Courses | Solana

https://solana.com/zh/developers/courses/program-security/security-intro#overview

Vulnerabilities and prevention

coral-xyz/sealevel-attacks: ☠️ Common Security Exploits and Protections on Solana

X 上的 Armani Ferrante 🎒：“Some more tips for developing secure programs on Solana.” / X

CTF

neodyme-labs/solana-ctf: A collection of Solana CTF challenges

Development Tutorials:
https://soldev.cn/topics/88