Zero Knowledge Mastery

1. Introduction

- An approximate introduction to how zk-SNARKs are possible
- zk-SNARK Concepts Explained Like You're 15
- Computer Scientist Explains One Concept in 5 Levels of Difficulty | WIRED
- How To Create a ZK Smart Contract
- What Is Zero-knowledge Proof and How Does It Impact Blockchain?
- Introduction to Zero Knowledge Proofs
- What to know about Zero Knowledge
- A beginner's intro to coding zero-knowledge proofs
- ZKPs for Engineers: Introduction
- Zero Knowledge Proofs: An Illustrated Primer by Matthew Green
- Understanding ZKPs Through Illustrated Examples
- Vitalik Buterin
  - Part 1: Proofs with Polynomials
  - Part 2: Thank Goodness It's FRI-day
  - Part 3: Into the Weeds

2. Mathematical Knowledge

- ZK Primer
- Polynomials 101
- Mathematics for ZK
- Quadratic Arithmetic Programs: from Zero to Hero
- Introduction to Mathematical Cryptography
- A Graduate Course in Applied Cryptography
- Modern Computer Algebra
- Algebraic Number Theory
- Computational Introduction to Number Theory and Algebra
- Lattice Cryptography

3. Courses

- Zero Knowledge Proofs MOOC Videos
- ZKP WhiteBoard Sessions
- ZK Learning
- Zero Knowledge Canon
- ZK Battleship sCrypt
- ZKP WhiteBoard SessionsZKP WhiteBoard Sessions
- Getting Started with zkSnarks on ZoKrates

4. Programming Languages

- Programming Languages in ZKP
- Cario
- Circom
- Noir
- Snarky
- Zinc
- ZoKrates
- Leo
- Juxiv
- zkVM
- ZKPDL
- Lurk

5. Libraries

- Libsnark
- Bulletproofs
- gnark
- Bellman
- libSTARK
- jellyfish
- Arkworks
- Circomlib
- DIZK
- plonky
- Spartan
- wasmsnark
- libiop
- Nova
- SnarkyJS
- DIZK

6. Layer1 and Layer2

- Layer 1
  - Iron Fish
  - Mir Protocol
  - Aleo
  - Lelantus
  - Mina
  - Neptune
  - Espresso Systems
  - DarkFi
  - Zeeka Network
  - Quark
  - Celo
- Layer 2
  - Aztec
  - StarkNet
  - ZEXE on Plasma
  - zkSync
  - Scroll
  - Twilight
  - Polygon Zero
  - Polygon Miden
  - Taikocha
  - Radius
  - Orbis
  - Nightfall

7. Puzzles

- Let's Hash It Out
- Sudoku
- Battleship
- Incomplete Information Games on Bitcoin
- Dark Forest
- Zordle
- Lottery
- zkAutoChess
- GoL2
- Cachebox
- Exgrasia
- Crypto Maze

8. Books

- Proofs, Arguments, and Zero-Knowledge
- A Graduate Course in Applied Cryptography
- The MoonMath Manual to zk-SNARKs

9. Papers

- Why and How zk-SNARK Works
- zk research
- A simplified polynomial protocol for lookup tables
- Dandelion: Redesigning the Bitcoin Network for Anonymity

10. Application and Use Cases

- Checks and balances: Machine learning and zero-knowledge proofs
- ZK Machine Learning: truly private machine learning, with zk-SNARKs and blockchain
- Reinventing Vulnerability Disclosure using Zero-knowledge Proofs
- Zero Knowledge Proof and its Applications in Bitcoin
- Zcash: Privacy-Protecting Digital Currency
- Awesome Privacy on Blockchains
- A Flexible Network Approach to Privacy of Blockchain Transactions
- Quisquis: A New Design for Anonymous Cryptocurrencies
- Pinocchio: Nearly Practical Verifiable Computation
- Waku: a suite of privacy-preserving, peer-to-peer messaging protocols
- StealthDrop: Anonymous Airdrops using ZK proofs
- zk-NftMint: Mint an NFT if you know a secret
- Loopring zkRollup Exchange
- zk-SQL: Self-sovereign SQL queries
- Hyper Oracle: Programmable zkOracle network
- Foundation's Proof Market
- Integrating Zerocash on Ethereum

11. Opensource Projects

- ZK EVM
- Starknet
- ZK Sync
- Light Protocol on Solana
- Tornado Cash
- ZKaggle
- ZKPhoto

12. Tools

- ZK Toolkit
- hello-noir: Hardhat x Foundry Template

13. Tweets

- I spent the past week reading hundreds of resources
- Solidity devs do you want to get into ZK but don't know where to start?
- ZK Fundamentals: What is proof aggregation, recursion, and composition?
- Explain ZK Proofs to someone new to web3
- Simplifying zkEVM for a 10year old
- ZK rollup categorization
- About zk
- Here are the best released (and unreleased) ZK projects to keep your eye on
- ZK setup process
- A question on ZK circuit development
- ConsenSys zkEVM is such a giant leap forward for the Ethereum ecosystem, and here's why...
- zk rollups

14. Communities

- ZK Hack : Discord Server
- Zero-knowledge podcast
- ZK Tech : Reddit
- 0xPARC : Supporting the next generation of cryptography-enabled applications.
- ZKProof : Open-Industry academic initiative

15. Writeups

- Hickup's ZK Journey
- Zero Knowledge Database : Notion
- Zero Knowledge Blog

16. Security

- Circom-Pairing: A Million-Dollar ZK Bug Caught Early
- ZK privacy landscape > Zero-knowledge privacy-enhancing solutions
- DeFi security Summit 2023 - Session 12: Vulnerabilities & Exploits - Dmitry Khovratovich
- Security Firms
  - Quill Audits
  - Diligence
  - Trail of Bits
  - ZK Labs
  - Least Authority
  - ABDK
  - Kudelski Security
  - Hashcloak
  - Taurus
  - Common Prefix