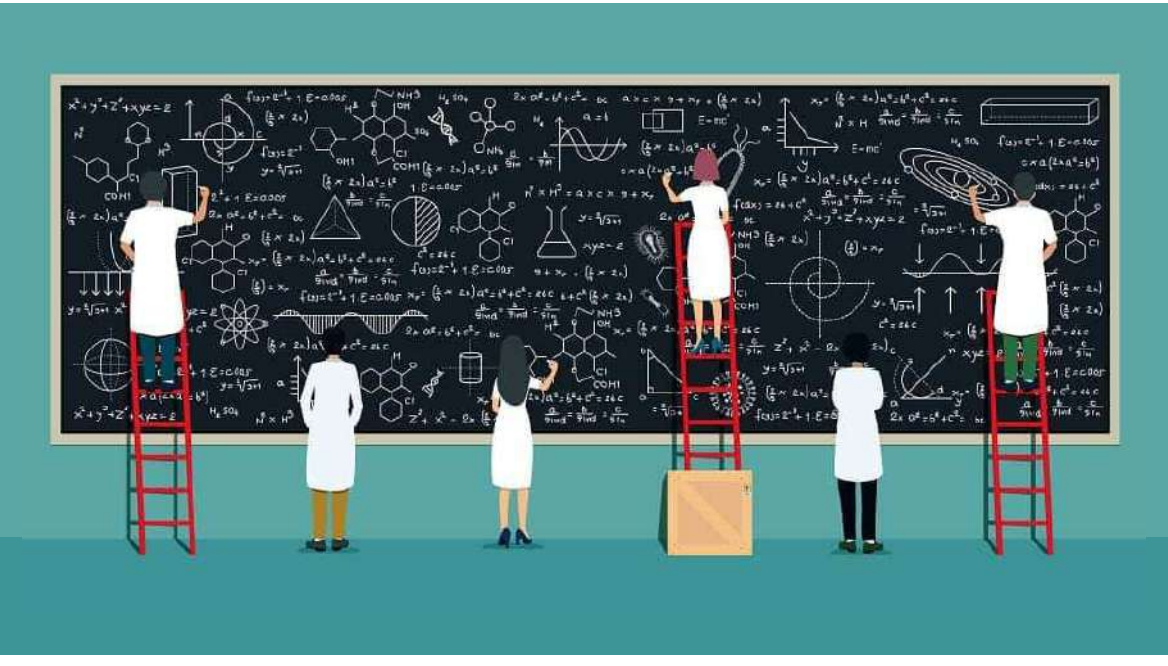
CRYPTOCURRENCY WORKBOOK 2026

For use in training courses and contest challenges



CRYPTOCURRENCY VILLAGE CHALLENGE

CRYPTOCURRENCY WORKBOOK 2026

For use in training courses and contest challenges

CRYPTOCURRENCY ADVOCATE

Cryptocurrency Workbook
by Michael Schloh von Bennewitz
Version 2026-1.0, licensed CC BY-SA 4.0

Published by Cryptocurrency Advocate, 30 N Gould St., Sheridan, WY 82801

For an electronic copy of the Cryptocurrency Workbook,
please visit https://www.cryptocurrencyvillage.cc/docs/

979-5-360-31275-7

Table of Contents

Preface

The Cryptocurrency Workbook is edited each year for up to date references to technology driven activities taken by the Cryptocurrency Advocate, the group responsible for the informative and educational content performed at events.

Purpose

This workbook was created with the intention of distribution at events where the Cryptocurrency Advocate appears and presents the content seen here. After completion, the literature serves as a historical review of cryptocurrency developments at DEFCON and other events where we appear.

Mission

The Cryptocurrency Advocate is a group working to prepare society for the likely adoption of modern cryptocurrency in legacy financial systems. We host a number of events, including the Cryptocurrency Village and Cryptocurrency Cyber Challenge at the DEFCON hacker convention in Las Vegas.

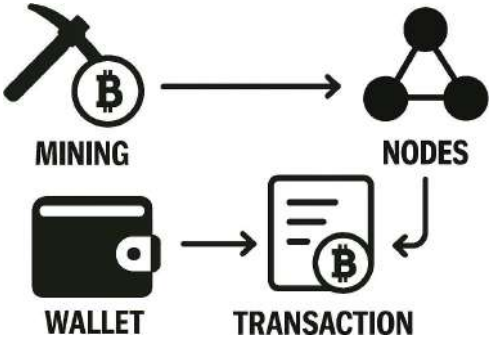
We also host events at other DEFCON appearances in Bahrain and Singapore.

Contact

Talk to a real human by sending email (info@cryptoadvocate.cc) or direct messages (https://discord.gg/8APBmBWKuk) in our Discord server.

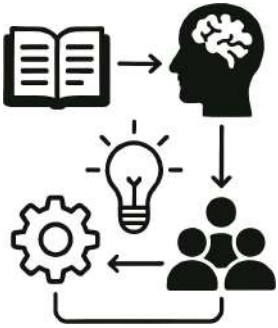
Examples

Code examples, exercises, and other supplemental material may be available for download. Please ask your instructor. If you have a technical question or a problem using the examples, please contact us with details.


MINING
NODES
WALLET
TRANSACTION

CHAPTER 1

Introduction



The Cryptocurrency Advocate supports your exploration of modern finance technology by hosting workshops and distributions at Defcon, the world largest hacker convention. A recent addition to the Defcon contest lineup is the bodacious:

CRYPTOCURRENCY CYBER CHALLENGE

...where teams of cryptohackers compete to win prizes by undertaking offensive and defensive security practices. If you've wondered how a POS, ATM, hardware wallet, or secure element really work, then come to the Cryptocurrency areas at Defcon to gain new perspectives of finance technology. The Cryptocurrency Village's educational offering covers more than just blockchain based technology. Visitors are encouraged to exchange ideas relating to any finance hacking practice for the common good. We distribute items relating to several classic projects including Litecoin, Monero, Bitcoin, Ethereum, and others. Show your cryptohacker style with high quality wearables, custom hacker badges, and simple addons. Try new devices, devkits, and electronics, with on site presence of manufacturers and staff mentors. Inform yourself of new developments in finance by exploring the Cryptocurrency areas at Defcon, your one stop shop for fintech hacker goods and information. Since Defcon 26 (2017) we have served a family and child friendly environment. A stable and balanced group, the Cryptocurrency Advocate especially thanks all the underage hackers for your regular visits to our convention areas.

CHAPTER 2

Workshops

Participation in this workshop is voluntary and at your own risk. The content, materials, and discussions provided during the workshop are for informational and educational purposes only. Nothing said, presented, or distributed in this workshop should be construed as legal advice or as establishing an attorney-client relationship. Participants are encouraged to consult with a qualified legal professional for advice specific to their individual circumstances.

The Cryptocurrency Village and its representatives, including but not limited to workshop facilitators, speakers, and staff, shall not be held liable for any direct, indirect, incidental, consequential, or special damages arising from or related to your participation in this workshop. This includes, but is not limited to, any reliance on information provided, actions taken based on workshop content, or any errors or omissions in the materials presented.

By participating in this workshop, you acknowledge and agree to these terms and assume full responsibility for any decisions or actions you take as a result of your attendance.

To register for workshops visit **https://www.cryptocurrencyvillage.cc/learn/**

Creator Stage

In addition to a full set of interactive workshops, the brightest minds in cryptocurrency academy, industry, and community present the topics:

Cryptocurrency Opening Keynote (Las Vegas 33)
Chad Calease, Param Pithadia, and Michael Schloh von Bennewitz
Join your fellow hackers managing the Cryptocurrency areas of Defcon, and get a sneak peak of what each workshop teaches as well as an overview of the showcases and programs happening in our Defcon Community, Contest, and Vendor areas. Chad and Param will report on cryptocurrency trends and perspectives from their distinguished positions in industry and academy. We will announce the teams competing in the Cryptocurrency Cyber Challenge, and give an overview of what's available in the vending area. Meet the organizers of years of cryptocurrency content at Defcon and bring your questions to the Community Stage!

Cryptocurrency Weekend Keynote (Las Vegas 33)
Nick Percoco, Elaine Shi, and Chelsea Button
Reporting on the state of affairs in Cryptocurrency trends, Nick and Elaine give insight from their esteemed positions in industry and academy. Additionally, we get a status report of workshops, showcases, and programs in the Cryptocurrency areas of Defcon. We announce the teams competing in the Cryptocurrency Cyber Challenge, and give an overview of what's available in the vending area. Meet the organizers of years of cryptocurrency content at Defcon and bring your questions to the Community Stage!

Cryptocurrency Sunday Panel (Las Vegas 33)
Diego and special guests
In this hour we hear from experts working to secure fiat and crypto hybrid services. A likely future includes large numbers of classic finance services integrating modern technology including cryptocurrency networks. Pitfalls exist to trap groups not well familiar with unique modern challenges, not present before in fiat based classic services. We hear from a panel what security strategies exist that mitigate the typical challenges of cryptocurrency adoption.

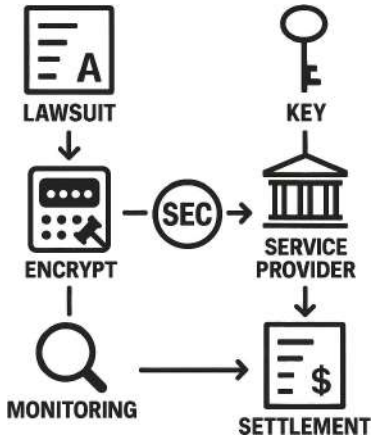
Solidity Smart Contract Attacks (EN, Singapore 1)
Kennashka DeSilva
Smart contracts power the decentralized economy, but their immutable nature makes vulnerabilities costly. In this speech presentation, listeners hear how attackers exploit Solidity smart contracts in real-world scenarios and how to emulate these attacks safely in a controlled environment.

Listeners will also learn of effective mitigations and security testing into the development lifecycle, bridging the gap between offensive insight and defensive best practices in blockchain security. By the end of this presentation, attendees will gain knowledge of vulnera-bilities, attack scenarios, and smart contract hardening methods.

Tracing Cybercriminal Financial Operations (EN, Singapore 1)
Alexander Wilczek
An investigation into cybercriminal financial operations, following the money to examine how threat actors generate, transfer, and launder illicit proceeds, including the operational security and threat modelling required to safely perform this research and which OSINT and blockchain tools and techniques to use. This presentation covers the full chain, from how cyber criminals steal or extort money to how they get to spend it. Listeners will start with OpSec, learning about operations to conduct this kind of research, the threat modelling involved and what options are available, from air-gapped laptops and Tails to Qubes OS and Vms. Since the majority of cybercrime transactions happen in crypto, we'll do a deep dive, from the basics of KYC, CEX, DEX and bridges and how they are used by criminals, then exploring in detail how chains like Monero are being leveraged and how smart contracts like Tornado Cash are used to successfully launder money. Participants will learn which techniques and tools to use to track transactions on and off chain, with a mix of OSINT, Tor and block explorer tools. We'll look at the masters of the game, the Lazarus Group, which managed to launder hundreds of millions, as well as how InfoStealers and ransomware groups go from demanding a ransom to laundering it.

Cryptocurrency Enforcement

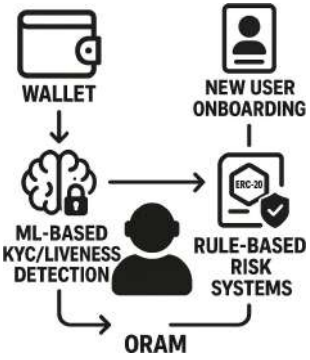
Chelsea and Joseph



Multiple agencies have attempted to regulate cryptocurrencies through various means. This workshop will begin with a short presentation about the different organizations with an interest in regulating cryptocurrency (SEC, CFTC, IRS, and DOJ) and provide examples of enforcement actions. Next, participants will break out into discussion groups to consider the pros and cons of regulation by enforcement. Then, participants will be given a hypothetical cryptocurrency and be assigned a role either as a 'regulator' or as a 'developer.' The participants will engage in a settlement type discussion to determine if the cryptocurrency should be regulated under one agency, multiple agencies, or not at all.

Red Teaming Financial Defense

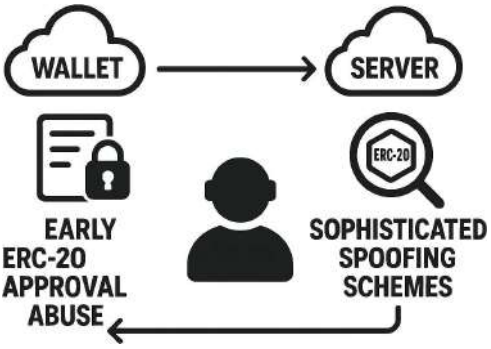
Chloe and Wei Hong



This workshop flips the script on financial security, focusing on a practical, hands-on level where attendees will learn by doing. Attendees will step into the shoes of sophisticated attackers targeting the interconnected financial ecosystem. Guided by us - Chloe, with experience in architecting B2B fraud solutions for acquiring banks in Singapore, and Weihong, with hands-on experience building ML-based KYC/liveness detection and rule-based risk systems for new user onboarding at OKX (a crypto exchange) - participants will learn how to think offensively.

Drain and Approval Attacks

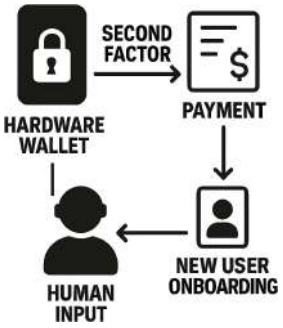
George and utvecklas



This interactive workshop explores the history and evolution of draining attacks across major blockchains such as Ethereum, Solana, and TON. Participants will witness live demonstrations of various draining techniques, from early ERC-20 approval abuse to sophisticated token spoofing. Learn to recognize, trace, and defend against these exploits while discussing popular laundering methods and current security measures. A final group challenge will involve tracking an attacker's wallet and evaluating how to recover stolen funds.

Cryptocurrency Hardware

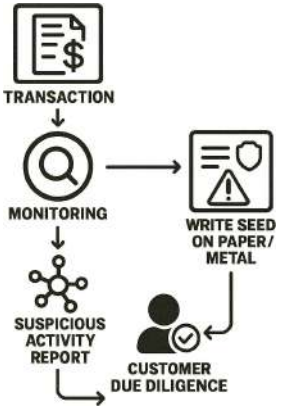
Michael and Param



Using an electronic circuit camera, we zoom in on cryptosecure devices and their circuits. Descriptions of existing cryptocurrency hardware lead to consideration of future integrations in the physical world and how secure elements work. We pass around a showcase of half a dozen wallets and similar hardware, as well as Nitrokeys (for defence) and ChipWhisperers (for attack.) We get set up with a set of hardware development software tools, and consider the physical production workflow that top manufacturers follow in high security areas.

AML Cryptocurrency Compliance

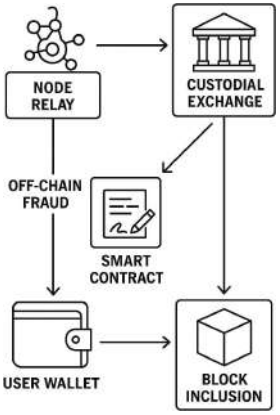
Chelsea and Joseph



Students receive exposure to the law side of cryptocurrency business, including certification, regulation, government policy, and risk assessment. Regulators around the world evaluate and implement diverse regulations governing the use and applications of Blockchain reflecting varying degrees of acceptance ranging from blanket prohibition to highly facilitating frameworks. Organisations, in turn, assess the related risks and legal challenges. This workshop considers emerging trends and security essentials vital for business and financial businesses, providing a brief overview of AML and KYC and suggestions to increase security and decrease risk exposure.

Hacking Custody and Exchanges

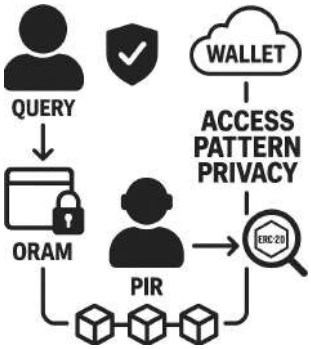
Sky Gul and Andrea



Custodial wallets and crypto exchanges are prime targets for attackers due to the high concentration of assets and complex infrastructure. This workshop explores how small implementation flaws can lead to significant vulnerabilities in these systems. Participants will walk through real-world inspired attack scenarios involving wallet infrastructure, deposit validation, and internal accounting logic. The session covers how attackers can spoof token transfers through improper event or topic filtering, exploit misconfigurations to manipulate internal transactions, and trigger vulnerabilities that result in inaccurate asset accounting. Along the way, we'll also explore defensive patterns and secure design strategies to help mitigate these issues in production environments.

Oblivious Access to Blockchains

Elaine Shi and Afonso Tinoco

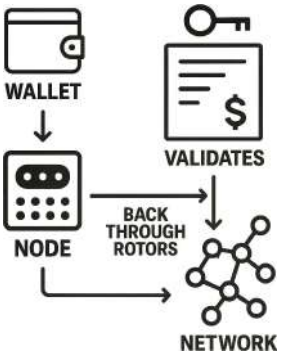


Accesses to the blockchain's state and logs leak highly sensitive information such as the user's identity, who it is trading with, and which crypto-asset the user is interested in trading. In this tutorial, we will go over two technologies for ensuring access pattern privacy, including Oblivious RAM (ORAM), and Private Information Retrieval (PIR). Unlike traditional encrypted databases that protect only the contents of data, our technologies additionally protect the queries, thus hiding users' intentions. We will describe two extremely simple constructions, one ORAM, and one PIR scheme. In particular, the ORAM algorithm is also the one used by industry leaders such as Signal and Meta. We will next show a demo for our oblivious key-value store implementation. We will also challenge the learners with a CTF problem that demonstrates how sensitive secrets can easily be leaked even when the memory contents are encrypted.

Cryptocurrency Nodes and Relays

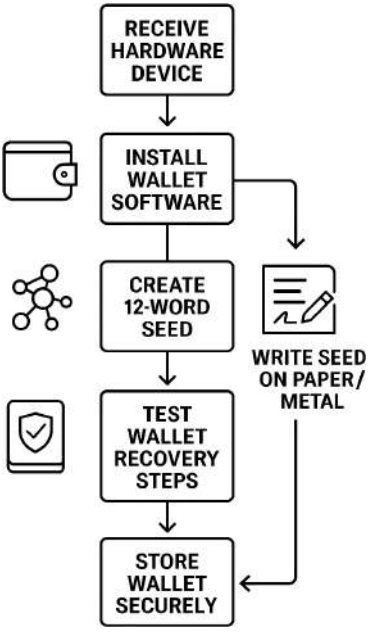
Dan and Diego

Cryptocurrency nodes validate and relay transactions across the network. Like servers in a traditional financial system, nodes store a copy of the blockchain and enforce the network's rules. Many of us want to run their own node for reasons of security, convenience, and independence of other people's node configurations. Come to understand nodes, build your own, and explore configurations to test wallet applications on your new cryptocurrency node.



Self Custodial Wallet Use

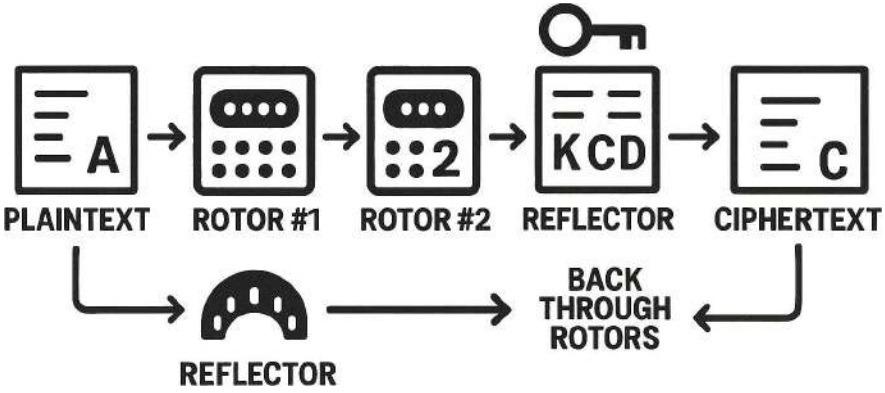
HalFinneyIsMyHomeBoy



The workshop will begin with brief presentation about cryptocurrency, exchanges, hardware wallets, hot wallets, cold wallets, and other introductory information needed to begin cryptocurrency transactions. Participants will be given a sample wallet for practice purposes only. Participants will be guided through the opening of a wallet, with a detailed discussion on public and private keys and the different types of wallets available for self custody and the different security features of wallets. The discussion will delve into hot security topics, including the importance of randomized seeds and consider a couple of case scenarios where wallets have been hacked due to a lack of security, followed by a discussion on how to prevent these types of security defects. Next, participants will create hot and a cold wallet, each with a twelve word seed. After completing set up of the cold wallet, participants will be required to simulate a lost/stolen/destroyed wallet and wipe the wallet and re-set up the wallet.

Let's Break Enigma!

Luke and Rigo



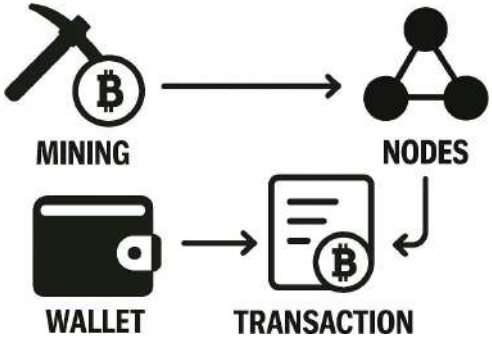
Enigma was the infamous German encryption machines that was used in World War 2. A group of British cryptographers successfully broke the sophisticated machine, and in doing so, gave rise to modern adversarial cryptography and the Turing Machine, which would later evolve into the computer. In this workshop, we will look at how adversarial cryptography initially formed and how many of the techniques used still apply today. Additionally, many of the mathematical principles used in both the construction of the Enigma machine and its subsequent breaking are used heavily in modern encryption, which directly relate to the technology used in cryptocurrency.

Financial Technologies

Michael Schloh von Bennewitz

Security experts teach you the basics of modern fintech, including:

Digital assets
Comparing coins
Stable coins
Nonfungible tokens
Smart contracts
Consensus algorithms
KYC and AML processes
Proof of work or stake
Decentralised finance
Blockchain transactions
Blockchain explorers
Public chain analysis
Cryptocurrency exchanges (custodial)
Cryptocurrency wallets (noncustodial)
Central Bank Digital Currency (CBDC)



Join your fellow hackers managing the Cryptocurrency areas of Defcon, and get a high level understanding of how cryptocurrency and other modern financial technology systems work. This workshop is meant for beginners and has no requirements, however those bringing a computer will benefit most from interactive learning. Attendees at this workshop receive a free gift.

Cryptocurrency Attacks

Michael Schloh von Bennewitz

Explore topics of offensive security with cryptocurrency experts including:

51% attacks
Cryptojacking
Merkle proofs
Proof of stake slashing
Blockchain forks
Double spend attacks
Blockchain immutability
Merkle roots in blockchain blocks
Staking security improvements
Sybil attacks
Eclipse attacks
Smart contracts
Genesis blocks
Block size limits
Front running attacks
Shamir secret sharing thresholds
Shamir secret sharing mathematics
Sybil attack mitigation
PoW prevention of double spends
Miner competitive manipulation
Layer 2 blockchain scalability
Importance of consensus block height
Smart contract reentrancy attacks
Zero confirmation transaction risks
Double spend exchange prevention
Merkle tree tamper proof root hash
Schnorr signatures superior to ECDSA
Prevention of front running attacks
Node validation of new block integrity
Dust attacks privacy compromisation
Nonce purpose in block mining
Blockchain hashing algorithms
Entropy role in key generation
Purpose of staking in blockchains
Significance of block timestamps
Transaction confirmation times
Risk of centralization in PoW
Consensus attacks to double spend
Timejacking attacks in consensus
Difficulty to prevent 51% attacks
Merkle tree security enhancement
Roles of validator nodes

Join your fellow hackers managing the Cryptocurrency areas of Defcon, and get a high level understanding of how past vulnerabilities worked to defeat flaws in cryptocurrency systems. A set of security concerns is presented with interactive group discussion about each topic. Each student receives a free of charge set of security trivia questions and answers arranged in a casino style card deck. Practice your study of cryptocurrency relevant offensive security by using the Cryptodeck as a flash card competence test, and we play a round of trivia to get warmed up with the idea of defending against the most common attacks on cryptocurrency systems. This workshop is best suited for moderately experienced hackers. If you attended the Cryptocurrency Basics workshop (one day before this workshop) then you are well prepared.

Defending Crypto Hacks

Arjun Suresh

An investigation into real-world cryptocurrency breaches, focusing on how attacks unfold, how funds move on-chain, and where detection fails. Using a Red vs Blue format, participants take on attacker and defender roles to analyze major incidents and uncover defensive gaps.

This workshop covers the full lifecycle of a crypto breach, from initial compromise to fund movement and delayed detection. Participants will begin with a brief introduction to how these attacks typically occur, then move into a Red vs Blue format where they actively investigate incidents and evaluate defensive strategies.

Participants will use tools like block explorers and basic scripting approaches to trace transactions, analyze patterns, and identify potential detection points. Through guided investigation, they will learn how to interpret on-chain activity and think like both attackers and defenders.

The workshop will examine major real-world incidents such as the Ronin Network hack and Mt. Gox collapse, highlighting how large-scale attacks unfolded and what could have been done differently. It concludes with a cross-team debrief, connecting attacker actions with defensive failures and practical lessons for improving security.

Solidity Smart Contract Attacks

Kennashka DeSilva

Smart contracts power the decentralized economy, but their immutable nature makes vulnerabilities costly. In this hands-on workshop, participants will learn how attackers exploit Solidity smart contracts in real-world scenarios and how to emulate these attacks safely in a controlled environment.

Through guided exercises, attendees will explore common vulnerabilities—including reentrancy, integer overflows, and access control flaws—while applying red teaming techniques to identify and exploit weaknesses. Participants will also learn how to design effective mitigations and incorporate security testing into the development lifecycle, bridging the gap between offensive insight and defensive best practices in blockchain security.

By the end of this workshop, attendees will gain practical skills to identify vulnerabilities, simulate realistic attack scenarios, and harden smart contracts against emerging threats.

Tracing Financial Operations

Alexander Wilczek

An investigation into cybercriminal financial operations, following the money to examine how threat actors generate, transfer, and launder illicit proceeds, including the operational security and threat modelling required to safely perform this research and which OSINT and blockchain tools and techniques to use.

This workshop covers the full chain, from how cyber criminals steal or extort money to how they get to spend it. Participants will start with OpSec, learning how to set up operations to conduct this kind of research, the threat modelling involved and what options are available, from air-gapped laptops and Tails to Qubes OS and Vms.

Since the majority of cybercrime transactions happen in crypto, we'll do a deep dive, from the basics of KYC, CEX, DEX and bridges and how they are used by criminals, then exploring in detail how chains like Monero are being leveraged and how smart contracts like Tornado Cash are used to successfully launder money.

Participants will learn which techniques and tools to use to track transactions on and off chain, with a mix of OSINT, Tor and block explorer tools. We'll look at the masters of the game, the Lazarus Group, which managed to launder hundreds of millions, as well as how InfoStealers and ransomware groups go from demanding a ransom to laundering it.

Features of the DCSG1 Badge

Arjun Suresh and Dani Weidman

The DEF CON Singapore 1 Badge is a device with several easy to use self evident features as well as some less obvious ones. The badge contains secrets, puzzles, easter eggs, and mysterious challenges as well. To learn about the various features, advanced use of base stations, and how to enjoy the badge to the maximum extent, please visit us during this interactive workshop where teams may develop to share resources while learning the basics.

We examine the physical aspects of the badge while describing various parts and how they support the rich feature set.

Bring a computer and USB cable if you want to explore the Infocomm Z-Machine simulator with I/O on the USB CDC console. The same requirement exists if you want to benefit from a quick start in examining the chip and optionally programming it.

Developing for the DCSG1 Badge

Michael Schloh and Joyce Ng

The DEF CON Singapore 1 Badge is a device powered by the Espressif ESP32-C6 MCU in a castellated module including eight megaoctets of flash storage. Developing firmware applications is rather easy with the right tools and training, so we ex plore the most common workflow used by the application design team. To begin we install the ESP-IDF toolchain and verify with a few simple examples, programming the chip and observing the outcome. A lot of alternative workflows exist, involving Visual Studio, Eclipse, Arduino, Rust, Tiny Go, Micropython, and RIOT.

We include information on FreeRTOS and the IPS display library LVGL, as well as a mo re detailed explanation of driving the parts on the printed circuit board. Bring a portable computer with a USB Type-C cable please, and optionally install the ESP-IDF software development environment as described on https://docs.espressif.com/projects/esp-idf/

Smart Contract War Room (ZH)

Antigone and Absurdity

EN: This interactive workshop places participants inside a live smart contract incident on a private test network. Working in small groups, attendees will exploit common Web3 security failures such as missing access controls, unsafe external calls, oracle assumptions, and approval misuse. After reproducing the attack, each team shifts into defense by tracing attacker activity, summarizing impact, and proposing patches. The session is designed to connect CTF-style challenge solving with practical smart contract auditing and incident response skills.

中文: 这是一场围绕私有测试网络展开的互动式智能合约攻防工作坊。参与者将以小组形式复现常 见的 Web3 安全问题，例如权限控制缺失、不安全外部调用、预言机假设错误以及授权滥 用。完成攻击路径后，学员将切换到防守视角，追踪攻击者行为、梳理影响范围，并提出修 复方案。

课程目标是把 CTF 式解题体验，与真实世界中的智能合约审计和安全响应实践连 接 起来。

Wallet Drainer Forensics (ZH)

FLY and baswvad

EN: Modern wallet drainers rarely rely on a single bug. Instead, they combine phishing pages, deceptive signing flows, stolen approvals, and fast fund movement across multiple services. In this workshop, participants analyze a simulated wallet-drainer campaign from the initial lure to the final on-chain transfers. Teams will inspect malicious front-end artifacts, decode approvals and signatures, identify attacker infrastructure, and trace the movement of funds.

The workshop emphasizes practical investigation habits for researchers, responders, and builders defending wallet users.

中文: 现代钱包盗刷攻击通常并不依赖单一漏洞，而是结合钓鱼页面、诱导签名、恶意授权以及跨 平台快速转移资金等多种手法。在本工作坊中，参与者将分析一条模拟的钱包 drainer 攻 击 链，从最初的诱导入口一直追踪到链上的最终资金流转。

学员将检查恶意前端痕迹、解> 析授 权与签名数据、识别攻击者基础设施，并追踪资金路径。课程重点是帮助研究者、应> 急响应 人员和开发者建立实用的调查与防御思维。

On-Chain Tracing Techniques

Josh

A hands-on workshop on blockchain investigation, covering transaction tracking techniques, fund flow analysis, identification of suspicious patterns, and wallet de-anonymization. We will explore tools and methodologies used in real-world cases of fraud, ransomware, and money laundering involving crypto assets—from the basics of on-chain analysis to advanced techniques such as clustering and cross-chain tracking.

CHAPTER 3

Organizers

Organizers at the Cryptocurrency Advocate plan events throughout the year.

Chelsea Button
Chelsea is a lawyer specializing in consumer finance, data and technology. She advises clients on updates in the law and defends them in litigation. She is a cryptocurrency advocate, with multiple professional publications.

Paul
Paul is a computer scientist specializing in software engineering, computer security and Bitcoin. He is an open source dev in the Bitcoin space who contributes to a variety of projects including the lightning network, payment pools, privacy, and a variety of other things.

Diego Salazar
Diego 'rehrar' Salazar has been around the FOSS and cryptocurrency communities for eight years. He owns and runs Cypher Stack, a company that performs novel research and makes contributions to various FOSS projects. He has organized and managed several villages at defcon, c3, and more.

Michael Schloh von Bennewitz
Michael Schloh von Bennewitz (MSvB) is a computer scientist specializing in embedded systems. As chairman of Monero Devices, he produces cryptosecure electronics while contributing to Opensource development communities. Michael teaches hardware security and organizes cryptocurrency groups at Defcon since 2017.

Tom
Tom is an electronic engineer and cryptocurrency enthusiast, bringing a novice perspective to help others practice good security while getting started. His interests include installation of nodes and wallets, comparisons among coins, as well as analysis of trends and the culture shift to modern finance technology.

Speakers

Experience the following expert speakers at the DEFCON Community Stage.

Nick Percoco
Nick Percoco is the Chief Security Officer at Kraken, where he spearheads the frameworks and protocols that ensure a secure and seamless trading experience for clients. An accomplished speaker and researcher, Nick has presented groundbreaking work on cryptocurrency security, targeted malware, mobile security (iOS & Android), and IoT vulnerabilities at leading global forums, including Black Hat, RSA Conference, DEFCON, CfC St. Moritz, and SXSW.

Chad Calease
Chad Calease designs for failure—on purpose. At Kraken, he hovers where crypto, resilience engineering, and human behavior collide. A systems thinker with instincts that cultivate resilience, Chad champions the Kraken value of being "Productively Paranoid"—as both a design principle and a survival trait. His work challenges us to outpace risk, interrogate ease, and own our exposures before they own us—by building with the assumption that failure isn't an if, but a when.

Sky
Sky is a holder of the OSWE, OSCE, and OSCP certifications. After gaining experience in Web2 security, he transitioned into the Web3 space and has been actively working in blockchain security for the past six years. Sky continues to work actively in the blockchain security domain, contributing to the security and resilience of decentralized technologies.

Kitboga
With more than 3M subscribers on YouTube and beyond, Kit pioneered scambaiting. "Everyday there are scammers taking advantage of people. I call them to waste their time, walk people through their *script* and lies, report info when I can, and otherwise make light of a dark situation."

Kennashka DeSilva
Kennashka DeSilva is a seasoned cybersecurity researcher with a strong track record of advancing security best practices in decentralized systems. She was a featured speaker at DEF CON 30's "Hacking & Defending Blockchain Applications" session, where she helped bridge the gap between traditional application security frameworks—such as the OWASP Top Ten—and the unique risks found in DEFI and smart contract ecosystems.

Kennashka is also an active participant in the cybersecurity community, having contributed to multiple HackMiami events and served on the executive councils of Women in Cybersecurity Florida and Black Girls in Cyber, helping to advance diversity, mentorship, and professional development in the field.

Her expertise spans vulnerability management, threat modeling, and policy-driven security in Web3 and enterprise systems. At DEFCON Singapore, she will share actionable strategies for identifying weaknesses in blockchain applications, correlating established security principles to emerging decentralized technologies, and empowering defenders to build more resilient ecosystems.

Alexander Wilczek
Alex is a digital nomad fighting cybercrime. While travelling Australia (and the world) full time for three years in a Landcruiser, Alex hacks the planet from the most pristine beaches to the most remote parts of the outback. He specialises in dark web, cybercrime and blockchain security. Alex is also the proud founder of Rivanorth.

Instructors

Our instructors bring academic and industrial experience. Meet the experts.

Elaine Shi
Elaine Shi is a Packard Fellow, Sloan Fellow, ACM Fellow, and IACR Fellow. A Professor with a joint appointment in CSD and ECE at Carnegie Mellon University, Elaine is also an Adjunct Professor of Computer Science at the University of Maryland. Her research interests include cryptography, security, mechanism design, algorithms, foundations of blockchains, and programming languages. Elain is a co-founder of Oblivious Labs, Inc. My research on Oblivious RAM and differentially private algorithms have been adopted by Signal, Meta, and Google.

Luke Szramowski
Luke Szramowski is a mathematical researcher, with a Bachelor's Degree in Mathematics and two Master's Degrees, one in Math, with a focus in Number Theory and another in Math with a focus in Coding Theory. In his free time, Luke works on a litany of different math problems, mainly regarding Number Theoretic conjectures and playing all different types of games.

Joseph McKay
Professor Joseph McKay is an accomplished educator and legal professional. Previously, Professor McKay worked as a Judicial Law Clerk for Judge William J. Bauer of the U.S. Court of Appeals for the 7th Circuit and Judge David W. Dugan of the U.S. District Court for the Southern District of Illinois. He also worked as a Pro Se Staff Attorney, focusing on cases involving prisoner civil rights and habeas corpus, at the U.S. District Court for the District of Nevada.

Dan Miller
Dan Miller has designed, deployed, and secured information systems for multinational banks, publishers, credit agencies, telecoms, and other enterprises for nearly three decades. He specializes in open-source solutions and system integration to reduce friction in computing and communication. His work with community currencies, barter networks, and timebanks has shaped his involvement with cryptocurrencies.

Afonso Tinoco
Afonso Tinoco is a PhD candidate currently on leave from Carnegie Mellon University and University of Lisbon. His research interests include Applied Cryptography and Distributed System Verification. He is a Co-Founder and a Research Engineer at Oblivious Labs, Inc. (https://obliviouslabs.com). Oblivious Lab's mission is to develop open-source toolchains for Oblivious Computation (https://github.com/obliviouslabs/), with the goal of accelerating the wide deployment of Oblivious Computations. He is also a co-captain of STT (https://sectt.github.io/) , the CTF team of University of Lisbon.

Param Pithadia
Param is an Electrical Engineering Student from Georgia Tech with a strong passion for and interest in crypto. Although he primarily got interested in cryptography and hardware security through a class at Georgia Tech, he is also working at a software company on crypto adoption and ease of use. With a unique blend of HW and SW skills, Param is truly enthusiastic about all aspects of crypto.

Wei Hong
Wei Hong is a machine learning practitioner with six years of experience in natural language processing and applied AI at one of the world's largest cryptocurrency exchanges. He has contributed to projects involving KYC systems, user risk profiling, and the deployment of AI in real-world financial applications. Fascinated by blockchain development, Wei Hong is particularly interested in the intersection of decentralization, transparency, and machine learning. He is currently pursuing a Master's in Computer Science at Georgia Tech, where he is an active member of the Blockchain Club@GT.

Chloe Chong
Chloe is a machine learning engineer and blockchain enthusiast with five years of experience in building ML systems for fraud detection and compliance in the traditional payments and fintech industry. Outside of work, she explores blockchain development with a focus on usability and real-world applications in the payment space. Chloe is an active member of the Georgia Tech Blockchain Club and is particularly interested in how decentralized technologies can improve financial infrastructure and user experience.is work with community currencies, barter networks, and timebanks has shaped his involvement with cryptocurrencies.

Utvecklas
Utvecklas is a computer scientist and privacy advocate who has integrated cryptocurrency into online businesses since 2016. Over time, cryptocurrency itself became his primary interest. Outside of work, his research specializes in exploits — whether past, ongoing, or potential.

George
George is a cryptocurrency enthusiast who has been actively involved in the space since 2018. With a focus on crypto marketing and security, he has successfully launched multiple projects aimed at improving both user adoption and safety. George is passionate about bridging the gap between complex technologies and mainstream audiences.

Arjun Suresh
Arjun Suresh is pursuing postgraduate studies in Cybersecurity at the University of Wollongong in Dubai, specializing in blockchain security, penetration testing, and applied cryptography. His interest in crypto security was shaped by analyzing major exchange breaches, including the Mt. Gox and Ronin Network hacks, where he studied the gap between attacker tradecraft and real-world defenses. Blending academic research with hands-on experimentation, he focuses on uncovering vulnerabilities and stress-testing the security assumptions behind modern blockchain systems.

Dani Weidman
Dani Weidman is a software engineer with interests in interactive devices, practical hardware hacking, and weird purpose-specific technology. By day, he works on secure AI software at an electronic medical records startup; outside of work, Dani builds interactive hardware and badge projects, and reverse engineers things like infrared-controlled light-up wristbands and Bluetooth trackers. Dani enjoys bringing software and hardware together in ways that are tangible, playful, and a little unusual.

Antigone
I am currently conducting smart contract audits at an auditing company. In my spare time, I write code and mine bugs on vulnerability bounty platforms. Mainly looking at various protocols in the EVM ecosystem, accustomed to reviewing and learning vulnerability logic through practical experience.

Absurdity
The hacker known as Absurdity currently works at an auditing company on Web3 security related work, mainly focusing on smart contract auditing and formal verification. In addition to blockchain, Absurdity also has a sustained interest and practice in traditional penetration testing, Internet of Vehicles (IoV), and IoT firmware analysis.

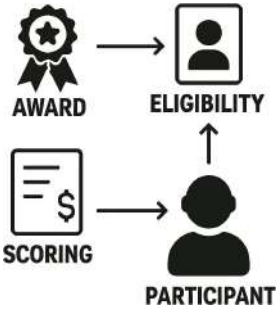
FLY
A computer science student, FLY's current main research direction is IoT vulnerability mining, mainly exploring the 0day of enterprise level firewalls, egress gateways and other devices, as well as common home routers and cameras. FLY is very interested in the web3 smart contract audit competition and DIY hardware wallets, and hopes to develop web3 into an amateur profession.

baswvad
A remote independent developer, baswvad is currently providing technical support for the gaming industry. They are accustomed to using Go and Rust for backend development, and have some personal practice in Android reverse engineering and protocol analysis in their spare time. Baswvad has also been learning how to introduce LLM (Large Model) into daily automated workflows recently.

Josh
Josh is an offensive security engineer with over 6 years of experience in penetration testing, red team operations, and adversary emulation across infra, web, mobile, and cloud environments (AWS/GCP). His work focuses on identifying and exploiting vulnerabilities to uncover weaknesses, validate defenses, and elevate security resilience. Currently, Josh specializes in red team operations focused on multi-cloud environments such as (aws/gcp/az), phishing campaigns, and also developing several templates for integration with gophish and evilginx, available on his GitHub account.

CHAPTER 4

Contests



To participate free of charge in the Cryptocurrency Cyber Challenge as an individual or team, register your (pseudo)name to receive confirmation and detailed instructions. Each member of a team must register. On site registration may be available at the event, but once contest seats fill the Cryptocurrency Cyber Challenge will close to new participants. Awarding of monetary prizes and other rewards is not guaranteed and may depend on the opinions and moods of sloppy judges as they review and test your newly acquired skills. Your physical presence is required. Good luck!

Levels

Level 1
To win the first level, answer five questions relating to offensive security practices in cryptocurrency systems. Use the list in this book to practice.

Level 2
To win this level, create a testnet wallet, write down the seed phrase safely, answer a few security questions, and send a test transaction.

Level 3
To win, connect your badge to a computer, and customize or reset the device.

Level 4
To win this level, find the hidden data stored in the badge electronics, and show the recovered messages or codes.

Level 5
To win this level, prove your understanding of currency flow. A wallet was violated, funds were drained and moved across multiple wallets to hide the trail. Your mission is to trace the transactions, recover the missing seed phrase word hidden in the on-chain data, and identify where the funds finally ended up.

Level 6
To win this level, deanonymize a given wallet. Participants are given a cluster of transactions where privacy techniques have been applied imperfectly. They must identify the fingerprint leak that breaks anonymity and name the wallet or actor behind it.

To learn what prizes accompany each level won, please ask a staffperson.

Capture the Flag
Draining the Merlion's Vault

SingaChain, a fictional digital bank backed by the fantasy *Singapore Authority of Money (SAM)*, has just launched the **Merlion Reserve Protocol (MRP).** This protocol allows users to deposit **Digital SGD (dSGD)** to mint LION stablecoins.

The bank claims the protocol is *uncrackable* because it uses a proprietary Regulatory Compliance Layer that validates every transaction against a whitelist. Your mission is to **find the cracks** in the vault.

They told us the Garden City was a fortress of glass and silicon. They said the CBDC was the final evolution of the euro—regulated, immutable, and backed by the weight of nation states."

But glass breaks, and silicon has a memory.

On a humid April night at Marina Bay Sands, during the first-ever **DEF CON Singapore,** we didn't just find a bug; we found a backdoor left open by the very people who built the walls. Project SingaChain was supposed to be the future of finance, but it forgot the oldest rule in the book: **Trust is a vulnerability.**

We bypassed the 'Kiasu' gatekeepers. We watched the Orchard Road exchange collapse under the weight of a single atomic transaction. We summoned the ghost of a dead signature to walk right into the National Insurance Fund.

This isn't just a write-up. It's a eulogy for a 'perfect' system that never stood a chance against a curious mind with a keyboard.

"Welcome to the Merlion's Vault. We've already left."

Challenge 1: The "Kiasu" Gatekeeper
Level: Easy (Warm-up)
The Vulnerability: Logic Flaw / Improper Access Control

- **The Scenario:** The *ComplianceManager contract* ensures only KYC-verified addresses can mint LION. However, the bank implemented a "Fast-Track" function for high-net-worth VIPs.
- **The Flaw:** The *fastTrackVerify()* function is public and doesn't check *msg.sender.*
- **The Goal:** Bypass the KYC process and mint your first 100 LION tokens without being on the whitelist.

Challenge 2: The Orchard Road Flash Crash
Level: Medium
The Vulnerability: Price Oracle Manipulation

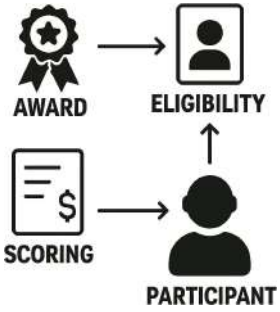
- **The Scenario:** The Merlion Vault uses a Decentralized Exchange (DEX) pool as its price oracle to determine the value of dSGD/LION.
- **The Flaw:** The protocol calculates the exchange rate based on the instantaneous balance of a low-liquidity pool rather than using a Time-Weighted Average Price (TWAP.)
- **The Goal:** Use a Flash Loan to pump the price of dSGD in the pool, tricking the Vault into letting you borrow a massive amount of LION against a tiny deposit.

Challenge 3: The Ghost in the CBDC
Level: Difficult
The Vulnerability: Cryptographic Signature Malleability / Logic Error

- **The Scenario:** The CBDC itself is a specialized **ERC-20.** It has a *permit()* function that allows the bank to move funds for "regulatory recovery"
- using **ECDSA** signatures.
  The Flaw: The implementation fails to check for "Signature Malleability" or doesn't include a nonce, allowing an attacker to replay a single recovery signature multiple times.
- **The Goal:** Drain the "Insurance Fund" address by replaying a legitimate recovery transaction from the bank's history.

CHAPTER 6

Hackathon



To participate free of charge in the Cryptocurrency Hackathon as an individual or team, register your (pseudo)name to receive confirmation and detailed instructions. Each member of a team must register. On site registration may be available at the event, but once contest seats fill the Cryptocurrency Hackathon will close to new participants. Awarding of monetary prizes and other rewards is not guaranteed and may depend on the opinions and moods of sloppy judges who evaluate your work according to the following criteria. Your physical presence is required. Good luck!

Privacy — "Hide"
- ZK (privacy pools etc...)
- Metadata minimization
- Private identity/credentials

Exploitation — "Break"
- Static analysis, Dynamic Analysis
- Runtime tracing / attack replay
- Fuzzing attack test
- Differential testers

Sovereignty — "Survive"
- Watchdog / monitoring agents
- Fraud proof systems
- Key management & Recovery
- Verifiable infrastructure

Escape — "Evade"
- Censorship resistance
- Surviving chain halts
- Fork-choice modeling
- Emergency migration

Classes

Application
Design a new cryptocurrency application and explain it with a series of use cases and stories. Judging considers uniqueness, novelty, and practicality.

Network
Discover a new network technology to support cryptocurrency application in a more secure, efficient, or beneficial way.

Hardware
Design a new electronic device using hardware engineering principles. Describe the design in plain language and convince it is implementable.

Software
Design a application, component, library, or driver, that runs in a server, workstation, or mobile environment. Judging considers degree of complexity

Firmware
Design a new firmware application using embedded development principles. The hardware device in question may be a wearable electronic badge.

Science
Replace the scientific implementation of an existing cryptocurrency system, to improve, broaden, or better secure the underlying application.

Analysis
Deliver an original analysis of an existing cryptocurrency system, by writing a whitepaper to educate, compare, or convince of merits in the application.

CHAPTER 7

Glossary

Event - Any occurrence where we appear as a team
Defcon - The largest hacking and security conference hosted in Las Vegas, Nevada (sometimes written DC, DEFCON, or DEF CON), hosting presentations, workshops, contests, villages and the premier Capture The Flag Contest.
DC34 - Thirty four years after the first Defcon, the number is used rather than 2025
Organizer- A person with management privileges, who can set policy in meetings
Volunteer - A catchall name for those participating by contributing anything
Role - A volunteer may have one or more roles, like press manager or webmaster
Distribution - Transfer of ownership of goods, whether commercial paid or free of charge
Village - A classic Defcon concept, granting a lot of generous resources. A lot of other similar concepts exist, for which we can apply. For example a vendor area or demolab hour
Contest - A very old Defcon concept, where the best contestants win a black badge (free entrance)
Crypto - If you like this abbreviation, understand that it's a problem term
Cryptocurrency - A digital form of currency based on code. The code can be either open source or closed source. Open source code reveals to the public the inner workings of the cryptocurrency, whereas closed source keeps its code secret from the public.
Hacker - A difficult term with many meanings, probably this means creative kids and adults competent at solving science problems in a unique or humorous manner.
QM - Quartermaster, the Defcon area where we can check out cables, projectors, and tools
Goon - A volunteer at the DC hacking conference who helps ensure the conference runs smoothly. Goons may perform a variety of tasks, including security, moderating, and helping with presentations
Lead - A term describing a leader of a DEFCON area, like vendor lead or village lead

Questions 1

01) What is a 51% attack?
02) What is cryptojacking?
03) How does a Merkle proof work?
04) What is 'slashing' in Proof of Stake?
05) What happens when a blockchain forks?
06) What does a double spend attack entail?
07) How does a blockchain ensure immutability?
08) What can an attacker do with a 51% attack?
09) What is a Merkle root in a blockchain block?
20) How does staking improve blockchain security?
21) What is a Sybil attack in blockchain networks?
22) What is the first block in a blockchain called?
23) What determines a blockchain's block size limit?
24) What is the threshold in Shamir's Secret Sharing?
25) What is an eclipse attack in blockchain networks?
26) How does Proof-of-Stake reduce Sybil attack risks?
27) What are smart contracts in blockchain technology?
28) How do blockchain networks mitigate Sybil attacks?
29) How does Proof of Stake differ from Proof of Work?
30) How do miners compete in Proof of Work blockchains?
31) What is a layer 2 solution in blockchain scalability?
32) How does Shamir's Secret Sharing work mathematically?
33) Why is block height important in blockchain consensus?
34) What is a reentrancy attack in smart contract security?
35) What is the main risk of zero-confirmation transactions?
36) What is a Merkle tree used for in blockchain technology?
37) What is the primary function of a block in a blockchain?
38) Why are Schnorr signatures considered superior to ECDSA?
39) How does Proof-of-Work prevent double spends?
41) How do blockchain networks prevent front-running attacks?
42) How do nodes in a blockchain network validate new blocks?
43) How does a dust attack compromise cryptocurrency privacy?
44) What is the purpose of a nonce in blockchain block mining?
45) Why do blockchain networks use Merkle trees inside blocks?
46) Which cryptocurrencies are most vulnerable to a 51% attack?

Answers 1

01) An attack where an entity controls more than 50% of a blockchain's mining power.
02) The unauthorized use of someone's computing power to mine cryptocurrency.
03) It demonstrates that a transaction is included in a block without revealing all transactions.
04) A penalty that takes away a validator's staked coins if they act maliciously.
05) The chain splits into two diverging paths due to disagreements in protocol or new upgrades.
06) A user fraudulently spends the same cryptocurrency twice.
07) Through cryptographic hashing and decentralized consensus mechanisms.
08) Reverse transactions, double spend coins, and prevent new transactions from confirming.
09) The final hash in the Merkle tree that represents all transactions within that block.
20) Validators have financial incentives to act honestly since they risk losing their stake if they cheat.
21) A malicious entity creates multiple identities to gain disproportionate influence.
22) The genesis block.
23) Protocol rules, which affect scalability and transaction capacity.
24) The minimum number of shares required to reconstruct the original secret.
25) A type of attack where a node is isolated and fed false information by malicious peers.
26) By requiring a substantial stake to participate in consensus.
27) Self-executing contracts with predefined conditions written in code.
28) Through Proof-of-Work, Proof-of-Stake, or identity verification measures.
29) Instead of computational effort, validators are chosen based on the number of coins they stake.
30) By solving complex mathematical puzzles (hash functions) to find a valid block hash.
31) An off-chain scaling mechanism designed to increase transaction throughput.
32) It uses polynomial interpolation to reconstruct a secret from a subset of shares.
33) It helps determine the longest chain and ensures consistency across nodes.
34) A vulnerability where a malicious contract repeatedly calls a function before the state updates.
35) They can be double-spent before being included in a block.
36) To efficiently verify and store large sets of transactions in a block.
37) To store a batch of transactions and link securely to the previous block.
38) They provide better security, efficiency, and privacy through aggregation.
39) By ensuring that the longest chain is valid, making transaction reversals difficult.
41) By implementing transaction ordering mechanisms like batch auctions.
42) By checking that the transactions are valid and the block follows consensus rules.
43) By sending tiny amounts of cryptocurrency to wallets to track transactions and link identities.
44) A variable used in Proof of Work to find a valid hash for a new block.
45) To efficiently verify transactions without needing the entire dataset.
46) Smaller Proof-of-Work chains with lower hashrate security.

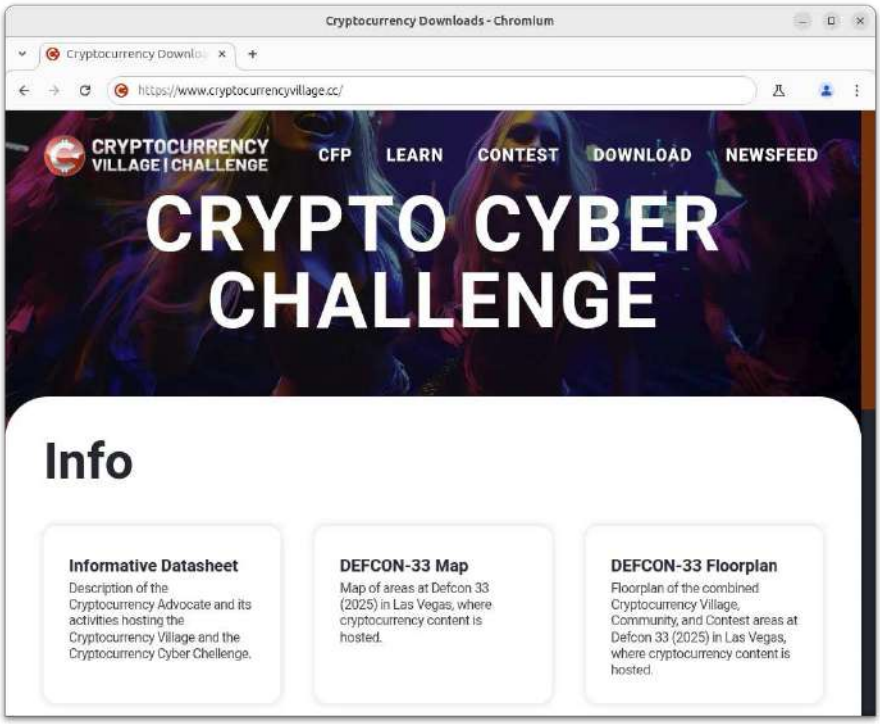
Questions 2

47) What is the role of rollups in Ethereum scaling?
48) What is the role of CoinJoin in Bitcoin privacy?
49) What is the difference between SHA-256 and Keccak-256?
50) What is the main purpose of Proof of Work in a blockchain?
51) How does a timejacking attack manipulate blockchain consensus?
52) What is the significance of block timestamps in cryptocurrency?
53) What feature does Mimblewimble offer for cryptocurrency privacy?
54) What is the purpose of a phishing attack in cryptocurrency security?
55) What mathematical concept is fundamental to Schnorr signatures?
56) What is finality in blockchain networks?
57) What is probabilistic vs deterministic finality?
58) What is Byzantine Fault Tolerance (BFT)?
59) What is a mempool and how is it used in a blockchain?
60) What is state in a blockchain and what does it refer to?
61) What is a seed phrase and how is it often used?
62) What is hierarchical deterministic (HD) wallet?
63) What is a nonce in Ethereum transactions?
64) What is an integer overflow/underflow vulnerability?
65) What is a denial-of-service attack in smart contracts?
66) What is front-running protection using commit-reveal?
67) What is interoperability in blockchain networks?
68) What is a wrapped token and give an example?
69) What is slippage in cryptocurrency trading?
70) What is modular blockchain architecture?
71) What is data availability in blockchain networks?
72) Why are private keys more important than passwords?
73) What is the oracle problem in smart contracts?
74) What is a fallback function in smart contracts?
75) What is a flash loan attack and how does it work?
76) What is a rug pull in DeFi network systems?
77) What is a bridge attack in cross-chain systems?
78) What is MEV (Maximal Extractable Value)?
79) What is the blockchain trilemma?
80) What is the difference between rollups and sidechains?
81) What is a zero-knowledge proof (ZKP)?

Answers 2

47) They bundle multiple transactions into a single batch to reduce on-chain processing.
48) It enables users to combine transactions, making it harder to link addresses to individuals.
49) SHA-256 is used in Bitcoin, while Keccak-256 is used in Ethereum.
50) To secure networks by requiring computational effort to validate transactions and add blocks.
51) By altering a node's system time to create invalid timestamps and disrupt synchronization.
52) They help verify the chronological order of transactions and prevent manipulation.
53) It hides transaction amounts and addresses to improve anonymity.
54) To trick users to reveal private keys or login credentials through fraudulent websites or emails.
55) Discrete logarithms in elliptic curve cryptography.
56) Finality is the guarantee that a transaction cannot be reversed once it is confirmed.
57) Probabilistic improves over time; deterministic is instant.
58) It is the ability of a system to function correctly even if some nodes act maliciously or fail.
59) A mempool is a pool of unconfirmed transactions waiting to be included in a block.
60) State refers to the current data of accounts, balances, and smart contracts at a given block.
61) A seed phrase is a human-readable backup of a private key used to restore a wallet.
62) An HD wallet generates multiple addresses from a single seed phrase.
63) It is a counter that ensures each transaction is processed only once and in order.
64) TIt occurs when arithmetic operations exceed storage limits, causing incorrect values.
65) An attacker prevents contract execution by consuming resources or triggering failures.
66) Users first commit a hashed value, then reveal it to prevent others from copying or exploiting it.
67) An off-chain scaling mechanism designed to increase transaction throughput.
68) It is a token representing a cryptocurrency from another blockchain (BTC on ETH.)
69) It is the reward earned by locking tokens in a Proof-of-Stake network.
70) It separates execution, consensus, and data availability into different layers.
71) It ensures that transaction data is accessible for verification by all participants.
72) Because ownership of funds is entirely determined by control of the private key.
73) The difficulty of securely bringing real-world data onto the blockchain.
74) A default function triggered when no function matches or Ether is sent.
75) An attack using instant loans to exploit protocols in one transaction.
76) A scam where developers withdraw funds leaving tokens worthless.
77) An exploit targeting cross-chain bridges to steal locked assets.
78) Profit from reordering or manipulating transactions in a block.
79) The trade-off between decentralization, security, and scalability.
80) Rollups use main chain security; sidechains operate independently.
81) Proof of knowledge without revealing the actual information.

Website



Sections in the appendix are taken from the current state of the website and developments relating to the Cryptocurrency Advocate's appearance at the DEFCON hacker convention in Las Vegas, USA.

For a more comprehensive or up to date impression, please navigate to:

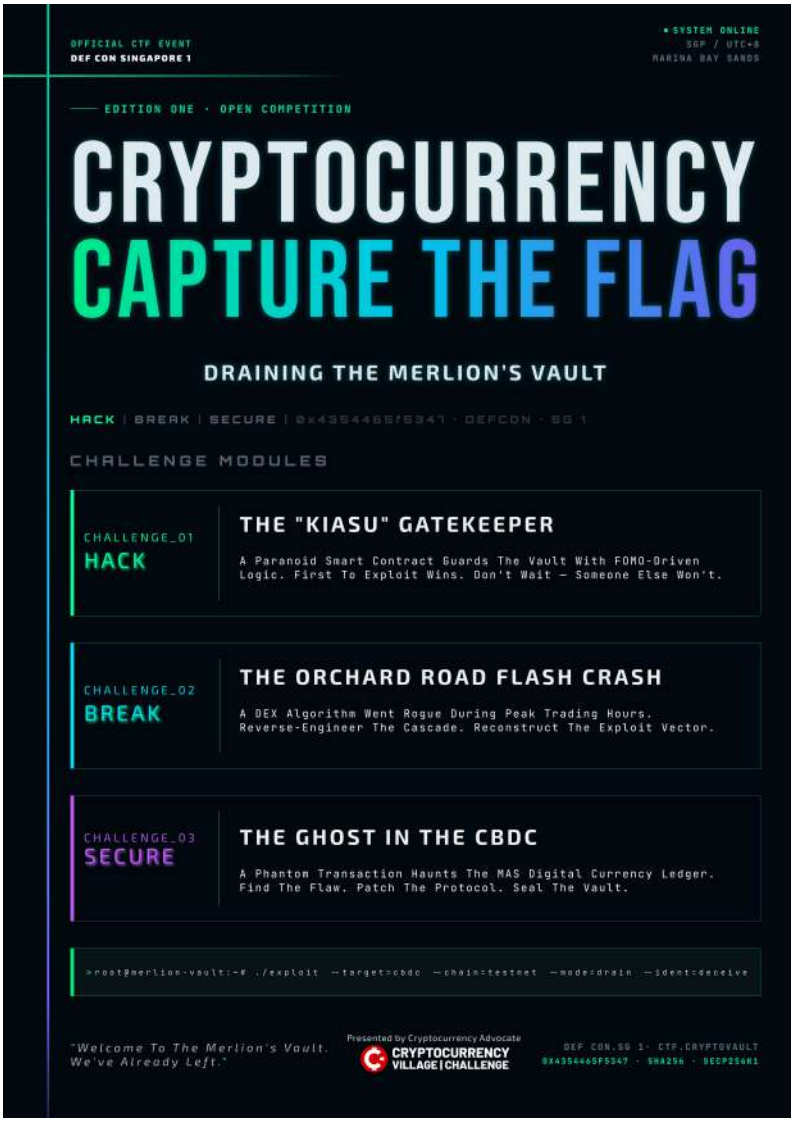
https://www.cryptocurrencyvillage.cc/

Volunteer Poster

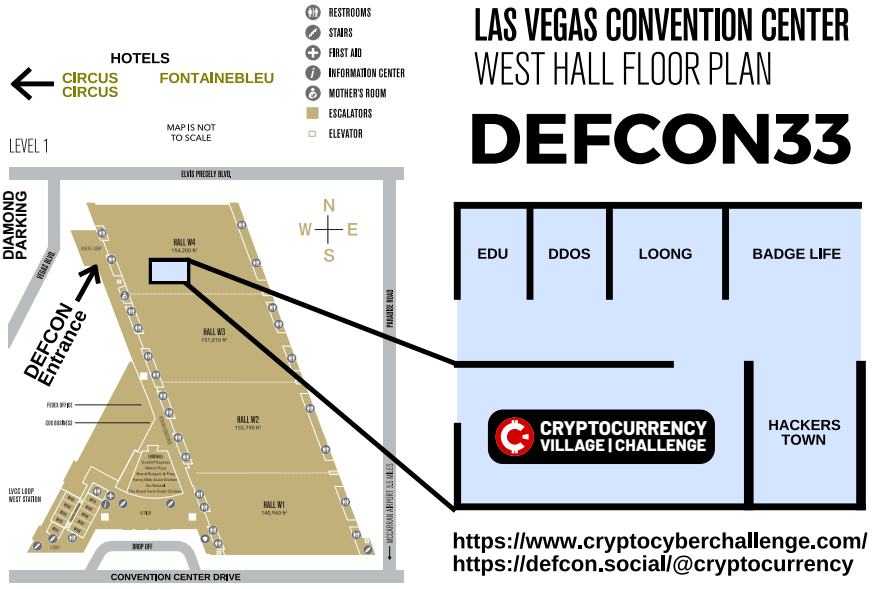
Contest Poster

Hackathon Poster

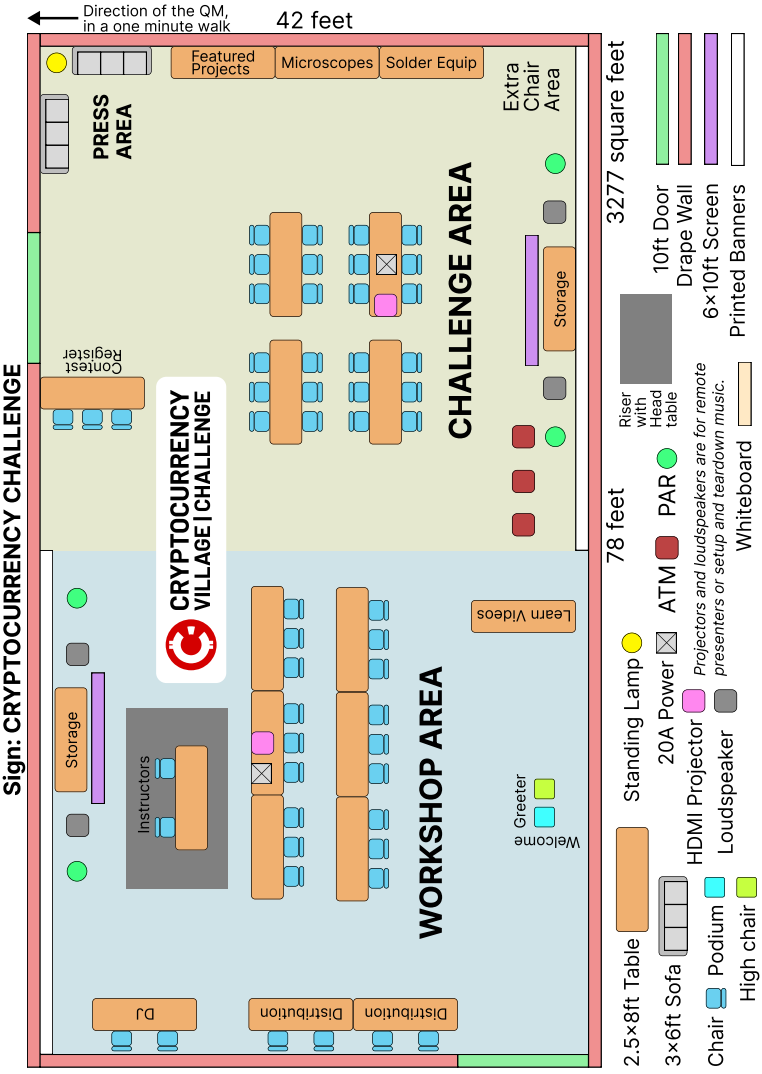
Capture the Flag Poster



Las Vegas Venue

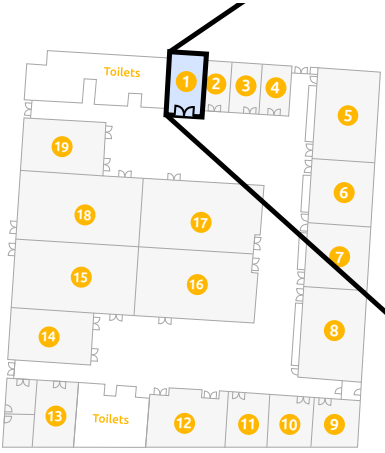


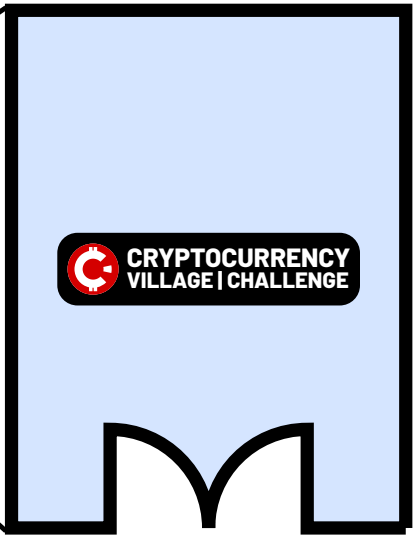
Las Vegas Area



Bahrain Venue

DEFCON-BAH
EXIBITION WORLD BAHRAIN
MEETING ROOM HUB C1

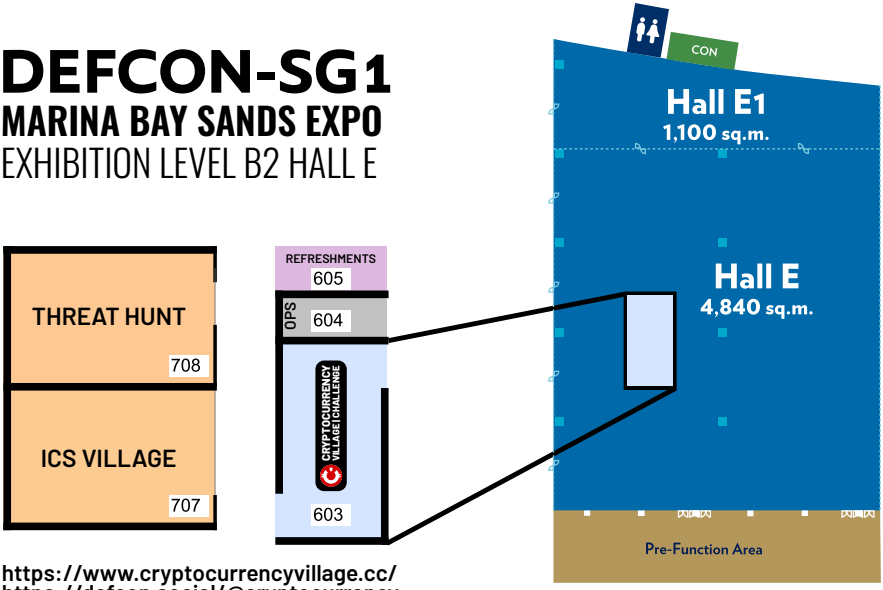




https://www.cryptocyberchallenge.com/
https://defcon.social@cryptocurrency

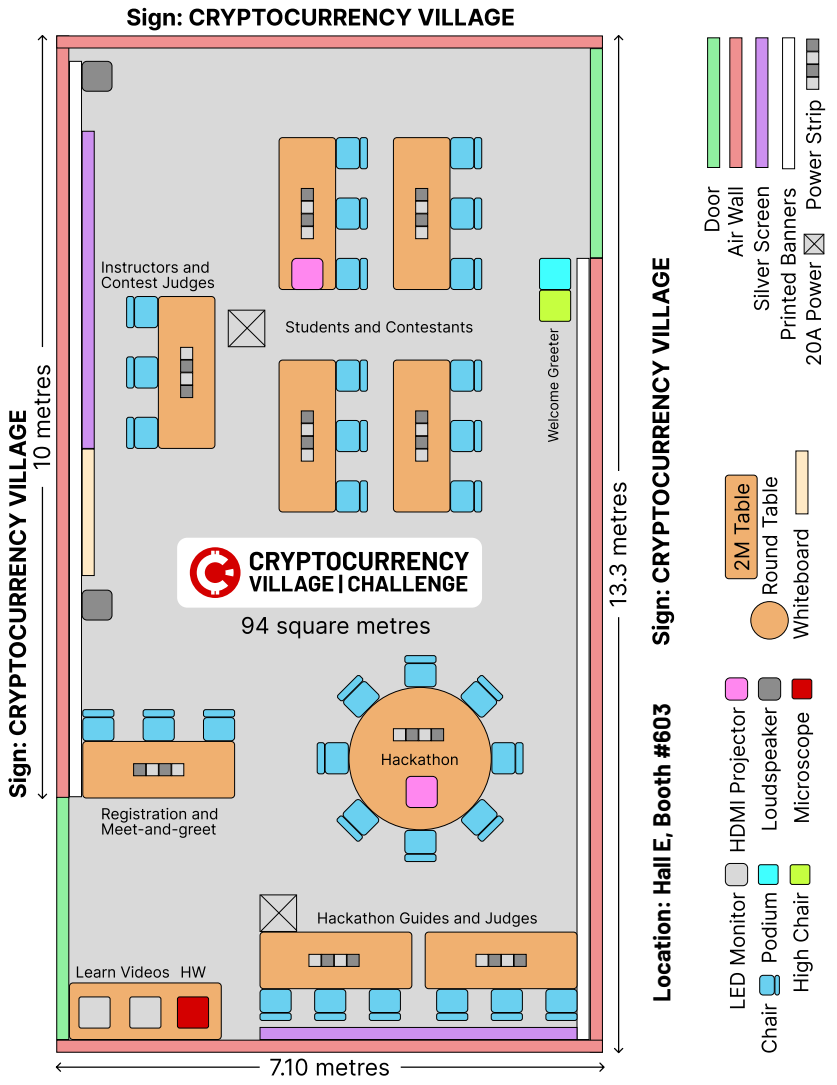
Singapore Venue

DEFCON-SG1
MARINA BAY SANDS EXPO
EXHIBITION LEVEL B2 HALL E



https://www.cryptocurrencyvillage.cc/
https://defcon.social/@cryptocurrency

Singapore Area



News

Defcon accepts Cryptocurrency Advocate as a Vendor
Exciting News! Defcon has officially welcomed Cryptocurrency Advocate as a conference vendor. Get ready for a fusion of cutting edge cryptocurrency innovation and top tier cybersecurity insights in a vending package you can visit at Defcon this August 8-10 2025.

https://www.defcon.org/html/defcon-33/dc-33-vendors.html

Find us in Hall 4 where all Defcon vendors distribute their goods. Products include electronics, textiles, and other branded merchandise.

The Cryptocurrency Advocate Website Launches
We wrote a website for visitors to our premium events taking place this August at Defcon in Las Vegas.

https://www.cryptocurrencyvillage.cc/

https://www.cryptocyberchallenge.com/

You can sign up to attend a workshop, compete in a contest, or propose an instructor. See you at Defcon!

Crypto Deregulation on the Radar
After a dozen nations completed integration or clarification of rules governing cryptocurrency, a trend towards deregulation is developing. Several governments are working to make cryptocurrency adoption more attractive in their countries.

The Cryptocurrency Village receives an assignment at DEFCON 33
Managers at DEFCON approved hosting content proposed by the Cryptocurrency Village at DEFCON 33, taking place at the Las Vegas Convention Center on 7-10 August 2025. The village occupies space in the DEFCON Communities area of the LVCC West Hall 4. See you at DEFCON!

The Cryptocurrency Cyber Challenge to take place at DEFCON 33
Managers at DEFCON approved hosting of the Cryptocurrency Cyber Challenge at DEFCON 33, taking place at the Las Vegas Convention Center on 7-10 August 2025. The contest occupies space in the DEFCON Communities area of the LVCC West Hall 4. Come to the contest to meet us!

DEFCON and AICS in Bahrain to Include the Cryptocurrency Village
Exciting News! DEFCON and the Arab International Cybersecurity Summit have decided to include the Cryptocurrency Village at DEFCON Bahrain this November 5-6 2025.

https://www.arab-cybersecurity.com/

Find us in the meeting room hub area C1 where all DEFCON villages reside. Find a fun mix of interactive workshops, cutting edge presentations, challenging contests, off-hand mentor chats, and free prizes too!

DEFCON SG 1 chooses the Cryptocurrency Village for inaurural event
Today the Cryptocurrency Village was chosen of a handful of villages and only four contests, to appear and perform its award winning activities, at the first ever DEFCON event in Singapore on 28-30 2026.

https://www.defcon.org/html/defcon-singapore/dc-singapore-index.html

We will bring several new activities including a hackathon, hardware zoo, and birds of a feather. We hope to see you at the Marina Bay Sands Expo!

Sponsors

We thank our sponsors for their tireless input, constructive feedback, monetary, and non-monetary contributions. You play an important role in helping accomplish the mission.

Attractive Opportunity

The Cryptocurrency areas at DEFCON 34 (2026) include about 3000 square feet of space for an estimated 30-40000 DEFCON attendees. Our areas are full of activities and host the Cryptocurrency Cyber Challenge as well as daily workshops. A third Cryptocurrency vendor area lies between these and the largest entrance doors near the sold out Fontainebleau and Marriott hotels. All of our areas are within eyesight of each other, in the most attractive Hall 4 floor space at DEFCON. For details, please see maps in the download tab of the website https://www.cryptocurrencyvillage.cc/docs/

Other presentations of the Cryptocurrency Village and related areas appear at DEFCON Bahrain and DEFCON Singapore.

Sponsor Relations

To contact us with questions relating to sponsorship, please email:
sponsors@cryptoadvocate.cc

power up privacy

OtterSec

asymmetric research

Disclaimer

Cryptocurrency Advocate
Cryptocurrency Village and Cryptocurrency Cyber Challenge
https://www.cryptocurrencyvillage.cc/ Last updated: March 31, 2026

1. General Disclaimer

All content, materials, activities, events, products, tools, training sessions, demonstrations, presentations, workshops, contests, challenges, and any other offerings (collectively, "**Offerings**") provided by, through, or in connection with The Cryptocurrency Advocate, the Cryptocurrency Village, the Cryptocurrency Cyber Challenge, and any affiliated events or platforms (collectively, "**the Organization**") are provided strictly for educational, demonstrational, research, and training purposes only.

The Organization is operated entirely by volunteers and does not charge for participation in its Offerings. No Offering shall be construed as professional, financial, investment, legal, tax, or any other form of licensed advice or recommendation.

2. Assumption of Risk

By attending, participating in, observing, accessing, or otherwise engaging with any Offering — whether in person at any venue or event location (including but not limited to events held in Las Vegas, United States; Singapore; or Bahrain), online, or through the Organization's website or any related digital platforms — you expressly acknowledge and agree that you do so entirely at your own risk.

Certain Offerings may involve inherent risks, including but not limited to the use of soldering irons, electronic tools, battery-operated devices, lithium battery components, chemical substances, hardware assembly kits, or other equipment and materials. You accept full responsibility for any injury, loss, damage, or liability arising from your participation.

3. No Warranty

All Offerings are provided on an "AS IS" and "AS AVAILABLE" basis, without warranty of any kind, whether express, implied, or statutory, including but not limited to warranties of merchantability, fitness for a particular purpose, accuracy, completeness, reliability, non-infringement, or uninterrupted availability.

Any products, kits, hardware, software, documentation, or other materials provided, distributed, or made available by the Organization — whether free of charge or otherwise — come with absolutely no warranty. The Organization makes no representations or guarantees regarding the safety, functionality, performance, or suitability of any such materials.

4. Limitation of Liability

To the fullest extent permitted by applicable law, the Organization, its volunteers, organizers, instructors, speakers, advisors, sponsors, partners, affiliates, and any associated individuals or entities shall not be held liable for any direct, indirect, incidental, consequential, special, exemplary, or punitive damages, including but not limited to damages for personal injury, loss of data, loss of profits, property damage, or any other loss arising out of or in connection with any Offering, regardless of the cause of action or the theory of liability, even if the Organization has been advised of the possibility of such damages.

5. Third-Party Content and Services

The Organization's Offerings may include or reference content, materials, products, services, presentations, or opinions provided by third parties, including but not limited to guest speakers, sponsors, partners, and linked external websites or resources. The Organization does not endorse, guarantee, or assume responsibility for the accuracy, completeness, safety, legality, or quality of any third-party content or services. Any reliance you place on such third-party content is strictly at your own risk.

6. Not Financial or Investment Advice

Nothing in any Offering constitutes financial advice, investment advice, trading advice, or any other form of advice intended to be relied upon for financial decision-making. The Organization, its volunteers, and its participants are expressly prohibited from providing financial or investment advice. Any discussion of cryptocurrencies, blockchain technologies, tokens, digital assets, or related topics is purely educational and for research purposes. You should consult a qualified financial advisor before making any financial decisions.

7. Website and Digital Content

Content published on the Organization's website (www.cryptocurrencyvillage.cc), related repositories, social media accounts, communication channels (including Discord, Mastodon, Nostr, and email), and any other digital platforms is provided for informational and educational purposes only. The Organization makes no guarantee that website content is current, accurate, or complete, and reserves the right to modify or remove content at any time without notice.

8. Intellectual Property

All original content, trademarks, logos, and materials produced by the Organization remain the property of The Cryptocurrency Advocate unless otherwise stated. Offerings that include open-source software or third-party materials are subject to their respective licenses.

9. Indemnification

By participating in or engaging with any Offering, you agree to indemnify, defend, and hold harmless the Organization, its volunteers, organizers, instructors, speakers, advisors, sponsors, partners, affiliates, and any associated individuals or entities from and against any and all claims, liabilities, damages, losses, costs, and expenses (including reasonable legal fees) arising out of or related to your participation in any Offering, your violation of this Disclaimer, or your violation of any applicable law or regulation.

10. Severability

If any provision of this Disclaimer is found to be unenforceable or invalid under applicable law, such provision shall be modified to the minimum extent necessary to make it enforceable, or if modification is not possible, severed from this Disclaimer. The remaining provisions shall continue in full force and effect.

11. Governing Law

This Disclaimer shall be governed by and construed in accordance with the laws of the State of Wyoming, United States, without regard to its conflict of law provisions. Any disputes arising under or in connection with this Disclaimer shall be subject to the exclusive jurisdiction of the courts located in the State of Wyoming.

12. Acknowledgment and Acceptance

By attending any event, participating in any activity, accessing any content on the Organization's website or related platforms, using any product or material provided by the Organization, or otherwise engaging with any Offering, you acknowledge that you have read, understood, and agree to be bound by this Disclaimer in its entirety.

13. Contact

Cryptocurrency Advocate <policy@cryptoadvocate.cc>
30 North Gould Street, WY 82801, United States

Notes 1

Notes 2

Get your Crypto-training Advantage

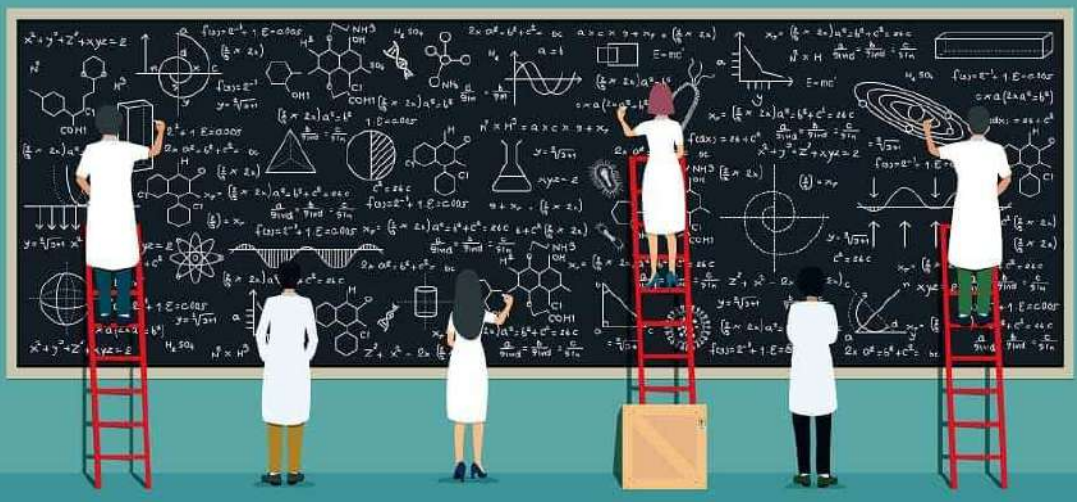
Learning Levels

BEGINNER
ADVANCED

To buy this document or book your training contact the staff of the Cryptoadvocate

CONTACT

Email: info@cryptoadvocate.cc
Nostr: cryptoadvocate@nostrcheck.me
Discord: https://discord.gg/8APBmBWKuk
Mastodon: https://defcon.social/@cryptocurrency
Repository: https://www.gitlab.com/cryptoadvocate/



US $25 CA $32 EU €20
ISBN: 979-5-360-31275-7

0 739394 634378

BOOKS
CARDS
SHIRTS
BADGES