CRYPTOCURRENCY WORKBOOK 2025

For use in training courses and contest challenges

CRYPTOCURRENCY ADVOCATE

Cryptocurrency Workbook
by Michael Schloh von Bennewitz
Version 2025-0.8, 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.

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.

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/**

Community 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
Chad Calease, Param Pithadia, and Michael Schlob 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
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
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.

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.

CHAPTER 3

Organizers

Organizers at the Cryptocurrency Advocate plan the event throught 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."

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.

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. Your physical presence is required. Good luck!

Levels

Level 1
To win this level, discuss and demonstrate on your own system the correct way(s) to backup mnemonic seeds and keys for your wallet.

Level 2
To win this level, track down a tx (that will be sent to a series of addresses in advance) and determine the ending address of the funds.

Level 3
To win this level, search for and find a specific emoji on Nostr that has encoded a steganographic bitcoin testnet private key hidden in it.

Level 4
To win this level, set up a multisig wallet (at least 2 of 2) and perform a testnet transfer into and out of the wallet.

Level 5
To win this level, demonstrate a complete privacy suite (i.e. Tor, Veracrypt/Age encryption, Simplex Chat, cryptocurrency wallet, Keepass, CryptPad.)

Level 6
To win this level, perform an atomic swap between two coins and explain output from block explorers.

Level 7
To win this level, break the privacy of any privacy coin (Monero, Firo, Zcash) that is utilizing its full privacy capabilities by tracking a transaction.

CHAPTER 5

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.
DC33 - Thirty three 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 an area at Defcon, like vendor lead or village lead

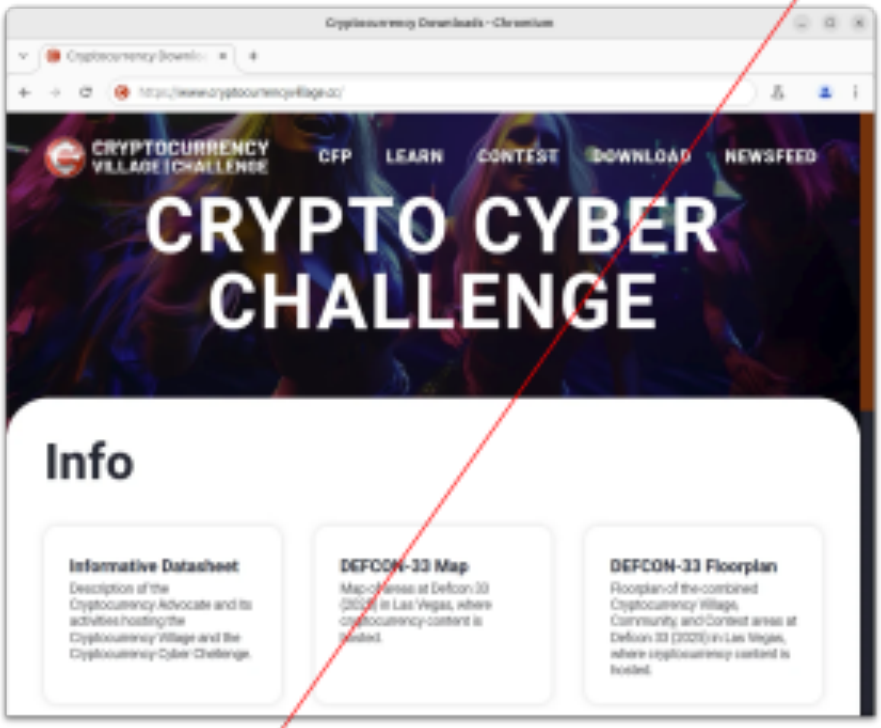
Questions

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) 10) 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

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.

Website

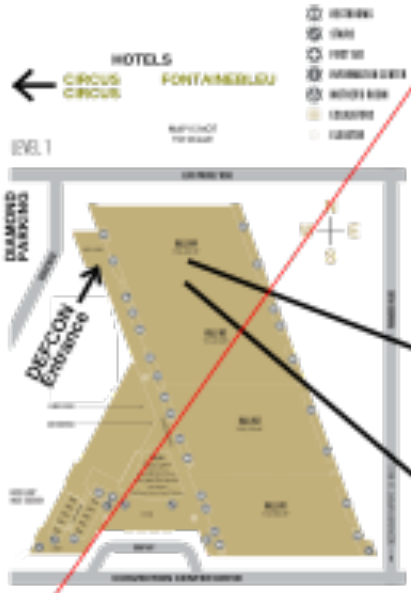


Sections in the appendix are taken from the current state of the website and developments relating to the Cryptocurrency Advocate's appearance at the DEFCON hacker convention in Las Vegas, USA.

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

https://www.cryptocurrencyvillage.cc/

Venue



LAS VEGAS CONVENTION CENTER
WEST HALL FLOOR PLAN

DEFCON33

EDU | DDOS | LOCKPICKING | BADGE LIFE

CRYPTOCURRENCY VILLAGE | CHALLENGE

HACKERS TOWN

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

Area

Direction of the GM, in a one minute walk
42 feet
Featured Projects
Microscopes
Solder Equip
PRESS AREA
Extra Chair Area
CHALLENGE AREA
Storage
Change Station
CRYPTOCURRENCY VILLAGE | CHALLENGE
Sign: CRYPTOCURRENCY CHALLENGE
Learn Videos
Storage
Instructors
WORKSHOP AREA
Workbenches
DJ
Distribution
Distribution
Sign: CRYPTOCURRENCY COMMUNITY
78 feet
3277 square feet
Riser with Hexlot table
10ft Door Drape Wall
6×10ft Screen
Printed Banners
Standing Lamp
20A Power
ATM
PAR
HDMI Projector
Loudspeaker
Projectors and loudspeakers are for remote presenters or setup and teardown music.
Whiteboard
2.5×8ft Table
3×6ft Sofa
Chair
Podium
High chair

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!

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

Our Cryptocurrency areas at DEFCON 33 (2025) include about 3000 square feet of space for an estimated 30000 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/

Sponsor Relations

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

kraken

power up privacy

Stack Wallet

ESPRESSIF

Notes 1

Notes 2

Notes 3

Notes 4