Hacking the Blockchain: Ethereum

Sleepy

Follow

Immunefi

--

14

Listen

Share

“Two roads diverged in a wood and I — I took the one less travelled by, and that has made all the difference”

– Robert Frost

I remember watching the events of the Poly Network hack and being at a loss for words. My mind began to fire off on all cylinders trying to piece together how it had happened. Blockchain-related hacks were quite common by this time, but this was one of the first that had made its way to my ears. And although the hacker returned the funds, the event itself was wild enough to be memorable, to spark my curiosity, and to set me on the path to become a hacker…again.

Blockchain hacking is one of the more elusive paths in cybersecurity, but taking it remains one of the best decisions I’ve ever made. It’s groundbreaking, challenging, and extremely rewarding, both intellectually and financially. I’ve had to get knee deep into the intricacies of how things work — something I didn’t do in other disciplines. Smart contract hacking is a form of art, and there’s nothing more beautiful than watching an exploit and the series of transactions that follow.

Being a whitehat hacker in the Web3 space feels a lot like being a superhero. Nothing beats the elation that comes from saving the common man millions of dollars, especially because many are just trying to get by in a system designed to fail them. The financial benefits that come from being at the forefront of technological breakthroughs aren’t bad, either. Bug bounties of up to 2.5 million USD are being paid out for critical bugs, and the average yearly salary at a blockchain security firm is $150,000.

To top it off, most of these opportunities are fully remote, meaning you can work from home.

Join me, Anon, on this path that very few walk. Join me in saving Web3 and becoming a legend. We need you

to prevent the next big hack.

So, how are blockchains hacked?

There are a variety of ways, but the most common and prominent attacks occur in smart contracts (programs that run on the blockchain). Other vulnerabilities can occur due to weaknesses in the protocol itself, or due to the number of validators controlled by a bad actor, e.g. a 51% attack. As the old saying goes, “More complexity, more bugs.”

The focus of this article is to get you knowledgeable about the technology, how these hacks happen, and to provide a roadmap for becoming a smart contract hacker/blockchain security practitioner in the shortest amount of time. There’s a severe shortage of security-focused people protecting the people’s internet, their money, and the dreams that come with it.

However, it is not meant to be an exhaustive guide, since the technology is still emerging, nor is it meant to teach you how to hack anything. Rather, it is meant to be a high-level overview of where and how to find the information you need, as countless people can teach the technical concepts better than I can. Before we get started, here is the content at a glance:

1. Blockchain Basics

Let's start off with what blockchains even are, and why everyone is so excited about them. No, it's not just about the money (for us cypherpunks, anyway.) A blockchain, as proposed by Bitcoin, was simply a global distributed ledger/database that uses cryptographic functions to verify transactions/data sent across the network. These transactions are verified by nodes aka miners that are rewarded with cryptocurrency for their efforts.

Bitcoin was solely meant to be a digital currency and an avenue for the average individual to be able to trade with anyone in the world.

A young programmer named Vitalik Buterin and Dr. Gavin Woods would take this concept further and introduce Ethereum to the world.

Ethereum is a blockchain protocol like Bitcoin. Unlike Bitcoin, Ethereum is Turing Complete, which means it can approximately simulate the computational aspects of any other real world, general-purpose computer and run programs. Translation? It's a global, decentralized computer that anyone can contribute computation power to and has been nicknamed "the world computer" as a result. The development of Ethereum — and other blockchains — has cultivated an ideology and hopeful vision for the future. You may have heard of it recently, an audacious claim about the next iteration of the internet…Web 3.0.

Web2 vs. Web3

Web3 is a vision for a more decentralized web, one where user information is truly one's own and ads and tracking across sites are an opt-in feature, rather than an omnipresent intrusion. A web where users are more in control of their privacy and what they reveal about themselves. A web where you benefit from the services of decentralized applications and gain financially. Privacy is not secrecy. Rather, it is the ability to selectively reveal oneself to the world. I don't like seeing my personally identifiable information get leaked and sold on the dark web, especially after taking great pains to clean up my online presence.

Think of a regular website or application. It has a frontend or user interface and a backend that stores and manipulates data and is usually written in Python, PHP, Ruby, or something else. Typically, this is hosted on a web server either in the cloud or on-premises and is susceptible to outages, natural disasters, etc. that may lead to downtime. On the blockchain, you have no such problem. For the application/website to go down, every node/miner running the network would have to be offline.

Web2 apps and hosting solutions are typically controlled by a single entity (Azure, AWS etc) and thus said entity can place their limits upon you and censor your opinions. Due to the immutable nature of blockchain protocols, it's borderline impossible to censor or delete data stored to the blockchain, except in certain cases we'll get to. Payments are built-in via the native token, ether (ETH), unlike Web2, where you need to integrate something like Stripe. Lastly, no one can prevent you from using the service for your app or boot you off a blockchain, because no one owns it.

Now, there are caveats. I will only address the technical ones. Web3 is not a panacea. Most DApps aren't even that decentralized for several reasons ranging from gas fees (Ether paid to use the world computer) to erroneously claiming DApp status, so as to ride it to the moon. It's extremely expensive to store data on the blockchain and unencrypted, sensitive data must never even be fed into it, as anyone can reverse-engineer the bytecode and reconstruct the data. (Easier said than done for the average person). Other protocols have solved the gas issue by implementing lower fees. ETH itself plans to fix this with the release of ETH 2.0.

For now, most use the InterPlanetary File System (IPFS), which is a protocol and peer-to-peer network for storing and sharing data in a distributed/decentralized file system, on-premise storage, or the cloud to store data off-chain. The resource-intensive nature of mining has also been criticized. Newer protocols have already adopted a Proof of Stake consensus algorithm, which is supposed to be significantly less resource intensive than Proof of Work, thus allowing more people to get involved in the verification process due to a lower barrier to entry. More nodes mean the protocol is inherently more secure.

Don't worry if you don't understand all this and how it connects right now. You will once you start studying.

What Web3 Means for the Traditional Web App Penetration Tester

Web application hacking will not change significantly on the client-side. A lot of the vulnerabilities you're used to might carry over to Web3. Things like SQL injection, file upload vulnerabilities, and RCE on the underlying server, however, will not. As we've previously covered, DApps do not need databases, and their backends are smart contracts, which opens up a whole different world of hacking.

2. Smart Contracts

Smart contracts are primarily where hacks happen in the blockchain space, so you're going to have to get comfortable playing around with them. The industry is somewhat cryptic for a beginner to get into, since it's a wild frontier. Luckily, I did most of the hard work of finding resources for you. So, without further ado, let's get hacking.

What Are Smart Contracts?

Smart contracts are simply computer programs that run on a blockchain network. The concept was first coined by computer scientist and cryptographer Nick Szabo in the late 1990s. However, they were first implemented by the Ethereum protocol. The scripting language designed for Bitcoin is intentionally designed to be Turing incomplete and constrained to simple true/false evaluation of spending conditions, while Solidity, the premier programming language built for the Ethereum Virtual Machine (EVM), was meant to facilitate the use of Ethereum as a globally distributed computer, not just a protocol for digital currency. Several new blockchain protocols have since emerged. Most have smart contracts that are written in Solidity. Others are written in more contemporary languages like Rust (NEAR, Solana), Python (Algorand) and even Go and C/C++ (EOS).

However, it is worth mentioning that Solana has been working on making Solidity smart contracts possible.

3. Foundations: Solidity and Ethereum

It is not the beauty of a building you should look at; it's the construction of the foundation that will stand the test of time.

-David Allan Coe

Now that you're probably dozing off and hopefully have an understanding of the basic terminology, it's time to discuss how to hack and secure smart contracts. I'm going to start with an overview of what you'll need to learn and how the knowledge ties itself together. Then, I'll give you a list of resources, my personal experience with them, and a few tips for success.

First off, you're going to have to learn the core blockchain (and how the tech itself works) that you'll be working with. For many, this will be Ethereum since it hosts the largest number of smart contracts, layer two protocols and has various other blockchains modeled after it. Starting with core blockchain tech is like learning networking in traditional security. Most concepts covered in Ethereum easily transfer over to other protocols, so picking Ethereum as your first step is a solid choice. The best resource for learning about Ethereum is Mastering Ethereum

by Andreas Antonopoulos and Dr. Gavin Woods. The best part? The book is free and open source on Github.

You'll want to read chapters 1, 2, 3, 4, 5, 6, 13, and 14. If you're not a book person, then there are video resources ahead that explain the same concepts, although not as in-depth as the book will.

GitHub - ethereumbook/ethereumbook: Mastering Ethereum, by Andreas M. Antonopoulos, Gavin Wood

Mastering Ethereum is a book for developers, offering a guide to the operation and use of the Ethereum, Ethereum…

github.com

Your next step is going to be learning the ins-and-outs of Solidity, or whatever language your smart contracts of choice are written in. If you aren't familiar with the code and its common implementations, then you'll lag behind, wasting time trying to Google unfamiliar functions or libraries.

Several auditors more experienced than me have told me this before. At the beginning of my journey, I didn't listen and tried my hand at a few Ethereum smart contract CTFs. Needless to say, the code looked like gibberish. So, I headed back to the proverbial Ethereum school and familiarized myself with the language. I used this course offered completely for free by freeCodeCamp.

It covers the basics of Ethereum and how mining works at a surface level. However, it shines above most other resources because it covers coding token standards like ERC20, ERC721 (NFTs), and DeFi (decentralized finance), which will give you an incredible understanding of the business logic of DApps and DEXs. This knowledge will be invaluable in breaking modern smart contracts.

Tip: You might not be able to pick up the syntax of Solidity easily from this course, so I recommend checking out CryptoZombies for additional practice. It'll take much less time to get acquainted with the syntax.

#1 Solidity Tutorial & Ethereum Blockchain Programming Course | CryptoZombies

CryptoZombies is The Most Popular, Interactive Solidity Tutorial That Will Help You Learn Blockchain Programming on…

cryptozombies.io

If you're looking to do some projects, then buildspace might be right for you, although in my experience, they're not the best

for learning the nuances of Solidity's syntax, and projects often require previous experience with React and JavaScript for the frontend/user interface (UI).

Note: It is not necessary to be able to code a UI or frontend with JavaScript, React, etc. to be a smart contract auditor/hacker. It's more necessary if you're trying to be a full-fledged blockchain developer.

buildspace

Start building cool web3 projects, earn NFTs, access secret work opportunities in crypto.

app.buildspace.so

With that out of the way, we can get into the fun stuff…hacking.

Extra mile:

This is by no means necessary, but it's something that will help you stand out. I highly recommend completing an introductory course on computer science, such as Harvard's CS50, ideally before beginning a course on Solidity. This has obvious benefits, like helping you pick up the syntax of other languages extremely quickly and exercising your skill in problem solving via the coursework and final project. This translates into being able to port to the other protocols quickly. Blockchain developers with a strong background in computer science are harder to find than you'd think.

I expect more blockchain protocols to pick up a memory-safe language like Rust. Aside from that, there are a few protocols that have their own languages as discussed before. Learning how to program (which is the course's purpose) is going to serve you well.

It also touches upon several languages like JS, CSS, and HTML in case you're really keen on making front-ends. For a full review of the course's benefits, see my article on it here.

Why I think all budding ethical hackers should take CS50x.

Oftentimes we're told that you don't need to learn to code/get a Computer Science degree to get into…

0xsleepy.medium.com

Here's the course link:

CS50x 2021

Introduction to the intellectual enterprises of computer science and the art of programming. This course teaches…

cs50.harvard.edu

4. Exploitation: How Companies Lose Millions With a Single Line of Buggy Code

"If a technological feat is possible, man will do it. Almost as if it's wired into the core of our being."

-Motoko Kusanagi, Ghost in the Shell

The Web3 space is such an interesting and fun playground for hackers. A single line of buggy code could lead to millions in Ether being locked up forever, countless millions being stolen in a matter of hours, or even the forking of a blockchain (Ethereum Classic hard fork) due to the fallout of a catastrophic re-entrancy attack (the DAO hack).

The rewards are great for both sides, with multiple $1,000,000+ bug bounty programs available on Immunefi, along with the possibility of becoming an absolute legend. Hackers, whether ethical or criminal, are still human, and we are all driven by a desire to be part of something greater than ourselves and also to make a name for ourselves.

Welcome to Web3 and the Cypherpunk Movement, Anon. Welcome to the revolution. We're glad to have you helping us secure the people's internet.

Onto the technical aspects then…

Security Best Practices and Common Attacks

The first thing on your list should be understanding smart contract security best practices and the discipline of securing code.

I've said it before, but Mastering Ethereum

is your one stop shop for most things Ethereum and contains best practices and explanations of common attacks, example code, and real world examples.

It's also worth taking a look at the ConsenSys material on the topic here.

Ethereum Smart Contract Best Practices

This document provides a baseline knowledge of security considerations for intermediate Solidity programmers. It is…

consensys.github.io

If you prefer a more visual approach, the Secureum bootcamp will serve you well. Stay on the lookout for new cohort announcements via their founder @0xRajeev. The bootcamp consists of the RACE (Readiness Assessment for CARE Endeavor) and CARE (Comprehensive Audit Readiness Evaluation) programs, covering a range of topics from the basics of Ethereum and Solidity to best practices and smart contract audit techniques.

As you wait, the material from Epoch 0 is available for free on Youtube.

Secureum

Share your videos with friends, family, and the world

www.youtube.com

The quizzes, their answers and assignments, are provided by 0xTaylor. I highly recommend doing all of the assignments, as they contain interesting talks and reads not linked here.

GitHub - x676f64/secureum-mind_map: This repo is actively maintained. Perform git pull's regularly…

All information was original created by 0xRajeev that he has developed from other public sources. This content is for…

github.com

Additionally, I recommend reading through audit reports from various well-respected smart contract security firms like Trail of Bits and ConsenSys.

Finally, we come to the Smart Contract Programmer who is one of my favourite YouTubers and one of the only ones providing technical explanations of common Solidity smart contract vulnerabilities via video. His Solidity content is also great for quick reminders or introduction to concepts. Below, I've linked his Hack Solidity playlist.

Smart Contract Security Challenges (Capture the Flags)

After learning the basics, you're going to need to practice your skills. This will form the core of your experience. The most common way to practice is with Capture the Flags (CTFs), which are challenges/games to learn security concepts. I have linked each CTF's site but without embeds, as that would take up too much space.

I recommend doing them in this order:

Ethernaut/CaptureTheEther -> Damn Vulnerable DeFi -> Paradigm CTF (One of the hardest out there created by Paradigm and notably samczsun, DeFi's most legendary security researcher. You can read Immunefi's interview with him here.)

Ethernaut/Capture the Ether overlap, so you can do one over the other. Damn Vulnerable DeFi requires understanding of DeFi implementations, as the solutions mainly lie in breaking the business logic of the smart contracts. As for Paradigm, I'm not sure, as I haven't tried it yet.

If you get stuck, plenty of write-ups exist, but I can vouch for Web3 Blockchain Developer's videos when it comes to Ethernaut. They're very detailed and walk you through the logic of the smart contracts, so they're excellent for learning.

Web3 Blockchain Developer

Hey, my name is Mark Muskardin and I'm helping developers learn blockchain development for Ethereum. I developed the…

www.youtube.com

For Damn Vulnerable DeFi, Smart Contract Programmer has you covered.

Paradigm has Christoph Michel.

Paradigm CTF 2021 Solutions

Paradigm CTF 2021 was a 48-hour Ethereum focused security competition held over the last weekend. It consists of 17…

cmichel.io

Real World Experience

This is your next step. You can and should hunt for bugs on Immunefi, which hosts a multitude of bug bounty programs, featuring a total reward amount of over $61 million dollars.

Immunefi

Review code. Prevent hacks. Build rep. Get paid.

immunefi.com

Finally, I encourage you to apply to the various smart contract security firms, as there's an extremely high demand for people like you. The experience requirements aren't as demotivating as more traditional security roles (5 years of cybersecurity experience for an entry-level job, am I right?) Bonuses? The salary is pretty good, and the roles are mostly remote.

Staying Ahead in the Web3 Hackspace

DeFi moves blazingly fast, and it's easy to lose your footing. Luckily, the following news providers will help keep you informed about the latest hacks and their technical breakdowns.

Immunefi

Immunefi is the premier bug bounty platform for smart contracts and DeFi projects, where security researchers review…

medium.com

Rekt - Home

DeFi / Crypto - Investigative journalism & creative commentary

rekt.news

Blockchain Threat Intelligence | Peter Kacherginsky | Substack

The latest in blockchain, DeFi and cryptocurrency threat intelligence, vulnerabilities, security tools, and…

www.blockthreat.io

Week in Ethereum News

Eth News and Links EIPs/Standards EIP4521: ERC721/20-compatible transfer EIP4546: Wrapped Deposits EIP4573: Entry…

weekinethereumnews.com

The Daily Gwei

Daily commentary on the Ethereum ecosystem.Click to read The Daily Gwei, by Anthony Sassano, a Substack publication…

thedailygwei.substack.com

Tying it all Together:

freeCodeCamp course -> Chapters 1, 2, 3, 4, 5, 6, 13 and 14 in Mastering Ethereum

(Optional) -> CryptoZombies -> Hack Solidity -> Smart Contract Security Chapter in Mastering Ethereum (Optional) -> SWC registry -> Secureum bootcamp -> CTFs -> Real life experience/job.

Note: It may be worthwhile to incorporate the Secureum bootcamp videos as part of your learning from the very beginning. I personally skipped the Ethereum and Solidity modules as I had already completed the freeCodeCamp course and read the corresponding chapters in Mastering Ethereum

.

5. Why Did I Choose Blockchain?

Why did I choose to specialize in blockchain security over other disciplines?

Aside from what we covered in our introduction, I'd be lying if I said I wasn't vaguely attracted to the prestige that came with being one of the very first 1337 Web3 hackers.

Web2 and other disciplines have had time to mature, and so have the hackers who have secured and hacked it. Why become just another face in the crowd of elites when you can learn what they don't know or are unwilling to see as relevant, due to their hubris?

A hacker is meant to be ever-curious about technology, how it works, and how to make it do the unexpected. In that respect, you and I have succeeded. I'm proud of you for making it this far, Anon. May you soar to new heights and have your name echoed through the decentralized web.

The opportunities in more traditional branches of cybersecurity are full of frantic competition. We all know that one friend who's been trying to break into the industry for ages — an industry that expects 5 years of experience for entry-level pay, alongside certifications worth thousands of dollars. And everyone wonders why there's a shortage of professionals…

Since switching to blockchain security, not many have asked for more than a year of experience or any fancy certifications. Hell, I never used to get offers to join any firms at all, but thanks to my awesome friends and mentors, there's an opportunity to join some of DeFi's greatest security firms. That's something that means so much to me and something I'll never forget. All I have to do is get past the gatekeeper that is myself and prove to myself that I can do the job. :)

Blockchain security is the only place where a broke kid like me felt at home, whether that was with the people who were experts at it or the opportunities that were laid out before me, and I pray that's the same for you.

6. Acknowledgements

I'd like to take a moment to thank everyone who helped make this article possible.

First off and most important is Halborn's Lead Offensive Security Engineer Timur Guvenkaya for setting aside time from his busy schedule to speak with me about getting started and continuously guiding me as I pestered him with silly questions. In the beginning of my studies, he was indeed the only one who didn't write me off as a waste of time and for that, I am eternally grateful. Without him, I'm not sure if I would've stepped into this full-time, and I doubt this article would be here. ❤

Immunefi's DeFi Security Triager Adrian Hetman for encouraging me to join the Immunefi community and occasionally mentoring me when it came to DeFi. Even the subtle requests and encouragement to join Immunefi for a full-time career. :)

Immunefi's community lead Jonah Michaels for facilitating the release of this article on Immunefi's Medium publication.

Immunefi's whitehat hackers ckksec and Jah for sharing their journeys with me for additional paths on becoming a DeFi hacker. Unfortunately, I elected to leave that out as the article is already too long but feel free to request for a follow up on their stories/how the white hat scholars became well…scholars XD.

Wenqing Yan aka Yuumei for her awe-inspiring art sprinkled throughout this publication. All her pieces inspired colourful worlds offering brief and wondrous escapes from reality. I'm especially grateful for Fisheye Placebo (a story about a young group of activists and hacktivists) that acted as one of the catalysts in my hacker journey. You can read it down below:

Fisheye Placebo - Yuumei

Technology is the tool. It gives power to the people, and gives power to control the people. For those born into this…

www.yuumeiart.com

I'd also like to thank all of the content creators and security firms referenced in this piece. Thank you for your work in giving back to the community and helping secure Web3.

Lastly, I'd like to thank you for making it to the end and taking the first step in your journey to becoming a DeFi hacker. Feel free to tag me on Twitter to let me know about your progress and pester me with requests for more technical pieces/videos if you wish. Given enough pressure, I'm sure I'll crack and give in. ;)

The DeFi world is now yours for the taking. I'm sure you will do well with the knowledge I have given you. Remember, with great power comes great responsibility.