# SEC554: **Blockchain and Smart Contract Security**

| 3 Day Course | 18 CPEs | Laptop Required |
|---|---|---|

### You Will Be Able To

- Compile and deploy smart contracts
- Exploit vulnerable smart contracts, nodes, and private keys
- Run automated security scans on smart contracts
- Use the latest blockchain tools for development, security, auditing, and exploiting
- Trace and discover blockchain transaction information
- Set up and protect a cryptocurrency wallet
- Crack partially exposed mnemonics keys
- Send transactions to blockchain
- Set up a local ethereum blockchain for testing
- Join a cryptocurrency mining pool, or create your own mining node
- Run static analysis on EVM bytecode
- Interact with cryptocurrency on main and test networks
- Investigate, install, and prevent crypto-jacking malware
- Protect and defend against privacy attacks on blockchain

**"SEC554 gives an excellent education on the next big technological revolution, taught by the folks on the front lines."**

—Ravi Danesh, **BMO Financial Group**

In 2008, an anonymous author, under the pseudonym Satoshi Nakamoto, published a white paper outlining a public transaction ledger for a decentralized peer-to-peer payment system entitled Bitcoin: A Peer-to-Peer Electronic Cash System, which is regarded as the "birth" of blockchain. Since then, the use of blockchain has evolved beyond its original implementation as a cryptocurrency. It has gained momentum in recent years, being adopted by some of the largest organizations in the world, including IBM, Amazon, PayPal, Mastercard, and Walmart. However, due to the relative newness of blockchain compared to more understood and traditional technologies, its use is still hindered by speculation, confusion, uncertainty, and risk.

In SEC554: Blockchain and Smart Contract Security, you will become familiar with essential topics of blockchain and smart contract technology, including its history, design principles, architecture, business use cases, regulatory environment, and technical specifications. The course takes a detailed look at the mechanics behind the cryptography and the transactions that make blockchain work. It provides exercises that will teach you how to use tools to deploy, audit, scan, and exploit blockchain and smart contract assets. Hands-on labs and exercises will enable you to interact with various blockchain implementations, such as ethereum and bitcoin, and you'll be provided with resources to take with you to further explore.

There have already been widespread security breaches, fraud, and hacks on blockchain platforms, resulting in billions of dollars in losses. These issues, along with growing scrutiny by government agencies to find malicious users abusing the technology, is tarnishing blockchain's reputation. SEC554 approaches blockchain and smart contracts from an offensive perspective to inform students what vulnerabilities exist, how they are exploited, and how to defend against attacks that are currently leveraged today. Some of the skills and techniques you will learn are:

- How to interact with and get data from public blockchains
- How to exploit several types of smart contract vulnerabilities
- How to test and exploit weak cryptography/entropy
- How to discover and re-create private keys
- What cryptojackers do and how to trace and track movements on blockchain
- How to combat non-technical or social engineering types of attacks that adversaries use to access and steal from victims

We can see the many solutions blockchain technology can provide as a payment system, but as the technology is increasingly adopted, its attack surface will continue to grow. While there are some educational resources available for blockchain, there is relatively little educational content around blockchain security. No other training provides the comprehensive level of blockchain testing, exercises and knowledge that is delivered in SEC554.

### Author Statement

"Blockchain is a revolutionary solution that solves multiple issues inherent in the social, economic, and technological challenges we face today. Decentralization and self-sovereignty are not just concepts, but fundamental ideals that should be made available and accessible for all to benefit from. But those processes need to be carried out responsibly and securely. In order to drive adoption, security must be a priority for all developers, users, or speculators interacting with blockchains or smart contracts. I've always thought the best way to protect something is to learn how to break it."
—Steven Walbroehl

# Section Descriptions

### SECTION 1: Blockchain Fundamentals

The first course section begins by establishing the fundamentals of blockchain technology and how it is applied to real-world problems. The most important technical aspects that make up blockchain architecture are discussed, along with examples and case studies. Students will generate public and private key pairs used by blockchain, create different type of cryptocurrency wallets, deep-dive into the different consensus mechanisms that make blockchain a decentralized system, learn how crypto currency mining works, and investigate what happens during transactions. The section will feature scenarios and exercises to send and receive blockchain transactions, and students will see live transactions on the public chain through various block explorers. We'll also look at smart contract technology and walk through examples of how it is applied today in various industries and market use cases.

**TOPICS:** What Is Blockchain?; What Is a Smart Contract?; Keys, Wallets, and Cryptography; Consensus Mechanisms; Blockchain Transactions; Blockchain Components

### SECTION 2: Blochchain Security – Attacks and Defenses

After the technical blockchain fundamentals are established and have become familiar to students, section two of the course builds on that knowledge with a focus on security topics scoped to blockchain systems such as the bitcoin network. Students will learn the security principles that make blockchain different from traditional technology systems, and then begin to discover some of the weaknesses in a blockchain system and how they are attacked. We'll spend time learning and using blockchain security tools that exploit private keys and users, and the common mistakes people make when using them. We'll also take a deep dive on how privacy can be compromised and used by adversaries or government agencies to monitor and identify user activity. Dark net markets have been one of the most notorious uses of cryptocurrencies, and this course section will also provide information on how these markets differ from the normal Internet, why they are used for illegal purposes. We'll also examine privacy crypto like monero, as well as the regulations enforced by agencies to prevent criminal activity. Finally, students will discover and attempt other malicious uses of blockchain, such as crypto-jacking.

**TOPICS:** The Bitcoin Network and Security Overview; Weaknesses and Vulnerabilities; Attacks on Private Keys; Attacks on Privacy; Malicious Uses of Blockchain; Regulatory Compliance and Investigation

### SECTION 3: Smart Contract Security – Vulnerability and Exploits

The final course section focuses on the security aspects of the most widely used smart contract platform, ethereum. Smart contracts differ in architecture from blockchains such as bitcoin because of their multi-purpose implementations. Developers write smart contracts in languages such as Solidity, which often contain bugs and vulnerabilities. The vulnerabilities can be exploited on the public main-net and cause massive amounts of financial and reputational damage. We'll introduce the ethereum smart contract programming language, Solidity, and examine how to compile, deploy, and interact with smart contracts locally and remotely. Then, after students are familiar with the development process from using tools like Truffle and Ganache, we'll deep-dive into the common ethereum vulnerabilities and walk through case studies of how they have been exploited in the past. Several tools and scanners, such as Slither, Mythril, and Remix, are provided for students to identify and validate these vulnerabilities. Finally, after students learn how to identify a smart contract vulnerability, we'll attack and exploit a custom smart contract on a locally created ethereum network deployed by the students.

**TOPICS:** The Smart Contract Lifecycle; Solidity; Smart Contract Vulnerabilities; Attacking and Exploiting Smart Contracts; Conclusion

**"SEC554 provided great foundational knowledge around blockchain security. Anyone interested in learning blockchain security should be able to go through this material and have a solid understand of how Bitcoin works."**

—Beau Bullock

### Who Should Attend

- Smart contract developers
- Blockchain developers
- Security engineers, architects, or analysts whose companies are creating blockchain or smart contract applications
- Penetration testers interested in expanding their set of skills to newer technologies, and in getting a head start on an emerging new discipline in security
- Compliance officers tasked with validating and investigating implementations that involve blockchain or smart contracts
- Executives or managers who are starting projects that involve blockchain or smart contracts and need to understand the technology, security issues, and mitigations involved
- Employees of government agencies who want to expand their knowledge and skills of blockchain networks
- Cryptocurrency users who want to learn how to protect their transactions, investments, and privacy

**"Amazing and unique one-of-a-kind course. No other learning experience quite like this one... wish there was more!"**

—Yenny Angzas, **BlockOne**