IEEE

IEEE SMC 2023
Maui, Hawaii

IEEE SMC Systems, Man, and Cybernetics Society

IEEE SMC 2023
International Conference on Systems, Man, and Cybernetics
Maui, Hawaii, October 1- 4, 2023
"Improving the Quality of Life"

Tutorial

Title

Ethereum Smart Contract Development

Abstract

Smart contract introduced by Ethereum opened the door for the development of various decentralized applications and even decentralized autonomous organization. This tutorial consists of four parts: (1) introduction to blockchain; (2) programming smart contract with Solidity; (3) advanced topics in smart contract development; and (4) vulnerabilities and attacks on smart contracts. Part I will cover the history, the fundamental design principles, and the nuts and bolts of the blockchain technology, including keys, addresses, transactions, blocks, cryptographic primitives, proof-of-work, proof-of-state, and double-spending attacks. Part II will cover the basic of the Solidity programming language and the development environment for smart contracts. Part III will cover several advanced topics in smart contract development, including the application binary interface, the design patterns for smart contracts, and how to save on gas consumption in smart contract. Part IV will cover the incidents that have happened to poorly designed smart contracts in Ethereum, the attack vectors, and the best practices in securing smart contracts.

Duration

Two hours

Motivation -

Smart contract introduced by Ethereum opened the door for the development of various decentralized applications (Dapps) and even decentralized autonomous organization. As such, we have seen huge number of Dapps being developed. For example, over 10,000 Dapps are tracked by dappradar.com. We have also seen huge interest from the research community. For example, a search for “smart contract” on Web of Science Core Collection returned 15,923 papers. Therefore, a tutorial on smart contract could be of interest to many participants of SMC 2023.

Expected audience

IEEE SMC 2023 participants who are interested in learning about Ethereum smart contracts.

Outline of contents

This tutorial consists of four parts: (1) introduction to blockchain; (2) programming smart contract with Solidity; (3) advanced topics in smart contract development; and (4) vulnerabilities and attacks on smart contracts.

<u>Part I. Introduction to blockchain</u>

This part will cover the history, the fundamental design principles, and the nuts and bolts of the blockchain technology. More specifically, this part consists of the following topics:

- The components in the blockchain that are easily visible, such as security keys, addresses, signatures, transactions, blocks, and blockchain.
- How smart contract is supported in Ethereum
- Security mechanism: cryptographic hash, public key algorithms, digital signatures
- Decentralized consensus: A general model. This model captures the essential requirements on decentralized consensus. Any decentralized consensus algorithm must offer a stochastic process in selecting the next block and must offer a rule to reconcile conflicts when two or more nodes both win the new block creation competition.
- Decentralized consensus: Proof-of-Work (PoW)
- Decentralized consensus: Proof-of-Stake (PoS)

Part II. Programming smart contract with Solidity

This part will cover the basic of the Solidity programming language, the development environment for smart contract. More specifically, this part consists of the following topics:

- Structure of a smart contract
- Variables, operators, statements, and modifiers in smart contracts
- Events in smart contracts
- Smart contract inheritance
- Smart contract development environment: Truffle Suite and Ganache
- Smart contract application development using Javascript and Python

Part III. Advanced topics in smart contract development

This part will cover several advanced topics in smart contract development. More specifically, this part consists of the following topics:

- Application binary interface
- Design patterns for smart contracts
- How to save on gas consumption in smart contracts
- Assembly in smart contracts
- Deconstruct smart contrasts
- Developing decentralized applications

Part IV. Vulnerabilities and attacks on smart contracts

This part will cover in incidents that have happened to poorly designed smart contract in Ethereum, the attack vectors, and best practices in securing smart contract. More specifically, this part consists of the following topics:

- History of attacks on Ethereum smart contracts
- Solidity related attacks
- Platform related attacks
- Reentry related attacks
- Denial of service attacks
- Best practices in securing smart contracts

Key references

1. Zhao, W. (2021). From Traditional Fault Tolerance to Blockchain. John Wiley & Sons.
2. Zheng, G., Gao, L., Huang, L., & Guan, J. (2020). Ethereum smart contract development in solidity. Springer Nature.
3. Zhao, W., Yang, S., & Luo, X. (2019, March). On consensus in public blockchains. In *Proceedings of the 2019 International Conference on Blockchain Technology* (pp. 1-5).
4. Zhao, W., Yang, S., Luo, X., & Zhou, J. (2021, March). On peercoin proof of stake for blockchain consensus. In 2021 The 3rd International Conference on Blockchain Technology (pp. 129-134).
5. Zhao, W. (2022). On Nxt Proof of Stake Algorithm: A Simulation Study. IEEE Transactions on Dependable and Secure Computing.

6. Zhao, W. (2022). On Blockchain: Design Principle, Building Blocks, Core Innovations, and Misconceptions. IEEE Systems, Man, and Cybernetics Magazine, 8(4), 6-14.
7. Gürsoy, G., Brannon, C. M., & Gerstein, M. (2020). Using Ethereum blockchain to store and query pharmacogenomics data via smart contracts. BMC medical genomics, 13(1), 1-11.
8. Kuo, T. T., Bath, T., Ma, S., Pattengale, N., Yang, M., Cao, Y., ... & Ohno-Machado, L. (2021). Benchmarking blockchain-based gene-drug interaction data sharing methods: a case study from the iDASH 2019 secure genome analysis competition blockchain track. International journal of medical informatics, 154, 104559.
9. Kushwaha, S. S., Joshi, S., Singh, D., Kaur, M., & Lee, H. N. (2022). Systematic review of security vulnerabilities in ethereum blockchain smart contract. IEEE Access, 10, 6605-6621.
10. Rouhani, S., & Deters, R. (2019). Security, performance, and applications of smart contracts: A systematic survey. IEEE Access, 7, 50759-50779.

List of speakers

Wenbing Zhao

Department of Electrical Engineering and Computer Science
Cleveland State University
2121 Euclid Ave., FH317, Cleveland, OH 44115, USA
Phone: 216-523-7480
Email: w.zhao1@csuohio.edu

Short bio: Dr. Zhao is a Full Professor at the Department of Electrical Engineering and Computer Science, Cleveland State University (CSU). He earned his Ph.D. at University of California, Santa Barbara, under the supervision of Drs. Moser and Melliar-Smith, in 2002. Dr. Zhao has been doing research on distributed systems since 1998. His research was sponsored by various US federal and state agencies, including the US National Science Foundation, the US Department of Energy, the UD Department of Education, the US Department of Transportation, the Ohio Bureau of Workers' Compensation, the Ohio Department of Higher Education, and the Ohio Development Services Agency. Dr. Zhao currently has an active research grant with Department of Energy on using blockchain technology to secure IoT sensing and data processing for power plants. Dr. Zhao authored a book on blockchain titled “From Traditional Fault Tolerance to Blockchain.” Dr. Zhao has over 250 peer-reviewed publications. He has served on several research panels for the US National Science Foundation. Furthermore, he has served as the Keynote Speaker, Tutorial Speaker, General Chair or Program Chair for several international conferences, and has served as a member of the technical program committee for many IEEE conferences. In recent years, Dr. Zhao has been working on blockchain consensus and the integration of blockchain in various applications.