Hacking The (Smart) Contract

Dev Mountain Tech Festival 2022
19 March 2022

<DEV> MOUNTAIN TECH FESTIVAL

ValiX Consulting

Speaker Profile

Education and Qualifications

- Master of Engineering (Computer Security), Prince of Songkla University
- Bachelor of Engineering (Computer Network), Prince of Songkla University
- Research student, National Ilan University, Taiwan

Phuwanai Thummavet

Background

Phuwanai is a lead smart contract auditor and blockchain security consultant. He specialized in blockchain development projects with over four years of experience. He was a Chief Technology Officer and Blockchain Developer who is specialized in Hyperledger Fabric and Ethereum blockchains. He have experience in developing blockchain software in several domains, including auction, logistics, IoT, and renewable energy. Furthermore, he was a blockchain technical and solutions consultant for one of the biggest agricultural companies in Thailand.

Throughout the past few years, he dedicated himself to develop a blockchain society in Thailand. He have written technical articles, spoken in public events, recorded an interview podcast, and even taught public and private courses regarding Hyperledger and Ethereum. He is also a core staff who organized many blockchain events in Thailand.

Professional and Industry Experience:

- Spoke on “Blockchain x Cryptocurrency ใช้อย่างไรให้ธุรกิจ Work” in SPARK STSP Innovation Fair 2022
- Spoke on “Hacking The (Smart) Contract For Developers” in Valix Security Conference
- Spoke on “Demystifying Hyperledger Fabric Blockchain with Example DApp” in Code Mania 1010
- Spoke on “Deep dive into LibraBFT consensus” in Libra Developer Meeting #1
- Was a guest interview on the launch of Hyperledger Fabric v2 for BitCast (EP14)
- Organized the Pizza Hackathon 2018, the first blockchain hackathon in Thailand
- Consulted for Blockchain-based projects for one of the biggest agricultural companies in Thailand
- Developed an energy market platform based on Hyperledger Fabric
- Developed a car auction system based on Hyperledger Fabric
- Developed a container delivery system based on Hyperledger Fabric
- Developed a geographical information system based on Hyperledger Fabric
- Developed a katinrun fundraising platform based on Ethereum
- Developed a private katinrun foundation token system based on Ethereum
- Developed the RTHB-ThaiBahtCoin, the demonstration of thai baht stable coin based on Ethereum and RSK
- Developed the PizzaCoin, the voting system based on Ethereum

Outline

1. Background and Experience
2. Working With Us
3. Learn Smart Contract Security By Hacking

ValiX Consulting

Background and Experience

Why Choose Valix

Security Professionals

Valix has a team with deep cyber security, blockchain security and consultancy experience. This gives us unique insights into the challenges that you face, and ensures we provide recommendations based on real-world experience. In addition, we have extensive experience in the blockchain development both public and private blockchain technologies. We will use this experience to help client avoid pitfalls and, using tried and tested approaches, rapidly resolve the challenges you face.

Independent and Commit Your Long-Term Goals

Valix brings a fresh, independent perspective and a passion to do an outstanding job. Our team structured, approach and deliverables are based on the simple notion that the success of this project is measured by the results obtained and not just successful completion. We want to be a true partner for you rather than simply acting as a service provider.

Service Quality

Valix deeply conducts security audit with our approaches; Static and Dynamic (Run-time) analysis, not just using an automated tools but manually analyzing the smart contracts code line-by-line in order to understand the application logic for identifying its vulnerabilities. Our holistic methodology is based on well-known industry standards; SWC Registry, CWE, Consensys best practice, and cover the latest exploitation cases.

Main Professional Services

ValiX

Smart Contract Security Audit

We provide a service for **assessing and certifying the security of smart contracts**. Our service also includes recommendations on smart contracts' security and gas optimization to bring the most benefit to users and platform creators.

Web3.0 Security Assessment

The web3.0 audit methodology is based on Smart Contract Weakness Classification and Test Cases (SWC Registry), CWE, Consensys best practice, and penetration testing approach. **The scope of work will be in 2 parts: Off-chain and On-chain transaction**. We will conduct smart contract auditing service for on-chain assessment and black box and gray box penetration test for off-chain system. We found that several platform are vulnerable because of their **insecure Off-chain system**.

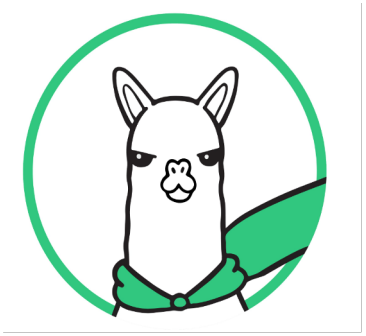
Full-Stack Security Consulting

We provide services for **assessing and analyzing the security of on-chain smart contracts and off-chain related systems**, studying potential breaches, and supervising the implementation of secure smart contract platforms.

SWC Registry | CONSENSYS MythX | NIST National Institute of Standards and Technology U.S. Department of Commerce | CVE | CWE | NVD

Featured Clients

ValiX



Alpaca Finance

Grazing Range

Warden Finance

Best Rate Swap

Vonder Finance

Yield Farming

Play to Earn Finance

NFT Marketplace

NFT & GameFi

Public Advisories (1/2)

Biswap

- **Business Type:** Yield Farming (with Transaction Fee Mining)
- **Networks:** BSC
- **Vulnerabilities:**
  - **Draining a total of 100 million BSW tokens (out of 700 million total supply)** allocated for the transaction fee mining with no actual trading fee to pay
  - **Impersonating any user's transaction**

- **Discovery report by Valix:** https://medium.com/valixconsulting/biswap-discovery-of-critical-vulnerability-on-biswaps-swap-function-ff2799f96c32

Public Advisories (2/2)

SushiSwap

- **Business Type:** Yield Farming
- **Networks:** Ethereum, BSC, Polygon, Arbitrum, etc.
- **Vulnerabilities:**
  - **Design flaws under the voting mechanism of the SUSHI token**
    - Voting Amplification Attack
    - Voting Displacement Attack
    - Redelegation Failure

- **Discovery report by Valix:** https://medium.com/valixconsulting/sushiswap-voting-vulnerability-of-sushi-token-and-its-forks-56f220d4c9ba

ValiX Consulting

Working With Us

We Are Hiring!!

ValiX

Junior/Senior Smart Contract Auditors

- Proficiency in Solidity language
- Proficiency in other programming languages, such as JavaScript/Node.js, Golang, Python, Rust, C++, is a plus
- Experience in back-end development, algorithms, and data structures
- Knowledge of cryptography and blockchain protocols
- Knowledge of best practices in blockchain development and data protection

We Are Hiring!!

Contact Us

- **Twitter:** @ValixConsulting
- **Facebook:** fb.com/ValixConsulting
- **Medium:** medium.com/valixconsulting
- **E-mail:** info@valix.io

ValiX Consulting

Learn Smart Contract Security By Hacking

Contact Us

For further information kindly E-mail to:
info@valix.io