



INSTITUTE OF
BLOCKCHAIN™
— **SINGAPORE** —

区块链学院 (新加坡)

UEN: 201801117M

(Incorporated in the Republic of Singapore)

IBS-03 Blockchain & Cryptography Syllabus

About Institute

Institute of Blockchain™ (Singapore), UEN: 201801117M) was founded on Jan 2018. We are a blockchain and EduTech private school with a primary focus on delivering blockchain education and certification. Secondary focus on blockchain research & development.

The Institute is a SkillsFuture Singapore's approved Non-WSQ Training Organisation, NTUC e2i's approved Training Provider and People's Association approved Private Operator, a registered Singapore government's Gebiz supplier and is a graduated start-up from the Alibaba Cloud-SUSS Entrepreneurship Programme.

As part of our CSR efforts, we joined the NVPC's Company of Good and adopted Singapore Children's Society as our official charity. Our strategic partners are DIFY, SUSS, Edufied, IBM Academic Initiative and Justicius Law Corporation and our past corporate clients include Deloitte, GCOX, ERA, Ninecoin (Hongkong), Tuandai (Guangzhou) and Singapore Customs.

About Lecturer

Mr Jordan Seet is an Associate Lecturer with IBS. Having been in the cybersecurity space since 2013, Jordan has gotten numerous placings and medals in CTF (Capture-the-flag) competitions. A ConsenSys Academy Developer Scholarship holder, he has worked on various Ethereum-based projects and is passionate about understanding Distributed Ledger Technology and its applications on society.

He pioneered SMU Blockchain, the first University Blockchain club in Singapore as Technology Director and is involved in various crypto-millennial groups. Currently doing blockchain protocol layer research for Jupiter Chain as well as hacking smart contracts.

Course Preface

Participants will:

- Learn the concepts various cryptography and encryption methods.
- Relate cryptography to Blockchain & Cryptocurrency use cases
- Understand the importance of Cryptography in Blockchain systems.

Course Content

1. Introduction to Cryptography
2. Intro to the laws of cybersecurity
3. Obscurity vs Open Source
4. Security by Legislation
5. Security Trilemma
6. Hashing introduction
7. Hash functions
8. How does Hashing work?
9. Broken Hashes
10. How does hashing work in Bitcoin?
11. Why does Ethereum use Keccak256?
12. Birthday Paradox
13. Is Crypto safe?
14. What about Quantum Computers?
15. Introduction to Encryption
16. Symmetric Cryptography
17. Stream Ciphers
18. Stream Ciphers
19. Cipher Techniques
20. Block Ciphers: DES
21. Block Ciphers: AES
22. Block Cipher modes
23. Asymmetric Cryptography
24. Enveloped Encryption
25. Use Cases in Blockchain
26. RSA Signature
27. ECDSA
28. ECDSA vs RSA
29. Ethereum Verification
30. Multisig wallets
31. Parity Multisig attack
32. MEW attack

- 33. How did Silk Road founder get caught?
- 34. Crypto use cases
- 35. Anonymity in Blockchain
- 36. Security in sharing economies
- 37. Discussion on potential of Cryptography and Blockchain

Course Administrative

Programme Mode: Part-Time

Part Time Duration: 3 weekday sessions (7pm to 10pm) – With 1 short break.

Class Size: 10 to 20 (minimum 15 to start)

Course Fees (per pax): \$278 (Local Rate) / \$360 (Overseas)

Language Medium: English

Certification

An Electronic Certificate of Completion will be issued on NEM Blockchain to participants who achieved at least 75% attendance, pass the assessment with a score of 50% and above and completed the end of course survey,

Please indicate the correct name during registration for certificate issuing. The Institute is not responsible for any wrong name indicated and may refuse to issue a subsequent certificate.

Progression

This is a 2 Block Units module which leads to a full Certificate/Diploma in Blockchain Technology.

Assessment

Course participants are given **1 hour** to attempt an assessment comprising of 30 Multiple-Choice Questions. To pass the assessment, the participant needs to score **50%** and above. For scoring 49% and below, participants have up to **ONE** attempt to re-take the assessment at no additional fee. In the event, the participant fails again, he/she shall repeat the respective module

Course Enquiry / Support

Email: admin@ibs.edu.sg

Phone: +65 6717-7722 or +65 8292 8452 (WhatsApp/LINE/Telegram/WeChat)