CORSO AVANZATO

PROGRAMMA DIDATTICO

BOOTCAMP BLOCKCHAIN - WEB3

INTRODUZIONE ALLA PROGRAMMAZIONE DECENTRALIZZATA

- Basi di crittografia
- La catena di blocchi
- Il consenso su una rete decentralizzata
- Gli smart contract
- Blockchain pubbliche e private - i “DLT”

IL MONDO ETHEREUM / SOLIDITY (~60 ORE)

- Il processo di standardizzazione di Ethereum (EIP, ERC)
- La Ethereum Virtual Machine (EVM)

1. Un’ampia scelta di blockchain con architetture e audience diverse (Ethereum, Polygon, Flare, BSC, ...)
2. Introduzione al linguaggio Solidity

CORSO AVANZATO

PROGRAMMA DIDATTICO

BOOTCAMP BLOCKCHAIN - WEB3

IL MONDO ETHEREUM / SOLIDITY (~60 ORE)

- Gli strumenti base: Remix, Visual Studio Code, Hardhat
- La programmazione ad oggetti in Solidity

1. Ereditarietà e composizione
2. Richiamare altri contract in ottica “library”

- Le librerie “foundation” - OpenZeppelin
- Design Pattern in Solidity

1. Behavioural: Guard Check, State Machine, Oracle, Randomness
2. Security: Access restriction, Secure Transfer, Pull over Push, Emergency Stop
3. Upgradeability: Proxy Delegate, Eternal Storage, Diamond
4. Economic: String Equality, Tight Variable Packing, Memory Array Building

CORSO AVANZATO

PROGRAMMA DIDATTICO

BOOTCAMP BLOCKCHAIN - WEB3

IL MONDO ETHEREUM / SOLIDITY (~60 ORE)

- I Token Fungibili (ERC-20)
- I Token Non fungibili - NFT

1. ERC-721 (token non fungibile)
2. ERC-1155 (token semi-fungibile)
3. ERC-2981 (Le Royalties)
4. Apertura degli NFT verso altri marketplace

- Le vulnerabilità

1. Dati confidenziali in blockchain
2. Integer overflow and underflow
3. Return value unchecked
4. Attacchi Re-entrancy
5. Attacchi Denial Of Service
6. Attachi Front Running
7. Attacchi Replay signature
8. Visibilità di default delle funzioni
9. Floating pragma
10. Loop su array lunghi
11. Wrong inheritance
12. Ether Balance non atteso
13. Violazione dei limiti di un array

CORSO AVANZATO

PROGRAMMA DIDATTICO

BOOTCAMP BLOCKCHAIN - WEB3

IL MONDO ETHEREUM / SOLIDITY (~60 ORE)

14. Chiamate delegate verso sorgenti non fidate sources
15. Chiamate (regolari) verso sorgenti non fidate
16. Insecure randomness
17. Block Timestamp manipulation
18. Contratti zero-code
19. Puntatori a storage non inizializzati
20. Smart contract non aggiornabili (upgradable)
21. Logica di inizializzazione

- Il test degli smart contract

1. Unit Testing
2. Il Fuzzing (Echidna)
3. Solcover
4. Hardhat
5. Gas Reporter

CORSO AVANZATO

PROGRAMMA DIDATTICO

BOOTCAMP BLOCKCHAIN - WEB3

ETHEREUM/EVM E APPLICAZIONI WEB3

- La libreria Ethers.js
- Altre librerie Web3
- Wagmi (framework per la connessione React ↔ Web3)
- Approfondimento interazione Server ↔ Blockchain (Node/Ethers.js)
- Approfondimento interazione Client ↔ Blockchain (Wagmi/Metamask/altri wallet)

DLT / BLOCKCHAIN PRIVATE / ALTRE BLOCKCHAIN

- DLT e blockchain private - applicabilità, vantaggi, svantaggi
- DLT e blockchain private - casi d'uso nel contesto enterprise
- Panoramica sulle architetture e sul funzionamento di altre blockchain pubbliche

1. Bitcoin / Algorand
2. Solana
3. EOS / Antelope

- Hyperledger Fabric (12 ore con approfondimento pratico)

CORSO AVANZATO

PROGRAMMA DIDATTICO

BOOTCAMP BLOCKCHAIN - WEB3

PROGETTO DI FINE CORSO - 60 ORE

- Sviluppo di un ecosistema decentralizzato utilizzando i concetti appresi nel corso del modulo 2
- Approfondimento end-to-end dell'utilizzo interoperabile di

1. DLT ad alte prestazioni in ambiente consortile / inter-aziendale / privato
2. EVM latency-resilient in ambiente pubblico