Corso Avanzato

PROGRAMMA DIDATTICO
BOOTCAMP BLOCKCHAIN - WEB3

Modulo 1: 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”

Modulo 2: IL MONDO ETHEREUM / SOLIDITY

- Il processo di standardizzazione di Ethereum (EIP, ERC)
- La Ethereum Virtual Machine (EVM)
    - Un’ampia scelta di blockchain con architetture e audience diverse (Ethereum, Polygon, Flare, BSC, …)
    - Introduzione al linguaggio Solidity

Modulo 3: IL MONDO ETHEREUM / SOLIDITY

- Gli strumenti base: Remix, Visual Studio Code, Hardhat
- La programmazione ad oggetti in Solidity
    - Ereditarietà e composizione
    - Richiamare altri contract in ottica “library”
- Le librerie “foundation” - OpenZeppelin
- Design Pattern in Solidity
    - Behavioural: Guard Check, State Machine, Oracle, Randomness
    - Security: Access restriction, Secure Transfer, Pull over Push, Emergency Stop
    - Upgradeability: Proxy Delegate, Eternal Storage, Diamond
    - Economic: String Equality, Tight Variable Packing, Memory Array Building
- I Token Fungibili (ERC-20)
- I Token Non fungibili - NFT
    - ERC-721 (token non fungibile)
    - RC-1155 (token semi-fungibile)
    - ERC-2981 (Le Royalties)
    - Apertura degli NFT verso altri marketplace
- Le vulnerabilità
    - Dati confidenziali in blockchain
    - Integer overflow and underflow
    - Return value unchecked

    - Attacchi Re-entrancy
    - Attacchi Denial Of Service
    - Attachi Front Running
    - Attacchi Replay signature
    - Visibilità di default delle funzioni
    - Floating pragma
    - Loop su array lunghi
    - Wrong inheritance
    - Ether Balance non atteso
    - Violazione dei limiti di un array
    - Chiamate delegate verso sorgenti non fidate sources
    - Chiamate (regolari) verso sorgenti non fidate
    - Insecure randomness
    - Block Timestamp manipulation
    - Contratti zero-code
    - Puntatori a storage non inizializzati
    - Smart contract non aggiornabili (upgradable)
    - Logica di inizializzazione

Modulo 4: 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)

Modulo 5: 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. 2. 3.
    - Bitcoin / Algorand
    - Solana
    - EOS / Antelope
- Hyperledger Fabric (12 ore con approfondimento pratico)

Modulo 6: PROGETTO DI FINE CORSO

- Sviluppo di un ecosistema decentralizzato utilizzando i concetti appresi nel corso del modulo 2
- Approfondimento end-to-end dell'utilizzo interoperabile di
    - DLT ad alte prestazioni in ambiente consortile / interaziendale / privato
    - EVM latency-resilient in ambiente pubblico