

Especialista em Blockchain e Criptografia

Programa de Estudo

Duração: 12 meses

Unidade 10: Fundamentos de criptografia e segurança

Criptografia simétrica (AES) e assimétrica (RSA, ECC) Funções hash: SHA-256, Keccak-256 e suas propriedades Assinaturas digitais: ECDSA e verificação de integridade PKI (Public Key Infrastructure) e certificados digitais

Unidade 20: Arquitetura blockchain e redes distribuídas

Estrutura de um bloco: header, Merkle tree e nonce Mecanismos de consenso: Proof of Work, Proof of Stake e variantes Redes P2P: propagação de transações e blocos Bitcoin: modelo UTXO, scripting e Lightning Network

Unidade 30: Ethereum e programação com Solidity

Ethereum: contas, gas, EVM e o modelo de execução Solidity: tipos de dados, funções, modificadores e eventos Contratos ERC-20 (tokens fungíveis) e ERC-721 (NFTs) Hardhat/Foundry: ambiente de desenvolvimento e testes

Unidade 40: Segurança em contratos inteligentes

Vulnerabilidades: reentrancy, integer overflow, front-running Auditoria com Slither e Mythril Padrões seguros: checks-effects-interactions, pull payment Contratos upgradeable com OpenZeppelin Proxy

Unidade 50: DeFi: finanças descentralizadas

Protocolos DeFi: AMMs (Uniswap), lending (Aave/Compound), stablecoins Liquidity pools, yield farming e impermanent loss Oráculos de preço: Chainlink e manipulação de oráculos Flash loans: mecânica, usos legítimos e vetores de ataque

Unidade 60: NFTs, DAOs e Web3

Padrões NFT: ERC-721 e ERC-1155, metadata on-chain vs off-chain IPFS e Arweave: armazenamento descentralizado DAOs: governança on-chain com Governor Bravo e Snapshot Ethers.js: integração de wallets (MetaMask) em dApps

Unidade 70: Regulação, compliance e casos empresariais

Marco regulatório: MiCA (Europa), SEC, AFIP/SAT e criptomoedas KYC/AML em aplicações blockchain e exchanges Blockchain privada: Hyperledger Fabric e Quorum Casos de uso: supply chain e tokenização de ativos reais

Unidade 80: Projeto final: dApp completa em Ethereum

Design e arquitetura de uma aplicação descentralizada Desenvolvimento, testes e auditoria do contrato inteligente Frontend web3 com React + Wagmi + IPFS Deploy em testnet e apresentação do projeto de certificação

