Fundamentos de Blockchain e Criptografia

Programa de Estudo

Duração: 8 Semanas

Unidade 10: Fundamentos de criptografia e segurança

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

Unidade 20: Arquitetura blockchain e redes distribuídas

Estrutura de um bloco: header, Merkle tree e nonceMecanismos de consenso: Proof of Work, Proof of Stake e variantesRedes P2P: propagação de transações e blocosBitcoin: modelo UTXO, scripting e Lightning Network

Unidade 30: Ethereum e programação com Solidity

Ethereum: contas, gas, EVM e o modelo de execuçãoSolidity: tipos de dados, funções, modificadores e eventosContratos 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-runningAuditoria com Slither e MythrilPadrões seguros: checks-effects-interactions, pull paymentContratos upgradeable com OpenZeppelin Proxy