RBK Tunisia – Web3 Learning Journey

Overview

This Web3 Journey is designed as a **progressive learning path** for RBK Tunisia, structured into **three main sections**: **Introduction**, **Coding**, and **Auditing & Best Practices**. Each section is divided into **levels**, moving learners from foundational knowledge to advanced, real-world expertise. The journey is practical, industry-oriented, and aligned with current Web3 standards.

SECTION 1: INTRODUCTION TO WEB3

Objective: Build strong conceptual understanding of Web3, blockchain ecosystems, and decentralized technologies.

Level 1 – Web3 Fundamentals

- Web1 vs Web2 vs Web3
- Why Web3 matters: decentralization, trustless systems, ownership
- Overview of blockchain technology
- Public vs private blockchains
- Key terminology (block, node, consensus, gas, wallet, smart contract)

Outcome: Learners understand the Web3 landscape and core concepts.

Level 2 – Blockchain Architecture

- How blocks are created and validated
- Hashing & cryptography basics
- Merkle trees
- Consensus mechanisms:
    - Proof of Work (PoW)
    - Proof of Stake (PoS)
    - Delegated PoS (DPoS)
- Layer 1 vs Layer 2

Outcome: Learners understand how blockchains technically function.

Level 3 – Web3 Ecosystem & Use Cases

- Ethereum, BNB Chain, Polygon, Solana (overview)
- DeFi (DEXs, lending, staking)

- NFTs & digital ownership
- DAOs
- Real-world use cases (finance, supply chain, gaming, identity)

Outcome: Learners can identify where and how Web3 is applied.

Level 4 – Wallets & On-chain Interaction

- Hot vs cold wallets
- MetaMask & wallet security
- Public/private keys
- Transactions lifecycle
- Reading transactions on block explorers (Etherscan)

Outcome: Learners can safely interact with blockchain networks.

SECTION 2: CODING & SMART CONTRACT DEVELOPMENT

Objective: Enable learners to design, develop, deploy, and interact with smart contracts across **two major ecosystems**: **EVM-compatible blockchains** and **Solana**. Learners can follow one path or complete both.

SECTION 2A: EVM ECOSYSTEM (Ethereum & EVM-Compatible Chains)

Focus: Ethereum, BNB Chain, Polygon, Arbitrum, Optimism

Level 5A – Smart Contract Basics (EVM)

- What are smart contracts?
- EVM architecture overview
- Solidity introduction
- Contract structure
- Variables, functions, modifiers

Outcome: Learners can read and write basic Solidity smart contracts.

Level 6A – Solidity Deep Dive

- Data types & mappings
- Structs & enums
- Events & logs
- Error handling (require, revert, assert)
- Gas optimization basics

Outcome: Learners can develop structured and optimized EVM contracts.

Level 7A – EVM Development Environment

- Remix IDE
- Hardhat / Foundry
- Local blockchain (Ganache / Anvil)
- Writing unit tests
- Contract deployment workflows

Outcome: Learners can deploy and test EVM contracts locally.

Level 8A – EVM Token Standards

- ERC20 (fungible tokens)
- ERC721 (NFTs)
- ERC1155 (multi-token standard)
- Token economics & supply models

Outcome: Learners can build and deploy standard-compliant EVM tokens.

Level 9A – EVM dApp Development

- Frontend connection with Ethers.js / Web3.js
- Wallet integration (MetaMask)
- Reading & writing on-chain data
- Transaction signing & gas handling

Outcome: Learners can build full EVM-based decentralized applications.

SECTION 2B: SOLANA ECOSYSTEM

Focus: Solana blockchain, high-performance Web3 applications

Level 5B – Solana Fundamentals

- Solana architecture overview
- Proof of History (PoH)
- Accounts model vs EVM model
- Solana CLI & wallets (Phantom)

Outcome: Learners understand Solana's unique design and tooling.

Level 6B – Solana Smart Contracts (Programs)

- What are Solana programs?
- Rust basics for Solana
- Program structure

- Instructions & accounts

Outcome: Learners can read and write basic Solana programs.

Level 7B – Solana Development Environment

- Solana CLI
- Anchor framework
- Local validator
- Program deployment
- Writing tests

Outcome: Learners can deploy and test Solana programs locally.

Level 8B – Tokens & NFTs on Solana

- SPL tokens
- Minting tokens
- NFTs on Solana (Metaplex)
- Token metadata & standards

Outcome: Learners can create and manage tokens and NFTs on Solana.

Level 9B – Solana dApp Development

- Frontend integration (Solana Web3.js)
- Wallet adapters
- Program interaction
- Performance-oriented UX design

Outcome: Learners can build scalable Solana-based decentralized applications.

SECTION 3: AUDITING & BEST PRACTICES

Objective: Train learners to write secure, auditable, and production-ready Web3 systems.

Level 10 – Smart Contract Security Basics

- Why security matters in Web3
- Common vulnerabilities:
    - Reentrancy
    - Integer overflow/underflow
    - Access control issues
    - Front-running
- Real hack case studies

Outcome: Learners recognize common attack vectors.

Level 11 – Auditing Methodology

- Audit process overview
- Manual code review techniques
- Static analysis tools (Slither, Mythril)
- Writing audit reports

Outcome: Learners understand professional auditing workflows.

Level 12 – Secure Development Best Practices

- OpenZeppelin libraries
- Upgradeable contracts
- Role-based access control
- Secure randomness
- Pausable & emergency mechanisms

Outcome: Learners write production-grade secure contracts

Level 13 – Testing & Monitoring

- Unit & integration testing
- Fuzz testing
- Testnet deployment
- Monitoring smart contracts

Outcome: Learners ensure reliability before mainnet deployment.

Level 14 – Governance & Compliance

- DAO governance models
- On-chain voting
- Regulatory considerations (high-level)
- Ethical development in Web3

Outcome: Learners understand governance and long-term sustainability.

FINAL CAPSTONE PROJECT

Description: Learners design and deliver a complete Web3 project including:

- Smart contracts
- Frontend dApp
- Security considerations
- Basic audit report

Final Outcome: Certified Web3-ready professionals with **development + security + best practice skills**.

Certification Levels

- Web3 Fundamentals Certificate (Section 1)
- Web3 Developer Certificate (Section 2)
- Web3 Security & Best Practices Certificate (Section 3)