Blockchain and Web3 for Digital Government Training Course

2 – 6 November 2026
Kuala Lumpur

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Blockchain and Web3 for Digital Government Training Course

Ref: 879_166357 **Date:** 2 – 6 November 2026 **Location:** Kuala Lumpur **Fees:** 5200 Euro

Overview

Blockchain and Web3 for Digital Government Training Course is a one-week course for digital government leaders, public-service transformation managers, enterprise architects, security specialists, governance advisers, and technology managers who leave with a Blockchain Public Service Decision Pack. Participants evaluate distributed ledgers, trusted registries, verifiable credentials, smart contracts, identity, privacy, cybersecurity, interoperability, and operating models. The course separates suitable public-service use cases from weak technology proposals. Agile Leaders Training Center develops blockchain and Web3 practice for digital government.

Who Should Attend

- Digital government functions responsible for service transformation and technology priorities
- Public-service functions responsible for trusted records, verification, and transparent workflows
- Enterprise architecture functions responsible for platforms, integration, and interoperability
- Security and privacy functions responsible for identity, access, data protection, and cyber risk
- Governance and legal functions responsible for accountability, procurement, and control design

The course assumes participants already evaluate digital services or technology investments; it leaves out blockchain coding, token trading, and platform certification.

Departments and Industries

The course supports departments and industries that issue, verify, exchange, or govern trusted digital records.

- Public administration, digital services, licensing, and records management
- Education, workforce, healthcare, and social-service credential functions
- Customs, trade, supply-chain, and product-provenance operations
- Financial services, identity providers, and regulated digital platforms
- Technology suppliers, system integrators, and professional advisers

Learning Objectives

By the end of this course, participants will be able to:

- Analyze whether a public-service problem needs a distributed ledger.
- Build trusted-registry and verifiable-credential use cases.
- Evaluate smart-contract, identity, privacy, and cybersecurity controls.
- Compare governance, interoperability, procurement, and operating models.
- Prioritize implementation options using value, risk, and readiness evidence.
- Build a Blockchain Public Service Decision Pack.

AGILE LEADERS
Training Center

Course Agenda

Day 1: Frame Blockchain Public Services

- NIST IR 8202 Blockchain Component Map
- Centralized and Distributed Service Comparison
- Public-Service Problem and Trust Canvas
- Blockchain Use-Case Suitability Matrix
- Participant, Node, and Governance Boundary Diagram

Day 2: Design Trusted Records and Credentials

- Trusted Registry Data and Authority Model
- W3C Verifiable Credentials Data Model 2.0 Ecosystem Map
- Issuer, Holder, and Verifier Responsibility Matrix
- Digital Identity and Wallet Interaction Flow
- Credential Status, Revocation, and Verification Workflow

AGILE LEADERS
Training Center

Day 3: Govern Smart Contracts and Data

- Smart Contract Trigger and State Diagram
- Business Rule and Code-Control Crosswalk
- On-Chain and Off-Chain Data Decision Matrix
- Data Oracle Trust and Failure Assessment
- Transparent Workflow and Audit-Trail Design

Day 4: Control Risk and Interoperability

- Blockchain Identity, Key, and Access Control Map
- Privacy and Data-Minimization Assessment
- Cyber Threat and Smart-Contract Risk Register
- Platform, API, and Credential Interoperability Matrix
- Procurement, Operating Model, and Accountability Scorecard

Day 5: Practice Government Blockchain Decisions

- Exercise: Test a Registry Use Case for Blockchain Fit
- Exercise: Design a Verifiable Credential Service
- Exercise: Review a Smart Contract Control Failure
- Exercise: Prioritize a Public-Service Implementation Portfolio
- Capstone: Blockchain Public Service Decision Pack

AGILE LEADERS
Training Center

Practical Exercises

The course uses suggested activities based on records, credentials, licensing, trade, education, and service verification.

- Suggested activity: compare a shared database and distributed-ledger approach for the same trust problem.
- Suggested activity: map credential issuance, holding, presentation, verification, and status checks.
- Suggested activity: identify privacy, key-management, oracle, and smart-contract failure paths.
- Suggested activity: defend an implementation roadmap using value, risk, governance, and readiness evidence.

FAQs

Who suits blockchain and Web3 for digital government training, and what does it assume?

Digital government, public-service, architecture, security, privacy, governance, and technology functions suit the training. It assumes regular involvement in digital-service or technology investment decisions.

How does blockchain for digital government training differ from general blockchain training?

Blockchain for digital government training focuses on public-service trust, records, credentials, governance, privacy, interoperability, procurement, and accountability, while general blockchain training often emphasizes broader technology concepts and applications.

When does a digital government service need blockchain?

A digital government service may need blockchain when multiple parties require a shared, tamper-evident record without relying on one controlling repository and when governance, privacy, cost, and interoperability remain workable.

How do verifiable credentials support public services?

Verifiable credentials support public services by enabling issuers to make protected claims, holders to present them, and verifiers to check authenticity and status through a defined trust ecosystem.

AGILE LEADERS
Training Center

What risks affect smart contracts in government services?

Smart-contract risks include incorrect business rules, coding defects, unsafe upgrades, compromised keys, unreliable data oracles, privacy exposure, unclear accountability, and weak exception handling.

Conclusion

Participants take back a Blockchain Public Service Decision Pack containing suitability tests, trust models, credential flows, smart-contract controls, risk registers, interoperability views, and an implementation roadmap. It changes technology-led proposals into governed public-service decisions. The pack supports transparent evaluation, accountable ownership, and traceable implementation choices.