

Développeur blockchain

RNCP42176 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	326
Formacode(s)	31004, 31006, 31082, 31032, 31067
Code(s) ROME	M1805
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	30/04/2026
Date d'échéance	30/04/2029

Certificateur(s)

FORMATIVES · SIRET : 44320061300026

Résumé de la certification

OBJECTIFS ET CONTEXTE

La blockchain s'est imposée comme une technologie stratégique pour la sécurisation, la traçabilité et l'automatisation des échanges, portée par l'essor du Web3 et des contrats numériques automatiquement exécutés (smart contracts).

Les entreprises françaises – fintech, banque, industrie, énergie, supply chain, santé, agriculture connectée – développent de nouveaux usages mais peinent à recruter des profils spécialisés, alors que les compétences blockchain sont jugées rares par 81 % des organisations.

Le métier de Développeur Blockchain répond directement à ces besoins : analyser un besoin métier, concevoir une architecture distribuée, développer et sécuriser des smart contracts, intégrer des solutions on-chain/off-chain et assurer leur conformité (MiCA, RGPD, PSAN).

La certification vise à former des professionnels capables de concevoir des applications décentralisées fiables, sécurisées et adaptées aux exigences techniques et réglementaires d'un écosystème en forte croissance.

ACTIVITÉS VISÉES

Conception de solutions décentralisées basées sur la blockchain : Analyse des besoins d'un projet blockchain ; Réalisation d'une veille technologique ; Définition de l'architecture des solutions décentralisées

Développement d'une solution durable intégrant la technologie blockchain : Développement des smart contracts et dApps ; Réalisation des tests et déploiement des smart contracts

Maintenance, optimisation et supervision des performances de solutions blockchain : Monitoring et diagnostic des dérives ; Maintenance et amélioration des solutions blockchain ;

Gestion de la sécurité et des risques des solutions blockchain : Sécurisation des solutions basées sur la technologie blockchain ; Mise en œuvre des dispositifs de continuité, de veille réglementaire et de cybersécurité blockchain

COMPÉTENCES ATTESTÉES

Identifier les processus métier pouvant être décentralisés ou automatisés via la blockchain, en mobilisant des outils d'analyse fonctionnelle (BPMN, UML, diagrammes de séquence, etc.) et des méthodes de modélisation des flux, afin de déterminer les opportunités, limites et points de valeur ajoutée d'une approche décentralisée.

Analyser les besoins fonctionnels et techniques d'un projet blockchain, à partir d'un cahier des charges, d'un cas d'usage ou d'entretiens avec les parties prenantes, etc., en mobilisant des outils d'ingénierie des exigences (User Stories, diagramme de cas d'utilisation, etc.) afin de définir les contraintes, fonctionnalités prioritaires et objectifs techniques du projet.

Rédiger la documentation de conception fonctionnelle et technique, en utilisant des outils professionnels de

documentation (Notion, Confluence, Markdown, Google Workspace, etc.), et une terminologie adaptée au domaine blockchain, tout en garantissant l'accessibilité et l'inclusivité de l'information (personnes en situation de handicap, équipe multiculturelle, etc.) pour l'ensemble des parties prenantes, afin de permettre le transfert clair et opérationnel du projet vers l'équipe de développement ou les parties prenantes.

Réaliser une veille technologique et stratégique sur les protocoles, standards, frameworks et tendances du Web3, en mobilisant des outils spécialisés de veille, de curation et d'analyse assistés par l'intelligence artificielle (Glasp, Notion AI, Copilot Labs, Dune Analytics, etc.), afin d'identifier les innovations pertinentes à la conception de solutions basées sur la technologie blockchain.

Analyser la faisabilité technique, économique, énergétique et organisationnelle des innovations identifiées lors de la veille, en mobilisant des grilles d'analyse multicritères et d'aide à la décision (TRL – Technology Readiness Level, matrices d'impact/risque, scoring de faisabilité, benchmark comparatif), afin d'orienter la conception vers les options les plus durables.

Construire l'architecture d'une solution applicative reposant sur une blockchain existante (publique, privée, consortium ou Layer 2), en analysant et comparant les protocoles existants (Ethereum, Hyperledger Fabric, Polygon, Avalanche, Solana, etc.), à l'aide d'outils de conception et d'architecture technique (UML, C4 Model, ArchiMate, Lucidchart, Draw.io), selon leurs caractéristiques de sécurité, de coût, de performance, de gouvernance et d'impact environnemental, afin de concevoir une solution techniquement cohérente, économiquement viable et durable.

Concevoir la gouvernance et les mécanismes d'incitation d'une solution ou plateforme décentralisée reposant sur une blockchain existante, en définissant les rôles, droits, règles de décision, de validation, de consensus et de récompense, à l'aide d'outils de conception (Tokenomics, DAO Framework, Smart Contract Design Patterns, etc.), afin d'assurer la transparence et la sécurité du système décentralisé.

Modéliser la structure fonctionnelle et technique d'une solution applicative intégrant des smart contracts et des interactions on-chain/off-chain, les flux de données, le modèle de stockage et les dépendances applicatives, à l'aide d'outils et méthodes de modélisation et de visualisation (UML, BPMN, Merise, ArchiMate, Figma, Miro, etc.), afin de garantir la cohérence et l'exploitabilité du modèle pour le développement et la maintenance.

Implémenter des smart contracts à partir des spécifications fonctionnelles et techniques, en mobilisant les langages adaptés (Solidity, Rust, etc.) et les environnements de développement intégrés (Remix IDE, Hardhat, Foundry, etc.), afin de traduire les logiques métiers définies dans le cahier de conception en code exécutable, fiable et sécurisé.

Intégrer des smart contracts dans des applications décentralisées (dApps), en synchronisant les échanges entre les composants applicatifs (front-end, back-end, API) et les contrats déployés, en optimisant les interactions on-chain permettant de réduire la consommation de gas et les coûts opérationnels, à l'aide d'outils et bibliothèques d'interfaçage (Web3.js, GraphQL, Hardhat, etc.), afin de garantir la fiabilité, la sécurité, la performance durable des échanges entre la couche applicative et des smart contracts déployés sur une blockchain existante.

Réaliser les tests unitaires, d'intégration et de sécurité des smart contracts et des dApps, en mobilisant des frameworks et environnements spécialisés (Hardhat, Truffle, Foundry, Cypress, etc.), ainsi que des outils d'automatisation et d'IA (GitHub Actions, ChatGPT, SonarQube, etc.) et en respectant les principes de sobriété numérique, afin de vérifier la conformité et la sécurité du code avant déploiement.

Déployer les smart contracts et les dApps sur des environnements blockchain existants (testnet, mainnet ou réseaux privés fournis par l'organisation), en optimisant les scripts et les interactions on-chain, en utilisant des outils de déploiement et de configuration spécifiques à la blockchain (Truffle Migrations, Alchemy, Infura, etc.), et en mobilisant des outils de supervision et d'analyse assistés par IA (Code Interpreter, Tenderly Debugger, etc.) et d'automatisation, afin d'assurer la performance et la reproductibilité du déploiement sur le réseau choisi.

Documenter les processus techniques du projet blockchain (développement, tests, déploiement) en appliquant les standards de documentation technique (Markdown, Doxygen, ABI, etc.) et en mobilisant des outils d'assistance IA (Copilot Docs, Notion AI, etc.), tout en garantissant l'accessibilité de l'information aux différents publics, y compris aux personnes en situation de handicap, afin d'assurer la transmission claire, inclusive et durable du projet dans une logique de développement sobre et réutilisable.

Mettre en place des mécanismes de supervision et d'alerte pour le suivi des performances, en utilisant des outils de monitoring open source et cloud (Prometheus, Grafana, Elastic Stack, Datadog, Tenderly) et des systèmes d'alerte prédictive basés sur l'IA (OpenAI Anomaly Detection, Grafana ML), afin d'assurer une détection préventive des incidents et une réactivité optimale.

Diagnostiquer les dérives, incidents ou anomalies d'une solution applicative reposant sur la technologie blockchain, en exploitant les données de supervision, les logs et les rapports de performance, à l'aide d'outils d'analyse et de corrélation (Elastic Stack, Grafana Loki, Tenderly Debugger, Hardhat Network, ChatGPT Code Interpreter), afin d'identifier les causes racines, d'évaluer les impacts et de proposer des actions correctives adaptées.

Corriger les anomalies ou failles identifiées dans les smart contracts, dApps et composants techniques intégrant la blockchain (API Web3, providers, oracles, etc.) en mobilisant des outils d'audit et de débogage (Slither, Tenderly, etc.) et des assistants IA de correction de code (Copilot, Code Interpreter, etc.) afin de rétablir le système sans altération des données on-chain.

Optimiser la performance et la fiabilité d'une solution applicative intégrant la technologie blockchain, en mobilisant des outils d'analyse et d'optimisation technique (Tenderly, Blocknative, etc.), en ajustant les paramètres de fonctionnement et la structure des composants (refactoring du code, optimisation des requêtes, rollups, caching, etc.), afin d'assurer la stabilité, la réactivité et la continuité du service dans des conditions d'exploitation réelles.

Intégrer des innovations et technologies émergentes dans l'écosystème blockchain, en expérimentant des solutions interopérables, performantes et sobres en ressources (Layer 2, rollups, ZK-proofs, etc.), et en évaluant leur impact sur la sécurité, la compatibilité et la durabilité du système, afin d'assurer l'adaptation continue du projet aux évolutions du Web3.

Auditer la sécurité d'une solution applicative intégrant la technologie blockchain, en mobilisant des méthodes d'analyse de risques (OWASP, STRIDE, ISO/IEC 27005) et des outils d'audit de sécurité (MythX, Slither, Oyente, Tenderly Security, OpenVAS), afin de proposer un plan de sécurisation adapté aux vulnérabilités techniques et organisationnelles identifiées.

Évaluer la résilience d'une solution applicative intégrant la technologie blockchain, en simulant des scénarios d'incident et d'attaque (tests de charge, déni de service, corruption de nœud, panne réseau) à l'aide d'outils de simulation et de chaos engineering (Hardhat Network, Foundry Fuzzing, Chaos Mesh, Gremlin, PenTestGPT), afin de mesurer la capacité du système à maintenir ses performances et sa continuité d'activité.

Assurer la sécurisation des smart contracts et des applications décentralisées, en appliquant les bonnes pratiques de cybersécurité (cryptographie, gouvernance des clés privées, permissions, audit de code, etc.), et en mobilisant des outils d'analyse et de supervision assistés par IA (Tenderly, Defender, Code Interpreter), afin de garantir la sécurité opérationnelle des solutions fondées sur la blockchain.

Élaborer les procédures de continuité et de reprise d'activité, en concevant et testant des plans de sauvegarde et de redondance (multi-nœuds, backup automatisé, DRP cloud), afin d'assurer la disponibilité et la reprise du service en cas d'incident ou d'attaque.

Contribuer à la gouvernance de la cybersécurité blockchain et la veille associée, en structurant la documentation (politiques, rapports, registres) selon les principes d'accessibilité et d'inclusivité et en assurant une veille sur les cadres réglementaires (RGPD, MiCA, etc.), afin d'assurer la conformité éthique, réglementaire et technologique du dispositif de sécurité.

Blocs de compétences

RNCP42176BC01 — Concevoir des solutions décentralisées basées sur la blockchain

LISTE DE COMPÉTENCES

- Identifier les processus métier pouvant être décentralisés ou automatisés via la blockchain, en mobilisant des outils d'analyse fonctionnelle (BPMN, UML, diagrammes de séquence, etc.) et des méthodes de modélisation des flux, afin de déterminer les opportunités, limites et points de valeur ajoutée d'une approche décentralisée.
- Analyser les besoins fonctionnels et techniques d'un projet blockchain, à partir d'un cahier des charges, d'un cas d'usage ou d'entretiens avec les parties prenantes, etc., en mobilisant des outils d'ingénierie des exigences (User Stories, diagramme de cas d'utilisation, etc.) afin de définir les contraintes, fonctionnalités prioritaires et objectifs techniques du projet.
- Rédiger la documentation de conception fonctionnelle et technique, en utilisant des outils professionnels de documentation (Notion, Confluence, Markdown, Google Workspace, etc.), et une terminologie adaptée au domaine blockchain, tout en garantissant l'accessibilité et l'inclusivité de l'information (personnes en situation de handicap, équipe multiculturelle, etc.) pour l'ensemble des parties prenantes, afin de permettre le transfert clair et opérationnel du projet vers l'équipe de développement ou les parties prenantes.
- Réaliser une veille technologique et stratégique sur les protocoles, standards, frameworks et tendances du Web3, en mobilisant des outils spécialisés de veille, de curation et d'analyse assistés par l'intelligence artificielle (Glasp, Notion AI, Copilot Labs, Dune Analytics, etc.), afin d'identifier les innovations pertinentes à la conception de solutions basées sur la technologie blockchain.
- Analyser la faisabilité technique, économique, énergétique et organisationnelle des innovations identifiées lors de la veille, en mobilisant des grilles d'analyse multicritères et d'aide à la décision (TRL – Technology Readiness Level,

matrices d'impact/risque, scoring de faisabilité, benchmark comparatif), afin d'orienter la conception vers les options les plus durables.

- Construire l'architecture d'une solution applicative reposant sur une blockchain existante (publique, privée, consortium ou Layer 2), en analysant et comparant les protocoles existants (Ethereum, Hyperledger Fabric, Polygon, Avalanche, Solana, etc.), à l'aide d'outils de conception et d'architecture technique (UML, C4 Model, ArchiMate, Lucidchart, Draw.io), selon leurs caractéristiques de sécurité, de coût, de performance, de gouvernance et d'impact environnemental, afin de concevoir une solution techniquement cohérente, économiquement viable et durable.
- Concevoir la gouvernance et les mécanismes d'incitation d'une solution ou plateforme décentralisée reposant sur une blockchain existante, en définissant les rôles, droits, règles de décision, de validation, de consensus et de récompense, à l'aide d'outils de conception (Tokenomics, DAO Framework, Smart Contract Design Patterns, etc.), afin d'assurer la transparence et la sécurité du système décentralisé.
- Modéliser la structure fonctionnelle et technique d'une solution applicative intégrant des smart contracts et des interactions on-chain/off-chain, les flux de données, le modèle de stockage et les dépendances applicatives, à l'aide d'outils et méthodes de modélisation et de visualisation (UML, BPMN, Merise, ArchiMate, Figma, Miro, etc.), afin de garantir la cohérence et l'exploitabilité du modèle pour le développement et la maintenance.

MODALITÉS D'ÉVALUATION

Oral individuel : présentation d'un projet

RNCP42176BC02 — Développer une solution durable intégrant la technologie blockchain

LISTE DE COMPÉTENCES

- Implémenter des smart contracts à partir des spécifications fonctionnelles et techniques, en mobilisant les langages adaptés (Solidity, Rust, etc.) et les environnements de développement intégrés (Remix IDE, Hardhat, Foundry, etc.), afin de traduire les logiques métiers définies dans le cahier de conception en code exécutable, fiable et sécurisé.
- Intégrer des smart contracts dans des applications décentralisées (dApps), en synchronisant les échanges entre les composants applicatifs (front-end, back-end, API) et les contrats déployés, en optimisant les interactions on-chain permettant de réduire la consommation de gas et les coûts opérationnels, à l'aide d'outils et bibliothèques d'interfaçage (Web3.js, GraphQL, Hardhat, etc.), afin de garantir la fiabilité, la sécurité, la performance durable des échanges entre la couche applicative et des smart contracts déployés sur une blockchain existante.
- Réaliser les tests unitaires, d'intégration et de sécurité des smart contracts et des dApps, en mobilisant des frameworks et environnements spécialisés (Hardhat, Truffle, Foundry, Cypress, etc.), ainsi que des outils d'automatisation et d'IA (GitHub Actions, ChatGPT, SonarQube, etc.) et en respectant les principes de sobriété numérique, afin de vérifier la conformité et la sécurité du code avant déploiement.
- Déployer les smart contracts et les dApps sur des environnements blockchain existants (testnet, mainnet ou réseaux privés fournis par l'organisation), en optimisant les scripts et les interactions on-chain, en utilisant des outils de déploiement et de configuration spécifiques à la blockchain (Truffle Migrations, Alchemy, Infura, etc.), et en mobilisant des outils de supervision et d'analyse assistés par IA (Code Interpreter, Tenderly Debugger, etc.) et d'automatisation, afin d'assurer la performance et la reproductibilité du déploiement sur le réseau choisi.
- Documenter les processus techniques du projet blockchain (développement, tests, déploiement) en appliquant les standards de documentation technique (Markdown, Doxygen, ABI, etc.) et en mobilisant des outils d'assistance IA (Copilot Docs, Notion AI, etc.), tout en garantissant l'accessibilité de l'information aux différents publics, y compris aux personnes en situation de handicap, afin d'assurer la transmission claire, inclusive et durable du projet dans une logique de développement sobre et réutilisable.

MODALITÉS D'ÉVALUATION

Oral individuel : présentation d'un projet

RNCP42176BC03 — Assurer la maintenance, l'optimisation et la performance durable de solutions blockchain

LISTE DE COMPÉTENCES

- Mettre en place des mécanismes de supervision et d'alerte pour le suivi des performances, en utilisant des outils de monitoring open source et cloud (Prometheus, Grafana, Elastic Stack, Datadog, Tenderly) et des systèmes d'alerte prédictive basés sur l'IA (OpenAI Anomaly Detection, Grafana ML), afin d'assurer une détection préventive des incidents et une réactivité optimale.
- Diagnostiquer les dérives, incidents ou anomalies d'une solution applicative reposant sur la technologie blockchain, en exploitant les données de supervision, les logs et les rapports de performance, à l'aide d'outils d'analyse et de corrélation (Elastic Stack, Grafana Loki, Tenderly Debugger, Hardhat Network, ChatGPT Code Interpreter), afin

d'identifier les causes racines, d'évaluer les impacts et de proposer des actions correctives adaptées.

- Corriger les anomalies ou failles identifiées dans les smart contracts, dApps et composants techniques intégrant la blockchain (API Web3, providers, oracles, etc.) en mobilisant des outils d'audit et de débogage (Slither, Tenderly, etc.) et des assistants IA de correction de code (Copilot, Code Interpreter, etc.) afin de rétablir le système sans altération des données on-chain.
- Optimiser la performance et la fiabilité d'une solution applicative intégrant la technologie blockchain, en mobilisant des outils d'analyse et d'optimisation technique (Tenderly, Blocknative, etc.), en ajustant les paramètres de fonctionnement et la structure des composants (refactoring du code, optimisation des requêtes, rollups, caching, etc.), afin d'assurer la stabilité, la réactivité et la continuité du service dans des conditions d'exploitation réelles.
- Intégrer des innovations et technologies émergentes dans l'écosystème blockchain, en expérimentant des solutions interopérables, performantes et sobres en ressources (Layer 2, rollups, ZK-proofs, etc.), et en évaluant leur impact sur la sécurité, la compatibilité et la durabilité du système, afin d'assurer l'adaptation continue du projet aux évolutions du Web3.

MODALITÉS D'ÉVALUATION

Oral individuel : présentation d'un projet

RNCP42176BC04 — Gérer la sécurité et les risques des solutions blockchain

LISTE DE COMPÉTENCES

- Auditer la sécurité d'une solution applicative intégrant la technologie blockchain, en mobilisant des méthodes d'analyse de risques (OWASP, STRIDE, ISO/IEC 27005) et des outils d'audit de sécurité (MythX, Slither, Oyente, Tenderly Security, OpenVAS), afin de proposer un plan de sécurisation adapté aux vulnérabilités techniques et organisationnelles identifiées.
- Évaluer la résilience d'une solution applicative intégrant la technologie blockchain, en simulant des scénarios d'incident et d'attaque (tests de charge, déni de service, corruption de nœud, panne réseau) à l'aide d'outils de simulation et de chaos engineering (Hardhat Network, Foundry Fuzzing, Chaos Mesh, Gremlin, PenTestGPT), afin de mesurer la capacité du système à maintenir ses performances et sa continuité d'activité.
- Assurer la sécurisation des smart contracts et des applications décentralisées, en appliquant les bonnes pratiques de cybersécurité (cryptographie, gouvernance des clés privées, permissions, audit de code, etc.), et en mobilisant des outils d'analyse et de supervision assistés par IA (Tenderly, Defender, Code Interpreter), afin de garantir la sécurité opérationnelle des solutions fondées sur la blockchain.
- Élaborer les procédures de continuité et de reprise d'activité, en concevant et testant des plans de sauvegarde et de redondance (multi-nœuds, backup automatisé, DRP cloud), afin d'assurer la disponibilité et la reprise du service en cas d'incident ou d'attaque.
- Contribuer à la gouvernance de la cybersécurité blockchain et la veille associée, en structurant la documentation (politiques, rapports, registres) selon les principes d'accessibilité et d'inclusivité et en assurant une veille sur les cadres réglementaires (RGPD, MiCA, etc.), afin d'assurer la conformité éthique, réglementaire et technologique du dispositif de sécurité.

MODALITÉS D'ÉVALUATION

Oral individuel : présentation d'un projet

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le développeur blockchain exerce principalement dans le secteur du numérique, mais intervient aujourd'hui dans un large éventail de secteurs économiques intégrant des technologies de registres distribués. Les usages de la blockchain se développent notamment dans la finance et la fintech, les banques et assurances, la logistique et les transports, l'énergie, l'industrie, la cybersécurité, la santé, le luxe ou encore les services numériques.

Le développeur blockchain peut ainsi exercer dans des environnements professionnels variés, notamment au sein : de startups technologiques spécialisées dans la blockchain et le Web3 ; d'entreprises de services numériques (ESN), de cabinets de conseil et de sociétés spécialisées intervenant sur des projets d'ingénierie, d'intégration ou d'audit blockchain ; de grandes entreprises et groupes industriels intégrant la blockchain au sein de leurs directions informatiques, de leurs équipes d'innovation ou de leurs laboratoires R&D ; de PME et d'ETI développant des usages liés à la traçabilité, à la sécurisation des données ou à l'automatisation de processus métiers.

TYPE D'EMPLOIS ACCESSIBLES

RÈGLEMENTATIONS D'ACTIVITÉ

Le métier de développeur blockchain n'est pas réglementé dans son accès. Toutefois, son exercice s'inscrit dans un environnement juridique et réglementaire structuré, lié aux usages technologiques mobilisés (smart contracts, crypto-actifs, données distribuées, sécurité des protocoles).

L'activité du développeur blockchain est notamment encadrée par les textes suivants :

- Réglementation française et européenne du Web3 : Loi PACTE (2019), définissant le cadre applicable aux prestataires de services sur actifs numériques (PSAN), et règlement européen MiCA (Markets in Crypto-Assets), encadrant l'émission et les services liés aux crypto-actifs au niveau européen.
- Protection des données et systèmes d'information : Règlement Général sur la Protection des Données (RGPD) : principes de minimisation, de protection des données dès la conception (privacy-by-design) et de gestion des données personnelles dans des environnements blockchain.
- Propriété intellectuelle et licences logicielles : Respect du droit d'auteur et des licences open source applicables aux protocoles, bibliothèques et frameworks blockchain utilisés.
- Réglementations sectorielles et normes techniques : En fonction des domaines d'application (finance, santé, énergie, logistique, etc.), prise en compte des cadres réglementaires spécifiques et des normes de sécurité et d'interopérabilité, notamment ISO/IEC 27001 (sécurité de l'information) et ISO/TC 307 (technologies blockchain).

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Très élevée (5/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 4 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 864 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (41 % des actifs en emploi)
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	27 458
Jugés difficiles à recruter	53 %
Emplois saisonniers	1 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Pour accéder à la formation menant à la certification professionnelle « développeur blockchain », ainsi qu'aux blocs de compétences constitutifs de la certification, les candidats doivent satisfaire aux conditions préalables suivantes :

- En formation initiale,
être titulaire soit :
 - o D'un niveau 4 reconnu par l'État (bac ou certification RNCP) pour un cycle de 3 années de formation au sein de l'établissement,
 - o D'un niveau 5 dans le domaine de l'informatique reconnu par l'État pour 1 année de formation,
 - o Niveau 4 reconnu par l'État + 3 années d'expérience en informatique

(livret VAPP à faire valider par le certificateur) pour 1 année de formation.

- En formation professionnelle continue :

o Niveau 5 validé dans le domaine informatique et justifier d'une expérience professionnelle d'au moins 3 ans dans un domaine du développement informatique ou blockchain / web ou digital.

Afin de sécuriser les parcours de formation et de garantir la capacité des candidats à suivre le programme menant à la certification Développeur Blockchain, chaque organisme de formation met en œuvre un test de positionnement préalable à l'entrée en formation.

PRÉREQUIS À LA VALIDATION

Le candidat doit remettre des livrables conformes aux exigences du référentiel pour accéder aux épreuves certificatives.

Afin de mettre en pratique les savoirs associés aux compétences, le candidat doit avoir réalisé au minimum 40 journées en entreprise par année de formation.

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, VAE

1 président du jury, professionnel externe et indépendant du certificateur, exerçant ou ayant exercé des fonctions de responsabilité ou d'expertise technique dans le domaine du numérique et/ou sécurité numérique, disposant d'une expérience professionnelle significative (2 ans) dans le développement blockchain.

2 professionnels du secteur, indépendants du certificateur, exerçant des fonctions en lien direct avec le métier de développeur blockchain.

Base légale

Date de décision	30/04/2026
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	30/04/2029
Date de dernière délivrance possible	30/04/2033

Liens avec d'autres certifications

CORRESPONDANCES (PAR BLOCS)

RNCP41312, RNCP41701, RNCP41719

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42176/>