



A KNOWLEDGE ALLIANCE FOR BLOCKCHAIN IN ACADEMIC, ENTREPRENEURIAL AND INVESTMENT
TRAINING
601063-EPP-1-2018-1-CY-EPPKA2-KA

Translated Syllabi-French

Deliverable 15
WP5: Content Development Task 5.3

30-10-2020



Table of Contents

I.	Authors and Reviewers	2
II.	Module d'apprentissage 0: Introduction du cours et du monde de la DLT:.....	3
III.	Module d'apprentissage 1: Conception de bases de données peer-to-peer.....	5
IV.	Module d'apprentissage 2: Techniques de cryptage	7
V.	Module d'apprentissage 3: Mécanismes de consensus.....	9
VI.	Module d'apprentissage 4: Signatures numériques	12
VII.	Module d'apprentissage 5: Contrats intelligents.....	14
VIII.	Module d'apprentissage 6: Confidentialité et droits de propriété.....	18
IX.	Module d'apprentissage 7: Applications décentralisées basées sur la blockchain	20
X.	Module d'apprentissage 8: Organisations autonomes décentralisées	22



Authors and Reviewers

Written by	Organization	Reviewed by	Organization
Martina Ianuzzi	EBAN		



Module d'apprentissage 0: Introduction du cours et du monde de la DLT:

Le module d'apprentissage 0 est divisé en deux parties logiques. La première partie fournit une introduction au cours DLT4All, identifiant différents publics ciblés et parties du curriculum qui s'adressent à chacun d'eux, et présentant un aperçu des options de certification. La deuxième partie donne une introduction aux technologies Blockchain d'un point de vue historique et technique. Un aperçu de la structure des Blockchains est présenté ainsi que ses concepts de base, qui seront développés dans les modules suivants du cours. Une taxonomie ou Des blockchains basées sur leurs autorisations de lecture et d'écriture sont données, et les concepts de crypto-monnaie, de contrats intelligents et l'application décentralisée sont introduits. Un aperçu des cas d'utilisation de la blockchain conclut le module d'apprentissage.

Objectifs d'apprentissage :

- Présenter la structure et le contenu du cours DLT4All
- Définir les différents publics ciblés du cours DLT4All
- Décrire les options de certification disponibles pour les participants
- Donner un aperçu historique du développement de la technologie Blockchain
- Donner un aperçu des composants technologiques d'un système basé sur la blockchain
- Présenter une caractérisation des Blockchains basée sur les autorisations de lecture / écriture de l'utilisateur
- Décrire les concepts de crypto-monnaie, de contrat intelligent et d'application décentralisée dans le contexte d'un système basé sur la blockchain
- Présenter un ensemble de cas d'utilisation pertinents de systèmes basés sur la blockchain

Résultats d'apprentissage :

- Se rappeler de la structure du cours DLT4All
- Déterminer de quel public ciblé il s'agit
- Comprendre les options de certification disponibles
- Décrire le développement historique des technologies blockchain
- Décrire les composants techniques d'un système basé sur la blockchain
- Expliquer comment les blockchains peuvent être classées
- Expliquer les concepts de crypto-monnaie, de contrat intelligent et d'application décentralisée
- Nommer et décrire les cas d'utilisation pertinents de la blockchain

Syllabus :

1. Introduction au cours DLT4ALL
 - 1.1. Public ciblé



- 1.2. Structure du cours
- 1.3. Options de certification
2. Introduction aux blockchains
 - 2.1. Aperçu historique
 - 2.2. Composants technologiques d'un système basé sur la blockchain
3. Caractérisation des blockchains
 - 3.1. Public vs privé, sans autorisation vs avec autorisation
4. Des blockchains aux dApps
 - 4.1. Crypto-monnaies
 - 4.2. Contrats intelligents
 - 4.3. Applications décentralisées
5. Application de cas d'utilisation



Module d'apprentissage 1: Conception de bases de données peer-to-peer

La possibilité d'avoir des bases de données ouvertes et partagées, avec des données certifiées et vérifiables publiquement peut conduire à la participation et l'autonomisation des citoyens dans de nombreux domaines. Le module d'apprentissage 1 fournit une discussion approfondie sur les problèmes de conception architecturale de la gestion des données. Les défis rencontrés dans la conception d'une base de données distribuée et décentralisée sont présentés et analysés dans le détail, en présentant les principes de base de la conception de bases de données et les mécanismes sous-jacents peer-to-peer Réseaux de communication.

Les difficultés rencontrées pour développer une base de données peer-to-peer fiable et les solutions potentielles à ces problèmes fournies par les technologies blockchain sont présentées. Les participants comprendront comment une base de données peut être partagée et synchronisée entre différents nœuds et pourquoi il n'est pas facile de modifier sa structure par la suite. Ils pourront ainsi déterminer quand il est approprié d'utiliser une base de données distribuée. Ils comprendront pourquoi une base de données distribuée est fiable et comment cette technologie peut sécuriser d'avantage les transactions et le partage de données au sein des chaînes d'approvisionnement. Elles vont être en mesure de reconnaître que dans certains cas, il vaut la peine de créer une nouvelle blockchain ad hoc, alors que dans d'autres, il est mieux d'utiliser une blockchain existante pour assurer l'intégrité des données échangées avec leurs fournisseurs.

Prérequis :

Ce module n'a pas de prérequis.

Objectifs d'apprentissage

- Expliquer ce qu'est une base de données et les bases de son fonctionnement.
- Présenter les concepts de base de la technologie de communication peer-to-peer (P2P) et ses avantages par rapport au paradigme traditionnel.
- Expliquer les méthodes utilisées pour créer une base de données dans un environnement P2P (la blockchain).
- Discuter des aspects critiques, des limites et des inconvénients de l'utilisation de la technologie blockchain au lieu d'une base de données centralisée.
- Présenter des cas d'utilisation dans lesquels l'utilisation de la technologie blockchain est bénéfique.

Résultats d'apprentissage

- Comprendre les bases de la conception de bases de données.
- Comprendre les mécanismes de fonctionnement de base des réseaux de communication peer-to-peer.
- Comprendre pourquoi la technologie blockchain a été développée comme solution aux problèmes rencontrés



- Concevoir une base de données distribuée peer-to-peer.
- Expliquer dans quels cas les bases de données peer-to-peer peuvent être utiles.
- Comprendre pourquoi l'intégrité des données n'est pas une garantie d'exactitude des informations lorsque l'humain facteur est impliqué.

Syllabus

1. Explication de ce qu'est une base de données et de son fonctionnement
 - 1.1. Principes de base de données, comment une base de données fonctionne aujourd'hui
 - 1.2. Où les bases de données fonctionnent mieux et pourquoi une nouvelle technologie est nécessaire
2. Qu'est-ce que le peer-to-peer et en quoi diffère-t'il du paradigme de communication traditionnel
 - 2.1. Meilleures performances sur la distribution et la décentralisation des données
 - 2.2. Echec « no point »
3. Comment créer une base de données fiable dans un réseau P2P, la blockchain
 - 3.1. Comment le bloc d'informations est lié
 - 3.2. Pourquoi l'intégrité des données de la chaîne est presque garantie
4. Criticité et limites de la technologie blockchain, cas d'utilisation dans lesquels elle est appropriée ou non
 - 4.1. Pourquoi cela n'est utile que lorsque les informations doivent être échangées entre plusieurs sujets
 - 4.2. Meilleur scénario : plusieurs acteurs avec un manque de confiance totale
5. Cas pratiques réussis et éventuelles mises en œuvre futures
 - 5.1. Contrôle de la qualité et de la chaîne d'approvisionnement
 - 5.2. Plus de transparence dans le système de santé privé



Module d'apprentissage 2: Techniques de cryptage

Les technologies blockchain reposent sur une grande variété de primitives et de techniques cryptographiques pour garantir leur fonctionnement. Les blocs successifs d'une blockchain en constante croissance sont liés entre eux au moyen de fonctions de hachage cryptographiques. Les comptes sur une blockchain sont identifiés par des clés publiques cryptographiques et les clés privées correspondantes sont utilisées pour autoriser les transactions. Les techniques de chiffrement sont au cœur concept pour la compréhension des DLT en général, et des blockchains en particulier.

Le module d'apprentissage 2 présente et décrit en profondeur les concepts de cryptographie qui sont au cœur de la blockchain La technologie. Les principes de base de la cryptographie et de la cryptanalyse sont présentés dans un premier aperçu. Le concept de fonction de hachage est introduit et des exemples de fonctions de hachage et de leurs applications sont donné. Les techniques de cryptographie symétrique et asymétrique sont discutées en détail, avec des exemples et une session de laboratoire dédiée. Le concept de preuves à connaissance nulle est introduit et les applications de la cryptographie dans l'espace blockchain est discutée.

Prérequis :

Ce module n'a pas de prérequis.

Objectifs d'apprentissage :

- Présenter les caractéristiques clés de la cryptographie et ses utilisations possibles dans Blockchain.
- Présenter comparativement différents cryptosystèmes et leur évolution.
- Décrire le concept de fonction de hachage et présenter comparativement un ensemble de fonctions de hachage utilisé dans les systèmes basés sur la blockchain.
- Expliquer les concepts fondamentaux des systèmes de cryptographie symétriques et asymétriques.
- Présenter des techniques cryptographiques préservant la confidentialité et des preuves sans connaissance.
- Illustrer comment les techniques cryptographiques sont appliquées dans les systèmes basés sur la blockchain.
- Présenter des cas d'utilisation pertinents construits autour de la cryptographie Blockchain.

Résultats d'apprentissage :

- Comprendre les concepts clés de la cryptographie.
- Examiner quel cryptosystème est le plus adéquat en fonction du cas d'utilisation prévu.
- Identifier et analysez les différentes fonctions de hachage.
- Identifier et analyser les applications de la cryptographie symétrique et asymétrique.
- Discutez et analysez les méthodes cryptographiques préservant la confidentialité et les preuves sans connaissance.



- Identifier et évaluer les applications des méthodes cryptographiques dans les systèmes basés sur la blockchain.
- Examiner comment les techniques de cryptage sont utilisées dans les cas d'utilisation pertinents de la blockchain

Syllabus :

1. Introduction à la cryptographie
 - 1.1. Qu'est-ce que la cryptographie?
 - 1.2. Classification des cryptosystèmes
 - 1.3. Principes de base
 - 1.4. Principaux cryptosystèmes classiques et évolution
 - 1.5. Conditions de cryptage parfaites
 - 1.6. Cryptanalyse
2. Fonctions de hachage
 - 2.1. Qu'est-ce qu'une fonction Hash?
 - 2.2. Types de fonctions de hachage : MD5, SHA-x
 - 2.3. Laboratoire : expérimenter les fonctions de hachage
3. Cryptographie symétrique
 - 3.1. Définition
 - 3.2. Cryptage Vernam, Flow et Block
4. Cryptographie asymétrique
 - 4.1. Définition
 - 4.2. Algorithmes d'échange de clés (Diffie-Hellman)
 - 4.3. RSA
5. Laboratoire : expérimenter le chiffrement symétrique et asymétrique
6. Aucune preuve de connaissance
7. Applications de la cryptographie blockchain
 - 7.1. Application dans les échanges QR
 - 7.2. Gérer les adresses Bitcoin et Ethereum



Module d'apprentissage 3: Mécanismes de consensus

L'un des problèmes centraux dans la conception d'un système blockchain est le choix du mécanisme utilisé par les nœuds du réseau pour parvenir à un consensus sur l'état du système de manière décentralisée sans recourir à un tiers de confiance central.

Le module d'apprentissage 3 explore les mécanismes actuels qui gèrent l'accord entre tous les nœuds qui participent à un système blockchain. Les mécanismes de consensus les plus utilisés seront discutés, avec un accent égal sur les aspects techniques et commerciaux du sujet.

Au début du module, la nécessité d'un mécanisme de consensus dans une configuration de base de données distribuée est présentée et les solutions pour les systèmes autorisés sont discutées. Le rôle de la théorie des jeux dans la conception ou un mécanisme de consensus est présenté. Une classification des différents mécanismes de consensus qui ont été mis en œuvre dans la pratique ou proposé en théorie dans les deux grandes catégories de preuve de travail (PoW) et les mécanismes de Proof of Stake (PoS) sont donnés et les attaques potentielles sur ces les mécanismes sont décrits. Par la suite, une cartographie des différents mécanismes au compromis entre les incitations à maintenir la blockchain et la sécurité contre les attaques malveillantes qui peuvent compromettre l'intégrité de la blockchain, en tenant particulièrement compte de la position que chaque le mécanisme occupe dans l'espace centralisation-décentralisation est présenté. La dernière partie du module présente un ensemble d'études de cas pratiques.

Les participants qui terminent ce module seront en mesure de saisir les avantages et les inconvénients de tout protocole de consensus dans le cadre de tout modèle économique spécifique basé sur un registre distribué ainsi que ses limites en termes de précision, de rentabilité, de degré de décentralisation, d'évolutivité, de débit et durabilité du réseau.

Prérequis :

Ce module d'apprentissage a les prérequis suivants :

- Conception de bases de données P2P (LM1)
- Techniques de cryptage (LM2)

Objectifs d'apprentissage :

- Expliquer la nécessité d'un mécanisme de consensus dans un système basé sur la blockchain.
- Présenter les mécanismes de consensus utilisés dans les configurations de blockchain autorisées
- Discuter du rôle de la théorie des jeux dans la conception d'un mécanisme de consensus.
- Présenter les protocoles de consensus Proof-of-Concept (PoX) plus largement utilisés dans les systèmes blockchain
- Discuter d'éventuelles attaques contre les protocoles de consensus distribués.
- Présenter et décrire les structures d'incitation utilisées dans les protocoles de consensus distribué.
- Présenter des attaques contre les protocoles de consensus liés aux structures d'incitation.



- Discuter des coûts des protocoles de consensus distribués couramment utilisés.
- Discuter des performances et des propriétés d'évolutivité des protocoles de consensus distribués largement utilisés.
- Présenter des solutions aux problèmes d'évolutivité basées sur des alternatives aux protocoles de consensus distribués utilisés des systèmes basés sur la blockchain.
- Présenter des cas d'utilisation de différents mécanismes de consensus distribués dans différentes blockchain systèmes.

Résultats d'apprentissage :

- Comprendre le rôle du consensus dans les DLT et les systèmes Blockchain.
- Comprendre le fonctionnement des protocoles de consensus distribués de type PoX.
- Comprendre les attaques possibles ou les protocoles de consensus distribués.
- Comparer les coûts, les performances, l'évolutivité et la sécurité entre les protocoles de consensus en analysant leurs spécifications de conception.
- Évaluer les caractéristiques souhaitées d'un protocole de consensus pour un modèle d'entreprise spécifique.

Syllabus :

1. Introduction
 - 1.1. La nécessité de mécanismes de consensus
 - 1.2. Blockchains autorisées : consensus via le vote byzantin tolérant aux pannes (BFT) mécanismes
2. Le rôle de la théorie des jeux par consensus
3. Protocoles de preuve de concept (PoX)
 - 3.1. Le concept de consensus probabiliste et ses propriétés
 - 3.2. Loteries de puzzle cryptographiques et leurs propriétés requises
 - 3.3. Principaux protocoles : Preuve de travail, Preuve d'enjeu, Preuve d'enjeu déléguée, Preuve d'autorité
 - 3.4. Une taxonomie d'attaques potentielles : attaques Sybil, attaques raciales, attaques Finney, 51% attaques
4. Incitations
 - 4.1. Théorie de base : coûts irrécupérables, problèmes principal-agent et compatibilité des incitations
 - 4.2. Compatibilité incitative dans les protocoles PoX: jetons, pools de minage et cartels miniers
 - 4.3. Marchés en jetons
 - 4.4. Vulnérabilités des protocoles PoX: extraction égoïste, retenue de bloc, pools de minage en attente, pool sautillant
5. Coûts
 - 5.1. La nature coûteuse des protocoles PoX
 - 5.2. Protocoles Proof-of-Stake (PoS) et la tragédie du problème des communs
 - 5.3. Problèmes de sécurité dans les protocoles PoS: attaques sans enjeu, attaques par broyage
6. Performance
 - 6.1. Les performances limitées des blockchains sans permission



- 6.2. Protocoles hybrides
- 6.3. Interopérabilité blockchain
- 6.4. Réseaux de chaînes de blocs non linéaires : protocole de sous-arbre le plus lourd observé (GHOST)
- 6.5. Protocoles basés sur le graphe acyclique direct (DAG)
- 7. Exemples
 - 7.1. Tissu Hyperledger (BFT)
 - 7.2. Bitcoin (PoW)
 - 7.3. Primecoin (PoUS)
 - 7.4. Filecoin (UPoW)
 - 7.5. SpaceMint (PoSP)
 - 7.6. Bytecent (PoH)
 - 7.7. Peercoin (PoS)
 - 7.8. Algorand (protocoles hybrides)
 - 7.9. Teechain sur Bitcoin (réseaux Side-chain)
 - 7.10. Implémentation Ethereum Casper (GHOST)
- 8. Pratique de la théorie des blocs
- 9. Cas d'utilisation : secteur financier, santé, services juridiques, défense, administration publique, industrie : Digitalisation, projets sociaux, lutte contre la pauvreté, gestion de l'identité individuelle



Module d'apprentissage 4: Signatures numériques

Les signatures numériques sont l'extension des signatures papier au domaine numérique qui est rendue possible grâce au développement de la cryptographie asymétrique. Comme les vraies signatures, elles sont un moyen de prouver l'identité et de certifier l'origine d'un message.

Le module d'apprentissage 4 décrit les propriétés et les exigences techniques nécessaires à la mise en œuvre des signatures numériques et des prérequis mathématiques. Les caractéristiques génériques d'une signature numérique des algorithmes sont ensuite présentés et des algorithmes spécifiques couramment utilisés dans les systèmes blockchain la mise en œuvre sont discutées en détail. Les algorithmes de signature numérique préservant la confidentialité sont discutés, en se concentrant sur leur utilisation dans l'espace crypto-monnaie et les concepts d'anonymat et de pseudonymat de transaction sur une blockchain sont présentées. La sécurité des signatures numériques et les schémas d'attaque possibles sont considéré et une analyse approfondie d'un vecteur d'attaque possible est analysée dans un laboratoire. La dernière partie de la Le module traite de l'avenir des signatures numériques, présentant de nouveaux algorithmes conçus pour résister aux menaces présentes et prévues liées à l'avènement des ordinateurs quantiques.

Prérequis :

Ce module d'apprentissage a les prérequis suivants:

Techniques de cryptage (LM2)

Objectifs d'apprentissage :

- Expliquer les propriétés de base qu'un algorithme de signature numérique doit satisfaire.
- Présenter les algorithmes de signature numérique les plus largement utilisés dans les systèmes basés sur la blockchain
- Présenter des algorithmes de signature numérique préservant la confidentialité.
- Discuter des fonctionnalités d'anonymat et de pseudonymat des systèmes blockchain.
- Présenter les attaques et les problèmes de sécurité liés aux algorithmes de signature numérique.
- Présenter au-delà du développement de pointe lié aux algorithmes de signature numérique.
- Présenter des cas d'utilisation de signatures numériques dans des systèmes basés sur la blockchain.

Résultats d'apprentissage :

- Comprendre les propriétés fondamentales des algorithmes de signature numérique.
- Comprendre les détails des algorithmes de signature numérique les plus utilisés
- Acquérir des compétences techniques liées à l'utilisation des signatures numériques.
- Comprendre le fonctionnement des algorithmes de signature numérique préservant la confidentialité.
- Réciter les attaques possibles sur les algorithmes de signature numérique couramment utilisés.

*Syllabus :*

1. Définitions, propriétés et demandes de signature
2. Préliminaires
 - 2.1. Courbes elliptiques
 - 2.2. Lab: la bibliothèque bitcoin-core / secp256k1
3. Algorithmes de signature numérique
 - 3.1. Introduction
 - 3.2. DSA
 - 3.3. ECDSA
 - 3.4. Signatures Schnorr
 - 3.5. Lab: implémentation et analyse des signatures Schnorr
4. Signatures d'anneau
 - 4.1. Propriétés
 - 4.2. Le rôle des signatures en anneau dans la blockchain Monero
 - 4.3. Laboratoire : implémentation de signatures en anneau
5. Anonymat et pseudonymat dans les transactions blockchain
6. Sécurité et attaques
 - 6.1. Vue d'ensemble des problèmes de sécurité et des attaques
 - 6.2. Lab: attaque spécifique sur les signatures Schnorr
7. L'avenir des signatures numériques : treillis, signatures de hachage et signatures de seuil
8. Cas d'utilisation



Module d'apprentissage 5: Contrats intelligents

Le terme «contrats intelligents» est utilisé avec deux interprétations distinctes:

- «Un contrat intelligent est un ensemble de code (ses fonctions) et de données (son état) qui réside dans un adresse sur la blockchain. »
- «Un contrat intelligent (en tant que contrat) est un protocole informatique destiné à faciliter, vérifier ou faire appliquer la négociation ou l'exécution d'un contrat. »

Le module d'apprentissage 5 examine les problèmes de conception des applications basées sur la blockchain (contrats intelligents) exécuter automatiquement les termes d'un contrat, en se concentrant à la fois sur les aspects technologiques et commerciaux du matière.

Le module commences par une introduction au concept de Smart Contract et une description de son historique développement. Un aperçu des langages de programmation utilisés pour le développement de contrats intelligents pour les systèmes blockchain et les environnements d'exécution sont présentés, suivis d'une description détaillée Machine virtuelle Ethereum et un laboratoire thématique sur le développement du contrat intelligent pour l'Ethereum plateforme utilisant le langage de programmation Solidity. Oracles, une catégorie spéciale de contrats intelligents qui communiquer avec des entités de confiance, sont décrits en détail. Coûts de calcul et problèmes de sécurité La programmation des contrats intelligents est discutée et les meilleures pratiques adoptées pour atténuer les problèmes et les risques présenté. Enfin, les Smart Contracts pourraient être utilisés comme contrat, les principaux enjeux réglementaires et juridiques sur les contrats intelligents doivent être identifiés et décrits.

Prérequis :

Ce module d'apprentissage a les prérequis suivants:

- Mécanismes de consensus (LM3)
- Signatures numériques (LM4)

Objectifs d'apprentissage :

- Pour définir et expliquer les propriétés de base d'un contrat intelligent.
- Présenter différents langages de programmation utilisés pour développer des contrats intelligents et leur execution environnements.
- Décrire la blockchain Ethereum et la machine virtuelle Ethereum.
- Expliquer comment utiliser le langage Solidity pour développer un Smart Contract pour l'Ethereum Blockchain.
- Présenter le concept d'Oracles leurs principes de fonctionnement de base.
- Discuter des coûts de calcul du déploiement et de l'exécution d'un contrat intelligent et du role Gaz sur la blockchain Ethereum.



- Discuter des problèmes de sécurité liés au développement et à l'utilisation des contrats intelligents.
- Présenter les cadres réglementaires affectant l'utilisation des Smart Contracts.
- Présenter les problèmes juridiques liés à l'utilisation de contrats intelligents dans un système basé sur la blockchain.

Résultats d'apprentissage :

- Décrire les concepts de base des contrats intelligents.
- Reconnaître les différents langages de programmation de Smart Contracts et leur execution environnements.
- Identifier les principales caractéristiques des différents langages de programmation de Smart Contracts.
- Décrire la blockchain Ethereum.
- Expliquer le fonctionnement de la machine virtuelle Ethereum.
- Mettre en œuvre des contrats intelligents dans Ethereum en utilisant Solidity.
- Examiner le coût de calcul du déploiement et de l'utilisation d'un contrat intelligent dans Ethereum.
- Démontrer les cas d'utilisation de Smart Contracts dans plusieurs domaines.
- Comprendre les restrictions et limitations des technologies actuelles.
- Identifier les problèmes liés au développement de contrats intelligents.
- Examiner les avantages et les inconvénients de l'utilisation d'un contrat intelligent.
- Identifier les préoccupations concernant la sécurité, la stabilité et le coût d'un contrat intelligent.
- Évaluer si une solution Smart Contract est adaptée au problème étudié.
- Évaluer comment et quand appliquer des contrats intelligents dans des applications réelles.
- Mettre en œuvre des contrats intelligents dans des applications réelles.

Syllabus :

1. Introduction aux contrats intelligents
 - 1.1. Définitions de base du contrat intelligent
 - 1.2. Où est exécuté un contrat intelligent?
 - 1.3. Comprendre la machine virtuelle d'une blockchain
 - 1.4. Affichage du code source d'un contrat intelligent
 - 1.5. Terminologie et concepts utiles n Contrats intelligents
 - 1.6. Bonnes pratiques dans l'utilisation des Smart Contracts
2. Introduction aux contrats intelligents Ethereum et à la machine virtuelle Ethereum (EVM)
 - 2.1. Prévalence de la blockchain Ethereum dans le développement de contrats intelligents
 - 2.2. Ether et gaz: le coût de l'exécution d'un contrat intelligent
 - 2.3. Obtenir un avant-goût: exemples de travail d'Ethereum Smart Contract
 - 2.4. Plusieurs contrats intelligents travaillant ensemble
3. Confiance, sécurité et efficacité ou contrats intelligents «sur le terrain»
 - 3.1. Impact sur le marché et innovation scientifique du contrat intelligent
 - 3.2. Comprendre la confiance



- 3.3. Construire des systèmes résistants au futur à l'aide de contrats intelligents
- 3.4. La double importance de la sécurité dans les contrats intelligents
- 3.5. Nouveauté des contrats intelligents
- 3.6. Hacks et scandales célèbres liés aux contrats intelligents
4. Langages de programmation et environnements d'exécution Smart Contract
 - 4.1. Rédaction de contrats intelligents
 - 4.2. Le flux de travail de l'élaboration d'un contrat intelligent
 - 4.3. La responsabilité du programmeur lors de la rédaction du Smart Contract
 - 4.4. Coût de l'exécution des contrats intelligents
 - 4.5. Présentation des différentes plateformes de développement de Smart Contract et de leurs différences
 - 4.6. Choisir la bonne blockchain pour vous: où développer votre contrat intelligent
5. Développer des contrats intelligents sur la blockchain Ethereum
 - 5.1. Le langage Solidity: un langage de haut niveau orienté objet pour la mise en œuvre de contrats intelligents
 - 5.2. Concevoir un contrat intelligent de solidité
 - 5.3. Exemples pratiques de contrats intelligents Solidity
6. Services Oracle
 - 6.1. Définition d'un Oracle blockchain: ce qu'ils sont, ce qu'ils font
 - 6.2. Injecter des données vérifiables sur la blockchain
 - 6.3. Points d'étranglement de centralisation introduits par les services Oracle
 - 6.4. Service Oracle décentralisé
7. Problèmes de sécurité dans les contrats intelligents et répercussions
 - 7.1. Passer de la confiance dans les personnes à la confiance dans le code
 - 7.2. Permanence des données dans la transaction Smart Contract
 - 7.3. Obscurité sélective dans les données de contrat intelligent
 - 7.4. Disponibilité quantique de votre contrat intelligent
 - 7.5. Responsabilité du développeur lors de la rédaction d'un contrat intelligent
 - 7.6. Smart Contract End of Life: rester agile
 - 7.7. Forks (Hard & Soft) et contre-mesures de sécurité communautaire contre l'exploit Smart Contract
8. Scénarios du monde réel d'utilisation des contrats intelligents (cas d'utilisation)
 - 8.1. Les contrats intelligents mis en œuvre: des cas d'utilisation réels
 - 8.2. Le paradigme Ant in the Anthill: les développeurs recherchant la meilleure plateforme pour écrire Smart
9. Contrats sur
 - 9.1. Opportunités de départ: concours de développement, primes, financement de projets Smart Contract
10. Contrats intelligents en entreprise
 - 10.1. Comment les contrats intelligents élèvent le paysage commercial européen / international
 - 10.2. Un problème de jouet créatif: la gestion de la chaîne d'approvisionnement agricole à travers des contrats intelligents



10.3. Opportunités de financement et appels d'offres pour soutenir la mise en œuvre de systèmes de contrats intelligents

11. l'UE

11.1. Cadre juridique entourant l'utilisation des contrats intelligents

11.2. Hacks et attaques majeurs: dangers de l'utilisation de Open Smart Contract



Module d'apprentissage 6: Confidentialité et droits de propriété

L'informatique ne fonctionne plus dans le vide et en tant que telle, elle affecte et est affectée par la société. En outre, dans la plupart des cas, la technologie est en avance sur la société et la législation et, dans la plupart des cas, la société et la législation doit rattraper son retard et s'adapter à la nouvelle situation telle que définie par la technologie. En de rares occasions, cependant, la technologie vient en aide à la législation et à la société, et permet à certaines opérations de se déroulent de manière plus transparente et plus rapide que ne le permettent les pratiques actuelles.

Le module d'apprentissage 6 explique comment la technologie blockchain peut soutenir la législation sur les droits de propriété, à la fois tangible et intangible et décrit les problèmes liés à la confidentialité dans la blockchain. La législation européenne sur les droits de propriété et les licences sont présentés et comment les technologies de la blockchain pourraient aider à concevoir un salon le régime de rémunération est discuté. Le RGPD et les problèmes liés à la vie privée sont ensuite discutés ensemble avec une implication liée à l'immutabilité de la blockchain pour les droits qui doivent être garantis dans le cadre du RGPD (comme le droit d'être oublié). Enfin, les technologies pour améliorer la confidentialité des systèmes basés sur la blockchain sont présentés et les questions connexes discutées en détail.

Prérequis :

Ce module d'apprentissage a les prérequis suivants:

- Introduction au monde DLT (LM0)
- Contrats intelligents (LM5)

Objectifs d'apprentissage :

- Présenter le cadre législatif européen actuel relatif aux droits de propriété.
- Décrire les types existants de licences logicielles.
- Expliquer les lois internationales sur le droit d'auteur.
- Discuter de la coordination des licences et du rôle des registres.
- Discuter des problèmes liés aux droits de propriété qui surviennent lors de l'utilisation des DLT.
- Présenter le RGPD européen et ses implications pour la confidentialité et la liberté d'information.
- Discuter des problèmes liés au RGPD qui surviennent lors de l'utilisation des DLT.
- Présenter un ensemble de techniques de chiffrement préservant la confidentialité.
- Discuter des problèmes liés à la confidentialité qui surviennent dans un système basé sur DLT.
- Comprendre le RGPD et ses implications pour les technologies blockchain
- Comprendre comment éviter les conflits avec la loi lors de l'utilisation de la technologie blockchain.
- Décrire les droits de propriété peuvent être protégés en utilisant la blockchain.
- Comprendre comment les données personnelles peuvent être sous le contrôle des individus grâce à la technologie blockchain.



- Décrivez comment les investisseurs providentiels peuvent valoriser les entreprises liées à la blockchain.
- Récitez le rôle des droits de propriété intellectuelle pour encourager l'innovation et la créativité et comment la blockchain peut accueillir / faciliter les DPI.
- Comprendre comment les droits de propriété peuvent être protégés à l'aide de la technologie blockchain.
- Examiner les considérations de sécurité et de confidentialité de l'intégration du stockage

Syllabus :

1. Droits de propriété
 - 1.1. La législation relative aux droits de propriété intellectuelle (CPDA 1988)
 - 1.2. Qu'est-ce qu'une licence logicielle
 - 1.3. Types de licence
 - 1.4. Droit international du droit d'auteur
 - 1.5. Token comme licence?
 - 1.6. Commande privée
 - 1.7. Fragmentation
 - 1.8. Coordination des licences
 - 1.9. Registres
 - 1.10. Formalités
 - 1.11. Œuvres orphelines et domaine public
 - 1.12. Informations sur la gestion des droits
 - 1.13. Rémunération équitable
2. Problèmes de DLT relatifs aux droits de propriété
3. RGPD - Problèmes de confidentialité et de liberté de l'information
4. Problèmes DLT relatifs au RGPD
5. Techniques de cryptage appliquées pour la confidentialité
 - 5.1. Fonctions de hachage Chameleon
 - 5.2. Adresses furtives
 - 5.3. Transactions confidentielles par signatures en anneau
 - 5.4. Mettre en œuvre la confidentialité grâce à la preuve de zéro connaissance
 - 5.5. Contrats intelligents privés - Enigma
 - 5.6. Stockage hors chaîne
6. Problèmes de confidentialité ou DLT



Module d'apprentissage 7: Applications décentralisées basées sur la blockchain

Les applications décentralisées diffèrent des alternatives centralisées, car elles améliorent le réseau peer-to-peer des participants. La nécessité pour les parties à la transaction de communiquer sans le caractère essentiel d'un l'autorité est un sujet commun de discussion et d'évaluation parmi les passionnés de technologie. Tel Les applications décentralisées (dApps) peuvent perturber diverses industries, qui ont été présentées au public comme cas d'utilisation, par exemple dans la finance, le milieu universitaire, la chaîne d'approvisionnement, le secteur de l'énergie et autres.

Le module d'apprentissage 7 analyse les dApps sous tous leurs aspects et s'adresse à la fois aux techniques et aux non-techniques publiques, en gardant le sujet stimulant. L'objectif principal du module est de permettre aux participants d'évaluer quelles industries sont prêtes à adopter la technologie Blockchain et dans quelle mesure. La décentralisation et la désintermédiation sont des nouveaux concepts difficiles à saisir dans leur totalité. Il y a beaucoup de composants qui doivent être pris en considération, comme le degré de sécurité, de confidentialité et d'interopérabilité. Chaque réseau DLT varie dans la mesure de la satisfaction de ces composants. C'est d'une importance capitale pour les créateurs de contenu d'évaluer les meilleures pratiques et les lacunes potentielles de cette technologie. La structure de base et les principaux modèles de conception des dApps sont présentés comme une introduction aux bases du développement de dApps. Des cas d'utilisation de dApps avancés dans divers secteurs sont présentés avec leur relation avec d'autres technologies de rupture dans le cadre de la 4e révolution industrielle.

Prérequis :

Ce module d'apprentissage a les prérequis suivants :

- Introduction au monde DLT (LM0)
- Contrats intelligents (LM5)

Objectifs d'apprentissage :

- Présenter comparativement les conditions dans lesquelles les modèles centralisés traditionnels et les dApps peut être utilisé.
- Associer les caractéristiques clés des dApps aux propriétés fondamentales des blockchains.
- Expliquer la signification des exigences fonctionnelles et non fonctionnelles dans le contexte dApps.
- Présenter comparativement différentes blockchains comme candidats pour le développement de dApps.
- Illustrer la manière dont les informations circulent au niveau architectural des dApps.
- Présenter la pile technologique des dApps.
- Présenter un certain nombre de cas d'utilisation indicatifs construits autour des dApps.
- Expliquer les synergies possibles des dApps avec d'autres technologies émergentes.



- Discuter des éventuelles implications juridiques des dApps.

Résultats d'apprentissage :

- Évaluer si une dApp est requise par rapport au modèle centralisé traditionnel.
- Analyser les caractéristiques clés des dApps avec les propriétés fondamentales des blockchains.
- Identifier et analyser les exigences fonctionnelles et non fonctionnelles des dApps.
- Évaluez la pertinence des différentes blockchains pour les dApps.
- Concevoir des architectures de flux d'informations pour les dApps.
- Identifier et analyser les principales couches technologiques des dApps.
- Examiner comment les dApp sont utilisées dans des cas d'utilisation spécifiques.
- Reliez les dApps à d'autres technologies émergentes
- Identifier toutes les exigences susceptibles de soulever des problèmes juridiques

Syllabus :

1. Anatomie de haut niveau ou dApp
 - 1.1. Vue d'ensemble de la pile d'applications blockchain
 - 1.2. Exemples de backend
 - 1.3. Exemples de frontend
2. Modèles de conception dApp
 - 2.1. Modèles d'interaction avec le monde extérieur
 - 2.2. Modèles de gestion des données
 - 2.3. Modèles de sécurité
 - 2.4. Modèles structurels de contrat
3. Développement de base de dApps
 - 3.1. Programmation de blockchains publiques
 - 3.2. Programmation de blockchains privées / autorisées
 - 3.3. Cycle de vie des dApps
4. Cas d'utilisation de dApps avancés
 - 4.1. Marchés des changes décentralisés
 - 4.2. Marchés de données décentralisés
 - 4.3. Certificats vérifiables par blockchain et identités auto-souveraines
 - 4.4. Sujets émergents dans le cadre plus large des dApps
5. Passer des dApps au 4ème révolution industrielle
 - 5.1. La relation entre les technologies IoT, IA et blockchain



Module d'apprentissage 8: Organisations autonomes décentralisées

Les Organisations Autonomes Décentralisées (DAO) sont des organisations qui fonctionnent de manière autonome et pourraient prendre des décisions décentralisées grâce à l'utilisation de la technologie, par exemple la technologie Blockchain, Directed Acyclic Technologie Graphs (DAG), algorithme Hashgraph, etc. Une Organisation Autonome Décentralisée (DAO) est généralement une organisation exécutée via des protocoles codés sous la forme de divers types de programmes informatiques appelés contrats intelligents.

Les DAO sont parfois également appelés sociétés autonomes décentralisées (DAC). Leur transaction financière et les enregistrements de protocole de programme sont conservés sur la blockchain ou des technologies similaires. Ces types d'organisations sont similaires à toute organisation dans le monde réel, mais dans le monde numérique, les règles d'une organisation (par exemple une entreprise) ne sont pas appliquées numériquement. Elles sont déjà numériques par nature. Les DAO sont comme une démocratie cryptographique pour une organisation, où chaque partie prenante peut voter d'ajouter de nouveaux protocoles, modifier les protocoles existants ou inclure et exclure un membre parmi d'autres types de ce type des droits.

Le module d'apprentissage 8 examine les principales caractéristiques des DAO, ainsi que leurs avantages et inconvénients. Une attention particulière sera accordée aux implications juridiques, culturelles et politiques de l'utilisation de ce paradigme perturbateur. Une étude de cas d'un DAO est analysée en détail. Enfin, un laboratoire spécialement conçu pour le public technique expliquera comment implémenter les DAO dans l'infrastructure Ethereum.

Prérequis :

Le module d'apprentissage a les prérequis suivants :

- Introduction au monde DLT (LM0)
- Contrats intelligents (LM5)
- Confidentialité et droits de propriété (LM6)

Objectifs d'apprentissage :

- Introduire le concept d'Organisation Autonome Décentralisée (DAO) comme extension d'un dApp.
- Présenter la structure et les mécanismes de gouvernance au sein d'un DAO.
- Discuter des avantages et des inconvénients de l'utilisation d'un DAO pour gérer une organisation.
- Présenter les problèmes de sécurité, les problèmes de responsabilité juridique et les risques des DAO.
- Discuter des implications culturelles et politiques des DAO.



- Analyser en profondeur un cas d'utilisation spécifique de DAO.
- Présenter les développements futurs possibles des DAO.
- Démontrer comment implémenter un DAO sur la blockchain Ethereum en utilisant Solidity

Résultats d'apprentissage :

- Comprendre le concept de base de DAO.
- Comprendre les avantages et les inconvénients de l'utilisation des DAO.
- Réciter les risques juridiques et de sécurité des DAO.
- Décrire les études de cas les plus importantes utilisant les DAO.
- Implémenter un DAO dans Solidity.

Syllabus :

1. Introduction aux organisations autonomes décentralisées (DAO)
 - 1.1. Définition des DAO
 - 1.2. Des dApps aux DAO
 - 1.3. Structure des DAO
 - 1.4. La démocratie au sein des DAO
2. Avantages et inconvénients
 - 2.1. Avantages des DAO
 - 2.2. Inconvénients des DAO
 - 2.3. Défis avec les DAO
 - 2.4. Efficacité des DAO
3. Sécurité, responsabilité juridique et risques
 - 3.1. Sécurité des DAO
 - 3.2. Responsabilité juridique des DAO
 - 3.3. Risques liés aux DAO
4. Implications culturelles et politiques
 - 4.1. Différences culturelles et implications des DAO
 - 4.2. Systèmes politiques et mise en œuvre des DAO
5. Etude de cas sur les organisations autonomes décentralisées (DAO)
 - 5.1. Explorer un cas de DAO
 - 5.2. Leçons tirées de l'étude de cas
6. Avenir des DAO
7. Lab: Implémentation d'un DAO dans Solidity