Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

SECURITE DES BASES DE DONNEES (O7CYASBD)

Marwane Ayaida

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

sommaire

- Rappels
- Système décentralisé
- Protocole de Consensus
- Robustesse
- Soft et Hard Forks

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Rappels

- Nous avons vu comment fonctionne la Cryptographie asymétrique à clés publique/privée.
- Les deux principaux types de Hachage utilisés dans la Blockchain sont le Hachage simple et le Hachage à base d'arbre Merkle.
- Une combinaison de mécanismes de Hachage et de chiffrement est utilisée pour sécuriser les différents éléments de la Blockchain (transactions et blocs).
- La paire de clés publiques privées et le Hachage sont des concepts fondamentaux et importants dans les réseaux décentralisés qui fonctionnent au-delà des limites de confiance.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Système décentralisé

Objectifs de ce cours

- Vous serez en mesure de :
  - Définir les éléments de confiance dans une Blockchain tels que : la sécurité, la validation, la vérification et le consensus
  - Discuter le protocole de consensus qui est une approche algorithmique qui permet d'ajouter un nouveau bloc et de sécuriser la Blockchain
  - Expliquer la confiance et la robustesse de la chaîne principale
  - Illustrer la confiance dans la gestion de situations exceptionnelles telles que le « hard fork » et le « soft fork ».

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Système décentralisé

Exemple d'un scénario réel

- Exemple d'un système centralisé : système aéroportuaire
  - Vous voulez partir de l'aéroport CDG.
  - L'administration aéroportuaire va établir à l'avance un environnement sûr pour que les gens puissent partir:
    - Cela établit la confiance de base.
  - Ensuite, il y a une confiance supplémentaire une fois que vous entrez à l'aéroport et que :
    - votre passeport et vos documents de voyage sont vérifiés et validés.
    - vos bagages sont contrôlés.
  - Encore plus de confiance en vous est établie lorsque le personnel de la compagnie aérienne vérifie votre carte d'embarquement à la porte d'embarquement et que vous entrez dans l'avion pour voler.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Système décentralisé

Exemple d'un scénario réel

- Maintenant, considérons un système décentralisé :
  - Personne ne vérifie vos identifiants et certifie que vous êtes digne de confiance.
  - Alors, comment fait-on ?
    - On le fait en utilisant les algorithmes et les techniques discutés dans le dernier cours.
    - Examinons comment ceux-ci aideront à résoudre les problèmes de confiance dans une blockchain :
      - Comme dans notre scénario d'aéroport, la confiance dans une blockchain décentralisée consiste également à sécuriser, valider, vérifier et s'assurer que les ressources nécessaires à l'exécution des transactions sont disponibles.
      - Ceci est réalisé en sécurisant la chaîne à l'aide de protocoles spécifiques permettant de :
        - valider les transactions et les blocs pour éviter la falsification,
        - vérifier la disponibilité des ressources pour les transactions,
        - exécuter et confirmer les transactions.

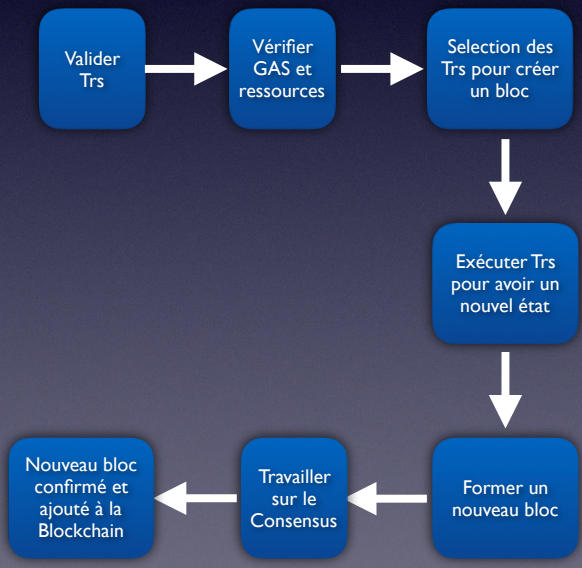
Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Système décentralisé

Le mécanisme de confiance

- Le mécanisme de confiance est défini par ces opérations :
  - valider les transactions,
  - vérifier le GAS et les ressources,
  - rassembler les transactions,
  - exécuter les transactions pour obtenir un nouvel état,
  - former le bloc,
  - travailler sur le consensus,
  - finaliser le bloc par le mineur gagnant,
  - tout le monde ajoute le bloc à sa chaîne et confirme les transactions.
- Par la suite, nous allons examiner chacune de ces étapes.



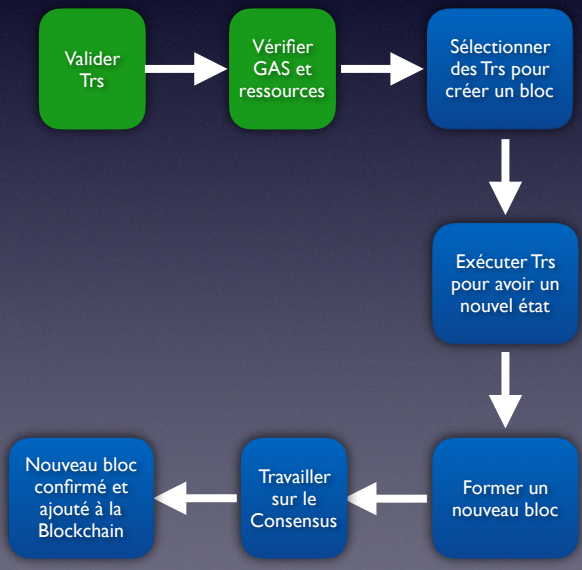
Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Système décentralisé

Le mécanisme de confiance

- Les étapes 1 et 2 concernent la validation des transactions et la vérification des ressources :
  - Dans le cas du Bitcoin, il y a environ 20 critères qui doivent être vérifiés avant qu'une transaction soit validée.
  - De la même manière dans le cas de la transaction Ethereum, il est vérifié avant l'exécution :
    - la syntaxe,
    - la signature de la transaction,
    - l'horodatage,
    - le Nonce,
    - la limite GAS,
    - le solde du compte de l'expéditeur,
    - le carburant ou les points de gaz,
    - les ressources disponibles pour l'exécution des Smart Contracts,
    - les signatures de la transaction et son hachage.



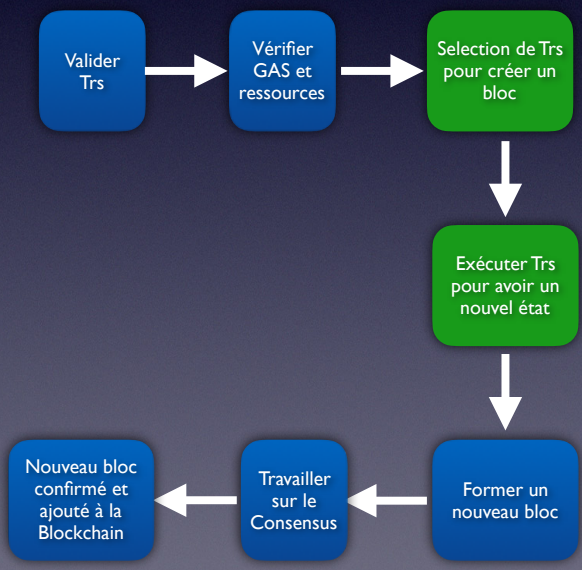
Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Système décentralisé

Le mécanisme de confiance

- Les étapes 3 et 4 concernent la sélection et l'exécution des transactions :
  - Le hachage à base d'arbre de Merkle des transactions validées est calculé :
    - C'est le cas dans Ethereum.
    - Il s'agit de la « Transaction Root » de l'en-tête du bloc.
  - Tous les mineurs exécutent la transaction pour le transfert d'Ether, ainsi que pour l'exécution des Smart Contracts.
    - L'état résultant de l'exécution des transactions est utilisé dans le calcul du hachage à base d'arbre de Merkle des états qui sera le « State Root » de l'en-tête de bloc.
  - Le « Receipt Root » de l'en-tête de bloc est également calculé.
- Dans la suite de ce cours, nous continuerons de parler des prochaines étapes du mécanisme de confiance qui concernent le processus de Consensus.



Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Système décentralisé

Quizz 1

La confiance dans une Blockchain décentralisée correspond en _____.

1. la sécurisation de la chaîne par des protocoles spécifiques.
2. la validation des transactions et des blocs pour l'inviolabilité.
3. l'exécution et la confirmation des transactions.
4. tout ce qui précède ✅

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Système décentralisé

Quizz 2

Les mineurs exécutent les transactions pour le transfert d'Ether mais ne sont pas responsables de l'exécution des Smart Contracts.

1. Vrai
2. Faux ✅

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Protocole de Consensus

Contexte

- Une chaîne sécurisée pour la Blockchain est une chaîne principale unique avec un état cohérent.
- Chaque bloc validé est ajouté à cette chaîne, il ajoute ainsi au niveau de confiance de la chaîne.
- Les mineurs sont en lice et rivalisent pour ajouter leur bloc à la chaîne.
- Que faire si tout le monde veut ajouter son bloc candidat à la chaîne ?
  - Chacun des blocs candidats est réalisé par un mineur concurrent.
    - Quel est le prochain bloc à ajouter à la chaîne ?
    - Peuvent-ils s'entendre sur le prochain bloc ?
    - Existe-t-il une méthode ou un protocole pour choisir le bloc suivant ?
  - Oui, il y en a ==> Cela s'appelle Proof of Work (Preuve de Travail).

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Protocole de Consensus

Proof of Work

- Le Proof of Work (PoW) utilise le Hachage : encore une autre application du hachage dans la Blockchain.
- Nous allons maintenant discuter le PoW comme utilisé dans le Bitcoin et historiquement dans Ethereum.
- Comment cela se passe du point de vue du mineur :
  - Tout d' abord, le mineur calcule le hachage des éléments de l'en-tête du bloc qui est une valeur fixe en utilisant un Nonce qui est lui variable :
    - Si le puzzle a été résolu :
      - condition pour Bitcoin : il faut un nombre spécifique de bits à zéro au début de la valeur du hash (ce nombre change à chaque fois tout les 2016 blocs dans le Bitcoin)
      - condition pour Ethereum : valeur hachée < fonction de difficulté
    - sinon, refaire l'opération après avoir modifié la valeur du Nonce —> consommation énergétique
  - Si le puzzle a été résolu, le mineur diffuse le bloc gagnant qui sera vérifié par les autres mineurs.
  - Les nœuds mineurs non gagnants ajoutent le nouveau bloc à la copie locale de leur chaîne et passent travailler sur le bloc suivant.
  - Le gagnant obtient un incitation pour avoir créer le bloc.
- Le PoW est un protocole de consensus utilisé par le Bitcoin et aussi par la version précédente d'Ethereum.
- Le protocole peut être le même, les implémentations dans ces deux Blockchain sont différentes.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Protocole de Consensus

Proof of Stake

- Les mineurs au Proof of Stake (PoS) doivent prouver qu'ils sont propriétaires d'un certain montant de la monnaie :
  - Pour être considéré comme validateur potentiel, il faut avoir au minimum 32 Ether dans son portefeuille.
- Après confirmation d'un certain nombre de transactions dans la Blockchain, le validateur récupère sa mise avec une récompense.
- Avantages du PoS Vs. PoW :
  - Il ne nécessiterait pas d'équipement minier coûteux et toute personne intéressée devrait pouvoir y adhérer.
  - On pense que les personnes disposant de plus de devises seraient moins susceptibles d'attaquer le réseau.
  - Contrôler la majorité du réseau coûterait cher aux validateurs, de sorte qu'un monopole deviendrait également très improbable.
  - Blockchain plus indépendante et éliminera le problème du monopole des pools de mineurs.
  - Ethereum estime économiser plus de 99% d'énergie en passant du PoW au PoS.
- Inconvénients du PoS Vs. PoW :
  - Malheureusement, comme le coût minier est presque nul, des attaques pourraient en découler.
  - La sélection est basée sur le solde du compte qui est assez injuste car la personne la plus riche est forcément dominante dans le réseau.
- Le 1er December 2020, Ethereum a lancé une Blockchain séparée basée sur PoS.
- Le 15 Septembre 2022, Ethereum a fusionné les deux Blockchains.
- De nombreuses Blockchains adoptent PoW au début et se transforment progressivement en PoS (comme Ethereum).

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Protocole de Consensus

Quizz 3

Le Proof of Work est _____ utilisé(e) par la blockchain Bitcoin et historiquement la Blockchain Ethereum.

1. La fonction incitative
2. La fonction de confiance
3. La confirmation de transaction
4. Le protocole de consensus ✅

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Robustesse

Définition de la robustesse

- La confiance doit être garantie non seulement avec l'exécution correcte des opérations régulières, mais aussi avec la gestion satisfaisante des exceptions.
- La robustesse est définie comme la capacité de gérer de manière satisfaisante des situations exceptionnelles.
- Ceci est d'autant plus important dans un réseau autonome décentralisé tel qu'une Blockchain où il n'y a pas d'intermédiaires.
- Nous ne discuterons que de deux exceptions dans ce cours :
  - Que se passe-t-il si plus d'un mineur résout le puzzle du consensus dans un temps très proche les uns des autres ?
  - Que se passe-t-il si plus d'une transaction fait référence comme entrée au même actif numérique ?
    - Cette situation est appelée « double dépense » ou « double spending »

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Robustesse

Cas 1 : résolution du puzzle en même temps

- Nous commençons par une Blockchain constituée de trois blocs et nous voulons ajouter un nouveau bloc.
- Deux mineurs ont résolu le puzzle en un temps très proche l'un de l'autre.
- Le protocole Bitcoin autorise une scission en deux chaînes pour le cycle suivant :
  - Un conduit par chacun des blocs concurrents.
  - La probabilité est faible que le prochain bloc :
    - se produise en même temps
    - dans ces deux chaînes.
  - Ainsi, le vainqueur du prochain cycle de création de blocs consolide l'une des chaînes et cette chaîne devient la chaîne acceptée.
  - Dans ce cas, le bloc le plus récent est ajouté à la chaîne principale.
- Maintenant, cette chaîne est la plus longue et devient la chaîne principale valide.
- Les transactions dans l'autre blocs sont renvoyées au pool des transactions non confirmées.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Robustesse

Cas 1 : résolution du puzzle en même temps

- Ethereum gère plus d'un mineur gagnant en autorisant les blocs « Ommers » ou « Runner-Up » (secondaires) et en allouant une petite incitation pour ces blocs secondaires.
- Ce modèle incitatif aide à maintenir la Blockchain sécurisée.
- Les nouveaux blocs sont ajoutés uniquement à la chaîne principale et donc il n'y a pas de chaîne secondaire.
- Les blocs secondaires sont maintenus pour six blocs après qu'ils soient ajoutés.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Robustesse

Cas 2 : double dépense

- Il es possible que la cryptomonnaie et d'autres consommables soient des actifs numériques à usage unique.
- Ils peuvent être réutilisés intentionnellement ou par inadvertance dans des transactions différentes.
- Revenons à notre analogie avec le système aéroportuaire :
  - C'est comme si une compagnie aérienne fait une double réservation pour un siège sur un vol.
  - Dans ce cas, l'agent d'escale va essayer de résoudre ce problème en utilisant des méthodes ad hoc telles que demander aux volontaires de renoncer à leurs sièges en leur proposant de l'argent en contrepartie, etc.
  - Dans un réseau décentralisé, comme une Blockchain, il n'y a pas d'intermédiaire.
  - Nous avons besoin d'une politique et d'une méthode déterministe automatique pour gérer cette situation.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Robustesse

Cas 2 : double dépense

- Solution dans le Bitcoin :
  - La politique de gestion des transactions et des double dépenses dans Bitcoin est d'autoriser la première transaction qui référence l'actif numérique et de rejeter le reste des transactions qui référencent le même actif.
- Solution dans le Ethereum :
  - Une combinaison entre l'adresse du compte et le Nonce globale est utilisée pour résoudre le problème de la double dépense.
  - Chaque fois qu'une transaction est initiée par un compte, un Nonce globale est inclus dans la transaction.
  - Après cela, le Nonce doit être incrémenté.
  - Le couple horodatage et le Nonce dans la transaction doit être unique et doit être vérifié afin d'éviter toute double utilisation du même actif numérique.
- Des processus bien définis pour la gestion des exceptions améliorent la confiance dans la Blockchain.
- Il y a beaucoup d'autres exceptions telles que le Hard et le Soft Forks qui seront discutées dans la suite de ce cours.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Robustesse

Quizz 4

Que se passe-t-il si plus d'un mineur résout le puzzle du consensus en un temps très proche dans Ethereum ?

1. Les mineurs secondaires quittent le réseau.
2. Des petites incitations sont accordées aux blocs secondaires et le nouveau bloc est ajouté à la chaîne principale. ✅
3. Le nouveau bloc est ajouté à la chaîne principale et non à la chaîne secondaire.
4. Des petites incitations sont accordées aux blocs secondaires.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Soft et Hard Forks

Forks et confiance

- Un Fork : c'est une bifurcation dans un chemin.
- Les Hard Fork and Soft Fork sont l'une des notions les plus courantes dans le contexte d'une Blockchain.
- Par exemple, Ethereum a fait un Hard Fork au bloc 4,7 millions.
- L'année 2018 est l'année des Hard Forks pour Ethereum.
- Dans ce cours, nous expliquerons à haut niveau, les Hard et Soft Forks.
- Les Forks sont juste des processus normaux dans l'évolution de la technologie naissante permettant de mettre en oeuvre la Blockchain.
- Si la robustesse et la confiance sont liées à la gestion des situations exceptionnelles, les Hard et Soft Forks sont en effet à la base de la Blockchain.
- Nous avons discuté de la scission de la Blockchain précédemment :
  - C'est considéré comme une perturbation mineure dans la chaîne.
  - Une telle situation est traitée comme une occurrence naturellement attendue dans la Blockchain.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Soft et Hard Forks

Soft et Hard Forks ?

- Occasionnellement, un ajustement mineur du processus doit être effectué généralement en intégrant un nouveau logiciel sur les processus déjà en cours d'exécution :
  - C'est un Soft Fork.
  - Par exemple, le concept du Pay-to-Script-Hash (P2SH) dans le Bitcoin (scripting avec conditions) a été introduit en utilisant cette méthode.
  - Vous pouvez considérer cela comme un correctif logiciel ou un correctif de bogue pour résoudre un problème.
  - La Blockchain reste valide et rétro-compatible après l'application du Soft Fork.
- Le Hard Fork implique un changement majeur dans le protocole.
  - Par exemple, le changement d'Ethereum Homestead à Metropolis Byzantium était un Hard Fork planifié.
  - Après un Hard Fork, les deux chaînes émergentes sont incompatibles.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Soft et Hard Forks

Exemple imprévu de Hard Fork dans Ethereum

- Exemple : Il y avait un Hard Fork imprévu dans le protocole Ethereum, Ethereum Core et Ethereum Classic split, qui a été adopté pour résoudre un problème logiciel critique :
  - Application des Smart Contracts : « Decentralized Autonomous Organizations »
    - Les DAO sont des organisations où les individus peuvent mettre de l'argent en commun et voter sur la façon de le dépenser.
  - En 2016, l'une de ces premières organisations, nommée « The DAO », a lancé un projet de financement participatif sur la Blockchain Ethereum :
    - créer un marché décentralisé où les gens pourraient partager des choses comme des véhicules ou des espaces de vie (pensez à Airbnb, mais sur une Blockchain décentralisée).
    - Cette idée est devenue populaire et a levé ce qui valait plus de 150 millions de dollars en ETH à l'époque auprès d'investisseurs du monde entier.
    - Des failles de sécurité dans le code ont laissé exposé la DAO et un pirate a pu siphonner plus de 3,6 millions de pièces ETH (d'une valeur d'environ 60 millions de dollars au moment de l'attaque).
  - Pour résoudre la perte des fonds pour leurs utilisateurs, Ethereum a exécuté un Hard Fork pour faire revenir en arrière la Blockchain Ethereum et effacer les transactions où les fonds ont été volés.
  - Ensuite, ils ont réaffecté les Ethers détenus dans le projet de financement participatif DAO à un autre Smart Contrat sur le réseau, ce qui a permis aux investisseurs de retirer les fonds qui avaient été volés.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Soft et Hard Forks

Exemple imprévu de Hard Fork dans Ethereum

- De nombreux utilisateurs du réseau Ethereum n'étaient pas d'accord avec la solution du Hard Fork.
  - Pourquoi? L'un des principes fondamentaux de la technologie Blockchain est le concept d'immuabilité du Ledger de la Blockchain qui est censé être permanent et immuable.
  - Donc, remonter le Ledger avant l'incident du piratage a violé ce principe et il est devenu controversé parmi les utilisateurs d'Ethereum et d'autres passionnés de crypto-monnaie.
- Donc cela a créer deux groupes :
  - Des utilisateurs qui ont accepté la mise à jour (en particulier, les victimes du piratage de la DAO)
    - Cette Blockchain a continué ce qu'on appelle aujourd'hui la Blockchain Ethereum avec ETH.
  - Des utilisateurs qui n'étaient pas d'accord avec le Hard Fork voulaient conserver l'ancienne programmation qui inclut les transactions du piratage de la DAO, car :
    - Les Smart Contrats sont conçus pour fonctionner sans aucune autorité centrale.
    - Ce qui signifie qu'en dehors du code lui-même, aucune partie au pouvoir n'est autorisée à modifier les règles, à valider ou à invalider des transactions.
    - En intervenant et en essayant de résoudre le problème, les responsables d'Ethereum sont allés à l'encontre du mouvement de décentralisation et ont agit en tant qu'organe directeur.
    - Cette Blockchain a continué sans effacer ces transactions et elle est devenue ce qui est maintenant Ethereum Classic avec ETC et qui vaut moins que la Blockchain Ethereum.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Soft et Hard Forks

Principaux Hard Forks prévus dans Bitcoin

- Bitcoin XT a été l'un des premiers Hard Forks notables du Bitcoin :
  - Le logiciel a été lancé par Mike Hearn fin 2014 afin d'inclure plusieurs nouvelles fonctionnalités qu'il avait proposées.
  - Alors que la version précédente du Bitcoin autorisait jusqu'à sept transactions par seconde, Bitcoin XT visait 24 transactions par seconde.
  - Pour ce faire, il a proposé d'augmenter la taille des blocs d'un mégaoctet à huit mégaoctets.
  - Bitcoin XT a d'abord connu le succès, avec plus de 1 000 nœuds exécutant son logiciel à la fin de l'été 2015.
  - Cependant, quelques mois plus tard, le projet a perdu l'intérêt des utilisateurs et a été essentiellement abandonné.
  - Bitcoin XT n'est plus disponible, avec son site Web d'origine désormais disparu.
- Bitcoin Classic :
  - Lorsque Bitcoin XT a décliné, certains membres de la communauté souhaitaient toujours que la taille des blocs augmente.
  - En réponse, un groupe de développeurs a lancé Bitcoin Classic au début de 2016.
  - Contrairement à XT, qui proposait d'augmenter la taille du bloc à huit mégaoctets, Classic l'a augmenté à seulement deux mégaoctets.
  - Comme Bitcoin XT, Bitcoin Classic a suscité un intérêt initial, avec environ 2 000 nœuds pendant plusieurs mois en 2016.
  - Le projet existe également toujours aujourd'hui, certains développeurs soutiennent fortement le Bitcoin Classic.
  - Néanmoins, la plus grande communauté de crypto-monnaie semble être généralement passée à d'autres options.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Soft et Hard Forks

Principaux Hard Forks prévus dans Bitcoin

- Bitcoin Unlimited :
  - Bitcoin Unlimited est resté une sorte d'énigme depuis sa sortie début 2016.
  - Les développeurs du projet ont publié le code mais n'ont pas précisé le type de Fork dont il aurait besoin.
  - Bitcoin Unlimited se distingue en permettant aux mineurs de décider de la taille de leurs blocs jusqu'à 16 mégaoctets.
  - Malgré un certain intérêt persistant, le bitcoin Unlimited n'a en grande partie pas réussi à être accepté.
- Segregated Witness (SegWit) :
  - Le développeur du Bitcoin Core, Pieter Wuille, a présenté l'idée de Segregated Witness (SegWit) fin 2015.
  - En termes simples, SegWit vise à réduire la taille de chaque transaction Bitcoin, permettant ainsi à davantage de transactions d'avoir lieu à la fois.
  - SegWit était techniquement un Soft Fork.
  - Cependant, cela a aidé à déclencher d'autres Hard Forks après sa proposition.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Soft et Hard Forks

Principaux Hard Forks prévus dans Bitcoin

- Bitcoin Cash :
  - En réponse à SegWit, certains développeurs et utilisateurs du Bitcoin ont décidé de lancer un Hard Fork afin d'éviter les mises à jour du protocole qu'il entraînait.
  - Bitcoin Cash est le résultat de ce Hard Fork.
  - Il s'est séparé de la Blockchain principale en août 2017, lorsque les portefeuilles Bitcoin Cash ont rejeté les transactions et les blocs Bitcoin.
  - Bitcoin Cash reste le Hard Fork le plus réussi de la principale crypto-monnaie.
  - En juin 2021, il s'agissait de la onzième plus grande monnaie numérique en termes de capitalisation boursière, en partie grâce au soutien de nombreuses personnalités de la communauté des crypto-monnaies et de nombreux échanges populaires.
  - Bitcoin Cash autorise des blocs de huit mégaoctets et n'a pas adopté le protocole SegWit.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Soft et Hard Forks

Principaux Hard Forks prévus dans Bitcoin

- Bitcoin Gold :
  - Bitcoin Gold était un Hard Fork qui a suivi peu de temps après le Bitcoin Cash, en octobre 2017.
  - Les créateurs de ce Hard Fork visaient à restaurer la fonctionnalité de minage avec des unités de traitement graphique (GPU) de base, car ils estimaient que le minage était devenu trop spécialisé en termes d'équipement et matériel nécessaires.
  - L'une des caractéristiques uniques du Hard Fork Bitcoin Gold était une "pré-mine", un processus par lequel l'équipe de développement a extrait 100 000 pièces après le Fork.
  - Beaucoup de ces pièces ont été placées dans une "dotation" spéciale, et les développeurs ont indiqué que cette dotation sera utilisée pour développer et financer l'écosystème du Bitcoin Gold, une partie de ces pièces étant également réservée pour le paiement des développeurs.
  - En règle générale, le Bitcoin Gold adhère à de nombreux principes de base du Bitcoin.
  - Cependant, il diffère en termes d'algorithme du PoW qu'il exige des mineurs.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Soft et Hard Forks

Principaux Hard Forks prévus dans Bitcoin

- SegWit2x :
  - Lorsque SegWit a été implémenté en août 2017, les développeurs ont prévu une deuxième version pour la mise à niveau du protocole.
  - Cet ajout, connu sous le nom de SegWit2x, déclencherait un Hard Fork stipulant une taille de bloc de deux mégaoctets.
  - SegWit2x devait avoir lieu en tant que Hard Fork en novembre 2017.
  - Cependant, un certain nombre d'entreprises et d'individus de la communauté Bitcoin qui avaient initialement soutenu le protocole SegWit ont décidé de se retirer du Hard Fork SegWit2x pour des questions de divergences.
  - Le 8 novembre 2017, l'équipe derrière SegWit2x a annoncé que leur Hard Fork prévu avait été annulé en raison de divergences entre les précédents sponsors du projet.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Soft et Hard Forks

Principaux Hard Forks prévus dans Ethereum

- Ethereum Frontier :
  - Au début, la plate-forme Ethereum était conçue uniquement pour les développeurs, pas pour les utilisateurs finaux, car elle ne comportait que des interfaces en lignes de commande.
  - Cette période a été nommée Frontier en référence à American Frontier, une période historique connue sous le nom de Far West.
  - Les fondateurs du projet Ethereum ont indiqué que ce nom avait été choisi pour ressembler à un lieu offrant d'immenses possibilités, mais aussi des risques énormes:
    - la plate-forme offrait un potentiel énorme qui attirait de nombreux développeurs de Blockchain,
    - mais était également instable et devait être améliorée.
- Ethereum Homestead :
  - À la fin de la période de la frontière américaine, la vie devint plus calme:
    - les nouveaux venus aux États-Unis ont commencé à s'installer sur leurs terres,
    - construisant des maisons pour l'avenir.
  - Une situation similaire s'est également produite sur la plate-forme Ethereum.
  - Une fois les erreurs corrigées et la plate-forme adaptée aux utilisateurs finaux, Ethereum a lancé sa première version publique
  - Le Hard Fork d'Ethereum Homestead a introduit trois améliorations :
    - Suppression des privilèges de l'équipe Ethereum qui leur permettaient d'interrompre certaines activités pour une plate-forme plus autonome.
    - Ajout du portefeuille ETH appelé « Mist » qui permet de stocker des Ether, mais aussi d'exécuter des Smart Contracts.
    - Introduction du langage de programmation Solidity utilisé dans la plate-forme.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Soft et Hard Forks

Principaux Hard Forks prévus dans Ethereum

- Ethereum Metropolis :
  - Au cours du dernier trimestre de 2017, les fondateurs d'Ethereum ont décidé d'aller plus loin et d'introduire une nouvelle mise à niveau permanente appelée *Metropolis*.
  - Des noms de grandes villes ont été utilisés car plusieurs mises à jour à faire : Paris, London, Berlin, Istanbul, Constantinople, Byzantium, etc.
  - L'objectif principal de cette phase est de passer du PoW au PoS.
  - Exemples d'Ethereum Improvement Proposals (EIP) :
    - Byzantium : Octobre 2017
      - Elle a ouvert la voie à la méthode PoS en restructurant le système de récompense des mineurs de la Blockchain.
      - La récompense pour le minage d'un bloc a été réduite de 5 à 3 ETH.
      - Elle a également augmenté la confidentialité au sein du système.
    - Constantinople : Février 2019
      - Elle a permis d'améliorer la vitesse de traitement des transactions dans la Blockchain Ethereum.
      - Elle a modifié les coûts GAS des opérations pour la réduction des coûts des opérations de base.
      - Elle va plus loin dans le PoS.
    - Etc.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Soft et Hard Forks

Principaux Hard Forks prévus dans Ethereum

- Ethereum Serenity : la phase finale
  - Les fondateurs d'Ethereum essaient continuellement d'améliorer leur Blockchain, fournissant des alternatives et des mises à jour.
    - Même si la plate-forme est finalement passée entièrement au nouveau modèle Proof of Stake avec le Hard Fork Paris (The Merge) le 15 Septembre 2022.
    - Le Hard Fork Shanghai est prévu pour 2023 avec des améliorations.
    - Donc, la phase Metropolis n'est pas encore entièrement achevée…
  - Une fois passé ce stade, c'est alors qu'Ethereum atteindra son quatrième état, appelé Ethereum Serenity.
  - Comme le suggère le dictionnaire, c'est l'état de calme, de paix et de tranquillité.
  - À ce stade, la plate-forme Ethereum devrait atteindre son plein potentiel.
- Pour plus de détails : https://ethereum.org/en/history/

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Soft et Hard Forks

Soft et Hard Forks

• Les Soft Forks et les Hard Forks pour la Blockchain sont comme considérés, respectivement, comme la sortie de correctifs logiciels, et de nouvelles versions des systèmes d'exploitation.
• Les Forks sont des mécanismes qui ajoutent de la robustesse au framework de la Blockchain.
• Des Forks bien gérés aident à renforcer la crédibilité de la Blockchain en fournissant des approches pour gérer les défaillances inattendues et les améliorations prévues.

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Soft et Hard Forks

Quizz 5

La mise en oeuvre du nouveau logiciel sur les processus déjà en cours d'exécution est appelée _____.

1. Scripting
2. Soft Fork ✅
3. Hard Fork
4. Hashing

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Soft et Hard Forks

Quizz 6

Après un Hard Fork, les deux chaînes émergentes sont incompatibles.

1. Vrai ✅
2. Faux

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Soft et Hard Forks

Quizz 7

La Blockchain Bitcoin a implémenté un Soft Fork pour intégrer la _____.

1. Fonctionnalité de script de paiement conditionnel P2SH ✅
2. Division en Bitcoin Core et en Bitcoin Cash
3. Fonctionnalité Peer-to-Shell P2SH

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Les bases de la Blockchain

Post-it

- Nous avons étudié comment se gère la confiance dans un système décentralisé par tout d'abord la validation et la vérification des transactions

- Ensuite, nous avons regardé quelques exemples d'algorithmes de Consensus pour l'ajout de nouveaux blocs dans la blockchain : PoW dans le Bitcoin et PoS dans Ethereum, il en existe d'autres…

- La robustesse est définie comme la capacité de gérer de manière satisfaisante des situations exceptionnelles et on a vu deux cas d'exception : résolution du puzzle en même temps par plusieurs mineurs et la double dépense et nous avons étudié comment les Blockchains Bitcoin et Ethereum font pour les résoudre.

- On a vu aussi les notions de Soft Fork et Hard Fork pour la Blockchain qui sont des correctifs plus au moins importants et qui peuvent rompre la rétro-compatibilité qu'ils soient prévus ou non et on a détaillé des exemples des Forks.