Blockchain

Cours

Master 2 La Sorbonne Université

1

Description des forks

Consensus

- Le consensus est central pour de nombreuses classes d'actifs :
  - ❑Les actions peuvent être très impactées par un « spin-off » ou des fusions/acquisitions.
  - ❑Les monnaies peuvent être très impactées par des dévaluations ou des « pegs »/ « unpegs ».
  - ❑L'euro est le fruit d'un consensus des pays de l'Eurozone. On a vu que des possibilités de sortie de certains pays avait un fort impact sur son taux de change avec les autres monnaies.
- Nous verrons qu'il s'avère particulièrement important de prendre en compte les mécanismes de consensus pour valoriser des crypto-monnaies.

Introduction

- Afin de procéder aux étapes de validation, les membres du réseau doivent se mettre d'accord sur **un ensemble de règles** permettant de déterminer si une transaction ou un bloc est valide ou non. **Ainsi, le consensus est essentiel à la pérennité d'une blockchain.**
- Une **fork** est le nom donné à une situation où la chaîne principale se sépare en plusieurs chaînes. Cette séparation peut être engendrée par un fonctionnement « normal » du système et se résorber d'elle-même ou avoir pour origine des changements du protocole de la blockchain ou des désaccords dans la communauté d'utilisateurs de la blockchain.
- Rappel: dans le cas d'un stale block sur Bitcoin, **il y a consensus pour abandonner la chaîne minoritaire**.
- Les forks peuvent être classées en deux grandes catégories : les hard forks et les soft forks. Nous allons voir des exemples de chaque type.

Hard fork

- Une hard fork est une mise à jour du protocole de la blockchain qui modifie les règles existantes ou en introduit de nouvelles et n'est **pas compatible avec l'ancienne version du protocole**. Dans le cas d'une hard fork, les nœuds n'ayant pas mis leur protocole à jour considéreront les transactions et blocs suivant le nouveau protocole comme invalides et continueront de valider des blocs correspondants à l'ancienne version.
- Si cette mise à jour fait consensus dans le réseau, l'ensemble des membres du réseau feront la mise à jour et la chaîne à jour deviendra la nouvelle chaîne officielle du réseau.
- **Des problèmes apparaissent lorsque cette mise à jour ne fait pas consensus** dans le réseau. Dans ce cas une partie du réseau pourra décider de rester sur l'ancienne version de la blockchain et de garder cette chaîne comme chaîne officielle, quelque soit son hashrate. La blockchain sera alors séparée en deux blockchains « officielles » ayant leurs communautés et, potentiellement, leurs développeurs. On parle de « hard fork contentieux ».

Soft fork

- Une soft fork est une mise à jour de la blockchain qui est **compatible avec l'ancienne version du protocole**. Dans le cas d'une soft fork, les nœuds n'ayant pas fait la mise à jour considèreront les transactions et blocs correspondants à la nouvelle version comme valides. Ce type de fork affectera surtout les mineurs de blocs dans le cas d'une blockchain PoW. En effet, si un mineur n'ayant pas fait la mise à jour continue à miner des blocs, ceux-ci seront considérés comme non valides par la partie du réseau ayant fait la mise à jour.
- **Une mise à jour effectuée par soft fork n'affectera donc que peu les utilisateurs non mineurs** et aura besoin d'une majorité de hashrate pour s'imposer.
- Si la soft fork ne mobilise pas une majorité du hashrate, deux solutions sont possibles.
  - La mise à jour pourrait simplement être rejetée par le réseau et, dans ce cas, la chaîne pré-mise à jour redeviendra la chaîne officielle.
  - La soft fork peut agir comme une hard fork et les chaînes pré- et post-mise à jour peuvent devenir deux chaînes officielles indépendantes.

*Un projet de smart contract public : **The DAO***

1 The DAO (Distributed Autonomous Organisation) est une plateforme de crowdfunding gérée par un smart contract hébergé sur la blockchain Ethereum permettant de voter pour des projets afin de leur accorder des financements et versant des ETH (jetons d'Ethereum) lancé le 30 avril 2016.

2 Les développeurs ont pris un engagement juridique de ne jamais modifier le code du contrat.

3 Le 17 Juin 2016 le market cap de The DAO a atteint 160 millions $ avec plus de 10 000 investisseurs.

4 Un hacker trouve une faille dans le code et un moyen de « vider » progressivement la cagnotte sous-jacente de ce smart contract : chute de -50% du cours en 3h.

5 Les développeurs s'empressent de dire qu'ils vont modifier le code pour empêcher le hacker de percevoir ce qu'il a « vidé ».

6 Le hacker fait valoir ses droits juridiques : le code ne doit pas être modifié.

7 Un autre hacker effectue le même « vidage » que le premier.

Conséquence de The DAO : le fork d'Ethereum

8 Les core développeurs d'Ethereum ont proposé une modification de la blockchain « contraire aux principes» : prendre tous les ETH récupérés par le hacker et les renvoyer à une adresse « convenable » du projet the DAO, malgré l'absence d'activation de clé privée.

9 Certains ont refusé ce choix, et ont donc persisté à miner de nouveaux blocs sur les blocs « post-hack ».

10 Il y a donc eu fork : la blockchain Ethereum s'est séparée en deux, Ethereum (ETH) et Ethereum Classic (ETC). Le hacker a bien des ETC, mais pas d'ETH.

11 Les 2 blockchains semblent pérennes aujourd'hui.

Le cours de l'ETH sur la période

Une quasi-unanimité en faveur du fork

YES

Ether: 1509168.02434456247385697

NO

Ether: 42916.371718509800079

Vote d'adoption du hard-fork par la communauté d'utilisateurs d'Ethereum

Les cours ETH/ETC en juillet 2016

2

Le débat de la scalabilité de Bitcoin

Deux visions qui s'opposent

- Une controverse portant sur la meilleure manière d'augmenter la capacité du protocole Bitcoin remonte à environ 2015.
- Une partie de la communauté de Bitcoin était en faveur d'une augmentation de la limite de la taille des blocs au-delà de 1 Mb.
- L'autre partie de la communauté était en faveur de la conservation de la limite de taille des blocs à 1 Mb, et préférait **implémenter prioritairement Segregated Witness** (SegWit) afin de permettre à des solutions dites de "layer 2", telles que Lightning Network, de voir le jour.
- En effet, le déploiement du Lightning Network nécessite de résoudre le bug de la malléabilité des transactions, ce que permet SegWit.
- Fondamentalement, les **deux visions qui s'opposaient** étaient :
  - **Un scaling "on-chain"** : augmenter le nombre de transactions par seconde via l'augmentation de la taille des blocs, au fur et à mesure que les blocs se remplissent.
  - **Un scaling "off-chain"** : augmenter le nombre de transactions par seconde via la mise en place d'un réseau de canaux paiements qui peuvent faire transiter un nombre élevé de transactions, dont le clearing se fait seulement périodiquement sur la blockchain Bitcoin.

Une recherche de compromis

- Une augmentation de la taille des blocs nécessite un hard fork de Bitcoin alors que SegWit nécessitait seulement une soft fork.
- Les partisans de SegWit ont argumenté que le risque de disruption du réseau étant moins grand avec une soft fork. Ils ont également affirmé que l'augmentation de la taille des blocs allait réduire le nombre de nœuds et donc la décentralisation du réseau.
- De leurs côtés, les partisans de l'augmentation de la taille des blocs ont affirmé que la priorité était de faire baisser les frais de transaction immédiatement pour éviter que Bitcoin perde des parts de marché par rapport aux altcoins.
- Un compromis visant à la fois à implémenter SegWit avec une soft fork puis à effectuer trois mois une hard fork (pour faire passer la limite de la taille des blocs de 1 Mb à 2 Mb) a été signé par les principaux mineurs et les plus grosses entreprises de l'écosystème lors d'une conférence à New York au printemps 2017. C'est ce qui a permis d'envisager l'activation de SegWit après plus d'un an de blocage.
- Les partisans de la taille des blocs ont craint qu'une fois SegWit activé, les acteurs impliqués ne respecteraient pas leur engagement d'effectuer un hard fork trois mois plus tard pour augmenter la taille des blocs.

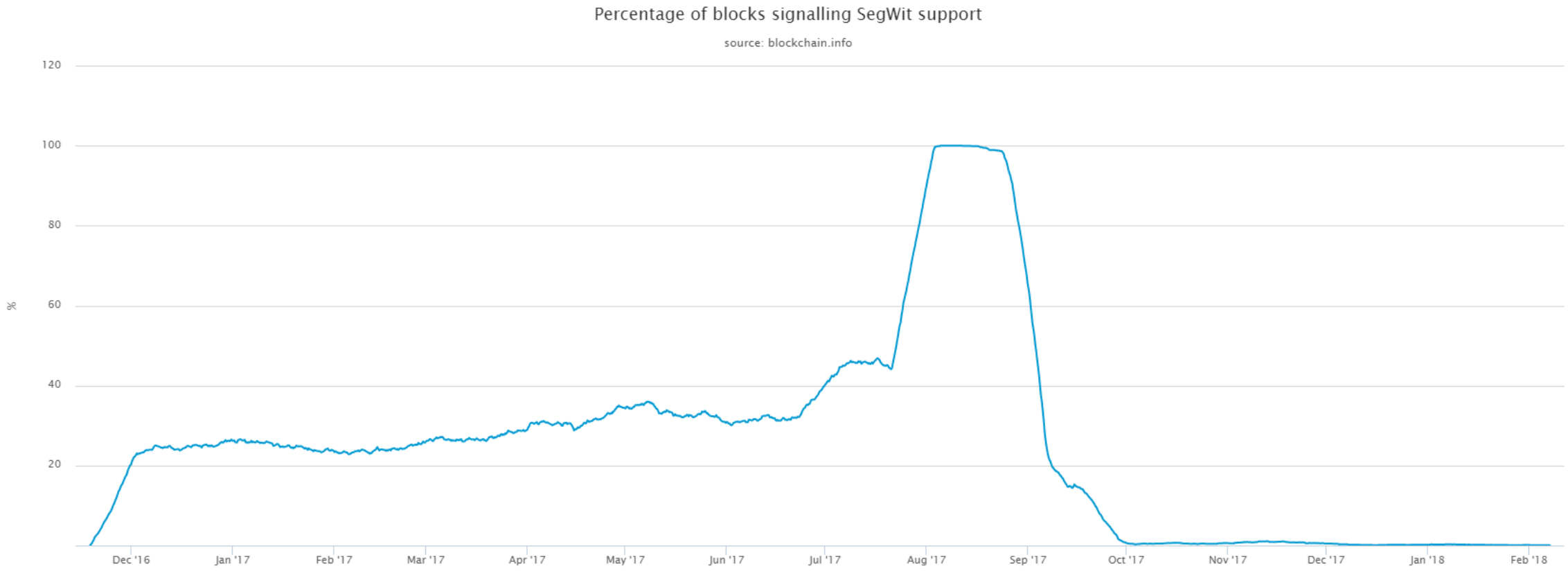
User Activated Soft fork (UASF)

- Afin qu'une soft-fork « standard » ait lieu, **les mineurs doivent signaler leur soutien** à la mise-à-jour en plaçant un identifiant dans les blocs qu'ils minent.
- Une User Activated Soft Fork (UASF) **ne requiert pas le soutien des mineurs afin d'être activée**. La nouvelle version du protocole est déployée et installée sur **les nœuds du réseau** validant les transactions.
- A partir de la date décidée de UASF, les nœuds ayant installé la nouvelle version du protocole ne valident plus que les blocs signalant leur soutien à cette mise-à-jour.
  - Exemple: A partir du bloc 468815 de Bitcoin, les nœuds ayant installé la mise-à-jour ne validaient plus que les blocs signalant leur soutien à Segwit. Au bloc 468815, 60% des nœuds du réseau ont fait la mise-à-jour, ainsi que de nombreux commerces et plateformes d'échanges.
  - A partir de ce point, si un mineur ne crée pas des blocs compatibles Segwit, ceux-ci seront ignorés par tous ces nœuds et commerces, ce qui pourrait lui être très couteux.
  - Les blocs Segwit sont compatibles avec l'ancienne version du protocole et seront validés par les nœuds n'ayant pas fait la mise-à-jour.
  - Il est alors potentiellement plus intéressant pour le mineur de miner un bloc compatible avec Segwit, qui sera validé par 100% des nœuds que de miner un bloc incompatible, qui ne sera accepté que par 40% des nœuds.
- Métaphoriquement, ***les utilisateurs imposent donc une mise à jour en faisant une clé de bras économique aux mineurs.***

Les modalités de l'implémentation de SegWit

- L'idée de SegWit est apparue en 2013 mais le projet fait vraiment surface en 2014 et est mis pour la première fois sur le devant de la scène en 2015 au cours des premiers débats sur la limite de taille des blocs de Bitcoin.
- L'architecture des blocs de Segwit a été imaginée de manière à pouvoir implémenter Segwit par soft fork. Cette mise à jour par soft fork a été proposée à la communauté Bitcoin le 21/12/2015 dans la « Bitcoin Improvement Proposal » 141. Afin de pouvoir être déployée, cette mise à jour requérait que 95% des mineurs lui signalent leur soutien.
- Devant l'impossibilité d'obtenir une adhésion si large et les problèmes croissant liés à l'engorgement du réseau Bitcoin, deux propositions ont vu le jour:
  - La première, nommée BIP 148, faite le 12/03/2017 consistait en une activation de Segwit le 1er août 2017 par UASF
  - La seconde, nommée BIP 91, faite le 17/07/2017 consistait en un relâchement du critère imposé par BIP 141. Ainsi, BIP 91 permettait l'activation de Segwit par le signalement du soutien à la mise à jour sur 80% des blocs dans une période de 336 blocs.
- A l'approche de la deadline de l'UASF, le soutien des mineurs en faveur de BIP 91 étant croissant, l'UASF a été repoussée afin de laisser à ces derniers le temps de faire passer BIP 91. Segwit a finalement été activé par BIP 91 le 09/08/2017.

L'évolution du signalement de SegWit par les mineurs



Le fork Bitcoin/Bitcoin Cash

- Alors que Segwit était sur le point d'être implémenté suite à un UASF, le 1er août 2017 a eu lieu la fork entre Bitcoin et Bitcoin Cash. Le dernier bloc commun entre ces deux blockchains est le bloc numéro 478 559.
- Ce jour-là, suite à l'upgrade protocolaire coordonné d'un sous-ensemble de nœuds, le réseau pair-à-pair de Bitcoin a été splitté en deux réseaux pair-à-pair distincts.
- A partir du bloc 478 560, un sous-ensemble des nœuds du réseau pair-à-pair à mis en place des règles de validation des blocs différentes de celles des nœuds du reste du réseau pair-à-pair.
- Plus spécifiquement, ce sous-ensemble de nœud a changé la limite de 1 Mb et l'a faite passer à 8 Mb. Ils se sont ainsi mis à déclarer valide les blocs ayant une taille jusqu'à 8 Mb.
- Par exemple, ***un bloc de 2 Mb est considéré comme valide par les nœuds du réseau Bitcoin Cash, mais n'est pas considéré comme valide par les nœuds du réseau Bitcoin***.
- Comme **les règles de validation des blocs étaient différentes sur ces deux réseaux**, les nouveaux blocs validés contenaient des ensembles de transactions différents. Ainsi, postérieurement au fork, **deux blockchains différentes, partageant un historique commun, sont apparues**.
- Ces deux blockchains ont un historique des transactions commun jusqu'au bloc du fork. Cela signifie qu'**un utilisateur qui avait des bitcoins (BTC) avant le fork détient, après le fork, à la fois des bitcoins (BTC) et des bitcoins cash (BCH).**
- En revanche, à partir du fork, il y a une divergence des blockchains et donc une divergence dans leur historique des transactions respectif. Ainsi l'utilisateur achetant un BTC ou un BCH après le fork, ne possède qu'une seule des deux crypto-monnaies.

Emergency Difficulty Adjustment 1/2

- Un changement additionnel introduit par Bitcoin Cash est celui de **la modification de l'algorithme d'ajustement de la difficulté de minage**.
- Cet algorithme, appelé **Emergency Difficulty Adjustement (EDA)**, a remplacé dans le protocole de Bitcoin Cash l'ajustement de la difficulté tous les 2 016 blocs en vigueur dans le protocole de Bitcoin.
- L'EDA était nécessaire pour permettre à la blockchain de Bitcoin Cash de survivre au cas où une faible proportion de la puissance de minage la soutienne.
- En effet, avec un ajustement tous les 2 016 blocs, il est nécessaire de miner 2 016 blocs, à la même difficulté qu'avant la fork, avec cependant une puissance de calcul très inférieure, avant le prochain ajustement de la difficulté à la baisse.
- Cela aurait pu potentiellement prendre des mois, voire des années, pour produire ces 2 016 blocs. De plus, lorsque les blocs produits sont peu fréquents, le réseau devient inutilisable pour effectuer des transactions. Cela aurait pu impacter négativement le prix de la crypto-monnaie, ce qui aurait renforcé l'incitation négative de miner un block sur cette blockchain pour les mineurs.
- Ce scénario aurait pu déclencher une spirale négative conduisant à l'abandon de la blockchain.

Emergency Difficulty Adjustment 2/2

- L'EDA prévoyait que s'il n'y avait pas de blocs qui avaient été minés lors des dernières 6 heures, il y avait un ajustement de la difficulté à la baisse lors du prochain bloc. La condition pour effectuer un ajustement était évaluée à chaque bloc miné, ce qui signifie qu'il pouvait y avoir plusieurs baisses de 20% successives.
- L'EDA a fonctionné comme prévu et il a permis à la blockchain de survivre, mais une fois la pérennité de la blockchain assurée, il a eu des effets négatifs en offrant la possibilité aux mineurs de manipuler ce système à leur profit, ce qui rendait l'intervalle entre la production de blocs très erratique sur Bitcoin Cash.
- C'est pourquoi a eu lieu le 13 novembre sur Bitcoin Cash une hard fork qui a remplacé l'EDA pour un nouvel algorithme d'ajustement de la difficulté.
- Ce nouvel algorithme ajuste dorénavant la difficulté à chaque bloc, selon le temps de minage des 144 derniers blocs.
- C'est pourquoi aujourd'hui, même si le Proof of Work de Bitcoin et Bitcoin Cash sont tous deux basés sur la fonction SHA256, leur algorithme d'ajustement de la difficulté n'est pas le même.

La fork Bitcoin/Bitcoin Cash a créé de la valeur 1/2

Du point de vue d'un détenteur de bitcoins, la fork a été profitable :

- Le 31 juillet à minuit (UTC), le prix d'un BTC était d'environ 2 850$
- Le 1er août à minuit : 1 BTC = 2 590$; 1 BCH = 690$

⇒1 BTC + 1 BCH = 3 280 $;

- Le 7 août minuit : 1 BTC = 3 430$; 1 BCH = 360 $

⇒1 BTC + 1 BCH = 3 790$;

- Le 31 août à minuit : 1 BTC = 4 735$; 1 BCH = 603$

⇒1 BTC + 1 BCH = 5 338$;

- Source de prix : Bitfinex.com qui a été une des premières plateforme d'échanges à permettre le trading et donc la cotation des BCH

La fork Bitcoin/Bitcoin Cash a créé de la valeur 2/2

- Une des idées dominantes jusqu'alors était qu'une hard fork non consensuel allait être destructeur de valeur en raison de la confusion qu'il allait créer pour les utilisateurs et la perte de sécurité due à la dispersion du mining sur les deux blockchains.
- Or il apparait au contraire que ***la hard fork a créé de la valeur pour les détenteurs de bitcoins pré-fork***. Ceci a été notamment démontré comme attendu théoriquement dans l'article « The Blockchain Folk Theorem » de Bruno Biais, Christophe Bisiere, Matthieu Bouvard et Catherine Casamatta.
- D'un point vue économique, on peut justifier cela par le fait que deux voies technologiques peuvent ainsi être explorées en parallèle, que cela met un terme à une situation de blocage, et que chacune des deux alternatives pourrait à terme adresser des besoins différents du marché.
- De telles forks peuvent-être assimilées à un spin-off d'entreprise, où les actionnaires détiennent des actions à la fois de l'ancienne et de la nouvelle entité créée.
- A terme, les forks pourraient s'avérer être des mécanismes d'évolution des blockchains efficaces : au lieu de perdre de l'énergie à convaincre l'ensemble d'une communauté des bienfaits d'une évolution technique et à devoir gérer la composante politique d'un tel processus, il est possible de simplement forker le réseau et ainsi de proposer un protocole alternatif au marché. De tels forks pourraient être un mécanisme permettant l'accélération de l'expérimentation et donc de l'innovation sur les blockchains.

Bitcoin Gold

- Suite à la fork réussi sur le plan technique de Bitcoin Cash (la blockchain a survécu) et sur le plan économique (de la valeur a été créée), des initiatives similaires ont vu le jour.
- La principale est celle de Bitcoin Gold qui a forké le 24 octobre à une hauteur de block de 491 407.
- L'objectif déclaré de cette fork est de permettre à nouveau le mining par GPU en remplacant l'agorithme de mining SHA256 par l'algorithme Equihash (utilisé notamment par Zcash)
- Cependant, cette initiative apparait essentiellement opportuniste car elle n'est pas réellement justifiée par une divergence fondamentale de vision concernant l'évolution technique du protocole. Par conséquent, elle a toutes les chances de se révéler anecdotique à terme. C'est également le cas, et à plus forte raison, pour toutes les forks qui lui ont suivi (Bitcoin Platinium, Bitcoin Diamond…)

Une problématique majeure lors d'une fork : la replay protection

- Exemple de **replay attack sur une fork BTC/Y**: on crée une transaction pour envoyer des BTCs reçus avant la fork à un autre utilisateur. Pour ce faire, on choisit un UTXO de cette chaîne à dépenser, on crée la transaction, on la signe et on envoie cette transaction dans le réseau P2P.
- Cependant, l'UTXO utilisée pour cette transaction existe aussi dans la chaîne Y. La transaction envoyée dans le réseau pour effectuer un paiement en BTC pourra donc être utilisée afin d'effectuer une copie de ce paiement en Y
- L'émetteur de la transaction transmettra alors, ***contre son gré***, des BTC ***et des Y*** tandis qu'il ne souhaitait transférer que des BTC. C'est la **replay attack.**
- La solution pour éviter la replay attack est de ne pas faire de transaction utilisant des UTXO pré-fork (dont deux copies identiques sont présentes sur les deux chaînes) avant que les développeurs n'aient mis le protocole à jour afin de rendre les replay attacks impossibles.
- **Pour les transactions ayant été signées après l'apparition de la fork, la replay attack est impossible** et il n'y a pas de risque. En effet, ces transactions n'existent que sur l'une des deux chaînes. Une transaction valide sur la chaîne où ces tokens sont présents ne sera donc pas valide sur l'autre chaîne.

La possession de sa propre clé

- Dans l'éventualité d'une fork, il est capital de stocker ses crypto-monnaies et tokens ***sur une adresse personnelle et non sur une plateforme d'échange***.
- En effet, une plateforme d'échange pourrait décider de ne lister que l'une des deux monnaies ou de ne reverser que la monnaie d'une chaîne à ses clients.
- Dans ces cas, les crypto-monnaies et tokens de l'autre chaîne stockés sur la plateforme d'échange ne pourront pas être retirés par l'utilisateur.
- Pour ne pas être soumis au bon vouloir et à la politique des plateforme d'échange, l'utilisateur devra retirer ses bitcoins des plateformes d'échange en prévision de la fork et les stocker sur un porte-monnaie personnel.

Des problématiques quantitatives émergentes

- De très fortes variations de cours émergent lors de « subdivisions » de blockchains suite à des forks.
- Un marché des futures liés aux crypto-monnaies issues de possibles forks commence à émerger sur certains exchanges.
- **De nouveaux besoins de modèles émergent**.