Développeur blockchain

Introduction

Les dessous des blockchains

ALYRA

cyril@alyra.fr / benjamin.brucher@alyra.fr

Promo Buterin

Topo du live

Une histoire des réseaux

Première approche

Définir la blockchain

Ses caractéristiques

Cryptographie

Consensus

ALYRA

Histoire d'internet "Choisie"

- Arpanet – un réseau universitaire et militaire
- Web 1.0 – un internet d'information mais grand public
- Web 2.0 – un internet d'interaction sociales, centralisé

ALYRA

Histoire de monnaies virtuelles

- Alan Turing
- David Chaum 1982 - Billets électroniques
- Haber et Stornetta 1991 - Merkle tree
- Cypherpunks en 1993:
- cypherpunk manifesto
- Assange, Zimmerman, Hughes
- Adam Back 1997 - Hashcash/PoW
- Satoshi Nakamoto en 2009 créé bitcoin (WP sorti en 2008)

ALYRA

De quoi la blockchain est elle la solution?

- Principe de bien immatériel sujet à rareté
  Exemple : DNS, Registre IP...

- Internet a échoué à décentraliser
  Exemple : SMTP vs GMAIL, FTP vs AMAZON, etc...

- La guerre de l'anonymat et pseudonymie
  Loi en France contre le chiffrement jusqu'en 96

- L'indépendance face aux autoritées
  Exemple : John Perry Barlow - Déclaration d'indépendance du cyberespace... 1996

ALYRA

Première approche

Mais du coup, c'est quoi?

- « Blocks » de data
- Immuables et datés
- Gérée par un groupe d'ordinateurs: Peer to Peer
- Chaque bloc est sécurisé et lié aux autres
- Utilisation d'outils de cryptographie

Détails techniques plus tard

ALYRA

Une définition - la blockchain

“ La blockchain est une technologie de stockage et de transmission d’informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle.”

Définition de Blockchain France

ALYRA

Les ingrédients magiques

Code Libre

Incitation au consensus

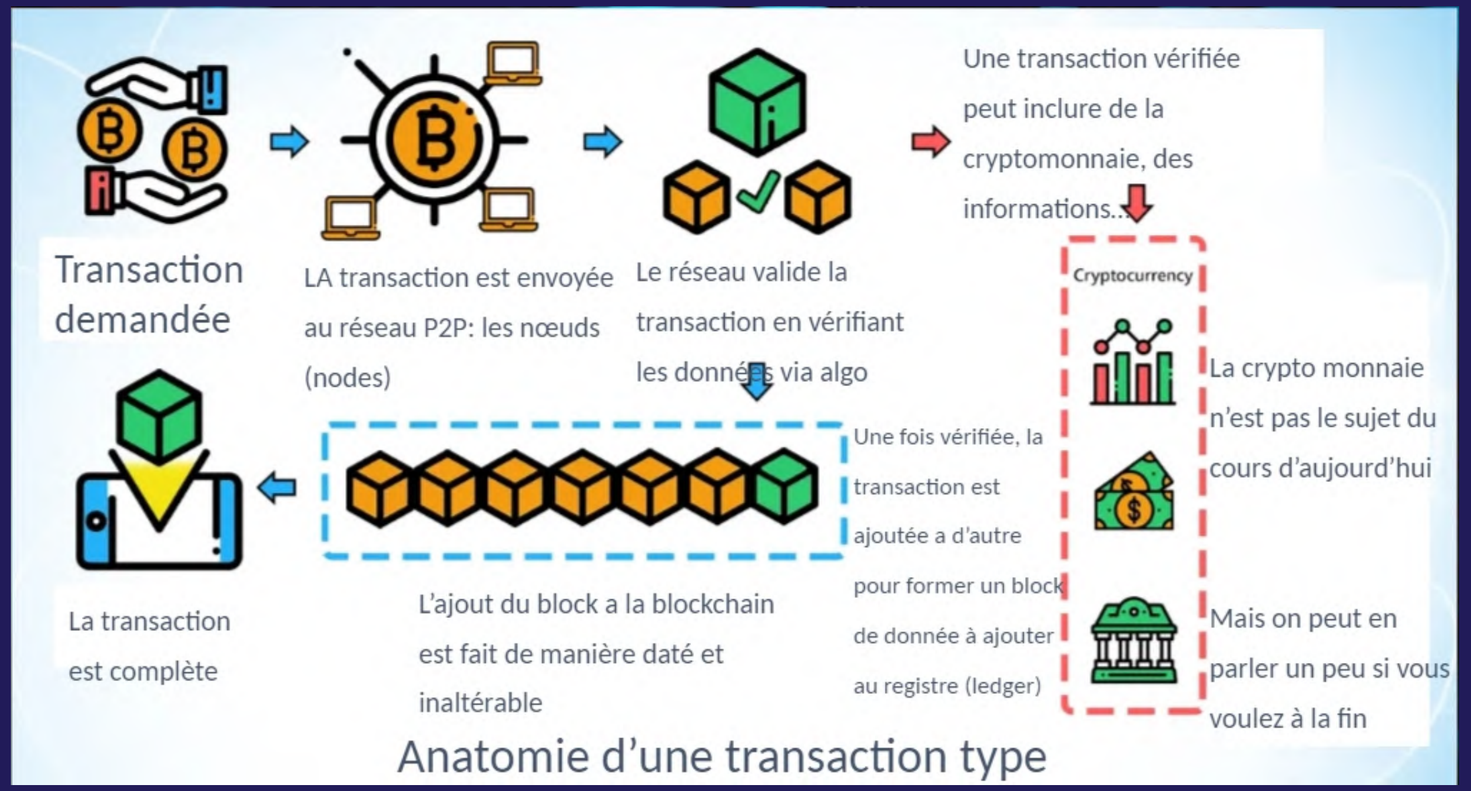
Développement de communauté

P2P

Chiffrement asymétrique

Empreinte numérique

ALYRA



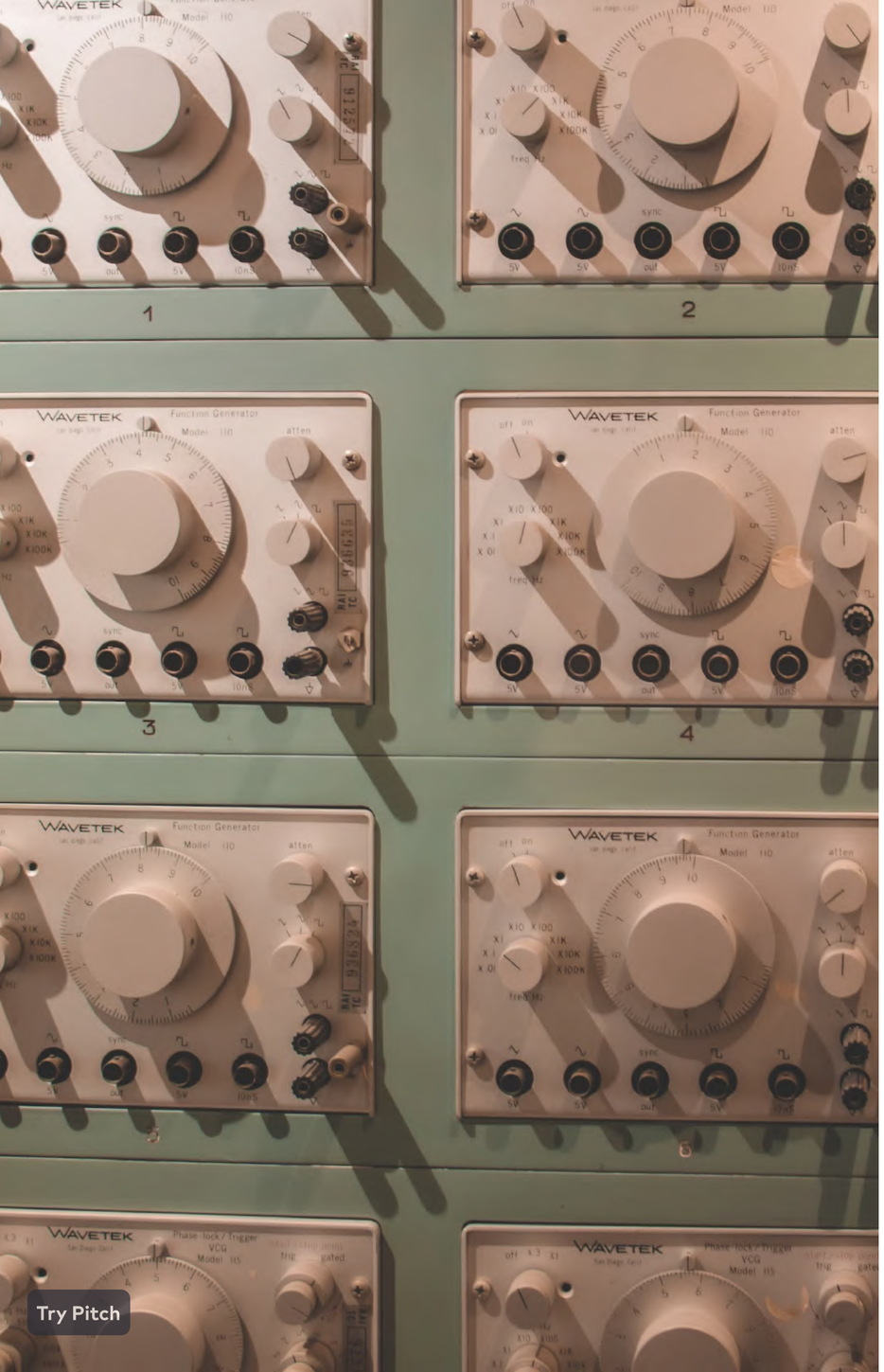
Prenons du recul

ALYRA

Principales caractéristiques

Technologie de partage des données	De nombreux utilisateurs	Modèles de confiance intégrés	Forme un journal de transaction
Décentralisée Propriété collective	Validateurs, spéculateurs, contributeurs, utilisateurs… Synchronisation en temps réel	Authentification par consensus Une histoire unique, vérifiable	Immuable Chaine chronologique de l’activité

ALYRA



Les caracteristiques

Décentralisation

Les systèmes actuels nécessitent des intermédiaires tiers mais le système de machine à machine utilisant la blockchain pourrait permettre une connexion directe entre les personnes.
Pas de centralisation des données: la blockchain possède les données, pas une entité unique (entreprise ou état)

Propriété collective

Tout le monde peut posséder un exemplaire complet de la blockchain.
L'entièreté de Bitcoin: environ 477go (lien)
Eth environ 950go (lien)
Dogecoin environ 52go (lien)

https://blockchair.com/fr

ALYRA

Les caracteristiques

Plusieurs utilisateurs

Les utilisateurs de la blockchain peuvent être de deux sortes différentes: ou bien des adresses qui vont interagir sur la blockchain en faisant des requêtes a la blockchain
Ou bien des nœuds, possédant partie ou entièreté de la blockchain, et validant les interactions

Synchronisation en temps réel

Chaque nœud validant une transaction envoie une copie de la transaction a l'ensemble du réseau, qui vient l'inclure en même temps à la blockchain.

ALYRA

Les caracteristiques

Confiance

Accès publique: à tout moment, tout état peut être vérifié: par exemple le solde sur un compte.

Culture de l'open source: les codes sont à disposition (très souvent) pour vérification.

Argent privé: on ne peut utiliser un compte que si l'on a les clefs privées de ce compte, personne d'autre que nous même ne peut interagir dessus.

Consensus

Le mécanisme de consensus d'une blockchain permet au réseau de se mettre d'accord sur une version unique de l'histoire. Plusieurs modèles de consensus existent, tous avec leurs avantages et inconvénients - **Proof of work** (PoW) / **Proof of Stake** (PoS)

ALYRA

Les caracteristiques

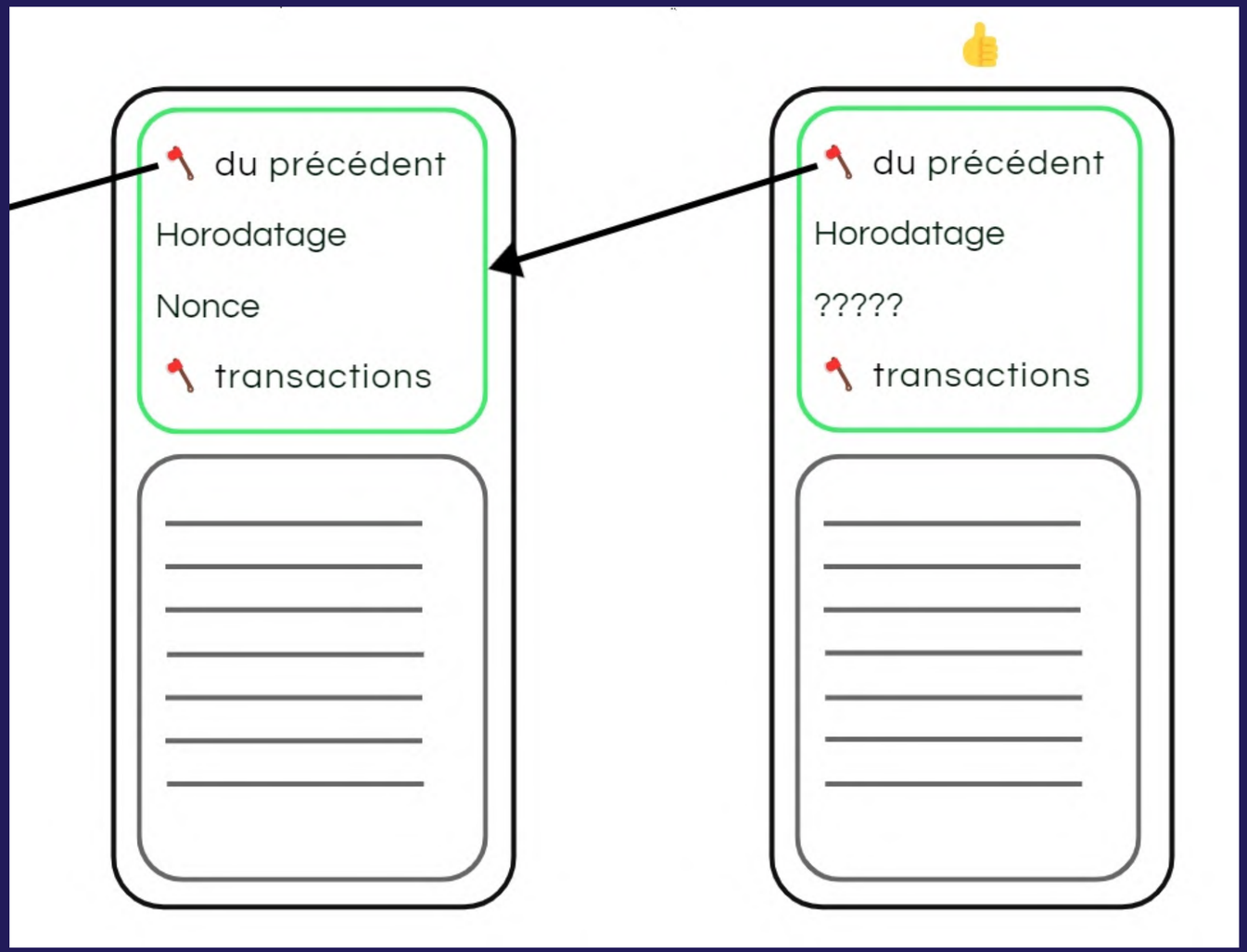
Immuable

Les détails techniques de la blockchains rendent immuable, donc non altérable, les données.

Horodaté

Chaque transaction est inscrite à un moment et ce moment est inscrit dans les données.

ALYRA



Voyons un bloc en PoW

ALYRA

Une définition - la cryptographie

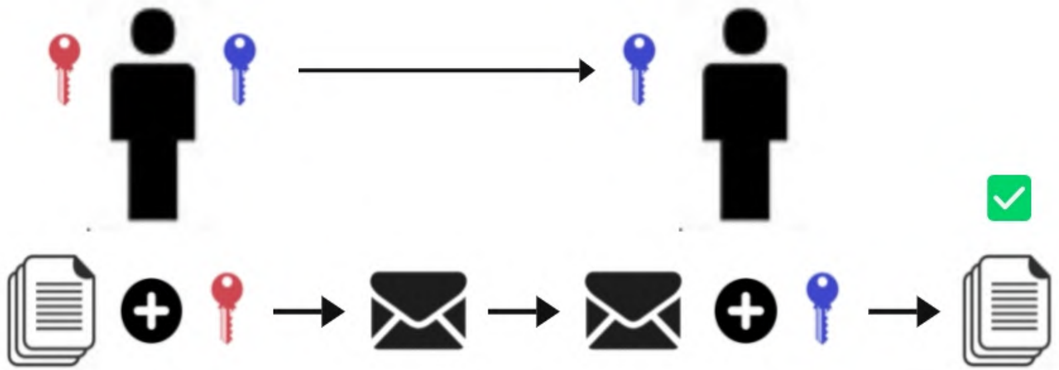
« Historiquement, la cryptologie correspond à la science du secret, c'est-à-dire au chiffrement. Aujourd'hui, elle s’est élargie au fait de prouver qui est l'auteur d'un message et s'il a été modifié ou non, grâce aux signatures numériques et aux fonctions de hachage. »

Définition de la CNIL

ALYRA

Chiffrement asymétrique

- La clef privée créée aléatoirement →
- La clef publique créée à partir de la clef privée →
- Ce qui se chiffre avec se déchiffre avec
- Ce qui se chiffre avec se déchiffre avec



Pourquoi on en parle?

ALYRA

Le chiffrement Asymétrique

- La cryptographie à clé publique, est également connue sous le nom de *cryptographie asymétrique*. Le terme asymétrique provient de la propriété des clés qui viennent toujours par paires et utilisées de façon complémentaire.
- Si vous avez chiffré quelque chose avec l'une des clés, vous avez besoin de l'autre pour le déchiffrer et vice versa. Ces clés sont la *clé publique* et la *clé privée* (ou *clé secrète*).
- Vos clés se traduisent par votre identité sur la blockchain. Vous recevez des fonds avec votre clé publique et envoyez des fonds avec votre clé privée. La cryptographie à clé publique est aussi l'origine du nom des cryptomonnaies.
- **La clef publique sert à envoyer une transaction, la clef privée sert à déchiffrer la transaction.**

ALYRA

Quelques détails

- Article Cryptoast sur la génération de clé
- La clé privée est un nombre hexadécimal très long généré aléatoirement.
- La clé publique est un nombre hexadécimal qui est calculé à partir de la clé privée.
- Il est possible de calculer la clé publique à partir de la clé privée, mais l'inverse n'est pas vrai. Il est pratiquement impossible de retrouver la clé privée à partir de la clé publique => un hash
- La clé privée doit rester privée. Vous ne devez jamais la communiquer à qui que ce soit. Par contre, la clé publique doit être publique et accessible à tous.
- Article Cryptoast sur les clef dans bitcoin

ALYRA

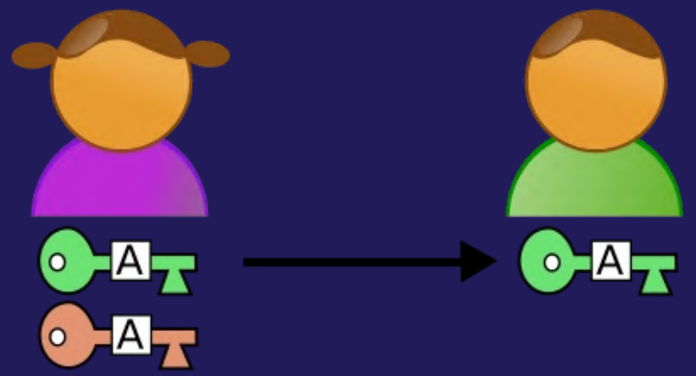
Signature crypto

- La clé publique va permettre de vérifier nos signatures. En effet, notre clé privée va servir à générer des signatures pour nos données.
- Si l'on donne à quelqu'un notre message et notre signature, cette personne est capable de vérifier l'authenticité du message. **Comment**?

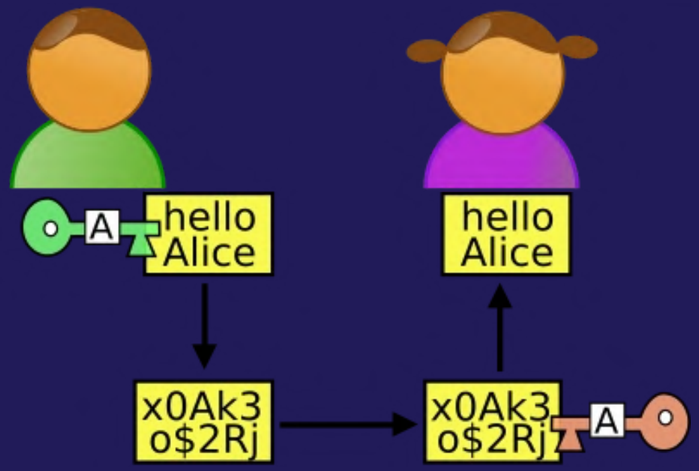
Simplement en allant chercher notre clé publique et appliquer l'algorithme de vérification cryptographique sur le message et sa signature. (ECDSA)

ATTENTION : La personne n'a pas accès à notre clé privée, mais en utilisant uniquement la clé publique, l'algorithme cryptographique va lui dire
"Oui, ce message a bien été écrit par la personne possédant la clé privée"

ALYRA



1re étape : Alice génère deux clefs: Sa clef publique (verte) qu'elle envoie à Bob et sa clef privée (rouge) qu'elle conserve précieusement sans la divulguer à quiconque.

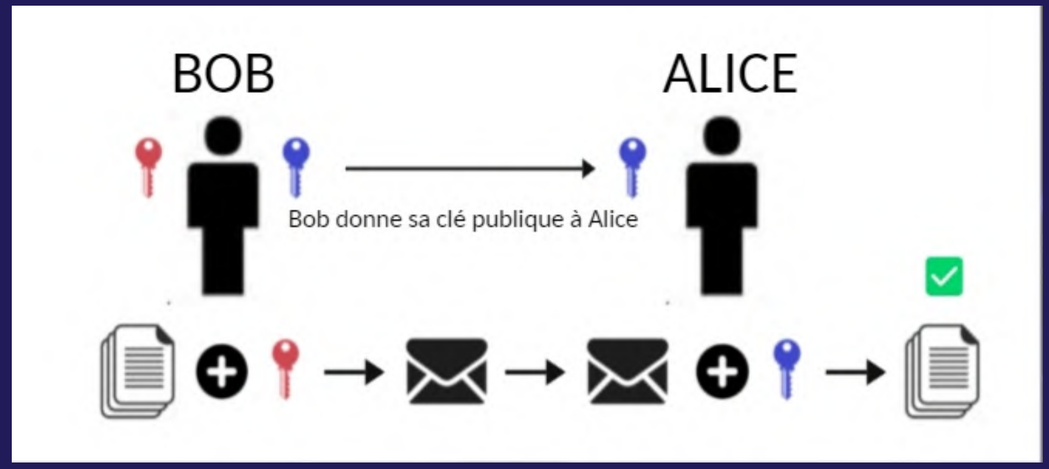


2e et 3e étapes : Bob chiffre le message avec la clef publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clef privée. Seul Alice peut déchiffrer le message, car elle est la seule à possèder la clé privée.

ALYRA

Mais, on peut aussi fonctionner dans le sens inverse.

- On peut utiliser la clé privée pour chiffrer, la clé publique servira à déchiffrer.
- Le message ainsi chiffré sera lisible par toutes les personnes qui detiennent la clé publique. Par conséquent, ce n'est pas très confidentiel. En revanche, on sait qu'une seule personne a chiffré ce message : Bob.
- Donc, si l'on peut déchiffrer un message avec la clé publique de Bob, c'est forcément la personne qui a chiffré le message.



Le hashage

Qu'est ce que c'est?

Il représente une empreinte digitale servant à identifier rapidement la donnée initiale.
Souvent un nombre hexadécimal, le hash est créé par un algorithme. Il en existe plusieurs dans la blockchain. Keccak que nous verrons pas mal en Solidity... le plus commun est le SHA256.
=> il transforme une chaîne de caractères en nombre de 64 caractères (256 bits)

ALYRA

Hash, propriétés

Unidirectionnel

Facile de calculer une sortie à partir d'une entrée donnée, mais impossible de calculer l'entrée à partir d'une sortie donnée

Pseudo aléatoire

Un changement dans l'entrée produira un changement imprévisible dans la sortie. Si la valeur de hachage de l'entrée "2" était "4", le hachage de l'entrée "3" ne doit pas être 6.

Résistant aux collisions

Il devrait être difficile (lire impossible) de trouver deux entrées pour une fonction de hachage donnant la même sortie.

Déterministe

La même entrée doit toujours produire la même sortie

Des détails en plus quand on parlera minage

ALYRA

Un exemple de hashage:

🪓 du texte : Ceci est une donnée

5b518804ca6d9c7e40c20e2bb5d0bdee0f2ca73edd95c0675220ef3ddc6c432b

🪓 du texte : Ceci est une Donnée

6e4cb6c34d8f283a5b4fefc103dd68639954144d8f0a51ce4d7c4b8d8cb9917b

Exemple ici : https://emn178.github.io/online-tools/sha256.html

Hashage et chiffrement a clef publique

- Un grand livre distribué, sécurisé, de pair à pair
- Partage sur le réseau
- Contient des transactions viables (prouvées, authentifiées)
- La preuve cryptographique est utilisée pour valider les transactions
- Les transactions sont regroupées en blocs
- Les hashs relient les blocs, créant ainsi une chaîne
- La chaîne ne peut pas être modifiée ou les hashs ne seront plus valables

ALYRA

Merkle tree

Modèle de structure de donnée

arbre de hachage, concept mathématique inventé en 1979 par Ralph Merkle
Utilisé pour avoir de nombreuses informations dans peu de données

Un résumé de données

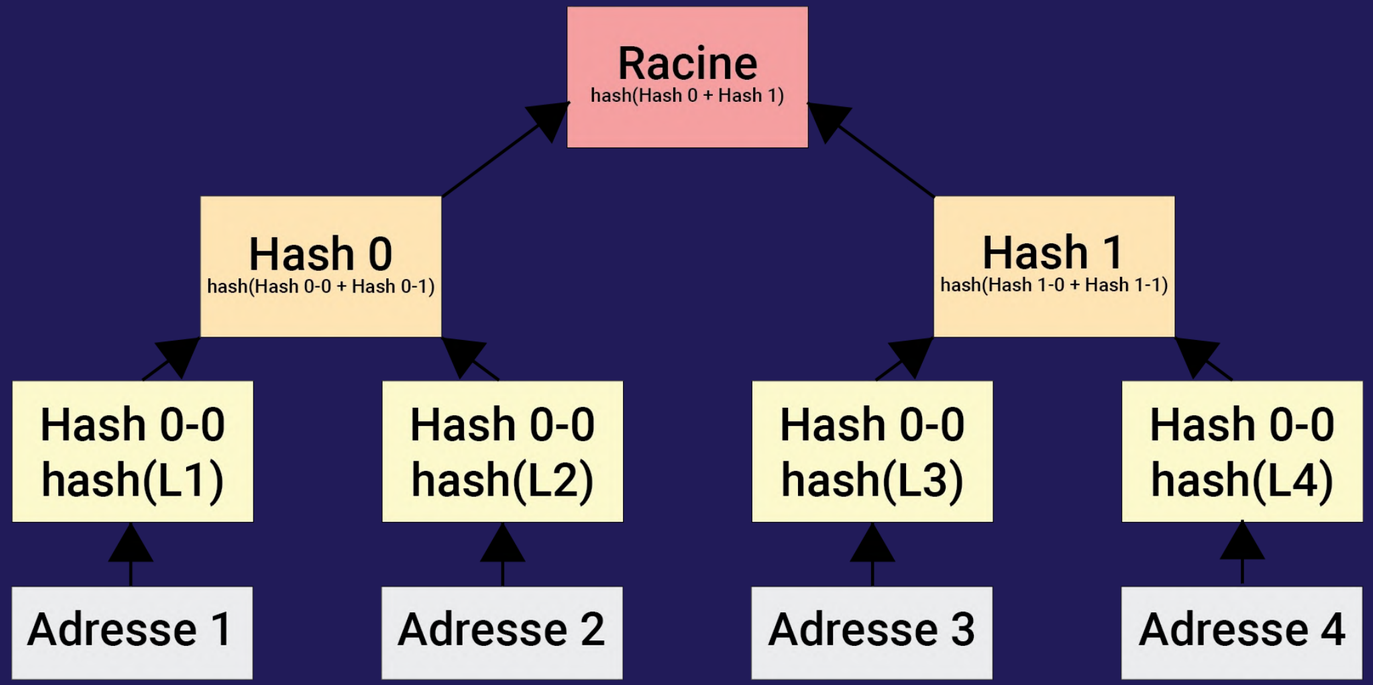
C'est utilisé à la base de la plupart des blockchain: on retrouve une racine de Merkle dans l'en tête d'un bloc, elle représente l'entièreté des transactions.

Comment ça fonctionne?

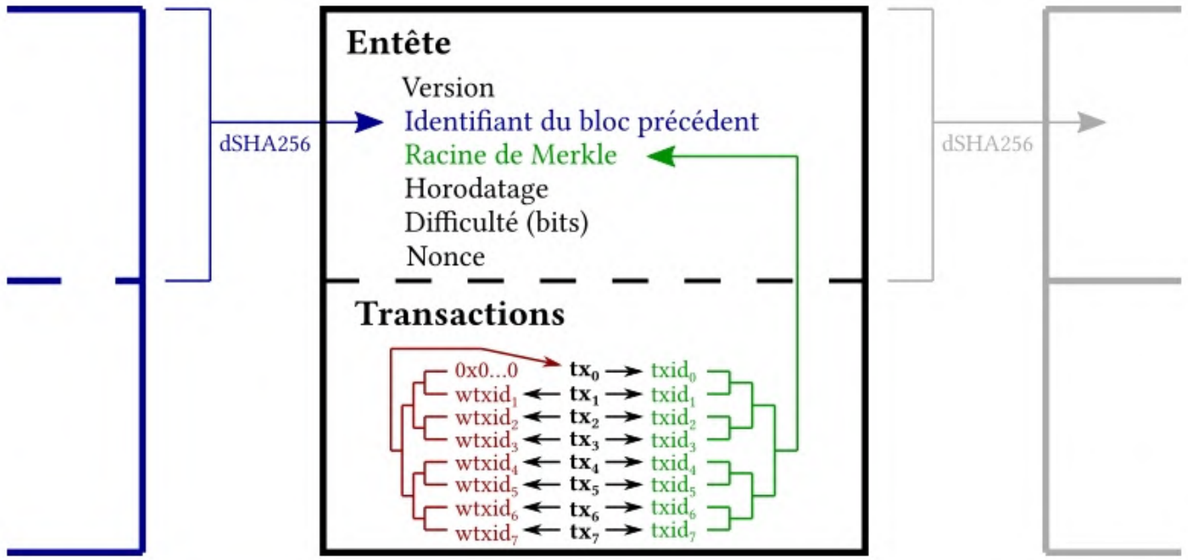
Supposons qu'on ait 4 adresses. Chacune est hashée en une feuille de l'arbre, « leaves».

De manière récursive on va hasher les adresses: "Adresse 1" et "Adresse 2" sont hashés en "Hash 0". "Adresse 3" et "Adresse 4" sont hashés en "Hash 1".

"Hash 0" et "Hash 1" sont hashés en "Racine" : le MerkleRoot.



ALYRA



Merkle tree – Pourquoi en parler?

Car cette méthode a été une évolution significative permettant l'existence même d'une blockchain. Cette méthode de hashage permet de revenir a une transactions précise, mais en même temps de vérifier un ensemble de transaction complet, sans avoir besoin de vérifier chacune des transactions.
L'efficacité de cette solution est à la base de la synchronisation entre les nœuds et donc du consensus accepté dans la blockchain.

Nous pouvons aller voir le site suivant pour plus de visualisation

Ici un block en JSON

Et là une explication technique

ALYRA

Le consensus

- L'élément clé d'une blockchain - l'accord sur la validité des transactions et des blocs - **nécessite le consensus de plusieurs parties**
- Dans **une blockchain privée**, c'est relativement facile, car l'accès est limité et toutes les parties ont intérêt à maintenir l'intégrité de la blockchain
- Dans **une blockchain publique**, c'est plus complexe et doit être intégré dans la solution

L'objectif est de garantir l'existence d'un accord sur la validité de toutes les transactions et de tous les blocs dans la blockchain

11 mai 2023

Pour saisir les différentes composantes des consensus qui existent, ils faut voir plus en amont les différences entre les blockchains.
POW, POS, POA, DPOS, POH... nous reviendrons dessus demain, on abordera ces consensus et les deux grandes blockchain historiques, Bitcoin et Ethereum.

Liens utiles

- Comprendre comment fonctionne une blockchain: https://andersbrownworth.com/blockchain/
- Comprendre comment fonctionne les signatures : https://andersbrownworth.com/blockchain/public-private-keys/keys

Merci de votre attention!

ALYRA