Développeur blockchain

Introduction

Bitcoin et Ethereum

ALYRA

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

Promo Buterin

Topo du live

- Minage
- BTC vs Eth
- Spécificités d'ethereum
- Wallets

ALYRA

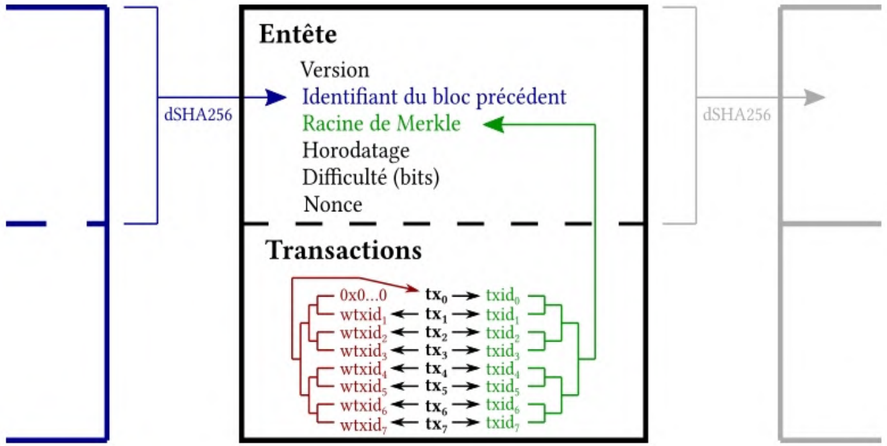
Leurs consensus historique

Proof of work

- Le consensus historique des blockchains
- Considéré très sécurisé
- Met en place des outils mathématiques pour assurer la validation des blocks.
- Les validateurs doivent « travailler », lancer des algorithmes
- Incentive financière: acquérir en contrepartie une reward
- L'investissement en temps et effort octroie une légitimité
- Légitimité toujours vérifiable par tous les utilisateurs

ALYRA

Miner un nouveau bloc



- On récupère l'ensemble des transactions disponibles sur le mempool,
- On récupère le hash de l'en tête précédent,
- On inclut les éléments fixes,
- Il nous reste donc l'horodatage du bloc et le nonce à trouver,
- Le nonce est un nombre hexadécimal aléatoire que le mineur va faire varier,
- Le but est que le hash de l'en tête du bloc trouvé corresponde à la difficulté en cours de la blockchain (notée en nombre de 0)
- Du matériel spécialisé va donc calculer des hashs d'en-tête en boucle en fonction du nonce

ALYRA

Le minage

Mining, minage en francais.

- Coûteux en énergie, et en matériel
- Compensé par la récompense
- 6,25 btc actuellement, nombre lié au halving (prochain halving en mars/avril 2024)
- Le btc, bitcoin, ou l'eth, l'ether, sont les monnaies de fonctionnement de leurs blockchains, Bitcoin et Ethereum
- On différencie les coins de blockchains, des tokens de protocoles.

A gauche: un rig de minage en CG pour du bitcoin, aujourd'hui on utilise des asics

ALYRA

Le proof of stake

- Le nouveau consensus très utilisé
- Beaucoup moins gourmand en énergie (-99.8%)
- Permet une décentralisation satisfaisante
- N'est pas une solution de scalabilité
- Utilise la beacon Chain pour gérer le processus
- Reward des nodes qui minent
- "Plus de décentralisation et de sécurité grâce à la social recovery"

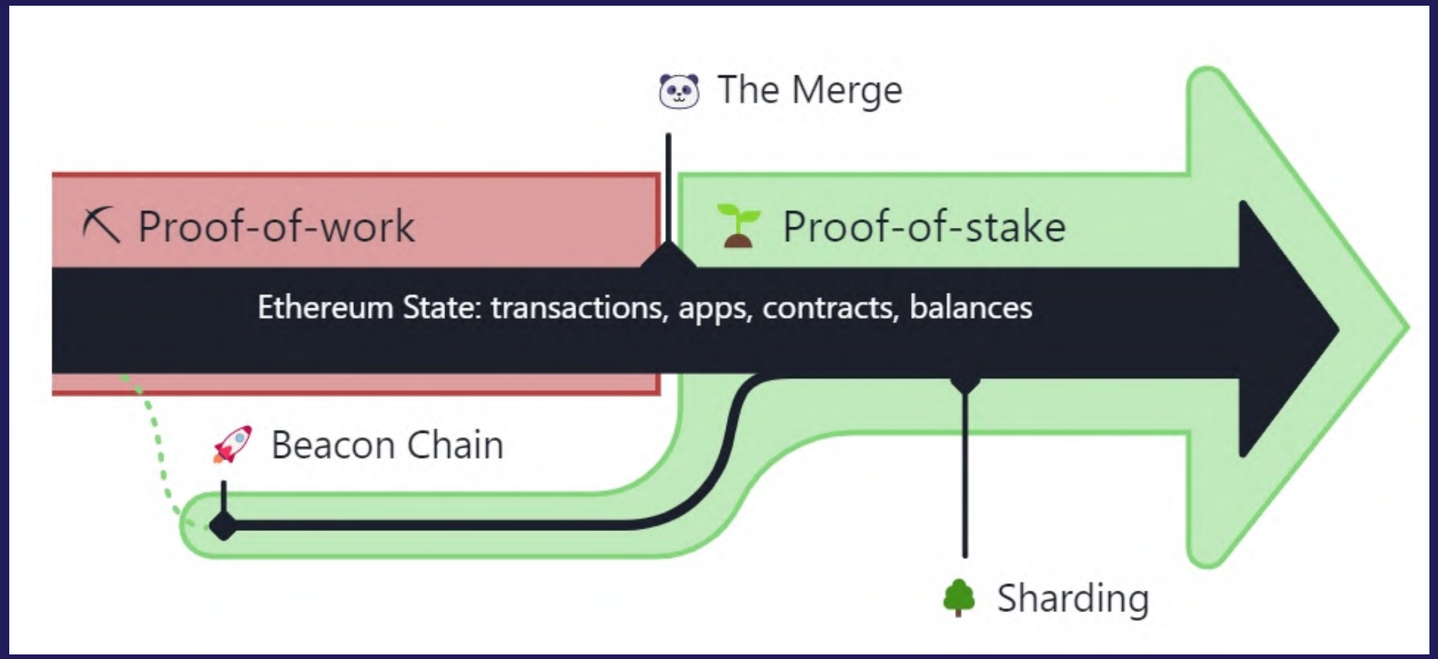
ALYRA

Processus du PoS

Proof of stake - Process

- Déposer 32 ETH dans le "deposit contract"
- Lancer un client exécution, un client consensus et le validateur
- Quand on a déposé les 32eth, on rejoint la file d'attente des validateurs
- Une fois qu'on devient validateur, on reçoit tous les blocks construits

- un tempo fixe: un block toutes les 12 secondes, un epochs tous les 32 blocs
- un validateur est rendu responsable de créer le bloc et l'envoyer au réseau
- puis un comité de validateurs atteste du bloc
- le comité réexécute les transactions de chaque blocs, on vérifie les signatures, et si tout va bien, on envoie une "attestation" de la validité du bloc sur le réseau
- les premiers blocks d'une epoch sont un checkpoint
- https://ethereum.org/en/developers/docs/consensus-mechanisms/pos



The merge

ALYRA

Deux blockchains aux vocations différentes

Bitcoin

Personnalités importantes:
Satoshi Nakamoto
Bitcoin Foundation

Inventé sur le temps long, premiers écrits en 2007, sortie en 2009

Inventé suite à des premieres tentatives de cryptomonnaies, celle-ci met en place la proof of work qui la rends viable

Ethereum:

Personnalités importantes:
Vitalik Buterin
Nick Szabo
Joseph Lubin

Inventé en 2013, mis en ligne en 2015

Volonté d'avoir un écosystème décentralisé, pas seulement une monnaie

ALYRA

« La blockchain de Bitcoin a été conçue spécifiquement pour des applications monétaires, alors que Ethereum permet de créer tout type d'applications »

le fondateur de Ethereum,
Vitalik Buterin.

ALYRA

Des spécificités

- Ethereum est un réseau géant qui consiste en un énorme nombre d'ordinateurs connecté entre eux.
- Ce réseau est appelé Ethereum Virtual Network (EVN) et fonctionne un peu comme un super-ordinateur, où toutes les transactions sont enregistrées sur chacun des ordinateurs du réseau.
- L'ETH est la crypto-monnaie permettant de faire fonctionner le réseau en étant utilisée comme "carburant".
- Une des fonctionnalités innovantes de la blockchain Ethereum était l'introduction des smart contracts.

ALYRA

Des différences

- Ethereum a des blocs plus petits que Bitcoin
- Dans Bitcoin, la taille maximale du bloc est spécifiée en octets alors que la taille du bloc sur Ethereum est basée sur la complexité des smart contracts en cours d'exécution - c'est ce qu'on appelle une limite de gas par bloc, et le maximum peut varier légèrement d'un bloc à l'autre.
- Actuellement, la taille maximale des blocs dans Ethereum est d'environ 15 000 000 gas (extensible à 30 000 000). Les transactions de base ou les paiements d'ETH d'un compte à l'autre ont une complexité de 21000 gas, ce qui fait que vous pouvez faire entrer environ 700 transactions dans un bloc (15 000 000 / 21 000).
- Dans Bitcoin, vous obtenez actuellement environ 1 500 à 2 000 transactions par bloc.
- En ce qui concerne les données, la plupart des blocs Ethereum ont actuellement une taille inférieure à 2 Ko.

ALYRA

Try Pitch

Bitcoin vs Ethereum

- Temps de bloc :

BTC: ~10 minutes / Eth 12 sec

- Nombre de coin gagnés pour chaque bloc miné :

BTC : 6,25 min (+ les frais de la tx) / Eth : 2 avant, 0.1 aujourd'hui

- Nombre de blocs minés:

BTC: plus de 652520 / Eth: 1 500 000

- Nombre de transactions par jour:

BTC: plus de 150 000 / Eth : >1 500 000

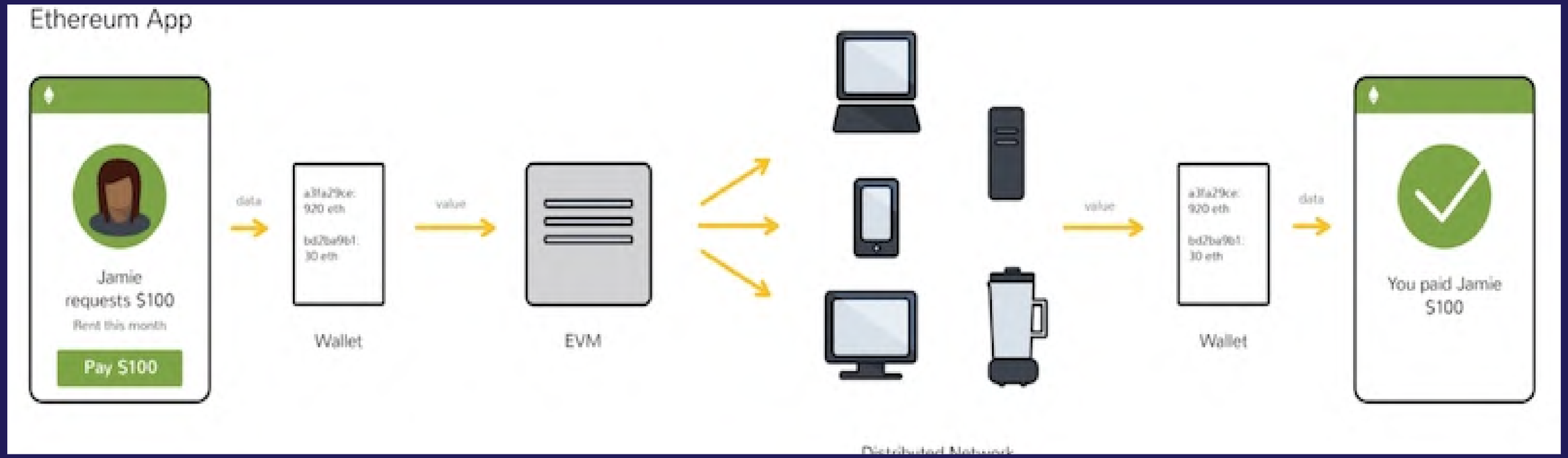
- Nombre de noeuds dans le réseau:

BTC: 10000 / Eth : à peu près 7 000

- Valeur des coins

BTC : 21000€ / Eth: 1500€ (01/2023)

ALYRA



Trajet d'une transaction Ethereum

ALYRA

Une spécificité d'ethereum : Les comptes

Un compte = une adresse (address)

Deux types de compte :

- **Compte personnel (clé privée)**
- **Compte de contrat (code):**
  - Balance (en Wei)
  - Contrat (hash du code)
  - Stockage (informations contrat):

Les smart contracts (ou contrats intelligents) sont des petits programmes informatiques qui sont stockés sur la blockchain Ethereum.

ALYRA

Un concept d'ethereum: Le gas

Lorsque vous déployez un smart contract, que vous effectuez une transaction que vous interagissez sur une dapp, vous demandez à tous les mineurs de l'ensemble du réseau d'effectuer individuellement les calculs qui s'y rapportent.

Cela leur coûte du temps et de l'énergie, et le gas est le mécanisme par lequel vous les payez pour ce service.
--> Le gas est une unité qui sert à mesurer le temps de travail informatique nécessaire pour faire fonctionner un smart contract sur le réseau Ethereum.

Pour simplifier:
C'est un système à peu près équivalent à celui des kilowatts pour mesurer la consommation électrique. On finira au final par payer en €, mais on mesure l'électricité consommée en KWH (kilowatts par heure).

ALYRA

Paiement (ETH) =
Gas amount (Gas) x
Gas price (ETH/Gas)

Plus la transaction est complexe (nombre et type d'étapes de calcul, mémoire utilisée pour le stockage, etc.), plus le réseau exige de gas pour l'exécuter et l'achever.
C'est le gas amount

Le prix du gas est spécifié par la personne qui souhaite que son smart contract soit déployé, au moment où elle le demande.
C'est le gas price

Chaque mineur examinera la générosité du prix du gas et déterminera s'il souhaite que le smart contract soit exécuté dans le cadre du bloc.
Si vous voulez que les mineurs exécutent votre contrat, vous proposez un prix du gaz élevé. Il s'agit donc d'une vente aux enchères concurrentielle qui dépend du montant que quelqu'un est prêt à payer pour faire fonctionner le contrat.
(Détails sous PoS différents)

ALYRA

Pourquoi le gas?

Faire en sorte que les smart contracts coûtent du gas/ETH/argent empêche les gens de les activer à leur gré, ce qui résout les problèmes liés au spam de transaction qui se produirait si l'exécution des smart contracts était gratuite.

ALYRA

Un wallet

Qu'est ce que c'est?

Un wallet, portefeuille en français, est un petit bout de cuir permettant de garder ses cartes de crédits et son liquide, voir sa monnaie, pour que ça tienne dans une poche sans en foutre partout

ALYRA

Un wallet

Qu'est ce que c'est?

Dans le monde de la blockchain, un wallet est un programme, permettant de stocker ses cryptomonnaies.
Plus précisément, en théorie, il garde la paire de clef privée et publique vous permettant d'accéder aux cryptomonnaies que vous possédez

ALYRA

Wallet - distinctions

Custodial (hebergé)

Non Custodial (non hebergé)

Hot Wallet

Cold Wallet

ALYRA

Custodial wallet

Aussi appelés web wallets hébergés, cloud wallets…

Le principe est que vos crypto soient stockées en ligne via un tiers de confiance, souvent une plateforme d'échange sur laquelle vous pouvez utiliser, acheter, vendre vos crypto

Exemples les plus connus:

Coinbase, binance, kraken, bittrex, crypto.com, ftx, kucoin, gate.io, okx okex, blockchain, Coinhouse…

Pros:

Fluidité des capitaux (peu de frais)

Récupération des données

Systèmes simples

Beaucoup de possibilités

Convertir fiat en crypto

Cons:

Il faut faire confiance à un site

On ne possède pas nos crypto

(faillite, malveillance…)

Cible privilégiée

Quid des futures régulations?

KYC

Non custodial wallet

Il en existe plusieurs sortes:

- Extensions navigateur,
- App mobile,
- Hardware Wallet,
- DU PAPIER

ALYRA

Try Pitch

Non custodial wallet

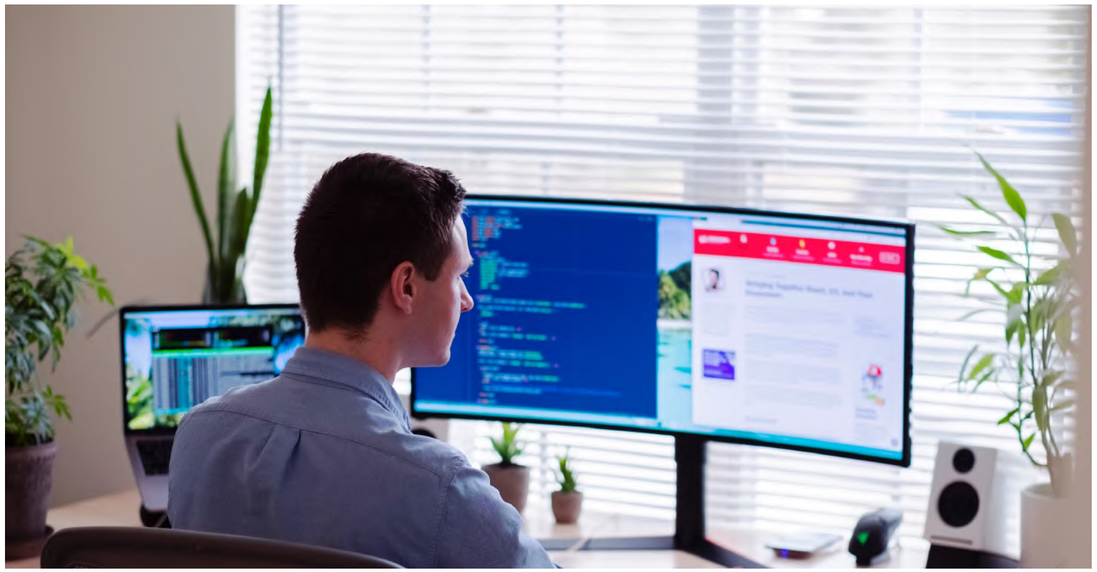
Les extensions navigateurs sont les plus utilisés:
Stockent en local sur votre ordi la paire de clef privée et publique de votre compte
S'executent sur un navigateur web, pour pouvoir intéragir directement avec la blockchain sur certains sites: les Dapp, Decentralised aplication

Mise en place d'une phrase mnémonique (12 a 24 mots) pour exporter son compte
À ne pas garder sur son ordi à priori

Exemples: métamask, myetherwallet, bravewallet, temple pour tezos, polkadot.JS, phantom pour solana

ALYRA

Les autres



app desktop

Permettent de voir et d'echanger ses crypto.

Très utile pout btc notamment.

Ex: Multichain: coinomi.

Pour eth metamask mobile

hardware wallet

ex: Ledger, trezor...

Tout est offline, et une fois branchée à un ordinateur, elles permettent l'utilisation des clefs sur les interfaces du constructeur.

Considérés comme très sécurisés, souvent

12 mai 2023

Bon week end!

Essayez d'aller au bout des chapitres d'introduction

Merci de votre attention!

ALYRA