

# Introduction aux Ethereum Virtual Machines

# Historique d'ethereum

- En 2013 Vitalik Buterin conçoit un concept de blockchain programmable.
- Il lance un livre blanc intitulé Ethereum : The ultimate Smart Contract and Decentralized Application Platform.
- Il lance la première ICO (Initial Coin Offering de l'histoire) à tous ceux qui souhaitent participer au projet. Il lève ainsi près de 31529 bitcoin pour développer son projet (environ 18 millions de \$ de l'époque)
-

# Comment fonctionne Ethereum

- Le réseau Ethereum est composé d'un grand nombre d'ordinateurs interconnectés partout dans le monde. Chacun de ces ordinateurs est nommé noeud.
- Chaque Noeud a pour but de conserver une copie du registre de la blockchain, et d'en maintenir sa sécurité.
- Ethereum est considéré comme une machine d'état qui ordonne toutes les transitions d'états de chaque compte et de chaque contrat.

# Les unités de valeurs pour Ethereum

- La BC Ethereum utilise comme unité de base : l'ether qui représente  $1^{18}$  Wei (1 ether = 1000000000000000000 wei)
- Le Gwei represente : 0,000000001 ether ou : 1000000000 wei
- Demo sur le site Ethereum unit converter

# Structure d'une transaction Ethereum

- Une transaction sur la BC Ethereum se compose a minima de :
  - L'adresse du sender
  - L'adresse du destinataire
  - D'un champ value (en wei)
  - Le champ gasLimit : qui autorise le nombre maximal d'étapes de calcul pour la transaction sinon elle sera considérée comme devant être annulée.
  - Le champ GasPrice : le prix maximal en du cout en gas que l'utilisateur autorise. (Voir le site <https://ethgasstation.info/>)
  - Visualisation des transactions en temps réel : <https://txstreet.com/v/btc-eth>

# Structure d'une transaction sur ethereum

- Comme toutes les transactions sont visibles pour les utilisateurs, elles sont visible via un site nommé etherscan dans lesquels nous pouvons retrouver :
  - Envoi d'ether
  - Interactions avec un contrat :
    - Envoi de tokens crée dans la BC
    - Échange de token via un échangeur décentralisé
    - Consulter le contenu du contrat et interagir avec

# Notions sur les frais de gas 1/3

- Le gas est à mettre en relation avec l'essence pour la blockchain:
  - Nous payons pour écrire dans la blockchain
  - La consultation de données est gratuite.
- Le fait de devoir payer pour utiliser la BC permet d'éviter une congestion, par rapport à un excès de travaux.

# Notions sur les frais de gas 2/3

- Chaque unité de gas met en concurrence tous les utilisateurs pour planifier les transactions. Plus les frais de gas sont élevés moins les utilisateurs voudront l'utiliser.
- Donc plus le réseau est saturé plus les frais de gas en gwei seront élevés et inversement.

# Notions sur les frais de gas 3/3

- Le gas est donc le cout par unité de calcul, multiplié par un prix en gwei (basé sur l'offre et la demande) permettant d'executer une transaction.
- Par exemple un envoi d'ether sera de 21000 (facilement détectable)
- Si un smart contract est complexe la quantité de gas sera bien plus élevée du fait des multiples opérations à réaliser.
- Le gas limite dans une transaction sera donc le nombre d'unité de calcul effectuée dans notre transaction. Et le gas price sera le prix en gwei par unité de calcul

# Rappel sur les unités :

Unit	Wei Value	Wei
wei	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
microether (szabo)	1e12 wei	1,000,000,000,000
milliether (finney)	1e15 wei	1,000,000,000,000,000
ether	1e18 wei	1,000,000,000,000,000,000

# Comprendre les EIP et ERC

- EIP : est une proposition d'amélioration du réseau Ethereum. (Ethereum Improvement Proposal)
  - Elles contiennent des améliorations ou des modifications de normes ou de mise à niveau.
- ERC : dès lors qu'une EIP est validée elle est définie en tant que ERC (Ethereum Request for Comment). Elle définit les usages d'une implementation. Par exemple les tokens sont aussi nommés ERC20. Les NFT ERC721.

# Utilisation d'un wallet

- Demo Echange ether
- Demo transfert de tokens

# Les tokens de la blockchain

- Il existe deux familles de tokens dans les blockchains programmables :
  - Les tokens dit fongible (divisibles en sous unités)
  - Les tokens non fongibles alias NFT qui sont unique et indivisibles.

# Les tokens fongibles ou ERC20

- Les tokens types ERC20, sont des tokens qui sont par natures divisibles. Ils sont souvent utilisés comme des monnaies pour les échanges. On retrouve par exemple des tokens ERC20 avec une parité à l'USD (USDT, USDC, BUSD, DAI)
- Ils possèdent un certain nombres de fonctions minimales décrite dans l'EIP.
  - Ils sont transférables
  - On peut connaître sa balance
  - Approuver le transfert de tokens par un tiers
  - Son nombre de décimales
  - Son symbol et son nom
  - <https://etherscan.io/token/0xdac17f958d2ee523a2206206994597c13d831ec7#writeContract>
- Certains tokens ont des fonctions un peu spéciales, il est important pour cela de bien comprendre leurs codes.

# Les tokens ERC721(x) ou NFT

- Ces tokens sont en quelque sorte une évolution du token ERC20.
- Il reprend certaines fonctions comme le transfert, la balance, ...
- De par sa nature non fongible il ne possède pas de décimale.
- Hormis les ventes d'images de singes, l'une des utilités peut être la gestion des places de concert, la gestion des licenses ou de titres de propriété. (Tokenisation d'un bien)
- La bonne gestion des tokens ERC721 peut à terme remplacer certaines professions complexes comme les notaires pour la gestion des titres de propriété. (Un frein législatif qui n'est pas prêt de sauter)