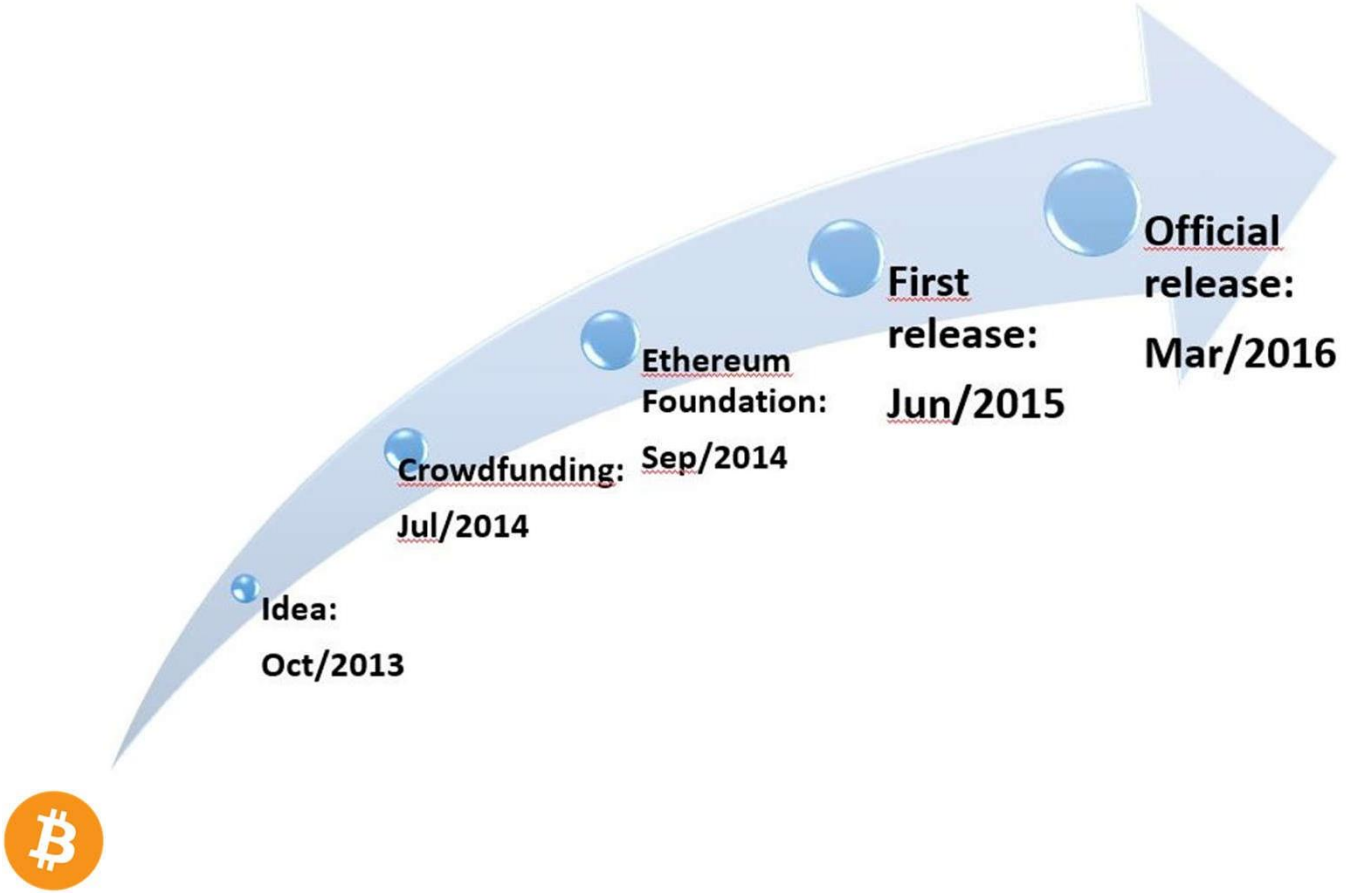
Blockchain Ethereum

History of Ethereum

- Russian-Canadian programmer :
- Vitalik Buterin
- Co-founded Ethereum when he was 19 years old

History of Ethereum - Timeline



Introduction et Histoire de Ethereum

- Vitalik Buterin. observait l'écosystème du bitcoin, il a remarqué un problème commun parmi les projets : beaucoup d'entre eux devaient créer leur propre blockchain. Cela a amené Vitalik à se demander si ce ne serait pas bien d'avoir une seule blockchain sur laquelle tout le monde pourrait construire ses applications.
- Tout comme nous avons un seul intranet sur lequel tout le monde peut construire ses sites web. Au lieu de chercher comment démarrer une blockchain, les développeurs pourraient alors se concentrer sur la construction de leurs propres applications.

Introduction et Histoire de Ethereum

- Donc, fin 2013, Vitalik a publié le livre blanc Ethereum qui s'appuie sur de nombreux concepts du Bitcoin. Le livre blanc est disponible aujourd'hui sur la page GitHub d'Ethereum.
- Dans le livre blanc, il a proposé une nouvelle blockchain à usage général, qui pourrait être utilisée comme une plateforme d'application décentralisée.

Introduction et Histoire de Ethereum

- Le livre blanc d'Ethereum décrivait sa propre monnaie native appelée Ether et un nouvel environnement d'exécution pour les contrats intelligents appelé **Ethereum Virtual Machine** ou EVM.
- Un livre jaune ultérieur a été publié mi-2014. Il définissait les spécifications techniques de l'EVM et son mode de fonctionnement.
- Le livre jaune a été utilisé pour créer plusieurs implémentations open source, dans différents langages, le plus populaire étant le langage GO, également connu sous le nom de Geth (**Go Ethereum**).

Introduction et Histoire de Ethereum

- Ethereum serait capable de faire tout ce que Bitcoin peut faire, comme envoyer des transactions entre comptes et bien plus encore.
- Le principal problème du bitcoin était l'absence d'un langage de programmation d'usage général qui permet de créer n'importe quelle sorte d'application sur sa blockchain.

Ethereum est-il similaire au Bitcoin ?

- Eh bien, en quelque sorte, mais pas vraiment. Bitcoin offre une application particulière de la technologie blockchain, un système de monnaie électronique de pair à pair qui permet les paiements en ligne en bitcoins.

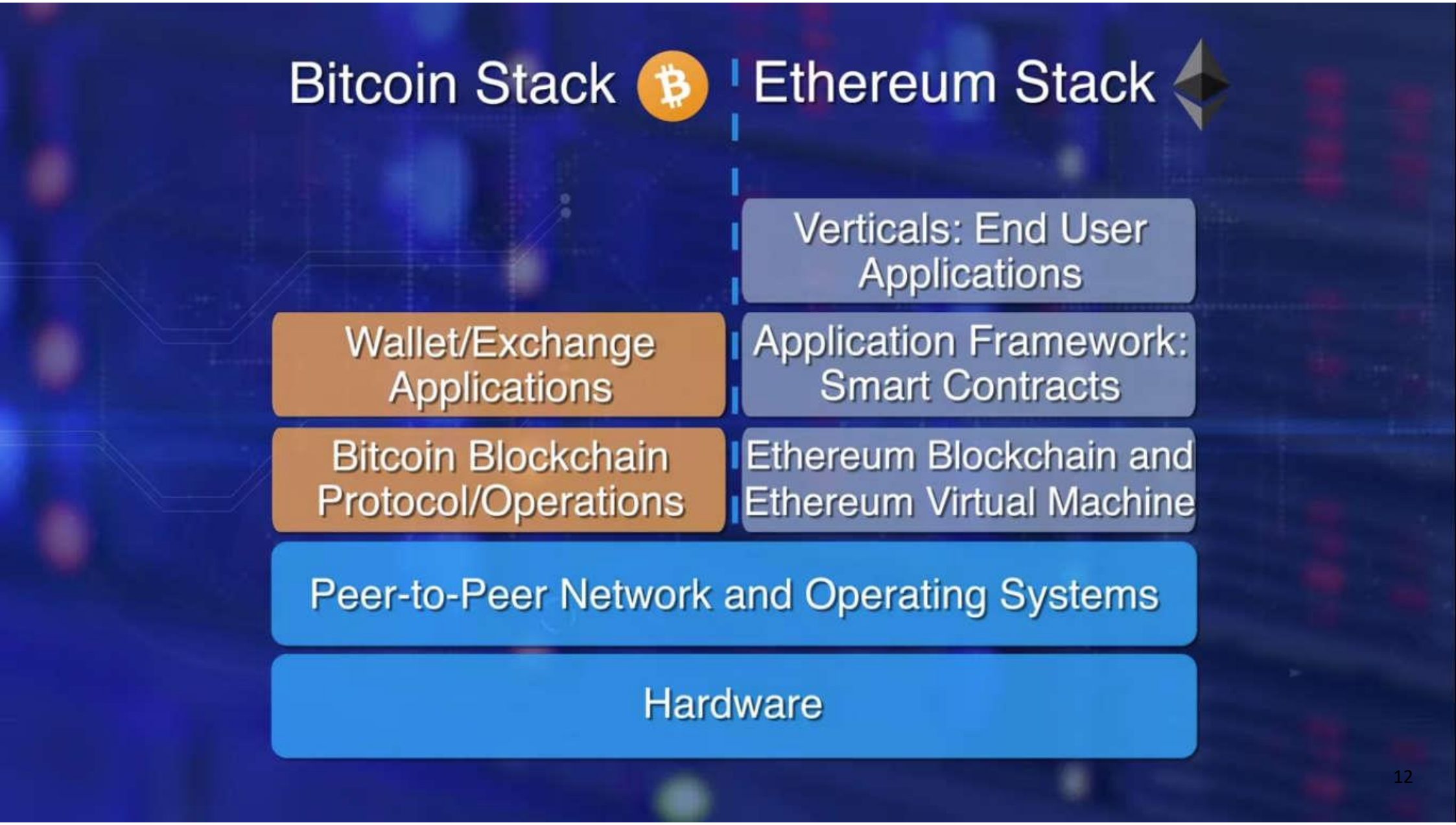
- Alors que Bitcoin est utilisé pour suivre la propriété de la monnaie numérique (bitcoins), Ethereum se concentre sur l'exécution du code de programmation de toute application décentralisée.

Résumons :

- ✓ Blockchain Bitcoin est la mère de toutes les blockchains. Elle est destiné uniquement à un transfert de valeur de pair à pair.
- ✓ Vers 2013, un cadre d'exécution de code a été introduit par les fondateurs d'Ethereum. La pièce maîtresse de cette blockchain Ethereum est un contrat intelligent.

- Lancé en 2015, Ethereum s'appuie sur l'innovation de Bitcoin, avec quelques grandes différences.
- Les deux permettent d'utiliser de l'argent numérique sans intermédiaires.
- Mais Ethereum est programmable et permet de créer et déployer des applications décentralisées sur son réseau.

Caractéristique	Ethereum	Bitcoin
Création	2015	2009
Objectif général	Une plateforme qui prend en charge les smart contract et les dApps	Monnaie numérique
Fonction de transaction	Envoyer uniquement lorsque les règles du smart contract sont respectées	Envoyer sans règles
Comment la monnaie est-elle utilisée ?	Monétiser les smart contracts et les dApps sur la blockchain Ethereum	Acheter et vendre des biens ou des services
Qu'est-ce qui influence la valeur ?	La demande de dApps, les normes réglementaires	Combien de tokens sont disponibles, normes réglementaires
Offre maximale	Aucune limite, mais vous ne pouvez en miner que 18 millions par an.	21 millions
Norme de minage	Preuve d'enjeu	Preuve de travail
Récompense de minage	Frais de transaction	Tokens


Bitcoin Stack
Ethereum Stack
Verticals: End User Applications
Wallet/Exchange Applications
Application Framework: Smart Contracts
Bitcoin Blockchain Protocol/Operations
Ethereum Blockchain and Ethereum Virtual Machine
Peer-to-Peer Network and Operating Systems
Hardware

- Considérons le diagramme précédent comparant Bitcoin et Ethereum blockchain :
  - Sur la gauche se trouve la blockchain Bitcoin, une application de portefeuille pour initier des transactions.
  - Sur la droite est Ethereum faisant un pas important vers la transformation de la blockchain en un cadre de calcul qui a ouvert tout un monde d'opportunités dans le domaine décentralisé.
- Ethereum prend en charge les contrats intelligents et les machines virtuelles sur lesquelles s'exécutent ces derniers.

- Toute personne exécutant un client est un nœud dans le réseau Ethereum, qui compte actuellement plus de 25 000 nœuds dans le monde.
- Les contrats intelligents ne sont que des logiques d'application qui peuvent être exprimées à l'aide des opérations définies dans l'EVM et ils peuvent également stocker des données sur la blockchain.

C’est quoi EVM ?

- La machine virtuelle Ethereum (EVM), est un logiciel complet de Turing qui fonctionne sur le réseau Ethereum.

- ✓ Elle permet à quiconque d'exécuter n'importe quel programme, quel que soit le langage de programmation, en disposant de suffisamment de temps et de mémoire.
- ✓ L’EVM rend le processus de création d'applications blockchain beaucoup plus facile et efficace qu'auparavant.

C’est quoi EVM ?

- L'EVM est responsable de l'exécution de tous les contrats intelligents et des transactions sur la blockchain Ethereum.
- Les contrats intelligents, qui sont des programmes autonomes stockés sur la blockchain, sont également exécutés par l'EVM.

C’est quoi EVM ?

- L'EVM utilise l’Ether (ETH) pour payer les frais de gaz nécessaires à l'exécution des transactions et des contrats intelligents.
- l'EVM est l'environnement d'exécution qui permet à Ethereum d'être une plateforme de contrats intelligents et de décentralisation des applications (DApps) en exécutant le code de manière sécurisée et fiable sur sa blockchain.

L’EVM

- Ethereum est une plateforme qui permet de coder des contrats intelligents avec le Langage solidity. En l'utilisant, le code est compilé en bytecode pour être interprété par la machine virtuelle Ethereum (EVM).

L’EVM

- Ethereum peut créer des applications utilisant la blockchain pour stocker des données ou contrôler ce que une application peut faire. Il en résulte une blockchain à usage général qui peut être programmée pour satisfaire toute tache.
- Ethereum ressemble plus à un marché : de services financiers, de jeux, de réseaux sociaux et d'autres applications qui respectent votre vie privée.

- Les opcodes EVM sont un langage machine de bas niveau, qui n'est pas très lisible par l'homme.
- Les développeurs écrivent donc des contrats intelligents dans un langage de haut niveau, qui se compile en opcodes EVM.
- Plusieurs langages de haut niveau existent, comme Serpent et Viper. Mais le plus populaire aujourd'hui s'appelle **Solidity** qui a une syntaxe similaire à JavaScript.

- N'importe qui peut utiliser Solidity pour écrire un contrat intelligent et le déployer sur la blockchain Ethereum en utilisant une simple transaction.
- Pour ce faire, vous devez compiler votre contrat intelligent Solidity en bytecode EVM, puis envoyer le bytecode dans le cadre d'une transaction sur le réseau Ethereum. Une fois la transaction minée, le contrat intelligent est déployé sur la blockchain et reçoit une adresse publique.
- Toute personne peut alors interagir avec le contrat intelligent en envoyant des transactions à son adresse et en spécifiant la méthode qu'elle souhaite invoquer.

- Le résultat de l'appel de la méthode est écrit sur la blockchain après que la transaction a été traitée.

- Il y a également un coût associé à l'invocation d'une méthode de contrat intelligent appelée **gaz**. Le gaz est simplement une unité de mesure qui détermine combien coûtent la quantité de calcul et les opération de code EVM.

Le GAS

Gas in Ethereum est une unité de mesure utilisée pour mesurer le travail effectué par Ethereum pour effectuer des transactions ou toute interaction au sein du réseau.

Une analogie pour comprendre ce qu'est le gaz dans Ethereum:

Vous souhaitez voyager en famille de Madrid à Barcelone, le voyage se fera dans votre voiture. À ce stade, vous savez à l'avance qu'il est à 500 km et que votre voiture consomme 1 litre d'essence tous les 10 km (pour simplifier le calcul), il vous faudra donc 50 litres d'essence pour atteindre votre destination. De plus, vous savez aussi qu'un litre d'essence coûte entre 1 € et 1,5 € selon la station-service où vous vous arrêtez pour faire le plein.

Le GAS

- C'est la même chose que dans Ethereum. D'une part, chaque tâche dans Ethereum a un coût spécifique et non variable stipulé dans Gaz, qui équivaut au litre d'essence que votre voiture utilise par 10 km.
- Bien sûr, les opérations dans Ethereum sont constituées de différentes fonctions plus petites , chacun avec une valeur d'essence spécifique (ou consommation d'essence) et leur somme est ce qui nous indiquera la valeur essence finale de ladite opération (le total d'essence à dépenser pour faire notre voyage).
- Il ne nous reste donc qu'une chose, combien allons-nous payer pour que ce gaz puisse réaliser l'opération à Ethereum?

Le GAS

- Le gaz a un prix en Ether qui est donné par la demande et l'offre d'opérations à Ethereum. Autrement dit, le prix du gaz dans l'éther est variable, bien que dans ce cas, vous puissiez choisir la valeur que vous allez payer pour ce gaz, et si un mineur est d'accord avec cette valeur, il prendra votre transaction et l'exécutera.

Le GAS

- Toutefois, **Dans Ethereum, les développeurs ont décidé d'attribuer des valeurs constantes aux différentes opérations pouvant être effectuées dans Ethereum.** De cette façon, chaque tâche dans Ethereum a une valeur de gaz stipulée, qui ne change pas et n'est pas modifiée par la hausse ou la baisse de la valeur de l'Ether, la monnaie native d'Ethereum.

Le GAS

- C'est pourquoi, avec la création de Gas, les développeurs d'Ethereum peuvent alors différencier entre ce que le coût de calcul et la valeur réelle desdites opérations à un moment donné.
- Par exemple, si un contrat intelligent a pour fonction **"Vérifier le solde d'une adresse"**, cette action dans le réseau peut avoir la valeur de 1000 gaz, et elle aura toujours cette valeur. Cela signifie que pour réaliser cette action dans Ethereum, une petite commission (en éther) doit être versée correspondant à la quantité de Gaz utilisée pour pouvoir réaliser ladite action sur la blockchain.

Le GAS

- Chaque opération effectuée sur la blockchain Ethereum a un coût en gaz, qui est déterminé en fonction de la complexité de l'opération.

Le GAS

Ce qui précède génère trois choses qui sont importantes et vitales au sein d'Ethereum:

1. **Unité de gaz**. L'unité de gaz est la quantité de gaz qui peut être attribuée à une instruction spécifique, mais elle n'a aucune valeur monétaire.
2. **Prix du gaz**. Le prix du gaz, quant à lui, est la commission que nous payons pour chaque unité de gaz. C'est un prix que nous choisissons de payer pour chaque unité et nous le faisons en utilisant des unités décimales d'Ether, appelées Gwei (10^-9 Ether).
3. **Limite de gaz**. Il s'agit d'une valeur qui indique le nombre maximum d'unités de gaz que le réseau Ethereum peut gérer à un moment donné. C'est leur limite maximale, et c'est un point que les mineurs ne peuvent dépasser à aucun moment.

Le GAS

Quelle est la limite de gaz?

1. **La limite de gaz d'une transaction est d'environ 21.000 unités de gaz**.
2. **le Gas Limit d'un smart contract est beaucoup plus élevé et variable**.
3. **Enfin, nous avons la limite de gaz d'un bloc, qui est établie pour ne pas dépasser 8 millions d'unités de gaz.** Cela signifie que les mineurs peuvent inclure autant de transactions et d'interactions avec des contrats intelligents que possible, tant qu'ils ne dépassent pas cette limite.

Le GAS

Comment les mineurs sont-ils payés pour leur travail?

Comme nous l'avons déjà mentionné, le gaz n'a pas de valeur économique, ce n'est pas non plus un jeton au sein d'Ethereum, ce n'est qu'une unité de mesure. C'est une unité importante pour établir la valeur des transactions. Ceci est dû au fait que chaque unité de gaz est facturée en Gwei (décimales d'éther). Ainsi, pour une transaction qui consomme une certaine quantité de Gaz, vous devez payer une certaine quantité d'éther afin qu'elle soit traitée.

Par exemple, si nous avons une opération « Pay Maria » avec un coût de 12.000 20 unités de gaz, et que le coût de l'unité de gaz est de 1 Gwei, nous devons :

*Coût TX en éther = 240.000 Gwei * 0.00000001 = 0.0024 Ether ~ 0,54 $ / 0,48 €*

Le GAS

- Tout le gaz restant est remboursé à l'initiateur de la transaction: l'utilisateur qui a lancé la transaction.
- Une transaction qui n'a plus de gaz est annulée, mais elle est toujours incluse dans un bloc et les frais associés sont payés au mineur.

Minage

- Ethereum utilise un algorithme similaire à celui de Bitcoin, qui est basé sur la preuve de travail, mais légèrement modifié.
- La récompense pour le minage d'un bloc Ethereum est donnée au mineur en éther. Et la récompense du bloc actuel vaut 2 Ether.
- Un bloc est miné sur le réseau environ tous les 15 seconde.

Minage

- Le modèle d'émission de l'Ether est différent de celui du Bitcoin, alors que le Bitcoin est plafonné à 21 millions de pièces. Ethereum n'a pas une telle limite, mais plutôt un plafond annuel, de sorte que seulement 18 millions d'éther peuvent être créés en un an.

Minage

- L'algorithme de minage de Bitcoin peut être exploité en utilisant du matériel de minage spécialisé appelé Asics. Ce qui donne à certains mineurs un avantage injuste sur les autres.
- Cela a conduit à la centralisation de l'exploitation minière du bitcoin, car très peu de personnes peuvent se permettre d'acquérir ce type de matériel spécialisé.
- L'algorithme a été modifié pour être orienté vers les GPUs qui sont plus communément disponibles. Et donc moins susceptibles d'être centralisés.

Minage

- Le débit maximal des transaction du réseau est actuellement inférieur à 16 transactions par seconde.
- Pendant les pics de charge du réseau, le temps entre les blocs peut augmenter et les frais de transaction peuvent s'accroître.
- Plusieurs solutions de mise à l'échelle font l'objet de recherches et de développement, notamment le sharding, la preuve d'enjeu et les canaux d'état.

- Au-delà d'une crypto-monnaie négociable, l'Ether est également utilisé par les développeurs d'applications pour payer les frais de transaction et les services sur le réseau Ethereum.
- Un deuxième type de jeton est utilisé pour payer les mineurs afin qu'ils incluent des transactions dans leur bloc. Il s'agit du gaz, et chaque exécution de contrat intelligent nécessite l'envoi d'une certaine quantité de gaz pour inciter les mineurs à l'inclure dans la blockchain.

Proof of Stake : Preuve de participation
La preuve d'enjeu

Un enjeu est la valeur/l'argent que nous parions sur un certain résultat.

- Proof of Stake (PoS) : conserve les avantages du PoW tout en surmontant certains de ses inconvénients, telle que la grande consommation d'énergie, tout en maintenant la sécurité du réseau et assurant plus de décentralisation.
- Pour la création de bloc, l'algorithme PoS choisit des validateurs aléatoires des nœuds du réseau Blockchain. La sélection aléatoire des nœuds est pondérée par la quantité de crypto-monnaie possédée par chaque nœud du réseau.

Proof of Stake

- En d'autres termes, plus l'utilisateur possède une grande quantité de crypto- monnaie, plus il est susceptible d'être tiré au sort et donc de disposer du droit d'ajouter le prochain bloc.
- Un utilisateur possédant 1000 jetons, a 10 fois plus de chance d'être sélectionné par rapport à un utilisateur n'en possédant que 100. Le nœud "élu" est appelé validateur.

Proof of Stake

- Un algorithme choisit parmi le pool de candidats le nœud qui validera le nouveau bloc.
- Cet algorithme de sélection combine la quantité de mise (montant de crypto-monnaie) avec d'autres facteurs (comme la sélection basée sur l'âge des pièces, le processus de randomisation) pour rendre la sélection équitable pour tout le monde sur le réseau.

Flux de travail de mécanisme basé sur PoS :

1.Les nœuds effectuent des transactions.L'algorithmePoS place toutes ces transactions dans un pool.

2.Tous les nœuds prétendant devenir validateur pour le bloc suivant lèvent une mise. Cette mise est combinée à d'autres facteurs tels que «l'âge des pièces» ou la «sélection de blocs aléatoires» pour sélectionner le validateur.

Flux de travail de mécanisme basé sur PoS :

3. Le validateur vérifie toutes les transactions et publie le bloc. Sa mise reste toujours verrouillée et la récompense de minage (2 Ether) n'est pas encore accordée non plus. C'est ainsi que les nœuds du réseau disent "OK" pour le nouveau bloc.

Flux de travail de mécanisme basé sur PoS :

4. Si le bloc est "OK", le validateur récupère la mise et la récompense également. Si l'algorithme utilise un mécanisme basé sur l'âge des pièces pour sélectionner les validateurs, le validateur du bloc actuel voit son âge des pièces remis à 0. Cela le place dans une faible priorité pour la prochaine élection du validateur.

5. Si le bloc n'est pas vérifié par d'autres nœuds du réseau, le validateur perd sa mise et est marqué comme "mauvais" par l'algorithme. Le processus recommence à partir de l'étape 1 pour forger le nouveau bloc.

Caractéristiques de PoS:

•**Existence de pièces fixes :**

Il n'y a qu'un nombre fini de pièces qui circulent toujours dans le réseau.

•**Frais de transaction comme récompense :**

chaque transaction est facturée par un certain montant de frais. Ceci est accumulé et donné à l'entité qui forge le nouveau bloc. Notez que si le bloc falsifié est trouvé frauduleux la mise du validateur est également perdue (ce qui est également connu sous le nom de **slashing**).

Caractéristiques de PoS:

- **Impraticabilité de l'attaque à 51 % :**

- Pour mener une attaque à 51 %, l'attaquant devra posséder 51 % de la crypto-monnaie totale du réseau, ce qui est assez coûteux. Cela rend l'attaque trop fastidieuse, coûteuse et peu rentable.

- De plus, la validation de mauvaises transactions entraînera la perte de la mise du validateur, ce qui entraînera une récompense négative.

Avantages de PoS :

- **Efficacité énergétique :**

❑ Comme tous les nœuds ne sont pas en concurrence les uns contre les autres pour attacher un nouveau bloc à la blockchain, l'énergie est économisée.

❑ De plus,les nœuds n'ont pas besoin de s'ajuster nonce plusieurs fois, au lieu de cela, la clé pour résoudre ce puzzle est le montant de la mise (pièces).

❑ Par conséquent, **le protocole du consensus PoS est une économie d'énergie**qui s'appuie sur un mode d'incitation monétaire au lieu de consommer beaucoup de calculs.

Avantages de PoS :

- **Sécurité:** une personne tentant d'attaquer un réseau devra détenir 51% des enjeux (assez cher). Cela conduit à un réseau sécurisé.

Faiblesse d'un mécanisme PoS :

- **Validateurs à grand enjeu :**

❑ Si un groupe de candidats validateurs se combinent et possèdent une part importante de la crypto-monnaie totale, ils auront plus de chances de devenir des validateurs.

❑ Des chances accrues conduisent à des sélections accrues, ce qui conduit à de plus en plus de gains de récompenses, ce qui conduit à posséder une énorme part de devises. **Cela peut entraîner la centralisation du réseau au fil du temps.**

Le flux de PoS est illustré dans la Figure suivante.