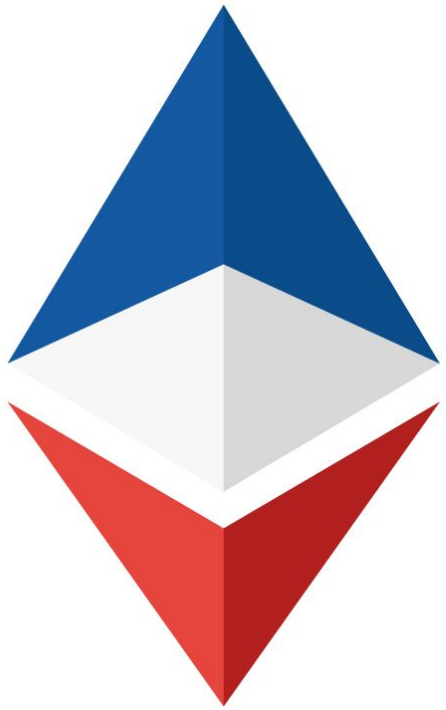


A S S E T H

Ethereum en 20 minutes

Contact: @jdetychey

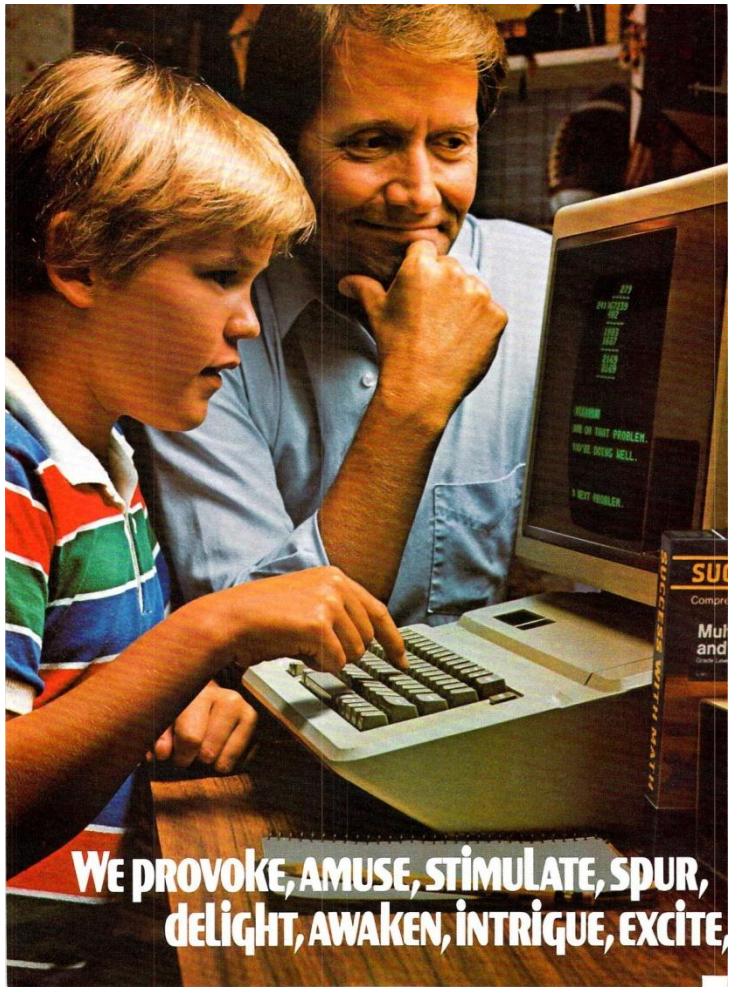
Un petit mot sur l'Asseth

Un association de passionnés aux profils multiples et destinée à faire croître l'éco-système d'Ethereum

Twitter: @AssethFR // Facebook Asseth // www.asseth.fr // Youtube: Asseth Association Ethereum

Pour nous soutenir → Adhérez ← (10€) et parlez de nous pour nous aider à trouver des sponsors

https://www.helloasso.com/associations/asseth/adhesions/adhesion-a-l-asseth



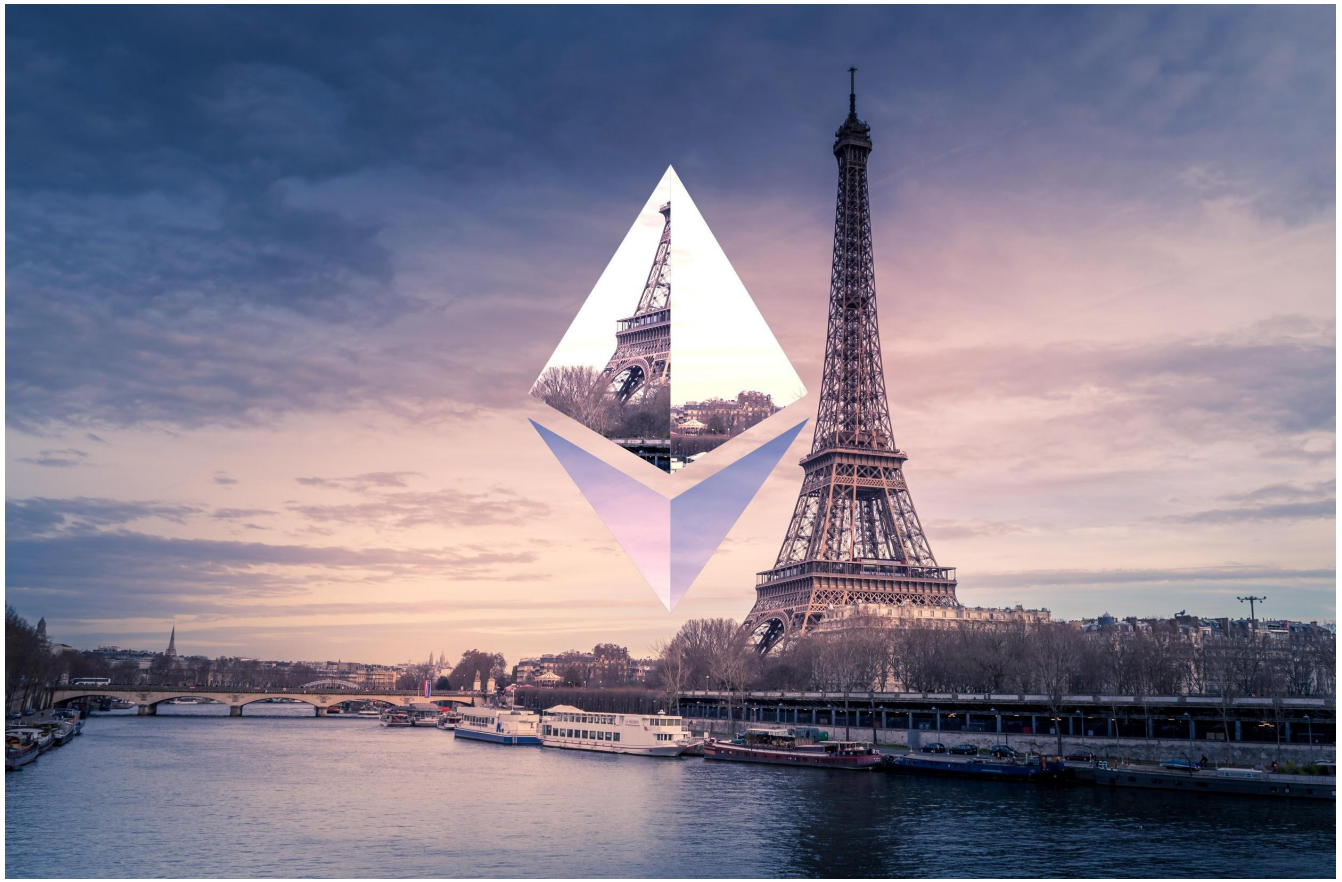
ASSETH

EthCC

Ethereum Community Conference, au CNAM les 8, 9 et 10 mars

- 4 amphithéâtres
- +1000 participants
- Plusieurs flux en parallèle
  - passage à l'échelle, anonymat, outils de développement, gouvernance, impact social, aspects légaux...
- Ateliers en petit comité

https://ethcc.io



ASSETH

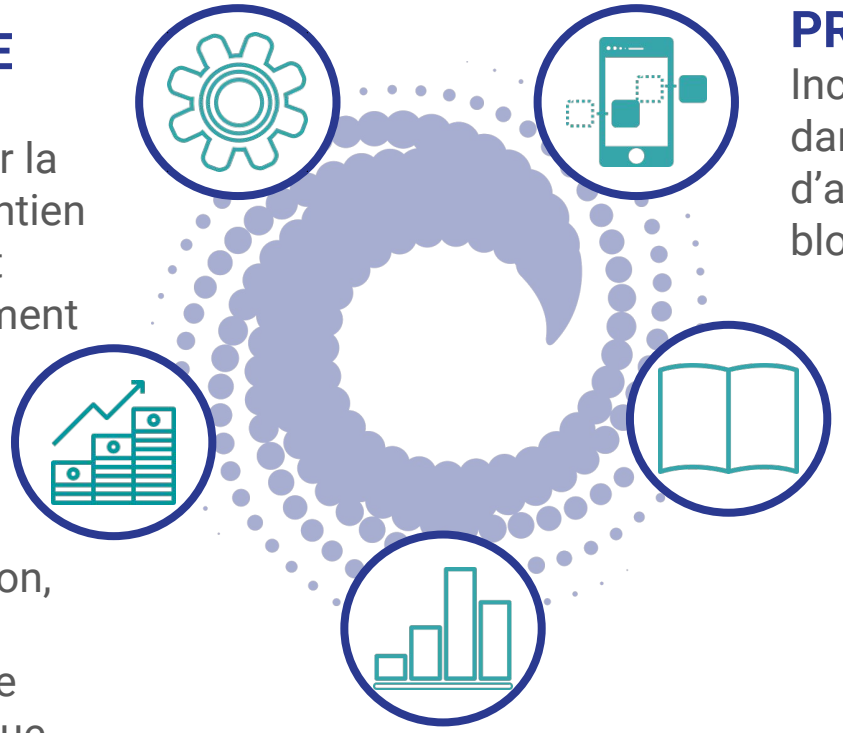
A propos de ConsenSys

Un startup studio

Développant l'infrastructure et l'écosystème, construisant des produits et fortement impliqué auprès des entreprises en leur apportant conseil, support et accompagnement pour la production

INFRASTRUCTURE

Aide l'écosystème Ethereum à grandir par la construction et le maintien de clients Ethereum et d'outils de développement



PRODUITS

Incubation de startups spécialisées dans le développement d'applications décentralisées sur la blockchain Ethereum

DÉVELOPPEMENT DE L'ÉCOSYSTÈME

Développement de l' écosystème au travers de mouvements

Enterprise Ethereum Alliance

Blockchain for Social Impact

CAPITAL

Services de tokenisation, management d'actifs cryptographiques et de gestion de captial-risque

EDUCATION

Formation de développeurs et d'entrepreneurs sur l' écosystème Ethereum à travers des programmes spécialisés

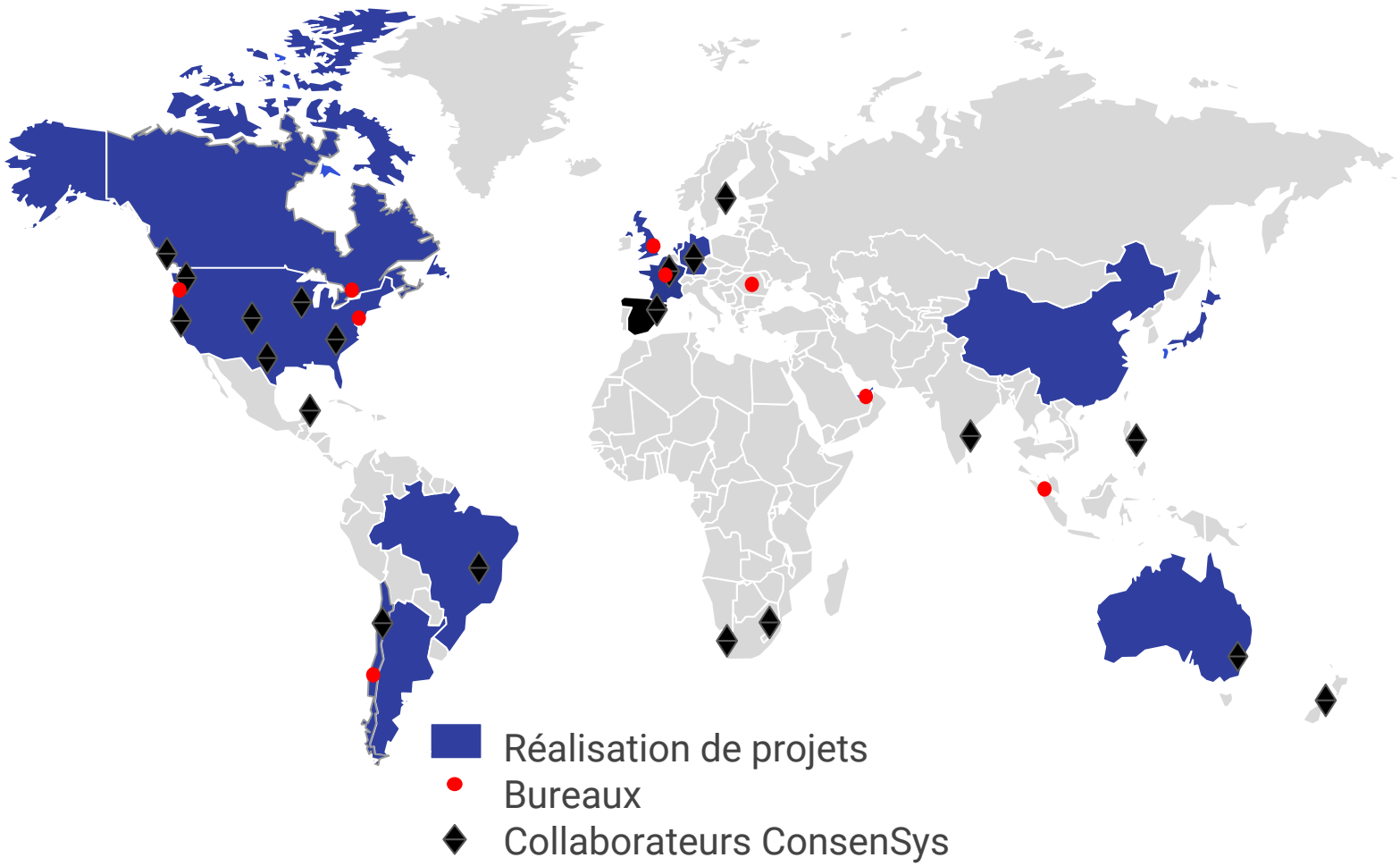
ENTREPRISES / GOUVERNEMENTS

Conseil et développement de solutions blockchain pour les entreprises et les institution gouvernementales

ASSETH

Un rayonnement mondial

Plus de 600 experts blockchain, entrepreneurs, informaticiens, designers, ingénieurs, chercheurs, consultants et business leaders menant des projets sur tous les continents



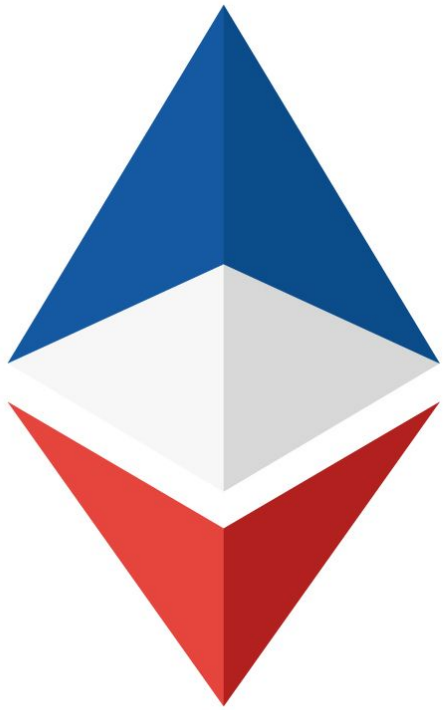
Santander

bhpbilliton

J.P.Morgan

دبـــي الذكية
SMART DUBAI

MAS
Monetary Authority of Singapore

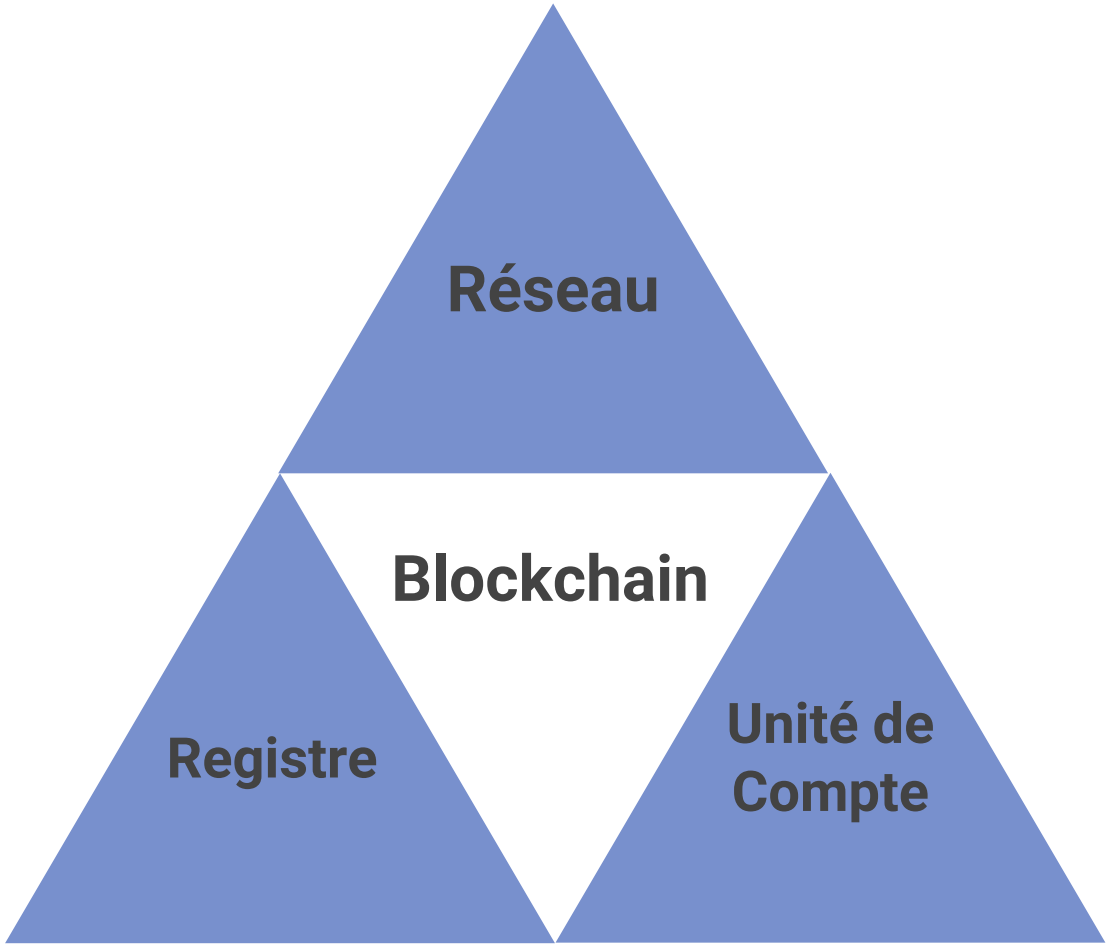


A S S E T H

Contact: @jdetychey

De quoi la blockchain est elle le nom?

Un équilibre subtil entre théorie des jeux (microéconomie), réseau pair à pair et cryptographie

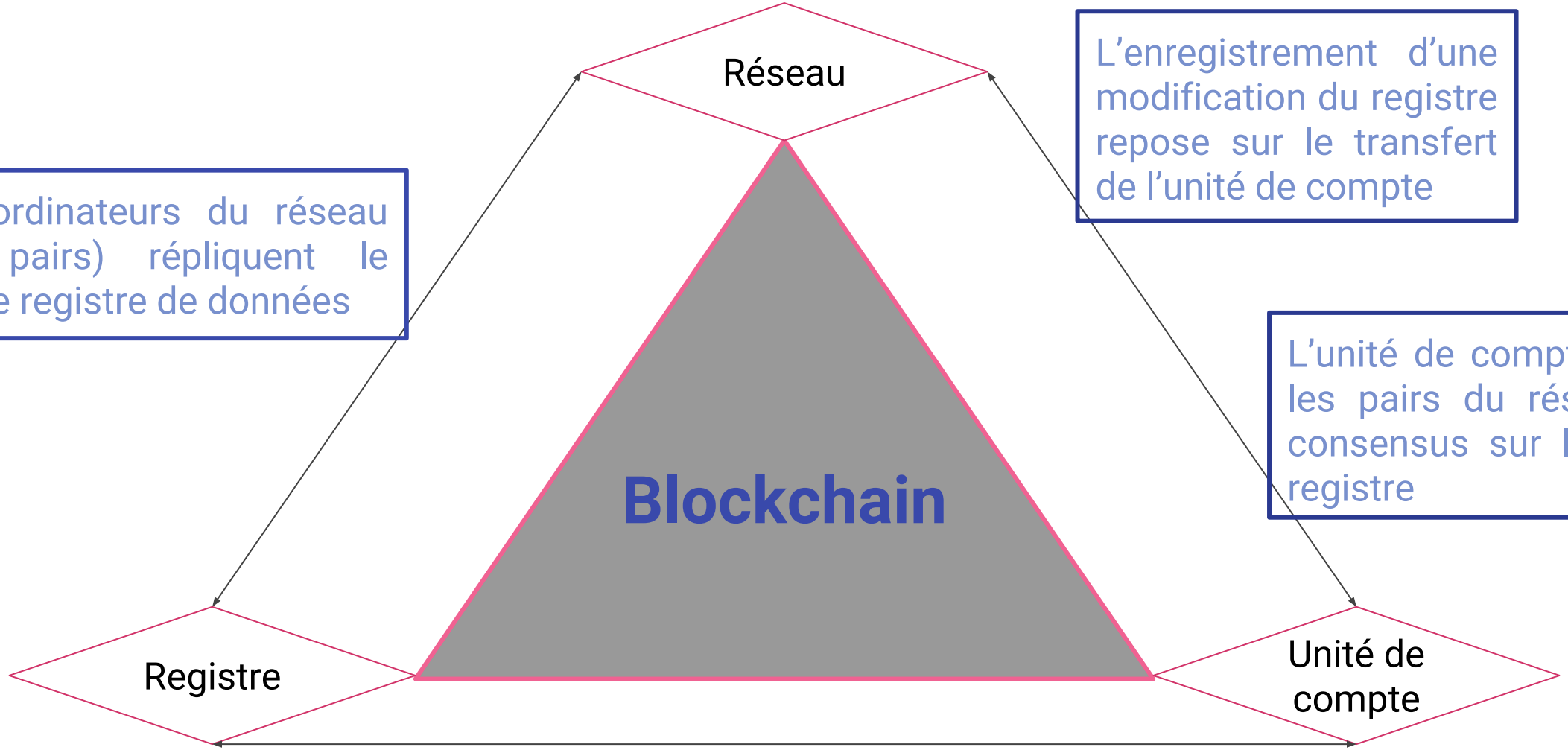


- Un Registre dont les modifications sont passées par bloc qui s'entre référencent, d'où le terme de "chaîne de blocs";
- La Blockchain conserve l'historique de toutes les modifications, le dernier état du registre est même construit par agrégation de cet historique via des techniques cryptographiques;
- Chaque pair (ou nœud) du réseau chacun conserve l'intégralité de la base;
- La réplication permet une grande disponibilité des données et une garantie contre les falsifications;
- Une unité de compte permet l'émergence d'un consensus entre les pairs sur l'état de la base via des mécanismes d'incitations;
- Cette unité de compte a une application monétaire immédiate.

ASSETH

La blockchain, quelques notions essentielles

Un terme polysémique qui recouvre à la fois, un réseau, un registre, et une unité de compte



Les ordinateurs du réseau (les pairs) répliquent le même registre de données

L'enregistrement d'une modification du registre repose sur le transfert de l'unité de compte

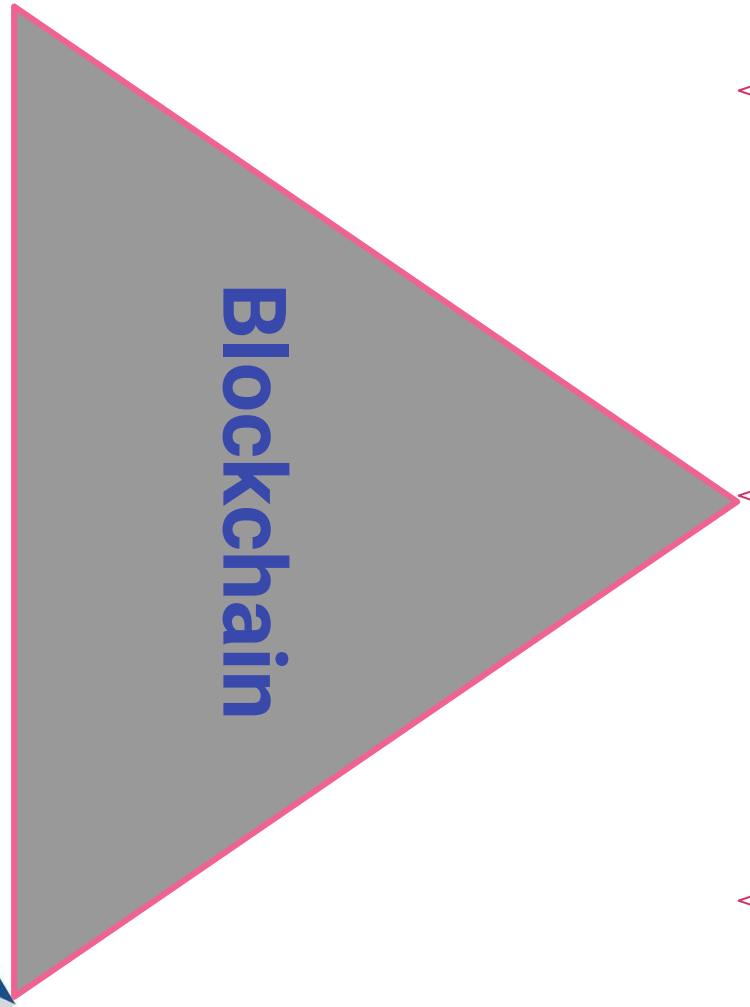
L'unité de compte incite les pairs du réseau au consensus sur l'état du registre

Le registre comprend (entre autres) des numéros de comptes et leur soldes

ASSETH

La blockchain a 3 piliers fondamentaux

Un protocole qui repose sur le hachage, la cryptographie à clé publique et la théorie des jeux



Hachage

Procédé générant une valeur unique et de taille fixe à partir de données de taille arbitraire. L'inversion du procédé est impossible sur le plan pratique. Il permet la cohérence et l'infalsifiabilité du registre.

Clés publiques

Elles sont les entrées du registre. La signature numérique permet une authentification très fortes des utilisateurs.

Théorie des jeux

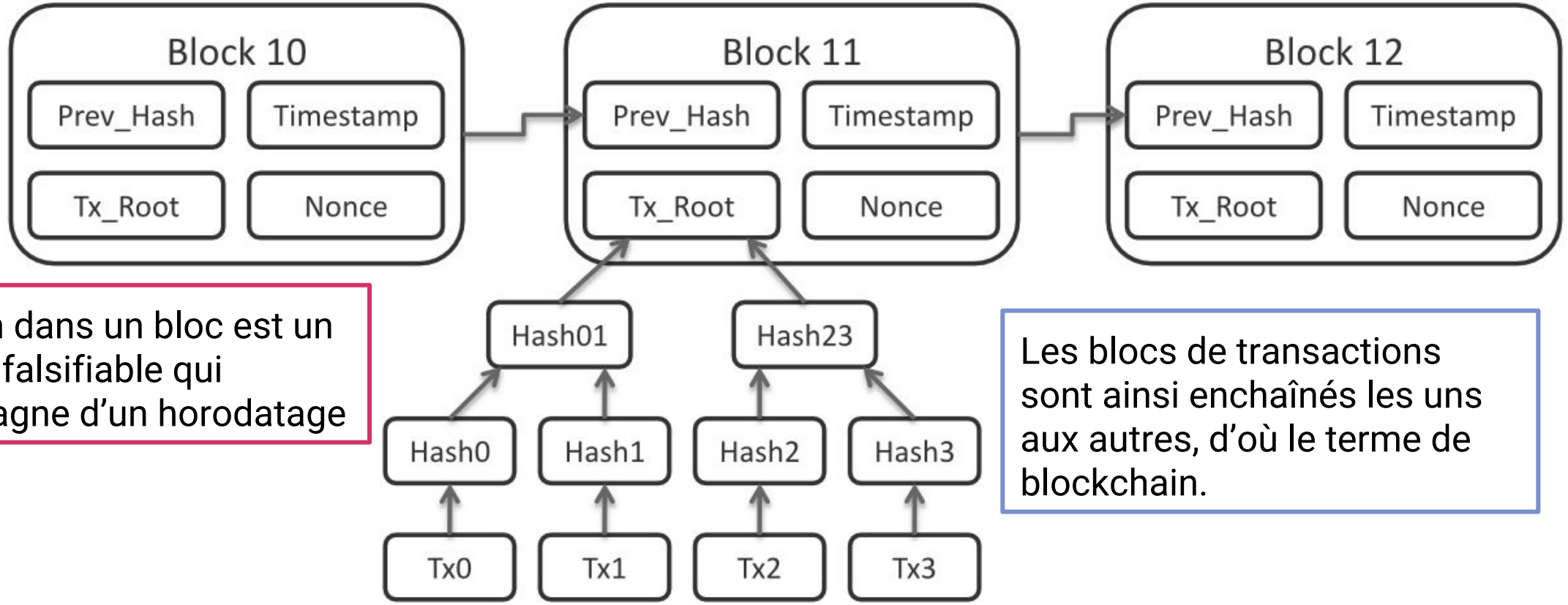
Des mécanismes interviennent pour garantir le bon fonctionnement du réseau pair à pair.

ASSETH

L’origine du mot

Le terme de blockchain provient de la structure des données dans le registre

Les utilisateurs de la blockchain peuvent modifier le registre en diffusant une transaction dans le réseau, les transactions nouvelles sont regroupés au sein d’un bloc qui fait référence au dernier bloc connu.



L’inclusion dans un bloc est un procédé infalsifiable qui s’accompagne d’un horodatage

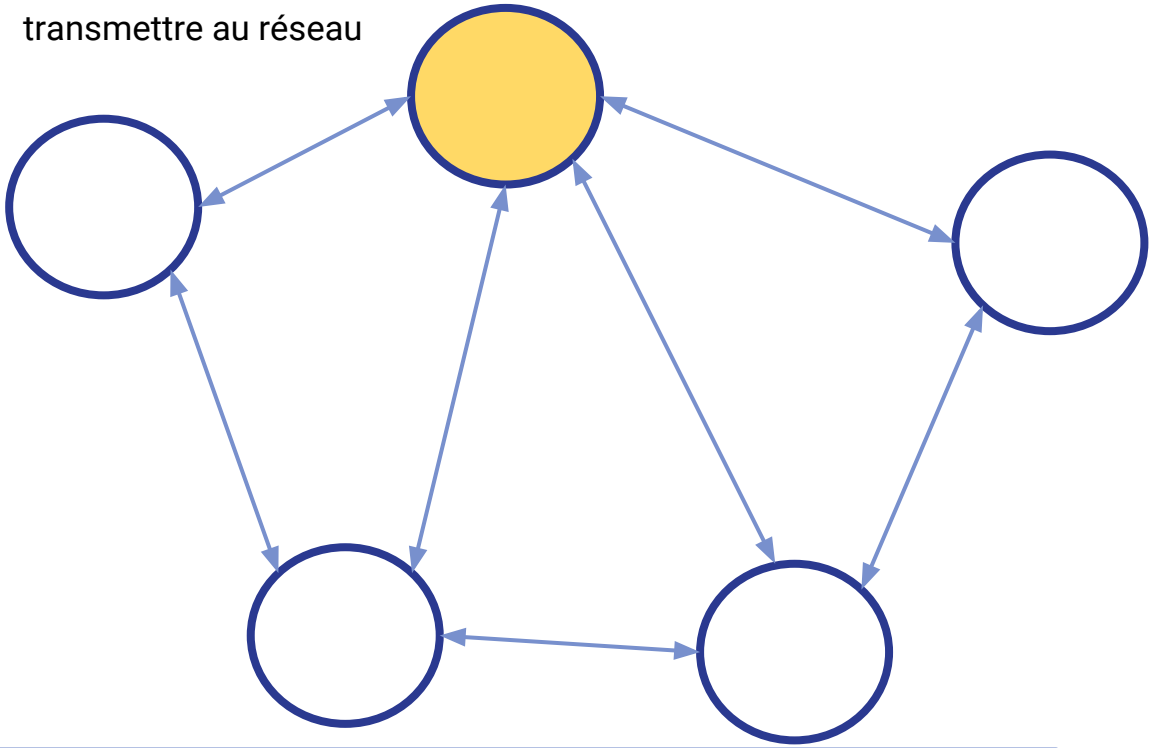
Les blocs de transactions sont ainsi enchaînés les uns aux autres, d’où le terme de blockchain.

ASSETH

Le consensus, pourquoi ce bloc plutôt qu'un autre?

L'innovation majeure réside dans l'algorithme permettant l'émergence d'un consensus sur l'état du registre dans un très grand réseau

- Un des noeuds doit être le leader
- Son rôle est de créer le nouveau bloc de transactions et de le transmettre au réseau



La théorie des jeux intervient pour concevoir des mécanismes d'incitation à partir de l'unité de compte

La selection du leader

- De nombreuses blockchains utilisent la **Proof of Work** (Méritocratie). Le droit d'être le leader repose sur un travail fourni dont tout le réseau peut attester de la difficulté. L'activité est accessible à tous et les pairs actifs travaillent pour être le leader à chaque nouveau bloc. Le travail fourni est perdu d'un bloc à l'autre. L'unité de compte sert à compenser le travail fourni par le leader.
- **Proof of Stake** (Capitalisme). Les utilisateurs peuvent engager leur responsabilité à conserver et entretenir le registre à hauteur de leurs fonds personnels. A chaque nouveau bloc, le leader est tiré au sort avec plus ou moins de chance selon les mises.
- RAFT (Démocratie). Le leader est désigné pour un mandat qui se termine prématurément si le noeud n'est plus actif
- Proof of Authority (Monarchie), une liste de leaders est établi avec un ordre de priorité
- ...

Les formes de consensus permettent plus ou moins de tolérance aux pannes dans le réseau et au manque d'intégrité des pairs

ASSETH

L’exemple de Bitcoin

Bitcoin, c’est à la fois un réseau, un registre, et une unité de compte

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sun Jan 14 2018 17:41:41 GMT+0100 (CET).

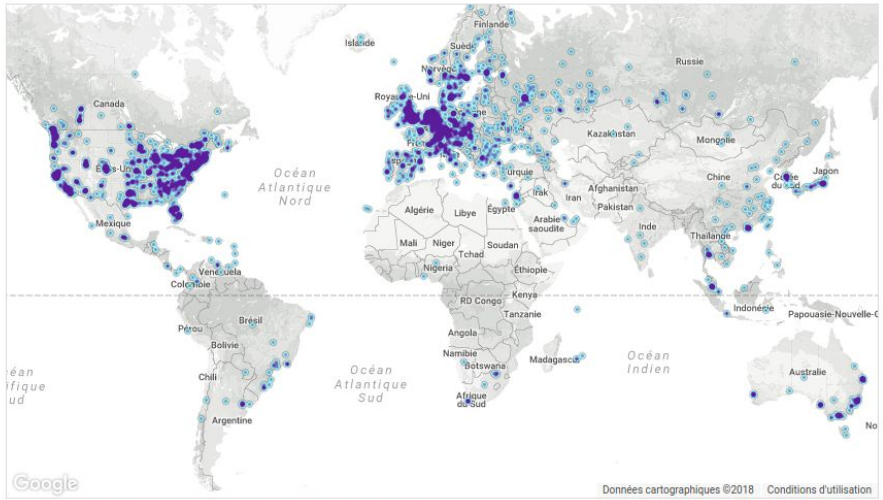
11681 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	3184 (27.26%)
2	Germany	1982 (16.97%)
3	China	812 (6.95%)
4	France	802 (6.87%)
5	Netherlands	542 (4.64%)
6	Canada	468 (4.01%)
7	United Kingdom	452 (3.87%)
8	Russian Federation	398 (3.41%)
9	n/a	297 (2.54%)
10	Singapore	244 (2.09%)

More (105) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

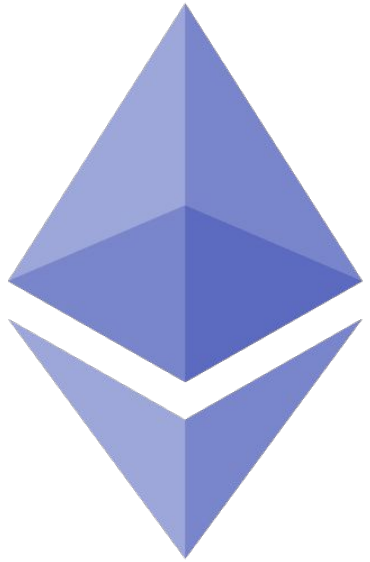
Le réseau bitcoin comprend une dizaine de milliers d’ordinateurs sur lesquels sont répliqués le registre bitcoin dont la taille est d’environ 150 Go et comprend le solde en bitcoin de millions de comptes. Actuellement le réseau est capable d’inclure jusqu’à 300 000 transactions par jour dans le registre.

Depuis 2009, Le réseau n’a toujours pas d’autorité centrale ni connu de panne ou de modification pirate

ASSETH

De l’application monétaire Bitcoin à l’ordinateur Ethereum

Conçue à l’origine sur le protocole Bitcoin, la technologie blockchain a su évoluer pour s’adapter au développement d’applications décentralisées avec l’introduction des “smart contracts”, ni plus ni moins que des logiciels en blockchain



> *Think of Ethereum as a world computer.*
> *What Bitcoin does for payments, Ethereum does for anything that can be programmed.*

Vitalik Buterin, fondateur d’Ethereum

En fonctionnement depuis juillet 2015, le réseau Ethereum comprend environ 30 000 d’ordinateurs sur lesquels est répliqué le registre ethereum dont la taille utile est d’environ 15 Go.
Ethereum héberge des logiciels et le solde en éther de millions de comptes.
Actuellement le réseau est capable d’inclure jusqu’à 1 350 000 transactions par jour dans le registre. Ces dernières transfèrent des unités de compte ou provoquent l'exécution de code, sans risque d’interruption ou d’interférence.

Les avantages d'Ethereum

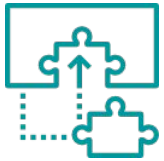
Ethereum est la seule blockchain basée sur une machine virtuelle dotée d'un langage nativement Turing-complet au sein d'un protocole sécurisé intrinsèquement par la blockchain (réplication, résistance à la censure, cryptographie)

Smart Contracts

Des possibilités supérieures apportées par les smart contracts et une sécurité accrue par le consensus utilisé

Impartialité

Ethereum est développé par une fondation sans but lucratif et non rattachée à des fournisseurs



Interopérabilité

Compatibilité entre blockchains privées et publiques ethereum et interopérabilité avec les autres protocoles

Gouvernance

Existence de blockchain privées et permissionnées adaptées aux cas d'usages des entreprises et des institutions gouvernementales

Communauté

Une communauté en constante expansion regroupant aujourd'hui plus de 50 000 développeurs

Confiance

La valeur totale des actifs protégés sur le réseau Ethereum public atteint plusieurs milliards de dollars

Enterprise Ethereum Alliance

L'EEA grandit plus rapidement que tout les autre consortia sur la blockchain combinés

Tokenisation

La plateforme prédominante pour l'écosystème des tokens

A S S E T H

Cas d’usage

Des cas d’usage à fort potentiel voient le jour dans de multiples domaines

Supply Chain

La provenance des biens devient vérifiable et traçable conduisant à une révolution de la supply chain et de la transparence

Modèles de gouvernance

Des Organisations Autonomes Décentralisées (DAO) basées sur la blockchain pour maintenir la transparence dans la gouvernance

Protection de l’Identité

La protection de l’identité ne se base plus sur une entité de contrôle centralisée, de même pour les objets connectés

Données médicales

La possibilité de gérer soi-même ses données de santé et les utiliser sans contrainte

Stockage décentralisé

Ne requiert pas de backup additionnel ou de plan de récupération en cas de catastrophe. Absence de point de défaillance unique ou de contrôle centralisé

Divertissement

Contrôle de la propriété et de la distribution des oeuvres par les artistes afin qu’ils ne soient pas exploités et qu’ils puissent recevoir directement la compensation pour leur travail

Vote

Des système de vote sécurisés et facilement auditables

IoT

La blockchain peut être utilisée comme un moyen de connecter et d’auditer l’Internet des Objets ainsi que le transfert de valeur entre machines

ASSETH

Merci de votre attention

Jérôme de Tychey

@jdetychey

https://www.asseth.fr

jerome@consensys.net

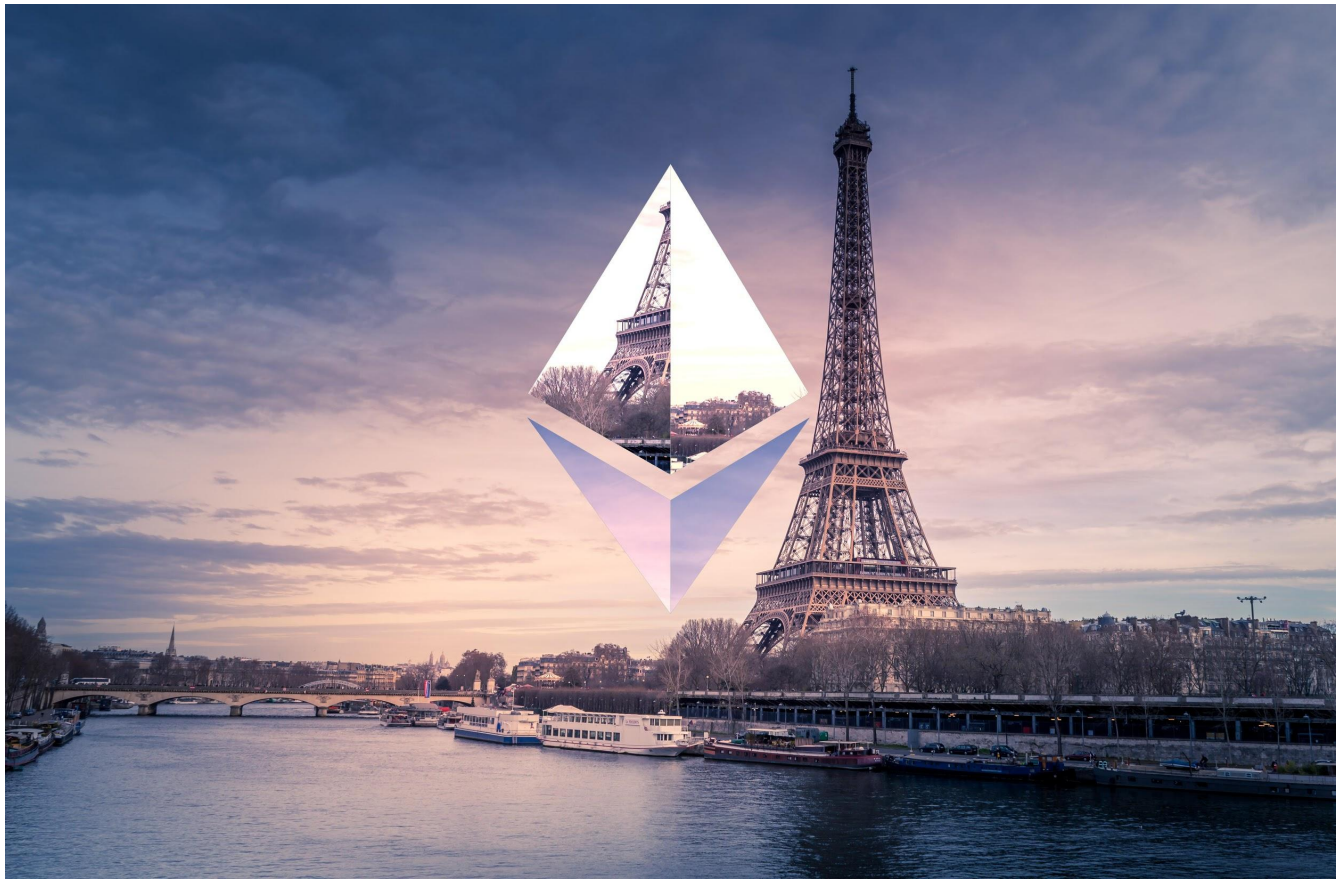
ASSETH

EthCC

Ethereum Community Conference, au CNAM les 8, 9 et 10 mars

- 4 amphithéâtres
- +1000 participants
- Plusieurs flux en parallèle
  - passage à l'échelle, anonymat, outils de développement, gouvernance, impact social, aspects légaux...
- Ateliers en petit comité

https://ethcc.io



ASSETH

ASSETH