



CONSENSYS

# COE Rexecode (Jan 30, 2018)

Introduction

# Sommaire

<b>A propos de ConsenSys</b>	<b>03</b>
<b>La Blockchain de Bitcoin à Ethereum</b>	<b>07</b>
<b>Joseph Lubin, CEO de ConsenSys</b>	<b>14</b>



# ConsenSys

Un startup studio utilisant la technologie blockchain pour construire des applications décentralisées

## VISION

Notre vision est un monde dans lequel les **applications décentralisées** et l'ordinateur mondial Ethereum **vont rendre possible un nouveau genre de commerce global harmonieux et ouvert à tous.**

## MISSION

Notre mission est de construire les outils nécessaires pour bâtir et mettre à l'échelle de la planète le **système de fonctionnement économique, social et politique émergent.**

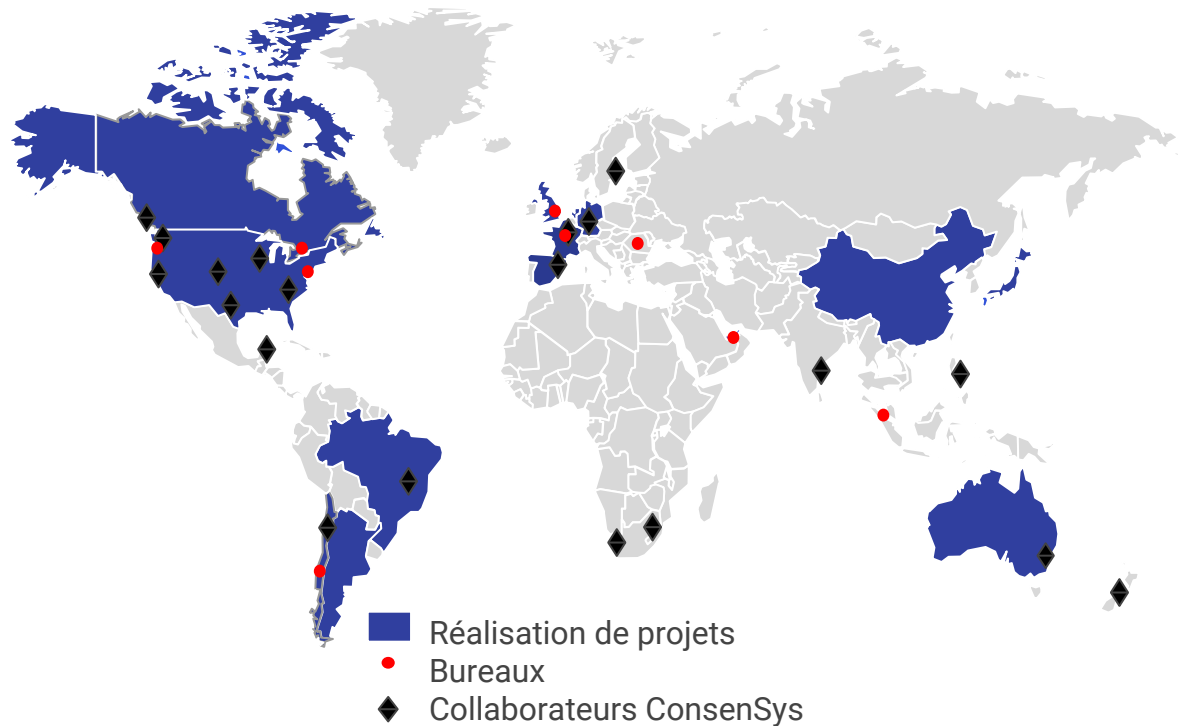
## PLATEFORME

Construite pour dépasser les capacités de Bitcoin, la blockchain **Ethereum** a vu le jour afin de devenir **l'ordinateur mondial.**



# Un rayonnement mondial

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



J.P.Morgan

دبي الذكية  
SMART DUBAI



Monetary Authority of Singapore  
ANNUAL REPORT 2015



# 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

## CAPITAL

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



## EDUCATION

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



Enterprise  
Ethereum  
Alliance



Blockchain  
for  
Social Impact

## ENTREPRISES / GOUVERNEMENTS

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



A S S E T H



# Ethereum Enterprise Alliance

ConsenSys a fondé l'Enterprise Ethereum Alliance qui est à ce jour le plus large consortium interinstitutionnel sur la technologie blockchain

L'EEA rassemble entreprises de premier plan, startups, universités et cabinets de conseil. Le partage d'expériences et la co-construction de solutions techniques permet de maintenir Ethereum comme le seul protocole blockchain de qualité professionnelle adapté aux besoins de l'entreprises.

L'EEA produit des standards open-source et des solutions aux exigences de déploiement des entreprises.



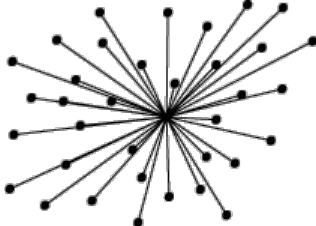
# La Blockchain de Bitcoin à Ethereum



# Constat sur l'économie numérique: elle tend vers la décentralisation

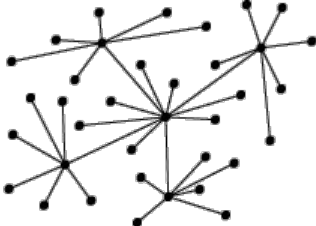
Les business models reposent de plus en plus sur la réduction des intermédiaires

## Platform Economy



2010

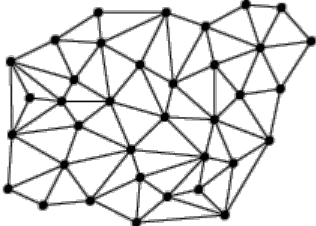
## Sharing Economy



UBER

2015

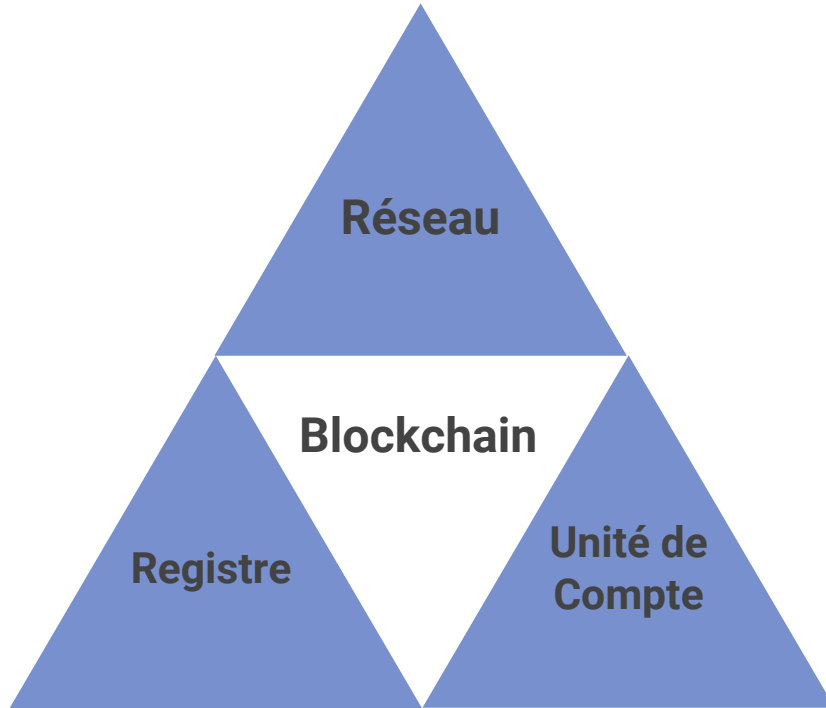
## P2P Economy





# De quoi la blockchain est elle le nom?

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

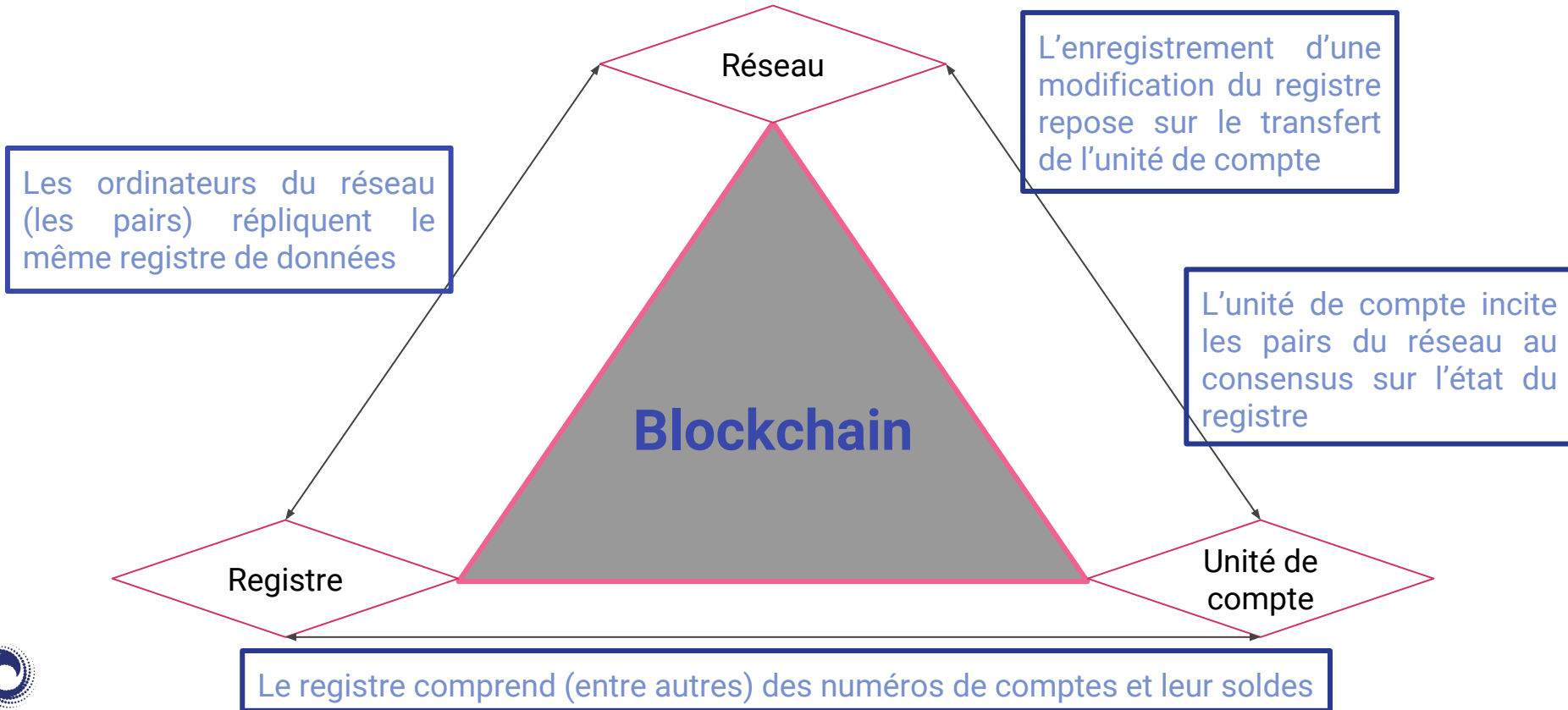


- Un Registre dont **les modifications sont passées par bloc qui s'entre référencent**, d'où le terme de "chaîne de blocs";
- **La Blockchain conserve l'historique de toutes les modifications**, le dernier état du registre est même construit par agrégation de cet historique via des techniques cryptographiques;
- **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.



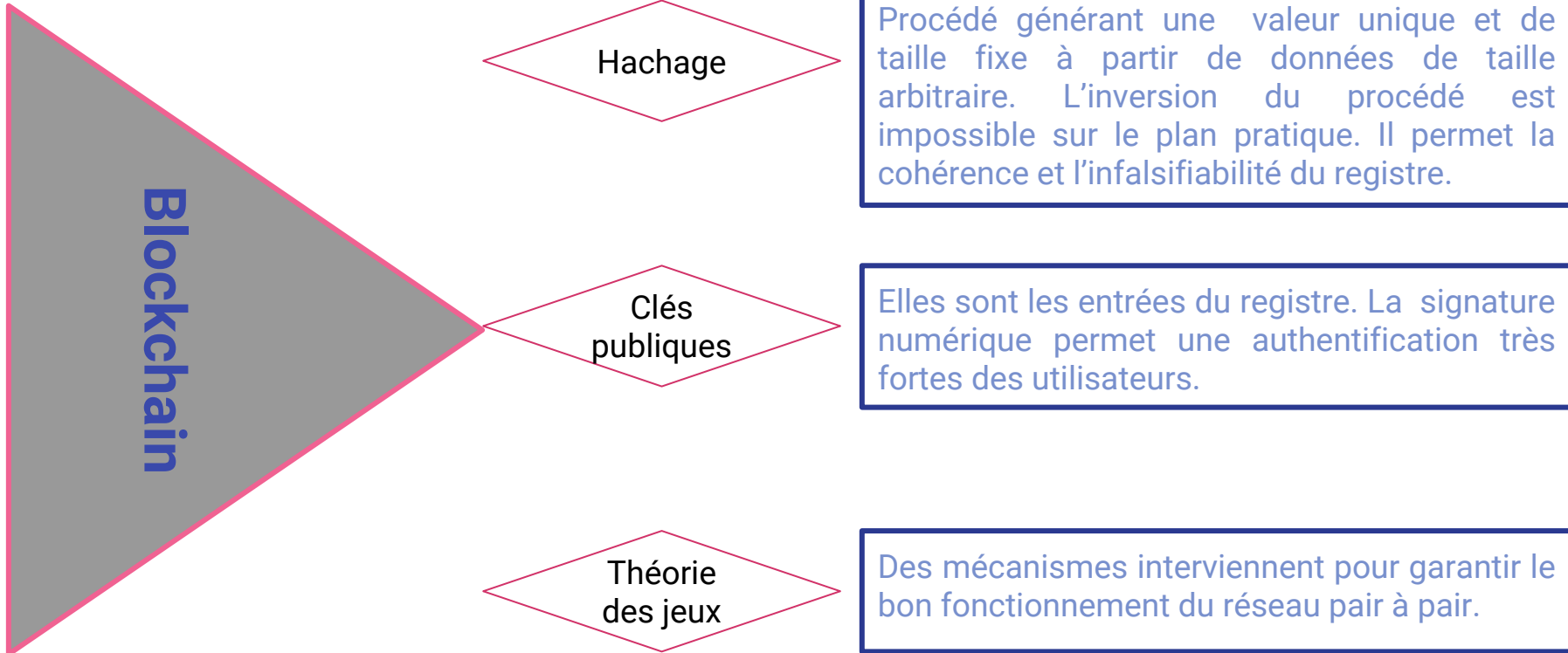
# De quoi la blockchain est elle le nom?

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



# La blockchain a 3 piliers fondamentaux

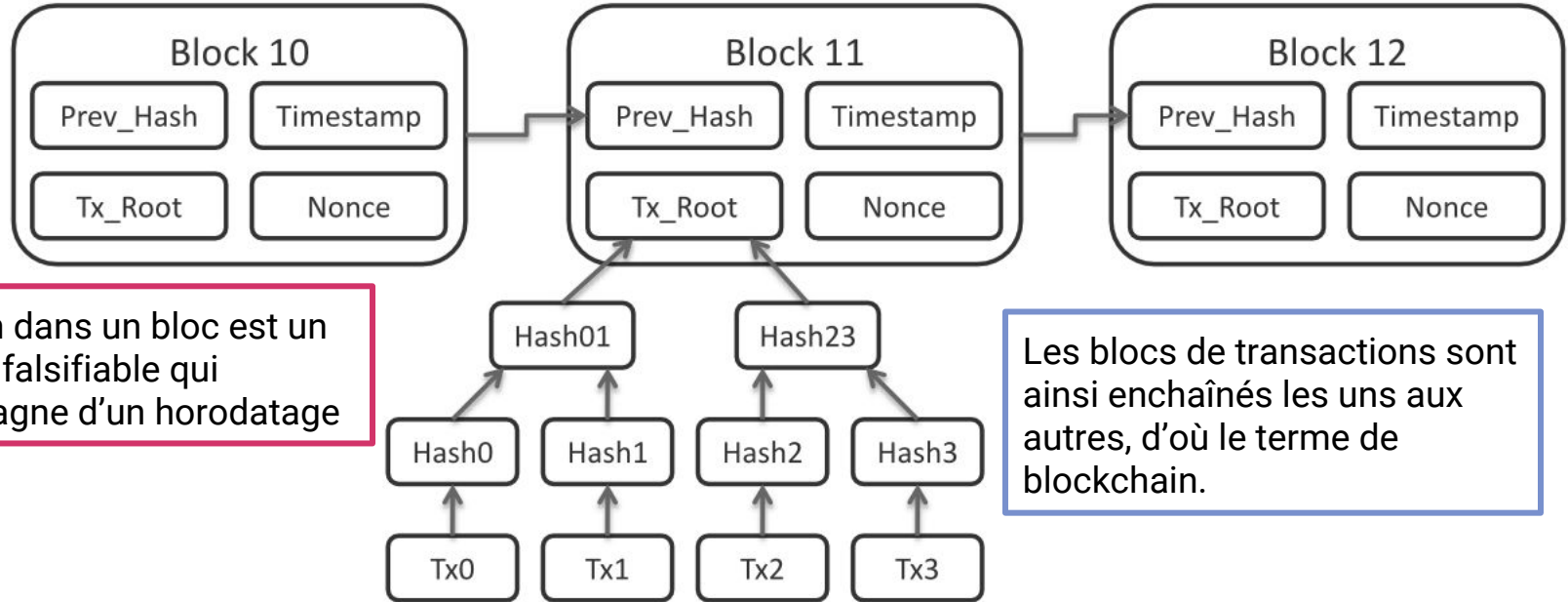
Un protocole qui repose sur le hachage, la cryptographie à clé publique et la théorie des jeux



# 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

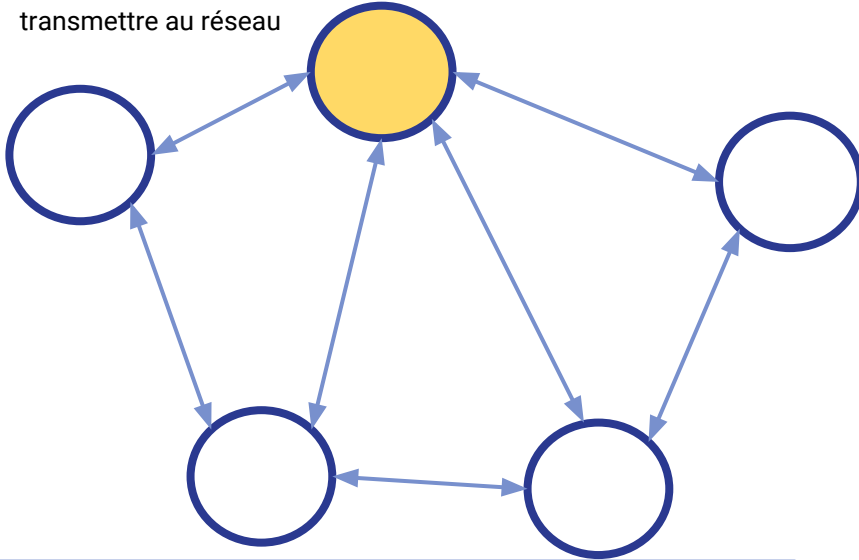
Les blocs de transactions sont ainsi enchaînés les uns aux autres, d'où le terme de blockchain.



# 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 sélection 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 nœud 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



# L'exemple de Bitcoin

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



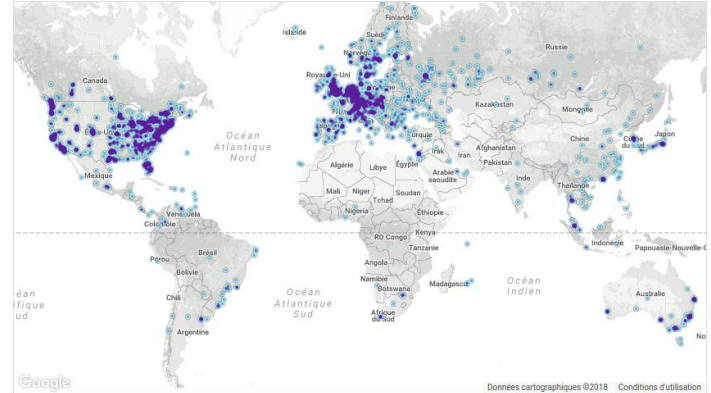
**GLOBAL BITCOIN NODES DISTRIBUTION**  
Reachable nodes as of Sun Jan 14 2018  
17:41:41 GMT+0100 (CET).

**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



# 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.



# Pourquoi utiliser envisager d'utiliser Ethereum?

Impacts potentiels



## Réduction des coûts

- Disparition des intermédiaires
- Les Smart Contracts réduisent les saisies manuelles et les erreurs de traitements



## Augmentation des revenus

- De nouveaux produits et services sont possibles
- De la valeur est créée par la transparence dans l'origine et le traitement



## Réduction des risques

- Pas de point de faille unique et une grande résilience face aux attaques
- La Non-répudiation réduit les fraudes
- L'immutabilité garantit la qualité de l'audit



## Plus rapide et plus satisfaisant pour l'utilisateur

- Suivi logistique grandement simplifié
- Le paiement et les conclusions d'un contrat deviennent possible à T+0





# 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 systèmes de vote sécurisés et facilement auditable



## 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



# Joseph Lubin, CEO de ConsenSys et cofondateur d'Ethereum



# Joseph Lubin

CEO de ConsenSys et cofondateur d'Ethereum



Entrepreneur de nationalité canadienne, diplômé de Princeton

## Carrière

- Robotique: Princeton Robotics Lab, Vision Application Inc.
- Conseil en systèmes d'informations, Blacksmith Software Consulting
- Vice President Technology chez Goldman Sachs
- ConsenSys





CONSENSYS

The background of the entire page is a vibrant blue. It is decorated with a complex, abstract pattern of white lines and dots. These elements form various geometric shapes, including triangles, polygons, and interconnected networks, resembling a molecular structure or a data visualization. The pattern is scattered across the entire surface, with some denser clusters and some sparse areas.

# Appendix

# Soirée d'ouverture du bureau de ConsenSys France le 1er Février

<http://bit.ly/consensysfr>



- 18h à 19h30 - Meetup et débat avec:
  - Laurent Benichou (Directeur R&D et Blockchain lead chez AXA)
  - Alexis Collomb (Professeur de Finance, CNAM)
  - Domitille Dessertine (Fintech Innovation & Compétitivité à l'Autorité des marchés financiers AMF)
  - Nadia Fidali (Programmes Blockchain, Caisse des Dépôts)
  - Eric Larcheveque (PDG Ledger)
  - Joseph Lubin (Fondateur de ConsenSys and co-fondateur de Ethereum)
- 19h30 à minuit: Boissons et networking pour la soirée de lancement



# Dozens of ventures and projects across industry sectors

## EXAMPLES

### // PLATFORMS & APPLICATIONS



**GNOSIS**  
A prediction markets as a service platform that can be used for various domains from sports to celebrity news.  
*Gnosis.pm*



**VIANT**  
A blockchain asset tracking & supply chain platform that provides domain-agnostic modeling.  
*Viant.io*



**GRID+**  
Grid+ leverages the public Ethereum blockchain to give consumers direct access to wholesale energy markets.  
*Gridplus.io*



**AIRSWAP**  
A platform that makes it easy to find, price, and trade tokens peer-to-peer on the Ethereum blockchain.  
*Airswap.io*




**TRUSET**  
A decentralized marketplace to crowdsource the collection, cleansing, and distribution of capital markets reference data.  
*Truset.com*



**CONSENSYS ADTECH**  
Helping advertisers secure supply chains leveraging the power of decentralized human subjectivity. Technical advisor to AdChain.



**UJO**  
A digital rights management platform enabling transparency, fairness and profitability in the creative.  
*Ujomusic.com*



**BALANC3**  
A distributed ledger system for triple-entry accounting and financial audit reporting.  
*Balanc3.net*



**VIRTUE POKER**  
A peer-to-peer community poker platform built on trust, transparency and provably fair gaming.  
*Virtue.poker*



**GOVERNX**  
A governance platform for creating and managing complex decentralized and distributed organizations.  
*Boardroom.io*



**FATHOM**  
A decentralized peer assessment protocol forming the foundation of a universal academic system.  
*Fathom.network*



**VARIABLE**  
A secure, efficient derivatives trading platform on Ethereum that matches traders in secure zero-sum smart contracts.  
*Variabl.io*



**SINGULAR DTV**  
A decentralized blockchain entertainment studio, smart contract-based rights platform and video on-demand portal.  
*SingularDTV.com*




**LOCALITIES**  
A loyalty network uniting independent merchants to their customers to incentivize spending in the local economy.  
*Localities.io*



**BENEFACTORY**  
A community platform for proposing and crowdfunding public goods that contribute to their mission.  
*Benefactory.cc*



**OMEGAONE**  
A decentralized, automated trade execution platform making crypto trading cheap and safe.  
*Omega.one*



**BOUNTIES NETWORK**  
Freelance task fulfillment, paying out in any Ethereum token upon successful completion.  
*Bounties.network*



**OPEN LAW**  
A blockchain-based protocol for the creation and execution of legal agreements in a user-friendly, compliant way.  
*OpenLaw.io*

### // CORE COMPONENTS



**UPORT**  
A self-sovereign identity management & KYC/AML attestation system with user-controlled disclosure.  
*Uport.me*



**METAMASK**  
An identity and transaction management solution in a browser, eliminating the need to install an Ethereum node.  
*Metamask.io*



**DILIGENCE**  
An Ethereum security best practices service provider, promoting legal precautions and ethical business models.  
*diligence@consensys.net*



**ALETHIO**  
A blockchain analytics platform providing insights to startups, projects, enterprises and empowering the community.  
*Aleth.io*

### // DEVELOPER TOOLS



**BTC RELAY**  
Ethereum smart contracts can trustlessly verify arbitrary Bitcoin transactions and payments.  
*Btcrelay.org*




**TRUFFLE**  
A development environment, testing framework and asset pipeline for Ethereum-based smart contracts & dapps.  
*Truffleframework.com*



**NETHEREUM**  
A .NET integration library for Ethereum allowing users to interact with Ethereum clients like geth or parity using RPC.  
*Nethereum.com*

### // BLOCKCHAIN INFRASTRUCTURE



**INFURA**  
A scalable, standards-based, globally distributed cluster and API endpoint for Ethereum, IPFS, and other infrastructures.  
*Infura.io*



**BLOCKAPPs**  
Develops STRATO, a scalable Haskell-based client with API to rapidly develop & deploy enterprise blockchain apps.  
*Blockapps.net*



Microsoft and ConsenSys have partnered to offer Ethereum Blockchain as a Service on Microsoft Azure so Enterprise clients and developers can have a single-click cloud-based blockchain developer environment.

# An end-to-end offering for Enterprise



## Consulting

Key area for testing market demand for products and validation of products, both for enterprises and for our B2C dApps.

Drives adoption of Ethereum and associated distributed technologies in addition to already being monetizable. Feeds into decision making process, for enterprise products and funding R&D for public DApps.

**Business model prototyping**

**Market analysis**

**Customer research**



## Training & Support

As more institutions are increasingly interested in blockchain applications and interacting with digital assets, greater need for training and support. ConsenSys is developing Enterprise training through ConsenSys Academy. Support focuses on both protocol level development and core tools and applications.

**Strategy workshops | 2-5 days**

**Education sessions | 2-5 days**



## Software & Products

From concept to functioning prototype, our solutions turn blockchain strategies into a proven reality. Our solutions include rapid prototyping, solution delivery, systems integration and pre-built, domain specific solutions.

**Rapid prototyping | 6-8 weeks**

**Solution delivery | month(s)**

**Systems integration | month(s)**

**Pre-built, domain specific solutions**





# Ethereum + ConsenSys impact



This is the first ever city-wide effort to implement blockchain technology led by the Smart Dubai Office under the leadership of Her Excellency Dr. Aisha Bin Bishr, who serves as the organization's Director General. ConsenSys will collaborate with government officials and IBM, the project's Lead Strategic Partner. The Dubai Blockchain Strategy 2020 is a unique mandate by the city of Dubai **requiring all government records and transactions to be documented using blockchain.**

## PROVENANCE

BHP Billiton, the world's largest mining firm, is using blockchain **to record movements of wellbore rock and fluid samples and better secure the real-time data that is generated during delivery.** This will enable benefits for its internal efficiency while allowing it to work more effectively with partners.



## ENTERPRISE ETHEREUM ALLIANCE

The EEA was launched in early March 2017 and today is the **world's largest open-source blockchain initiative.** It comprises **150+** blockchain startups, technology companies, and established firms across multiple industries. ConsenSys is a founding member whose goal is to lead the development and improvement of the Ethereum platform to meet enterprise needs.



## GNOSIS PLATFORM

ConsenSys built Gnosis, a decentralized prediction market platform on Ethereum, to trade outcomes of events. It allows users to easily build new predictions markets for specific topics. **It reached its goal of \$12.5M USD sale of Ether within 10 minutes.** Gnosis can be used by many users: trader, proposition writer, market maker, data feed provider, oracle, insurer, etc. It's the first Ethereum-based prediction market that **utilizes the wisdom of the crowd to accurately forecast events before they happen.**



## CROSS-BORDER SETTLEMENT AND PAYMENTS

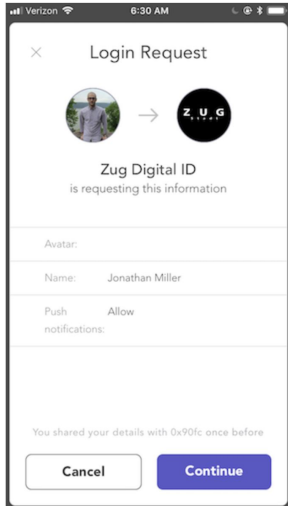
In collaboration with Santander, ConsenSys has developed a **cash tokenization utility and a real-time payment system for both domestic and international payments on Ethereum** to prove that money can be digital and interoperable. Its operation development required minimal integration with core banking system and could be easily scaled to work with additional actors thank to the shared ledger. Benefits include International payments cleared, settled and disbursed in 10-15 seconds

## PRIVACY J.P.Morgan

JP Morgan has developed and deployed **Quorum, an Enterprise-ready distributed ledger and smart contract platform.** It is ideal for any application requiring high speed and high throughput processing of private transactions within a permissioned group of known participants.



# Landmark projects in the field of digital identity



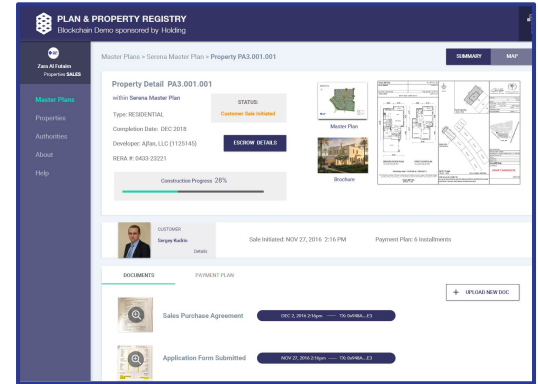
## Zug digital ID

On November 15, 2017, Ethereum-based self-sovereign identity platform uPort opened identity registration on the Ethereum blockchain to inclined citizens.



## Brazil digital ID

Digital signature for the verification of important notarized documents



## Land Registry

The Property Development Approval process involves many different parties and documents. This complex multi-party, multi-step approval process required real time visibility for all participants in the workflow and immutable, non-repudiable audit trail. The process can be time consuming and paper intensive. ConsenSys was engaged to develop a blockchain based alternative as a Proof of Concept then Pilot.

