
KEYTRONIC

Du Bitcoin à Ethereum : l'ordinateur monde

Jean-Paul DELAHAYE,
CRISTAL UMR **CNRS** 9189

Paris 15 novembre 2016

Quel est l'intérêt d'un ordinateur réparti sur toute la surface du globe ?

• On attribue à l'ingénieur mathématicien Héron d'Alexandrie (premier siècle après J-C) l'invention d'une **machine à distribuer de l'eau.**

Elle marchait en y introduisant des pièces de monnaie.

• Distributeurs automatiques de tabac dans les tavernes anglaises au XVII^{e} siècle.

Machines à café.

Distributeurs de paquets de bonbons, de sachets de gâteaux, de barres chocolatées.

Machines à distribuer des billets.

Parcmètres.

Bandits manchots des casinos.

Flippers dans les bars tabac.

• *V*élos et autos mis à disposition dans la rue.

L'idée :

Concevoir et fabriquer un système

qui travaille et fait des affaires tout seul.

Toujours mieux !

L'informatique vient d'inventer une version perfectionnée et plus pure de ces

« entreprises autonomes automatiques »

(qui n'étaient que partiellement autonomes et automatiques)

Ces descendants de la machine de Héron d'Alexandrie :

• sont **décentralisés** et ne sont pas nécessairement au service d'un propriétaire identifié.

• fonctionnent selon des procédures sans **limite de complexité**.

• peuvent **recevoir des informations** variées et en faire dépendre leur comportement.

• **possèdent, reçoivent** et **dépensent** de l'argent.

• sont quasiment **indestructibles** et **inviolables** car leur marche s'appuie sur des protections cryptographiques et sur la copie en multiple exemplaire de leur mémoire.

• une fois lancés, leur **autonomie** et leur **indépendance** sont totales.

Organisations autonomes décentralisées

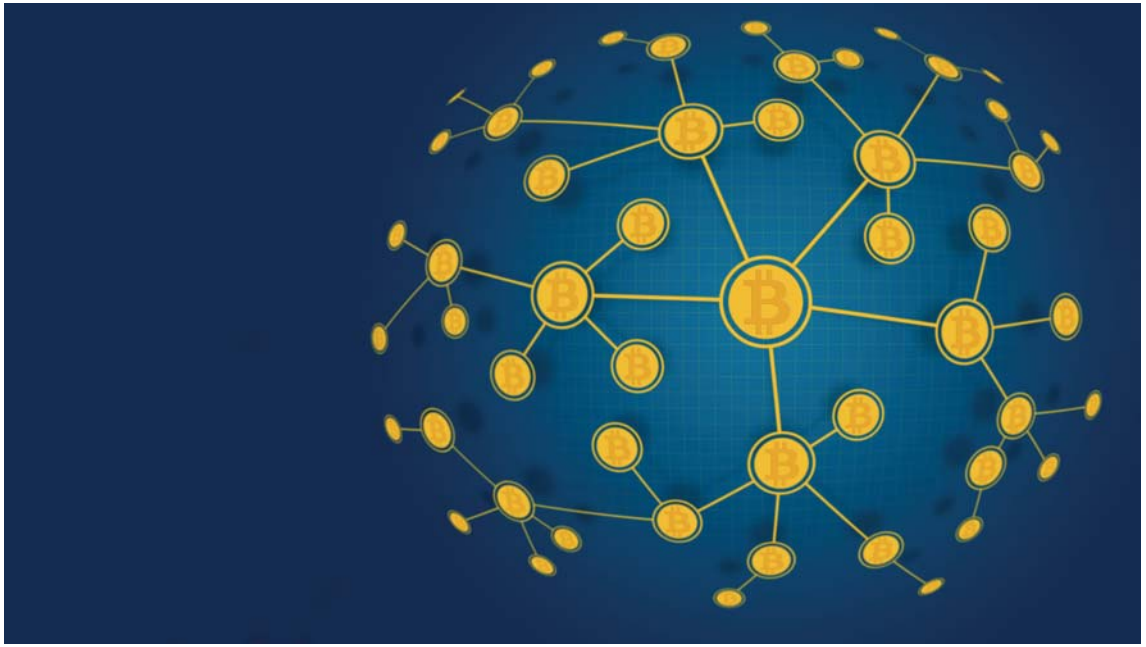
(Decentralised autonomous organisations)

ou

DAO

Dapps : *Decentralised Applications*

smart contract



World-computer ou **ordinateur-monde**

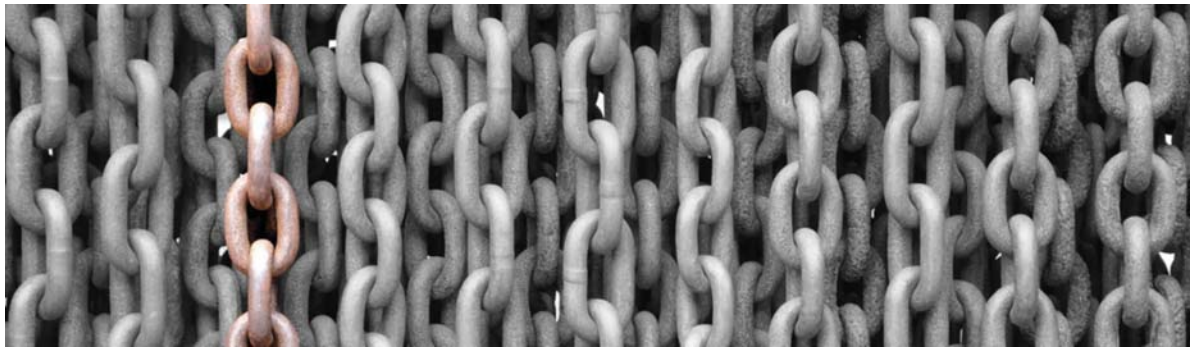
Origine : monnaies cryptographiques (donc le Bitcoin créé en 2009).

réseaux pair à pair

blockchains (chaînes de blocs)

Le fonctionnement en parallèle des programmes est une forme de gâchis.

Avec les puissances de calcul dont nous disposons, c'est sans grande importance si cela assure la sécurité de l'ensemble et rend possible des applications d'un type nouveau.



La blockchain

La mémoire de cet "ordinateur" est ce qu'on nomme la blockchain (ou chaîne de blocs).

C'est un fichier informatique présent en chaque nœud du réseau P2P.

Il évolue en parallèle sous la forme de multiples copies identiques.

On ne peut rien y effacer. On ajoute des pages périodiquement.

Qu'importe que certaines machines du réseau tombent en panne,

Les machines présentes continueront de faire fonctionner l'ordinateur-monde dont la **blockchain** poursuivra son évolution.

Elle sera toujours prête à se recopier sur les machines un moment défaillantes ou à s'installer sur des machines nouvelles rejoignant le réseau pour en augmenter encore la résilience.

Personne n'a le pouvoir d'effacer ou de manipuler cette **mémoire commune partagée**.

Cette blockchain est conçue d'une manière simple qui facilite sa mise à jour simultanée sur tous les ordinateurs de base :

- on ajoute des pages périodiquement et rien jamais n'y est effacé.

Ces **pages** ou **blocs** sont chaînés les uns aux autres ce qui assurent le repérage de toute modification des parties anciennes, et les empêchent.

Le Bitcoin, première DAO

Satoshi Nakamoto n'a peut-être pas compris en 2008 que ce qu'il venait d'inventer pour l'émission d'une monnaie sans autorité centrale d'émission et de régulation pouvait se généraliser.

Les opérations autorisées par l'ordinateur à blockchain du réseau Bitcoin ne sont (pour l'essentiel) que des opérations élémentaires de déplacement d'argent d'un compte vers un autre.

Ces **transactions** exécutées par le réseau Bitcoin déplacent de manière presque instantanée des sommes d'argent même élevée, qui passent sans quasiment aucun coût d'un point sur terre à un autre.

Un Bitcoin vaut environ 650 euros. **(651 euros le 14-11-2016)**

Leur valeur totale atteint **10 milliards d'euros environ.** **(10,4 milliard d'euros le 14-11-2016)**

La fiabilité de l'ordinateur-monde du Bitcoin, attestée par bientôt huit ans de bon fonctionnement, explique la confiance que les utilisateurs ont aujourd'hui dans cette monnaie originale.

Des opérations légèrement plus complexes que les simples transactions sont permises.

Le réseau des Bitcoins est une DAO car personne ne peut l'empêcher de fonctionner, et que sa blockchain est recopiée environ 5000 fois (novembre 2016).

Pour le détruire, il faudrait réussir à interrompre le réseau partout à la fois.

On a imaginé la perfectionner !

Ethereum, DAO et support à DAO

Premier projet d'envergure mis en place pour reprendre et généraliser l'idée de l'ordinateur à blockchain du Bitcoin : **Ethereum**.

C'est une DAO comme le réseau Bitcoin, mais surtout c'est

un outil pour créer facilement de nouvelles DAO.

Repères

• **Janvier 2009 :** La monnaie cryptographique bitcoin est lancée par la mise en fonctionnement du réseau bitcoin.

• **Fin 2013 :** Vitalik Buterin propose une description de projet Ethereum (white paper décembre 2013)

Gavin Wood a précisé le projet (yellow paper avril 2014)

• **Janvier 2014 :** Vitalik Buterin annonce le projet Ethereum et commence à y travailler avec une petite équipe de développeurs.

• **Juillet 2014 :** La fondation Ethereum vend pendant 42 jours des Ethers avant la mise en marche du réseau Ethereum. **Dix-huit millions de dollars** sont tirés de la vente. Ils correspondent à

60 millions d'Ethers.

12 millions d'Ether sont aussi distribués aux développeurs.

10 millions d'Ethers créés chaque année.

• **Juillet 2015 :** Une plateforme de test est rendue disponible.

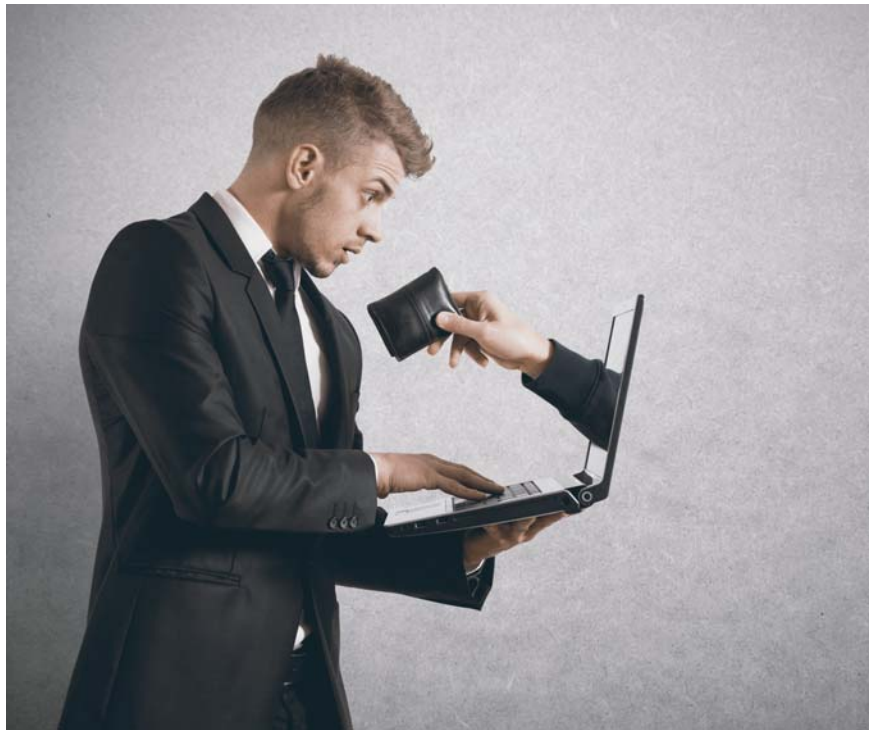
• **Le 30 juillet 2015 :** la blockchain d'Ethereum se met à fonctionner.

• **Janvier 2016** : Onze banques dont le Crédit Suisse et HSBC entreprennent des essais avec une plateforme de test d'Ethereum. Des *start-up* Ethereum naissent et lèvent des fonds.

• **Mars 2016 :** Les Ethers en circulation valent un milliard de dollars.

• **Mai 2016 :** Le programme THE DAO (qui est une DAO sur la blockchain d'Ethereum) collecte des fonds pour des investissements liés à Ethereum. 160 millions $ sont collectés.

- **Juin 2016 :** Le programme THE DAO est victime d'une attaque rendue possible par un bug. 50 millions de dollars sont déplacés mais restent bloqués.



• **Juillet 2016.** L'annulation de certaines opérations de la blockchain d'Ethereum (**hardfork**) mise en œuvre à la suite d'un vote des mineurs d'Ethereum règle partiellement le problème.

Le cours de l'éther est peu affecté par cette attaque qui n'a pas concernée directement le réseau Ethereum, mais seulement une DAO construite maladroitement sur lui.

• Certains nœuds du réseau refusent ce **hardfork** : dédoublement du réseau.

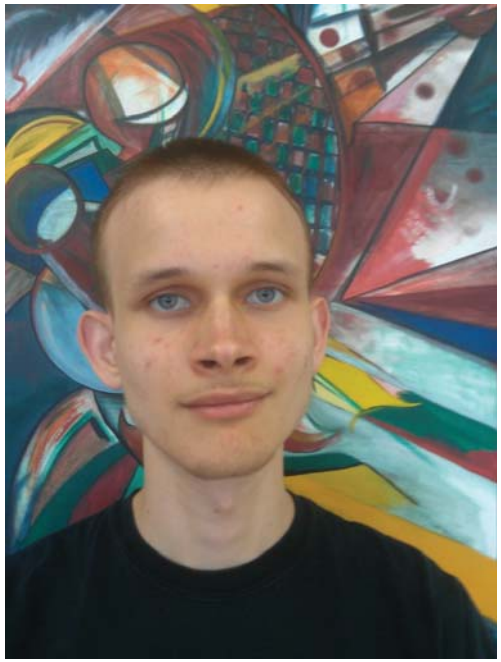
Il y a aujourd'hui le deux types d'Ether **ETH** et **ETC**

• **Octbre 2016.** Suite à une attaque par déni de service, un autre **hardfork** est opéré.

• **Novembre 2016.** Le minage des Ether s'est développé.
Aujourd'hui 4,7 TH/s ("terahash par seconde") = $4{,}7\ 10^{12}$ hash par seconde
(pour le Bitcoin c'est 2 000 PH/s = $2\ 10^{18}$ hash pas seconde)

#	Name	Market Cap	Price	Available Supply	Volume (24h)
1	Bitcoin	€10420692995	€652.26	15,976,404 BTC	€61975928
2	Ethereum	€796277377	€9.26	85,948,640 ETH	€4361730
3	Ripple	€269767520	€0.007543	35,765,131,899 XRP *	€1560484
4	Litecoin	€174018281	€3.59	48,433,879 LTC	€2774888
5	Monero	€97308747	€7.30	13,337,664 XMR	€5998962
6	Ethereum Classic	€71619930	€0.834138	85,861,043 ETC	€305290
7	Dash	€61239573	€8.90	6,882,425 DASH	€552638
8	Augur	€45981514	€4.18	11,000,000 REP *	€90547
9	NEM	€36759668	€0.004084	8,999,999,999 XEM *	€158977
10	Waves	€35973683	€0.359737	100,000,000 WAVES *	€101622
11	MaidSafeCoin	€33416562	€0.073840	452,552,412 MAID *	€109020

14 novembre 2016



Vitalik Buterin

Né à Moscou en 1994 — il a 22 ans — surdoué, il abandonne ses études à 20 ans

L'idée que Buterin est de faire fonctionner un **ordinateur à blockchain** comme celui du Bitcoin, mais sans en limiter les opérations de base. Il veut autoriser l'exécution de **programmes aussi généraux que possibles** écrits dans un langage de programmation qualifié de « **Turing complet** ».

Si Ethereum tient, il pourrait rattraper le **Bitcoin**.

Bien comprendre !

• Avec l'Open source : on peut vérifier les programmes (en particulier qu'ils ne font que ce qui est annoncé qu'ils font)

• Avec les DAO : on peut vérifier les programmes, et **EN PLUS** on est assuré qu'ils ne seront pas interrompus parce que cela arrange ceux qui les ont conçus où ceux qui contrôlent l'ordinateur qui exécute le programme.

• Écrire une DAO oblige à être transparent et oblige à s'engager.

• À terme, ce sera un moyen de créer de la sécurité de fonctionnement, particulièrement pour tout ce qui concerne des échanges et transferts de valeurs :

échanges monétaires ou commerciaux, paris, votes, engagements divers, assurances, etc.

Exemple de DAO construite sur la blockchain d'Ethereum.

• Une loterie de fête foraine est un mécanisme qui reçoit de l'argent des joueurs et qui, après un tirage au hasard avec une roue, prend l'argent des perdants et en donne aux gagnants.

• Les opérations consistant à recevoir de l'argent, à effectuer un tirage au hasard, à redistribuer certaines sommes aux gagnants, sont parfaitement automatisables.

• Il leur correspond un programme qu'on peut déposer sur la blockchain d'Ethereum et qui s'exécutera automatiquement quand des joueurs se présenteront.

• Le programmeur peut décider qu'une partie de l'argent misé lui reviendra.

• Cette commission — par exemple de 1% — se versera automatiquement sur un compte particulier dont seul le créateur du programme détiendra la clé.

Avantages d'une DAO de type loterie

- Pas besoin d'être au même endroit que la roue de la loterie pour jouer.

- Celui qui joue connaît de manière parfaitement précise le programme qui simule la loterie.

Il peut donc vérifier que le tirage au sort est équitable et que le calcul de la redistribution de l'argent misé est conforme à ce qui est annoncé.

Pas besoin donc de faire confiance à l'organisateur

qui ne peut rien cacher,

et qui ne contrôle pas l'ensemble des machines faisant fonctionner le programme.

- Après coup, tout le monde voit tous les déplacements d'argent qui ont été effectués.

Leurs traces restent présentes sur la blockchain permettant des analyses *a posteriori*.

- Autre avantage encore d'une loterie Ethereum :

On est certain qu'une fois en marche l'organisateur initial — celui qui l'a programmée — ne la modifiera pas, et n'interrompra pas son fonctionnement.

Garder les sommes misées et empêcher la distribution des gains est impossible.

Pas de filou qui part avec la caisse !

(a) Transparence : tout est public.

(b) Sûreté absolue (si aucun bug !?) :

l'ordinateur qui organise les tirages n'est pas une machine isolée aux mains d'un inconnu.

(c) Possibilité d'auditer et de vérifier l'équité et la correction du fonctionnement

dont tout le passé reste présent indéfiniment.

Satoshi Dice sur Ethereum

vDice (https://www.vdice.io) :

« There is the **software side** and **the gambling side**.

vDice is fully decentralized. it's a world first. it's a new paradigm.

The code, the logic, it's all on the p2p network.

As the games are on the network, we don't control them.

They are bits of software loaded onto the network.

Because of proof of work, we can't take them off. No one can.

So most of the work is software development, so there is a separate entity for that. »

vDice (https://www.vdice.io) :

Règles "Provably fair"

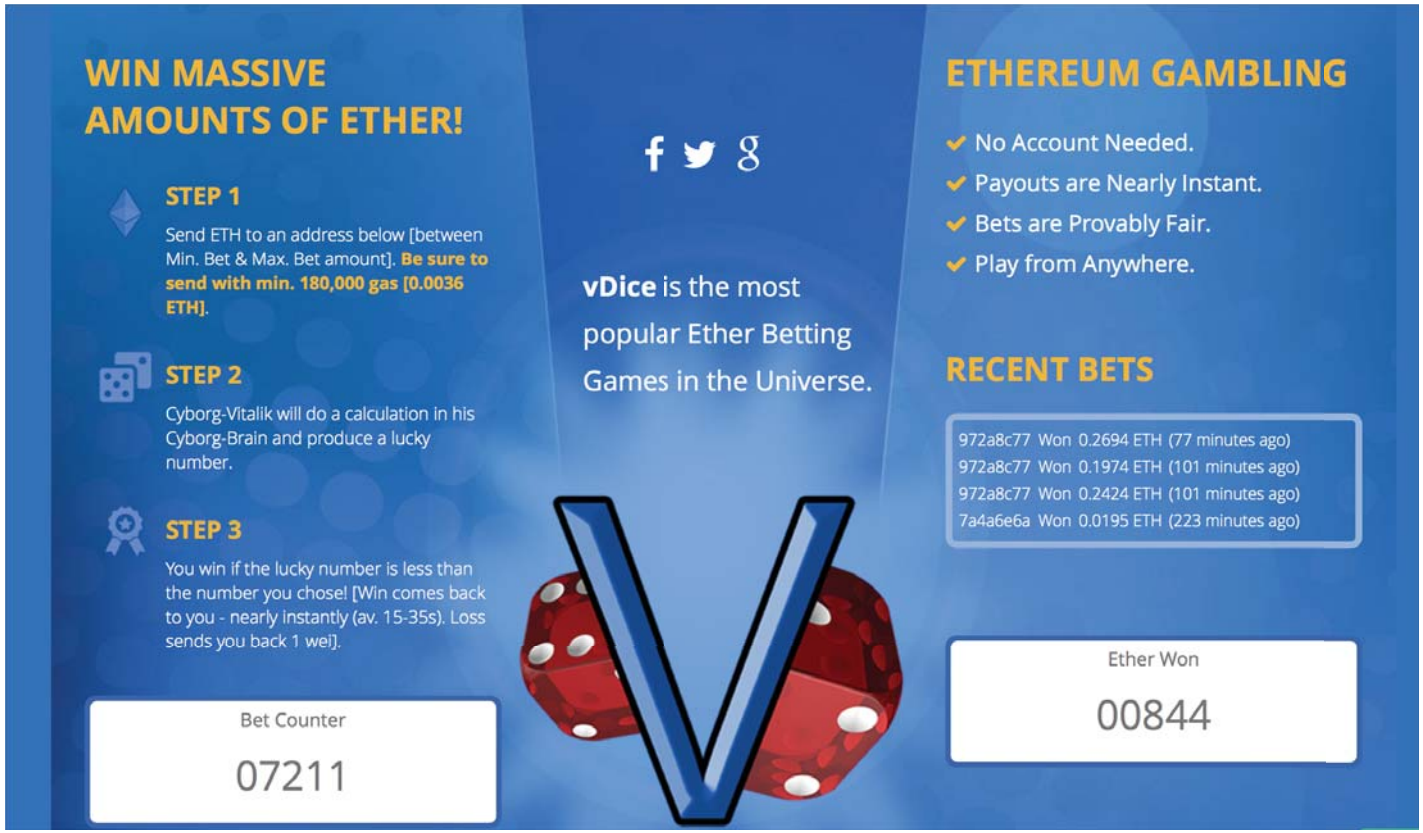
Copiée sur : **SatoshiDice** (https://en.bitcoin.it/wiki/Satoshi_Dice)

Random Number Generation

To determine if a wager is a winner or loser, the site uses a method to produce a number between 0 and 65 535, similar to how a random number generator (RNG) would be used. The service uses a combination of the transaction hash from the wager transaction from the blockchain and performs a 512-bit SHA2 hash for that transaction hash using a secret unknown to the player. The first four bytes of that hash become the lucky number in determining winner or loser.

Odds

Each wager address has different odds, and each gives the house an edge of 1.90%
The website shows the full list of wager addresses and odds.


WIN MASSIVE AMOUNTS OF ETHER!
STEP 1
Send ETH to an address below [between Min. Bet & Max. Bet amount]. Be sure to send with min. 180,000 gas [0.0036 ETH].
STEP 2
Cyborg-Vitalik will do a calculation in his Cyborg-Brain and produce a lucky number.
STEP 3
You win if the lucky number is less than the number you chose! [Win comes back to you - nearly instantly (av. 15-35s). Loss sends you back 1 wei].
Bet Counter
07211
vDice is the most popular Ether Betting Games in the Universe.
ETHEREUM GAMBLING
No Account Needed.
Payouts are Nearly Instant.
Bets are Provably Fair.
Play from Anywhere.
RECENT BETS
972a8c77 Won 0.2694 ETH (77 minutes ago)
972a8c77 Won 0.1974 ETH (101 minutes ago)
972a8c77 Won 0.2424 ETH (101 minutes ago)
7a4a6e6a Won 0.0195 ETH (223 minutes ago)
Ether Won
00844

Le mode de fonctionnement d'une DAO **crée de la confiance**,
même entre partenaires ne s'étant jamais rencontrés.

Sans le contrôle d'une autorité centrale et
sans avoir à faire appel à un **tiers de confiance**.

Le stockage multiple de la blockchain rassure mutuellement les acteurs.

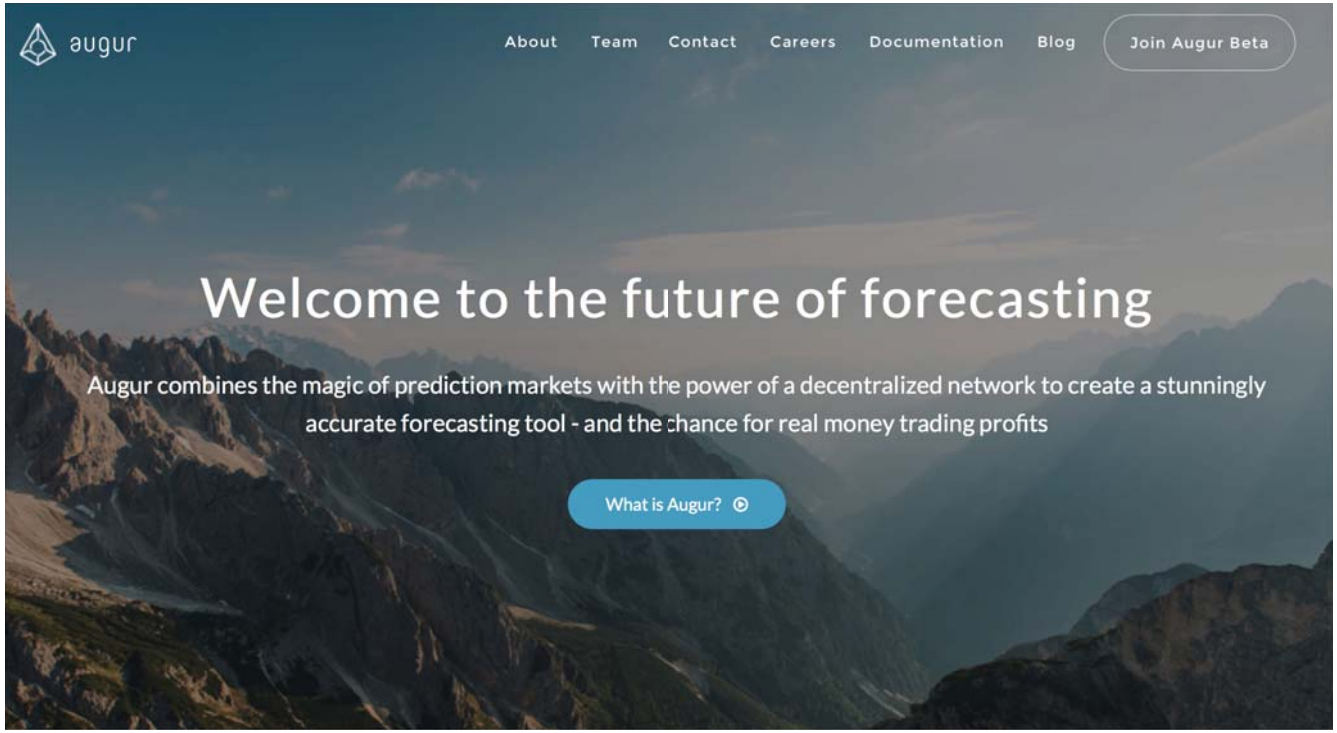
Une multitude d'applications où de l'argent circule entre les acteurs est rendue possible.

On a créé des systèmes gérant des **outils financiers** et des **engagements** divers.

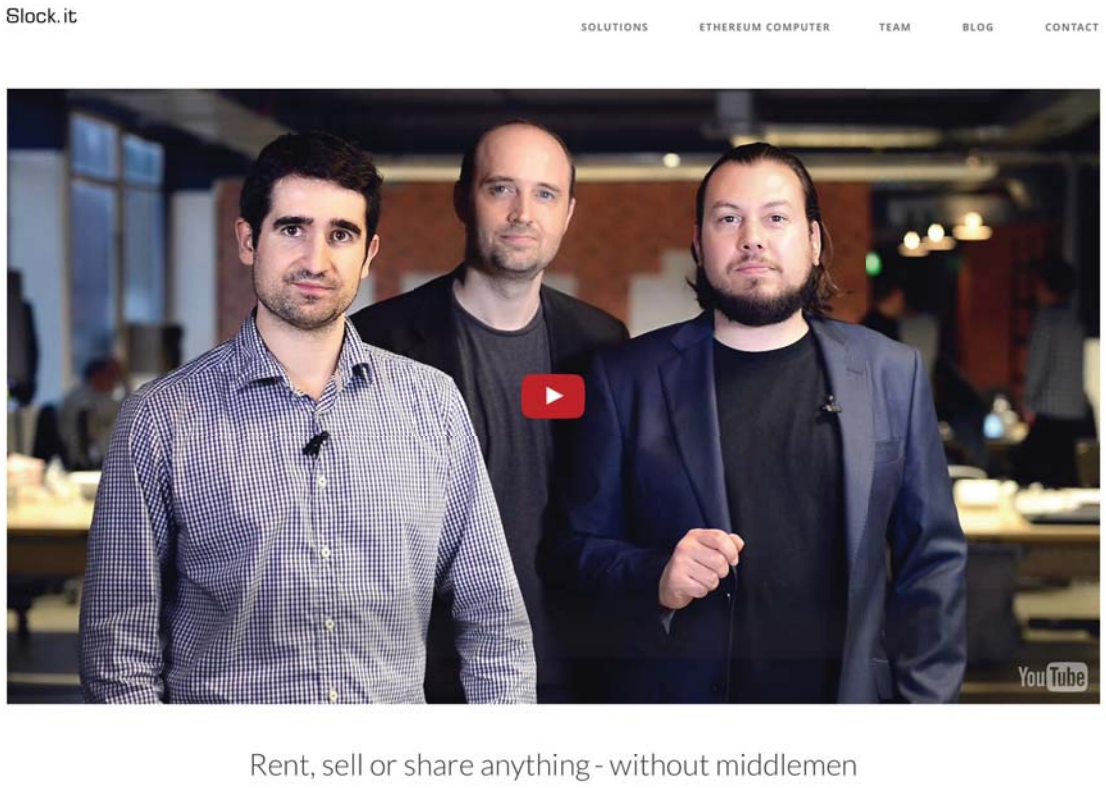
Des **monnaies cryptographiques** fondées sur Ethereum ont été créées
(en plus de l'Ether).

L'option offerte aux programmes d'aller rechercher des informations sur internet (oracle) et de faire dépendre leur comportement permet l'organisation de **paris sportifs** ou de toute nature.

Augur : Marché de la prédiction



Serrures connectées au réseau https://slock.it



Une fois la serrure installée à l'entrée de l'appartement que vous proposez à la location, tout se fera automatiquement.

Le locataire intéressé, paiera un mois de location, et obtiendra en échange un code lui permettant d'ouvrir la serrure de l'appartement.

Le code cessera d'être actif à l'issue du mois.

Le paiement de la location, le transfert vers votre compte de l'argent reçu, la détermination du code pour l'ouverture de la porte, sa mise en fonctionnement pendant un mois, tout cela sera géré par le programme mis sur la blockchain.

Personne ne pourra tricher avec ses engagements, ni le propriétaire, ni le locataire.

Ethereum : résistance aux attaques ?

Si l'utilisation des programmes n'exigeait aucune contrepartie, on pourrait y faire fonctionner un programme qui tourne indéfiniment et consomme la puissance des nœuds.

Sans un moyen de freiner cette consommation de puissance, on arriverait vite à saturation.

Il serait facile de mettre en panne le réseau.

Un mécanisme a été prévu qui interdit cela.

Lorsqu'on utilise un programme déposé sur la blockchain, il faut associer une certaine somme.

Cette somme est faible mais cruciale pour le bon fonctionnement du système.

Ces sommes dépensées par les utilisateur d'un programme sont aussi destinées à récompenser ceux des membres du réseau qui détiennent une copie de la blockchain et mènent les opérations qui en organisent l'évolution et le contrôle, les **mineurs**.

Le système des commissions

- empêche les programmes trop gourmands en puissance de tout faire s'effondrer,
- encourage les programmes économes en calcul,
- interdit les attaques par déni de service,
- et en même temps constitue une incitation à participer à la surveillance de la blockchain.

Les mineurs fixent un prix pour les opérations qu'ils exécutent sur la blockchain.

Si le prix que propose un utilisateur est trop faible, les opérations de ce programme attendent.

L'utilisateur d'un programme doit donc proposer une commission raisonnable.

Une sorte de marché s'établit.

Le système est fondé sur des idées économiques qui y jouent un rôle régulateur.

Les constructions informatiques modernes que sont les ordinateurs à blockchain ont en leur cœur même des **unités de valeur économique** qu'ils manipulent et sans lesquelles ils ne pourraient pas exister.

Une forme « **d'économie numérique fondamentale** » doit être maitrisée.

Les programmes déposés sur la blockchain sont eux-mêmes des acteurs économiques.

Limites et danger

La délicatesse et la fragilité de ces constructions, créent des risques et des difficultés dont il n'est pas certain aujourd'hui qu'on en maîtrise tous les aspects.

Cette informatique du futur est dans une phase expérimentale.

Elle n'exclut pas les accidents, voire les catastrophes.

Six points délicats

1

L'accroissement de la taille de la blockchain ne doit pas être sans limite, de même que la quantité de calcul exécutées par les mineurs d'un ordinateur à blockchain. Aujourd'hui plus de 30 GigaOctets

On espère profiter de loi de Moore.

Mais, un trop grand succès d'un ordinateur-monde provoquerait un problème d'encombrement.

2

Les **primitives cryptographiques** pour assurer l'intégrité de la blockchain, la signature des transactions, et le bon fonctionnement d'un réseau P2P ne sont pas sûres à 100%.

L'exploitation d'une faille dans l'un de ces composants pourrait tout mettre par terre.

Un soin particulier doit présider à leur choix.

Nécessité de prévoir des procédures efficaces de substitution.

On a déjà trouvé des failles dans le protocole P2P.

3

Les programmes même s'ils sont publics ne sont pas nécessairement sans erreurs.

Les bugs peuvent entraîner de graves disfonctionnements, voire autoriser un hacker ayant repéré l'un d'eux de s'emparer de l'argent stocké dans le compte d'une DAO.

C'est ce qui s'est produit le 17 juin 2016.

Exploitation d'une erreur dans le programme d'une DAO de la blockchain d'Ethereum.

4

La **gouvernance** d'un système comme celui d'Ethereum est délicate.

En théorie, il n'y en a pas besoin.

Seules les évolutions majeures du système sont effectuées à la suite du vote des mineurs qui détiennent collectivement une forme de pouvoir « démocratique » sur le système.

Le « hard-fork » de juillet 2016 est une opération de gouvernance réalisée suite à une sorte de vote.

Cependant en cas d'urgence, **une réaction rapide est parfois indispensable**.

Dilemme entre

- automaticité du système essentiel à la confiance

- réactivité, essentielle dans certaines situations.

5

Rien n'empêche une DAO d'avoir été conçue pour exploiter ses utilisateurs.

Il faut donc pouvoir exercer un certain contrôle sur les DAO créées ?

Comment l'organiser sans annuler les bénéfices des principes à la base des DAO ?

6

Dernier point :

Le **statut légal et juridique** des DAO est à concevoir et définir précisément.

Expérimentale aujourd'hui, cette nouvelle technologie réserve toutes sortes de surprises.

Elles seront bonnes et mauvaises.

Nous n'en avons pour l'instant qu'une idée très partielle !

Bitcoin vs Ethereum

A

- Le nombre total de **Bitcoins** qui seront émis est **21 millions**, leur émission va en décroissant : aujourd'hui **12,5 bitcoins** sont émis toutes les **10 minutes**.

- Les **Ethers** sont émis à raison de **5 Ethers** toutes les **12-15 secondes**, ce rythme restera inchangé.

Le nombre d'**Ethers** en circulation continuera de croître, mais le nombre d'Ethers émis par an sera de plus en plus faible comparé au nombre d'éthers déjà en circulation.

La pression d'inflation créée par les émissions tendra vers zéro.

B

- Le réseau **Bitcoin** ne peut qu'effectuer des transactions entre comptes :

  sa blockchain est une liste ordonnée de transactions.

- Le réseau **Ethereum** effectue des opérations plus complexes.

Sa blockchain contient des transactions et des programmes qui sont exécutés sans possibilité pour personne d'en prendre le contrôle ou de les arrêter.

Cela permet facilement la création d'Organisations autonomes décentralisées (DAO)

C

- La taille des pages de la blockchain du **Bitcoin** est limitée et exige un accord entre les mineurs pour évoluer, accord introuvable aujourd'hui.

- La taille des pages de la blockchain Ethereum n'est pas bornée.

D

- Le nombre de transactions par seconde que peut traiter le bitcoin est d'environ cinq ou sept.

- Pour Ethereum c'est environ trois fois plus.

E

- Le coût d'une transaction entre comptes bitcoin est en principe gratuit sauf qu'il faut accepter de payer une commission directement liée à la **taille de la transaction** pour qu'elle soit validée (cette obligation récente résulte du problème de la taille bornée des pages de la blockchain).

- Le coût d'une transaction pour l'Ether dépend **de sa complexité** et de l'utilisation qu'elle fait des ressources des machines qui font tourner les programmes.

F

- La valeur des Bitcoins émis est aujourd'hui (novembre 2016) dix fois supérieure à celle des éthers.

G

- Les équipes travaillant autour du Bitcoin sont plus nombreuses que celles travaillant pour l'Ether.

H

- Le procédé d'incitation à participer à la surveillance de la blockchain du **Bitcoin**, appelé « **preuve de travail** », a conduit au développement de puces spécialisées (ASIC) et à une compétition, jugée absurde, provoquant une dépense électrique considérable et une concentration des mineurs aujourd'hui majoritairement en Chine.

- Le procédé équivalent pour **Ethereum** ne permet pas le développement de puces spécialisées et évite donc plusieurs des inconvénients du bitcoin.

Preuve de travail : **Ethash** qui dissuade l'utilisation d'ASICs et de CPUs tandis qu'il encourage le mining décentralisée par des **GPU** (Graphics Processing Unit) isolées.


Bitcoin Charts
Zoom 1d 7d 1m 3m 1y YTD ALL
From Apr 28, 2013 To Nov 13, 2016
$15B
$10B
$5B
$0B
Market Cap
$1500
$1000
$500.00
$0.0
Price (USD)
24h Vol
0M
Jul '13
Jan '14
Jul '14
Jan '15
Jul '15
Jan '16
Jul '16
2014
2015
2016
Market Cap
Price (USD)
Price (BTC)
24h Vol
Highcharts.com


Ethereum Charts
Zoom 1d 7d 1m 3m 1y YTD ALL
From Aug 7, 2015 To Nov 13, 2016
$1 500M
$1 000M
$500M
$0M
Market Cap
24h Vol
0M
0.03000000 BTC
0.02000000 BTC
0.01000000 BTC
0.000 BTC
Price (BTC)
Sep '15
Nov '15
Jan '16
Mar '16
May '16
Jul '16
Sep '16
Nov '16
Oct '15
Jan '16
Apr '16
Jul '16
Oct '16
Market Cap
Price (USD)
Price (BTC)
24h Vol
Highcharts.com

Deux citations

Travis Patron :

• L'une des caractéristiques fondamentales de la société du XXIe siècle est que le rôle de l'employé est tenu par des machines aussi bien que par des humains. [...]

• Ethereum porte cette idée plus loin. Le rôle du client qui est actuellement réservé aux humains pourra tout aussi bien être tenu par des machines puisque le système des **Organisations autonomes décentralisées** permet des transactions entre elles sans nécessiter d'initiateur humain.

• **Ethereum** facilitera une économie de dispositifs interconnectés où les machines transmettent de l'argent et des données d'une manière sensiblement plus efficace que ne le font les humains.

• Les entreprises qui négligeront ces possibilités le paieront cher car elles n'utiliseront pas ces nouveaux systèmes de communication et d'action qui simplifient le monde ancien en éliminant les **tiers inutiles**.

• Dans un monde d'affaires où les entreprises fonctionnent de manière autonome, **l'argent classique laissera sa place à l'argent numérique** du type Bitcoin ou Ether.

• Le consommateur attend aujourd'hui des **modes de paiement mondiaux instantanés et sans friction**.

• Les progrès des crypto-monnaies et des DAO permettront à l'argent de se déplacer à une vitesse conforme à l'idéal attendu pour une bonne conduite des affaires aussi preste que la pensée. »

Ari Juels, Ahmed Kosba, Elaine Shi.

• L'ensemble des propriétés des DAO a un côté sombre : **elles facilitent le crime.**

(a) Les échanges équitables qu'elles rendent possibles des transactions entre parties criminelles mutuellement méfiantes [...]

(b) Les interactions réduites entre acteurs rendent les activités illégales plus difficiles à surveiller.

(c) Un criminel peut créer une DAO et disparaître, la laissant s'exécuter de façon autonome à son profit.

Conclusion

Une belle idée et un beau début de mise en œuvre !

Un nouveau type de transparence et de robustesse pour des applications informatiques.
Donc : **une meilleure sécurité rendue possible**.

L'opportunité (en théorie) de créer de larges réseaux de confiance mutuelle
et de liens forts de solidarité entre utilisateurs.

Une révolution ?

Le vocabulaire

- **Réseau pair à pair** : système d'échanges de messages entre ordinateurs connectés entre eux et leur permettant d'émettre et de recevoir des informations sur un pied d'égalité.

- **Blockchain (chaîne de blocs)** : fichier partagé sur un réseau pair à pair où, par exemple, est inscrite la totalité des transactions entre les comptes. La blockchain évolue uniquement par ajout périodique de pages ou blocs.

- **Ordinateur à blockchain ou ordinateur-monde** : l'ensemble des ordinateurs d'un réseau pair à pair partageant une blockchain sur laquelle sont présents des programmes avec les informations sur l'état de leurs calculs.

Une sorte d'ordinateur virtuel délocalisé et indestructible où chaque machine du réseau contrôle tous les autres et est contrôlé par eux. Pannes et les fraudes rendues presque impossibles.

- **Monnaie cryptographique** : monnaie créée par un ordinateur à blockchain lorsque la blockchain contient des informations sur les comptes des utilisateurs et sur les transactions faites entre comptes.

La plus importante (dix milliard d'euros) est le **Bitcoin**.

La seconde est l'éther (un milliard d'euros) du réseau **Ethereum.**

- **Smart-contract ou contrat intelligent** : programme d'un ordinateur à blockchain.

Terme est à éviter car ces programmes exécutés par chacun des ordinateurs du réseau ne sont en rien des contrats au sens juridique.

- **Transaction, clé privée, clé publique** : si un ordinateur à blockchain gère des transactions, celles-ci s'opèrent entre comptes, chacun possédant deux clés. La première assimilable à un numéro de compte est publique. La seconde, privée, permet à celui qui la connaît (celui qui a créé le compte) d'agir sur le compte. Les transactions faites par un détenteur de compte sont vues par tous et peuvent grâce à la clef publique être contrôlées et validées par tous.

- **Organisation autonome décentralisée (DAO)**. Programme fonctionnant grâce à un réseau pair à pair, qu'il est impossible d'arrêter.

Sa fiabilité et les protections cryptographiques dont il bénéficie crée de la confiance entre personnes utilisant le programme.

Le système du Bitcoin et celui d'Ethereum sont des DAO.

Les programmes déposés sur la blockchain d'Ethereum (sauf s'ils sont trop simples) aussi.

Bibliographie

• Ethereum Project, consulté en juillet 2016 : https://www.ethereum.org

• Ethereum France, consulté en juillet 2016 : https://www.ethereum-france.com

• CoinDesk : Understanding Ehtereum, 2016.

• Joon Ian Won, Ian Car, Everything you need to know about the Ethereum “hard fork”, 2016 : http://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/

• Morgen Peck, The Uncanny Mind That Built Ethereum : Vitalik Buterin, 2016 : https://backchannel.com/the-uncanny-mind-that-built-ethereum-9b448dc9d14f#.v9srx7ntc

• Ari Juels, Ahmed Kosba, Elaine Shi, The ring of gyges: Using smart contracts for crime. *Aries* 40: 54, 2015.

• Jean-Paul Delahaye, Les blockchains, clefs d'un nouveau monde, Pour la science, mars 2015, pp. 80-85.

• Ahmed Kosba, Andrew Miller, Charalampos Papamanthou, Elaine Shi, Zikai Wen, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, 2015 : https:// eprint.iacr.org/2015/675.pdf.

• Gavin Wood, Ethereum, A secure decentralised generalised transaction ledger. *Ethereum Project, Yellow Paper*, 2014.

• Jean-Paul Delahaye, Du bitcoin à Ethereum : l’ordinateur-monde, *Pour la science*, novembre 2016, pp. 104-109.