

La blockchain

David Teruzzi

fondateur blockchain-conseil.fr

blogueur : blogchaincafe.com

chroniqueur blockchain pour [***BLOCKCHAIN DAILY NEWS***](#) / [***FINYEAR***](#)





www.blockchain-conseil.fr



IPFS et la décentralisation du WEB



microaens

Il y a eu dans le passé de nombreuses tentatives d'implémentation

Recherche...

AUTEUR

David TERUZZI

- * Consultant blockchain
- * Co-fondateur de blockchain-conseil.fr
- * Développeur affilié du projet [DECRED](#)
- * Chroniqueur blockchain pour FINYEAR

www.blogchaincafe.com

Qu'est-ce qu'une BLOCKCHAIN ?



« LA BLOCKCHAIN EST AUSSI RÉVOLUTIONNAIRE QUE L'ARRIVÉE D'INTERNET »

1179

52

19

f J'aime

Tweeter

in Share

PROPOS RECUEILLIS PAR LA RÉDACTION LES CLÉS DE DEMAIN - 18 AVRIL 2016



Primavera De Filippi

Primavera de Filippi est chercheuse rattachée au Cersa (Centre d'études et de recherche en sciences administratives et politiques), une unité mixte du CNRS et de l'université Paris-II...

La blockchain, un registre numérique de transactions inaltérable et décentralisé, a été inventée en même temps que la crypto-monnaie bitcoin afin d'éviter les fraudes. Mais il s'avère que cette technologie possède d'autres applications intéressantes pour des secteurs comme l'Internet des objets ou la finance. Primavera De Filippi, chercheuse au Cersa et à l'université d'Harvard, analyse son impact sur les entreprises et l'économie.

"La blockchain est en passe de devenir la cinquième grande technologie de rupture après les mainframes, les PCs, Internet et les réseaux sociaux mobiles."

- *Melanie Swan, founder of the Institute for Blockchain Studies* -

Fortune a dit que bitcoin est le **napster** pour la finance:

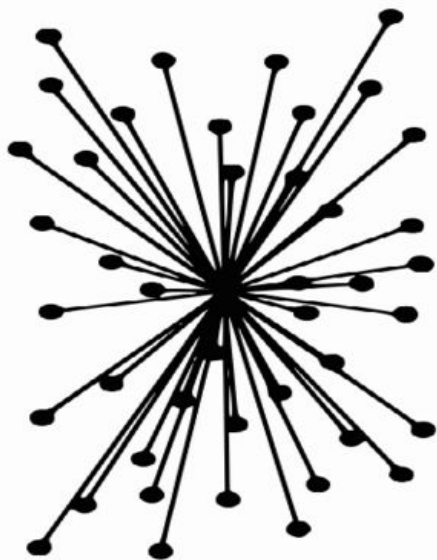
"À long terme, la finance blockchain va faire aux banques ce que le partage de fichiers p-2-p a fait à l'industrie de la musique"

"La blockchain est une technologie de rupture tout comme l'ont été le moteur à vapeur et à combustion."

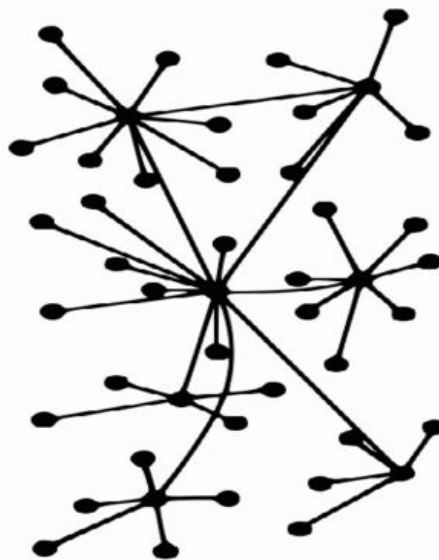
- *BNP Paribas, juillet 2015* -

"Je demeure convaincu que la technologie Blockchain sera aussi importante pour le monde que l'invention de l'imprimerie par Gutenberg"

- *Nicolas Cary, cofondateur de Blockchain.info* -

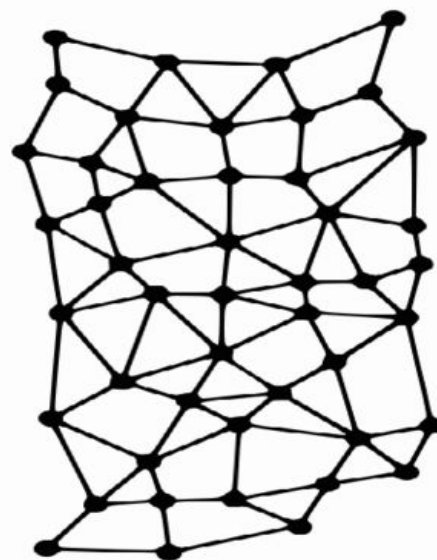


Centralized



Decentralized

Internet /  Facebook



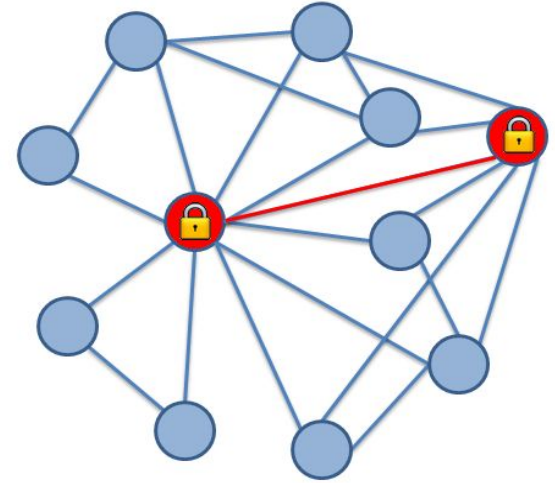
Distributed



types de réseaux



1996



PROTOCOLE SSL

=>

naissance de l'e-commerce

SSL = (1/1000ème du potentiel BC)

BC est aussi un protocole qui de plus va toucher tous les domaines (contrairement à SSL)

HTTP

built on top of

TCP/IP

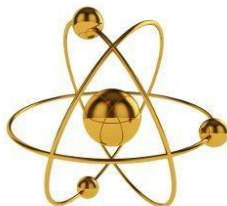
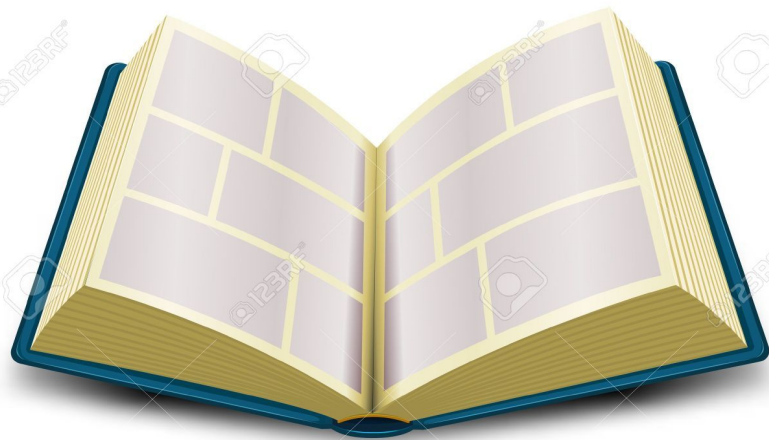
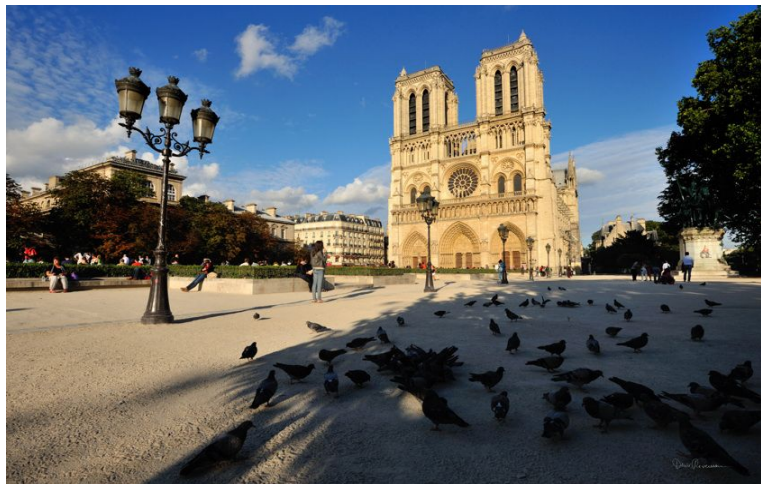
BITCOIN / ETHEREUM

built on top of

BLOCKCHAIN

PROTOCOLS

- Base de données accessible librement sur internet, sans contrôle central
- Hébergée et mise à jour par des milliers de noeuds qui empêchent toute modification irrégulière des données.
- Les données sont publiques mais anonymes, protégés par les clés privées
- La Blockchain est résistante à toute forme de censure ou de détournement: pour la première fois l'informatique a une source indépendante et infalsifiable de vérité.
- La Blockchain permet de construire des applications jusque là impensables, sans autorité centrale.



Une technologie peer-to-peer qui permet à des gens
qui ne se connaissent pas d'interagir en toute confiance.



+



règles vérifiées



protocole inaltérable



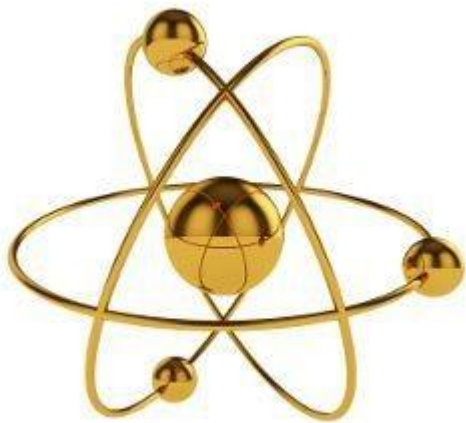
données indélébiles

**La BC fournit un cadre “juridique” décentralisé où le consensus
majoritaire des acteurs p-2-p est par convention la vérité.**

Les échanges sont possibles sans intermédiaires.

les crypto monnaies

Pourquoi l'or est digne de confiance ?

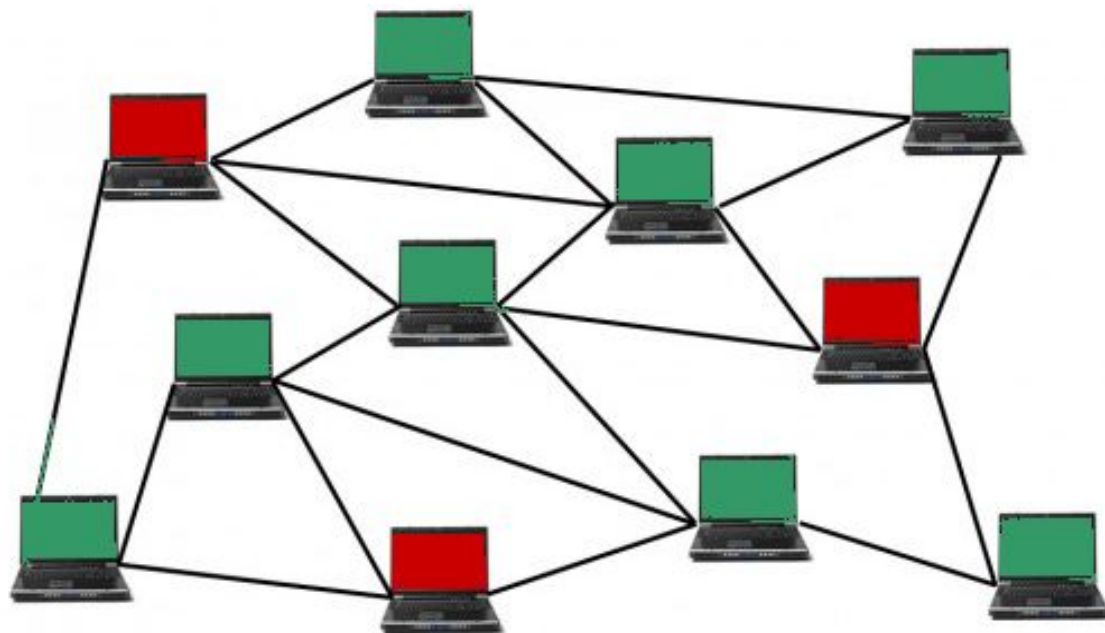


Parce qu'une loi mathématique lie 79 protons dans son atome et que jusqu'ici l'alchimie ne nous a pas permis de renverser cette relation.

Il en va de même pour les crypto monnaies.

(n = nombre atomes dans l'univers, 100 ans de calculs => pas de forcing)

Les ingrédients



 **noeud honnête**  **pirate**

- un réseau PEER 2 PEER
- un protocole de règles
- un CONSENSUS par vote majoritaire
- un système de rémunération des noeuds qui valident



Deux personnes
s'accordent sur
une transaction.



la blockchain valide et encrypte la transaction par consensus.

The diagram illustrates a sequence of three Bitcoin blocks, each containing a set of transactions. The blocks are labeled Block 52, Block 53, and Block 54. Each block has a 'Proof of work' hash, a 'Previous block' hash, and a list of transactions. Arrows indicate the flow of transactions from Block 52 to Block 53 and from Block 53 to Block 54.

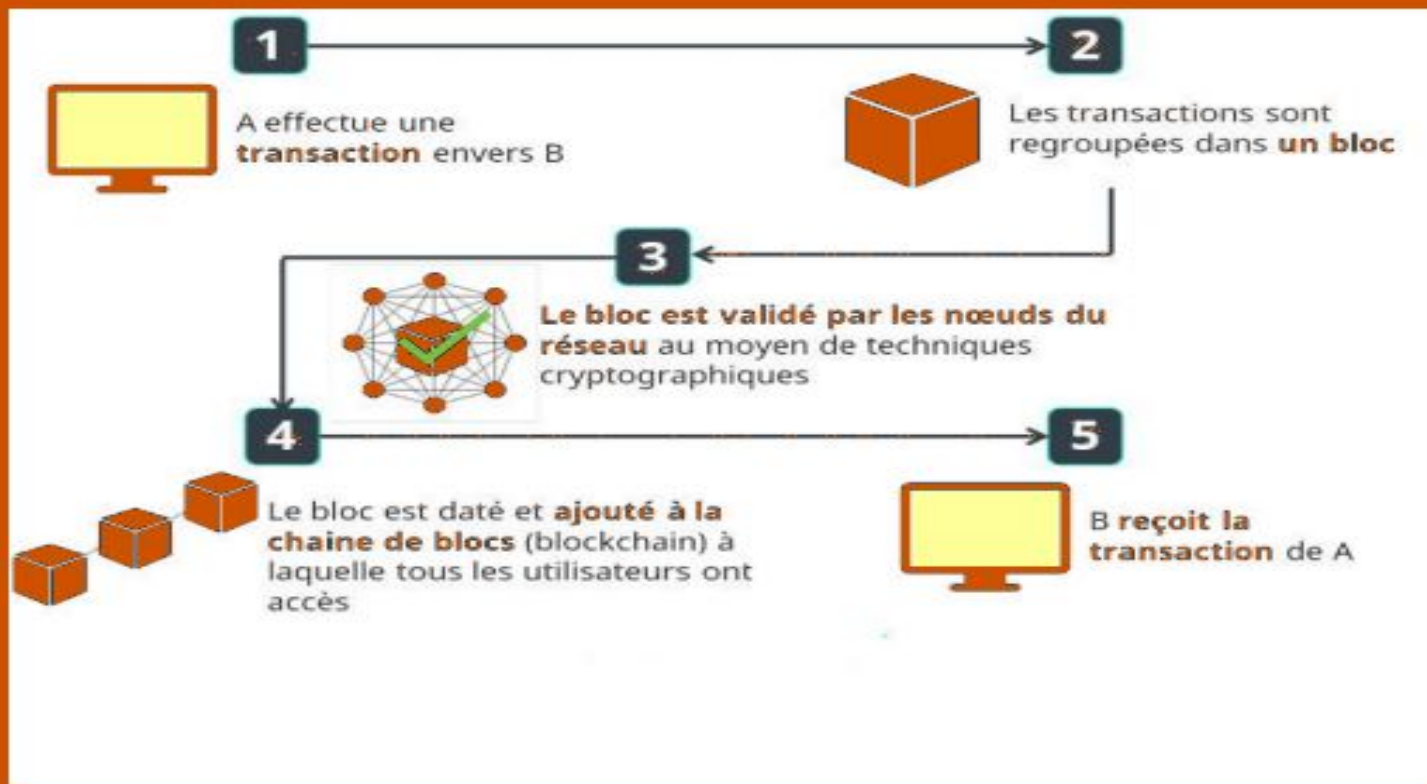
Block 52	Block 53	Block 54
Proof of work: 000002a9e9c5	Proof of work: 000000bada15	Proof of work: 000000c9a9e9
Previous block: 00000088f7ee	Previous block: 000000a9c075	Previous block: 000000bada15
Transaction: a5f931f0	Transaction: 94fca74	Transaction: 2585a15
Transaction: 2f8b807	Transaction: 68b7e93	Transaction: b7a4d00
Transaction: 3f46d05	Transaction: 34d48fa	Alice -> Bob

On l'inscrit dans le
dernier bloc de la blockchain

The diagram illustrates a network topology. At the top center is a server icon. Below it, there are several client computer icons (monitors with towers). These clients are interconnected in a mesh-like fashion, with many lines connecting them to each other and to the central server. Red arrows indicate the direction of data flow, showing a complex, multi-path network structure.

Le nouvel état est repliqué dans tous les noeuds du réseau.

Bitcoin | transactions (dessin)



Block 52

Proof of work:
000000zzxvzx5

Previous block:
0000009857vvv

Transacton
dd5g31bm

Transacton
22qsx987

Transacton
001hk009

Block 53

Proof of work:
00000090b41bx

Previous block:
000000zzxvzx5

Transacton
94lxcv14

Transacton
abb7bxxq

Transacton
34oiu98a

Block 54

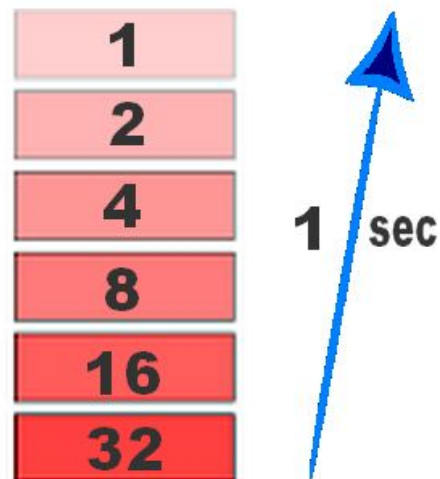
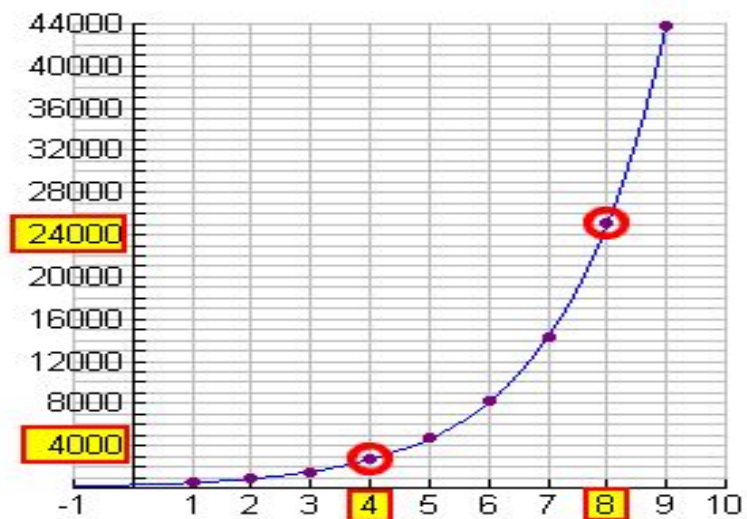
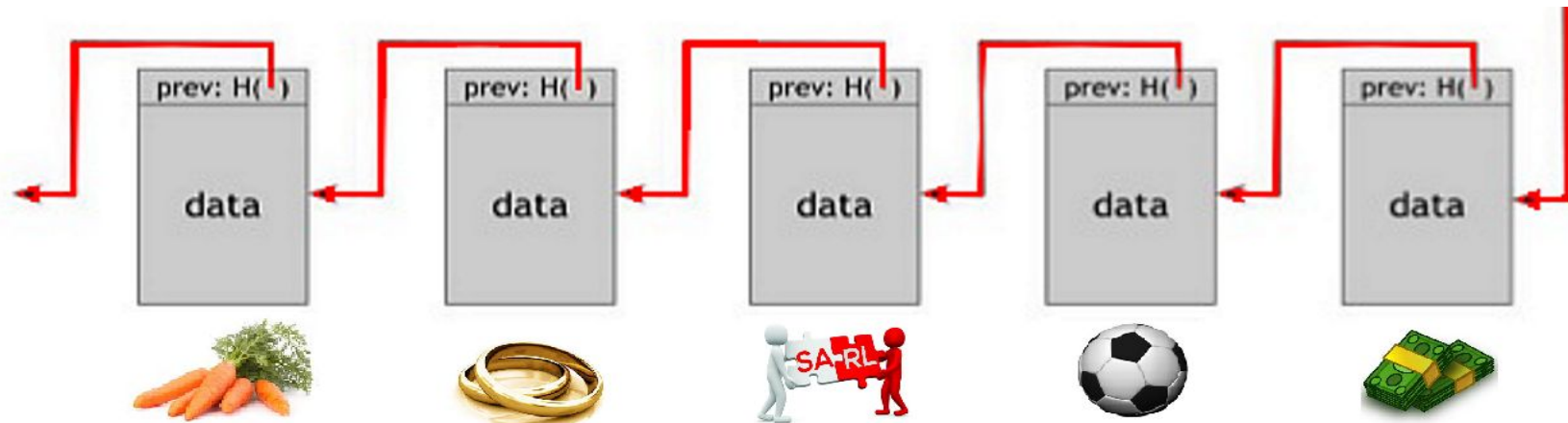
Proof of work:
000000jll93xq49

Previous block:
00000090b41bx

Transacton
555l bj4j12

Transacton
bn24xa0201

Transacton
555lba0201



Bitcoin et Ethereum



VS



ethereum

le bitcoin sait faire une seule chose:

le transfert d'argent



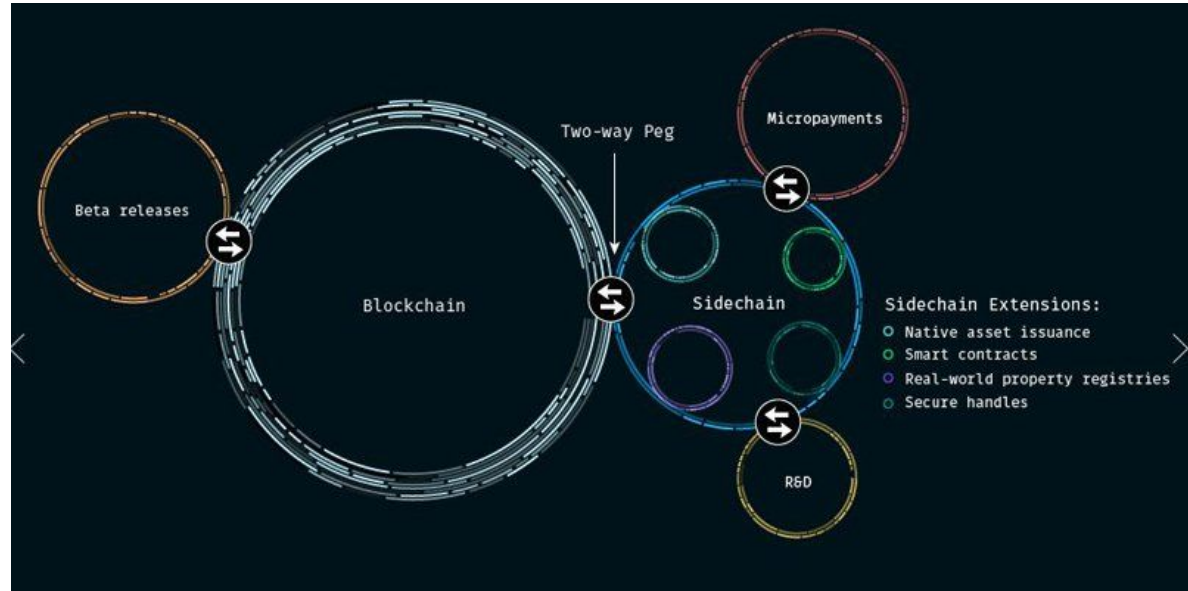
mais il le fait très bien

Le bitcoin s'étend aux *smart contracts* ...

Sidechains = extensions qui boostent les possibilités limitées de la blockchain bitcoin

trading -> Bitstamp,
Kraken, Poloniex...

dev -> Mastercoin,
Counterparty...





Counterparty



stratumn



BITSTAMP





L'intuition géniale de Vitalik Buterin:

une seule blockchain qui intègre un langage de programmation

Contrairement à la blockchain du bitcoin, Ethereum intègre un langage de programmation Turing-complet qui permet d'**exposer des méthodes** qui sont **appelées dynamiquement par d'autres** contrats ou par des agents externes.

Contracts

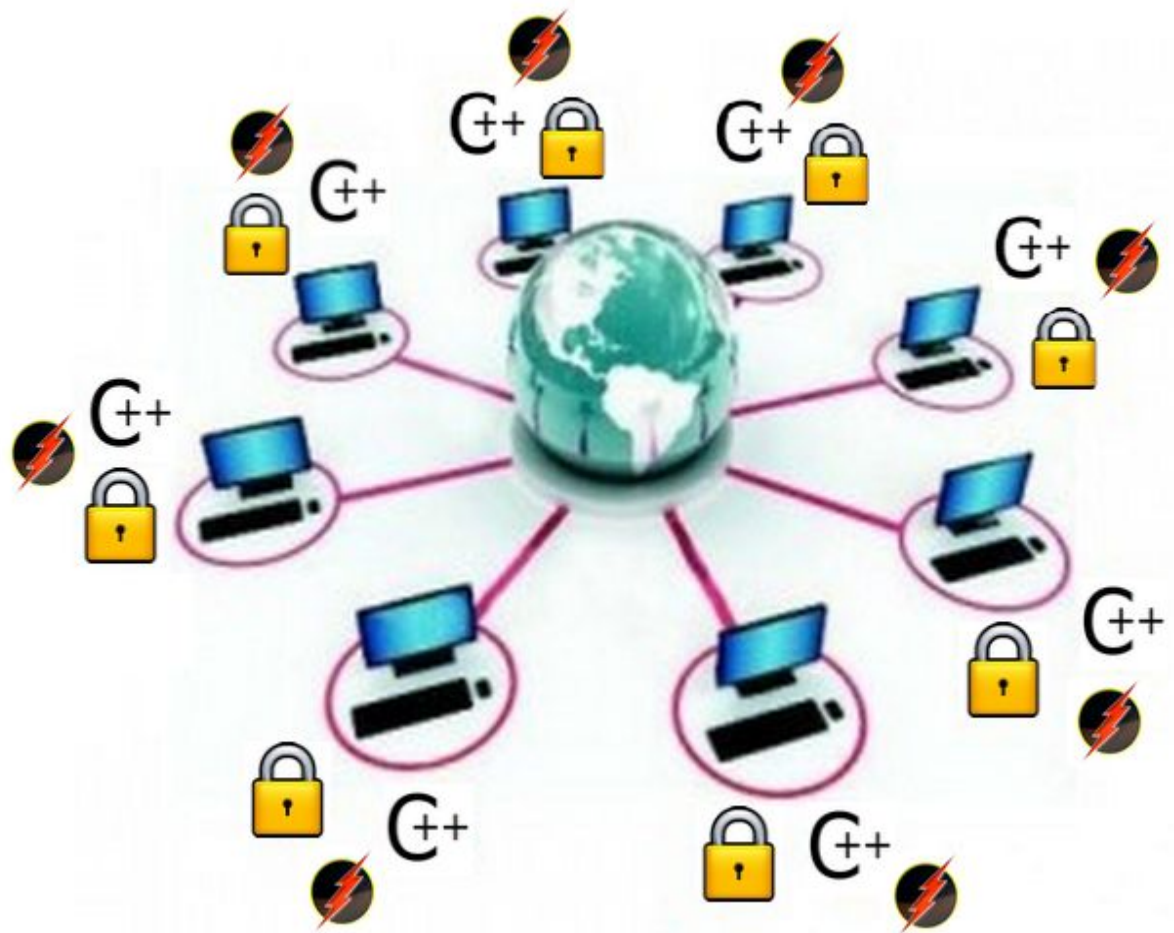
- Idea: when a message is sent to a contract, code executes
- Code can:
 - Read/write storage
 - Send ether
 - Send other messages

Bitcoin

Programmable
money

Ethereum

Programmable
peer-2-peer
event-driven
platform



Smart Contracts

et

aspects juridiques

“CommonAccord is an open, collective and international effort for the standardization of law”



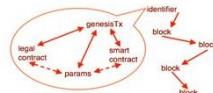
CommonAccord.Org

Overview:

- CommonAccord is an initiative to create global codes of legal transacting by codifying and automating legal documents, including contracts, permits, organizational documents, and consents. We anticipate that there will be codes for each jurisdiction, in each language. For international dealings and coordination, there will be at least one "global" code. [Center for Collaborative Law](#)
- Codification of legal form documents makes them transparent and continuously improving. It is part of the tradition of legal codification - from Hammurabi through Napoleon, the UCC, the ALI, and Creative Commons. Codification demystifies law and encourages [transparency and autonomy](#).
- We "code-ify" them by treating them like software source code - files in folders shared on GitHub. Code-ifying is neither hard nor complicated. The infrastructure is robust, widely-used, and free. The form documents will converge into legal codes of transacting.
- The legal code is part of a "distributed data model" for transacting. Each participant has their own files stating their legal relationships and transaction histories with each of their partners. The files are private, under their control, shared and handled exactly as they want. In this respect, it is like conventional, custom legal documents done in word-processing by lawyers.
- Participants transact by synchronizing files with partners. Synchronization can be done by git, blockchain, or any other method that the parties find satisfactory (even email). [Blockchain is a particularly important fit](#). Blockchain "smart contracts" can automate routine transaction functions while the legal text provides a frame for legal enforceability.
- All of the text, and the little bit of code that brings it together, is on [GitHub](#).
- This website uses a parser done by [Primavera De Filippi](#) of Harvard's Berkman Center. It supports a "DRY" [peer-to-peer transaction model](#), including with [blockchain](#) and [UMA \(pdf\)](#). There can be [close coupling of "smart contracts" and contract text](#), enabling "Ricardian" contracts. A taste of the "experience" can be seen in this [YouTube video](#). The vision was articulated in an [OSCON interview with Slashdot](#). The files can also be expressed as [JSON](#) or as [graphs](#).
- We are working toward a "Center for Collaborative Law," a trustee for global legal code. The project is open source. You can contribute: as a lawyer to legal documents, as a coder to our software, as a platform by interfacing with our materials, as a business by using the system, as a benefactor by supporting the effort. [Contribute on GitHub](#) or [email commonaccord@gmail.com](#).

Some Links:

Unchaining the chain



[join commonaccord.slack.com](#)

Tweets by @CommonAccord



Latest Activity on GitHub

[Top level](#) folder of files.
[Subject Index](#) of (some) materials.
[Recent Work](#)

Les applications

(DAPP)

Gartner Hype Cycle

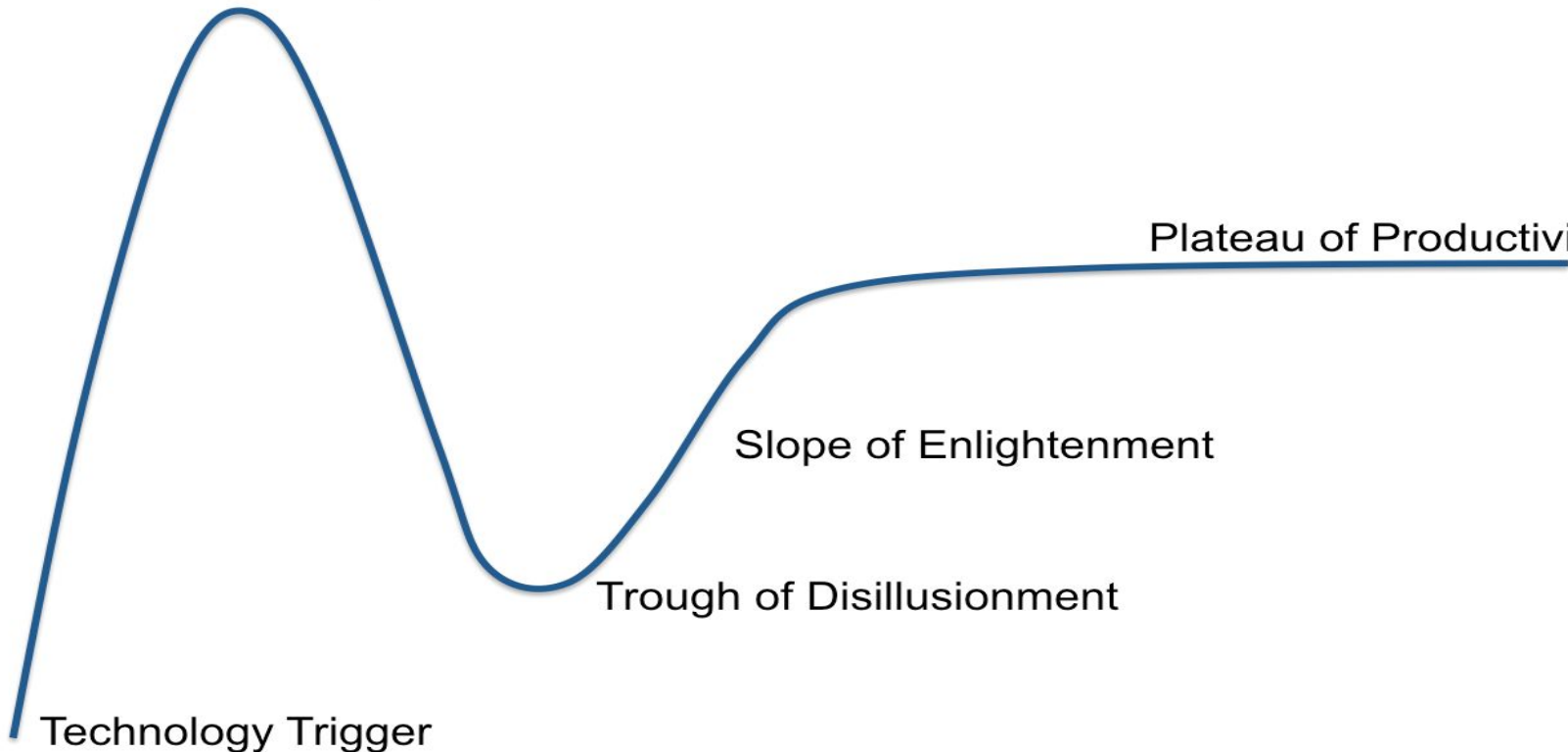
Peak of Inflated Expectations

Plateau of Productivity

Slope of Enlightenment

Trough of Disillusionment

Technology Trigger



L'adoption de la blockchain

1. par les montants que les gros dépensent **HyperLedger**, **R3**, **Wall Street**
2. par la pré-adoption (en 2015) de la part des grands acteurs

IMB “We are all in on BC”

Microsoft: “We want all blockchains on our platform” + **Red Hat**

Samsung + **Overstock** + **Amazon** + **bank UBS** + **30 autres**

Philips BC lab

SEB to Build Blockchain Channel Between New York and Stockholm

Pete Rizzo (@pete_rizzo_) | Published on November 7, 2016 at 12:20 GMT

NEWS



198



74



1



HIER

06/09/2016

Les blockchain et Microsoft

**MIT
Technology
Review**

Business

Microsoft Bets That Bitcoin-Style Blockchains Will Be Big Business

Giant banks are experimenting with software inspired by Bitcoin, and Microsoft wants a piece of the action.

by Tom Simonite January 22, 2016

 **CoinDesk**

TRENDING
Cast your vote in the
Blockchain Awards

BITCOIN PRICE INDEX (24H)
\$417
\$415
\$414

NEWS ▾ PRICE & DATA ▾ GUIDES ▾ EVENTS ▾ RESEARCH ▾ PRESS RELEASES ▾ CONSENSUS ▾

FEATURES • INTERVIEWS

Why Microsoft Wants 'Every Blockchain' on its Azure Platform

Pete Rizzo (@pete_rizzo_) | Published on February 9, 2016 at 11:17 BST

607

328

28

484

5





The blockchain is one of the eight top technology trends to watch out for in 2016 ...

... they “will disrupt entire industries”.



Today: International Payments Require a Relay Process



Low-Volume High-Value Slow Batch Payments

TECH FUTURE OF WORK

Ripple Just Raised \$55 Million
and Signed on These Major Bank
Partners

Septembre 2016

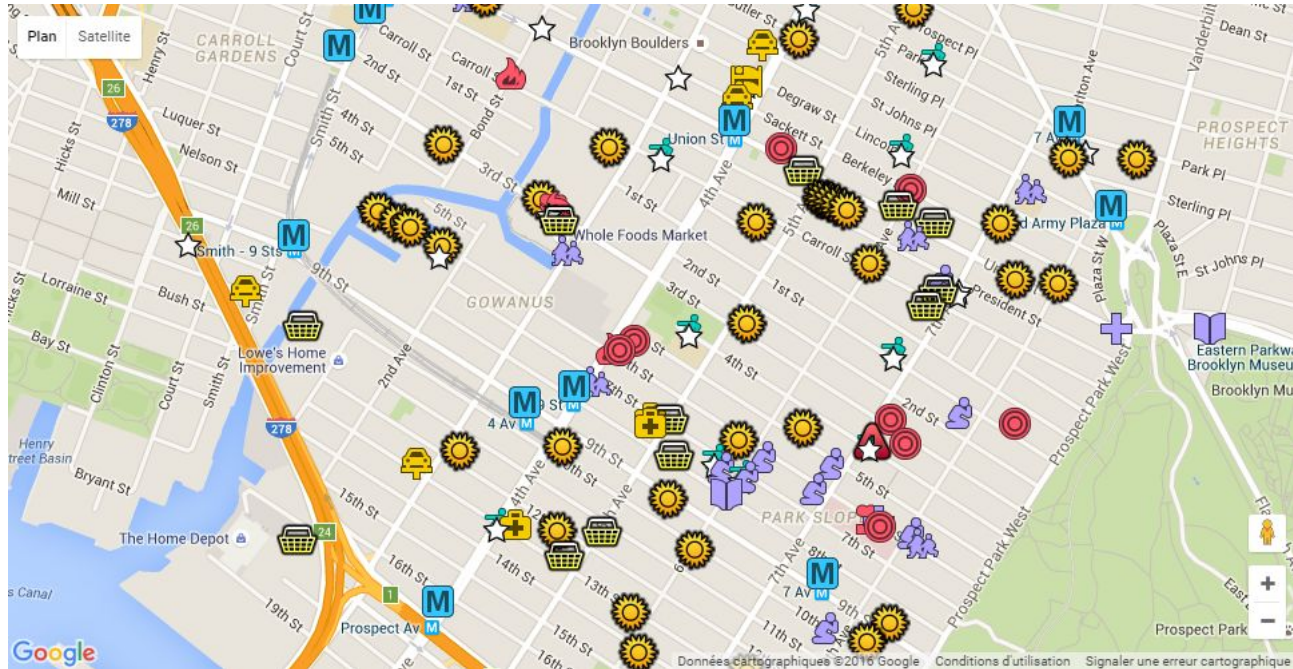
Ripple: Real-Time Payments with No Settlement Risk



High-Volume Low-Value Real-Time Individual Payments



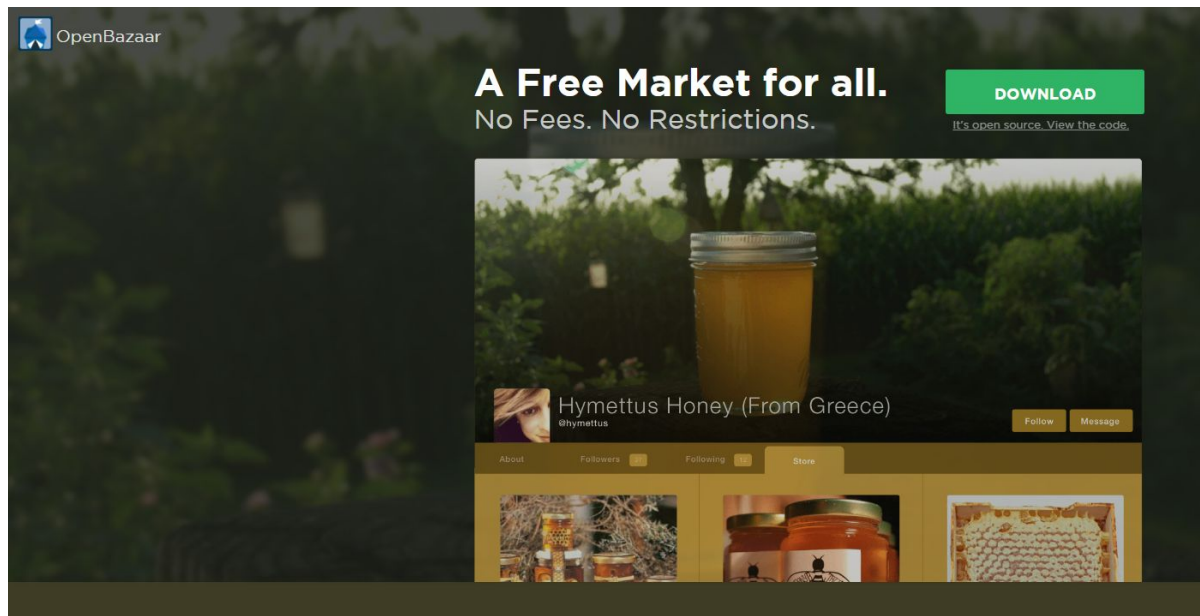
BROOKLYN MICROGRID



For Business

Whether you run a farm in Peru or a boutique in Soho, your products have a story to tell. Provenance provides you the digital tools to build trust and loyalty with technology-powered transparency.

OpenBazaar



- Openbazaar : le commerce à portée de tous
- eBay rencontre BitTorrent

STEEMIT



STEEM



DECENT



DC
DECENT



DC
DECENT



HOME

SERVICES

PUBLIC NOTARY

CITIZENS

EMBASSIES & CONSULATES

ALLIES



HOME

SERVICES

PUBLIC NOTARY

CITIZENS

EMBASSIES & CONSULATES

ALLIES

EVENTS

RESOURCES

LOGIN

JOIN



BITNATION

JOIN

Blockchains Publiques vs Privées

et la question de l'interopérabilité