

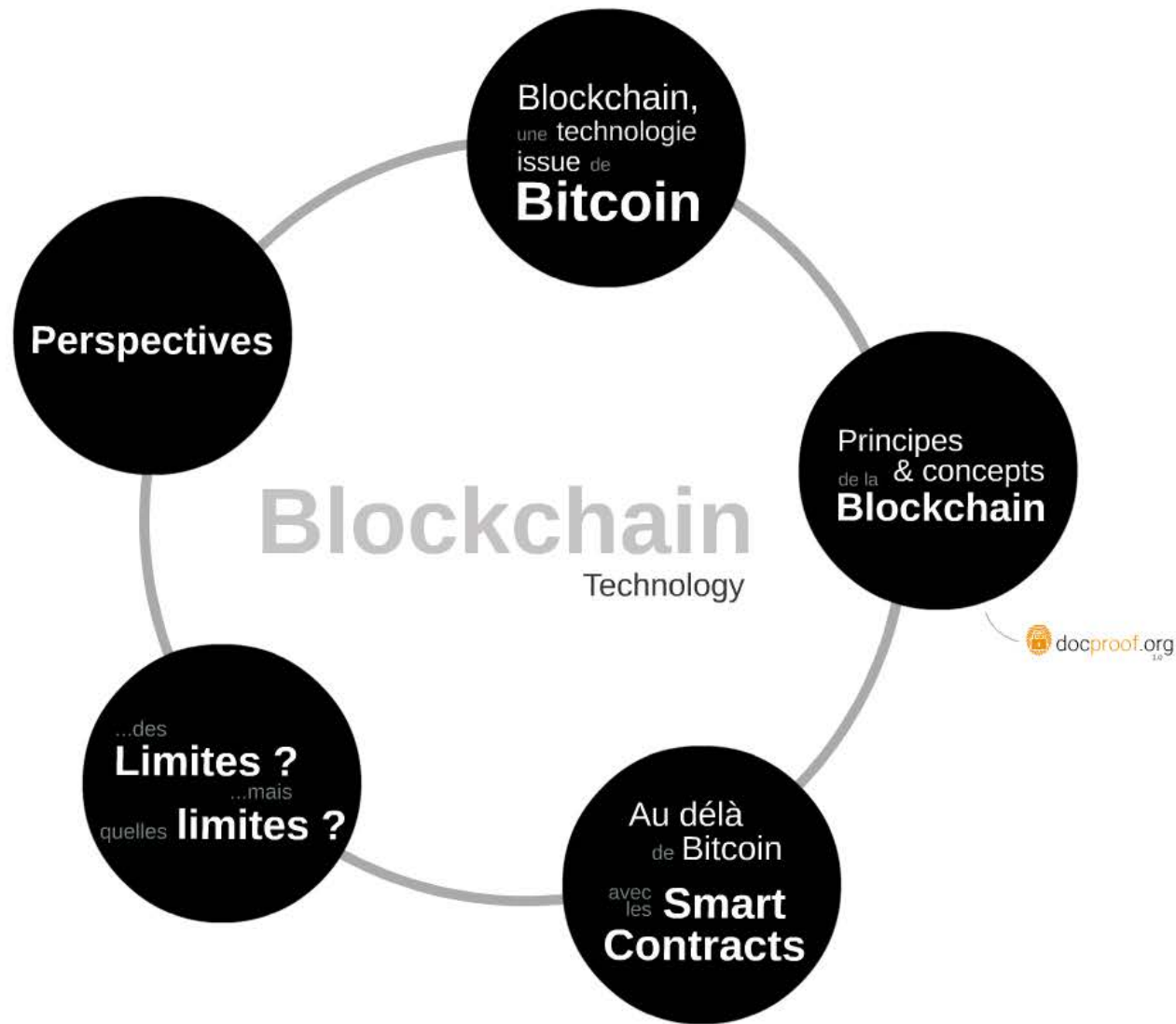
# De la **Confiance** À LA **Preuve...**

Technologie blockchain - Principes, usages & perspectives

 | 23 juin 2017

Jean-Luc Parouty - CNRS/IBS







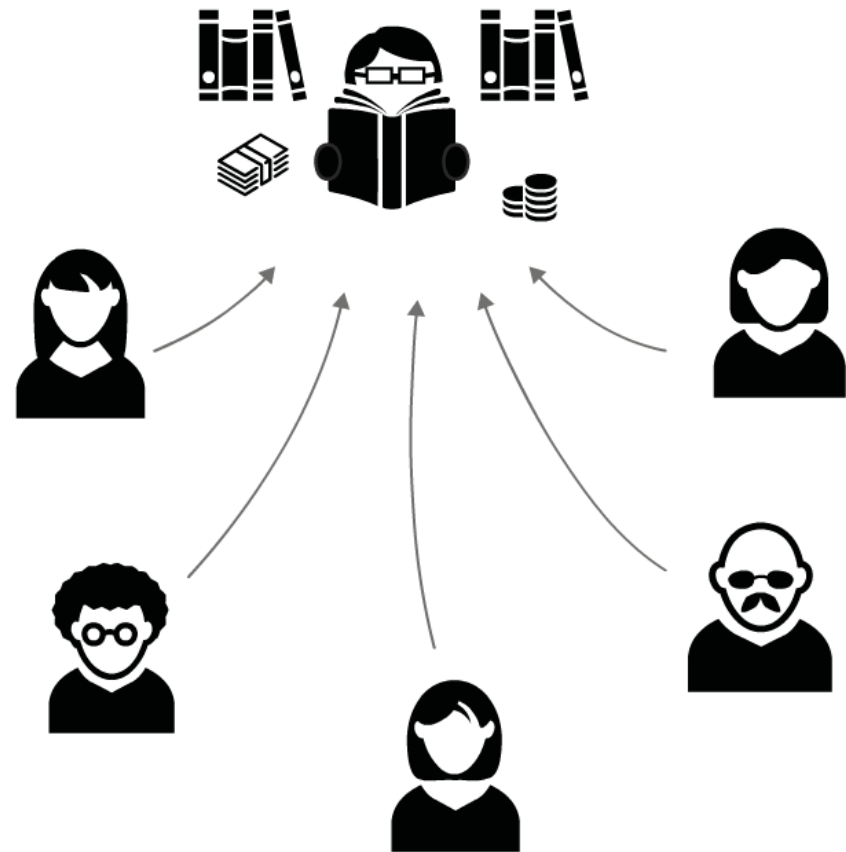
Blockchain,  
une technologie  
issue de  
**Bitcoin**

## De la confiance à la preuve

### Modèle d'échanges traditionnel :

Monnaie  
Échange  
Propriété

Tiers de confiance

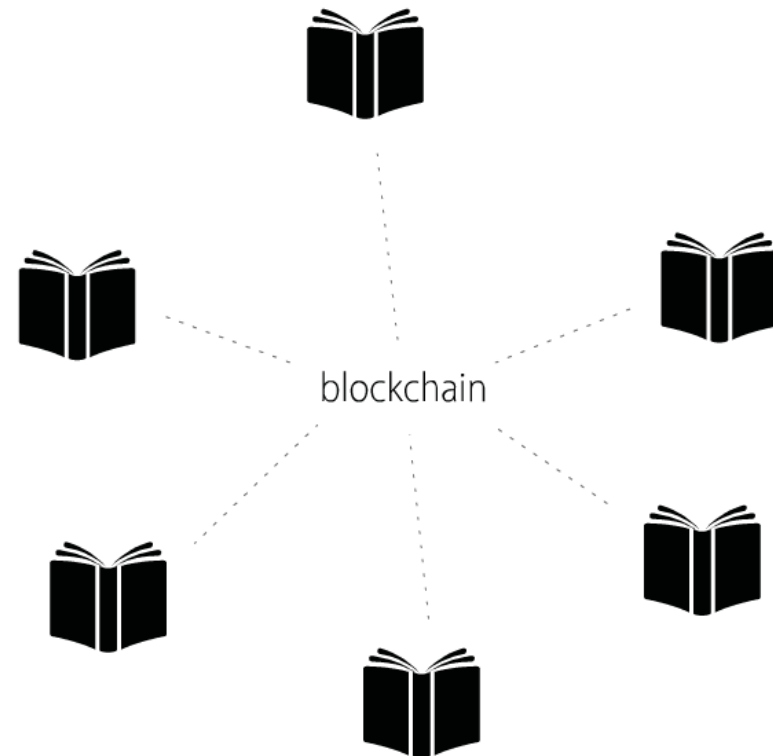


De la  
confiance  
à la preuve

## Modèle "Bitcoin"

Monnaie  
Échange  
Propriété

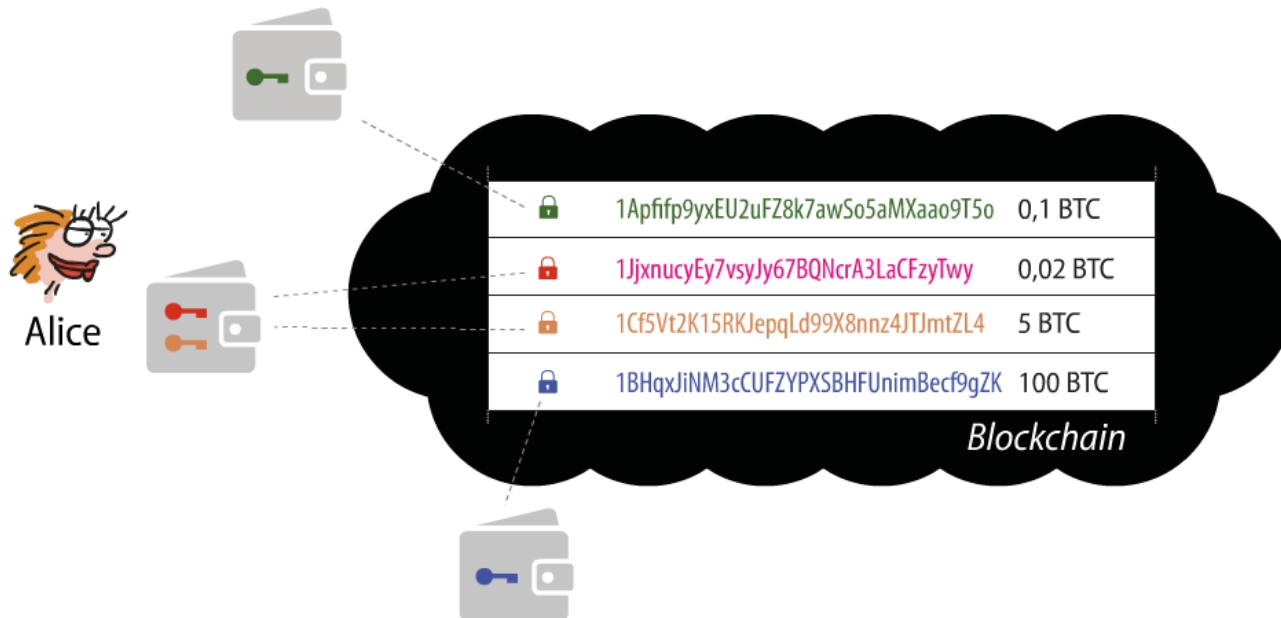
Quantité limitée  
Transparence  
Preuve



**Blockchain**

= Bitcoin

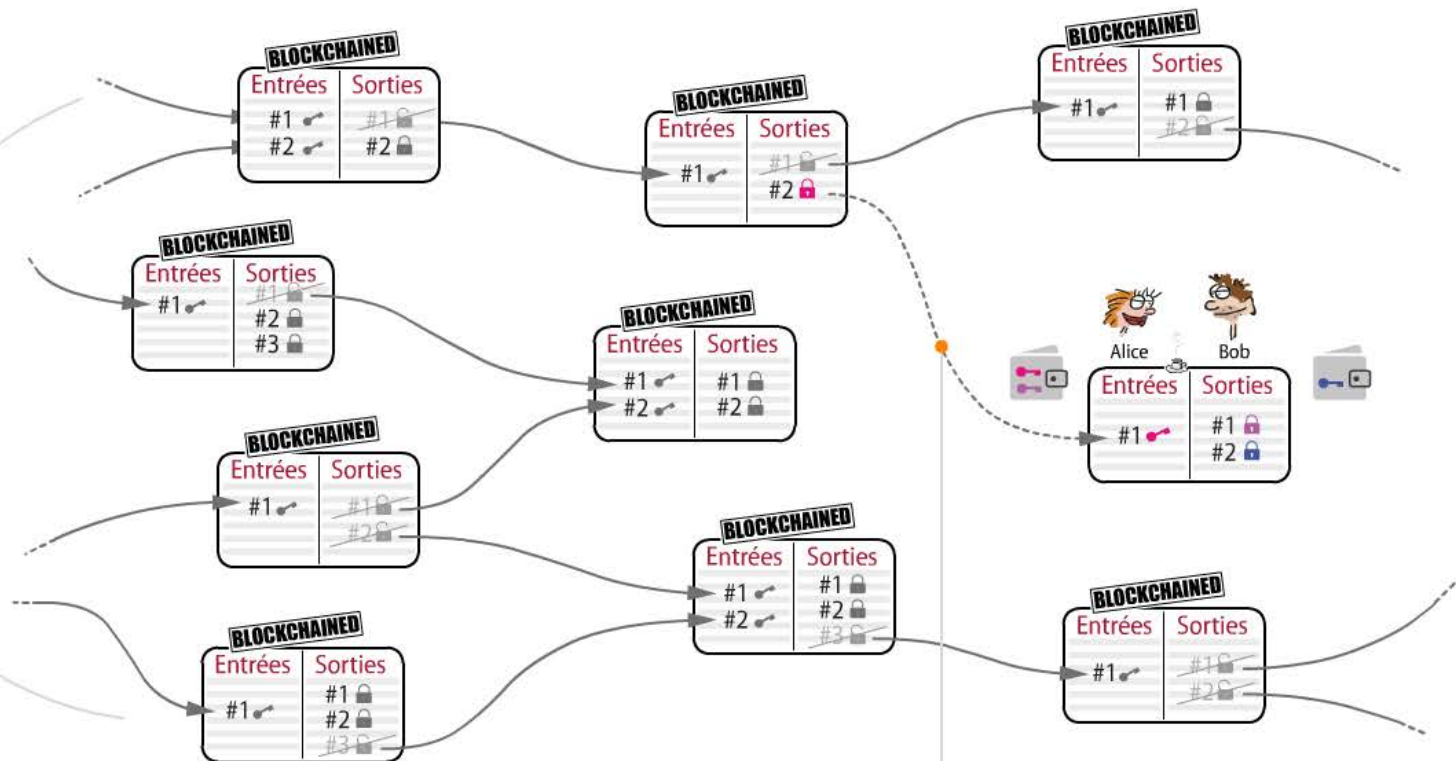
**Livre de  
compte**



**Livre de  
compte  
=  
Toutes les  
transactions**

|                               |          |
|-------------------------------|----------|
| 1q9p8yDnEUZfZ87W6oSaMm5ao9TSo | 0.1 BTC  |
| 1j9wgyGzCnpvLgH2xanUagVxkay   | 0.02 BFC |
| 1J5dK2tP3R4Bppd48FDMwzrL3AmU4 | 5 BTC    |
| TH6qnNGULCFZFQSRHDeenRozXc    | 100 BTC  |

*Blockchain*



Toute **entrée** (input) doit correspondre à une **sortie** (output) non dépensée

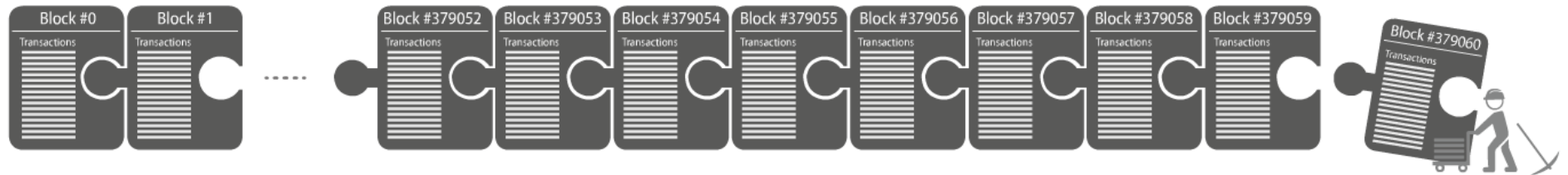
## Unspent Transaction Output (UTXO)



Principes  
d'une & concepts  
**Blockchain**



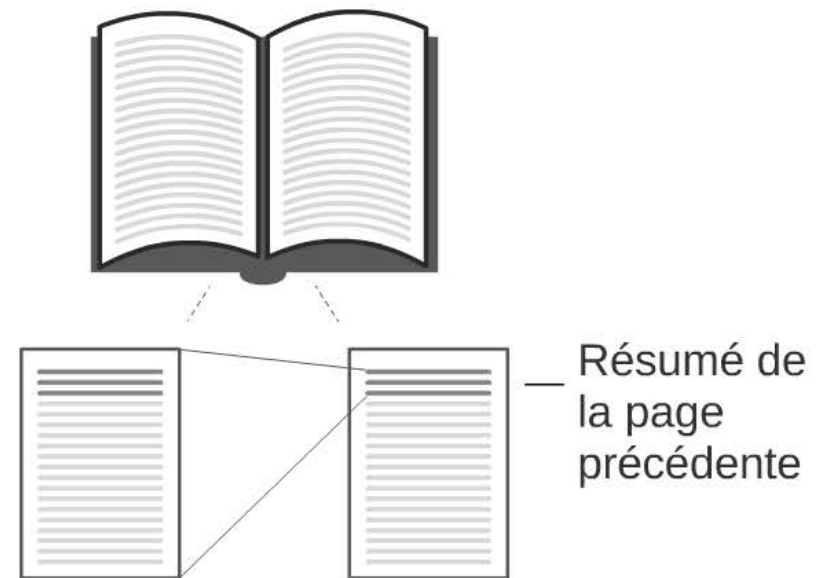
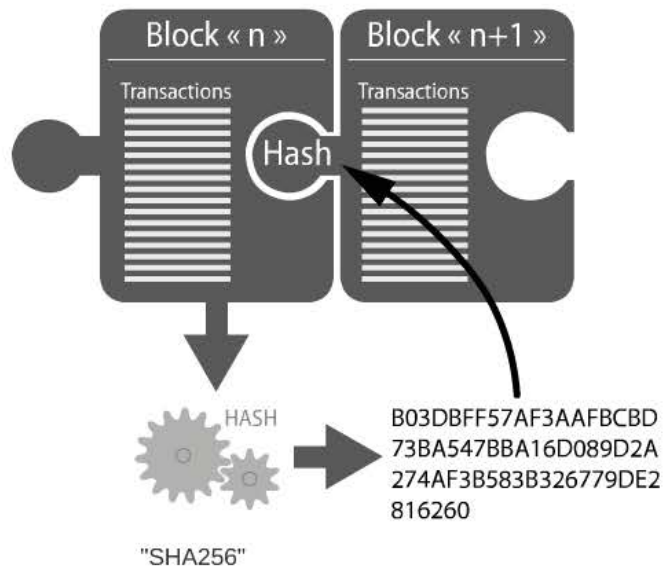
**Blockchain**  
=  
**Chaine  
de blocs**



Les blocs sont enchaînés les uns aux autres

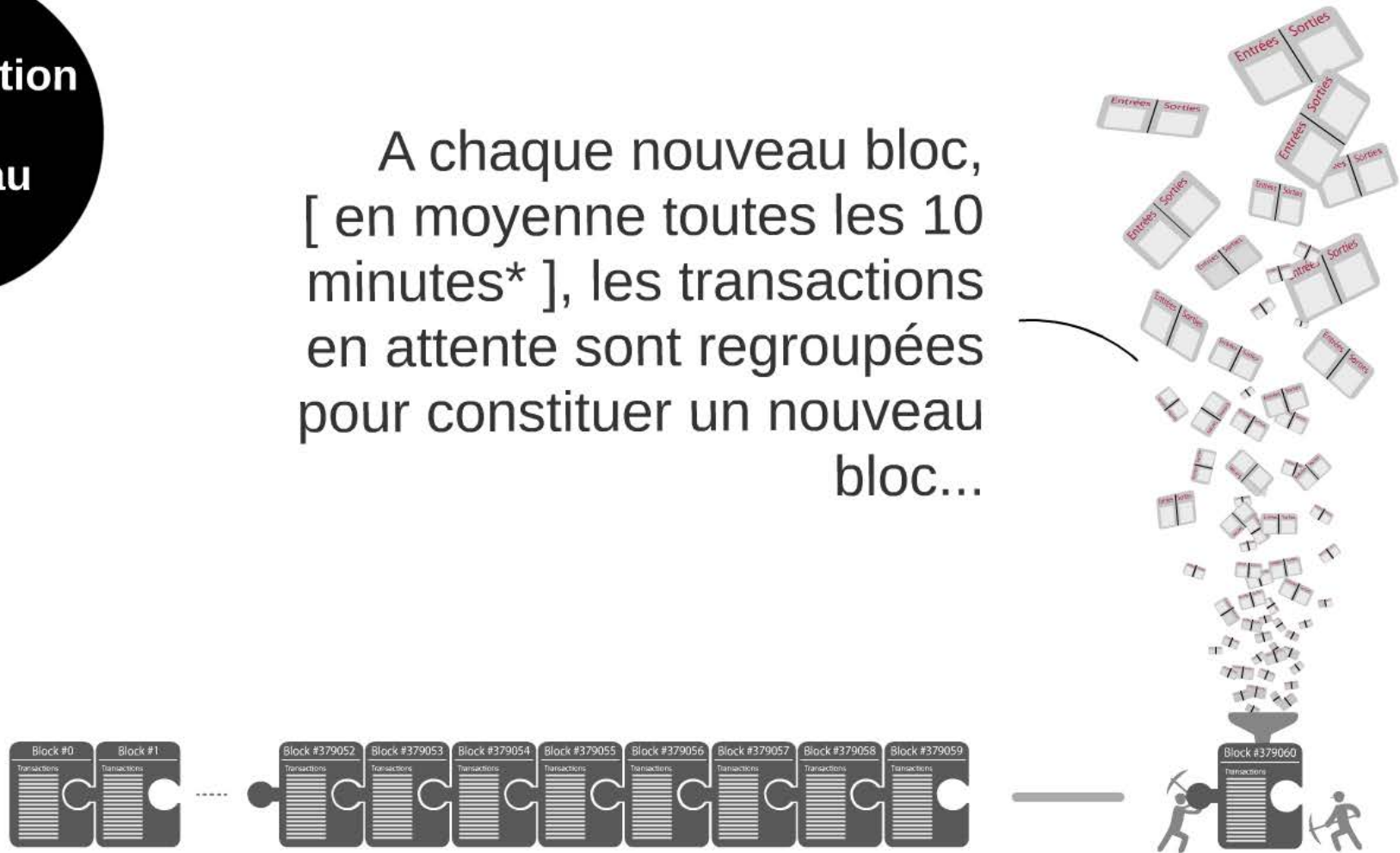
Toute modification d'un bloc nécessiterait de modifier  
tous les suivants

Chaque bloc  
"protège" le  
précédent



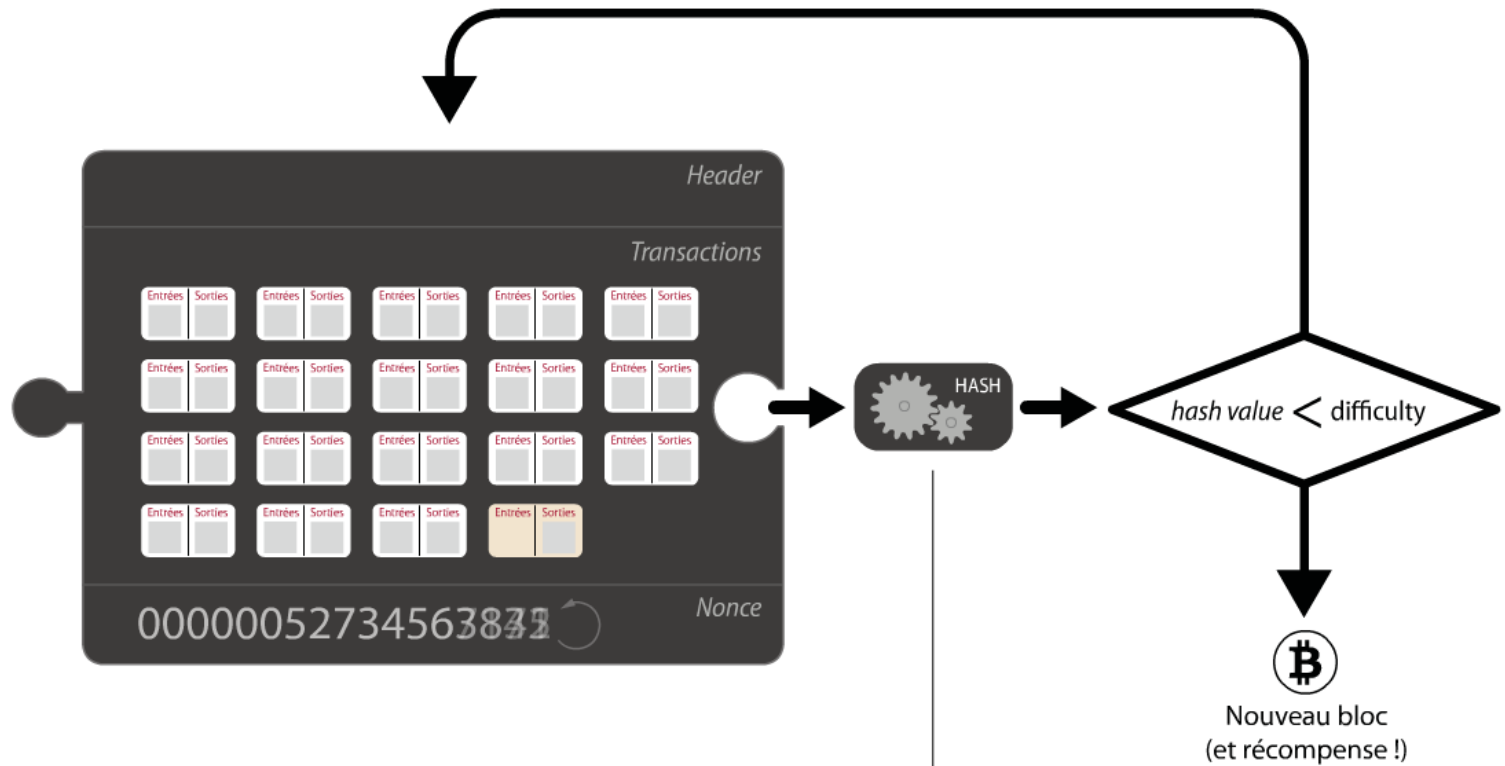
## Construction d'un nouveau bloc

A chaque nouveau bloc,  
[ en moyenne toutes les 10  
minutes\* ], les transactions  
en attente sont regroupées  
pour constituer un nouveau  
bloc...



\* Blockchain Bitcoin

# Principe de la preuve par le travail

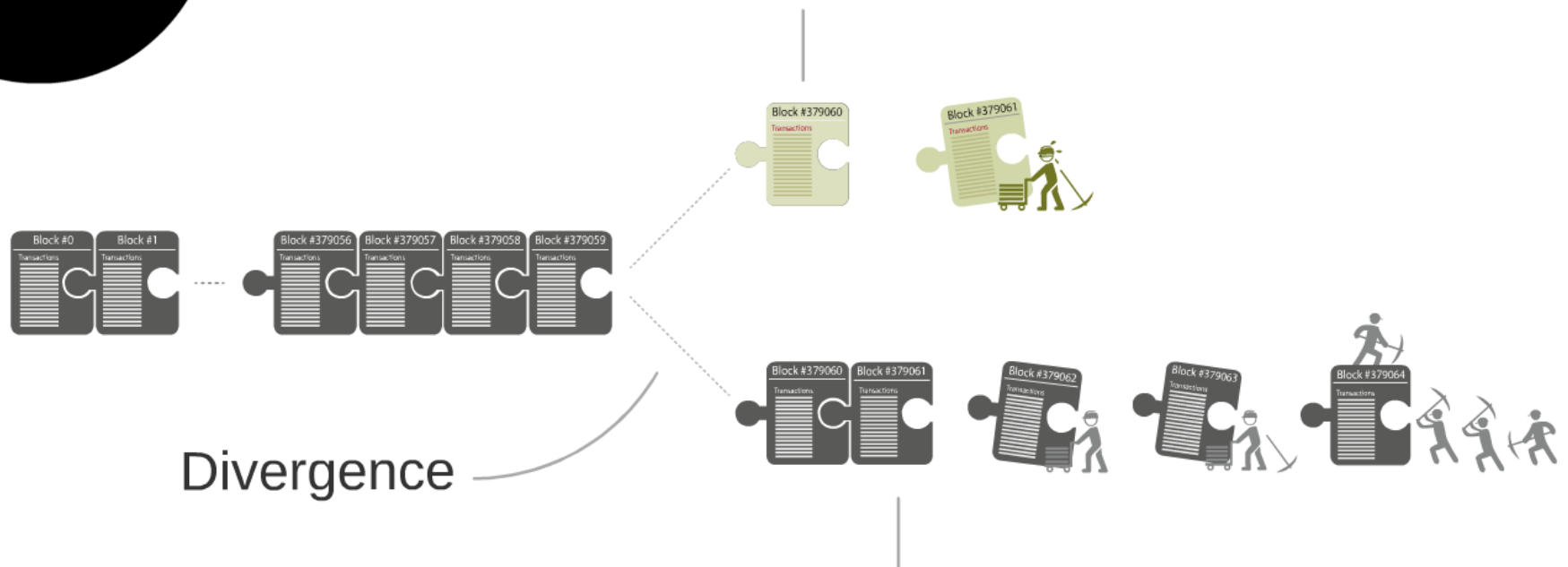


Exemple :

00000000000000000002be4d6e740fa56cb6a00be18e7d8319c618b80f6fff22ec

# Intégration dans la blockchain

Un mineur malhonnête peut aisément miner et diffuser un bloc malhonnête



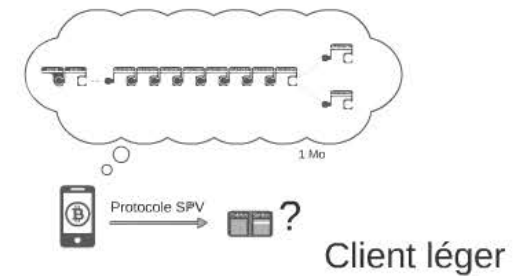
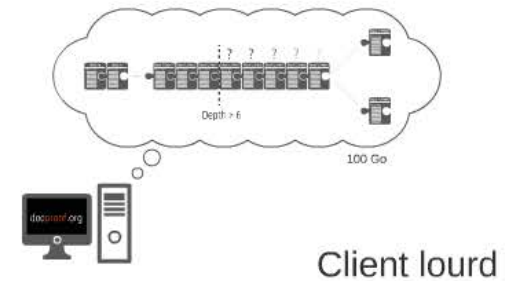
Si les mineurs honnêtes sont majoritaires, ils progresseront plus rapidement

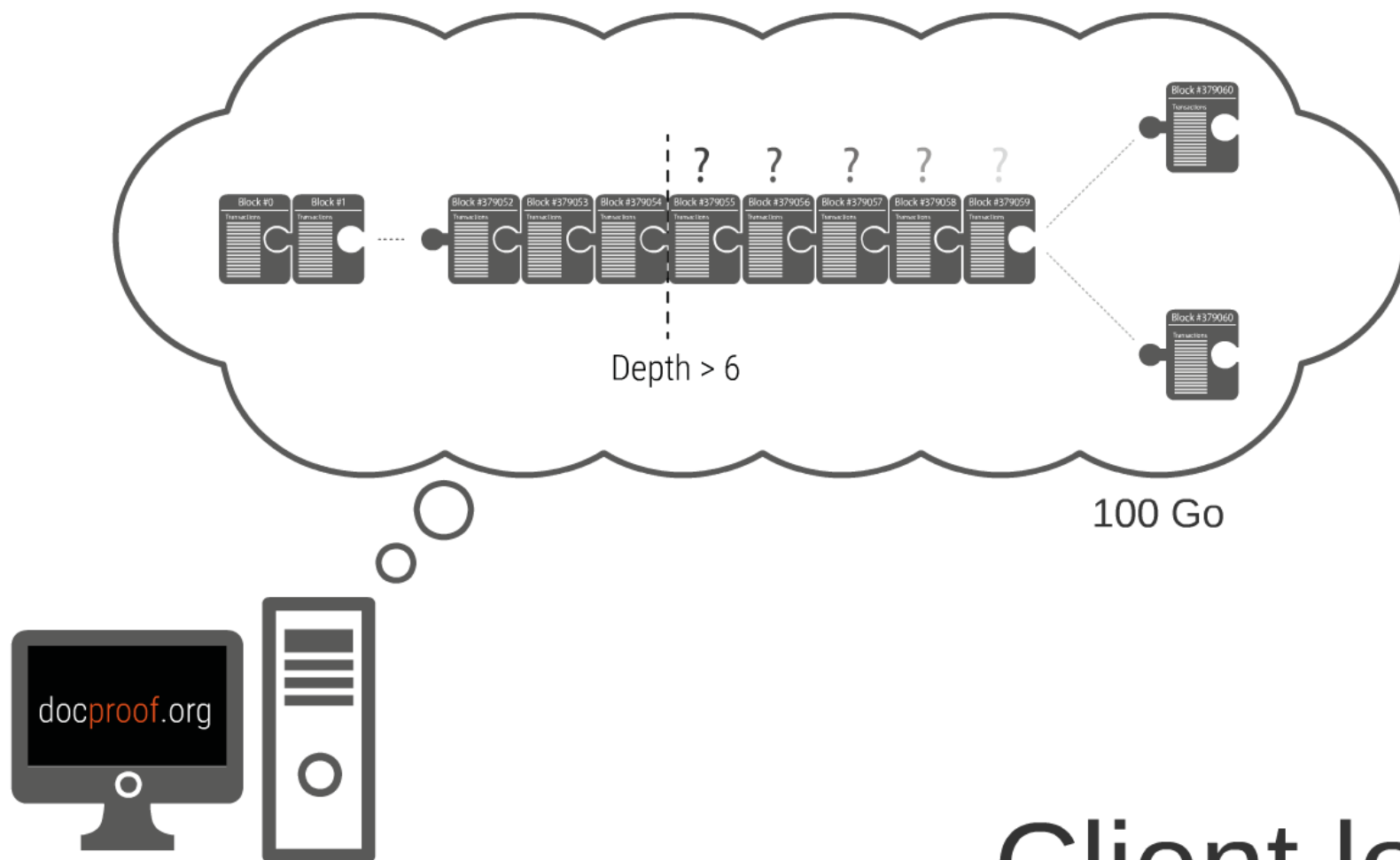
# Vérification

La transaction  
est-elle dans la  
blockchain ?

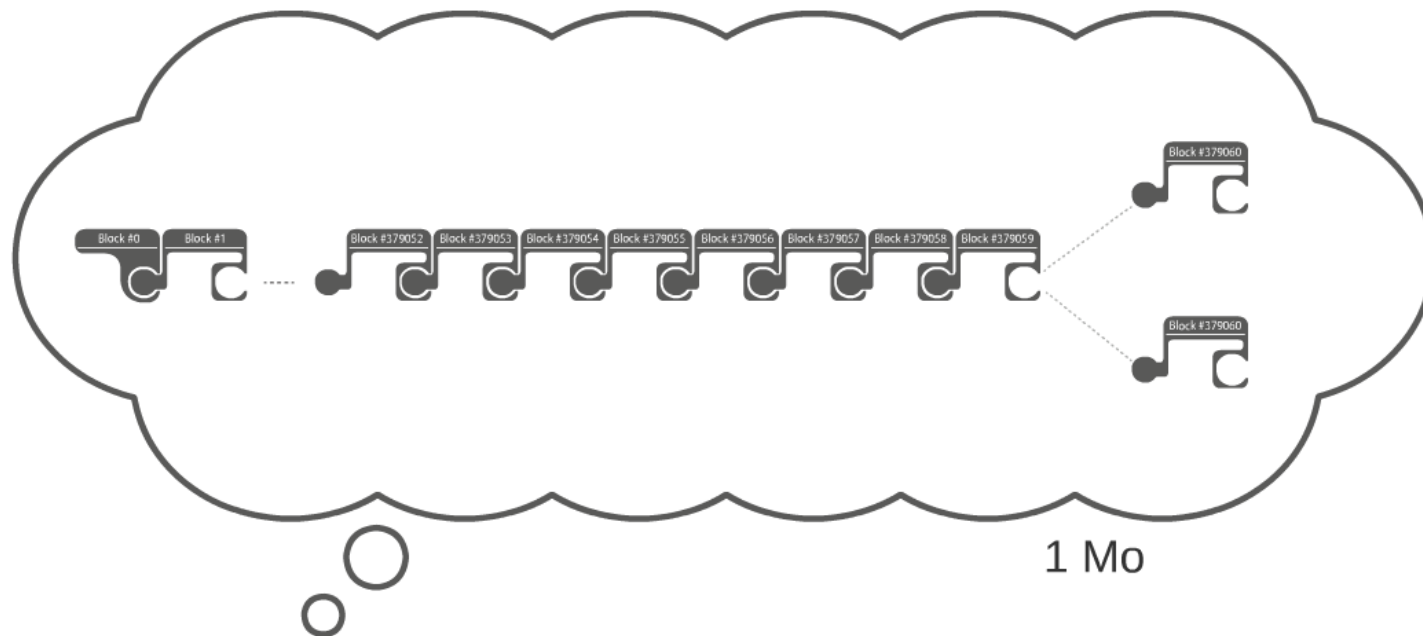


La sortie a-elle  
été dépensée ?





Client lourd



Protocole SPV



?

# Client léger





Enregistrer une preuve  
d'antériorité en 2 minutes  
...et pour moins de 5 €

# Contexte & historique

Projet académique\*  
Institut de Biologie Structurale



Veille technologique & Besoins internes

Blockchain

Notariat électronique

(\*) Présentations JRES2015, JSSI2016

# Objectifs



Enregistrement de preuves d'antériorité

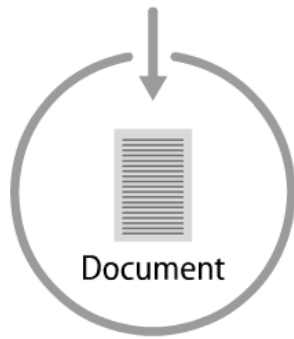
Simple,  
Coûts réduits,  
Intégrable au sein de processus  
existants,  
Ouvert

Démonstrateur / blockchain

Modèle de confiance -> Preuve

# Principe

## 1. Déposer



HASH  
1083b7b2facc2bd3b8f284  
48f1640208a4d9f1f990af  
3e4a66a8093dbe724b6d

Client side

## 2. Enregistrer

\*\*\*\*\*

or

Thanks to contribute 0.005 BTC to the following address :  
1CpssaULHLQZGHhwnwfiDwvEZcqL4qiECp

Server side  
(API)

Transaction



## 3. Garder une trace

Great :-)

Your document's hash was included in the Bitcoin blockchain,  
into the block 383346, with the transaction id :

7999b2c934ce38385989437b4ca995930ea01fb7cd54bedb6a386ccbba1c5e2d

  
[blockchain.info](https://blockchain.info)  
[blockexplorer.com](https://blockexplorer.com)  
[blocktrail.com](https://blocktrail.com)  
...

OP\_RETURN DOCPROOF 1083b7b2facc2bd3b8f28448f1640208a4d9f1f990af3e4a66a8093dbe724b6d



docproof.org

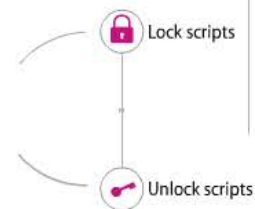
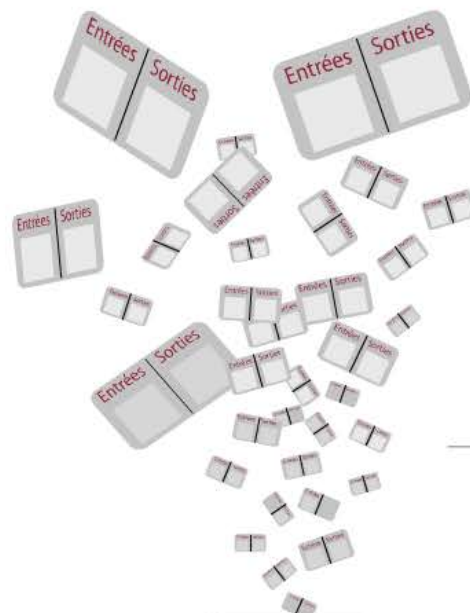
Une démonstration  
Vaut toujours  
PLUS que 1000 Mots...



Au delà  
de Bitcoin

avec  
les **Smart  
Contracts**

# Des scripts Bitcoin...



**P2PKH**  
Pay-to-Public-Key-Hash  
**Multi Signature**  
M signatures sur N possibles  
**P2SH**  
Pay-to-Script-Hash  
**OP\_RETURN**  
Enregistrement de données

Exemple : OP\_DUP OP\_HASH160 39ee7f7d4c88367d27e7657cbfe7048d0eb84e5 OP\_EQUALVERIFY OP\_CHECKSIG



Lock scripts



Unlock scripts

**P2PKH**

Pay-to-Public-Key-Hash

**Multi Signature**

M signatures sur N possibles

**P2SH**

Pay-to-Script-Hash

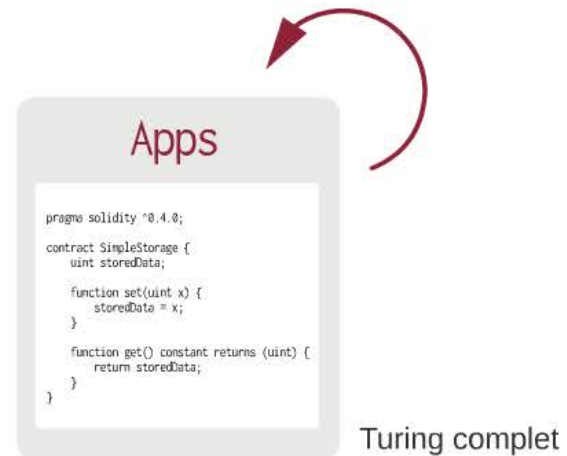
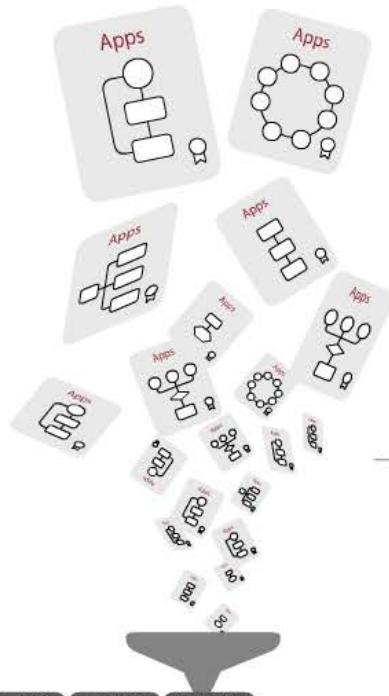
**OP\_RETURN**

Enregistrement de données

Exemple : OP\_DUP OP\_HASH160 39ee7f7d4c80307d27e7657cbfef0d48d0eb84e5 OP\_EQUALVERIFY OP\_CHECKSIG



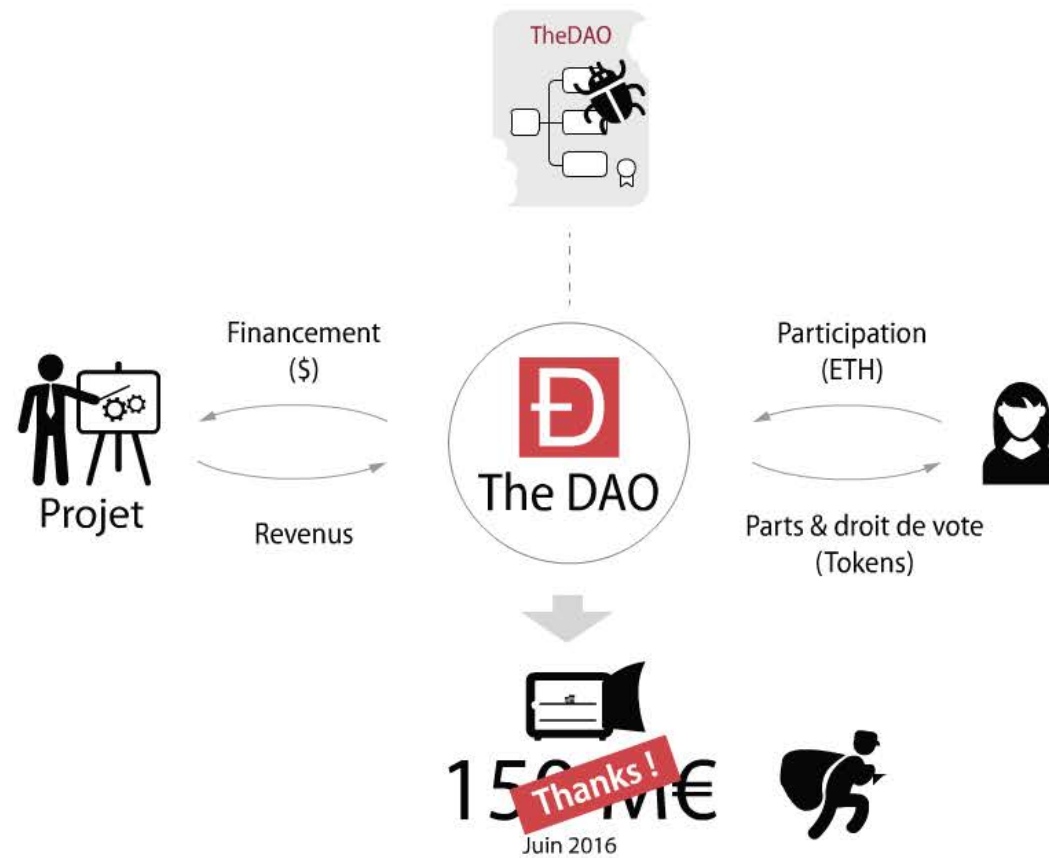
...aux smart  
contracts  
Ethereum



```
pragma solidity ^0.4.0;  
contract SimpleStorage {  
    uint storedData;  
  
    function set(uint x) {  
        storedData = x;  
    }  
  
    function get() constant returns (uint) {  
        return storedData;  
    }  
}
```

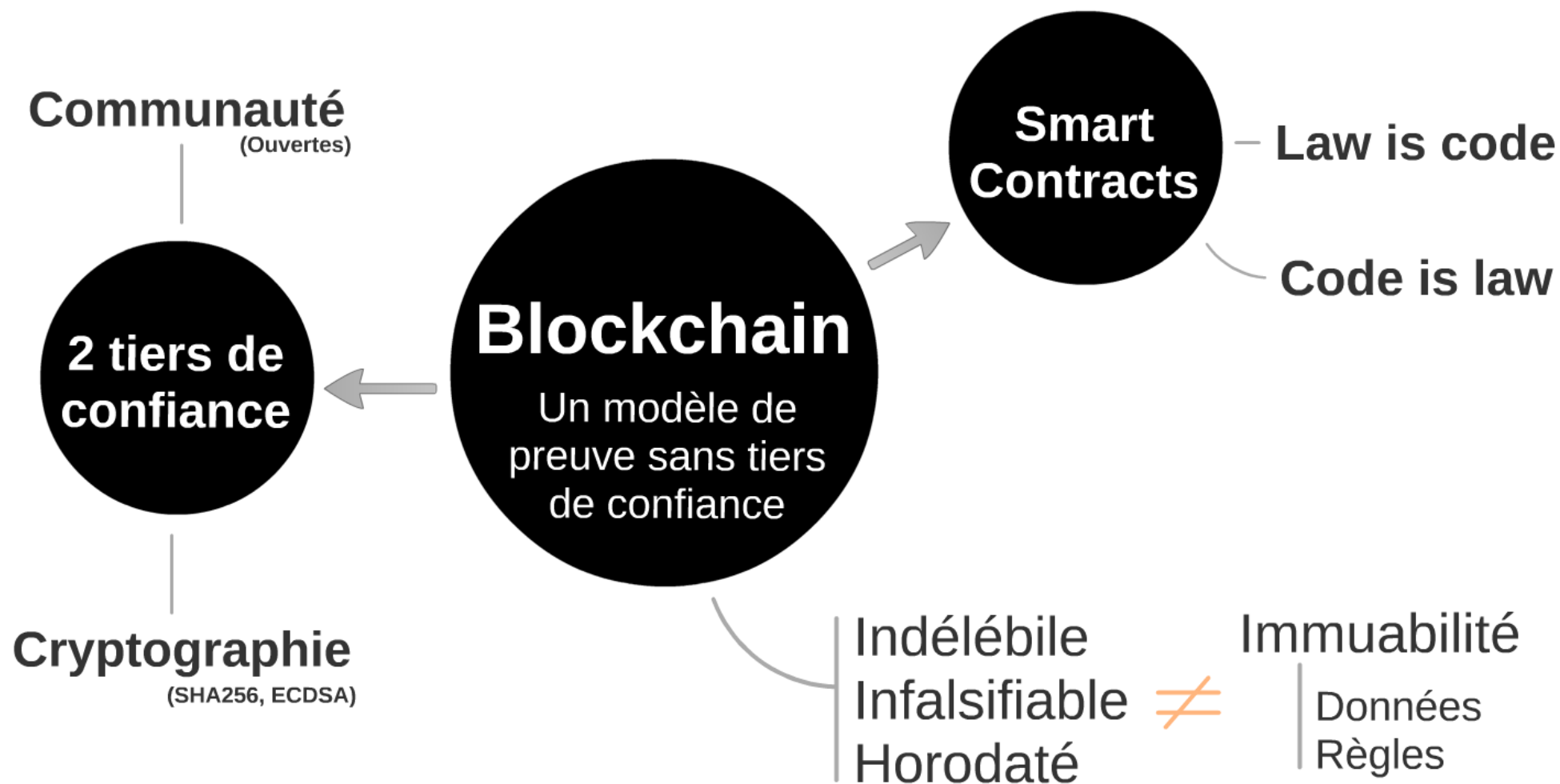
Turing complet

# DAO\* Organisation Autonomes Décentralisées



(\*) *Decentralized Autonomous Organization*







**Perspectives**

Technologie  
**blockchain**



Contrat de propriété 15ème av.JC Cuneiforme Akkadien  
Source : Gallica.bnf.fr

**Crypto-monnaies**

Plus de  
**700**

Capitalisation  
Top 4

**80 MM€**

**Preuve  
d'antériorité**

...simple is beautiful

**Gestion d'actifs  
et de contrats,  
DAO**



**Blockchains privées / souveraines**

Consortium financier R3 CEV  
Microsoft AZUR

...

## KeeX

Sécuriser, chainer, partager, signer et horodater n'importe quel document, donnée ou processus, sans altération...

<https://keeex.me>

## Everledger

Everledger is a global startup that uses the best of emerging technology including blockchain, smart contracts and machine vision to assist in the reduction of risk and fraud for banks, insurers and open marketplaces.

<https://www.everledger.io>

## Wal-Mart

Supply chain management - Wal-Mart started tracking two products using blockchain: a packaged produce item in the U.S., and pork in China.

## Stratum

Secure processes between partners through blockchain technology

- Digital Notarization
- Universal Traceability
- Digital Ownership
- Proof of Process Reporting
- Direct Settlements

<https://stratumn.com>

## Verisart

Verisart delivers a new way to certify and verify artworks and collectables in real time. By using distributed ledger technology provided by the blockchain, Verisart aims to build a permanent, decentralized and anonymous ledger for the world's art and collectables.

<http://www.verisart.com>

## Blockverify

Blockchain Based Anti-Counterfeit Solution - Improve anti-counterfeit measures in different industries and have a significant positive social impact (pharmaceuticals, luxury items, diamonds, electronics, ...)

<http://www.blockverify.io>

## Followmyvote.com

A secure online voting platform that will allow for greater election transparency.

<http://www.blockverify.io>

## Filament

Distributed Exchange and the Internet of Things. Deploy a long-range wireless network anywhere

<https://filament.com>

