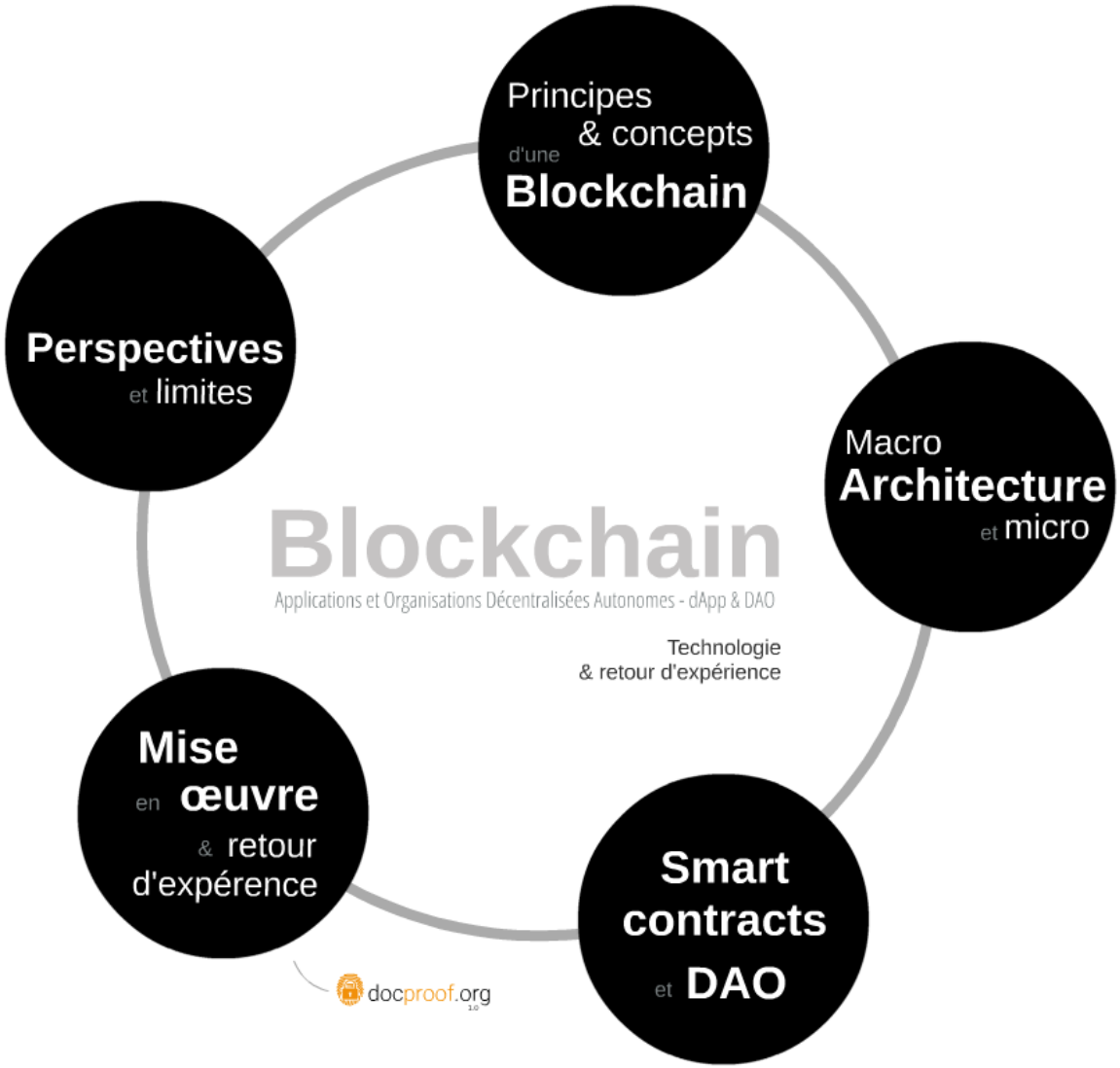
Blockchain

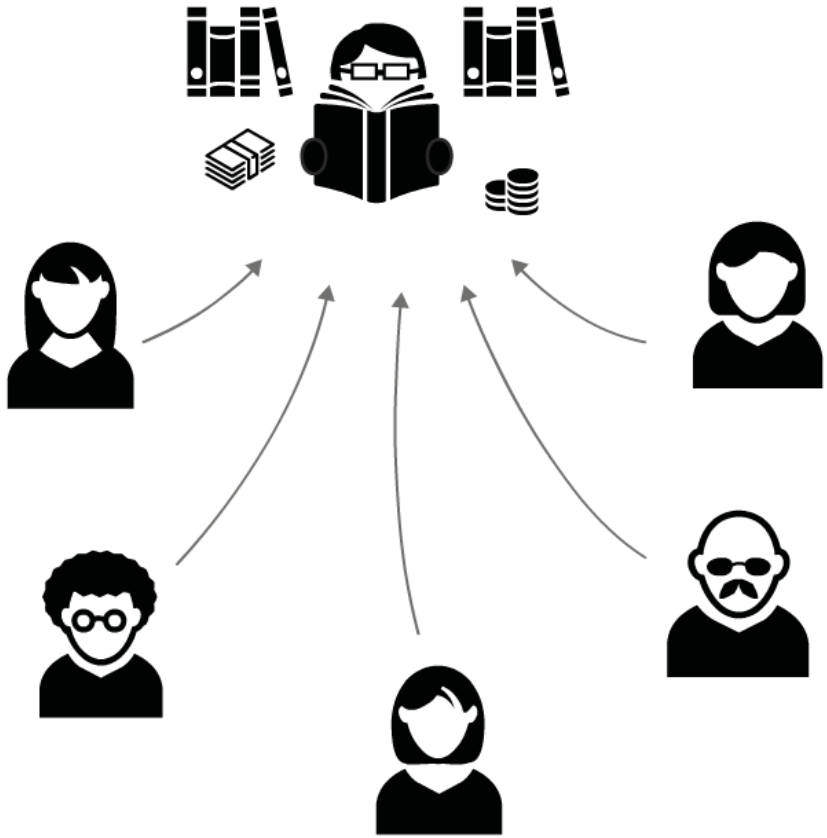
Applications et Organisations Décentralisées Autonomes - dApp & DAO

Technologie & Retour d'expérience

Jean-Luc.Parouty@ibs.fr - CNRS/IBS


Principes
& concepts
d'une
Blockchain
Macro
Architecture
et micro
Smart
contracts
et DAO
Mise
en œuvre
& retour
d'expérence
Perspectives
et limites
Blockchain
Applications et Organisations Décentralisées Autonomes - dApp & DAO
Technologie
& retour d'expérience
docproof.org

De la
confiance
à la **preuve**

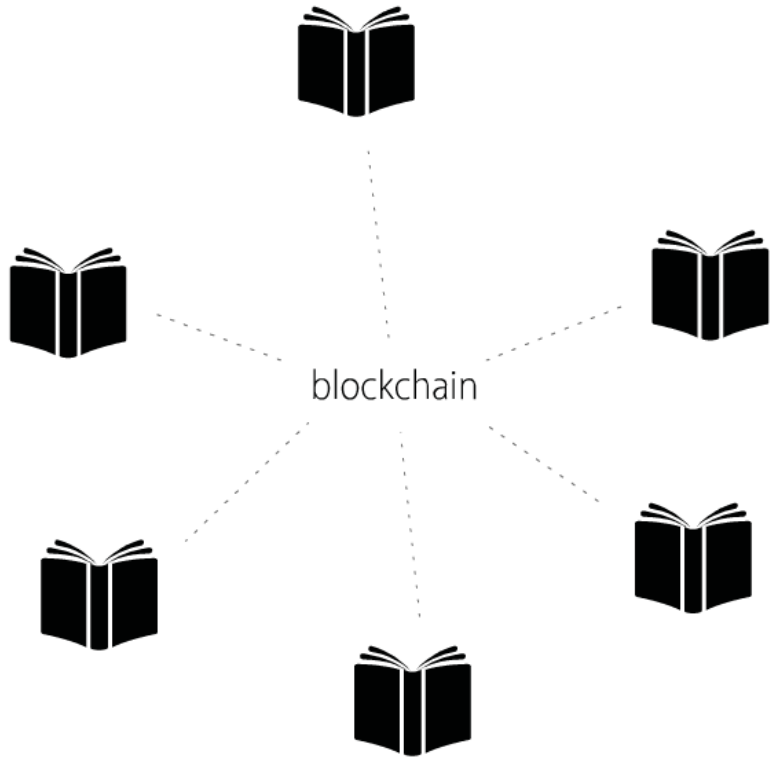


Modèle d'échanges traditionnel :

- Monnaie
- Échange
- Propriété

→ Tiers de confiance

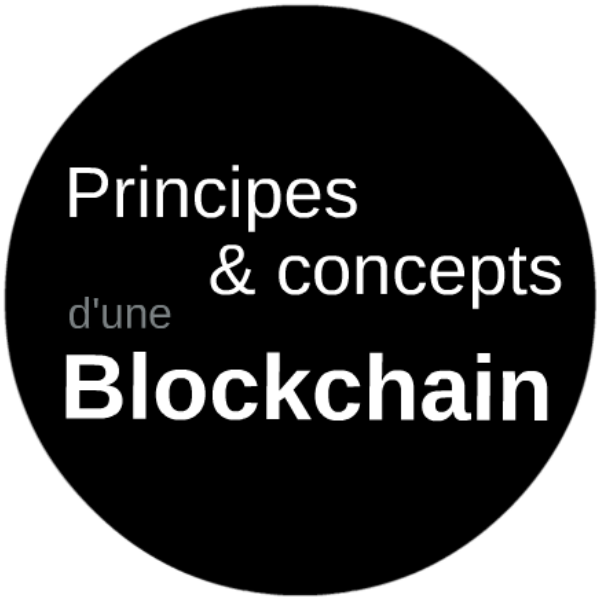
De la
confiance
à la **preuve**



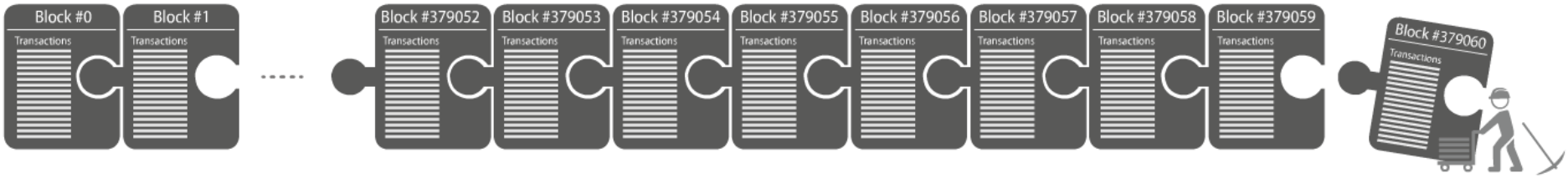
Modèle "Bitcoin"

Monnaie
Échange
Propriété

Quantité limitée
Transparence
Preuve


Principes
& concepts
d'une
Blockchain

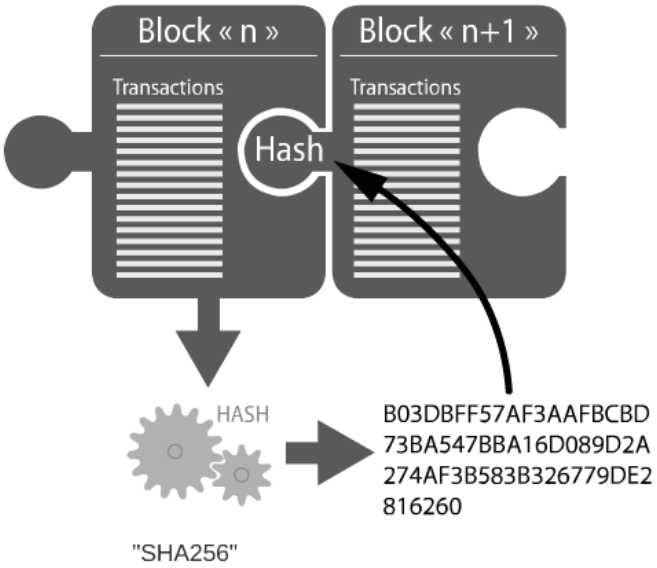
Blockchain
=
Chaine de blocs

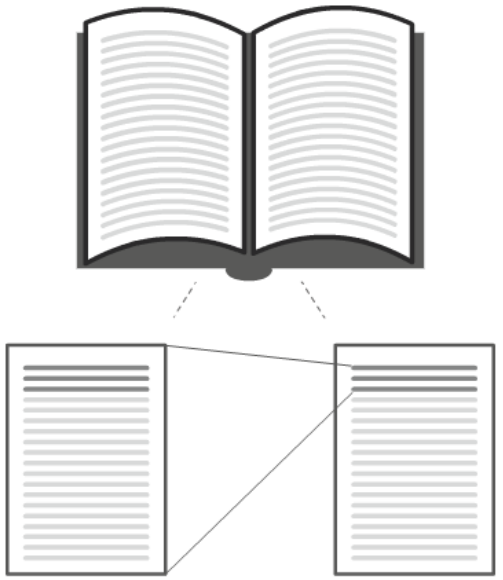


Les blocs sont enchaînés les uns aux autres

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

Chaque bloc "protège" le précédent

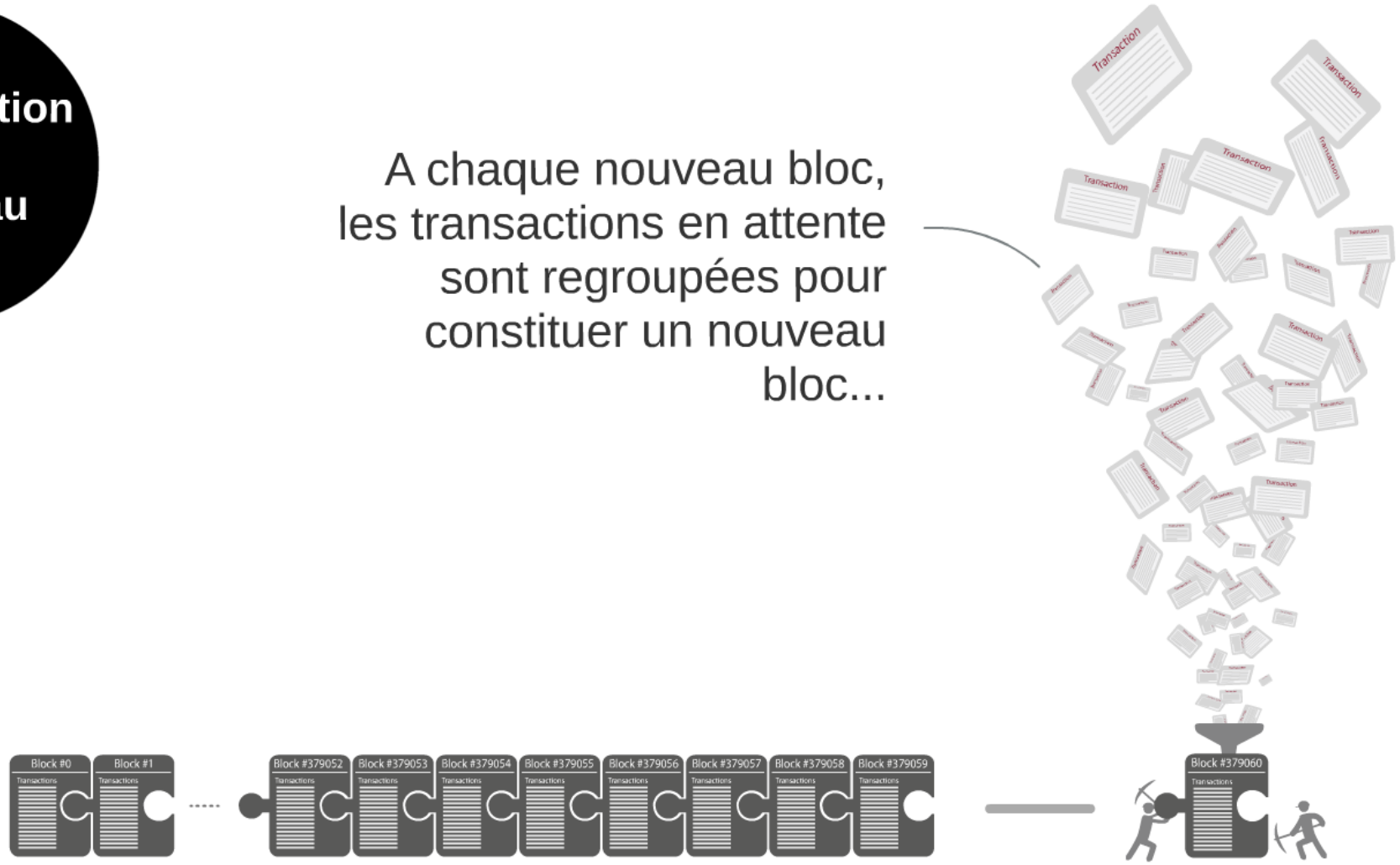




Résumé de la page précédente

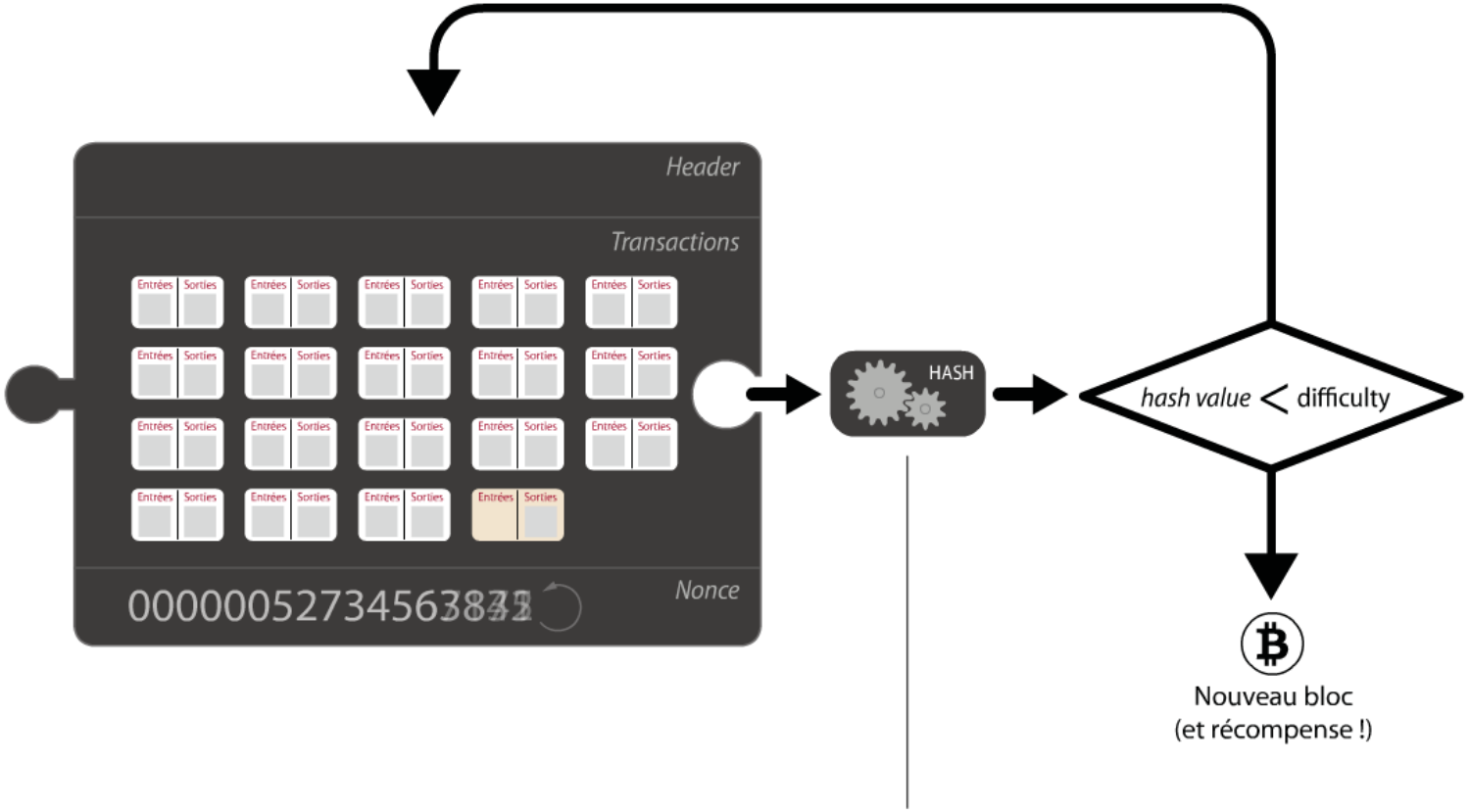
Construction d'un nouveau bloc

A chaque nouveau bloc, les transactions en attente sont regroupées pour constituer un nouveau bloc...



Preuve par le travail (PoW)

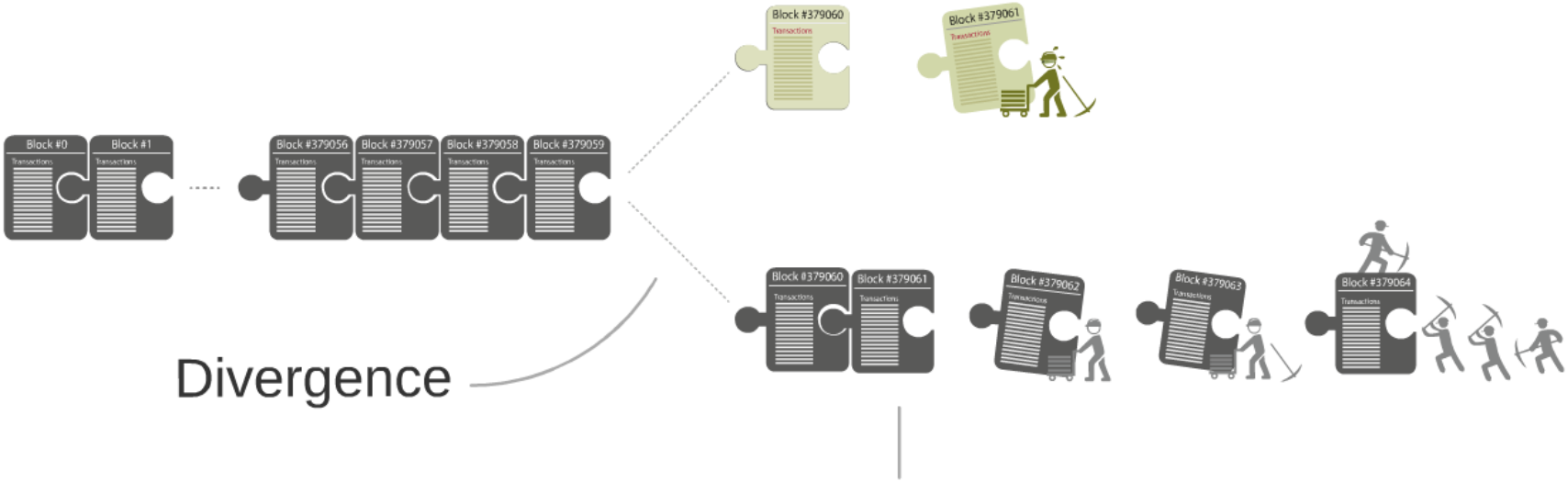
Preuve de possession (PoS)



Exemple :
0000000000000002be4d6e740fa56cb6a00be18e7d8319c618b80f6fff22ec

Intégration dans la blockchain

Un mineur malhonnête peut aisément miner et diffuser un bloc malhonnête



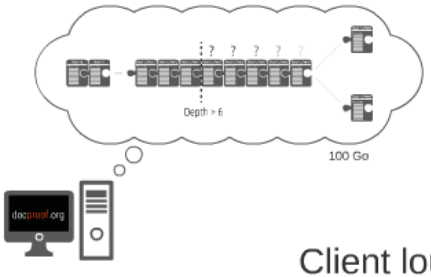
Divergence

Si les mineurs honnêtes sont majoritaires, ils progresseront plus rapidement

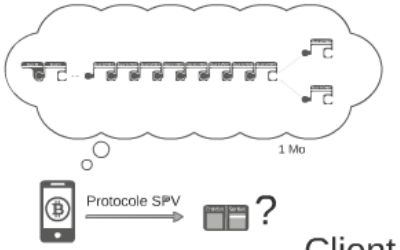
Vérification

La transaction est-elle dans la blockchain ?

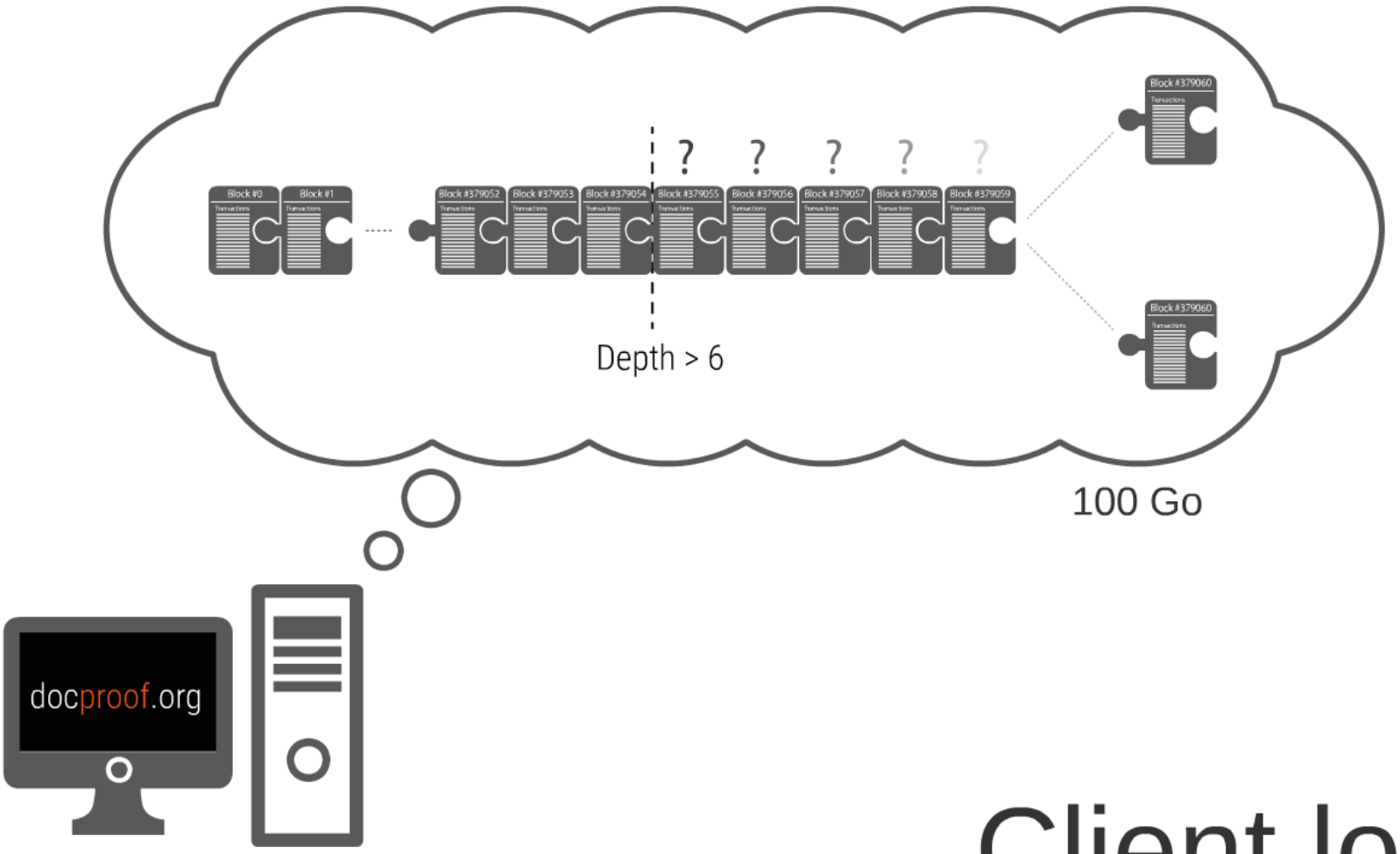
L'information est-elle toujours valide ?



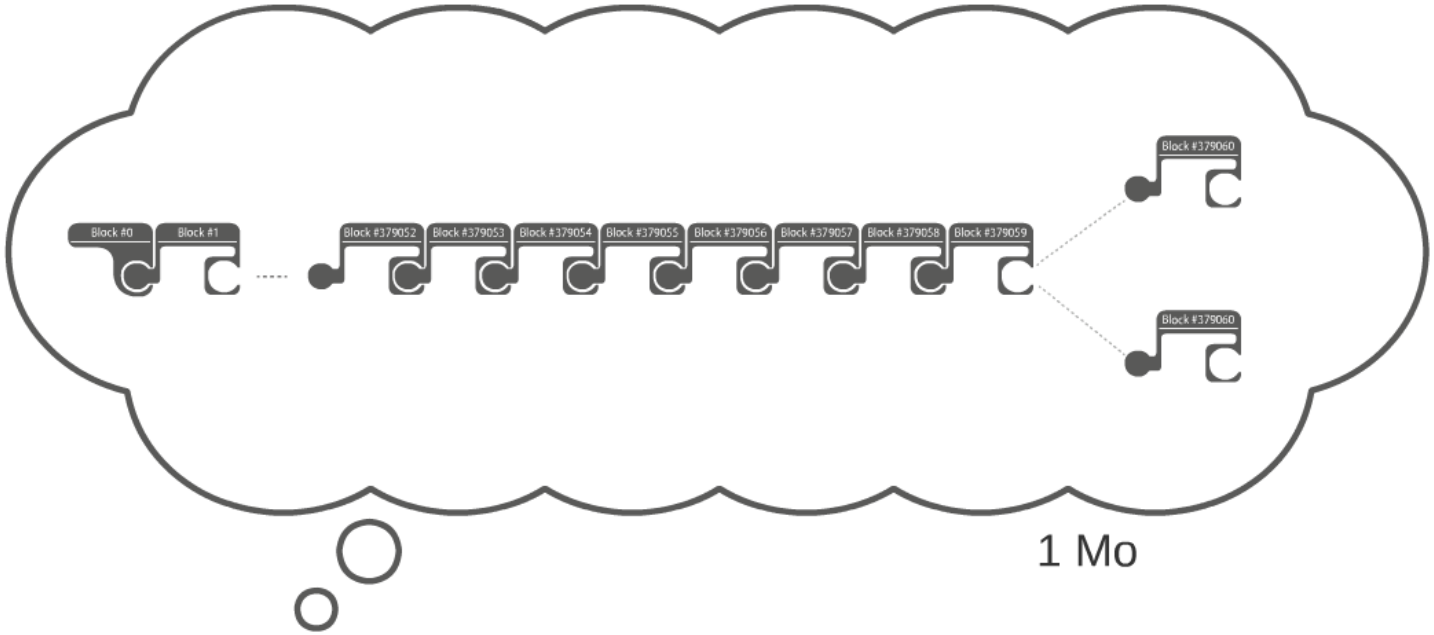
Client lourd

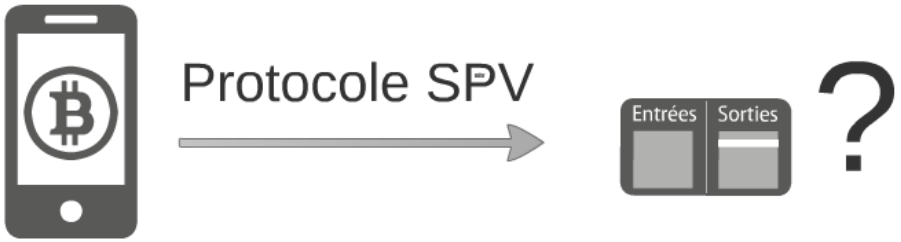


Client léger

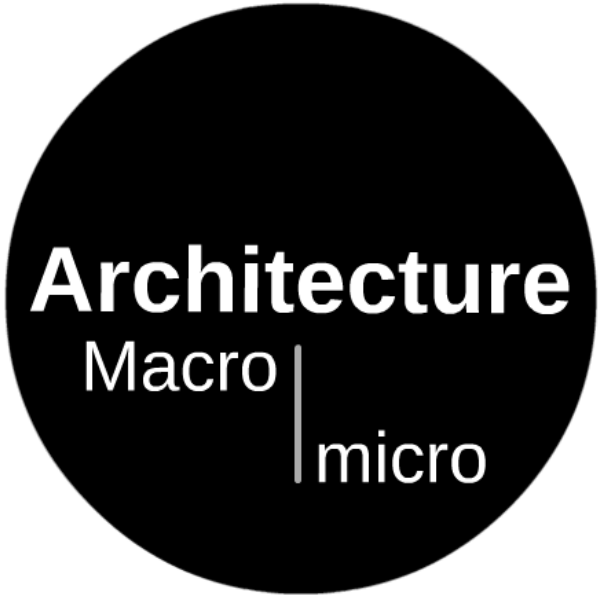


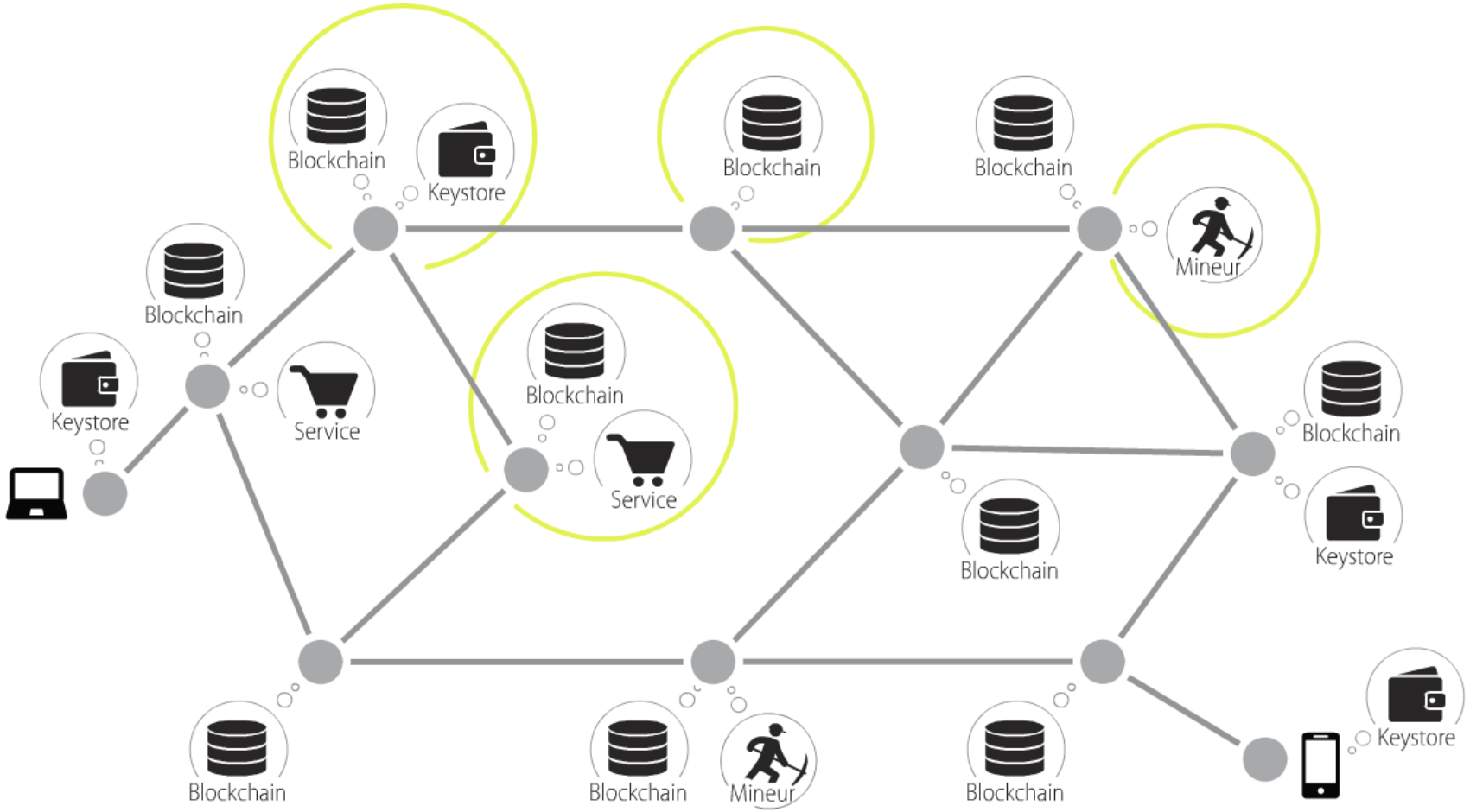
Client lourd

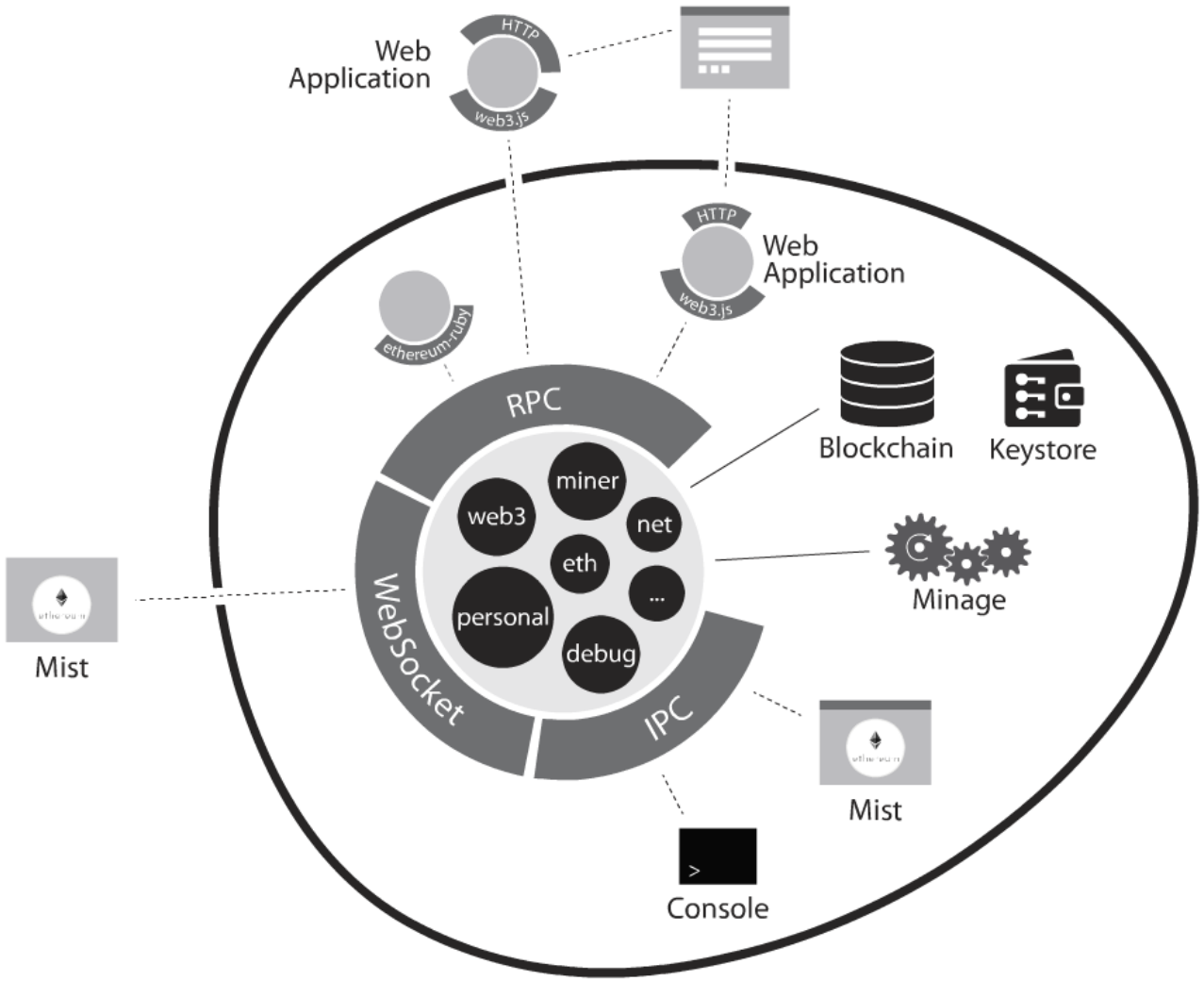




Client léger


Architecture
Macro
micro


Blockchain
Keystore
Blockchain
Blockchain
Mineur
Blockchain
Keystore
Service
Blockchain
Service
Blockchain
Blockchain
Keystore
Blockchain
Blockchain
Mineur
Blockchain
Keystore

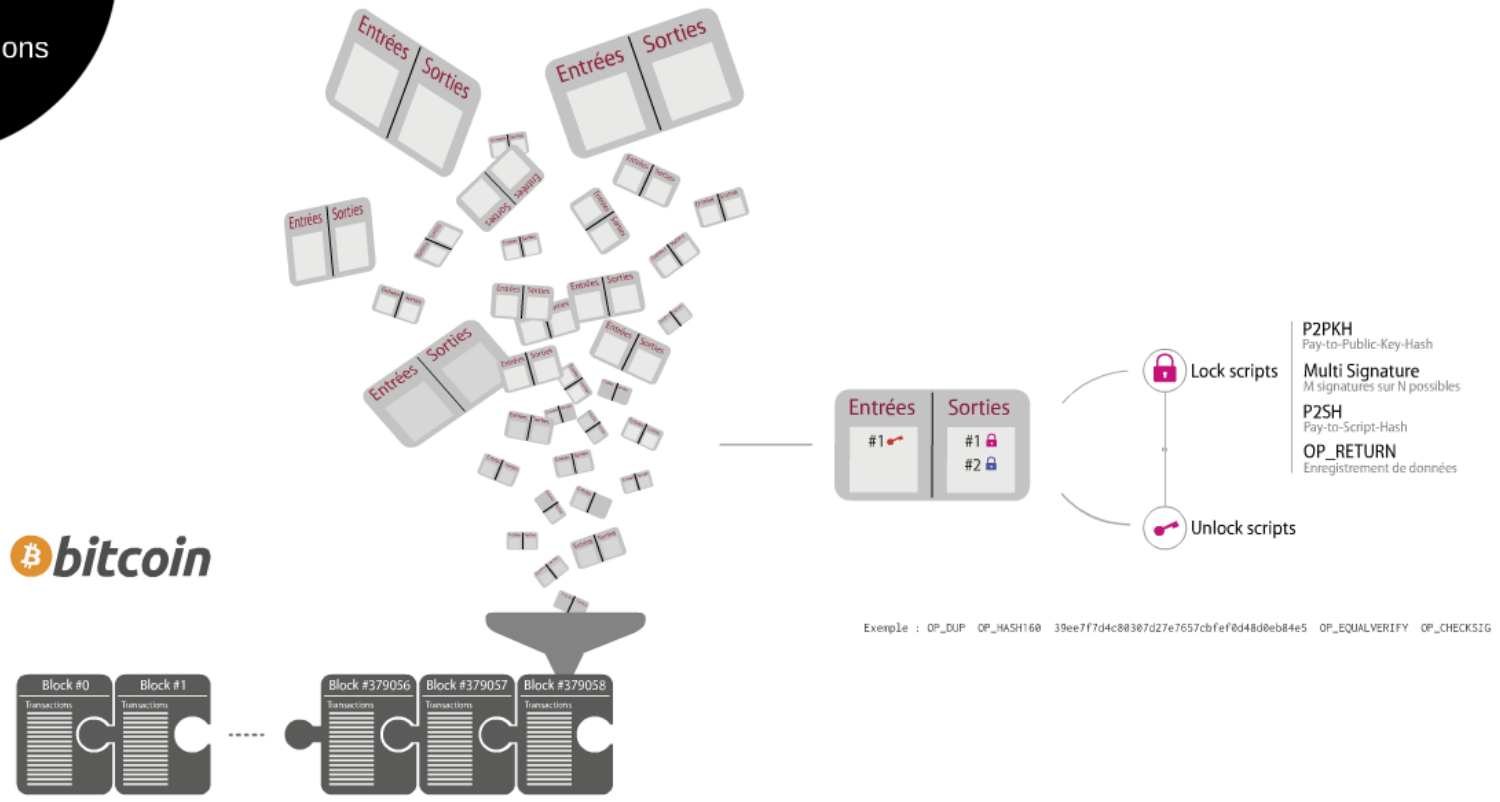


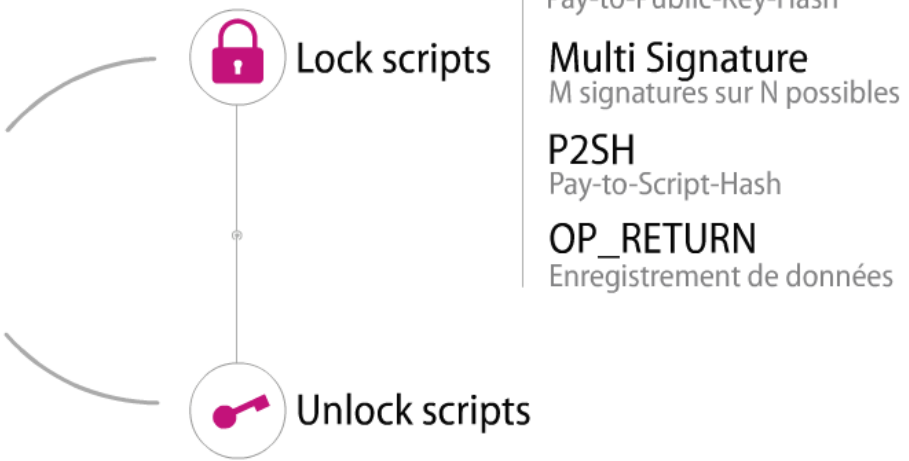
Ethereum node


Smart
contracts
et DAO

Bitcoins

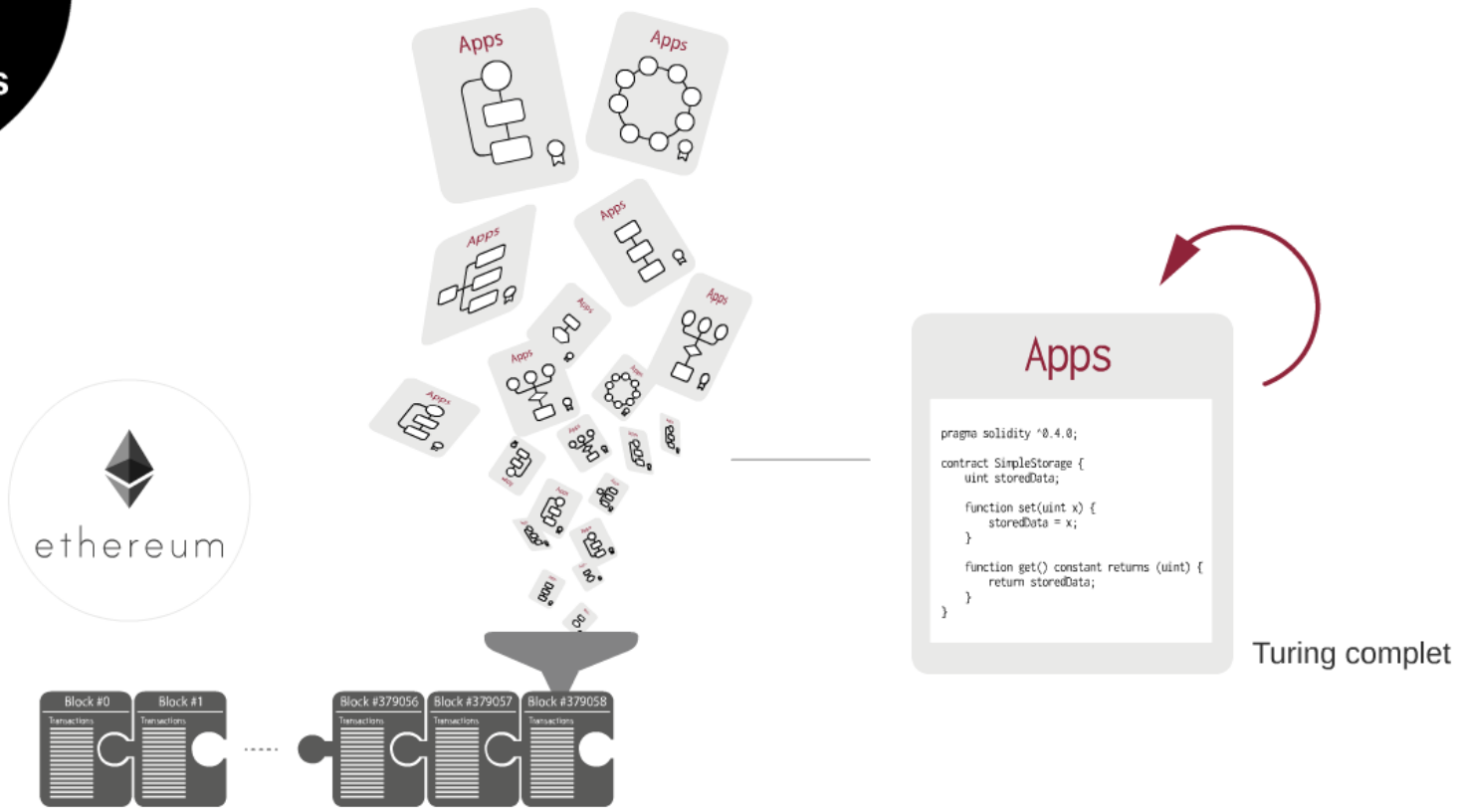
100% transactions

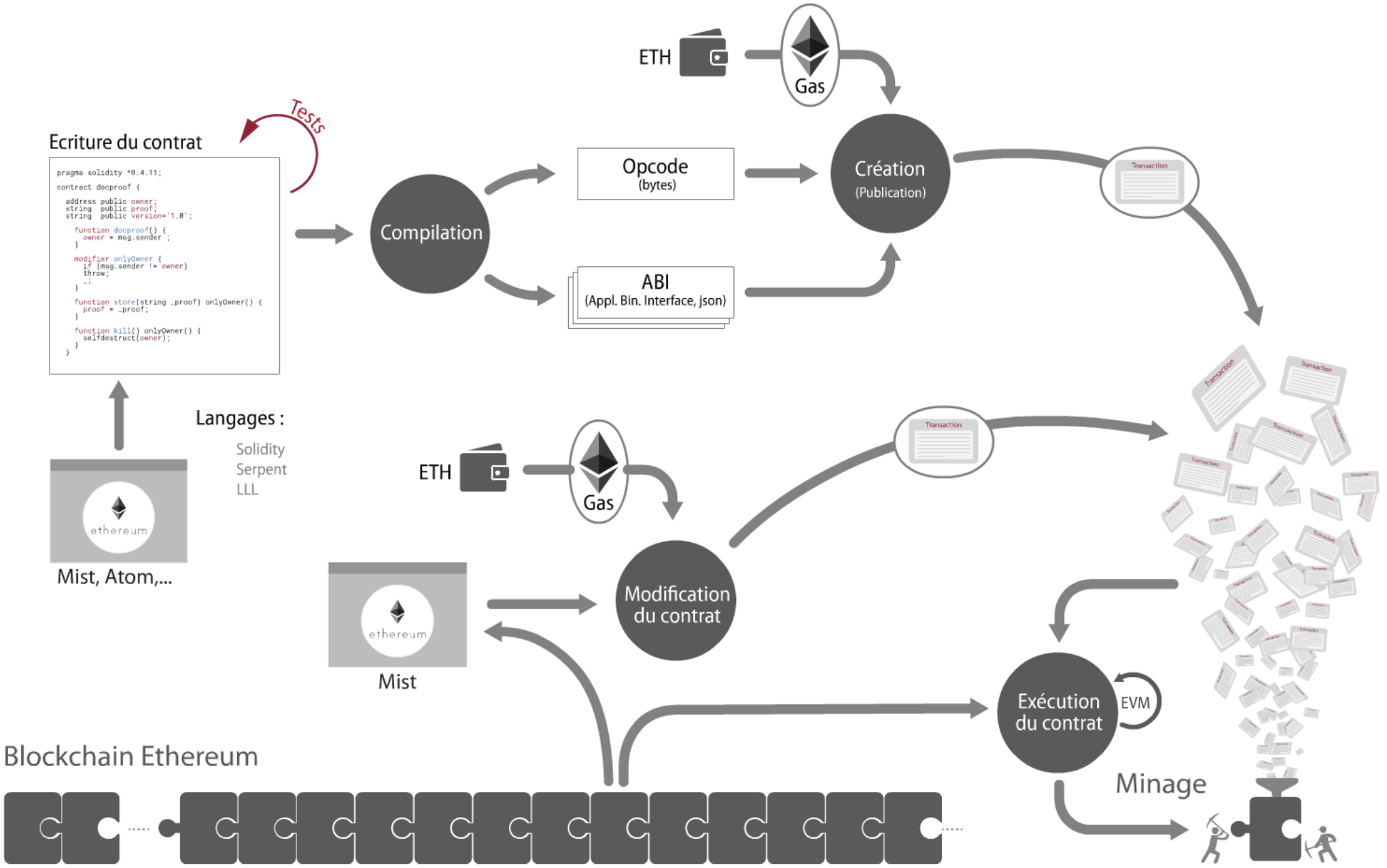




Exemple : OP_DUP OP_HASH160 39ee7f7d4c80307d27e7657cbfef0d48d0eb84e5 OP_EQUALVERIFY OP_CHECKSIG

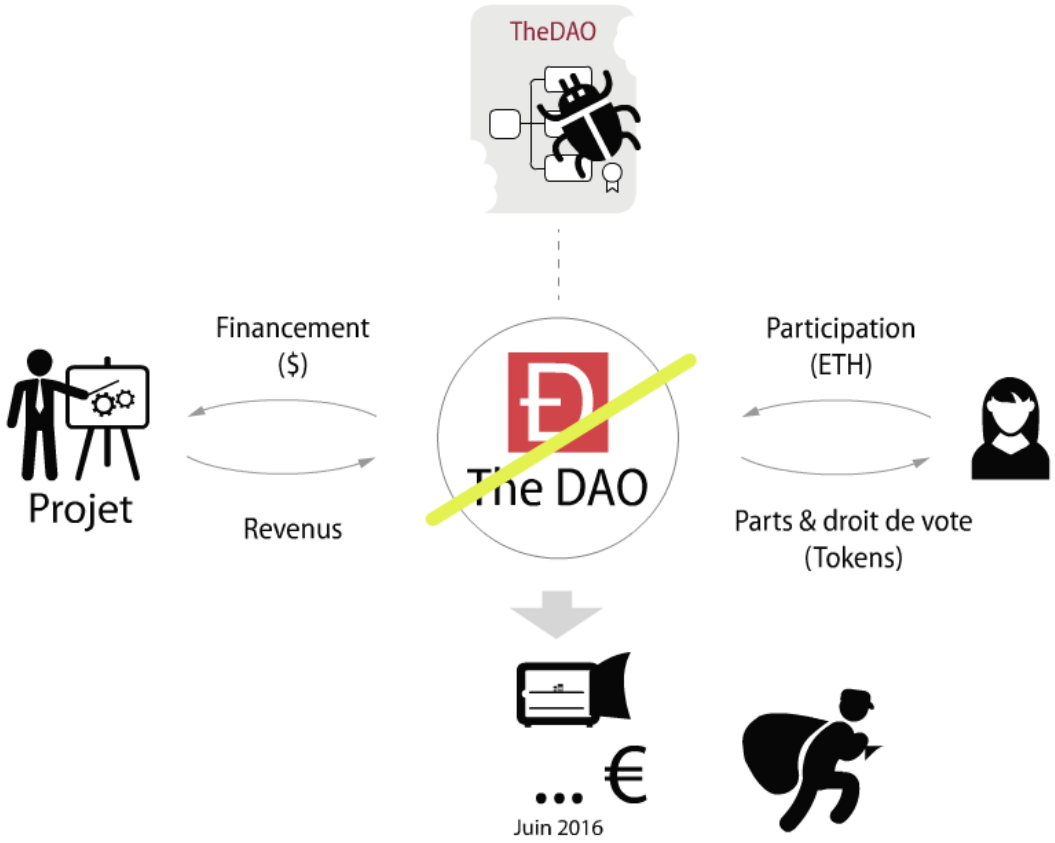
Ethereum
Smart & Contracts




ETH
Gas
Tests
Ecriture du contrat
pragma solidity ^0.4.11;
contract docproof {
address public owner;
string public proof;
string public version='1.0';
function docproof() {
owner = msg.sender ;
}
modifier onlyOwner {
if (msg.sender != owner)
throw;
_;
}
function store(string _proof) onlyOwner() {
proof = _proof;
}
function kill() onlyOwner() {
selfdestruct(owner);
}
}
Compilation
Opcode
(bytes)
ABI
(Appl. Bin. Interface, json)
Création
(Publication)
Transaction
Langages :
Solidity
Serpent
LLL
ethereum
Mist, Atom,...
ETH
Gas
Transaction
Modification
du contrat
ethereum
Mist
Exécution
du contrat
EVM
Minage
Blockchain Ethereum

DAO*

Organisation Autonomes Décentralisées



(*) Decentralized Autonomous Organization

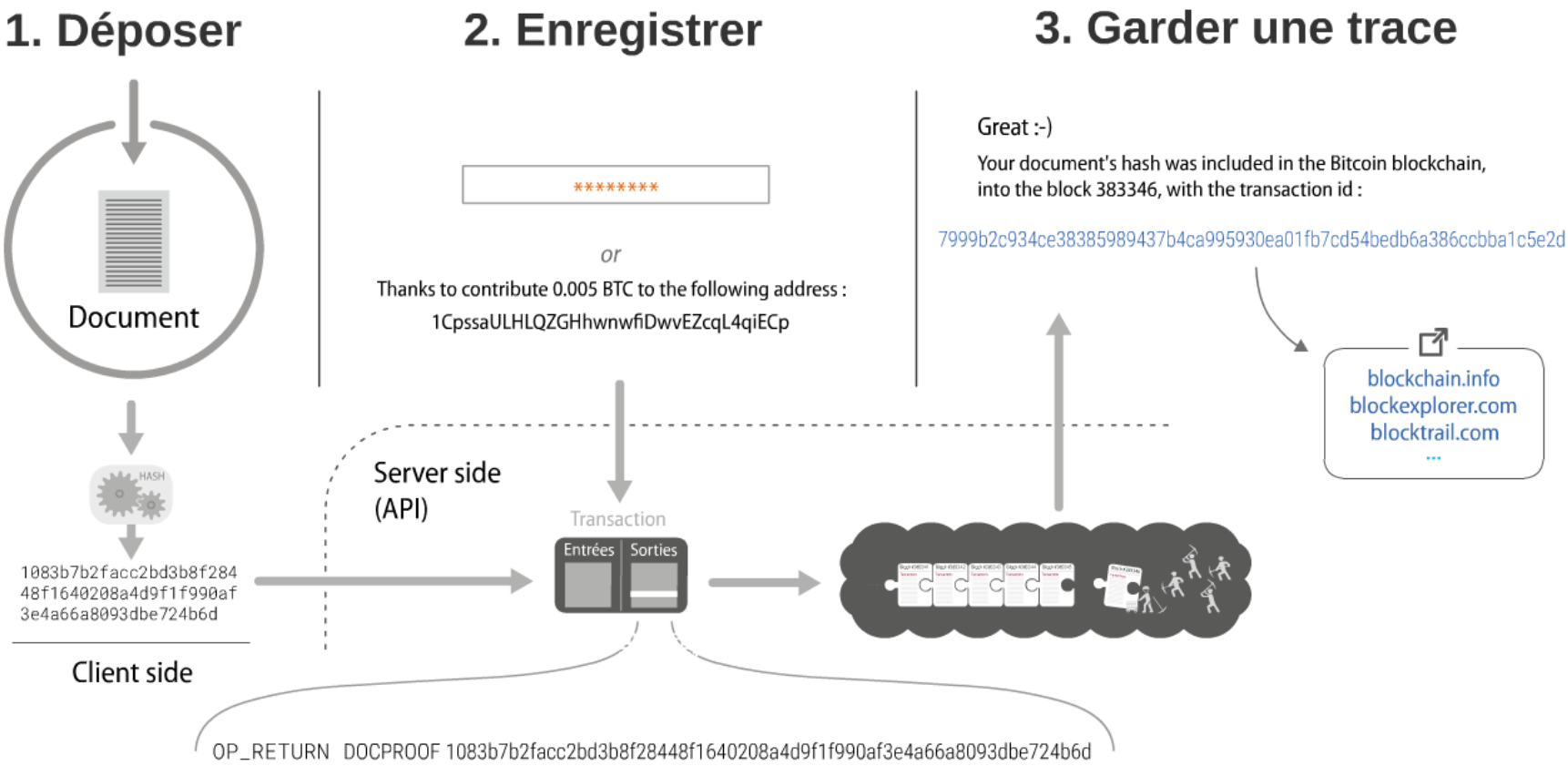
docproof

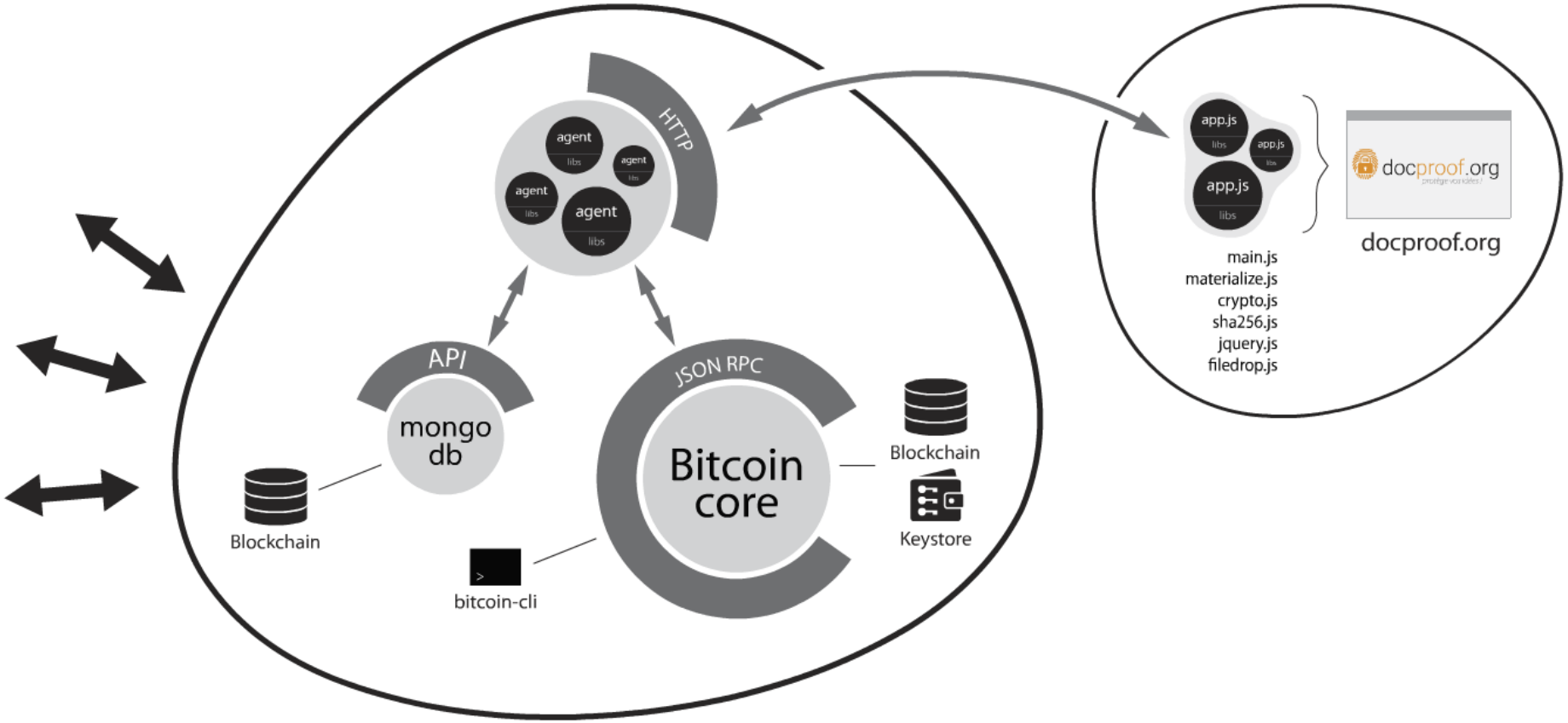
une solution de consignation numérique

docproof.org 1.0

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

Principe


1. Déposer
2. Enregistrer
3. Garder une trace
Document
HASH
1083b7b2facc2bd3b8f284
48f1640208a4d9f1f990af
3e4a66a8093dbe724b6d
Client side
****
or
Thanks to contribute 0.005 BTC to the following address :
1CpssaULHLQZGHhwnwfiDwvEZcqL4qiECp
Server side
(API)
Transaction
Entrées
Sorties
Great :-)
Your document's hash was included in the Bitcoin blockchain,
into the block 383346, with the transaction id :
7999b2c934ce38385989437b4ca995930ea01fb7cd54bedb6a386ccbba1c5e2d
blockchain.info
blockexplorer.com
blocktrail.com
...
OP_RETURN DOCPROOF 1083b7b2facc2bd3b8f28448f1640208a4d9f1f990af3e4a66a8093dbe724b6d


HTTP
agent
libs
agent
libs
agent
libs
agent
libs
API
mongo
db
JSON RPC
Bitcoin
core
Blockchain
Blockchain
Keystore
bitcoin-cli
app.js
libs
app.js
libs
app.js
libs
docproof.org
docproof.org
main.js
materialize.js
crypto.js
sha256.js
jquery.js
filedrop.js


Mise
en œuvre
& retour
d'expérence

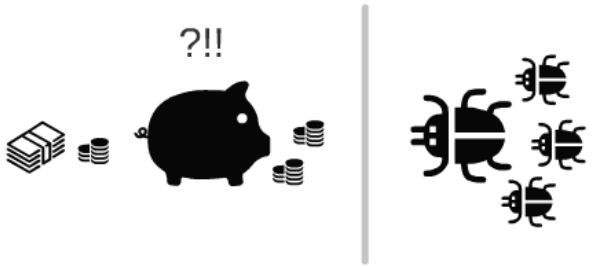
It works !

BTC : 37 Mds €
ETH : 23 Mds €

Mise en oeuvre

Blockchain de test

- Bitcoin / testnet
  https://en.bitcoin.it/wiki/Testnet
- Ethereum / ropsten
  https://github.com/ethereum/ropsten



Blockchain privée

- Indépendante et locale
- Bitcoin core : regtest mode
  https://bitcoin.org/en/developer-examples#regtest-mode
- go-ethereum : private network
  https://github.com/ethereum/go-ethereum

Points de départ ?

Projet
https://ethereum.org/

Yello paper (description formelle)
https://github.com/ethereum/yellowpaper

Github
https://github.com/ethereum/

Ethereum Wiki
https://github.com/ethereum/wiki/wiki

Homestead documentation
http://www.ethdocs.org

Solidity language
https://solidity.readthedocs.io/en/develop/

Go Ethereum

Racine
https://geth.ethereum.org/

Wiki
https://github.com/ethereum/go-ethereum/wiki

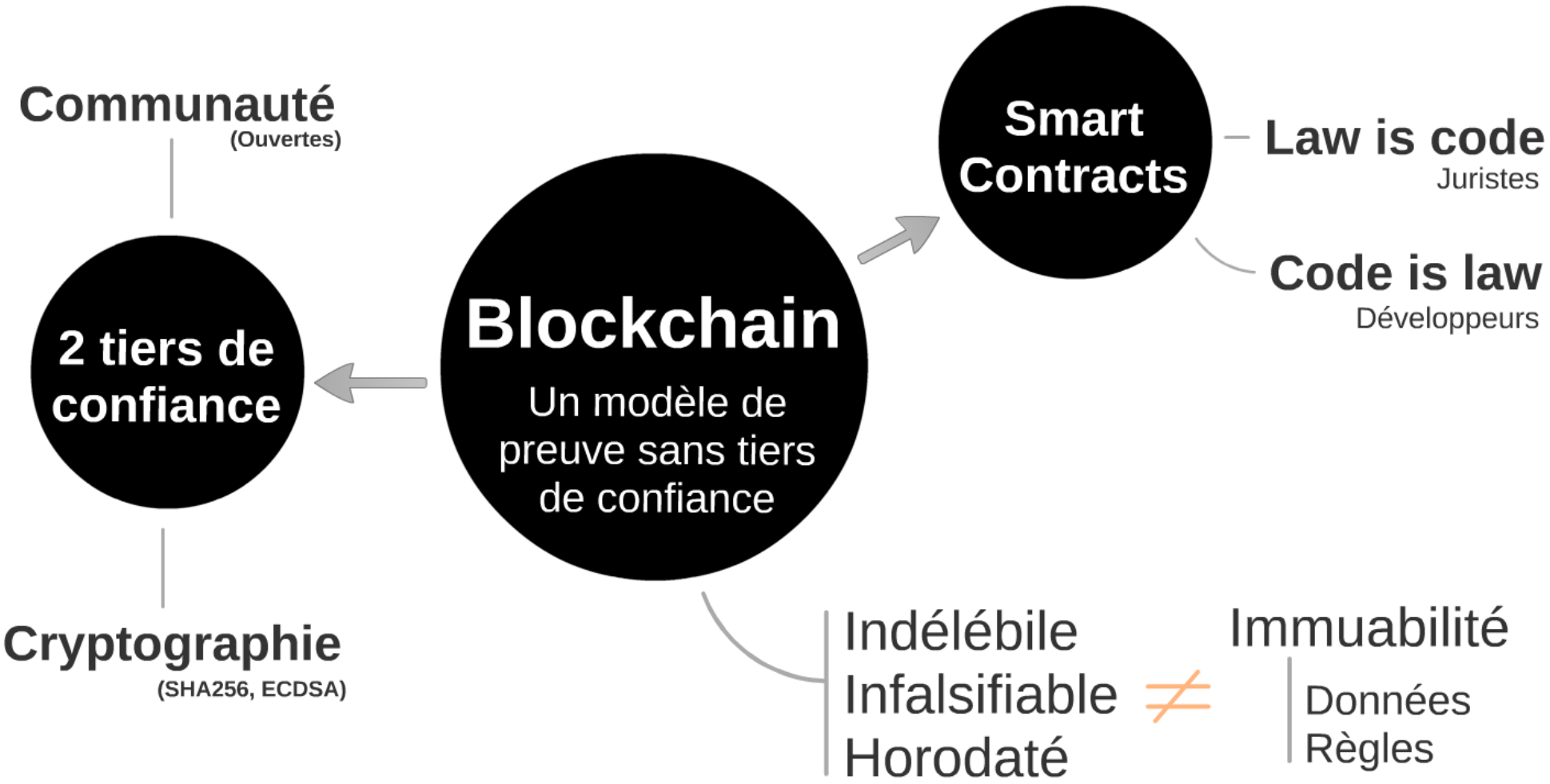
github
https://github.com/ethereum/go-ethereum

Mist

Github
https://github.com/ethereum/mist/releases

Perspectives

...et limites ?


Communauté
(Ouvertes)
2 tiers de confiance
Cryptographie
(SHA256, ECDSA)
Blockchain
Un modèle de preuve sans tiers de confiance
Smart Contracts
Law is code
Juristes
Code is law
Développeurs
Indélébile
Infalsifiable
Horodaté
≠
Immuabilité
Données
Règles


...des
questions ?

Blockchain

Applications et Organisations Décentralisées Autonomes - dApp & DAO

JDEV2017