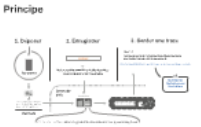
JSSI 2016

Paris,
8 mars
2016





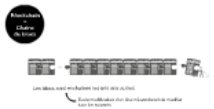


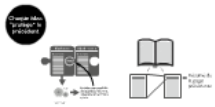


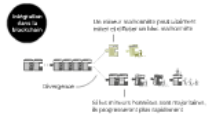



questions ?







# JOURNEE DES SYSTEMES D'INFORMATION 2016

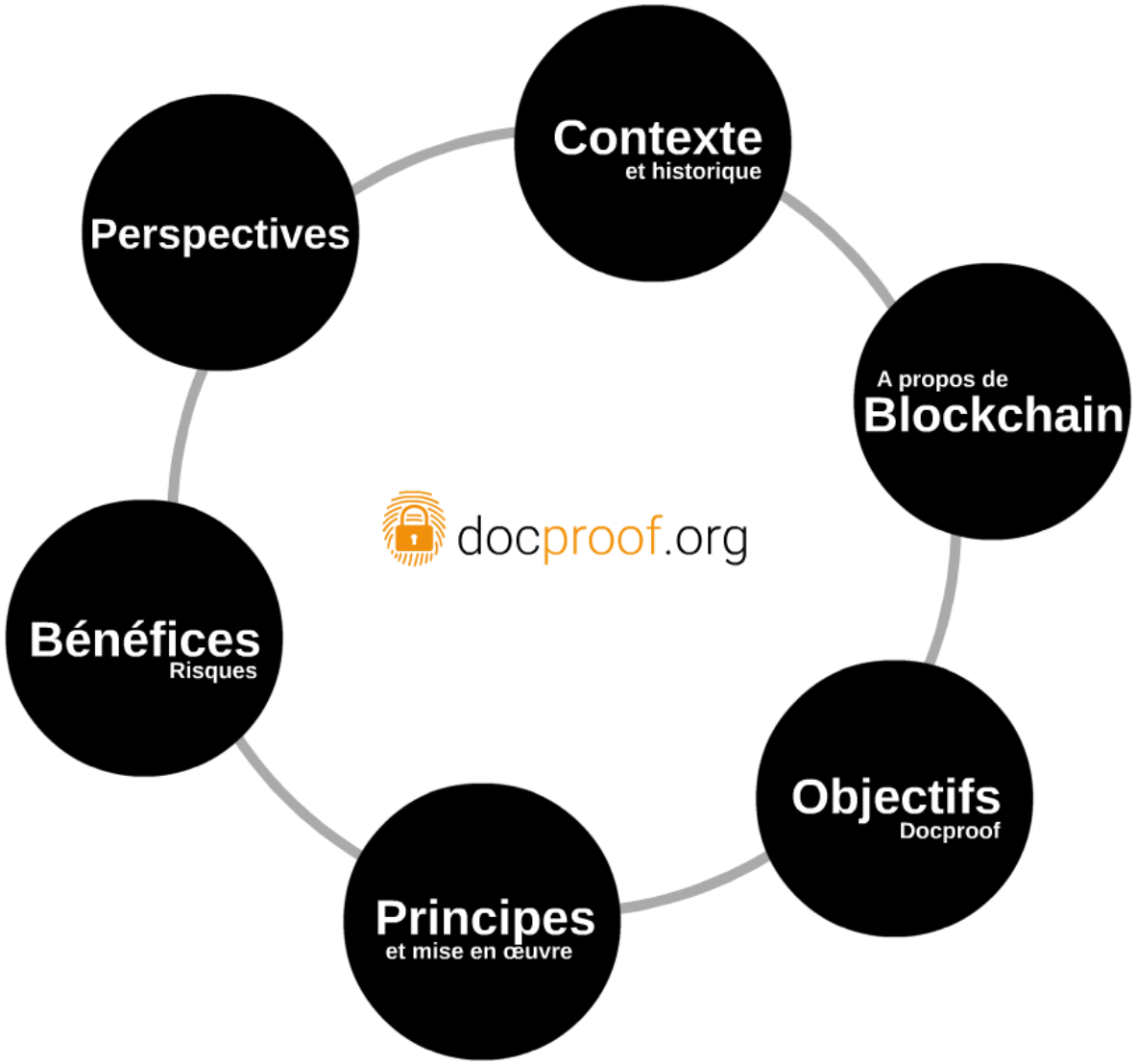
v2.0

# De la Confiance À LA Preuve...

Un service de notariat électronique basé sur la technologie blockchain

## JSSI 2016

Jean-Luc Parouty - CNRS / Institut de Biologie Structurale (IBS)


Contexte
et historique
A propos de
Blockchain
Objectifs
Docproof
Principes
et mise en œuvre
Bénéfices
Risques
Perspectives
docproof.org

# Contexte & historique

Projet académique*
Institut de Biologie Structurale

CEA
CNRS
UGA

Veille technologique & Besoins internes

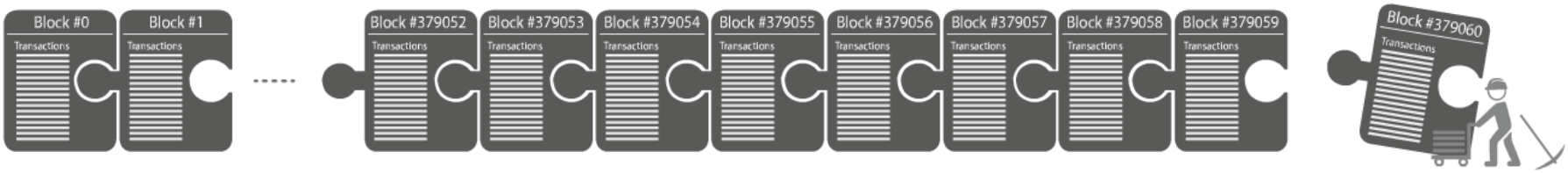
Blockchain

Notariat électronique

(*) Présentations JRES2015, JSSI2016

# Une blockchain, c'est quoi ?

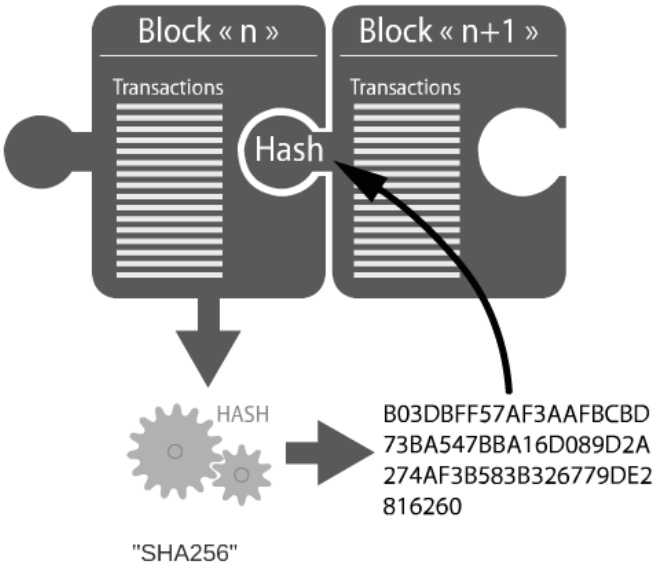
**Blockchain**
**=**
**Chaine de blocs**

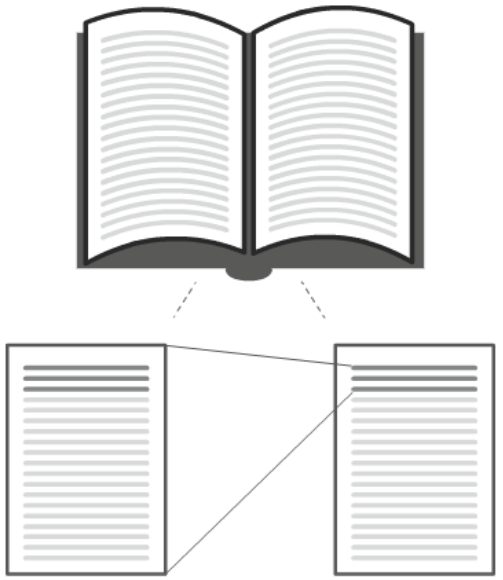



Les blocs sont enchaînés les uns aux autres

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

**Chaque bloc "protège" le précédent**

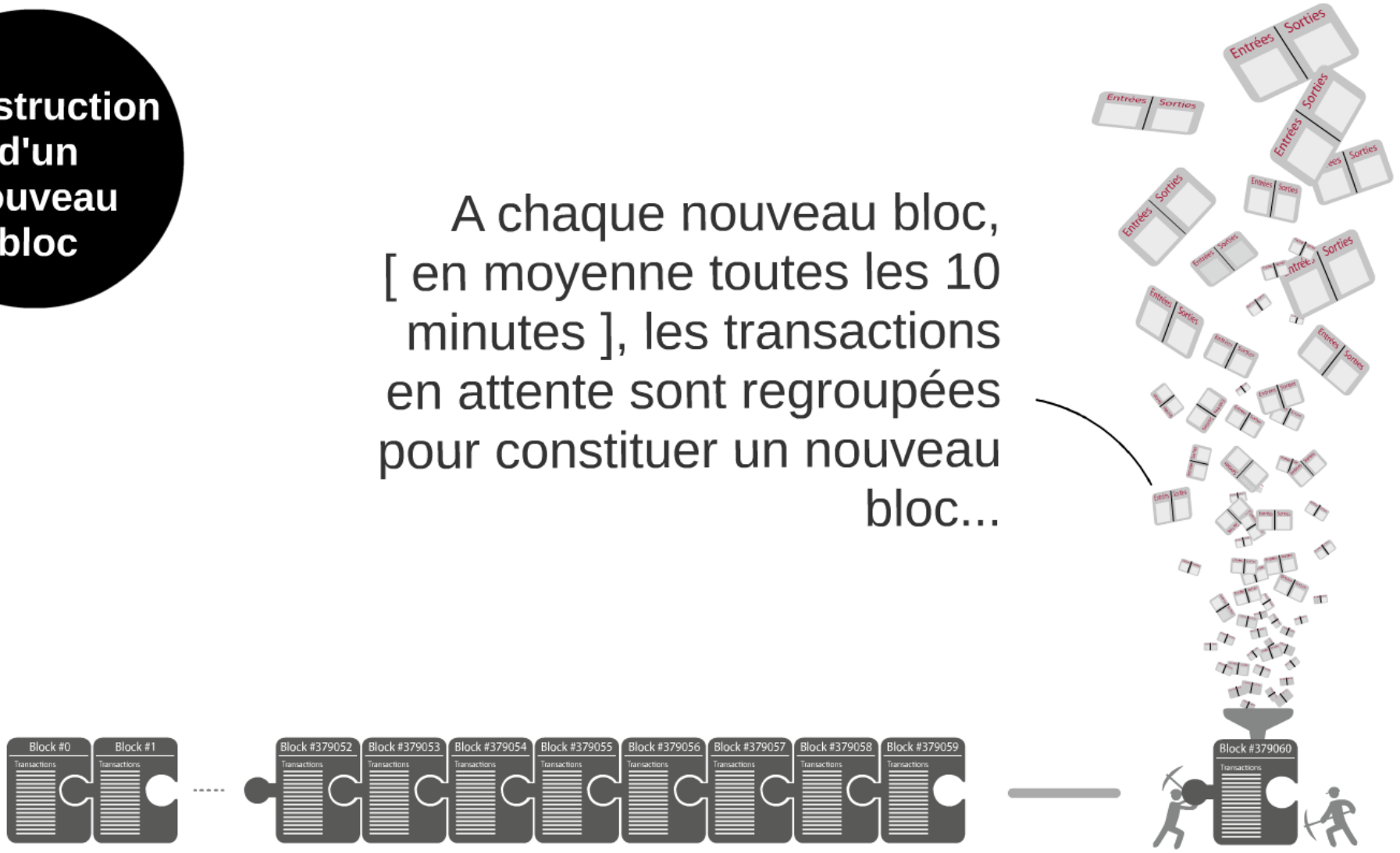


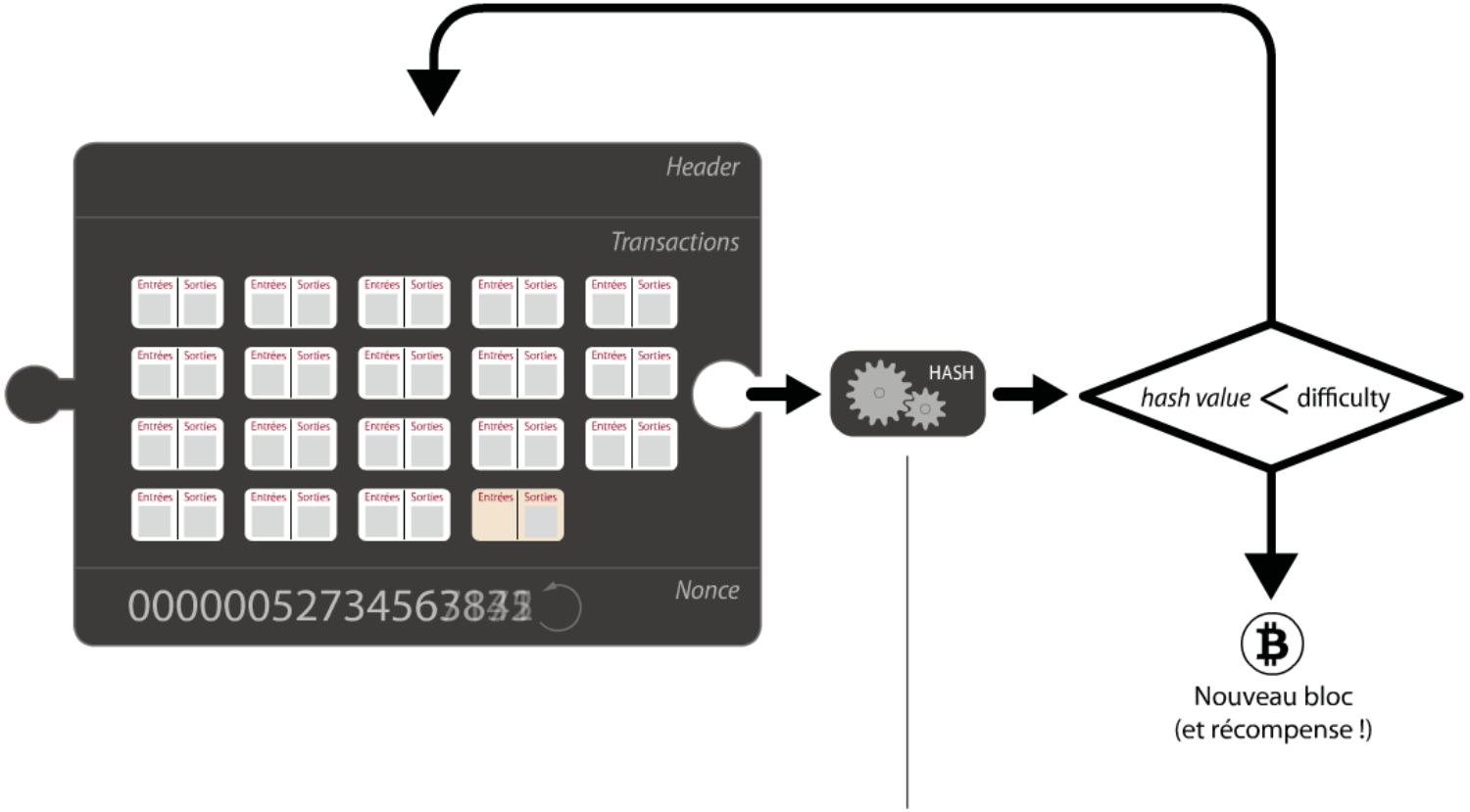
Résumé de la page précédente

## Construction d'un nouveau bloc

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



# Principe de la preuve par le travail

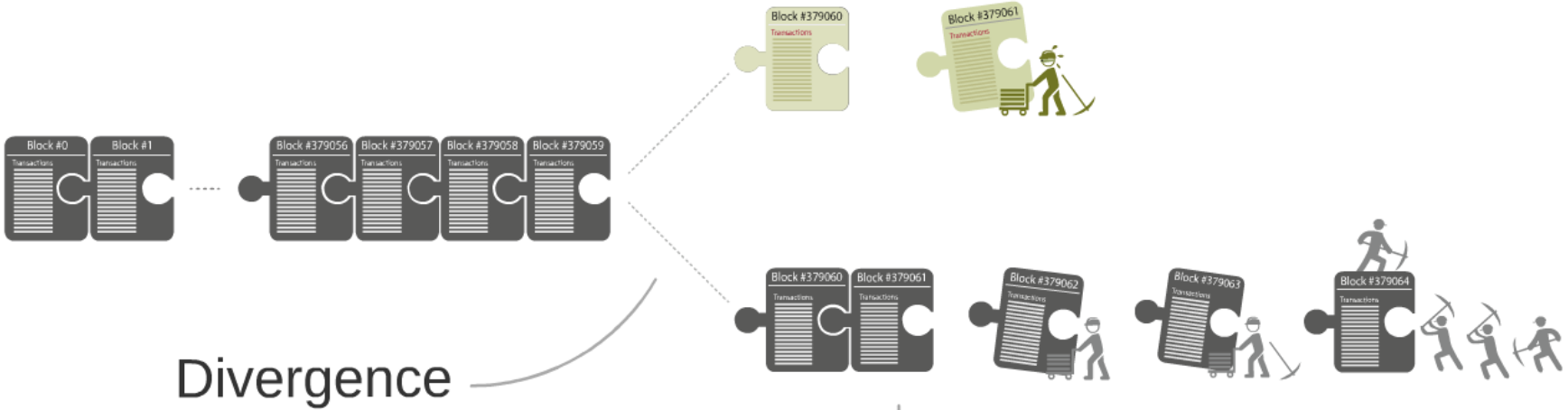



Exemple :
0000000000000002be4d6e740fa56cb6a00be18e7d8319c618b80f6fff22ec

0000000000000002be4d6e740fa56cb6a00be18e7d8319c618b80f6fff22ec

## Intégration dans la blockchain

Un mineur malhonnête peut aisément miner et diffuser un bloc malhonnête




Divergence

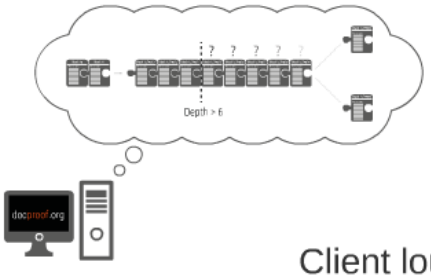
Si les mineurs honnêtes sont majoritaires, ils progresseront plus rapidement

ils progresseront plus rapidement

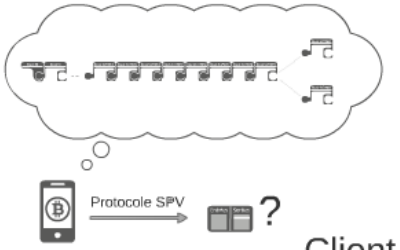
**Vérification**

La transaction est-elle dans la blockchain ?

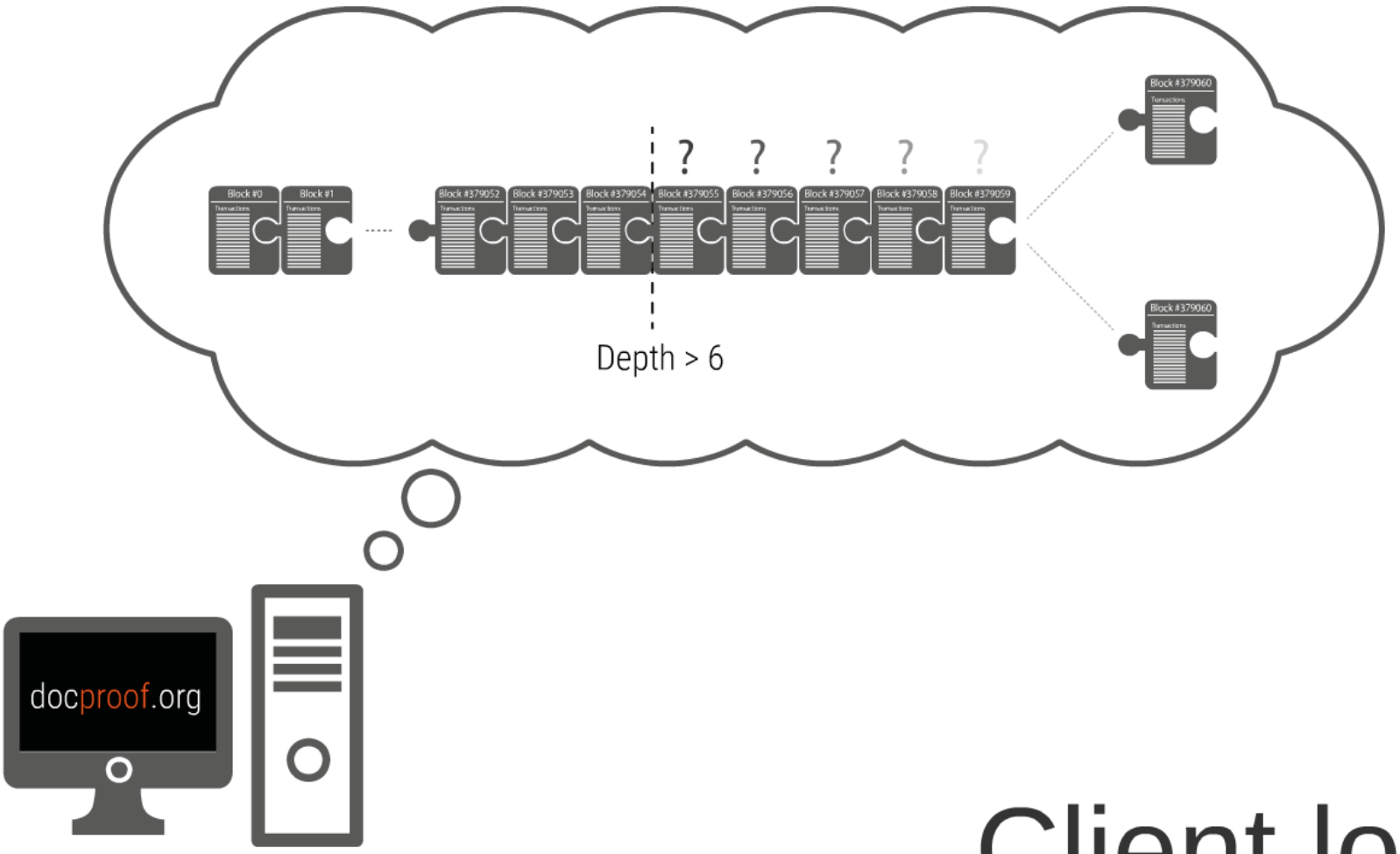

La sortie a-elle été dépensée ?



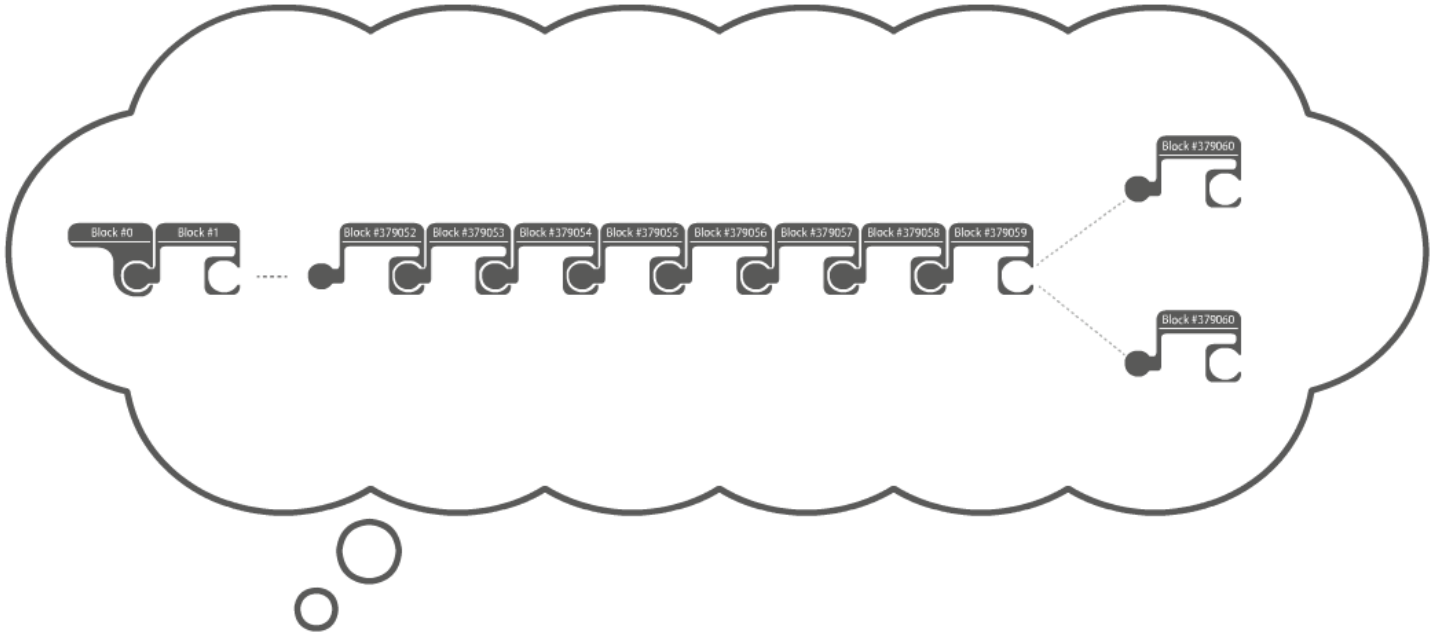

Client lourd

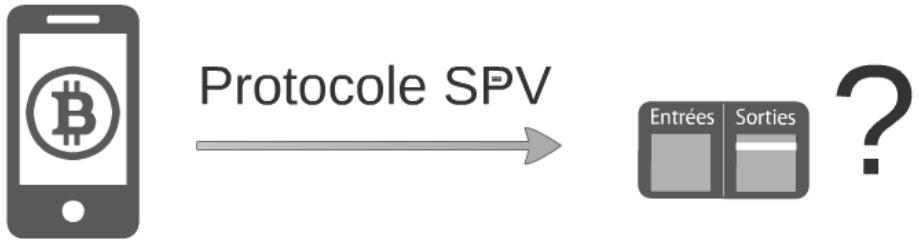



Client léger

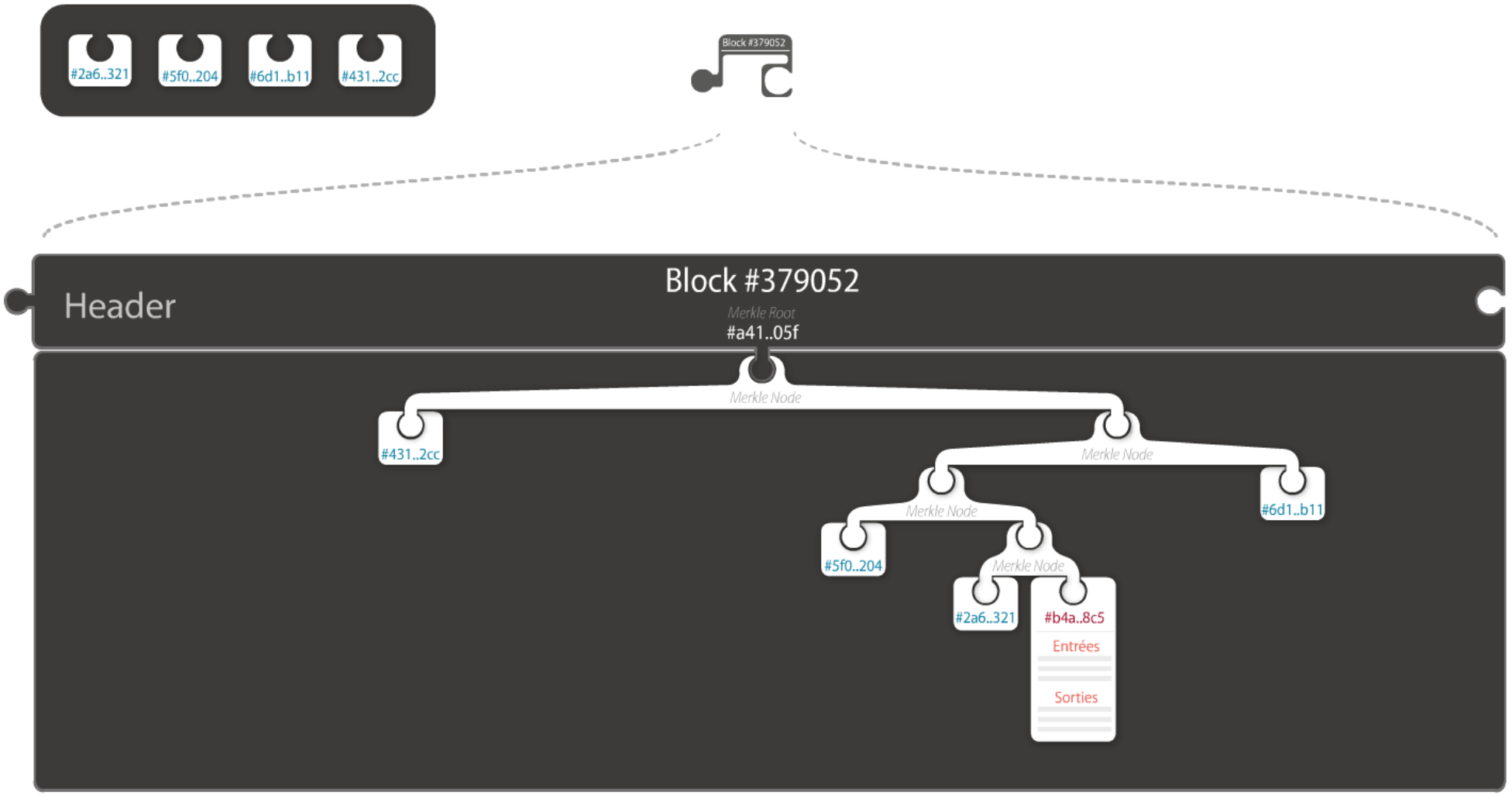



# Client lourd




# Client léger


#2a6..321
#5f0..204
#6d1..b11
#431..2cc
Block #379052
Header
Block #379052
Merkle Root
#a41..05f
Merkle Node
#431..2cc
Merkle Node
Merkle Node
#6d1..b11
#5f0..204
Merkle Node
#2a6..321
#b4a..8c5
Entrées
Sorties

# Une blockchain, c'est quoi ?


Communauté
Ouvertes
2 tiers de confiance
Un modèle de preuve sans tiers de confiance
Cryptographie
SHA256, ECDSA
Indélébile
Infalsifiable
Horodaté

# Objectifs

docproof.org

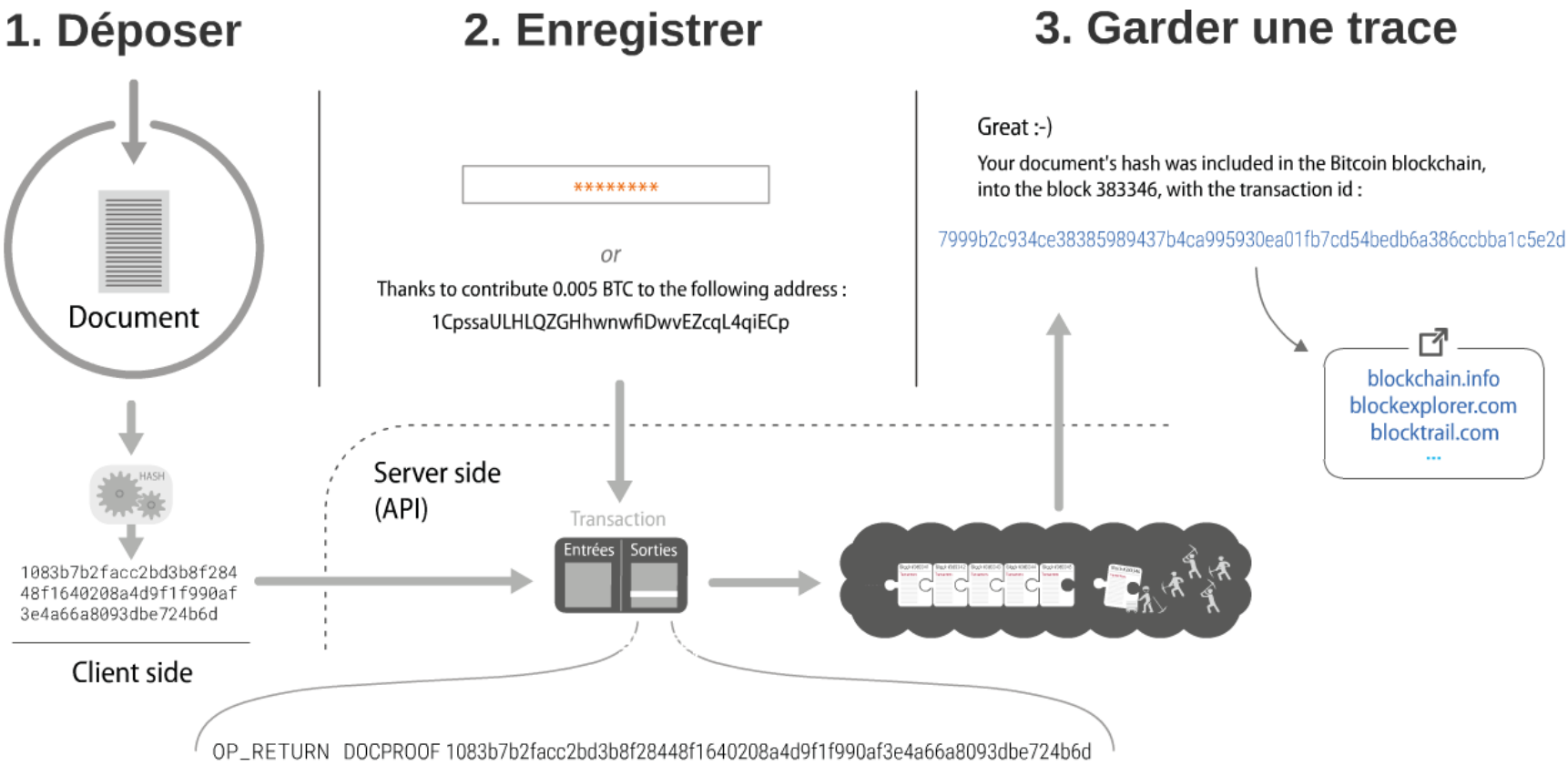
Enregistrement de preuves d'antériorité

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

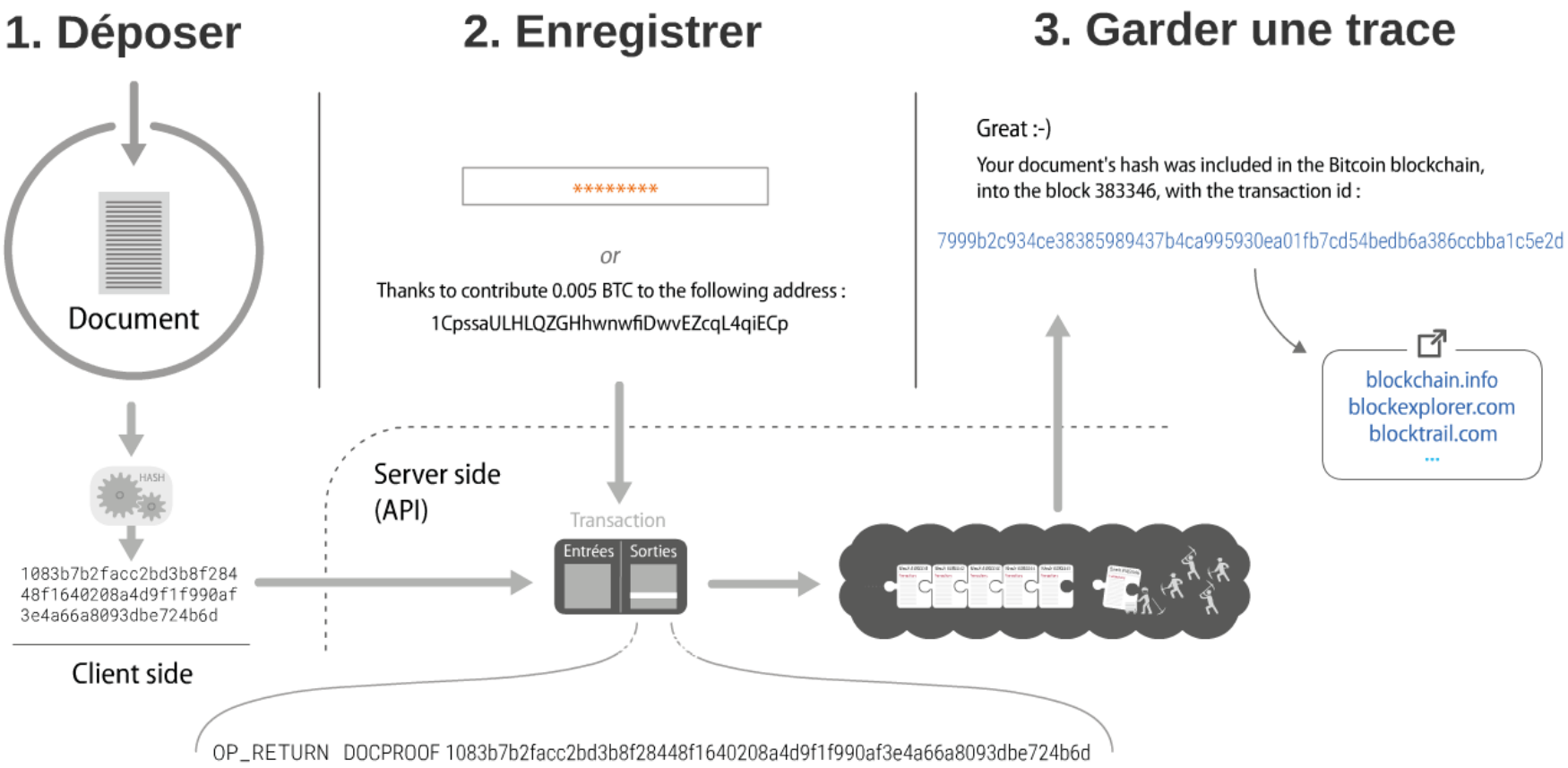
Démonstrateur / blockchain

Modèle de confiance -> Preuve

# 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

# 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

Une petite
démonstration
Vaut toujours
PLUS que 1000 Mots !

docproof.org

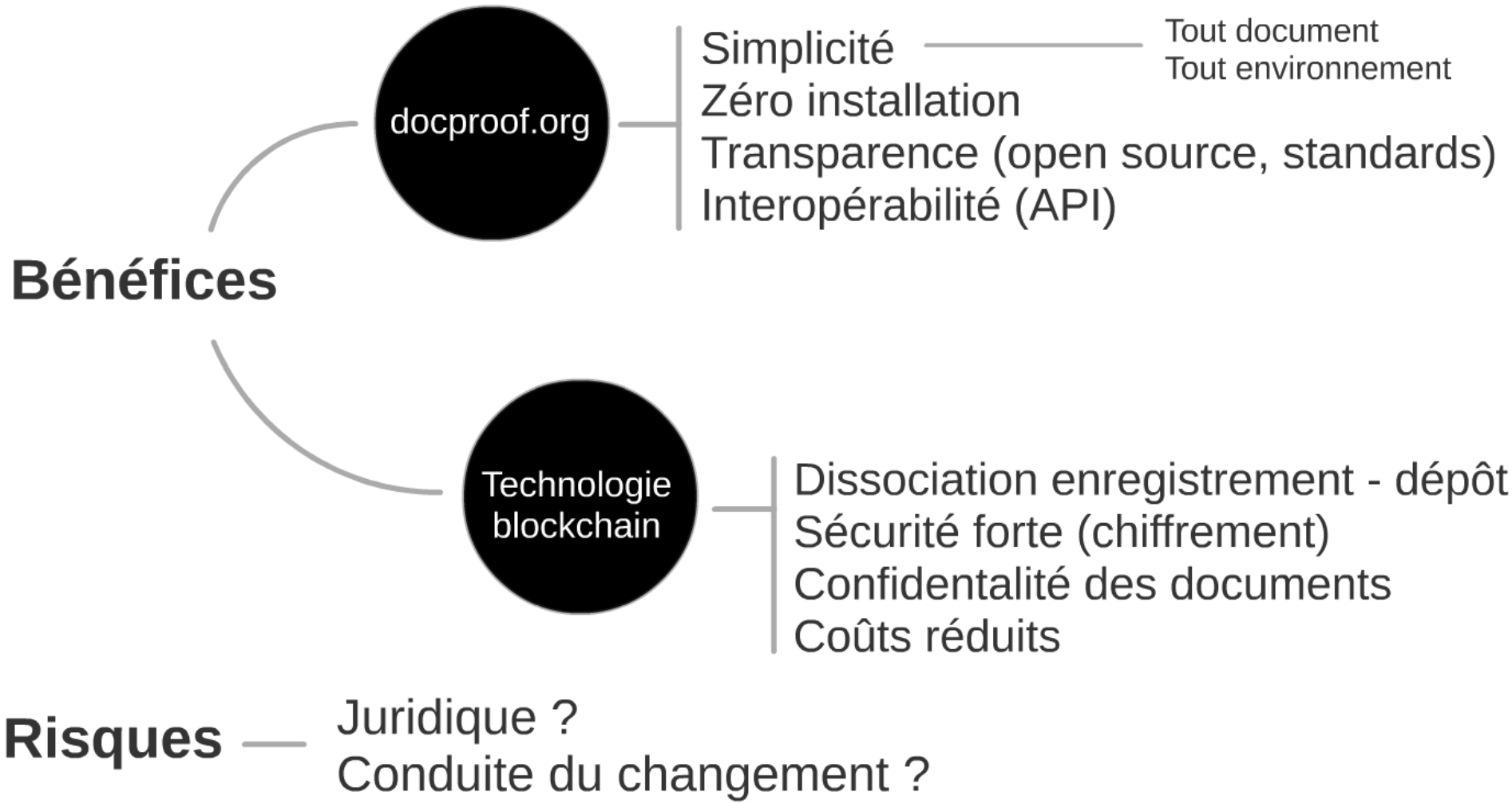
# Aspects juridiques

« L'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous. »

Article L.111-1, Code de la propriété intellectuelle

Preuve d'antériorité

- Preuve d'existence de l'œuvre
- et
- Identité du créateur


docproof.org
Simplicité
Tout document
Tout environnement
Zéro installation
Transparence (open source, standards)
Interopérabilité (API)
Bénéfices
Technologie blockchain
Dissociation enregistrement - dépôt
Sécurité forte (chiffrement)
Confidentalité des documents
Coûts réduits
Risques
Juridique ?
Conduite du changement ?

## Bénéficiaires

Toute personne ou organisation soucieuse de protéger une "oeuvre de l'esprit"

Données, logs, documents, objets, oeuvres, ...

## Perspectives

# Perspectives

**court terme**


**Communautés**
artistiques, scientifiques,
administratives, etc.

**Usages**
Propriété intellectuelle, preuve de dépôt,
consignation, etc.

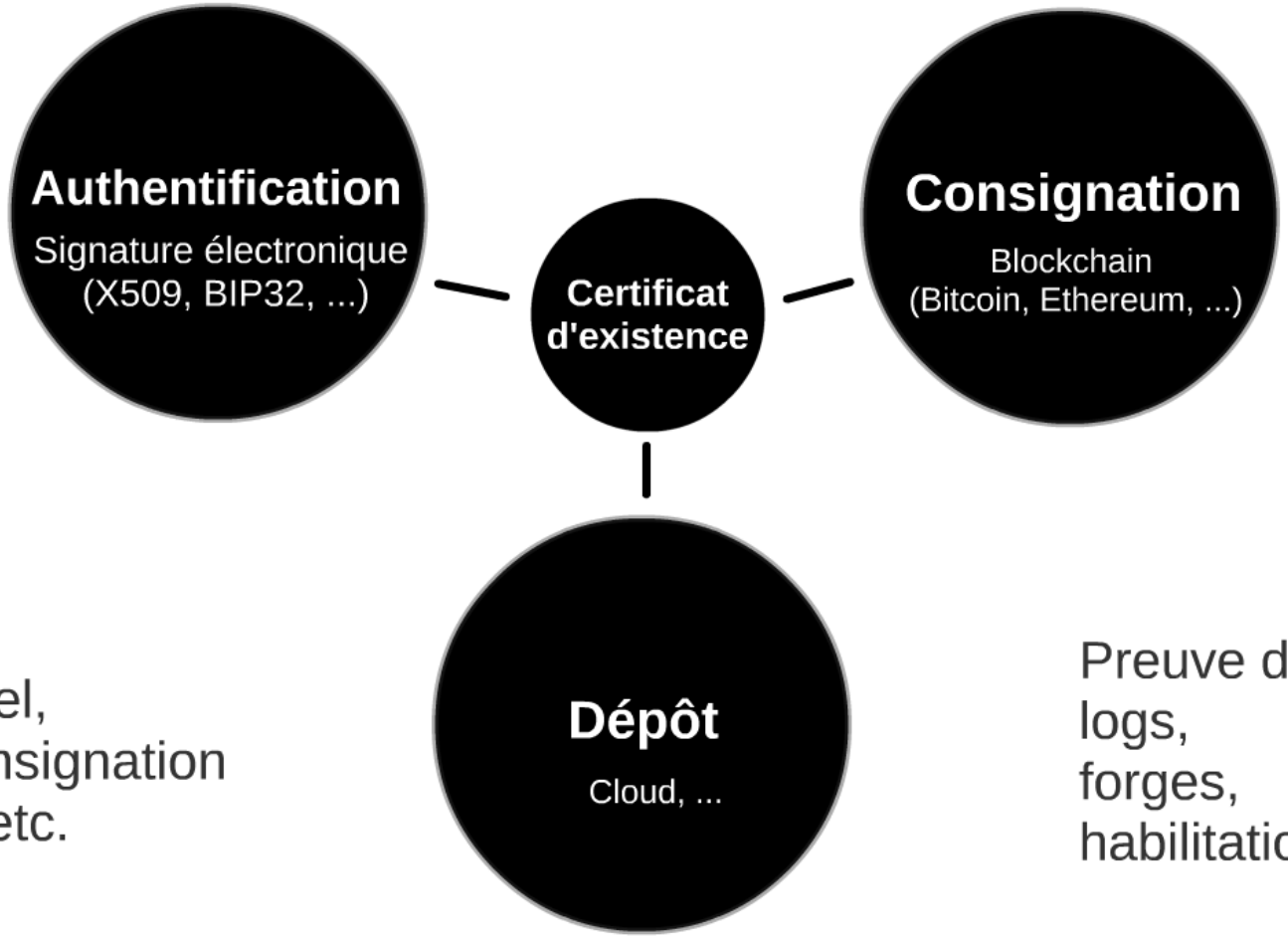

Hébergement — Conventions,
Partenariats, ...

Évolution

**#opportunité**

# Perspectives

**moyen/long terme**




Journal officiel,
cadastre, consignation
de diplôme, etc.

Preuve de données,
logs,
forges,
habilitations, ...

...des

# questions ?