Cas d'usage d'une blockchain - Démonstrateur

Prouver l'antériorité d'un contenu via une blockchain publique

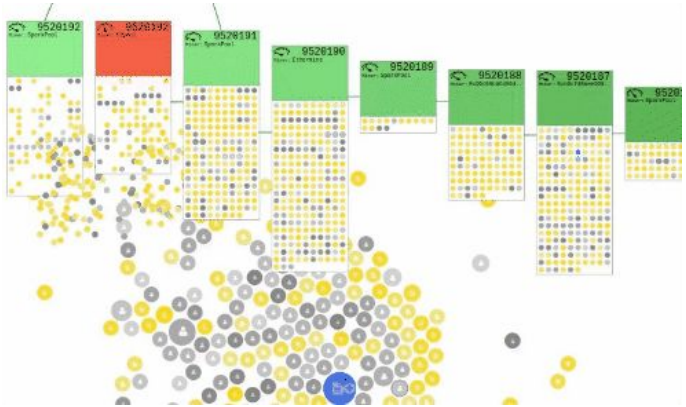
Gevrey-Chambertin Paris Lyon Dijon Nantes

atol Conseils & Développements

Cas d’usage d’une blockchain - Démonstrateur

Les concepts des blockchains sont parfois difficiles à appréhender

- Stockage linéaire, Immuabilité
- Registre distribué, Consensus
- Transparence, Sécurisation, Crypto
- Smart contract, Oracle de confiance
- ...



ATOL Conseils & Développements

- anime des **événements sur le sujet** : petits-déj’, afterworks, présentations sur demande
- et vous **accompagne** : conseils, ateliers de conception, développements

Cas d'usage d'une blockchain - Démonstrateur

"Un bon exemple vaut mieux qu'un long discours"

Nous avons développé **un démonstrateur** qui permet de **prouver l'antériorité d'une idée, d'une création, etc. via une blockchain publique Ethereum** directement depuis son navigateur.

Ceci est possible sans blockchain, mais :

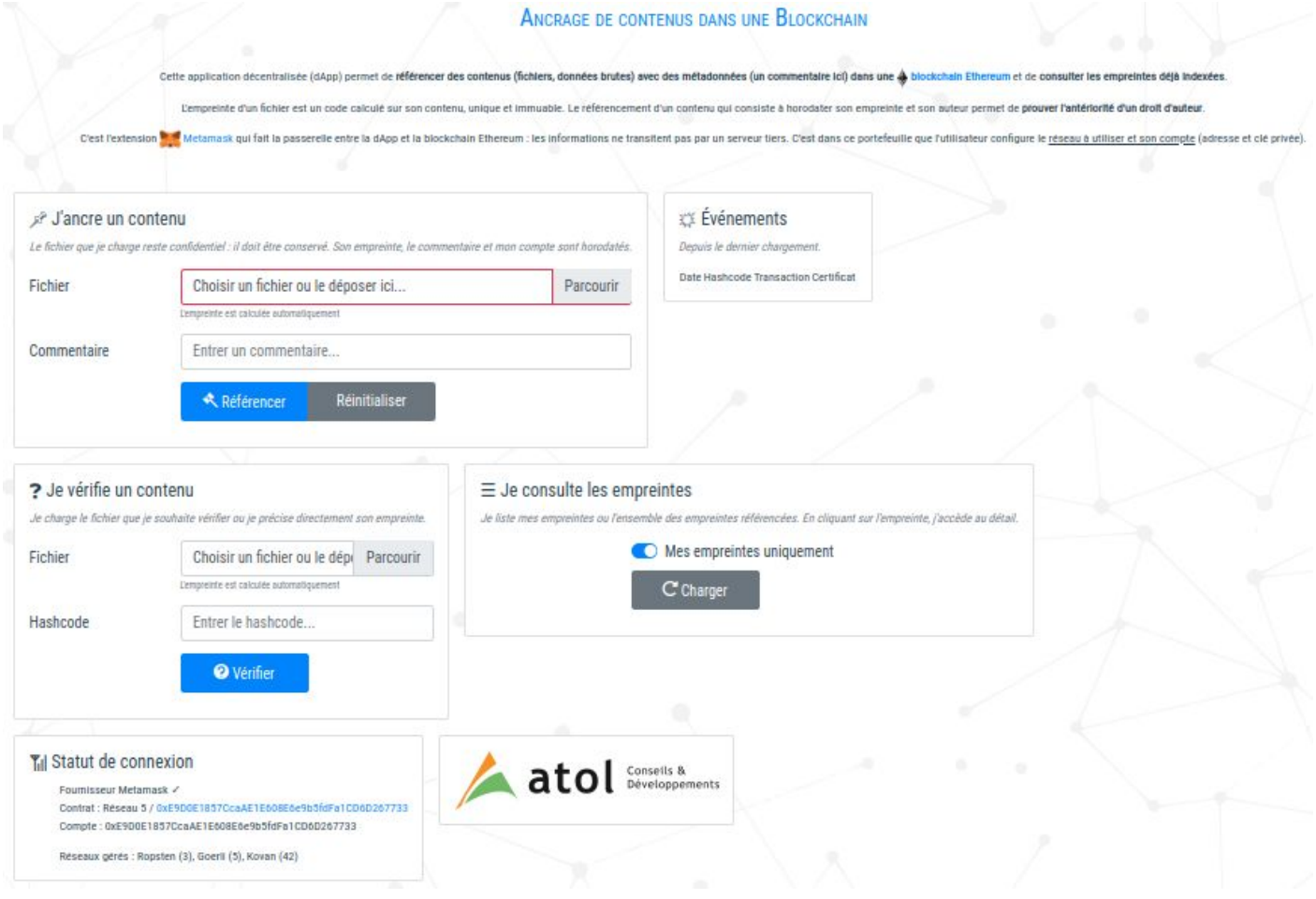
- **Dépendance d'un tiers de confiance**
- **Démarches administratives**
- **Parfois coûteux** selon la méthode employée

Lettre recommandée AR à soi-même, société d'auteurs, constat d'huissier ou acte notarié, …

Avec une blockchain :

- **Le tiers de confiance est la blockchain**
- **Coût faible** d'un enregistrement < *20c€*
- Et **pas d'infrastructure** serveur à mettre en place et à gérer !

Cas d'usage d'une blockchain - Démonstrateur



Cas d’usage d’une blockchain - Démonstrateur

Avant de commencer

Que faut-il savoir ?

Cas d'usage d'une blockchain - Démonstrateur

"L'enregistrement d'une transaction a un coût"

de quelques dixièmes €, qui est exprimé en Ether, l'unité monétaire d'Ethereum.

Il permet de **récompenser le validateur** de la transaction pour sa participation.

*coût transaction = gaz utilisé * prix du gaz*

Plusieurs blockchains Ethereum existent :

- Une blockchain principale pour la production *Mainnet* (1)
- Des blockchains de tests *Testnets* : Ropsten (3), Goerli (5), Kovan (42), etc.

Les Ethers ne valent rien dans **les blockchains de tests : les transactions sont gratuites** !

Cas d'usage d'une blockchain - Démonstrateur

"Metamask représente son portefeuille"

Portefeuille = Compte utilisateur

Il est nécessaire pour **l'interaction avec la blockchain**.

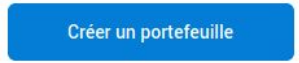
Exemple d'adresse : `0xcC52Ff86BF0335984715EF0C5fa4D664A95e281B`

1. Installation de METAMASK

   Application iOS, Android
   Extension Chrome, Firefox,

   Ou utilisation de Brave

2. Création du portefeuille



   Possibilité de connecter un portefeuille physique (clé USB)

Cas d’usage d’une blockchain - Démonstrateur

“Plusieurs moyens existent pour alimenter son compte”

Lorsqu’on démarre, son portefeuille est vide. On peut recevoir des Ethers :

- **depuis un autre compte**
- à partir d’un **paiement par carte bancaire** (ex : coinhouse.com)
- en passant par un **virement vers une plateforme d’échange** (ex : kraken.com)

Et pour les **blockchains de tests**, on peut en demander gratuitement via “les robinets”

Ex : pour la blockchain Goerli

Plutôt commode pour les tests !

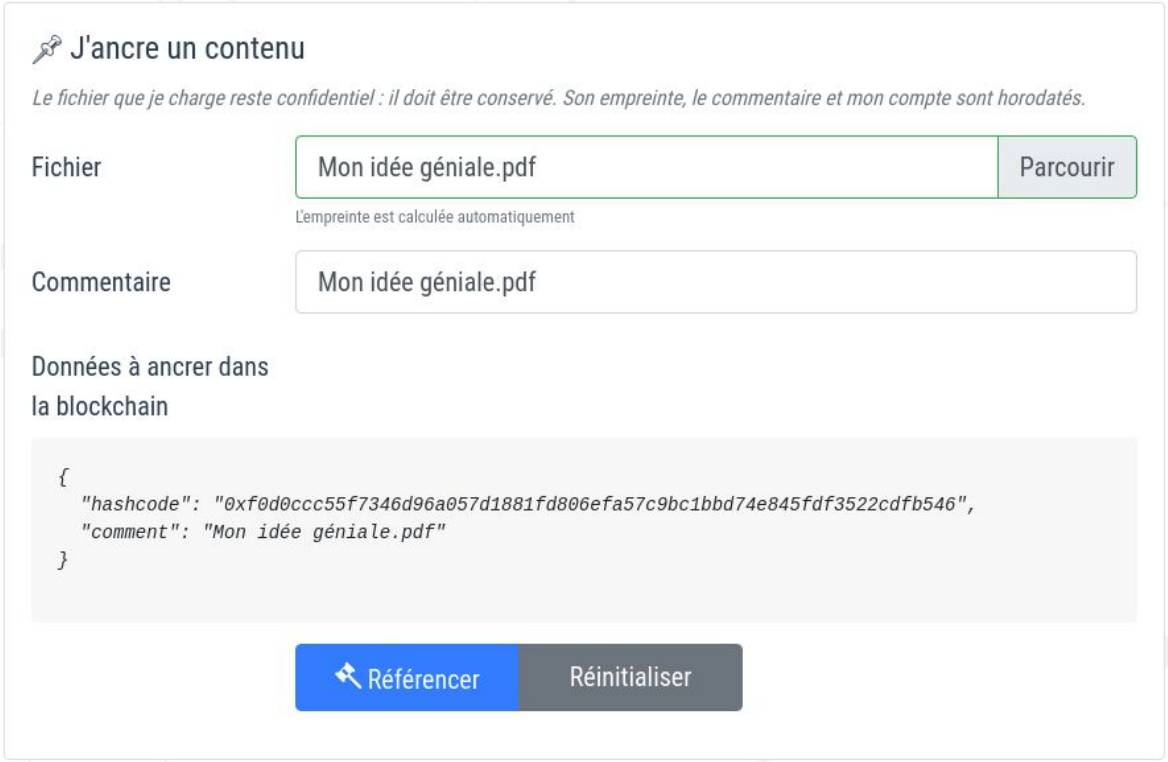
Cas d’usage d’une blockchain - Démonstrateur

Comment enregistrer son document ?

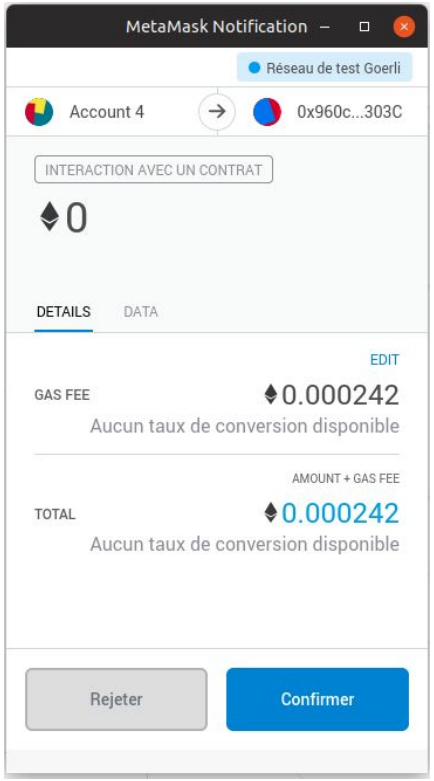
et lui associer un commentaire

Cas d'usage d'une blockchain - Démonstrateur

1. Chargement d'un fichier et commentaire



2. Consentement transaction



Cas d’usage d’une blockchain - Démonstrateur

Transaction

0x22c3b344e267028f310bedbe62b4faed57e52085ea1dbd1523e1c116588b3031

Lorsqu'elles sont validées, les transacions apparaissent dans le bloc "événements". Veuillez récupérer le certificat afin de le conserver avec le document.

Informations publiques :

- Bloc
- Horodatage
- Initiateur
- Données transmises

[Lien vers la transaction (données brutes)]

Transaction Details

Overview | Event Logs (1) | State Changes New

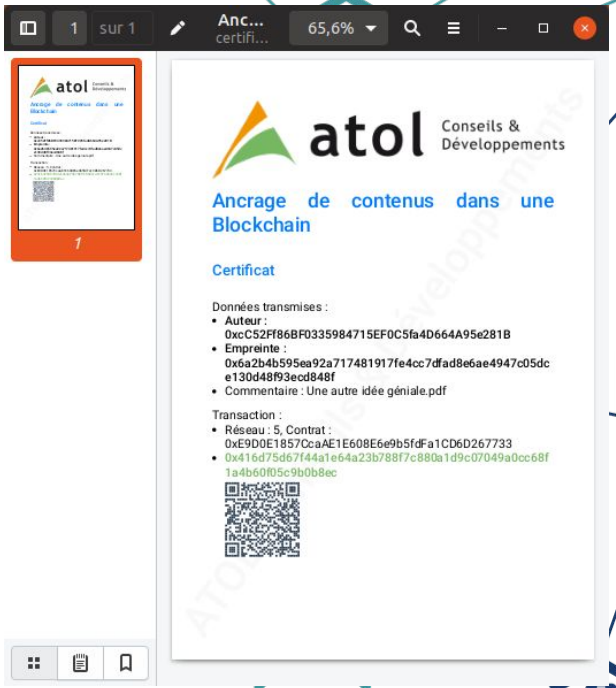
[This is a Goerli **Testnet** transaction only]

Transaction Hash:	**0x22c3b344e267028f310bedbe62b4faed57e52085ea1dbd1523e1c116588b3031**
Status:	Success
Block:	1491353 2 Block Confirmations
Timestamp:	32 secs ago (Oct-18-2019 08:56:52 AM +UTC)
From:	0xcc52ff86bf0335984715ef0c5fa4d664a95e281b
To:	Contract 0x960c23336e18e5f9144caaf7f0e732190a93303c
Value:	0 Ether ($0.00)
Transaction Fee:	0.000161014 Ether ($0.000000)
Gas Limit:	241,521
Gas Used by Transaction:	161,014 (66.67%)
Gas Price:	0.000000001 Ether (1 Gwei)
Nonce Position	3 1
Input Data:	0xbf3ccf48f0d0ccc55f7346d96a057d1881fd806efa57c9bc1bbd74e845fdf3522cdfb5460000000000000000000000000000000000000000000000000000000000000040000000000000000000000000000000000000000000000000000000000000000164d6f6e206964c3a9652067c3a96e69616c652e70646600000000000000000000000

Cas d'usage d'une blockchain - Démonstrateur

Conservation

- Document
- Certificat pdf



Cas d’usage d’une blockchain - Démonstrateur

Comment vérifier un document ?

date d’enregistrement, commentaire, émetteur

Cas d'usage d'une blockchain - Démonstrateur

? Je vérifie un contenu

Je charge le fichier que je souhaite vérifier ou je précise directement son empreinte.

Fichier: Mon idée géniale.pdf — Parcourir

L'empreinte est calculée automatiquement

Hashcode: 0xf0d0ccc55f7346d96a057d1881fd806efa57c9bc1bbd74e845fdf3522cdfb5

Vérifier

Données ancrées dans la blockchain

```
{
  "hashcode": "0xf0d0ccc55f7346d96a057d1881fd806efa57c9bc1bbd74e845fdf3522cdfb546",
  "comment": "Mon idée géniale.pdf",
  "sender": "0xcC52Ff86BF0335984715EF0C5fa4D664A95e281B",
  "block": "1491353",
  "mineTime": "2019-10-18T08:56:52.000Z"
}
```

☰ Je consulte les empreintes

Je liste mes empreintes ou l'ensemble des empreintes référencées. En cliquant sur l'empreinte, j'accède au détail.

Mes empreintes uniquement

Recharger

Empreinte

0xaee336df71c4cf7f28e2b1415fc70e32a2663bfc4f36bbd5fa28bf5f95791e7a

0xf0d0ccc55f7346d96a057d1881fd806efa57c9bc1bbd74e845fdf3522cdfb546

« ‹ 1 › »

Cas d’usage d’une blockchain - Démonstrateur

“Le démonstrateur est accessible ici”

https://cvagner.keybase.pub/blckchn/ancrage/

Cas d’usage d’une blockchain - Démonstrateur

Comment est-ce construit ?

en savoir plus...

Cas d’usage d’une blockchain - Démonstrateur

Côté serveur

- Utilisation d’une *Blockchain publique Ethereum*
- Développement et déploiement d’*un smart contract*

Nous n’hébergeons aucun serveur !

Interface utilisateur avec la blockchain

- Une interface *dans son navigateur* : html/js/css
- Une extension pour lire ou valider les transactions de la blockchain (consentement)

La page peut être ouverte sur son PC ou déposée sur n’importe quel serveur HTTPS.

Cas d'usage d'une blockchain - Démonstrateur

"Le projet est publié en opensource"

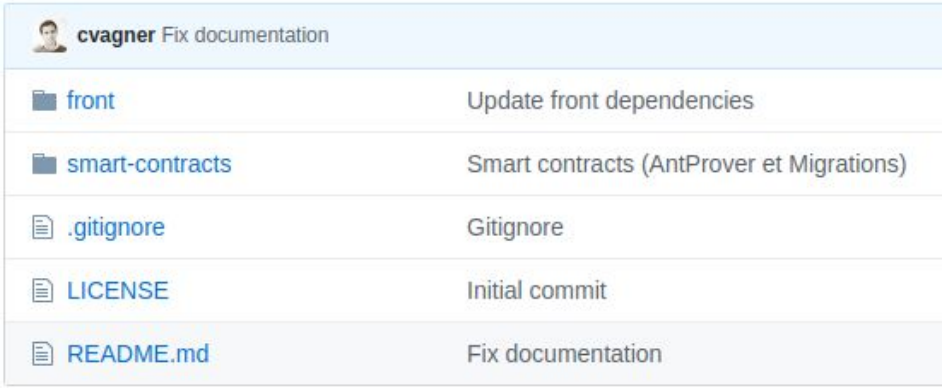
Démarrage rapide des développements

Smart contracts

Webapp

https://github.com/cvagner/blckchn-ant-prover

Licence Apache 2.0



ATOL Conseils et Développements

#puissance et agilité pour votre SI

Gevrey-Chambertin (siège)
ZAE Les Terres d'Or
Route de St philibert
21 220 Gevrey-Chambertin

Atol CD Paris
32 avenue de la République
75 011 Paris

Atol CD Lyon
136 cours Lafayette
69 006 Lyon

Atol CD Dijon
4 bis rue Dr Maret
21 000 Dijon

Nantes
Le 144
144 rue Paul Bellamy
44000 Nantes

Contact
Tél : 03 80 68 81 68
Courriel : contact@atolcd.com
Web : www.atolcd.com

suivez-nous @ATOLCD sur Twitter, Linkedin, Youtube