

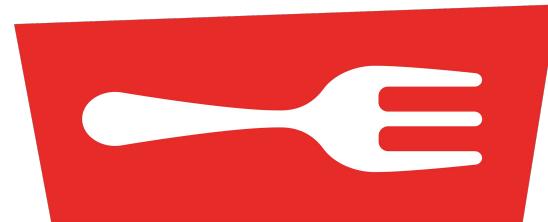
Une expérience

#Block3 - 22 Octobre à La Cuisine Du Web à 18h30

Vos idées en pratique pour le Blockathon

Lors de cet atelier vous allez découvrir comment utiliser la blockchain pour automatiser des processus (smart contrat) et la connecter sur des données extérieurs (utilisation d'oracles). Seront présentés des cas d'usage existants : inspiration pour l'émergence de vos idées pour le hackathon.

Format : 1h30 suivi apéro



Une expérience

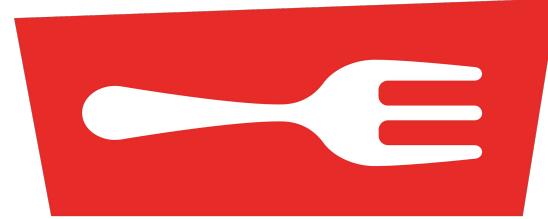
Soirée OnBoarding - 12 novembre à 18h30 à La Cuisine Du Web

Choix des sujets et constitution des équipes.

La veille, tous les participants sont invités à la soirée Ice Breakers. L'objectif est que vous appreniez à vous connaître pour ainsi constituer votre équipe et choisir votre sujet pour le Blockathon. Et bien sur, tout ça en mode fun et convivial !

- 18h30 : Accueil
- 19h : Ice Breaker
- 19h30 : Pitch Time : Pitch ton idée !
- 20h30 : Vote des participants pour les meilleures idées
- 20h45: Constitution des équipes

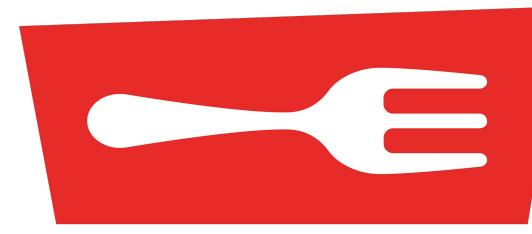
BLOCKATHON : 13 & 14 nov



Une expérience

BLOCKATHON : 13 et 14 novembre 2019

- **Une accompagnement par des coaches tout au long des deux jours** : 2 personnes de la team iExec, Camille Allary et Tiphaine Frugier pour la partie Business Model et pitch.
- **Repenser la relation de l'assurance avec ses assurés ou la relation entre les différentes filiales** du groupe.
- **De la formation en live à la Blockchain.**
- **Des super lots à gagner.**



Vivre l'expérience Blockathon !

- **Revoir la conférence, #Block1 du 25 Juin dernier : Les apports de la blockchain dans mon business ?**
animée par Jean-Charles Cabelguen, directeur Innovation et Adaptation à iExec.
- **Atelier #Block2 du 25 septembre à 18h30 - Amphi April :**
Démarrer avec la Blockchain ? animé par François Braniard, Lead Dev chez iExec. [Voir la vidéo qui présente cet atelier](#)
- **Atelier #Block3 - 22 Octobre à 18h30 à La Cuisine Du Web :**
Vos idées en pratique pour le Blockathon. Présentation de cas concrets d'application de la Blockchain dans l'assurance.
- **Soirée OnBoarding - 12 novembre à 18h30 à La Cuisine Du Web**
Choix des sujets et constitution des équipes.
- **13 et 14 novembre : BLOCKATHON APRIL à BlendWebMix dès 8h00**

Réservez votre place auprès de Mélanie Sutter, Groupe APRIL.

Plus d'infos auprès de tiphaine@lacuisineduweb.com pour l'organisation ou jb@iex.ec pour parler outils, technos, etc.

Des rdv d'information sont également organisés pour tous pour venir échanger avec l'équipe organisatrice :

- Le 30 septembre midi
- Mercredi 9 octobre au soir
- Mercredi 16 octobre matin
- Mercredi 30 octobre midi
- Vendredi 8 novembre matin

Plus d'infos Tiphaine Frugier tiphaine@lacuisineduweb.com pour l'organisation et/ou Julien Béranger jb@iex.ec pour parler outils, technos, etc.



Démarrer avec la Blockchain ?

Préparation au "Blockathon" du
BlendWebMix 2019

Francois Braniard
@fbraniard
github/braniard

Démarrer avec la Blockchain

- Les éléments d'une blockchain
- Je rejoins une blockchain
- J'interagie avec la blockchain
- Je développe avec la blockchain

Les éléments d'une blockchain

Les éléments d'une blockchain

Agencement ingénieux d'un ensemble de technologies existantes:

- Protocole internet
- Réseau pair-à-pair
- Base de données distribuées
- Cryptographie asymétrique (clef privée/clef public)
- Chaînage des blocs cryptographique

Règles de cet agencement ingénieux : **protocole**

Protocole de messagerie = e-mail

Protocole de publication = internet

Protocole

Les éléments d'une blockchain

Blockchain : Protocole de transfert pair-à-pair

Protocole = Ensemble des règles à respecter pour communiquer

Transfert = non duplication de jetons, atomicité

Pair-à-pair = sans intermédiaire (de confiance)

Transaction

Les éléments d'une blockchain

Une transaction simple :

- une information (transfer 10 jetons)
- signée par un émetteur (Alice)
- pour un destinataire (Bob)

Des blocs de transactions, chainés

Les éléments d'une blockchain



Blocs de transactions chaînée dans le temps :

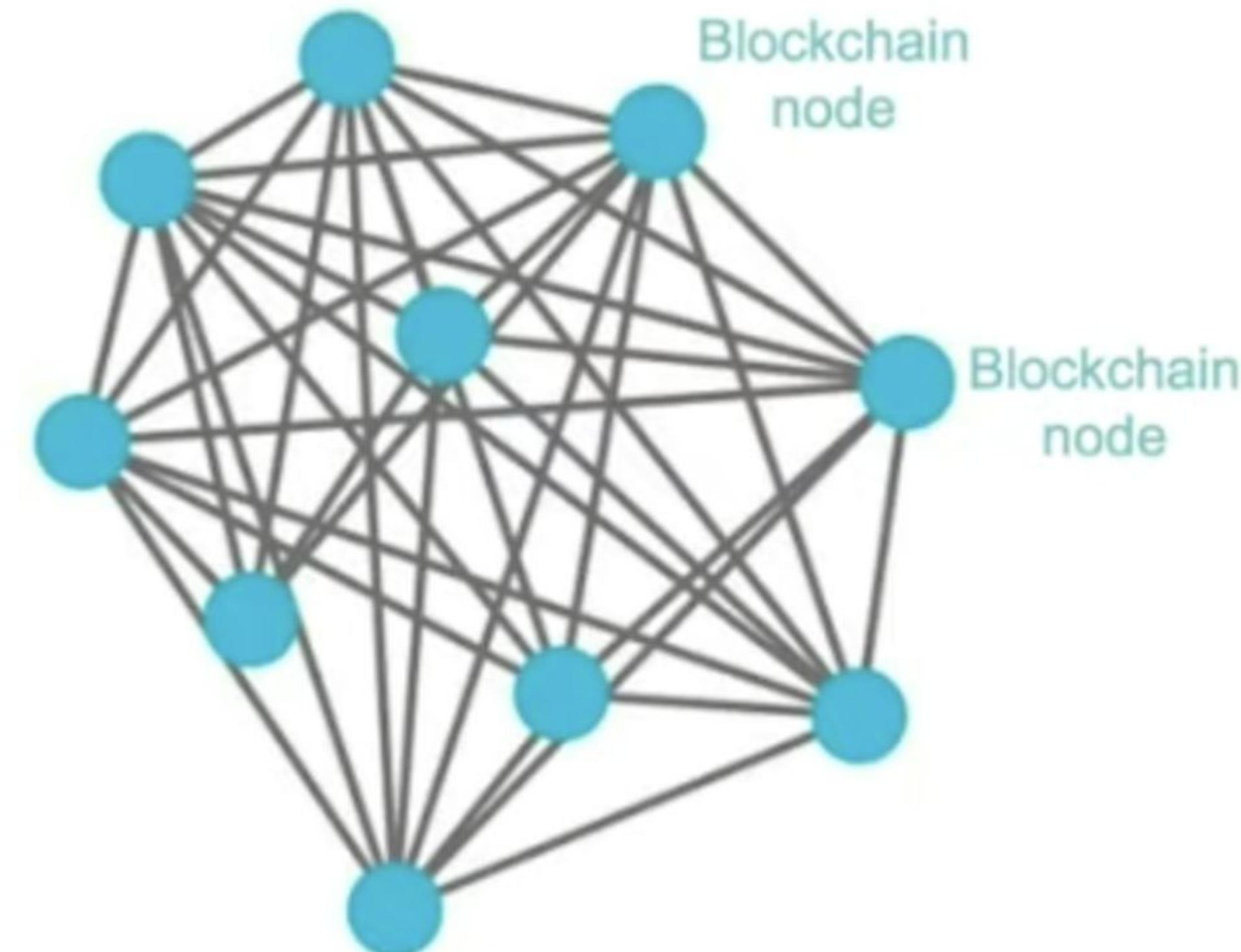
Des transactions :

- historisées
- ordonnancées
- hordatées
- validées

avec des preuves cryptographiques consultable par tous.
stockées ou ? centralisées ?

Réseau pair-à-pair

Les éléments d'une blockchain



Les mineurs / validateurs et Consensus

Les éléments d'une blockchain

- Des noeuds particuliers qui créent les blocs
- Règles à définir dans le protocol pour cette création blocs :
 - POW = preuve de travail
 - POS = preuve d'enjeux
 - POA = preuve d'autorités
- Règles pour un consensus de l'état dans le réseau (exemple Nakamoto consensus)

ELI5 break : Explain Like I am 5

Les éléments d'une blockchain



Demo : synchroniser un noeud (via DAppNode)

Les éléments d'une blockchain

Je démarre et synchronise un noeud

Je rejoins une blockchain



<https://dappnode.io/>



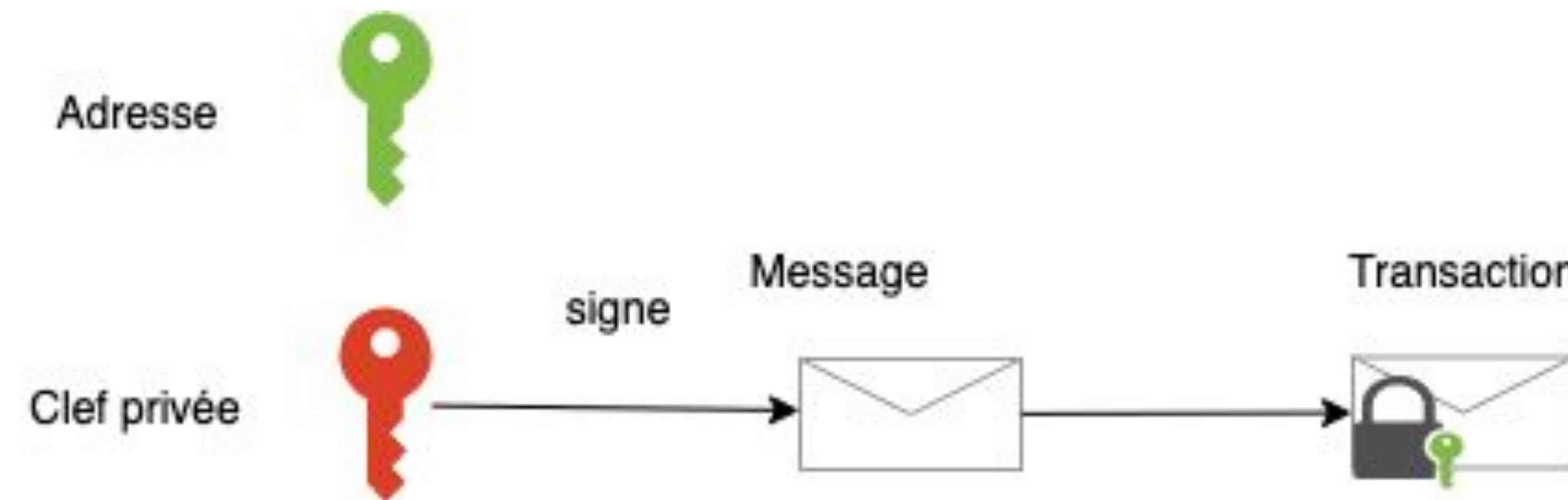
La wallet

Les éléments d'une blockchain

Une transaction est signée.

Comment ?

Signée par une clef privée.



La wallet

Les éléments d'une blockchain

- Une partie privée
 - clef privée
 - pour signer
- Une partie public
 - clef public
 - votre adresse

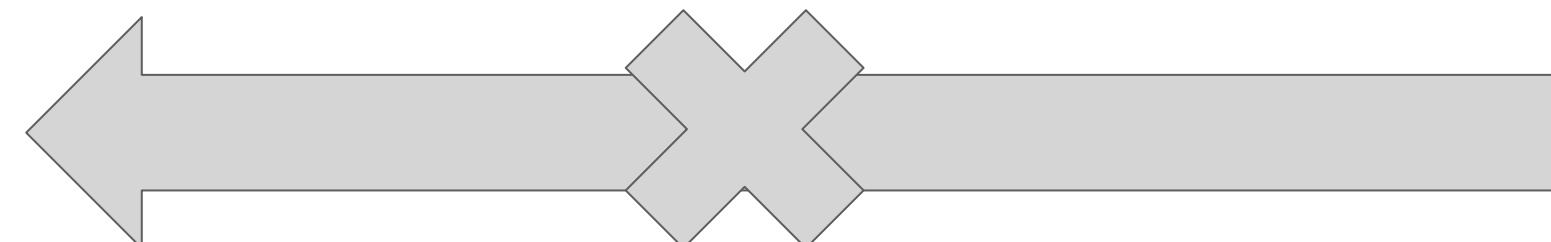
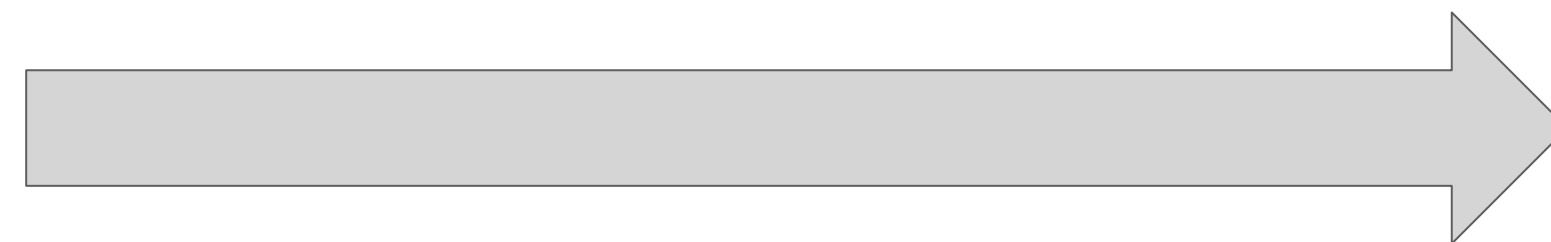


La wallet

Les éléments d'une blockchain



Possible



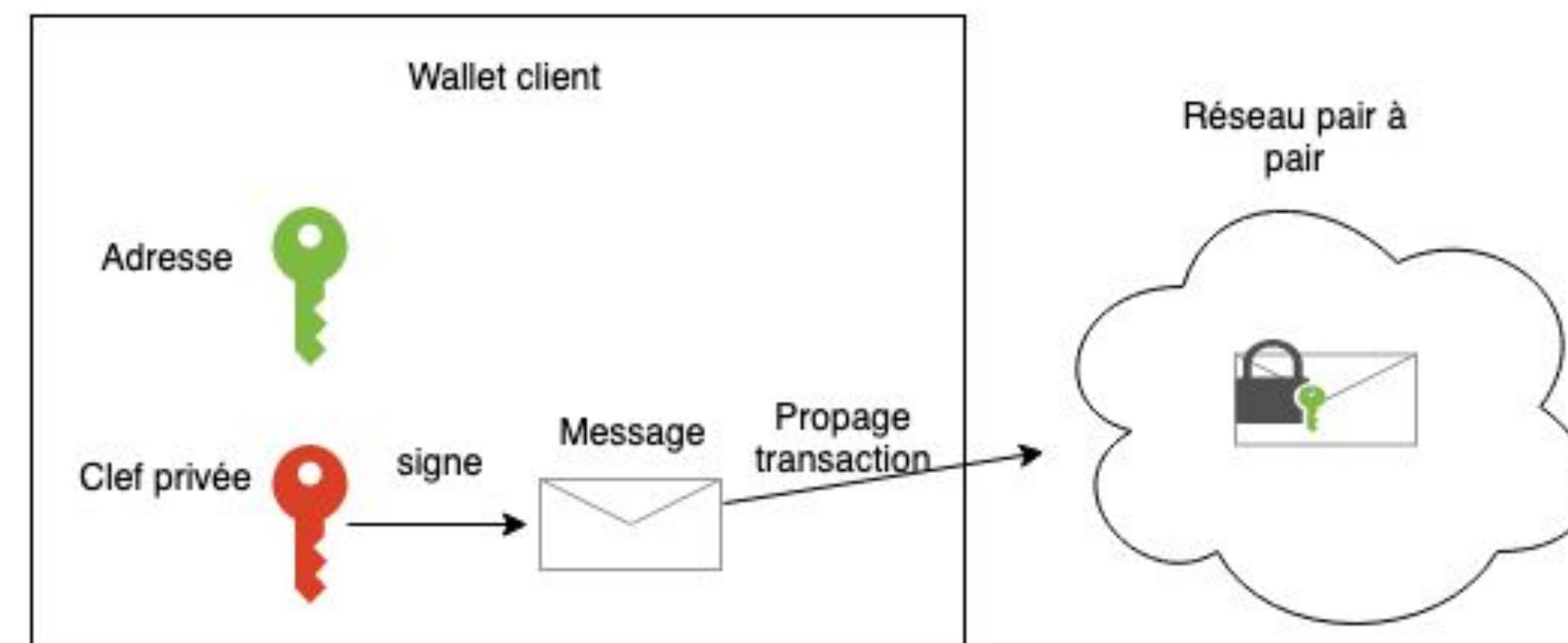
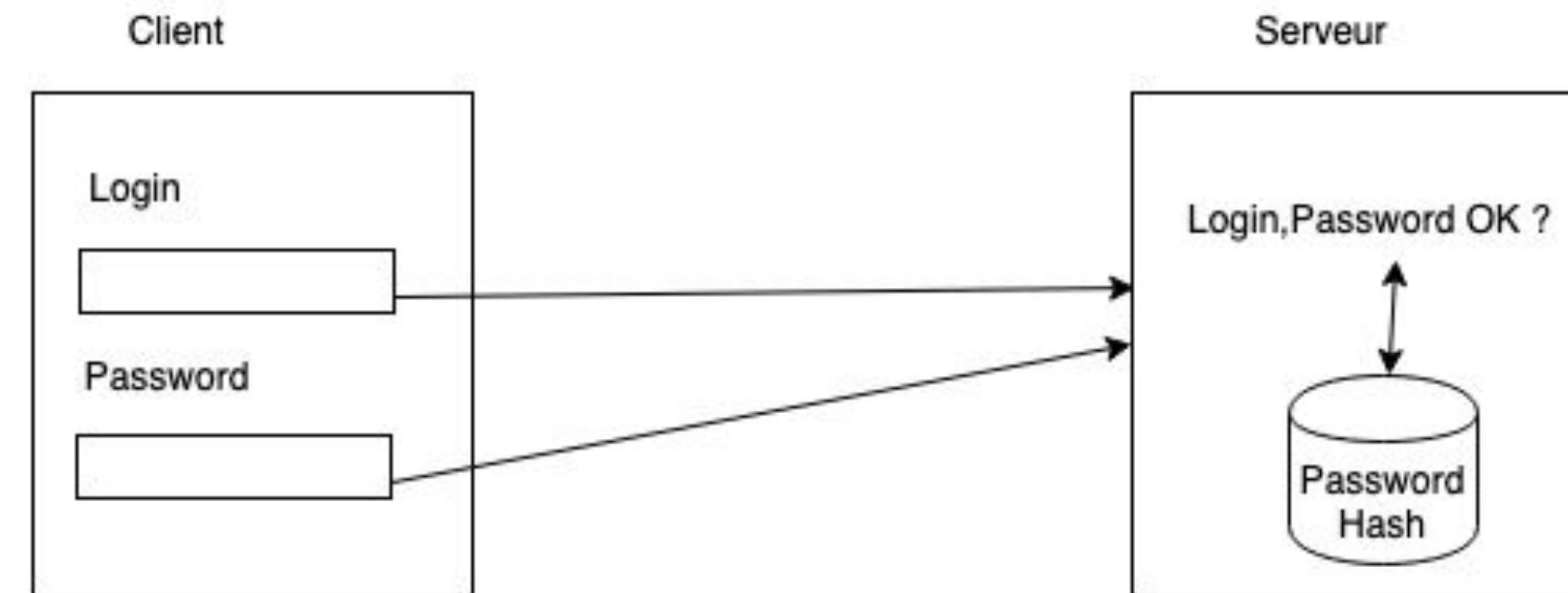
Impossible

- Trouver la clef public à partir de la clef privée = possible
- Trouver la clef privée à partir de la clef public = impossible
- Trouver la clef public à partir d'un message signé par la clef privée = possible



La wallet vs login/mot de passe

Les éléments d'une blockchain



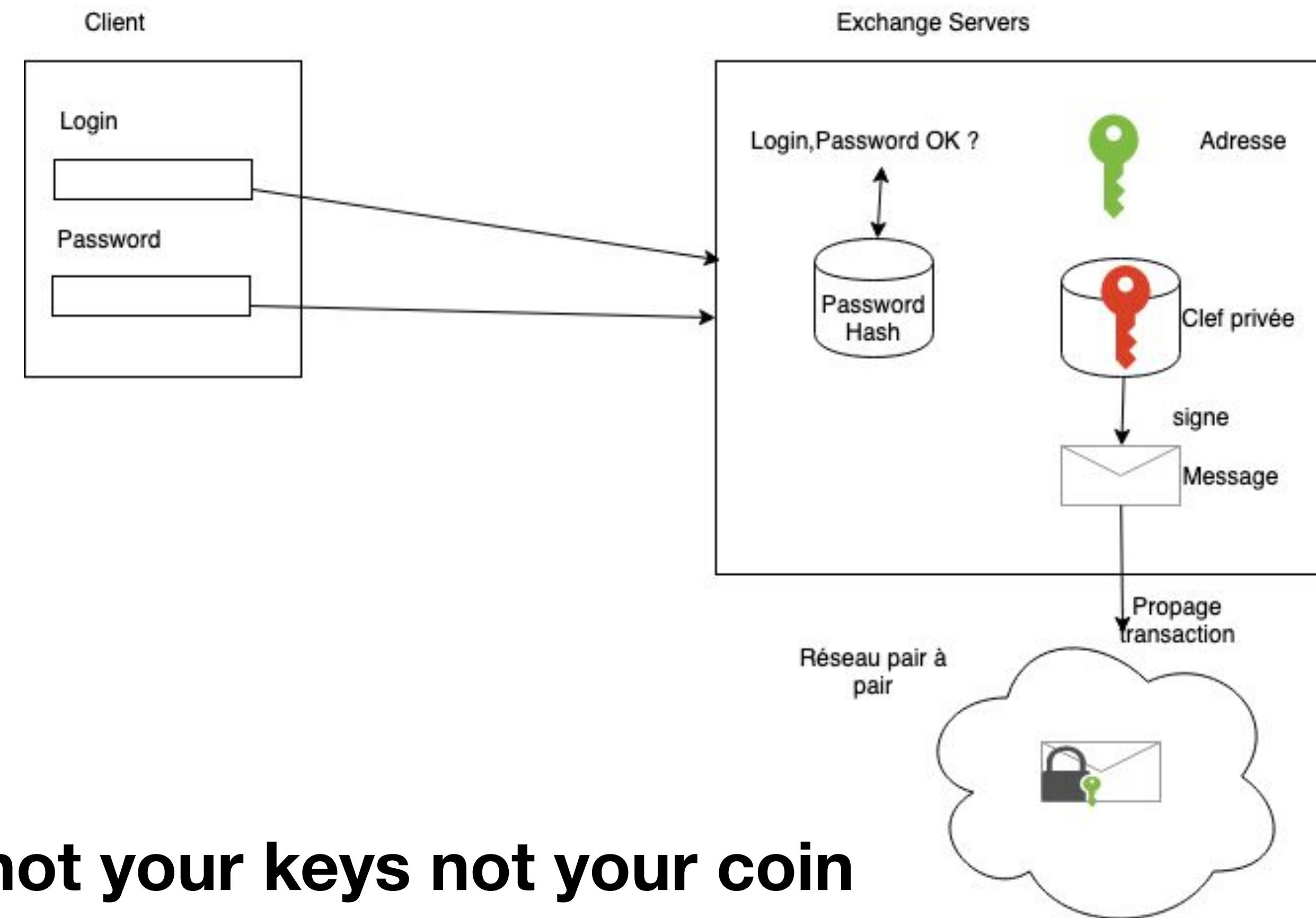
La wallet

Les éléments d'une blockchain

Wallet = Autonomie = Responsabilité des clefs!

Les “wallets” des plateformes d'échange

Les éléments d'une blockchain



Attention : not your keys not your coin

Je rejoins une blockchain

Je crée une wallet

Je rejoins une blockchain

<https://metamask.io/>



Je crée une wallet

Je rejoins une blockchain

Un password dans métamask ??? Je croyais que c'était fini les login/password !!

C'est une protection **locale**

Si je regarde sur votre disque dur ou si je prends votre PC, c'est un mot de passe pour ne pas laisser trainer en clair votre clef privée : celle qui sert à signer les messages qui seront propagés sur le réseau.

Je crée une wallet

Je rejoins une blockchain

12 mots ????

Je croyais qu'il y avait une clef public et une clef privée uniquement !!

Comprendons le liens entre les 12 mots et les clefs privées/public ici :

<https://iancoleman.io/bip39/>

Conclusion :

Les 12 mots permettent de retrouver la clef privée : 12 mots à conserver précieusement. C'est le sésame de votre wallet.

J'interagie avec la blockchain

J'envoie ma première transaction

J'interagie avec la blockchain

The JAXX wallet interface shows a balance of 0.8778 ETH. Below the balance are two buttons: "Déposer" (Deposit) and "Envoyer" (Send). A transaction history section shows a recent transaction: #48 - 8/14/2019 at 16:42, where Ether was sent (-0.01 ETH). The status of this transaction is "CONFIRMÉ" (Confirmed).

The DAppNode interface is shown in the "Logs" tab. It displays a log of network activity and transactions. A specific entry from August 14, 2019, at 14:43:06 UTC is highlighted:

```
2019-08-14 14:43:06 UTC 55/50 peers 6 MiB chain 30 MiB db 0 bytes queue 40 KiB sync RPC: 1 conn, 1 req/s, 21.92 μs
Transaction mined (hash 0xaf96058536fbb55b1468b58f3198e84c8ee46b6d6cd6e0dcc64479145ab8b9a)
Imported #8349234 0x9e52..8d4e (125 txs, 8.00 Mgas, 429 ms, 21.92 KiB)
```

Recevoir des Ethers

J'interagie avec la blockchain

Rien ne se perd,
Rien ne se crée :
Tout se transfert !



inscrivez l'adresse public de votre wallet ici:

<http://bit.ly/toutsettransfert>

J'explore les reçues de transactions

J'interagie avec la blockchain

The screenshot shows a detailed view of a single Ethereum transaction on the Etherscan platform. The transaction hash is 0xaf96058536fbb55b1468b58f3198e84c8ee46b6d66cd6e0dcc64479145ab8b9a. The status is marked as 'Success'. It was included in block 8349234, which has 1 block confirmation. The transaction occurred 50 seconds ago on Aug-14-2019 at 02:42:44 PM UTC. The sender's address is 0x6c6558dab14054d950bde08a659d4a9af113b243, and the recipient's address is 0x6c6558dab14054d950bde08a659d4a9af113b243. The value transferred was 0.01 Ether (\$2.05), and the transaction fee was 0.000021 Ether (\$0.04). The gas limit was set to 21,000, and the gas price was 0.00000001 Ether (10 Gwei). The nonce was 48, and the position was 36.

Etherscan

Eth: \$204.76 (-0.67%)

Home Blockchain Tokens Resources More Sign In

Transaction Details

Sponsored: YO YoBit.Net - Add your ERC20 Token to Yobit.Net Exchange!

Overview State Changes New Comments

② Transaction Hash: 0xaf96058536fbb55b1468b58f3198e84c8ee46b6d66cd6e0dcc64479145ab8b9a

② Status: Success

② Block: 8349234 1 Block Confirmation

② Timestamp: 50 secs ago (Aug-14-2019 02:42:44 PM +UTC)

② From: 0x6c6558dab14054d950bde08a659d4a9af113b243

② To: 0x6c6558dab14054d950bde08a659d4a9af113b243

② Value: 0.01 Ether (\$2.05)

② Transaction Fee: 0.000021 Ether (\$0.04)

② Gas Limit: 21,000

② Gas Used by Transaction: 21,000 (100%)

② Gas Price: 0.00000001 Ether (10 Gwei)

② Nonce Position

48 36

J'utilise une cold wallet

J'interagie avec la blockchain

La partie privée de la wallet
ne sort jamais de la clef physique.

Les messages sont signés
dans la clef physique
elle-même.

Puis les transactions sont
propagées comme précédemment



Je développe avec la blockchain

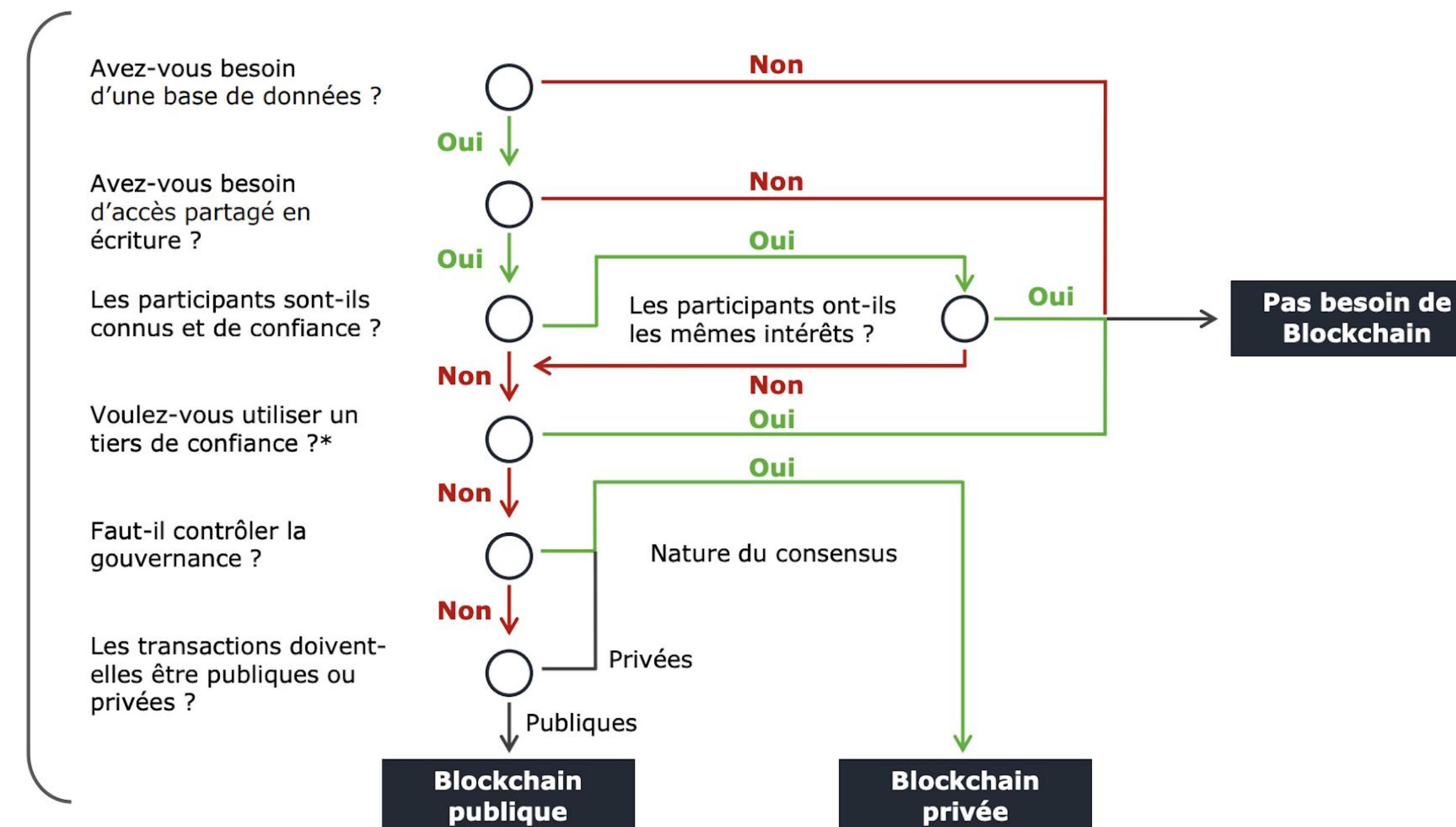
Ai-je besoin d'une blockchain ?

Je développe avec la blockchain

Les types de Blockchain

Comment construire une stratégie Blockchain?

**Avez-vous
besoin d'une
Blockchain ?**



Tiers de confiance traditionnel déjà existant. Excluant les Oracles qui jouent le rôle de confiance au sein d'une Blockchain.

Introduction Smart Contract

Je développe avec la blockchain

Une transaction simple :

- une information (transfer 10 ETH à bob)
- signée par un émetteur (Alice)
- pour un destinataire (Bob)

Des transactions **plus évoluées** :

- **Deployer un nouveau smart contract**
 - une information (voici mon code)
 - signée par un émetteur (createur du contrat)
 - pour un destinataire (aucun, résultat : une nouvelle adresse avec le code)
- **Appeler un smart contract**
 - une information (j'appelle une fonction d'un contrat avec des paramètres)
 - signée par un émetteur (l'appelant)
 - pour un destinataire (l'adresse du contract, résultat : le code de la fonction est exécuté)

Problème à résoudre

Je développe avec la blockchain

Un exemple de scénario :

- Je veux que les votes du jury du "Blockathon" soient vérifiables dans un smart contract.
- Les participants du "Blockathon" peuvent créer des projets dans le smart contrat avec une liste de membres et une description.
- Des wallets sont données aux membres du jury pour voter.
- Les sponsors déposent de l'argent dans le smart contrat pour des récompenses.
- Le jury vote pour le/les projet(s)
- Les membres du projet gagnant peuvent retirer des gains

Problème à résoudre

Je développe avec la blockchain

Un exemple d'utilisation de blockchain :

- Transparence des votes. (en gardant pseudo-anonymat pour le jury)
- Paiement automatique selon des règles : “monnaie programmable”
(paiement de l'équipe du projet gagnant par vote d'un jury ici)
- Non stocké sur une serveur centralisé
(pas de super Administrateur système BDD pouvant modifier les votes ou les fonds).

Lister les Acteurs du smart contract

Je développe avec la blockchain

- Créateur du contrat
- Les membres du jury
- Les sponsors
- Les hackeurs
- Les hackeurs regroupés en équipes

Quel sont les responsabilités, leurs actions possibles

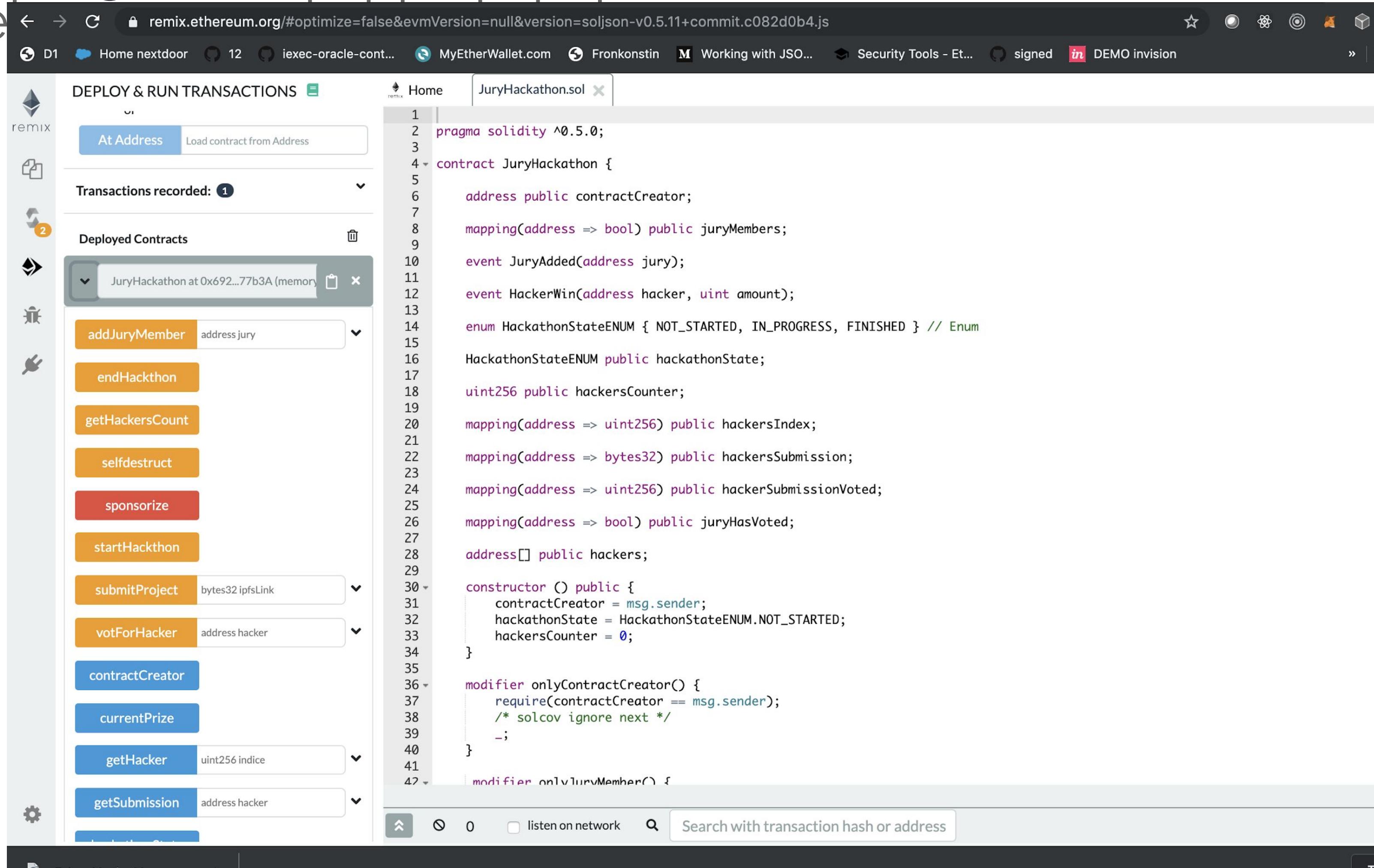
Lister les fonction du smart contract

Je développe avec la blockchain

- Le cycle de vie du contrat : avant, pendant, après le hackathon.
- Expliciter les contraintes et permissions de chaque acteurs.
- Exemple de fonctions :
 - ajouter les membres du jury
 - demarrer/arreter le hackathon
 - enregistrer un projet
 - envoi d'argent par le sponsor
 - voter
 - recevoir l'argent pour le gagnant

Deployer le smart contract

Je déve



The screenshot shows the Remix Ethereum IDE interface. On the left, there's a sidebar titled "DEPLOY & RUN TRANSACTIONS" with various buttons for interacting with deployed contracts. The main area displays the Solidity source code for the "JuryHackathon" contract. The code defines a contract with methods for managing jury members, tracking hacker submissions, and controlling the hackathon state. A specific transaction is highlighted, showing it was deployed at address 0x692...77b3A.

```
1 pragma solidity ^0.5.0;
2
3 contract JuryHackathon {
4     address public contractCreator;
5
6     mapping(address => bool) public juryMembers;
7
8     event JuryAdded(address jury);
9
10    event HackerWin(address hacker, uint amount);
11
12    enum HackathonStateENUM { NOT_STARTED, IN_PROGRESS, FINISHED } // Enum
13
14    HackathonStateENUM public hackathonState;
15
16    uint256 public hackersCounter;
17
18    mapping(address => uint256) public hackersIndex;
19
20    mapping(address => bytes32) public hackersSubmission;
21
22    mapping(address => uint256) public hackerSubmissionVoted;
23
24    mapping(address => bool) public juryHasVoted;
25
26    address[] public hackers;
27
28    constructor () public {
29        contractCreator = msg.sender;
30        hackathonState = HackathonStateENUM.NOT_STARTED;
31        hackersCounter = 0;
32    }
33
34    modifier onlyContractCreator() {
35        require(contractCreator == msg.sender);
36        /* solcov ignore next */
37        ;
38    }
39
40    modifier onlyJuryMember() {
41
42    }
43}
```

Utilisation (inarrêtable !) du contrat

Je développe avec la blockchain

- Utilisation via wallet comme précédemment.
- Au lieu de signer des transfert de token, l'utilisateur signe des appels à des fonctions du smart contract.
- Exemple de contrat :
- <https://goerli.etherscan.io/address/0x80c88De4B9556730B1EF18e6e183E8df20Fd6417>
- Montrer la transaction de création du contrat

D'un “contrat jury” pour le Hackathon vers une DAO post Hackathon...

- DAO : Pour Decentralized Autonomous Organization
- Tous les projets peuvent postuler pour un financement et continuer leur projet après le hackathon
- Tous les participants hackathon ont des crédits de réputation et peuvent voter.
- D'un vote à la majorité, vote quadratique ? etc ...
- Exemple avec DAOstack

alchemy.daostack.io/dao/0x0c88aa3c4fe9f9f8da766e9b8bfbbaa1235928cc/members/

D1 Home nextdoor 12 iexec-oracle-cont... MyEtherWallet.com Fronkonstin Working with JSO... Security Tools - Et... signed DEMO invision » Autres favoris

Alchemy > ETHBerlin dHack.io > Reputation Holders Francois Branciard Connect

ETHBerlin dHack.io

For more info join our TG group - t.me/dhack0

Menu

- Home
- Reputation Holders
- History
- Redemptions (3)
- DAO Discussion

DAO Holdings

- +0 ETH
- 14,75 GEN

Home
Buy GEN
Help Center

Reputation Holders

Name	Address	Reputation	Social Verification
No Profile	0x84e94f8032b3f9fec34ee05f192ad57003337988	397 (2,49 % Rep.)	
No Profile	0xeeef9530b42dd9df11ca01dbd4d5d44264dff9934	300,88 (1,89 % Rep.)	
No Profile	0x21d5e578dc101a132b1457f8a696e8eff97a4b1	300 (1,88 % Rep.)	
No Profile	0xdcbeffbecce100cce9e4b153c4e15cb885643193	262,77 (1,65 % Rep.)	
No Profile	0x774d556f7c2cae79f28a35b8e1f57371df8b8bca	200,65 (1,26 % Rep.)	
No Profile	0x4499631feadfe802798ddf72e24ae1de0162dd1d	200 (1,25 % Rep.)	



ETHBerlin dHack.io

For more info join our TG group -
t.me/dhack0

Menu

Home

Reputation Holders

History

Redemptions (3)

DAO Discussion

DAO Holdings ↗

+0 ETH

14,75 GEN

Home

Buy GEN

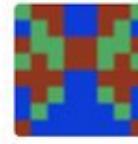
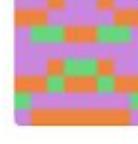
Help Center

Get Involved

Privacy Policy

DAOstack

History

 0x9329c2...	Sep 4, 2019	Contribution Reward	'catbox' like encrypted dropbox for Ethereum & IPFS, open source lib	 3,22 %  1,07 %	 0  700	 Failed Time out	
 0x002781...	Sep 4, 2019	Contribution Reward	SUDZ Game Submission	 2,19 %  2,19 %	 0  650	 Failed Time out	100 Rep 
 0x0e7001...	Sep 3, 2019	Contribution Reward	dHack ICO	 0,00 %  4,76 %	 0  1,22k	 Failed Time out	
 wslyvh	Sep 2, 2019	Contribution Reward	DAO Dashboard - Integrate DAO Stack + other improvements	 5,56 %  0,00 %	 620  200	 Passed Relative Majority	
 0x1057be...	Sep 2, 2019	Contribution Reward	Hotspot me!	 8,11 %  2,70 %	 4,4k  805	 Passed Relative Majority	100 Rep 
 0xeeef953...	Sep 2, 2019	Contribution Reward	DeLAMP: make your smart contracts compliant	 3,69 %  1,17 %	 3,49k  755	 Passed Relative Majority	
 0x9c6d44...	Sep 1, 2019	Contribution Reward	VotezUp - Socializing DAOs [25 ETH]	 13,13 %  0,00 %	 3,3k  702	 Passed Relative Majority	
 Pat	Sep 1, 2019	Contribution Reward	Slash Reputation of dishonest dHack proposer and judge (#2)	 5,27 %  0,00 %	 1,75k  200	 Passed Relative Majority	
 Tobias	Sep 1, 2019	Contribution Reward	Mapcovery - Recover your wallet simply and securely with 5 locations that you remember <5ETH>	 8,98 %  3,00 %	 3,39k  620	 Passed Relative Majority	100 Rep 
 ...	Sep 1, 2019	Contribution Reward	... (truncated)	 5,42 %	 1,11k	 Passed	





ETHBerlin dHack.io

For more info join our TG group -
t.me/dhack0

Menu

Home

Reputation Holders

History

Redemptions (3)

DAO Discussion

DAO Holdings

+0 ETH

14,75 GEN

Home

Buy GEN

Help Center

Get Involved

Privacy Policy

DAOstack

Passed

Mapcovery - Recover your wallet simply and securely with 5 locations that you remember <5ETH>



Tobias



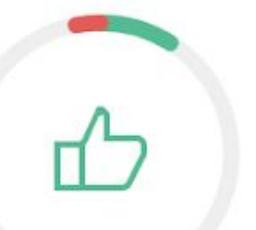
Votes

12 Votes >

You voted - For

For
8,98 % Rep

Against
3,00 % Rep



Predictions

Predictions are disabled

3,39k Pass

620 Fail

Base de connaissance pour Hackathon

<http://hack.iex.ec>

<https://github.com/iExecBlockchainComputing/knowledge-base>

liens vidéos explicatives

liens vers doc :

liens vers tutoriaux développeur :

- Déployer votre premier smart contract solidity sur testnet et connecter un frontend (app react) déployé sur IPFS.
- Pour aller plus loin : Oracles, DeFi, stable coin, DAO, Marketplace iExec

Conclusion

**Les smart contract, c'est bien mais pour l'accès aux données extérieures à la blockchain alors ?
DataWallet, Oracles etc...**

**Rendez-vous le pour le prochain workshop 22 octobre
#Block 3 Vos idées en pratiques pour le hackathon**

dans le cadre de la préparation du "Blockathon" BlendWebMix !!



Merci !

Francois Branciard
@fbranciard
github/branciard