Alexandre David

La gouvernance sur la blockchain

Pas Sage En Seine

Samedi 2 juillet 2016

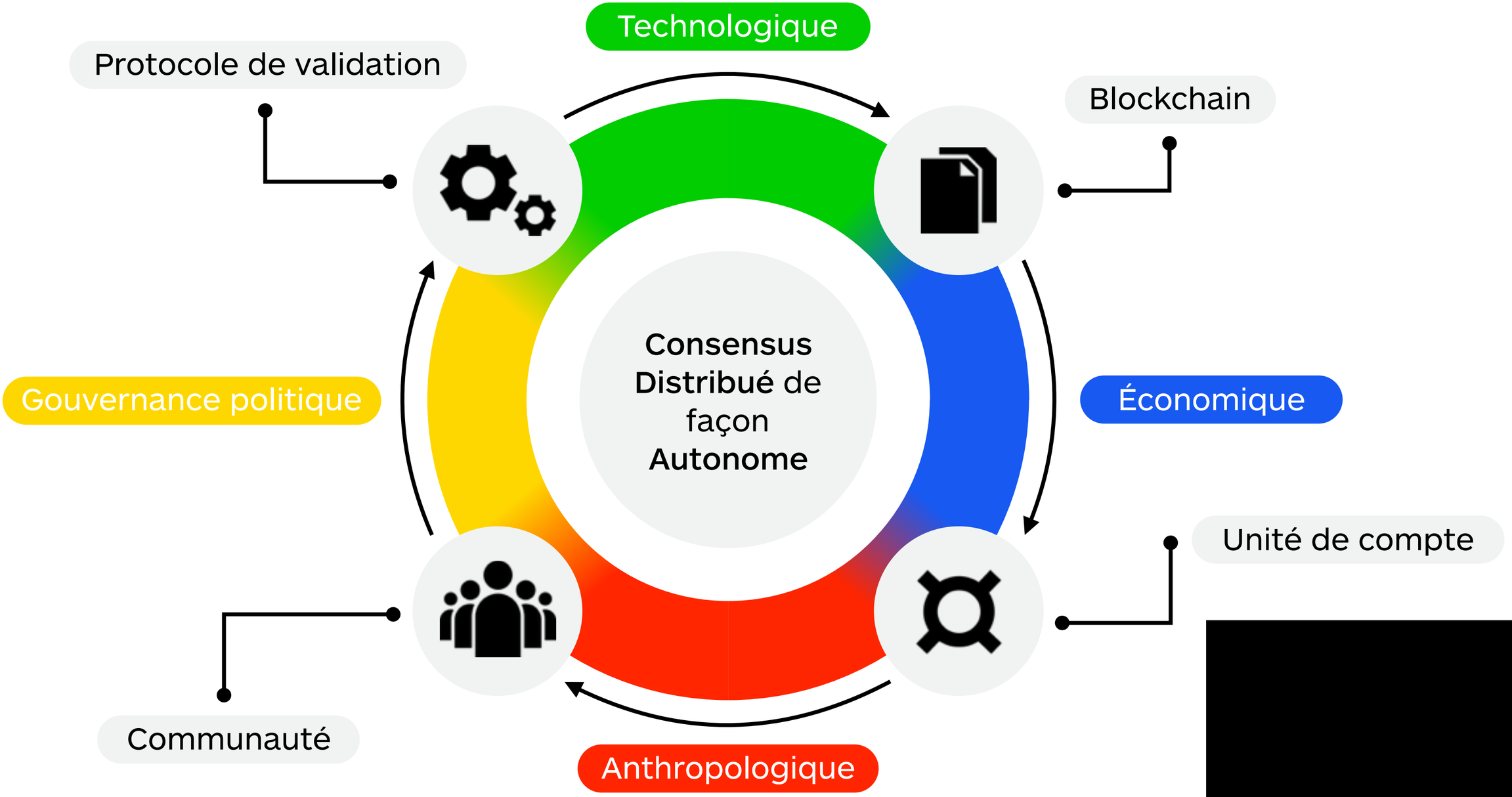
Alexandre David

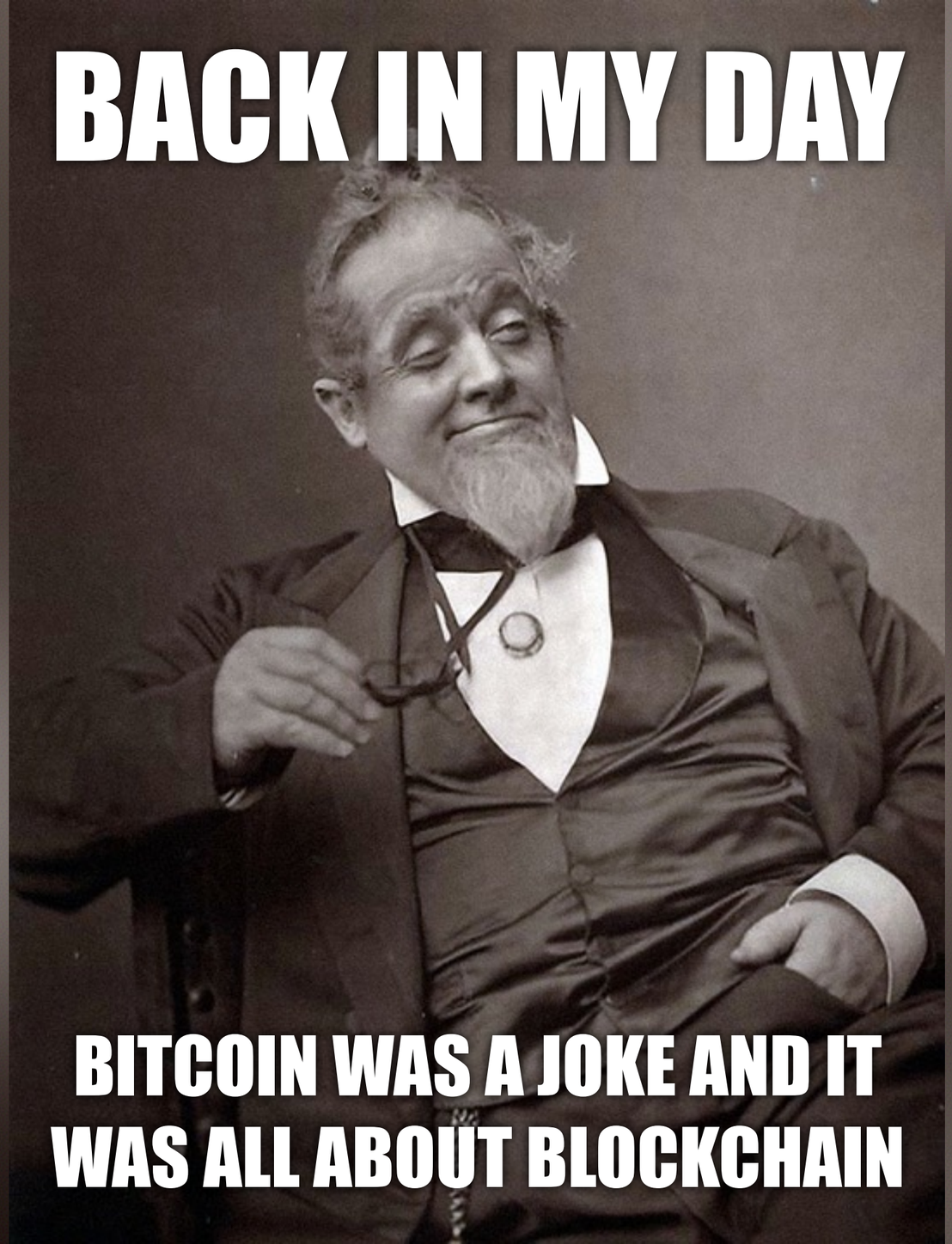
@Daboloskov

@EurekaCertif

Partagez vos réactions en temps réel sur twitter. #**PSESHSF**

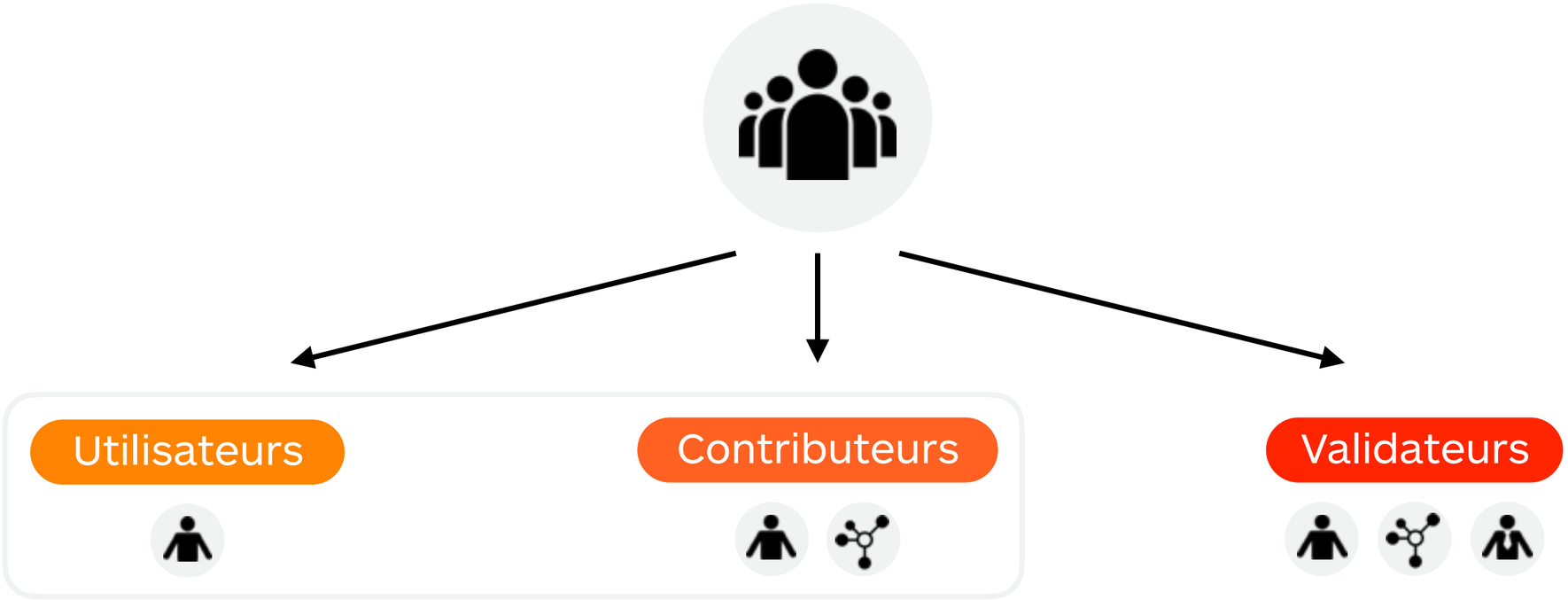

« Les États sont exactement dans la même situation que l'Église d'il y a mille ans. »


Technologique
Protocole de validation
Blockchain
Consensus
Distribué de
façon
Autonome
Gouvernance politique
Économique
Unité de compte
Communauté
Anthropologique


BACK IN MY DAY
BITCOIN WAS A JOKE AND IT WAS ALL ABOUT BLOCKCHAIN

Anthropologique

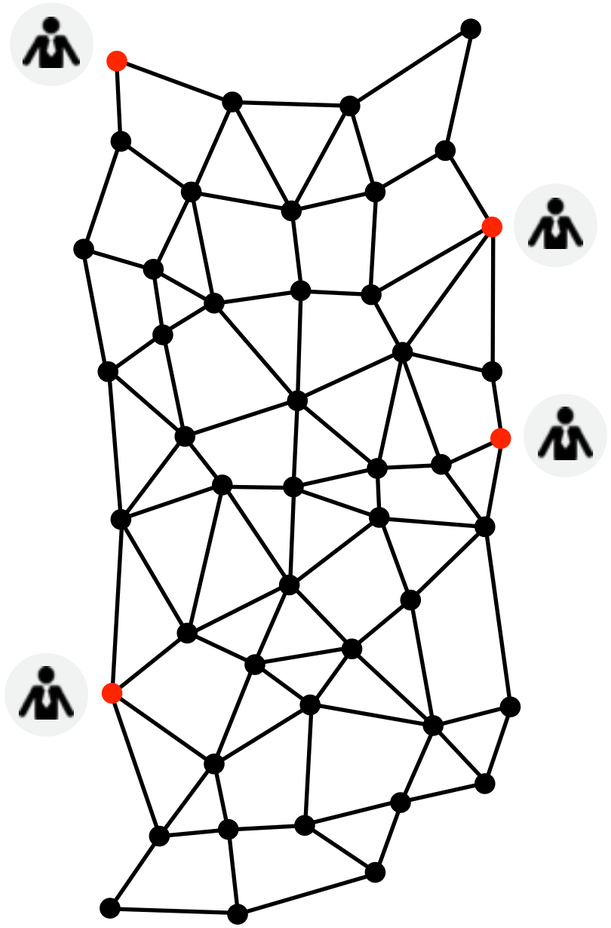
Types de populations



Technologique

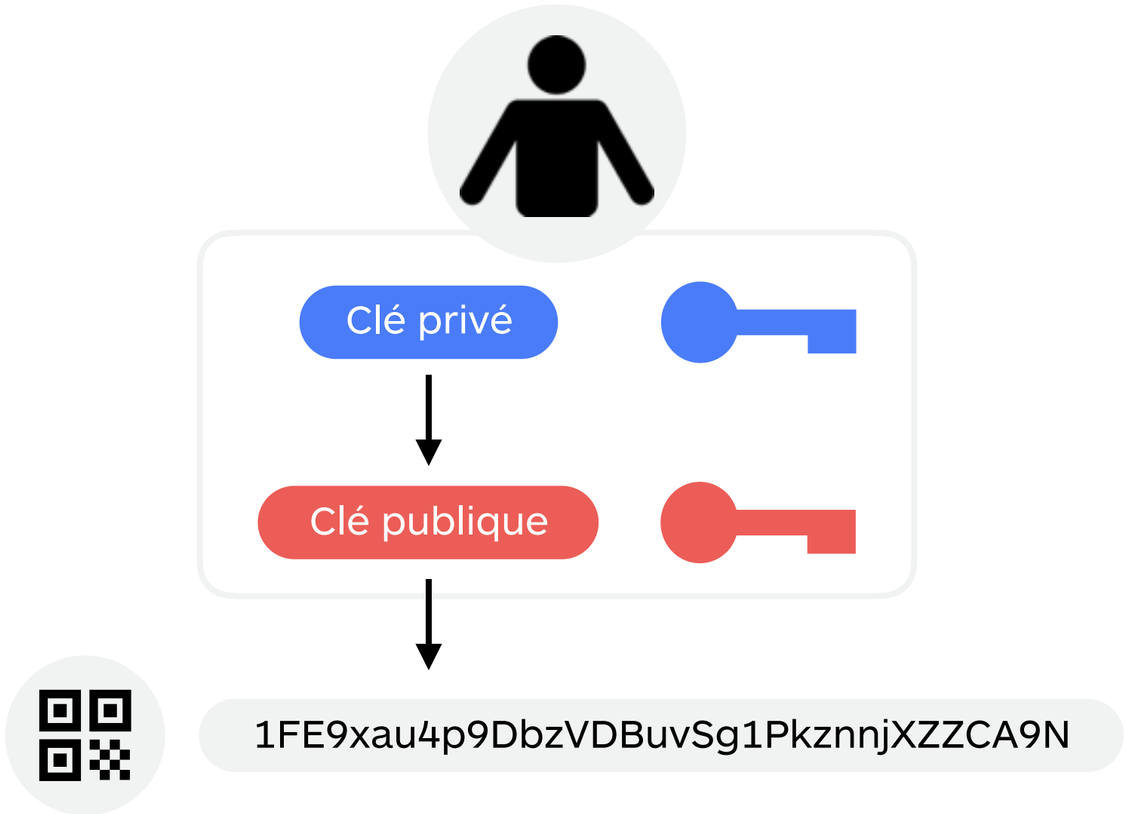
Un réseau en p2p*

*Chaque noeuds disposent d'une réplique de la blockchain.



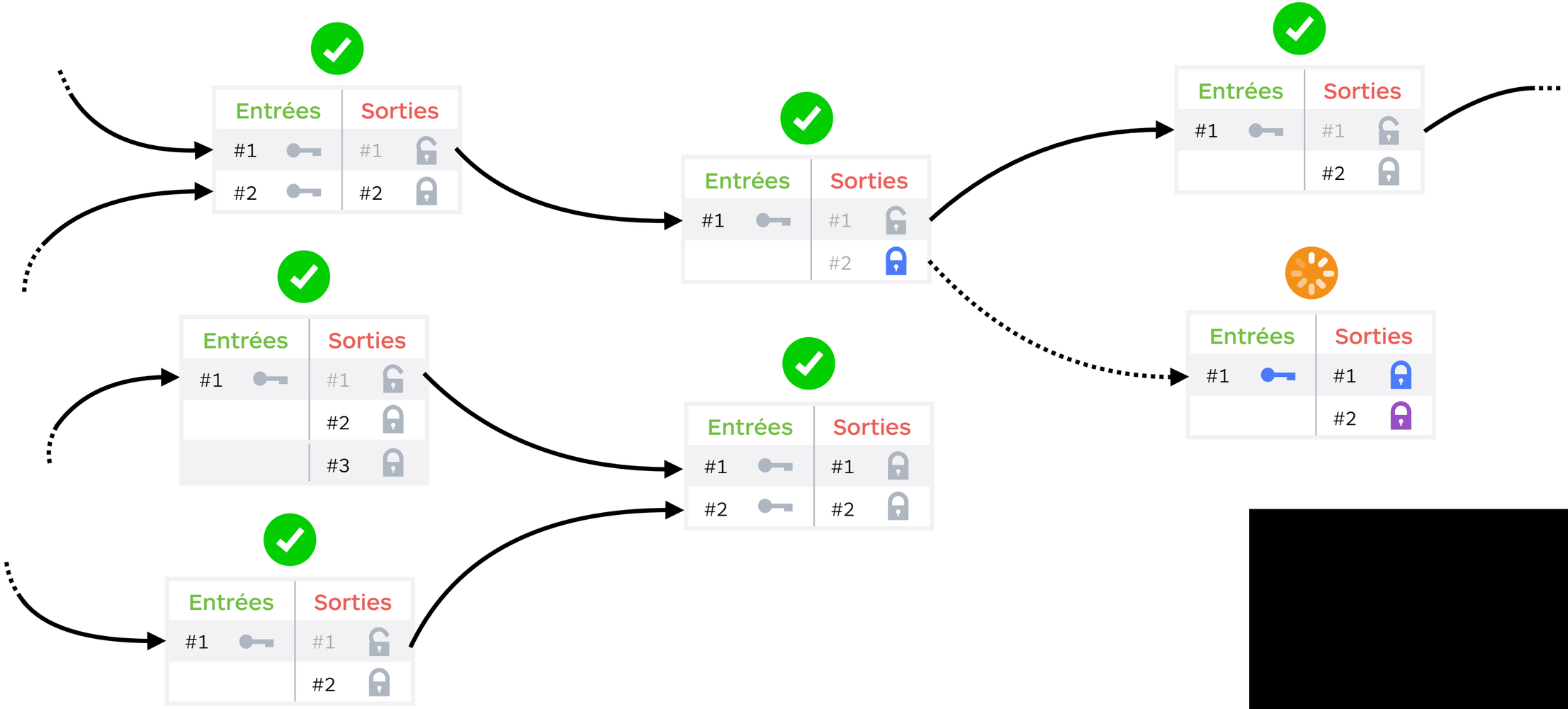
Technologique

Les clés



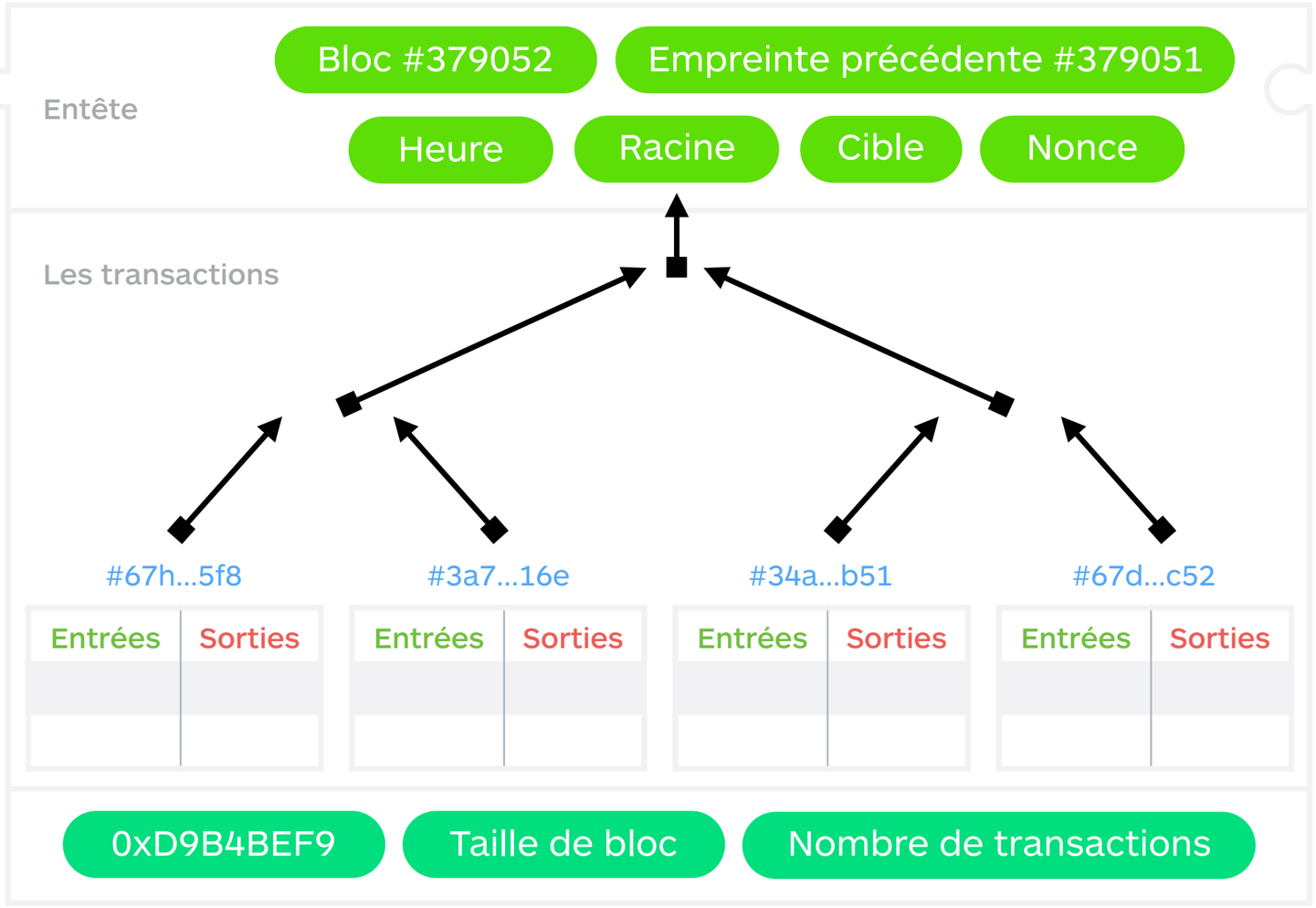
Technologique

Chaînage des transactions



Technologique

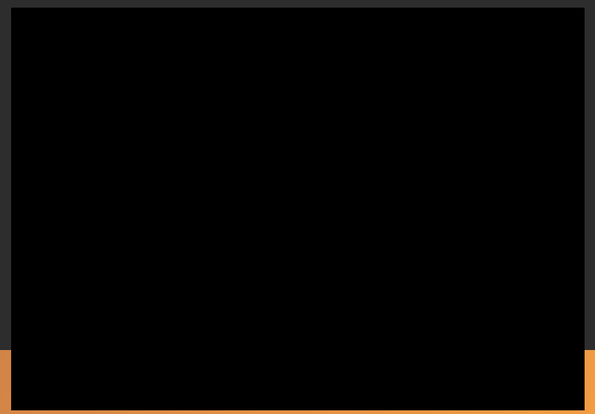
Les éléments d'un bloc



Calcule du hash d'un bloc

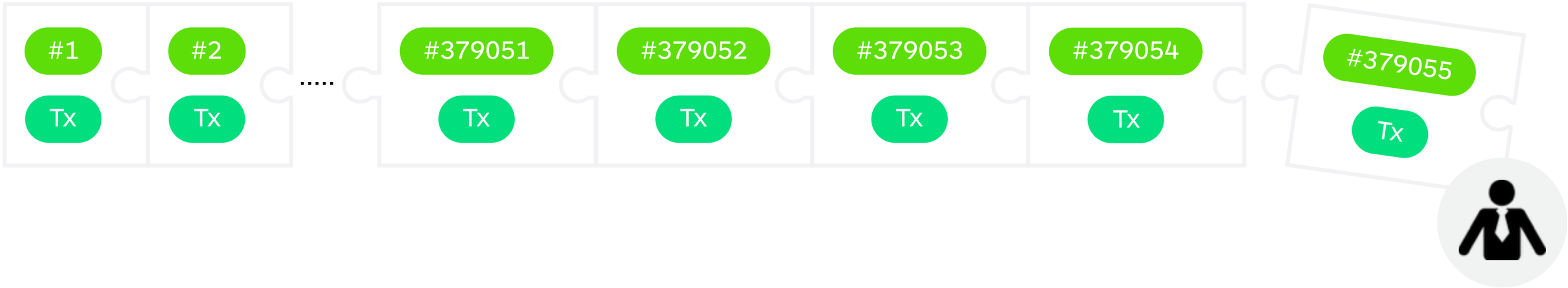
BlockHash 00000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d

```
>>> import hashlib
>>> header_hex = ("01000000" +
 "81cd02ab7e569e8bcd9317e2fe99f2de44d49ab2b8851ba4a308000000000000" +
 "e320b6c2fffc8d750423db8b1eb942ae710e951ed797f7affc8892b0f1fc122b" +
 "c7f5d74d" +
 "f2b9441a" +
 "42a14695")
>>> header_bin = header_hex.decode('hex')
>>> hash = hashlib.sha256(hashlib.sha256(header_bin).digest()).digest()
>>> hash.encode('hex_codec')
'1dbd981fe6985776b644b173a4d0385ddc1aa2a829688d1e0000000000000000'
>>> hash[::-1].encode('hex_codec')
'00000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d'
```



Technologique

La blockchain



Taille de la blockchain de Bitcoin : ~ 80 Go

Gouvernance politique

Technologique

Hashocracy (PoW)

*__Google__ = 10M serveurs x 10 CPU x 10MH/s = 1Ph/s

Gouvernance politique

Technologique

… et stakocracy (PoS)

Live transactions	Age	Total Sent (PPC)	Destroyed (PPC days)
f777aa3171f6636011d4...	2 minutes	16.371205	38.98
a8f17f6cc4735136c7cf...	9 minutes	43.3812	1487.10
2dbdd0ef4c851041101a...	19 minutes	34.441625	2.57
c699a5db31a11eba450b...	27 minutes	31.242397	4.19
bbcfcc4c9b732f185169...	27 minutes	53.567504	7.18
ad418ac6ae376044fd52...	27 minutes	53.251904	7.14
a877cec4112274fef104...	27 minutes	3.970714	0.53

La chaîne la plus longue

Anthropologique

Économique

Une crypto-économie

Anthropologique

Économique

Une crypto-économie

Anthropologique

Technologique

Gouvernance politique

Économique

Le consensus de Nakamoto

Toutes les **10 minutes** un accord est obtenu de façon **autonome** entre les différents participants du **réseau** (distribué) sur l'ajout d'un nouveau bloc dans la **base de données** (distribuée) appelée blockchain qui devient la **chaîne la plus longue**.

Anthropologique

Technologique

Gouvernance politique

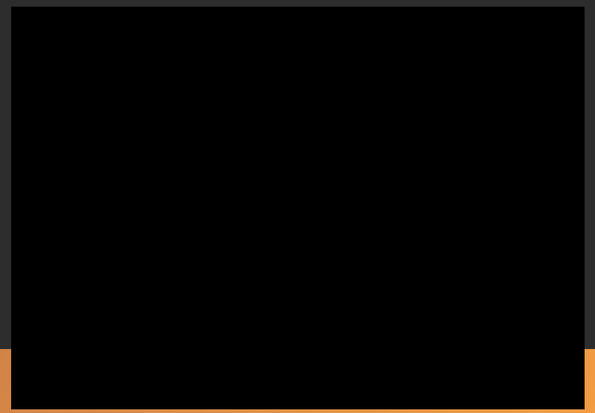
Économique

La 1er application

La monnaie numérique est un script

Pay to Public Key Hash (p2pkh)

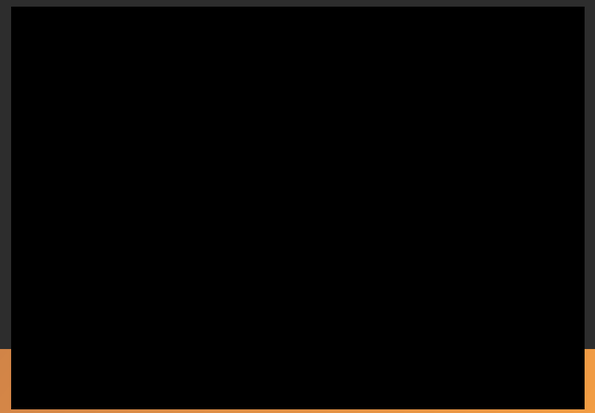
```
var address = Address.fromString('1NaTVwXDDUJaXDQajoa9MqHhz4uTxtgK14');
var script = Script.buildPublicKeyHashOut(address);
assert(script.toString() === 'OP_DUP OP_HASH160 20 0xecae7d092947b7ee4998e254aa48900d26d2ce1d OP_EQUALVERIFY OP_CHECKSIG');
```



Plus d'opérateurs, plus d'applications

Pay to Multisig (p2ms)

```
var pubkeys = [
  new PublicKey('022df8750480ad5b26950b25c7ba79d3e37d75f640f8e5d9bcd5b150a0f85014da'),
  new PublicKey('03e3818b65bcc73a7d64064106a859cc1a5a728c4345ff0b641209fba0d90de6e9'),
  new PublicKey('021f2f6e1e50cb6a953935c3601284925decd3fd21bc445712576873fb8c6ebc18'),
];
var threshold = 2;
var script = Script.buildMultisigOut(pubkeys, threshold);
assert(script.toString() === 'OP_2 33 0x022df8750480ad5b26950b25c7ba79d3e37d75f640f8e5d9bcd5b150a0f85014da'
      + ' 33 0x03e3818b65bcc73a7d64064106a859cc1a5a728c4345ff0b641209fba0d90de6e9'
      + ' 33 0x021f2f6e1e50cb6a953935c3601284925decd3fd21bc445712576873fb8c6ebc18 OP_3 OP_CHECKMULTISIG');
```



Les différentes applications

La monnaie numérique n'est que la **première application**.

Entité
Distribuée
de façon
Autonome

La **monnaie** numérique
Le **contrat** Intelligent
Le financement participatif en p2p
L'emprunt en pair à pair
Le **notariat** électronique
L'assurance en pair à pair
Le **vote** électronique
L'agent autonome
L'Internet des objets
Le **marché** prédictifs
Le **transport** en pair à pair
...


DAO... ETIENNE ?
NOPE

Distributed Autonomous Organisation

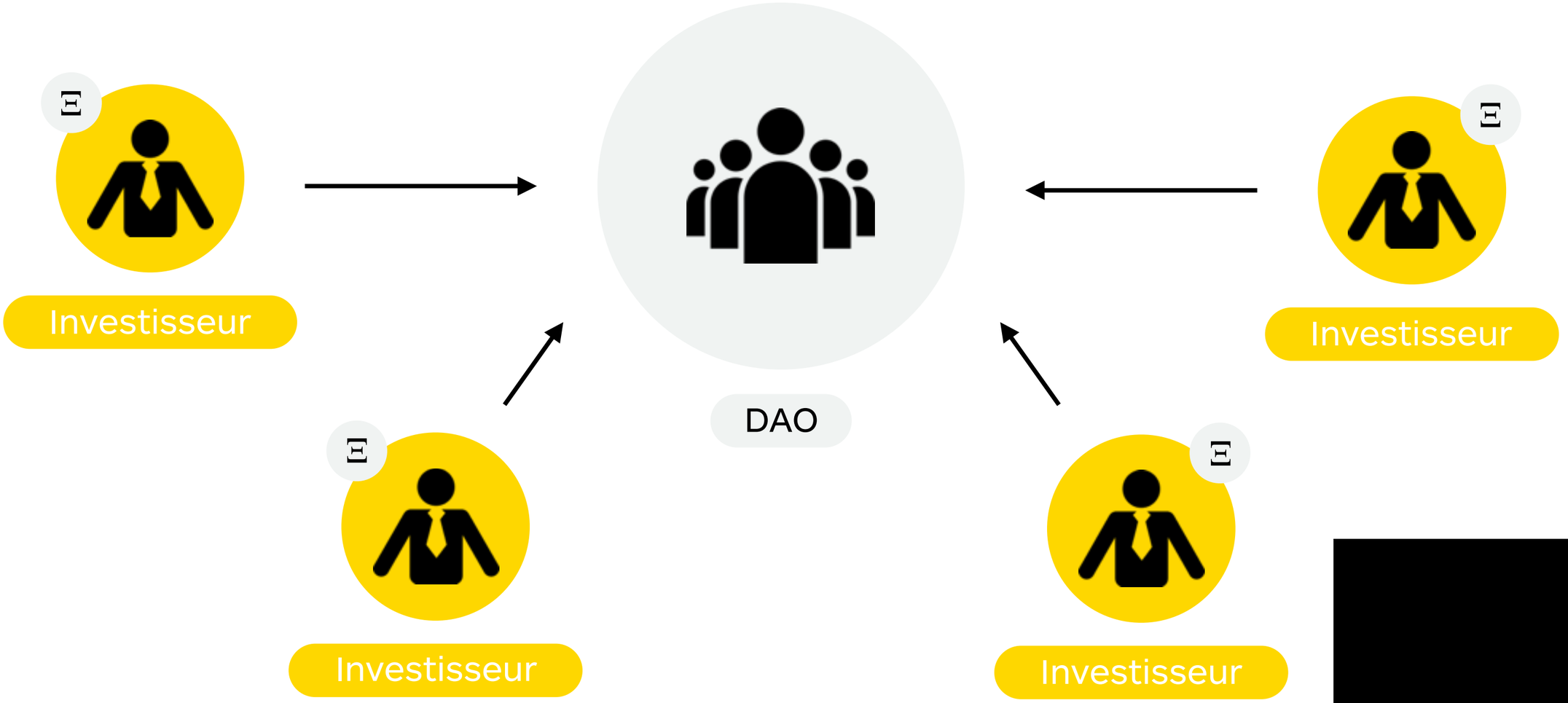
C'est une entité qui existe uniquement sur un protocole de registre distribué et ceci, de façon strictement autonome.

Les **DAO**s reposent sur une main d'oeuvre qui ne peut pas être automatisée : **les Contractors**.

Personne physique

Personne morale

Phase de création de 27 jours



Le prix des actions

- Les 20 premiers jours de l'IPO. Ð = Ξ
- Après deux semaines d'IPO, le prix de l'action augmente à 0,05 ethers par jour. Ð = Ξ + 0,05 /jrs
- Les quatre derniers jours le prix de l'action grimpe à 1,5 ethers.

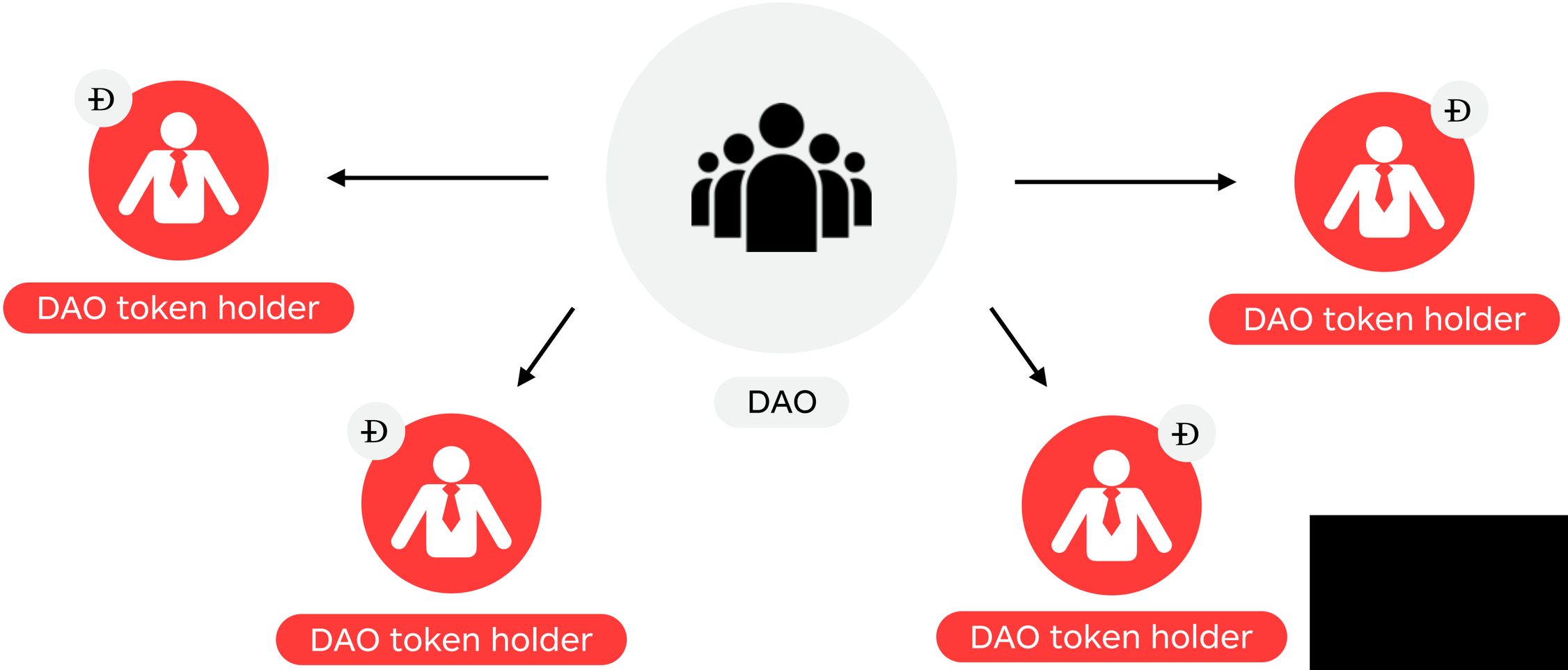
Ð = 1,5 Ξ

Les DAO tokens

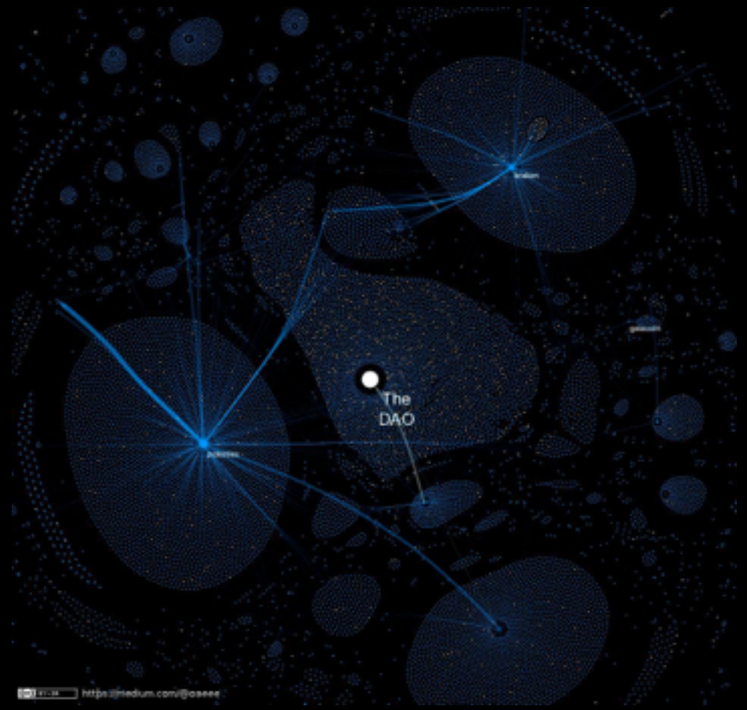
- À la fin de la phase de création, les droits de propriétés sont transférables à faible coût.
- Le nombre de token est proportionnel aux nombres d'unités de comptes envoyées.
- La **DAO** stock les **ethers** et l'équivalent en **DAO tokens** sont envoyés aux investisseurs qui deviennent des **DAO token holders**.

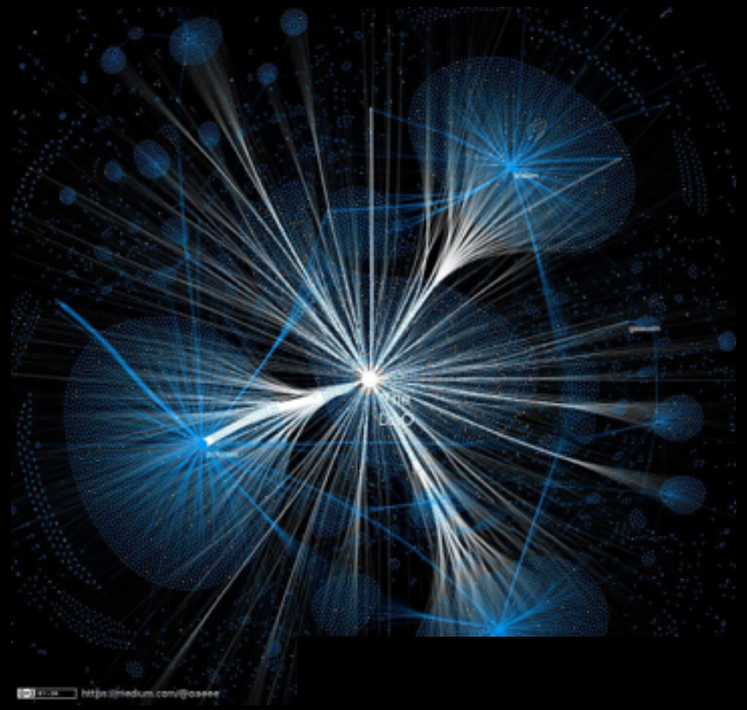
1 Ether Ξ = 1 DAO token Ð

La DAO est investie

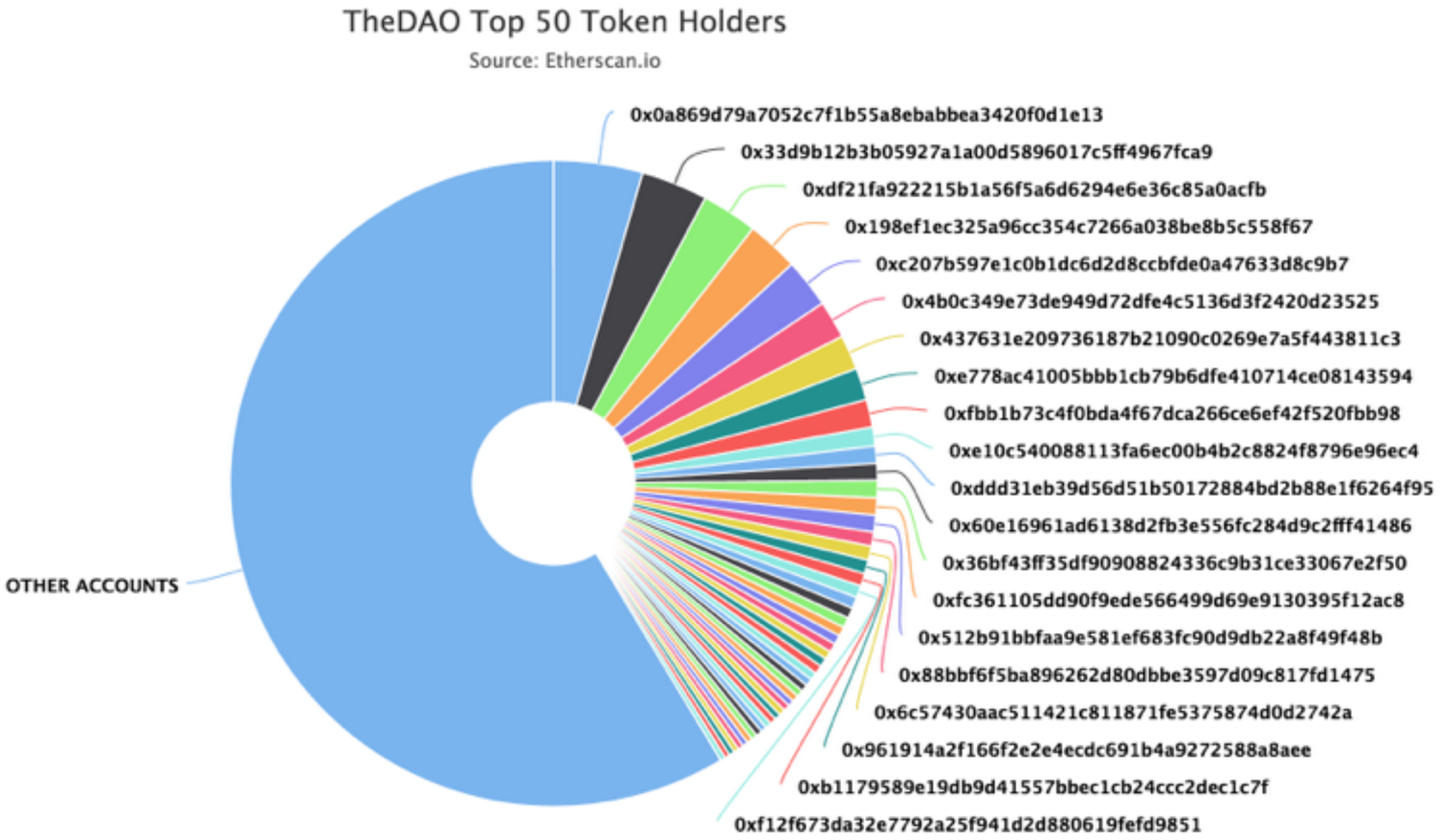


Phase de création de TheDAO (mai 2016)

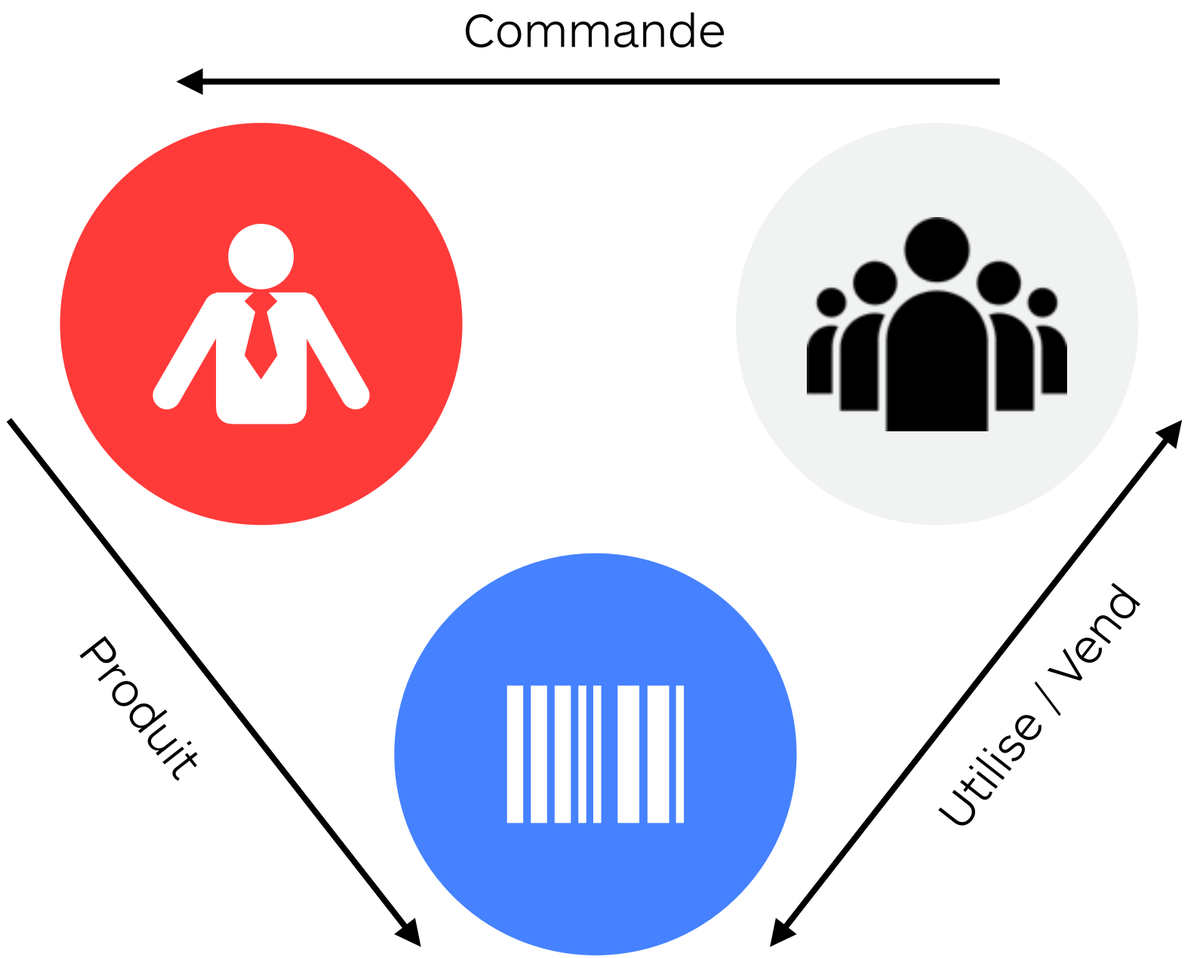




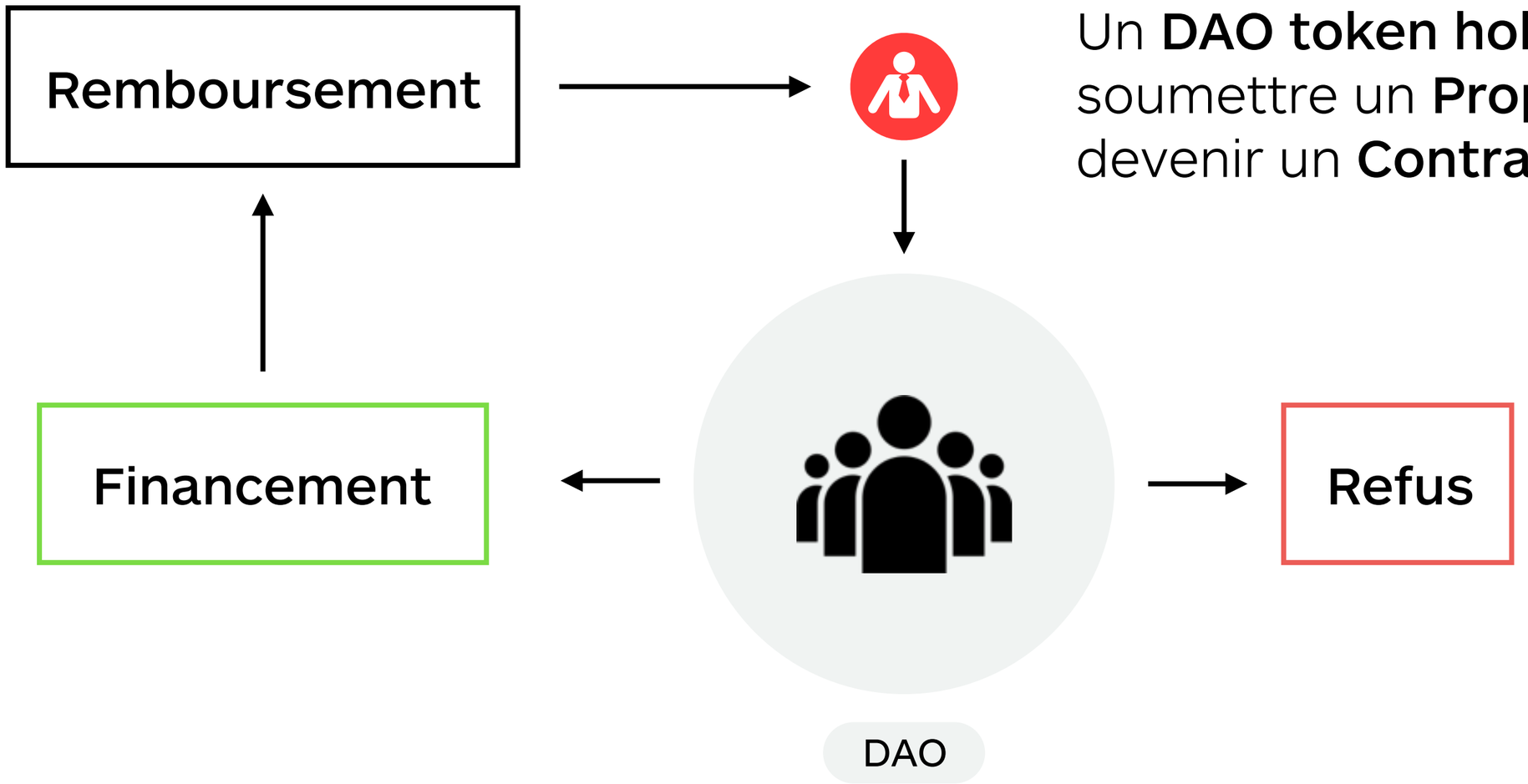
Liste des actionnaires de TheDAO



Les Contractors



Soumettre un Proposal



Un **DAO token holder** peut soumettre un **Proposal** et devenir un **Contractor**.

Les Proposals

Regular proposal

- Temps du débat : Minimum 20 jours.
- Dépôt minimum (remboursé après le quorum si le **Proposal** est approuvé).
- Suivant le nombre de **DAO tokens** dans la **DAO** le quorum minimum se situe entre 20% et 53.33%.

Split proposal

- Temps du débat : 7 jours.
- Aucun coût de dépôt.


PROPOSALS
LIGHTYEAR
PROPOSALS EVERYWHERE

Liste des Proposals de TheDAO

DAO Stats | Home | Search | Accounts | Proposals | Graphs | Options | About

Open Proposals

Number of open proposals: 50

Hide Splits

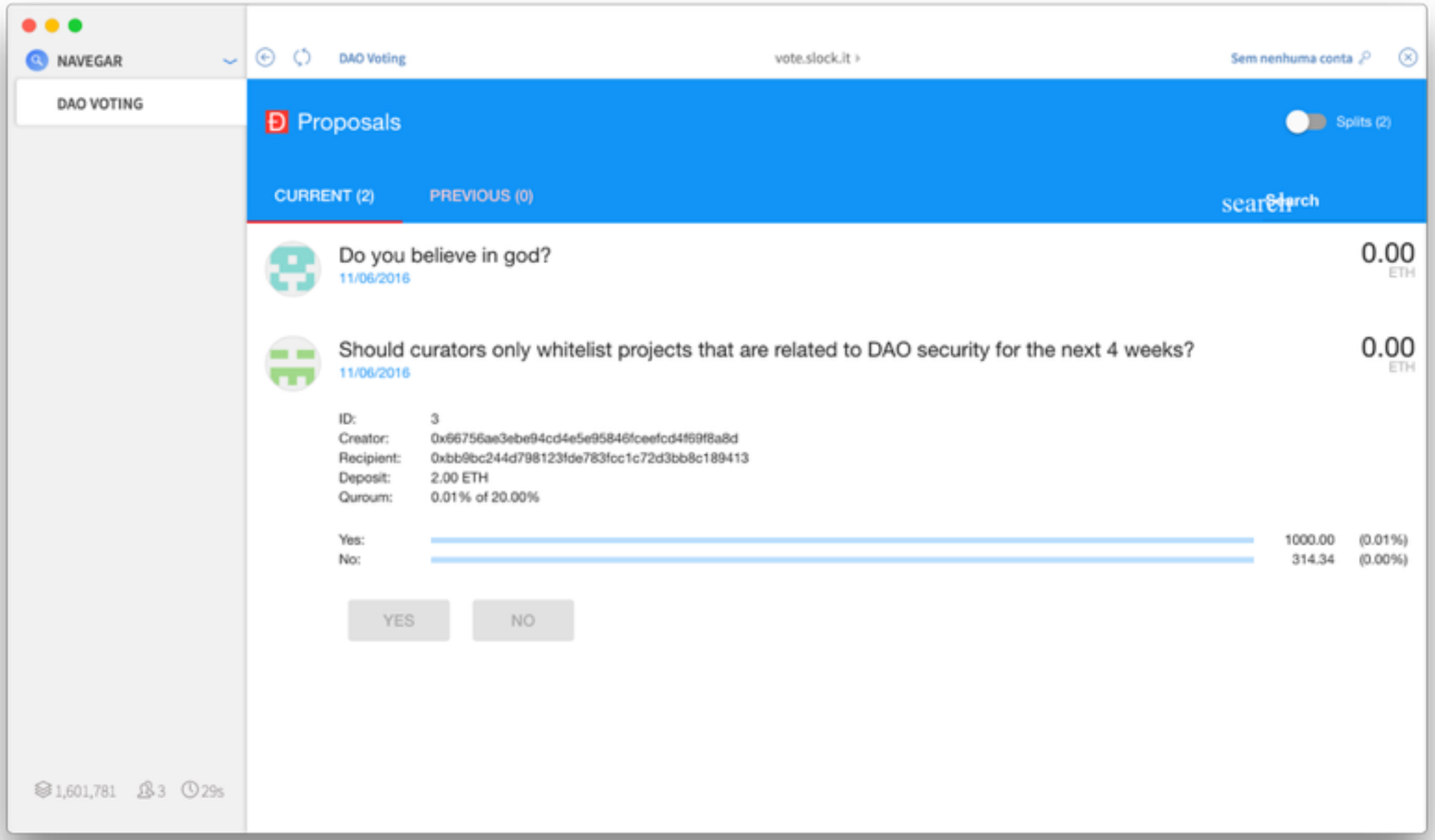
Search Proposal ID: Go

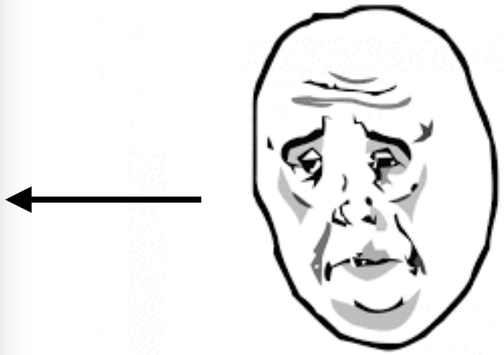
ID	Description	Deposit	Time Left	Turnout	
2	Do you believe in god?	2 ether	6 days	0.56%	
50	m split	0 ether	6 days	0%	Split
5	Moratorium on proposals until the DAO contract is ...	2 ether	6 days	6.68%	
11	Curators, please hire somebody to fix the DAO code...	2 ether	7 days	1.48%	
15	Dear DAO - Tokenholders, I am a simple DAO-Tokenho...	2 ether	8 days	1.6%	
17	Raising the Proposal Deposit to 11 ETH \n This P...	2 ether	8 days	5.31%	
40	Return dao tokens accidentally sent to TheDao. 56...	2 ether	12 days	2.67%	
43	Would you try (or contribute to) a collaborative m...	2 ether	12 days	0.03%	
1	No Description	0 ether	Finished	0.45%	Split
4	split	0 ether	Finished	0.37%	Split
6	Original intent, non-interventionist curator. Spl...	0 ether	6 days	0.01%	Split
7	Leave me alone	0 ether	Finished	0.35%	Split
8	No Description	0 ether	Finished	0.35%	Split

Le contenu d'un Proposal

- Le business-model
- Liste des produits
- Les questions sur les responsabilités
- Les paramètres des opérations
- Termes du paiement

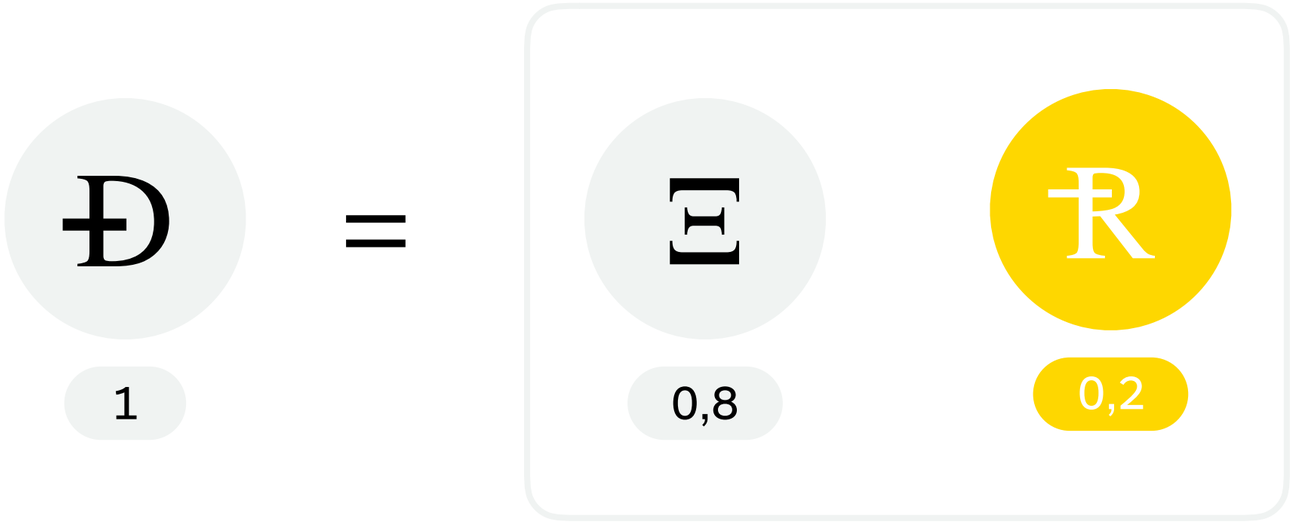
UI pour les Proposals de TheDAO





DAO reward token

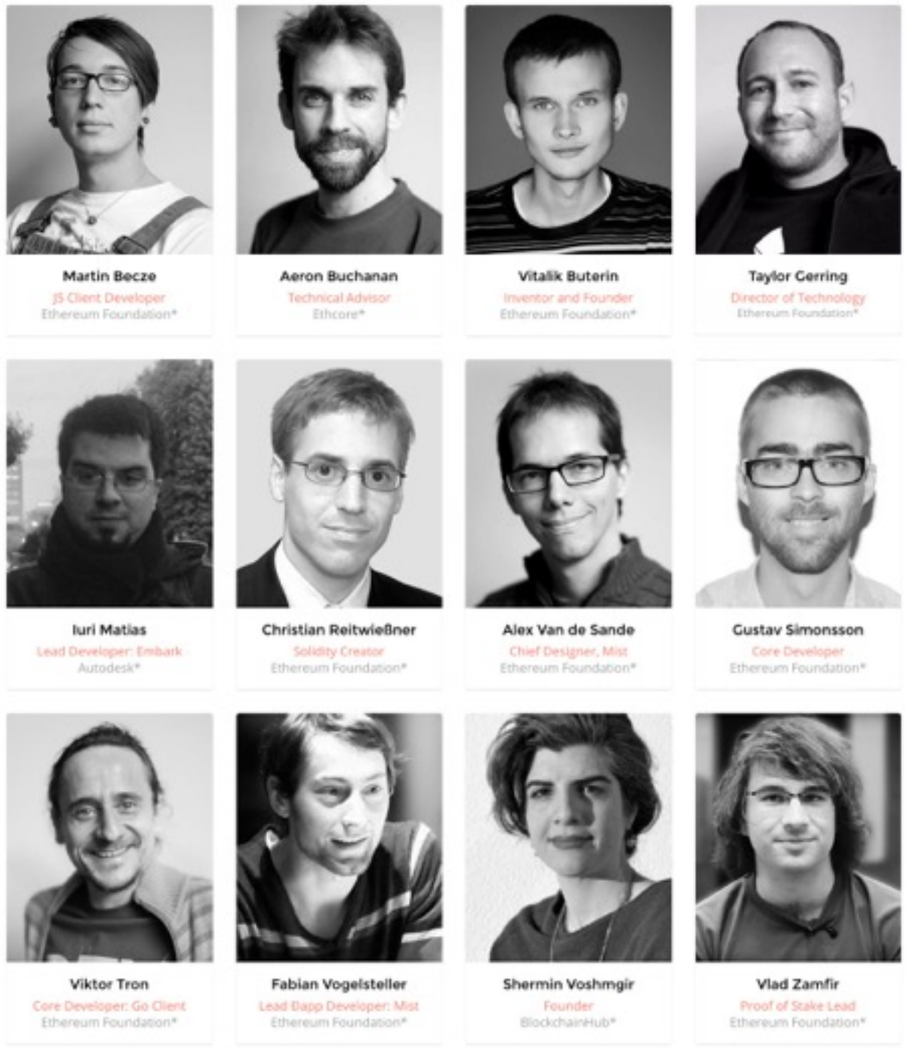
Si le **Proposal** d'un **Contractor** obtient un quorum de 20%, alors ...



Les Curators

- Afin de protéger les membres inactifs, la DAO introduit le concept de **Curator**.
- Tous les actionnaires de la DAO peuvent soumettre un **Proposal** pour se proposer en tant que **Curator**.
- Les **Curators** contrôlent une liste d'adresses (**Whitelist**) utilisées pour débloquer les fonds appartenant à la DAO pour financer un **Proposal**.

Les Curators de TheDAO



Martin Becze
JS Client Developer
Ethereum Foundation*

Aeron Buchanan
Technical Advisor
Ethcore*

Vitalik Buterin
Inventor and Founder
Ethereum Foundation*

Taylor Gerring
Director of Technology
Ethereum Foundation*

Iuri Matias
Lead Developer: Embark
Autodesk*

Christian Reitwießner
Solidity Creator
Ethereum Foundation*

Alex Van de Sande
Chief Designer, Mist
Ethereum Foundation*

Gustav Simonsson
Core Developer
Ethereum Foundation*

Viktor Tron
Core Developer: Go Client
Ethereum Foundation*

Fabian Vogelsteller
Lead Dapp Developer: Mist
Ethereum Foundation*

Shermin Voshmgir
Founder
BlockchainHub*

Vlad Zamfir
Proof of Stake Lead
Ethereum Foundation*

L'attaque « Multi-Stage »

C'est un appel récursif à la fonction « Split » au sein des **child-DAOs** recueillant ainsi plusieurs fois des ethers en une seule transaction.

Contract authors should take care to (1) be very careful about recursive call bugs, and listen to advice from the Ethereum contract programming community that will likely be forthcoming in the next week on mitigating such bugs, and (2) avoid creating contracts that contain more than ~$10m worth of value, with the exception of sub-token contracts and other systems whose value is itself defined by social consensus outside of the Ethereum platform, and which can be easily "hard forked" via community consensus if a bug emerges (eg. MKR), at least until the community gains more experience with bug mitigation and/or better tools are developed.

TheDAO IPO : $150M

~~L'attaque~~ Le « Multi-Stage »

C'est un appel récursif à la fonction « Split » au sein des **child-DAOs** recueillant ainsi plusieurs fois des ethers en une seule transaction.

> Contract authors should take care to (1) be very careful about recursive call bugs, and listen to advice from the Ethereum contract programming community that will likely be forthcoming in the next week on mitigating such bugs, and (2) avoid creating contracts that contain more than ~$10m worth of value, with the exception of sub-token contracts and other systems whose value is itself defined by social consensus outside of the Ethereum platform, and which can be easily "hard forked" via community consensus if a bug emerges (eg. MKR), at least until the community gains more experience with bug mitigation and/or better tools are developed.

TheDAO IPO : $150M

DAO.sol

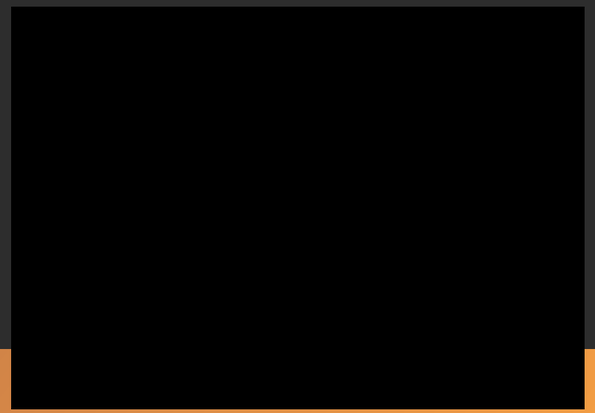
```
function splitDAO(
    uint _proposalID,
    address _newCurator
) noEther onlyTokenholders returns (bool _success) {

    [...]

    // Move ether and assign new Tokens
    uint fundsToBeMoved =
        (balances[msg.sender] * p.splitData[0].splitBalance) /
        p.splitData[0].totalSupply;
    if (p.splitData[0].newDAO.createTokenProxy.value(fundsToBeMoved)(msg.sender) == false)
        throw;

    [...]

    // Burn DAO Tokens
    Transfer(msg.sender, 0, balances[msg.sender]);
    withdrawRewardFor(msg.sender); // be nice, and get his rewards
    totalSupply -= balances[msg.sender];
    balances[msg.sender] = 0;
    paidOut[msg.sender] = 0;
    return true;
}
```




ANNNNNNNNNNNNNNND
SFYL!!

Commit f01f3bd

slockit/DAO

COMMIT COMMENTS

LefterisJP

5 days ago

Protect against recursive withdrawRewardFor attack

1 changed files with 2 additions and 1 deletions.

FILES CHANGED

DAO.sol

+2 -1


CHILD-DAO!
I AM YOUR FATHER

Bilan de The ĐAΩ (Juin 2016)

- 29 424 contributeurs uniques ont effectués 65 528 transactions.
- 19,6% des ethers envoyés à **TheDAO** proviennent d'adresses Genesis (Pre-sale).
- Les 100 plus gros contributeurs ont investit 47,4%.
- Les transactions vers **TheDAO** représentent 1,7% de toutes les transactions de la blockchain Ethereum.
- 50% des contributeurs ont acheté entre 2 et 50 ethers en moyenne.
- TheDAO possède 14% des ethers en circulation.
- ~3.6M d'ethers ont été « dérobés » soit 4,5% des ethers en circulation.

Đ

Distributed & Decentralized Autonomous Society

Crypto-médiation

Crypto-marché

Crypto-communication

Crypto-collaboration

Crypto-création

Vers des sociétés horizontales

Hétérarchie : un système d'organisation qui se distingue de la hiérarchie parce qu'il favorise l'**interrelation** et la **coopération** entre les membres plutôt qu'une structure ascendante. Les structures sociales à l'intérieur du système se **chevauchent** et s'**entrecroisent** ; les liens entre les membres sont multiples et l'ascendance est affaiblie par cette multiplicité de liens.

Wikipedia

SPACEX

Elon Musk veux commencer à coloniser Mars dès 2024 en y instaurant la démocratie directe comme forme de gouvernance.

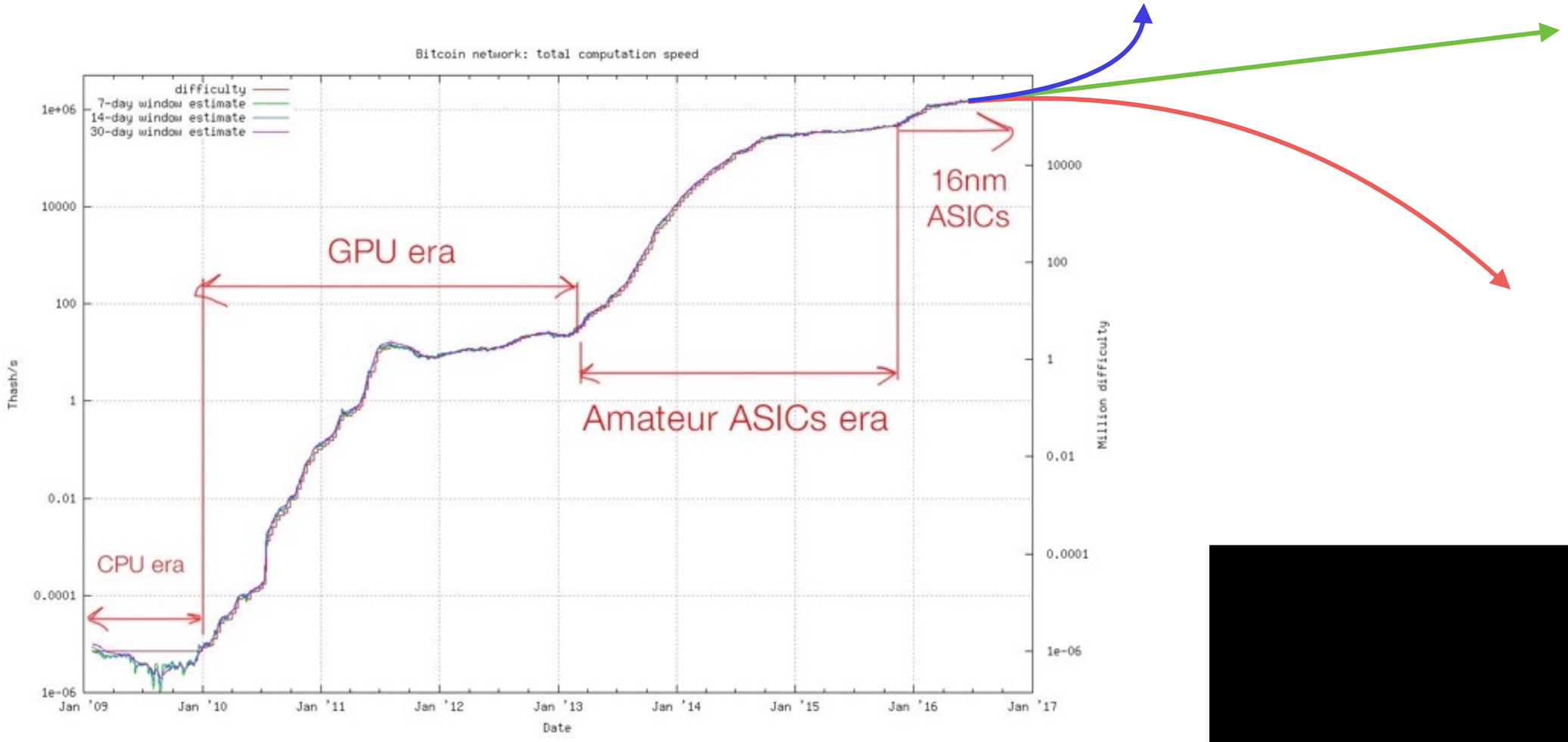
Questions & Réponses

alex@eurekacertif.com

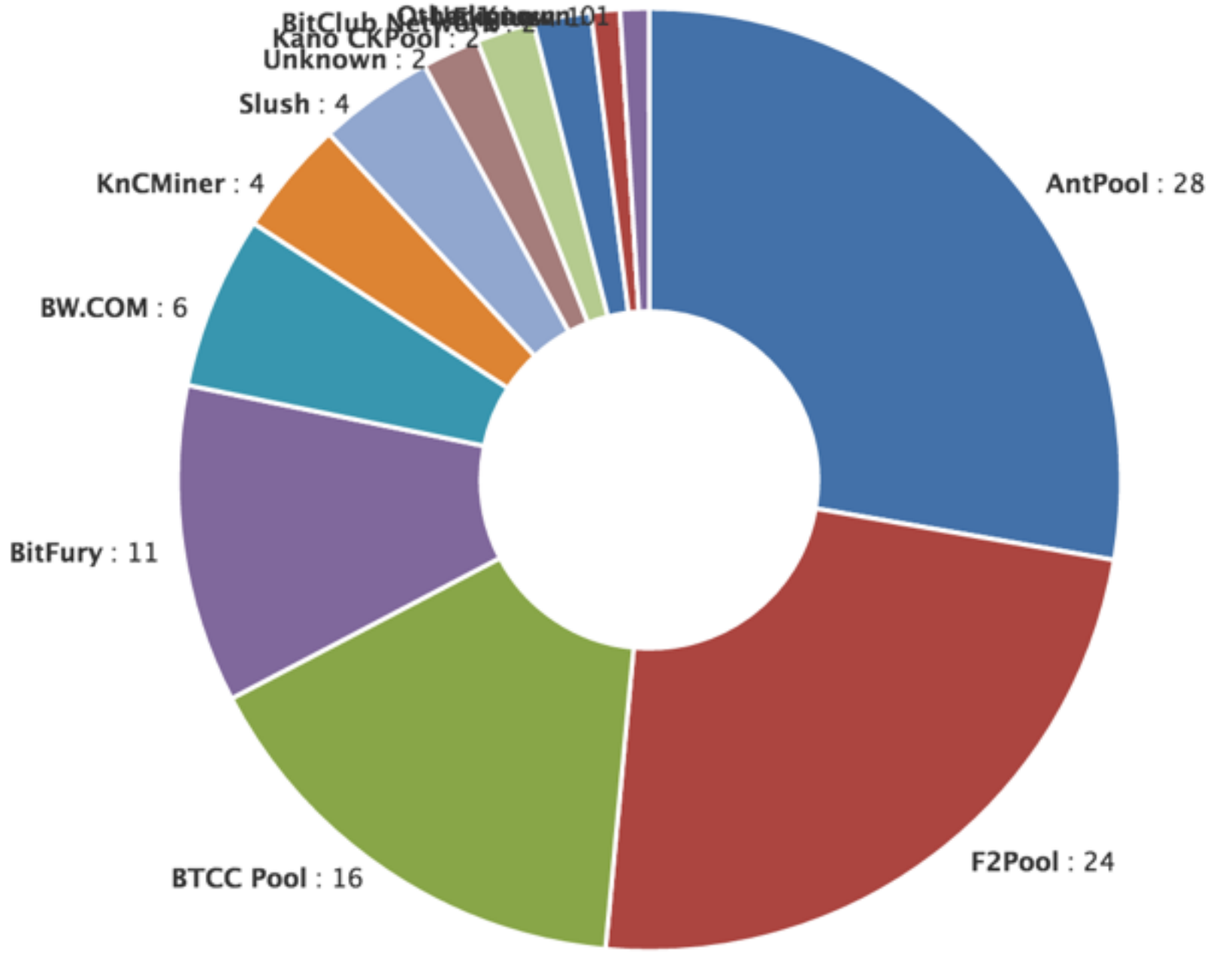
@EurekaCertif

VIVA TECHNOLOGY
STARTUP CONNECT / PARIS 2016

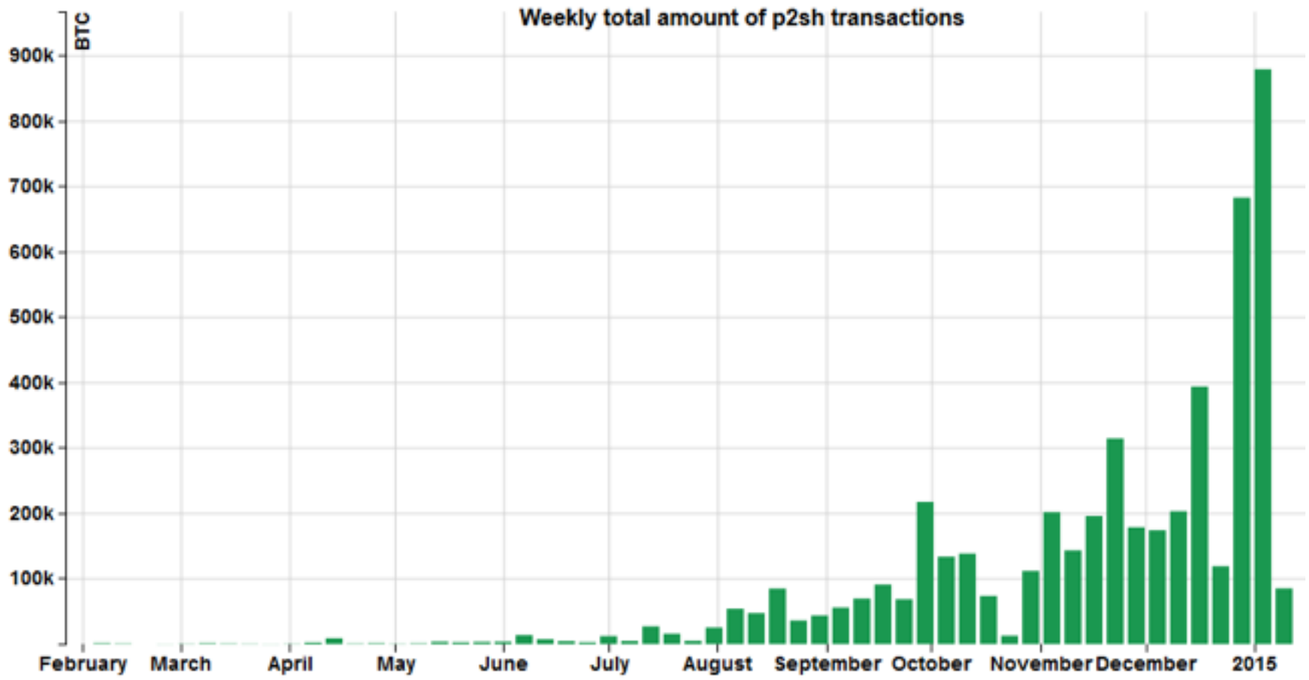
L'équipement dans le minage de Bitcoin



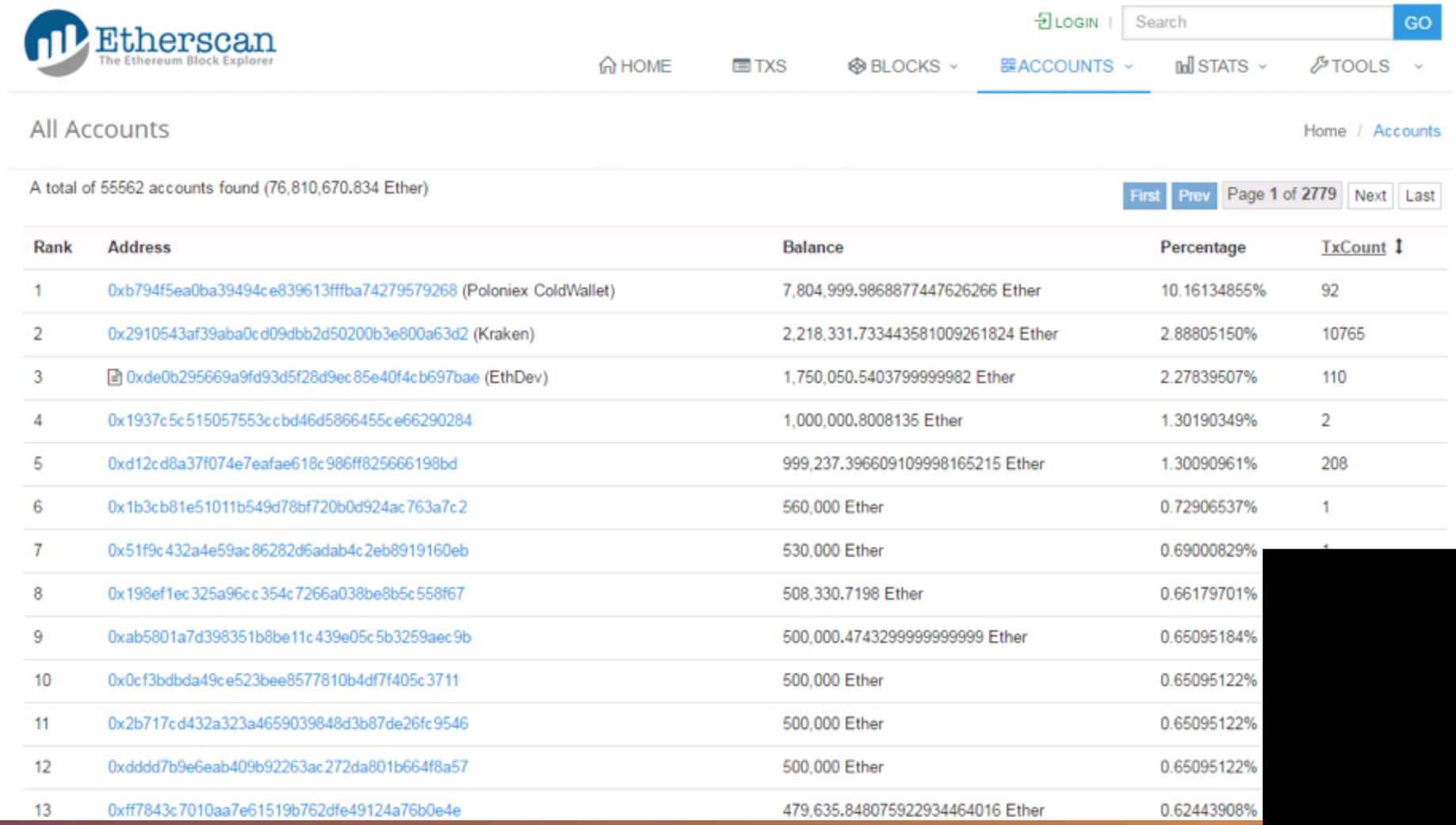
Les Pools de minages dans Bitcoin



Multi-signature (Bitcoin)



Les plus gros possédants d'ethers



Etherscan
The Ethereum Block Explorer

LOGIN | Search GO

HOME TXS BLOCKS ACCOUNTS STATS TOOLS

All Accounts

Home / Accounts

A total of 55562 accounts found (76,810,670.834 Ether)

First Prev Page 1 of 2779 Next Last

Rank	Address	Balance	Percentage	TxCount
1	0xb794f5ea0ba39494ce839613fffba74279579268 (Poloniex ColdWallet)	7,804,999.9868877447626266 Ether	10.16134855%	92
2	0x2910543af39aba0cd09dbb2d50200b3e800a63d2 (Kraken)	2,218,331.733443581009261824 Ether	2.88805150%	10765
3	0xde0b295669a9fd93d5f28d9ec85e40f4cb697bae (EthDev)	1,750,050.5403799999982 Ether	2.27839507%	110
4	0x1937c5c515057553ccbd46d5866455ce66290284	1,000,000.8008135 Ether	1.30190349%	2
5	0xd12cd8a37f074e7eafae618c986ff825666198bd	999,237.396609109998165215 Ether	1.30090961%	208
6	0x1b3cb81e51011b549d78bf720b0d924ac763a7c2	560,000 Ether	0.72906537%	1
7	0x51f9c432a4e59ac86282d6adab4c2eb8919160eb	530,000 Ether	0.69000829%	1
8	0x198ef1ec325a96cc354c7266a038be8b5c558f67	508,330.7198 Ether	0.66179701%	
9	0xab5801a7d398351b8be11c439e05c5b3259aec9b	500,000.4743299999999999 Ether	0.65095184%	
10	0x0cf3bdbda49ce523bee8577810b4df7f405c3711	500,000 Ether	0.65095122%	
11	0x2b717cd432a323a4659039848d3b87de26fc9546	500,000 Ether	0.65095122%	
12	0xdddd7b9e6eab409b92263ac272da801b664f8a57	500,000 Ether	0.65095122%	
13	0xff7843c7010aa7e61519b762dfe49124a76b0e4e	479,635.848075922934464016 Ether	0.62443908%	

Sources

[1] https://www.reddit.com/r/TheDao/comments/4oifss/myetherwallet_dao_splits_information/
[2] **Explication de l'exploit dans TheDAO** http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/
[3] http://ethereum.stackexchange.com/questions/3748/how-to-withdraw-ether-from-the-dao
[4] **Motiver les mineurs au soft fork** https://github.com/ethcore/hardforkbounty/blob/master/hardforkbounty.sol#L50-L52
[5] **Arrêt des retraits ETH -> FIAT des places de marchés** http://pastebin.com/aMKwQcHR
[6] **« Stalker Attack » sur un Split de DAO** https://github.com/slockit/DAO/wiki/Why-The-Stalker-attack-is-a-non-issue
[7] **La DAO contre-attaque** https://blog.slock.it/a-dao-counter-attack-613548408dd7#.9bphbeaiq
[8] **DAO 2.0** http://www.coindesk.com/cornell-prof-discovered-dao-vulnerability-reveals-10-exploits/
[9] **Réseau stellaire de la NASA** http://www.journaldugeek.com/2016/06/22/nasa-nouvel-internet-ultra-performant-iss-dtn/
[10] https://www.cryptocoinsnews.com/bitcoin-100-times-powerful-google/