

Les chaînes de blocs

Fonctionnement, perspectives et
approches stratégiques

Définition

« Protocole de registre distribué ouvert »



Les « altcoins »



<http://coinmarketcap.com/>

Une adresse Bitcoin





Open Source JavaScript Client-Side Bitcoin Wallet Generator

Single Wallet Paper Wallet Bulk Wallet Brain Wallet

Vanity Wallet Split Wallet Wallet Details

Generate New Address Print

Bitcoin Address **Private Key**

 **SHARE** **SECRET** 

1HVjW8d3e5uggYBVSqKRdque5pCaQFW5FB

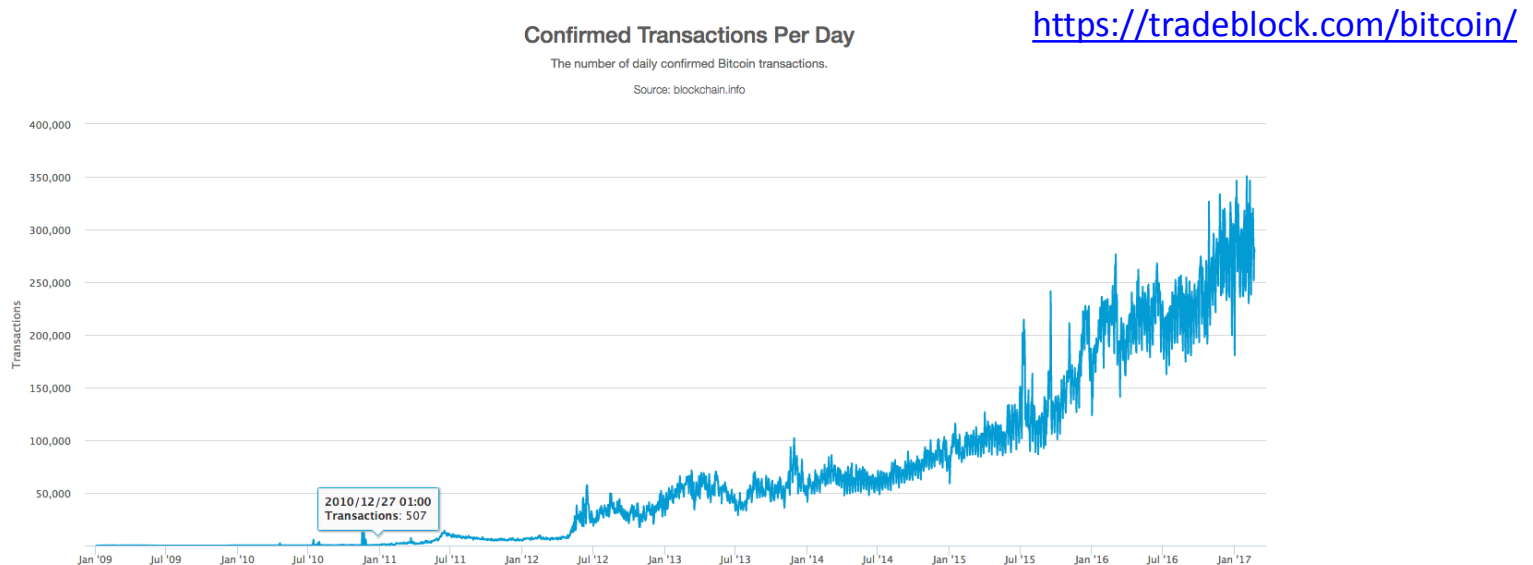
L4PbjBVakemwtrupLE1WS5SEx6tn9dPEfoNf1DAjcXi49gdJVe4

A Bitcoin wallet is as simple as a single pairing of a Bitcoin address with its corresponding Bitcoin private key. Such a wallet has been generated for you in your web browser and is displayed above.

To safeguard this wallet you must print or otherwise record the Bitcoin address and private key. It is important to make a backup copy of the private key and store it in a safe location. This site does not have knowledge of your private key. If you are familiar with PGP you can download this all-in-one HTML page and check that you have an authentic version from the author of this site by matching the SHA256 hash of this HTML with the SHA256 hash available in the signed version history.

Une transaction Bitcoin

- Je télécharge un « wallet » (portefeuille)
- Je protège ma clé privée
- Je donne mon adresse publique
- Je reçois le paiement



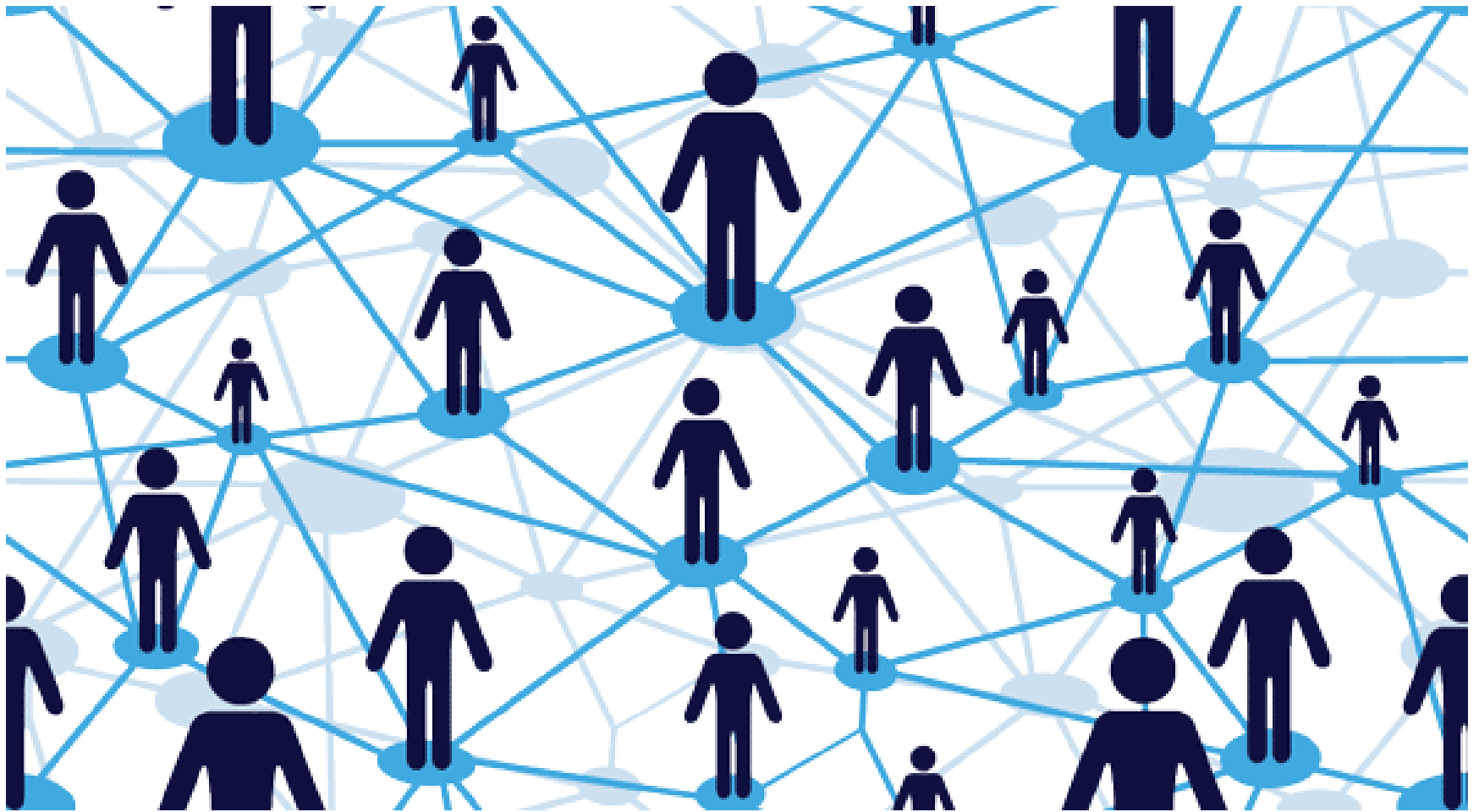
Les aspects monétaires

- Bitcoin peut être considéré comme une monnaie complémentaire
- Mais c'est avant tout un protocole
- C'est aussi une expérience humaine
- La quantité de BTC est limitée en valeur

« It's very attractive to the libertarian viewpoint if we can explain it properly. I'm better with code than with words though. »

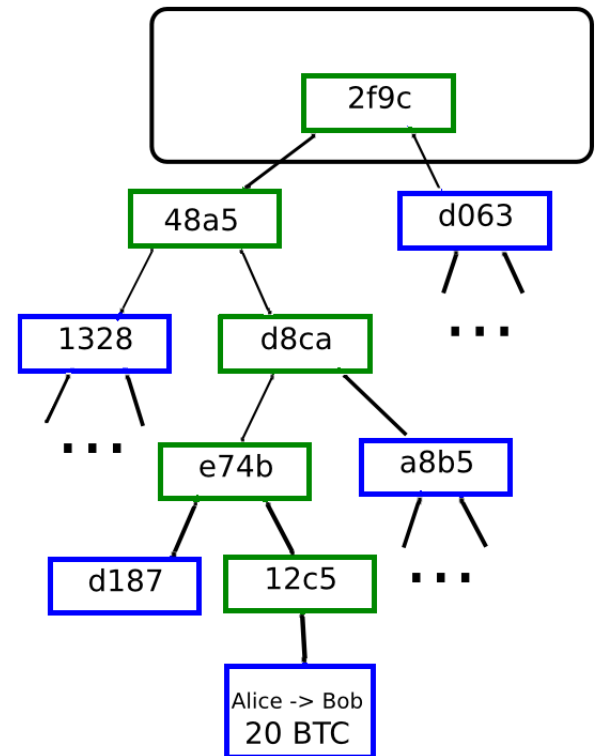
Satoshi Nakamoto

« L'Internet de la valeur »



Une combinaison de technologies

- Réseaux pair-à-pair
- Les arbres de Merkle
- Cryptographie asymétrique
 - Fonctions de hashage



Comment ça marche ?

- Démo

Blockchain

Block: # 1

Nonce: 11316

Data:

Prev: 00

Hash: 000015783b764259d382017d91a36d206d0600e2c

Mine

Block: # 2

Nonce: 35230

Data:

Prev: 000015783b764259d382017d91a36d206d0600e2c

Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5

Mine

<https://anders.com/blockchain/blockchain.html>

The Genesis Block



Ethereum

- Une « plateforme d'application distribuée »
- Créée à la fin de l'automne 2013
- Live depuis juillet 2015
- Du PoW au PoS...



Lire « Les premiers pas d'Ethereum »

Vitalik Buterin



2 types d'adresses

- Adresses classiques (comme avec Bitcoin)

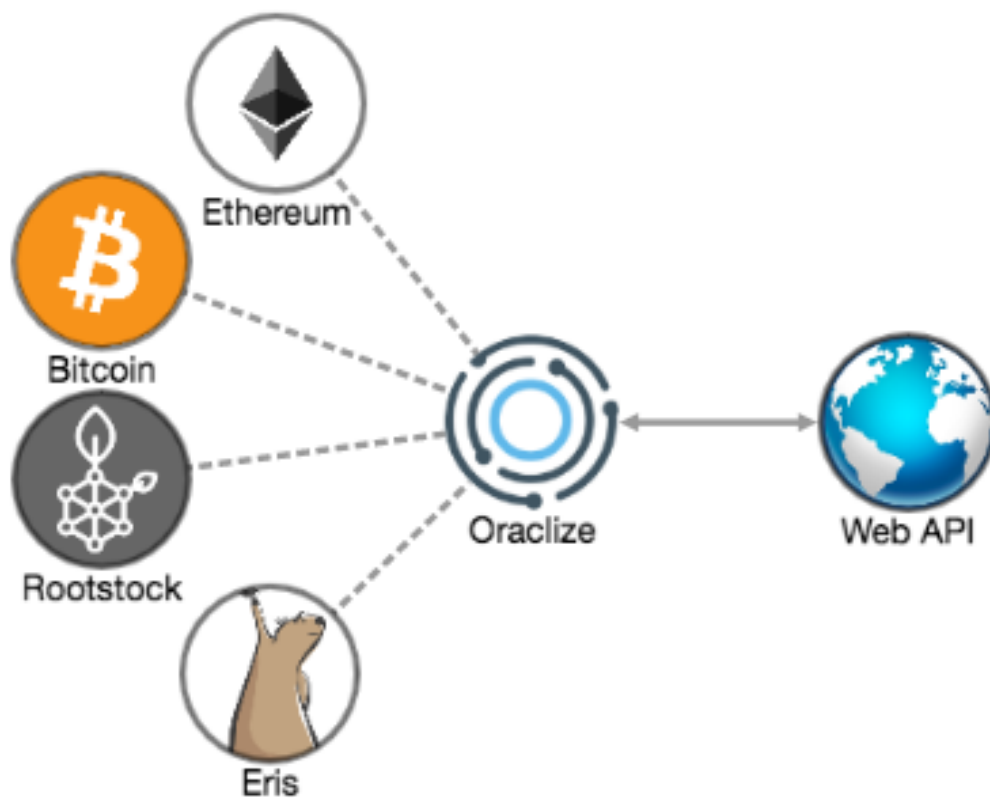
<https://www.myetherwallet.com>

- Contrats autonomes (« smart contracts »)

```
Roulette.sol
1  contract Roulette {
2
3      uint public lastRoundTimestamp;
4      uint public nextRoundTimestamp;
5
6      address _creator;
7      uint _interval;
8
9      enum BetType { Single, Odd, Even }
10
11     struct Bet {
12         BetType betType;
13         address player;
14         uint number;
15         uint value;
16     }
17
18     Bet[] public bets;
19 }
```

<https://www.ethereum-france.com/ecrire-une-dapp-pour-ethereum-1-smart-contract/>

Les oracles



La notion d'actif numérique

Actif numérique infalsifiable = titre numérique
= Token = Jeton = Coin

- Obligations
- Monnaies complémentaires
- Documents officiels
- « App coin »
- Droit de vote
- Bons de fidélité
- ...

Démo

- Déployer un contrat autonome
- Interagir avec un contrat

JujuCoin !

Le cas « The DAO »

- Un faille dans le contrat
- Investissement sauvage
- « No funds at risks »
- The Dark DAO
- Les règles propres au contrat
- Discussion au sein de la communauté
- Le « hard fork »

5 types d'acteurs



- Les mineurs
- Les développeurs principaux (core devs)
- Les plateformes d'échanges
- Les développeurs de dapps
- Les utilisateurs

Expérience utilisateur

- iExec demo app
 - <http://52.44.51.109:8080/>

On utilise Metamask :

CONFIRM TRANSACTION ● Ropsten Test Net

Número1
7e80fE...60EF  **>**  197EcC...c851

5.983 ETH
76.09 USD

Amount	...
Max Transaction Fee	0.004000 ETH 0.05 USD
Max Total	0.004000 ETH 0.05 USD

Data included: 4 bytes

ACCEPT **REJECT**

Les cas d'utilisations actuels

- Transfert de fonds
- Obligations/crowdfunding
- Jeux d'argent
- Assurance (<https://fdd.etherisc.com/>)
- Gouvernance

Les enjeux pour un état

- Trop de régulation gênerait l'innovation
- Pas de régulation peut engendrer des risques
- L'état peut et doit prendre l'initiative
- Il devrait expérimenter activement
- Se prémunir des risques d'évasion fiscale

Identité numérique

- Notion de « Self Sovereign Identity »
 - Pour les citoyens
 - Pour les réfugiés
- L'état ou les mairies peuvent s'affirmer en tant qu'organismes validateur
- Beaucoup plus sain (Open Source)
- Le « paradigme Satoshi »



Le vote en ligne

- Le Graal à portée de main
- Défi d'inclusivité
- Des millions d'économie



Mutuelles et assurances

- Gestion transparente d'une caisse commune
- Coût de gestion beaucoup plus faibles
- Rapidité du service

Outil de l'aide a développement

- L'argent va directement dans les mains des bénéficiaires
- Réduction des risques de corruption

Gestion des droits d'auteur

- SACEM
- INPI
- Documents protégés à vie à un coût ridicule

Réglementation des casinos

- Remise en cause du monopole de la Française des jeux

Traçabilité

- Certificats on-chain pour tous types de produits

Gouvernance supra-étatique

- Global Challenge 2017
- ...

Julien Béranger

06 30 90 54 48

jb@iex.ec

@julienbrg