Les chaînes de blocs

Fonctionnement, perspectives et approches stratégiques

Définition

« Protocole de registre distribué ouvert »

Les « altcoins »

http://coinmarketcap.com/

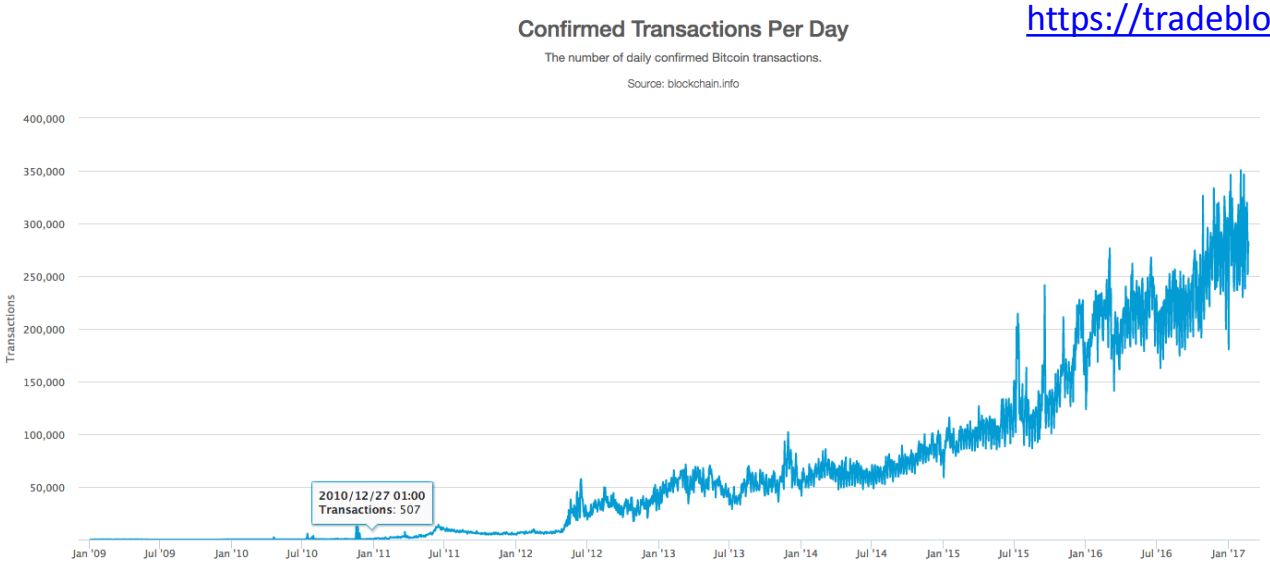
Une adresse Bitcoin

https://www.bitaddress.org

Une transaction Bitcoin

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

https://tradeblock.com/bitcoin/



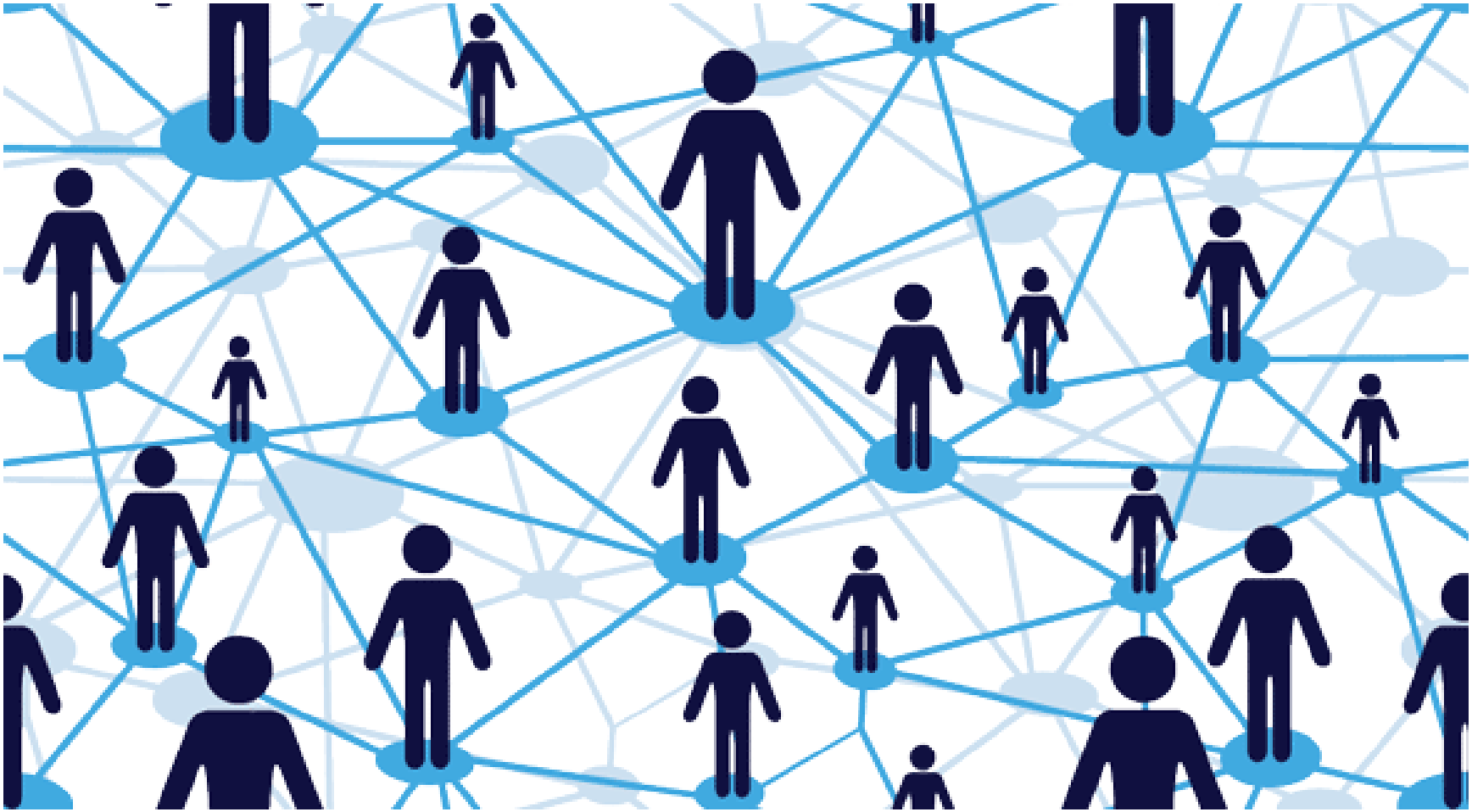
Les aspects monétaires

- 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. »

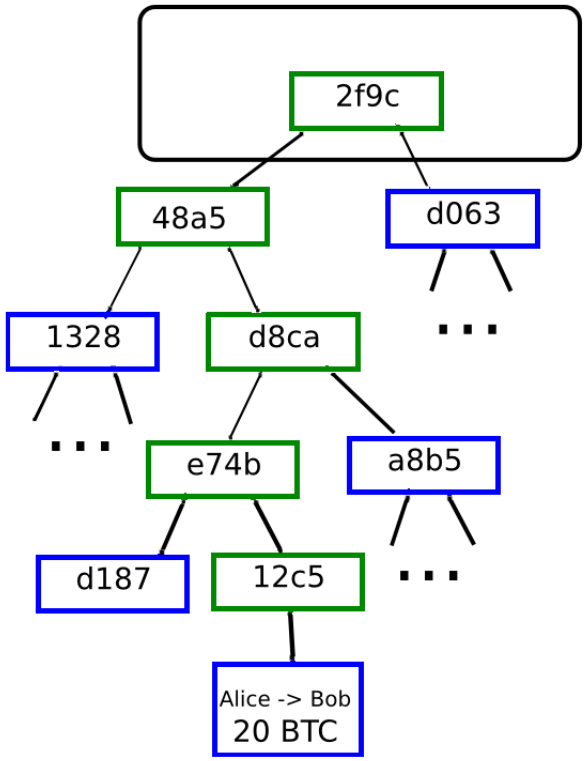
Satoshi Nakamoto

« L’Internet de la valeur »



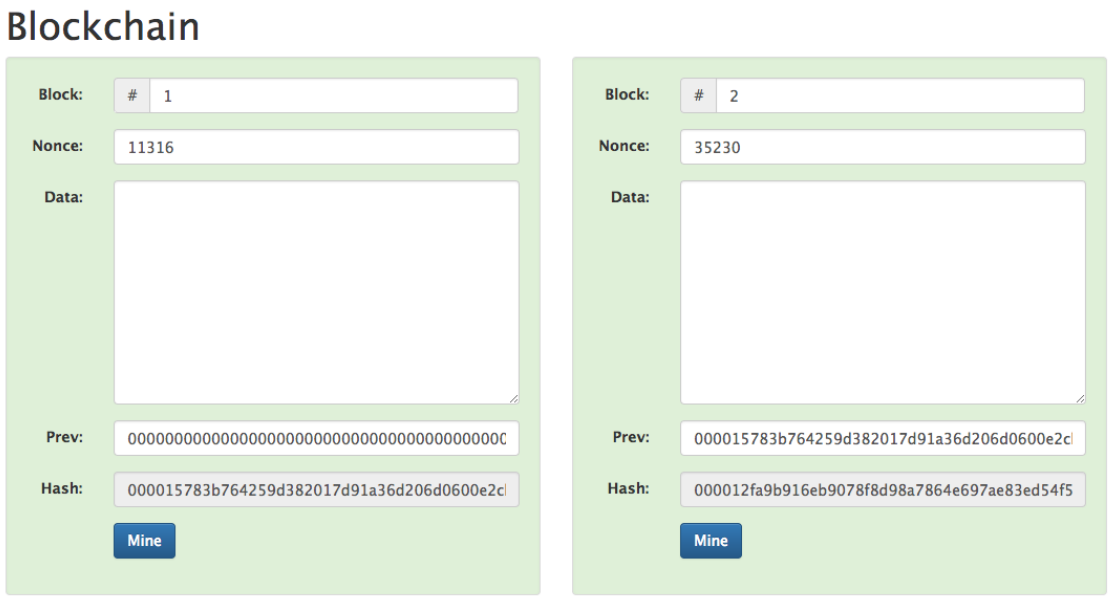
Une combinaison de technologies

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



Comment ça marche ?

- Démo



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 »

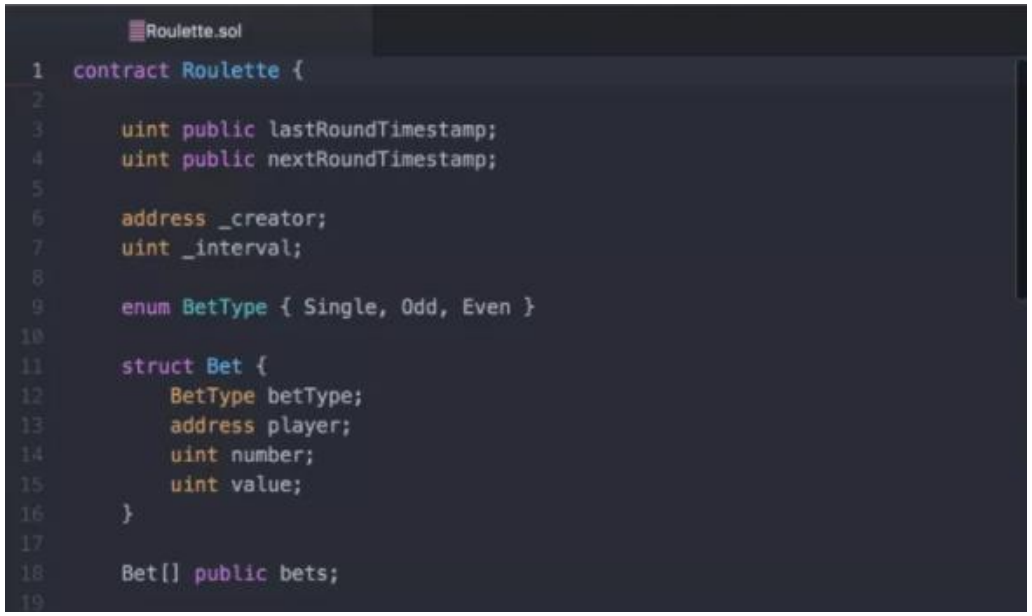
Vitalik Buterin

2 types d’adresses

- Adresses classiques (comme avec Bitcoin)

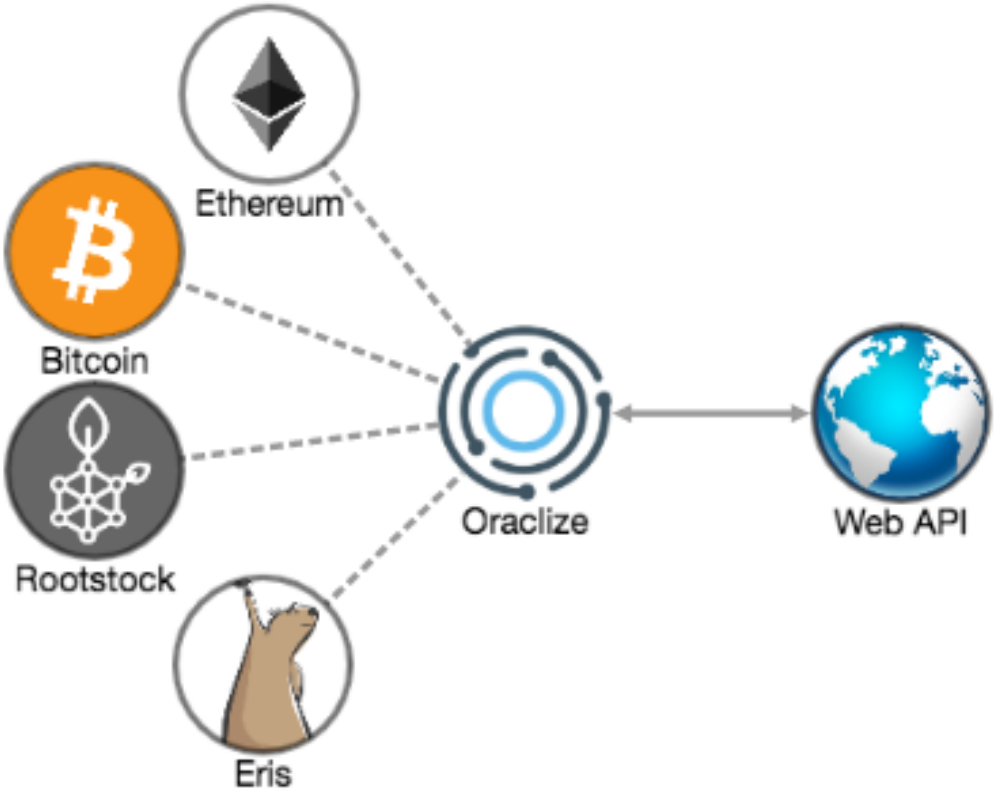
  https://www.myetherwallet.com

- Contrats autonomes (« smart contracts »)



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 »

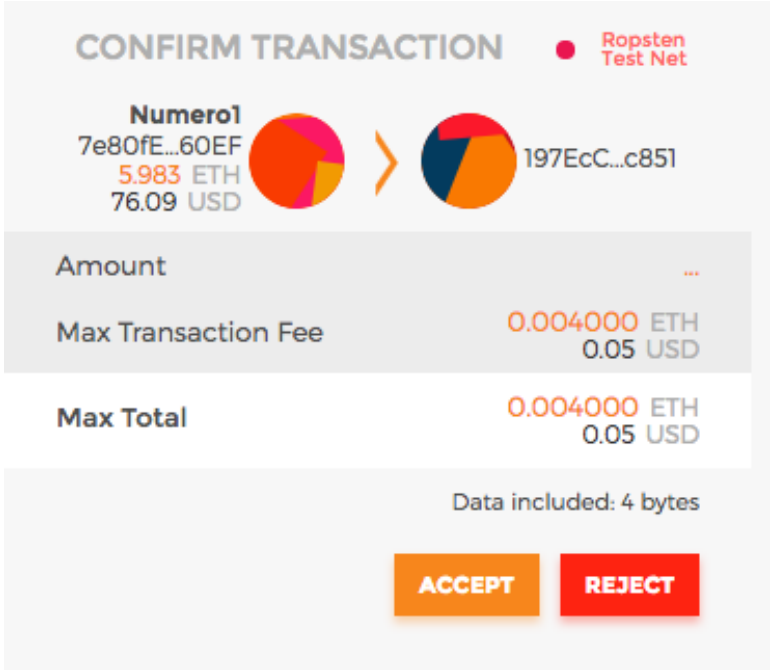
5 types d’acteurs

- 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 :



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