



Analyse critique du phénomène blockchain

Meetup du 8 avril 2019

rjouin@ayming.com

0652868730

La blockchain fête ses 10 ans

Une invention datant de 2009

Satoshi Nakamoto

Naissance 5 avril 1975 (44 ans)

Profession Informaticien, entrepreneur, programmeur

Activité principale Créeur du Bitcoin

1 Bitcoin égal

4 596,60 Euro

7 avr. à 21:34 UTC · Clause de non-responsabilité

1	Bitcoin
4596,60	Euro



Poussant à la numérisation du monde

Bloc 46

Transaction 92
Transaction 93
Transaction 94
Transaction 95

Bloc 47

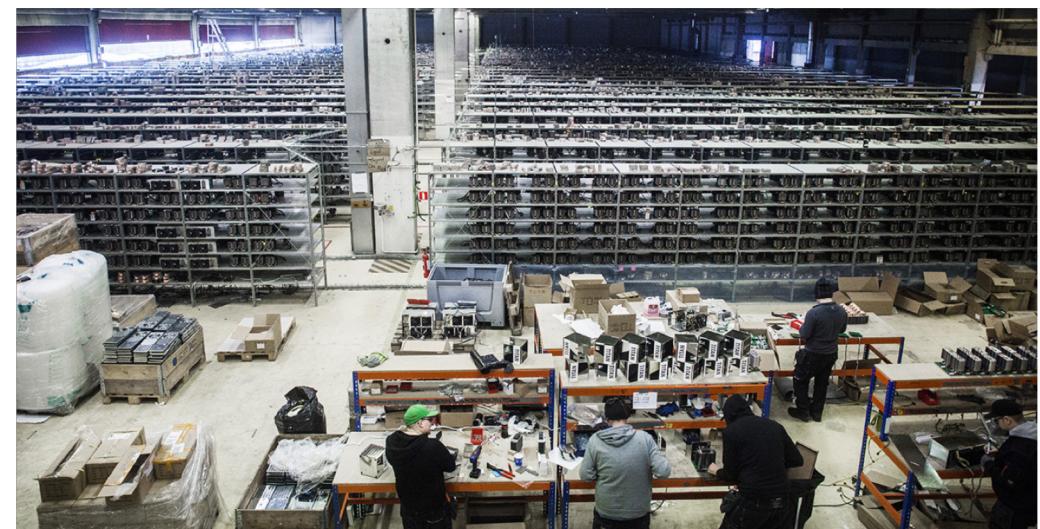
Transaction 96
Transaction 97
Transaction 98

Bloc 48

Transaction 99
Transaction 100
Transaction 101

Bloc 49

Transaction 102
Transaction 103
Transaction 104
Transaction 105

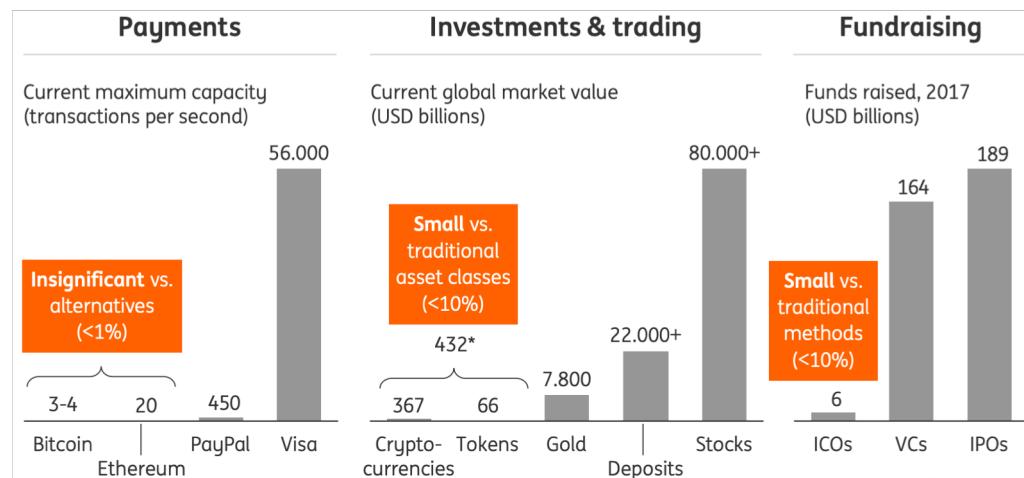


Les mineurs ont plus de moyens que vous on dirait (ici KnC Miner) - Crédits Stefan Bladh



La blockchain vit son premier hiver

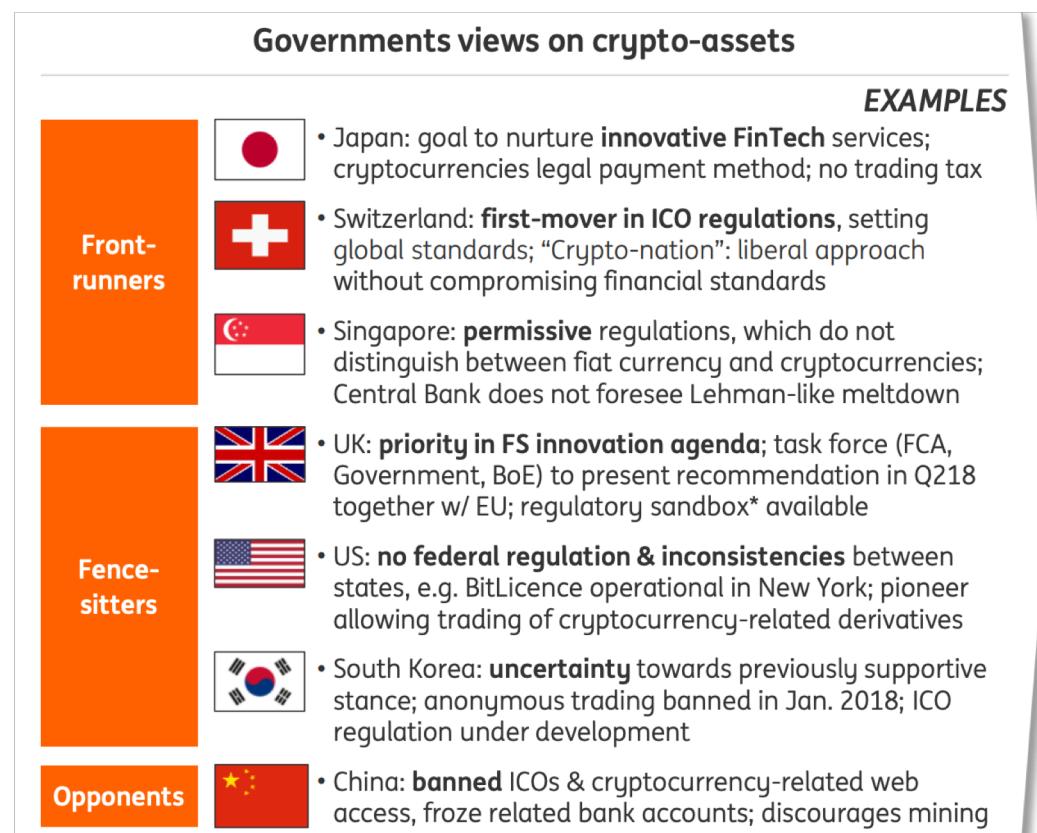
May 9th, 2018



Des risques nombreux :

- Manque de standardisation
- Investisseurs insuffisamment formé pour évaluer les risques
- Les lois de protection des consommateurs doivent être clarifiées
- cyber-menaces
- Abus de marché

La réaction des états est mitigée



https://www.ecb.europa.eu/paym/groups/pdf/fxcg/2018/20180906/Item_2a - Cryptocurrencies_and_tokens.pdf



Abus du marché ? Abus de marché ?

<https://insights.coinhouse.com/fr/bce-abandonne-euro-au-profit-cryptoeuro/>



par MANUEL VALENTE le 01/04/2019

LES COURS EN DIRECT

EUR	GBP	BTC	USD
฿	BTC	€ 4,608.29 (2.89%) ▲	
♦	ETH	€ 154.74 (5.02%) ▲	
✗	XRP	€ 0.3214 (2.03%) ▲	

+200 crypto-monnaies

- ADA (Cardano) - AVYARTBYTE ARK (Ark) - ADT (AdToken) - AEON (Aion) - AID (AidCoin) - AMP (Synereo) - AGRS (Adni Agoras) - ANT (Aragon) - AUR (Auroracoin) - ARDR (Ardor) - ADX (Adex) - B - (BTC) (Bitcoin) - BCH (Bitcoin Cash) - BTG (Bitcoin Gold) - BSD (Bitsend) - BAY (Bitbay) - BLOCK (Blocknet) - BLT (Bloom) - BLT (Bloom) - VEE (BlockV) - BCPT (Block Mason Credit P) - BAT (Basic Attention Token) - BFT (BnkToTheFutur) - SWIFT (Bitswift) - BLK (Blackcoin) - BLITZ (Blitz cash) - BNT (Bancor) - BCY (Bitcrystals) - BITB (Bean cash) - BNK (Bankex) - BURST (Burstcoin) - BRK (Breakout) - BRX (Breakout Stake) - BYC (Bytecent) - C - (CMCT) (Crowd Machine) - CANN (Cannabis Coin) - CBC (CashBet) - CFI (Cofoundit) - CLAMS (Clam) - CLUB (Clubcoin) - CPC (Capricoin) - CRB (Creditbit) - CRW (Crown) - CURE (Curecoin) - CVC (Civic) - COVAL (Circuit of value) - CLOAK (Cloakcoin) - D - (DCR) (Decred) - DCT (Decent) - DNT (Districtox) - DOGE (Dogecoin) - DASH (Dash) - DGB (Digibyte) - DYN (Dynamic) - DOPE (Dopecoin) - DTB (Detabits) - DMD (Diamond) - DMT (Dmarket) - E - (EBST) (Eboost) - EDG (Edgeless) - EFL (e-Gulden) - EGC (Evergreen Coin) - EMC (Emercoin) - EMC2Einsteinium ENRG (Energycoin) - ENG (Adni Enigma) - ERC (Europecoin) - EX-P (Expanse) - ETH (Ethereum) - ETC (Ethereum Classic) - EXCL (Exclusivcoin) - F - (FAIR) (Faircoin) - FCT (Factom) - FLO (Flocash) - FLDC (Foldingcoin) - FTC (Adni Feathercoin) - GBYTE (Byteball bytes) - G - (GAM) (Gambit) - GCR (GlobalCurrency) - GBG (Golos Gold) - GOLOS (Golos) - GLD (Goldcoin) - GNO (Gnoisis) - GNT (Golem) - GRC (Gridcoin) - GRS (Groestlcoin) - GUP (Matchpool) - GAME (Game credit) - GEO (Gift) - H - (HMQ) (Humaniq) - I - (IGNIS) (Ignis) - INCNT (Incent) - INFX (Influxcoin) - IOC (IO coin) - ION (Ion) - IOP (Internet of people) - K - (KMD) (Komodo) - KORE (Kore) - L - (LBC) (LBRY Credit) - LRC (Loopring) - LMC (Lomoco) - LOOM (Loom Network) - LSK (Lisk) - LTC (Litecoin) - LUN (Lunyr) - M - (MAID) (MaidSafeCoin) - MANA (Decentraland) - MCO (Monaco coin) - MFT (MainFrame) - MONA (MonaCoin) - MOR (More Coin) - MER (Mercury) - MEME (Memetic Pepecoin) - MLN (Melon) - MUE (Monetary Unit) - MUSIC (Musicoin) - N - (NGC) (Naga) - NAV (Navcoin) - NEO (Neo) - NEOS (Neos coin) - NLG (Gulden) - NMR (Numeraire) - NLC2NoLimitCoin NXC (Nexium) - NXS (Nexus) - NXT (Nxt) - O - (OCN) (Odyssey) - OMNI (Omni) - OK (OK cash) - OMG (OmiseGo) - P - (PART) (Particl) - PDC (Project decorum) - PINK (PinkCoin) - PIVX (Privx) - POLY (Polymath) - PRO (Propy) - POWR (Power Ledger) - PAY (TenX) - PKB (Parkbyte) - PPC (Peercoin) - PT-C (Pesetacoin) - PTOY (Patientory) - POT (Potcoin) - Q - (QRL) (Quantum Resist) - QTUM (Qtum) - QWARK (Qwark) - R - (RADIS) (Radium) - RBY (RubyCoin) - RCN (Rcoin) - RDD (Reddcoin) - REP (Augur) - RCN (Ripio Credit Network) - RISE (Rise) - RLC (Iexec RLC) - RVR (RevolutionVR) - RVN (Raven) - RFR (Referum) - S - (SALT) (Salt) - SBD (Steem dollar) - SEQ (Sequence) - SHIFT (Shift) - SNRG (Synergie) - SC (SiaCoin) - SIB (Sibcoin) - SRN (Sirin Labs Token) - SLR (SolarCoin) - SLS (SaluS) - SNT (Status) - SPR (Spredcoin) - SPHR (Sphere) - START (StartCoin) - STEEM (Steem) - STORM (Storm) - STORJ (Storj) - SYNX (Syndicate) - SYS (Syscoin) - SWT (Swarm City Token) - STRAT (Stratis) - T - (THC) (Hempcoin) - TIX (Blocktix) - TRON (Tronix) - TRUST (Trustplus) - TRST (WeTrust) - TUSD (TrueUSD) - TX (Transfercoin) - TKS (Tokes) - TUBE (Bitube) - U - (UNB) (Unbreakablecoin) - UKG (Unikoin Gold) - USNBT (NuBits) - UHQ (Ubiq) - UP (UpToken) - V - (VIA) (ViaCoin) - VIB (Viberate) - VTC (Vert Coin) - VRC (Vericoin) - VRM (Verium) - VTR (Vtorrent) - W - (WAVES) (Waves) - WAX (Wax) - WINGS (Wings dao) - X - (XDN) (Digital note) - XEL (Elastic) - XLM (Stellar) - XCP (Counter Party) - XMG (Magi) - XMY (Myriad) - XRP (Ripple) - XST (Stealthcoin) - XVC (Vcash) - XVG (Verge) - XWC (Whitecoin) - XZC (Zcoin) - Z - (ZCL) (Zclassic) - ZEC (Zcash) - ZEN (Horizen) - ZRX (Ox)



Trois siècles de glissement vers le nombre

- Foucault : Le marché comme lieu de justice (<XVIII)

- Un prix juste, lié au travail
- Un prix distributif
- Une protection de l'acheteur, anti fraude
- Un lieu de juridiction
- Puis le marché comme lieu de vérification (XVIII)
 - Mécanismes spontanés
 - La main invisible
 - Bon prix, prix naturel, Juste prix
 - La valeur produit
 - Prix validé par les parties prenantes

- Glissement sur la gouvernementalité

- D'une gouvernementalité de justice
- A une gouvernementalité de la vérité
 - Vérité dans le chiffre
 - Via le commerce, source de la puissance de l'état
 - Westphalie
 - Colonies et or
 - Croissance économique et démographique
 - Education de technicien / écoles
 - Théories économiques

- Question de la vérification

- Quels sont l'ensemble des prérequis culturels qui permettent l'émergence d'une distinction entre vrai et faux ?
- Cad : quelle philosophie sociale nous amène à utiliser la blockchain et l'IOT pour décider de la réalité du monde ?



Le droit comme outil d'analyse historique

6

● Les cultures juridiques s'adaptent aux contextes

○ Ex : le droit social

○ XIX :

- solidarités traditionnelles déplacées par le capitalisme
- Émergence de l'état social

○ XX :

- « Projet de marché total peuplé de particules contractantes n'ayant entre elles de relations que fondées sur le calcul d'intérêt » (p15)
- État social remis en cause par l'ubérisation
- Mouvement de réidentification religieuse, ethnique, régionaliste, nationalité
 - Solidarité de combat via une vision binaire »ami/ennemi»

● Alain Supiot :

- L'être humain exosomatique (Stiegler) projette ses pensées sur le monde
- Révolution industriel = imaginaire industriel (*Métropolis*)
 - Lois de la physique classique
- Révolution numérique = imaginaire du calcul
 - Gouvernance par le nombres
 - Rêve de l'harmonie par le calcul
 - Like Facebook
 - Imaginaire cybernétique
 - Normativité non législative mais programmatique
 - « On n'attend plus des hommes qu'ils agissent librement dans le cadre des bornes que la loi leur fixe, mais qu'ils réagissent en temps réel aux multiples signaux qui leur parviennent pour atteindre les objectifs qui leur sont assignés » (p23)



Le chiffre comme rêve de contrôle du monde

● Normativité sur le chiffre

- Pythagore : « Tout est arrangé d'après le nombre »
- Bible : Dieu « a tout réglé avec mesure, nombre et poids » (Sg. XXI 20)
- Villani : « le monde est mathématique »

● Mathématique

- clé d'accès au divin
- Intelligibilité du monde
- Maîtrise du monde
- Percer les secrets de l'harmonie universel, ressort de la science

● Dénégation de la spécificité de l'être humain : capacité à rêver

● La loi n'est pas rationnelle

- Le fruit de heurts, de désir, de confrontation, d'injustice, de passion
- Aristote
 - Justice distributive : géométrique , au mérite
 - Justice réparatrice : arithmétique, dédommagement
 - Justice réciproque : a-mathématique, les besoins
 - L'argent comme étalon
 - Fondée sur la loi (monnaie *nomisma* de *nomos*, la loi)
- Des mathématiques irrationnels :
 - Racine carré : nombre irrationnels



La blockchain comme clôture du numérique sur lui même

- Blockchain

- Smart contract

- Absence de discussion

- Qui programme ?

- IOT

- Comment vérifier ?

- Décision

- Comment contester ?

- La foi dans les nombres supplante la confiance dans les personnes

- Quantifier c'es objectiver en apparence

- Mais le monde ne se réduit pas à la mesure

- Il y a de l'immesurable, et de l'imprédictible

- L'être humain n'est pas soumis aux lois de la nature

- Freud

- Folie

- Pulsion

- Les faits sont des construits, qui dépendent de nos perceptions et outils

- L'homme n'existe pas, il est en en perpétuelle évolution

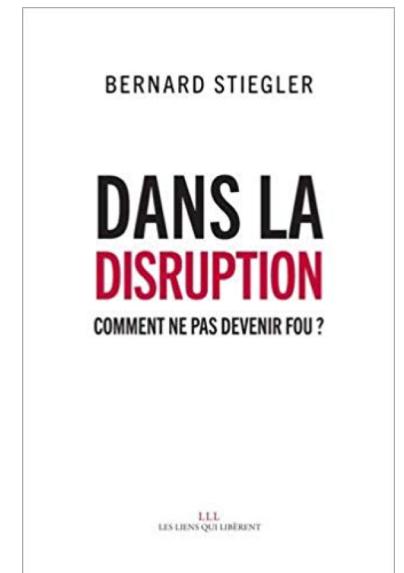
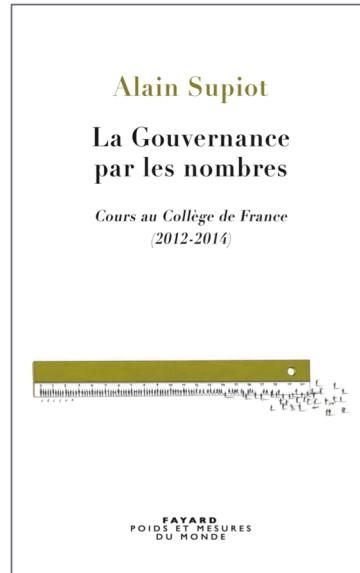
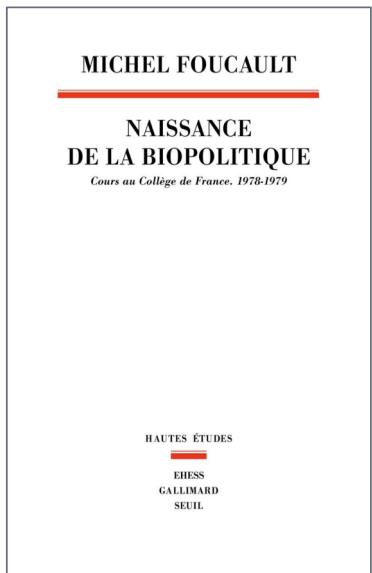
- Il y a des mondes en dehors de la physique

- Biologie

- Chimie



Références



Antoinette Rouvroy
La gouvernementalité
algorithme ou l'art de ne
pas changer le monde

<https://youtu.be/bNN3PMkMSfY>