

Vocabulaire de base

DYOR (Do Your Own Research)

Sigle qu'on retrouve souvent sur les plates-formes (forums, réseaux sociaux, etc.) qui s'intéressent aux crypto monnaies et aux blockchains.

Les sujets crypto/blockchains évoluent vite, l'information est contradictoire, les sujets sont techniques... or il y a beaucoup de bêtise et d'intérêts en jeu.

DYOR ça veut dire :

- Ne PAS faire confiance à une seule source
- Croiser et confronter l'information
- Vérifier l'information

Nodes, noeud, server...

Ordinateurs font fonctionner le même logiciel et qui participent constituer un même "réseau" qui se superpose à internet.

Crypto Chemists

L'équipe

Glenn Rolland (aka Glenux)

- **Senior Infrastructure Engineer**
- Open-source lover & doer
- glenn@cryptochemists.com

Hayat Outahar

- **Senior Digital Project Manager**
- CypherCulture enthusiastic
- hayat@cryptochemists.com

Notre vision

Nous pensons que les technologies des Blockchain & des crypto-actifs qui vont changer nos vies dans un futur très proche.

Ce qu'on fait

- **Vulgariser les concepts de la Blockchain et des crypto-actifs pour rendre accessible la compréhension de ces sujets par tous.**
- Donner des formations et des conférences en entreprise et des des workshops.
- Traiter tant l'aspect théorique que l'aspect pratique grâce à nos compétences complémentaires.

Nous contacter

- Facebook : CryptoChemists
- Twitter : @cryptochemists
- Instagram : @cryptochemists
- Linkedin : CryptoChemists
- Reddit : r/CryptoChemists

- Youtube : [CryptoChemists](#)
- Telegram: t.me/CryptoChemists
- Email : hello@cryptochemists.com
- Web : cryptochemists.com

No financial advice!

Ceci n'est pas du conseil en investissement

- Nous aborderons les SEULEMENT les questions technologiques, économiques, politiques, philosophiques liées aux blockchains et crypto-actifs
- Nous ne parlerons PAS de stratégie d'investissement ou de trading

Avertissement

- Les investissements liés aux crypto-actifs sont risqués par nature
- Faire vos propres recherches avant d'entreprendre toute action liées aux crypto-actifs
- N'investir que dans les limites de vos capacités financières
- N'investir que ce que vous êtes prêts à perdre
- Nous vous recommandons de consulter un conseiller financier indépendant

Limites du conseil en investissement pour les crypto-actifs

- Encadrement juridique des prestataire de services sur actifs numériques (PSAN)
- Obligations : s'enregistrer auprès de l'Autorité des marchés financiers (AMF)

References

- [AMF, Investir en crypto-actifs : quel professionnel choisir ?](#)

Cryptographie

Définition

- branche des mathématiques
- pour échanger des messages en assurant leur confidentialité, leur authenticité et leur intégrité
 - rendre illisible un message
 - à l'aide de secrets ou de clés
- autrement dit:
 - transformer un message par un mécanisme simple (algorithme)
 - s'assurer que mon correspondant peut le déchiffrer, mais personne d'autre
 - (en option) s'assurer que c'est un vrai
 - (en option) s'assurer qu'ils n'ont pas été modifiés

Cryptographie symétrique

Histoire

Existe depuis l'antiquité

- Xe siècle av J.C : Technique Grecque, la Scytale lacédémonienne (permutation/transposition)
- Ve siècle avant J.C : Technique des Hébreux, l'Atbash
- IIe siècle avant J.C : Technique Grecque, le carré de Polybe (substitution d'une lettre par sa position X,Y dans un carré)
- Ie siècle avant J.C : Technique Romaine, le Code de César
- IXe siècle : premier manuscrit de cryptanalyse par Al-Kindi
- XIVe siècle : recueil de code et de clés, le nomenclateur par Gabriele de Lavinde, pour chiffrer des mots ou syllabes courants, utilisé pendant plusieurs siècles par les diplomates.
- accélération des méthodes de chiffrement et méthodes de cryptanalyse depuis ...

Fonctionnement

Méthodes classiques

- Substitution
 - Atbash (substitution alphabétique inversée)
 - Code de César (substitution par décalage d'une lettre)
 - le chiffre de Vigenère
 - Enigma
- Permutation / Transposition

Méthodes modernes

- Algorithmes en blocs
- Algorithmes à flots (bit à bit, cf Vernam)

Contrainte

- il faut se rencontrer avant pour échanger une clef, un procédé mécanique ou un algorithme

Principe de Kerckhoffs

Le secret doit résider dans la clé de chiffrement et de déchiffrement, et non pas dans une quelconque confidentialité de l'algorithme (ici de la machine) qui ne peut être raisonnablement garantie

Cryptographie asymétrique

Histoire

Existe depuis les années ~1970

Coté USA

- 1976 : Whitfield Diffie et à Martin Hellman présentent le concept de cryptographie à clé publique (mais sans exemple concret) à la National Computer Conference
- 1978 : Ronald Rivest, Adi Shamir et Leonard Adleman, fournissent un exemple fonctionnel : le RSA

Coté Britanique

Recherches secretes au GCHQ, Government Communications Headquarters

- James Ellis aurait proposé le concept avant Hellman et Diffie
- 1973 : Clifford Cocks aurait décrit un algorithme proche du futur RSA
- 1974 : Malcolm J. Williamson aurait inventé un protocole d'échange de clef très proche de celui de Diffie et de Hellman

Fonctionnement

Système basé sur la fabrication de deux clés complémentaires :

- ce que l'une fait, l'autre le défait
- une publique, l'autre privée

Ce système permet trois choses majeures :

- **chiffrer le message à envoyer :**
 - l'expéditeur utilise la clef publique du destinataire pour chiffrer son message.
 - le destinataire utilise sa clef privée pour déchiffrer le message de l'expéditeur,
 - => garantie de la confidentialité du contenu !
- **s'assurer de l'authenticité de l'expéditeur :**
 - l'expéditeur utilise sa clef privée pour chiffrer un message
 - le destinataire peut déchiffrer avec la clef publique de l'expéditeur
 - => mécanisme utilisé par la signature numérique pour authentifier l'auteur d'un message
- **il n'est pas pas nécessaire de se rencontrer au préalable** pour échanger la clef

Références

- [Wikipédia: Cryptographie symétrique](#)
- [Wikipédia: Cryptographie asymétrique](#)
- [Wikipédia: Histoire de la cryptologie](#)
- [Kerckhoffs](#)

Le mouvement Cypherpunk

Définition

- Mouvement depuis la fin des années 1970
- Groupe d'activistes répartis dans le monde
- Pronent l'utilisation proactive de la cryptographie
- Fabriquent des outils pour des futurs souhaitables
- Terme inventé par Jude Milhon

Contexte

- Choc pétrolier (1973) qui affecte le monde occidental
- Seconde guerre froide / "Guerre fraîche"
 - contexte de guerre froide post Viêt Nam
 - fin de la politique de détente
 - repli sur soi des états
- Toute l'information sur les réseaux est en clair
 - n'importe qui peut écouter, lire les communications ou les transactions
 - des problèmes peuvent arriver : gouvernements, entreprises ou individus

Idéologie (résumée)

- "si vous n'avez rien à cacher de quoi vous avez peur ?"
- là c'est le principe inverse : pourquoi je laisserai X accéder à mes conversations / mes transactions ?
 - internet est-il un groupe d'amis à qui on peut tout dire ?

- ou un espace public avec des gens à qui l'on ne fait pas forcément confiance ?
- sous-courants politiques
 - approche libertarienne
 - approche anarchiste
 - => forme d'anarcho-capitalisme

Années ~1970

- les états financent la cryptographie pour leurs armées
 - sur le terrain, c'est les militaires
 - dans les laboratoires ce sont des civils * conçoivent et utilisent la cryptographie * qui écrivent les outils pour qu'elle fonctionne
- les chercheurs & ingénieurs en imaginent les usages civils
 - dans le futur
 - tous seront reliés par le réseau
 - communiquer de façon secrète / privée
 - sans être contrôlés par quiconque (gouvernement, entreprise, etc.)
- mouvement américain "le moins de gouvernement il y a, mieux c'est"
- informatique = catalyseur, car permet d'accélérer le calcul mathématique de la cryptographie

Années ~1980

Des mailing lists Cypherpunk

- Organisées notamment par John Gilmore
 - fondateur ultérieur de l'EFF
 - EFF: NGO de défense des libertés sur internet et très présente actuellement
- Longues conversations entre gens passionnés
 - qui veulent s'en servir dans le civil
 - sur les concepts variés
 - autour de vie privée

- pour un monde libre, non-censurable
- comment protéger les communications entre les personnes
 - par des moyens technique ?
 - par des actions collectives ?
 - par des lois ?

The Crypto Anarchist Manifesto (1988)

A specter is haunting the modern world, the specter of crypto anarchy.

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. [...] These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.

The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. [...]

The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. [...]

Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. [...]

Arise, you have nothing to lose but your barbed wire fences!

-- Timothy .C May, 1988

En résumé

- a partir de maintenant les gens peuvent communiquer de façon secrète
- les gouvernements ne peuvent plus rien y faire
- ça va changer radicalement la façon dont les société civiles fonctionnent avec leurs gouvernements

A noter

- Le ton provocateur
- Le titre "crypto-anarchiste" qui est une blague (troll), en référence aux crypto-communistes (cf. guerre froide)
- A l'époque il étaient considérés comme des rigolos / gens pas sérieux

Années ~1990

Cypherpunk Manifesto (1993)

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world. [...]

We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak. [...] -- **Eric Hughes, 9 March 1993**

Résumé :

- Modalités de la vie privée dans la vie électronique
- Explication point par point des conditions pour exercer la vie privée dans une ère numérique
 - La cryptographie va inéluctablement se répandre sur l'ensemble du globe, et avec elle les systèmes de transactions anonymes qu'elle rend possibles.
 - Pour que la vie privée soit généralisée, elle doit faire partie d'un contrat social. Les gens doivent venir et déployer ensemble ces systèmes pour le bien commun.
 - La vie privée ne s'étend que dans les limites de la coopération des autres membres de la société.
- Appel à de la monnaie électronique
- Définition du terme cypherpunk
 - Cypherpunk = des gens qui écrivent du code, pour protéger la vie privée

A noter :

- Marque la création du mouvement Cypherpunk
- Totalement d'actualité, moderne et adapté à ce qu'on vit aujourd'hui

- A lire absolument !

The Cyphernomicon (1994)

Document écrit par Timothy C. May en 1994

- Diffusé sur la liste de diffusion Cypherpunk.
- Décrit certaines des idées du crypto-anarchisme.

Déclaration d'indépendance du cyberspace (1996)

- Rédigé le 8 février 1996 à Davos en Suisse
 - par John Perry Barlow (un des fondateurs de l'Electronic Frontier Foundation)
 - en réponse à la Loi sur les télécommunications de 1996 aux États-Unis.
- En résumé :
 - Aucun gouvernement (ou qu'aucune autre forme de pouvoir) ne peut s'imposer et s'approprier Internet, alors en pleine extension.
 - Le cyberspace / le cypherpunk est un sujet éminamment politique

The Cryptonomicon (1999)

- Roman de science-fiction paru en 1999
- De l'auteur américain Neal Stephenson.
- Réflexion sur l'impact de la cryptographie sur la société humaine
 - Parallèle entre l'usage passé de la cryptographie durant la WWII et le monde moderne
 - Utopie de la création d'un paradis informatique virtuel
 - Utopie de la création d'une monnaie électronique

Années ~2000

- Julian Assange fonde Wikileaks
 - donner une audience aux lanceurs d'alertes et aux fuites d'information,
 - tout en protégeant leurs sources

- Plusieurs millions de documents ont été publiés sur le site depuis sa création
 - relatifs à des scandales de corruption, d'espionnage et violations de droits de l'homme
 - concernant des dizaines de pays à travers le monde

Années ~2010

- Révélation d'Edward Snowden
 - Les citoyens des USA sont sur écoute (par leur propre gouvernement)
 - Les USA surveillent toutes les communications sur internet
- Scandale Facebook-Cambridge Analytica (CA)
 - Facebook qui exploite et revend les infos aux entreprises
 - Manipulation massive de l'opinion
 - Influencer les intentions de vote en faveur des hommes politiques qui mandaté CA

Références

- [Cypherpunk Manifesto](#)
- [Wikipedia: Déclaration d'indépendance du cyberspace](#)
- [Wikipedia: WikiLeaks](#)
- [Wikipedia: Révélation d'Edward Snowden](#)

Les solutions cypherpunk

PGP (1991)

- Créé par Phil Zimmerman
- Permet de chiffrer les messages emails et des documents
- cryptographie asymétrique
- Le système n'a pas eu bcp de succès (sauf chez les cypherpunk et les communautés open-source)

Ce que ça aurait pu éviter :

- Macron leaks
 - fuite de plus de 20 000 courriers électroniques liés à la campagne d'Emmanuel Macron
- Affaire des courriels d'Hillary Clinton
 - utilisation durant son mandat de secrétaire d'État des États-Unis (2009-2013) d'une adresse électronique personnelle non-protégée
 - au lieu de la messagerie officielle
 - hébergement de documents importants / secrets de façon non protégée
- etc.
- [Affaire des courriels d'Hillary Clinton](#)

Free Software Foundation & Projet GNU (1983)

- Fondé(s) par Stallman
- Permettre l'émergence d'une informatique indépendant du contrôle des grandes entreprises
- Pas revendiqué Cypherpunk, mais très proche de son idéologie:
 - Pas de tiers de confiance => Tout le monde peut vérifier
 - Reprises de contrôle par l'individu => Tout le monde peut corriger & améliorer
 - Approche horizontale => Tout le monde peut partager le code d'origine et le code modifié

e-cash (1983)

- Système de monnaie privée
 - Basée sur de la cryptographie
 - centralisée (une banque centrale validant les transactions)
- Créé par David Chaum
- Mais faillite...

La preuve de travail (1993)

Fonctionnement

- Sorte de challenge
 - Recherche de la solution à un probleme
 - Ou la solution constitue une "preuve"
- Fortement asymétrique
 - Nécessite un grand nombre d'essais avant de trouver la solution
 - Mais très rapide à vérifier (en un seul coup)
- Inventé par Cynthia Dwork et Moni Naor in 1993
- Mis en oeuvre pour la premiere fois dans Hashcash en 1996
- Formalisé par Markus Jakobsson et Ari Juels dans une publication scientifique en 1999

Hashcash (1997)

- Systeme antispam pour email basé sur une preuve de travail
- On demandait à l'émetteur d'un message electronique de fournir avec son message une preuve de travail
- objectif : rendre le spam non-viable économiquement
 - pour chaque message : un calcul, ça coute bcp en ressources processeur
 - ex: 10ct par messages... ça rend l'envoi d'emails en grande quantité non-viable économiquement

Bitgold (1998)

- créé par Nick Szabo

- monnaie privée sans état

BitTorrent (2002)

- Protocole de transfert de données pair à pair (P2P) à travers un réseau informatique.
- conçu par Bram Cohen (2001-2002)
- Objectif:
 - distribuer largement de grandes quantités de données
 - répartissant la charge inhérente en matière de matériel, hébergement Internet et bande
 - éviter d'avoir un distributeur central unique

Bitcoin (2008)

... suspense :-)

Autres inventions cypherpunk ?

- fondation Apache
- protocole SSL/TLS, utilisé partout aujourd'hui
 - HTTP + TLS : connexions chiffrées
 - SSH : connexion entre deux ordinateurs

Références

- [Proof of work](#)

Et ensuite ?

Généralisation des modèles pair à pair (peer-to-peer)

- échanges entre 2 individus
 - qui se font confiance (=responsabilité)
 - sans passer par un tier (=horizontalité)
 - communication P2P = application de l'anarchisme
- opposé aux systemes centralisés ou verticaux (entreprises, gouvernements, etC.)
 - difficile de controler les échanges
- des observateurs des communication
- ou qui veulent contrôler ces échanges

La preuve par les faits

- ils font la preuve que ça marche
 - ... depuis 11 ans pour bitcoin
 - ... depuis 19 ans pour bittorrent
 - ... depuis 49 ans pour internet
- un potentiel multiple
 - nouvelles possibilités techniques
 - nouvelles façons de faire
 - nouvelles façon de s'organiser
- des systèmes résistants (anti-fragiles)
 - bittorent : les institutions et société de gestion droits d'auteurs dépensent des milliards pour les arreter mais rien n'y fait
 - internet : la commande au DARPA était « on voudrait un réseau qui résiste aux attaques nucléaires : plein de noeuds de part le monde qui permette l'acheminement des messages »

Une résistance des organisations

- Les états & entreprises ne sont pas encore prêts
 - pas encore "cablés" pour comprendre ou participer à ce modèle de gouvernance
 - ou bien ils ont intérêt à ne pas le faire
 - centralisation = contrôle
 - centralisation = possibilité de créer un péage
- Mouvement de fond pour centraliser internet et les réseaux (ex: 5G)

La data est une nouvelle forme de capital

- Nouvelles formes d'exploitation (click-workers)
- Nouveaux outils de production (IA, Machine Learning, automatisation, etc.)
- Nouvelles formes de droits & protections (RGPD, etc.)
- Les outils cypherpunk & P2P
 - comme nouvelles formes de rapports de force ?
 - comme levier de lutte sociale ?
 - pour obtenir de nouvelles libertés et lutter contre les oppressions ?

Des signaux faibles

- Art Of Hosting (fin ~1990)
 - approche et méthodologie pour la facilitation de groupe et la gestion du changement
 - développées selon un modèle de communs ou open-source
 - par une communauté internationale de praticiens de la facilitation
- BarCamp (2005)
 - événements "non-conférences", sans sélection à l'entrée
 - tous participants, auto-organisation sur place
 - marque communautaire / dé-centralisées
- Organisations opales (~2000)
 - organisations dé-centralisées ou en gouvernance horizontale (ie: sans management)

- ex: Officiene (200 salariés), ex: Buurtzorg (10.000 salariés)

Valeur, échanges et confiance

Inter-dépendances, écosystèmes & flux

Au niveau planétaire, des espèces animales comme des humains, nous sommes tous inter-dépendants

- On a besoin d'échanger avec les autres pour vivre :
 - On a des besoins
 - Il y a les biens qu'on a ou qu'on peut produire
 - Il y a des biens que les autres peuvent nous apporter
 - Les biens ne sont équitablement/également répartis
- Cela crée des flux d'échanges
 - ex: biens matériels, émotions, savoirs, etc.
 - L'économie c'est l'ensemble des flux d'échanges entre les besoins / richesses
- Parfois ça ne coïncide pas directement
 - ... alors on a besoin d'intermédiation

La fonction de la monnaie, c'est de permettre à chacun d'échanger ce qu'il produit (son travail, son art, son artisanat, ses marchandises, bref, le temps qu'il passe et les ressources qu'il utilise pour produire quelque chose) contre ce que les autres produisent. -- Gérard Foucher, Les secrets de la monnaie

La monnaie

Définition

- Un intermédiaire, en rapport ces flux de besoins \Leftrightarrow biens
- Définition classique (en économie)
 - mesurer la valeur
 - stocker la valeur (thésauriser)
 - échanger la valeur

Quelle est sa valeur ?

- Valeur du support ?
 - coquillages ? des bouts de fer ? des bouts de papier ? ou de plastique ?
- valeur d'usage ?
- Cout de production ?
- Valeur relative d'échange par rapport à N biens ?
 - attention au nombre de combinaisons, car nécessite $(N*(N-1) / 2)$ valeur relatives à définir !

Monnaie = dette ?

- Exemple: un bien donné vendu par A à B en échange d'unités
 - A perd la valeur du bien, B s'enrichit du bien
 - B a une dette envers A
 - les unités que possède A est le marqueur de cette dette
 - il peut la faire valoir auprès de B (plus tard) ou auprès d'autres gens reconnaissant cette monnaie
- ce qui lui donne sa valeur à la monnaie, c'est la CONFIANCE (ou la peur)
 - que l'on place dans les unités d'intermédiation
 - dans la groupe de gens qui reconnaissent ces unités

Les types de monnaies

Il y a 3 types de monnaies, toutes les trois créés par les banques

- La monnaie fiduciaire
 - Pièces et billets
 - Créé par les banques nationales (en EU)
 - En respectant les quotas décidés par la banque centrale
- La monnaie scripturale
 - Simple écriture comptable : pas de représentation physique, c'est un chiffre dans une colonne d'un tableau (désormais dans un programme d'ordinateur)
 - Créée par les banques privées, ex-nihilo, au moment des emprunts
 - C'est un chiffre en bas de votre relevé de compte bancaire

- Monnaie de base
 - utilisé entre banque centrale et banque privées
 - une forme de titre
 - valeur “garantie” par la capacité des citoyens des états à créer plus de biens et plus de services.

Dans tous les cas, cette monnaie créée est considérée comme un passif, c’est à dire comme une dette

Références

- « L’argent dette, 5000 d’histoire », David Graeber (anthropologue)
- <https://brettscott.substack.com/p/structure-vs-functions-of-money>
- [Dossier: Histoire de la monnaie et des systèmes économiques](#)
- [Melchior : Question 1. Connaitre les fonctions et les formes de la monnaie](#)
- [Wikipedia : Histoire de la monnaie](#)
- [Simple comme bonjour](#)
- [Banque Centrale Européenne](#)

L'économie de la dette

Masses monétaires

- Masse monétaire = total de tout l'argent, pour chacun des types.
- Masse monétaire totale = totale de la masse monétaire fiduciaire et de la masse monétaire scripturale
- Répartition (juin 2012)
 - 924 milliards d'euros en pièces et billets
 - 9.003 milliards d'euros de monnaie scripturale.

Quel impact sur l'économie ?

- La quantité de monnaie disponible, en circulation à un instant est une information cruciale
- Rythme de la création monétaire ?
 - Plus on crée de monnaie, plus on "dilue" la valeur, moins la monnaie vaut qqchose
 - Quel est impact sur l'économie et sur les gens ?

Création monétaire, avec intérêt

Monnaie créé par le crédit

- La monnaie est créée à une seule occasion : le crédit accordé par une banque privée.
- TOUTE la monnaie correspond à un crédit que quelqu'un a fait quelque part.
 - Corollaire 1 : Si tout le monde rembourse ses dettes (états, entreprises, particuliers), il n'y a PLUS DE MONNAIE DU TOUT.

- Corollaire 2 : TOUTE LA MONNAIE émise est soumise à intérêt. A l'échelle globale, si on a X euros qui circulent, collectivement, nous devons rembourser $X + Y\%$ euros.
- Cette contrainte sur une monnaie qui n'existe pas préalablement dans l'économie a pour effet d'augmenter la concurrence entre les acteurs du système.
 - Corollaire : il y aura des baissés. Mathématiquement. Rembourser toutes nos dettes est STRICTEMENT et MATHEMATIQUEMENT impossible à un instant T.

Un problème de croissance

- Tout ceci est transparent et ne pose pas de problème tant que le flux de la monnaie va croissant : si la monnaie créée dans l'année N suffit à payer les intérêts des années précédentes, tout va bien.
 - Corollaire 1: Il faudra payer les intérêts de ce qu'on a créé en N => Cercle vicieux dont on ne peut sortir, et qu'on ne peut poursuivre qu'à la condition d'avoir une croissance économique infinie.
 - Corollaire 2: Cela nécessite des ressources infinies sur une planète finie.

Crise des subprimes

Origine et fonctionnement

- Hausse des taux directeurs de la Réserve fédérale
- Augmente le coût de remboursement des prêts bancaires
- Taux de défaut préalable de 15%
- Baisse du prix de l'immobilier
- Conséquences
 - Incapacité des gens à rembourser
 - Incapacité des agences à se renflouer
 - Titrisation des dettes et spéculation

➔ Faillites en cascades

La fin de la confiance

- 15 septembre 2008 - Lehman Brothers se déclare en faillite
- Les marchés internationaux dévissent
- La confiance en les banques et le système financier s'effondre
- Ruine de nombreux consommateurs
- Constat de la perte de contrôle des acteurs de la société (citoyens, états) envers un système qui joue avec lui voire contre lui

Causes primaires

- Titrisation
- Spéculation
- Banques et monnaie-dette

Références

- [Wikipedia: The Big Short \(livre\)](#)

Face au probleme

Questions ouvertes

- Comment créer un actif non-dette ?
- Comment on fait pour se passer des banques et des acteurs financiers dangereux ?
- Quels contre-pouvoirs ?
 - pour ne pas donner le pouvoir à une organisation ou un groupe d'organisations qui pourraient profiter de ce pouvoir ?
 - la meilleure garantie n'est-elle pas la décentralisation ?

Proposition de solution : un registre distribué ?

Ce qui permet de donner de la valeur à un actif c'est la confiance que l'on place en cet actif (et dans les tierces parties)

Et pour que ce soit un actif, il faut une forme d'unicité => Le problème de la copie sur le numérique

L'élément le plus important sur un billet de banque est le numéro de série : on a besoin de pouvoir vérifier sa véracité, son unicité.

Si on veut créer du cash numérique, il faut que ce soit un actif unique, identifiable, et infalsifiable.

Objectif : créer de la confiance dans un actif numérique en utilisant le biais de la cryptographie.

Le projet Bitcoin

Le concept

- Un projet de système monétaire
- Créé par Satoshi Nakamoto

Un white-paper

Bitcoin: A Peer-to-Peer Electronic Cash System

- Publié en 2008
- Description technique et feuille de route pour le protocole et le système monétaire
- Semblable à une publication de recherche
- Explication claire et simple (seulement 9 pages)

Assemblage des 3 concepts précédents

- cryptographie
- pair à pair
- preuve de travail

➡ pas une invention, simplement la réutilisation pertinente des technologies existantes

Totalement décentralisé

- pas contrôlé
- pas manipulé par une autorité centrale
- pas de tiers de confiance
- Projet sans gouvernance (plutôt une gouvernance dé-centralisée)
- Totalement infalsifiable
 - Contrôle croisé des transactions par l'ensemble des nœuds (panoptique)
 - (sauf si majorité coordonnée de "nœuds tricheurs")

➔ Ça le rend différent de tous les autres systemes monétaires (et de nombre de projets)

Bitcoin VS crise financiere

- La légende dit que Bitcoin est la réponse à la crise des subprimes
- Satoshi a annoncé travailler sur BTC depuis 2006/2007
- Pas une réaction donc, mais une jolie coïncidence
- La crise de 2008 sert de catalyseur
 - pour lancer le protocole à ce moment là
 - pour faire connaitre le projet
 - pour trouver des contributeurs
- Satoshi fait un clin d'oeil à la crise dans la premiere transaction « le chancelier britannique se décide à faire un 2nd programme d'aide aux banques »

Les grandes dates de Bitcoin

- 2008 : publication du Whitepaper par Satoshi Nakamoto
- 2009 : premier bitcoins minés
- 2010 : première transaction commerciale
- 2013 : le bitcoin atteint \$1.000 l'unité
- 2017 : le bitcoin atteint \$20.000 l'unité.
- 2021 : Bitcoin est utilisé par plus de 70m de personnes.

Références

- [Blockchain.com: Number of Blockchain wallets](#)
- [Cryptography Mailing List: Bitcoin P2P e-cash paper](#)

Un projet technique d'envergure

Qualité du code

- Le code de bitcoin est relativement simple, clair et agréable à lire
- les concepts utilisés sont bien connus

➡ c'est ce qui a fait le succès de ce système

Un projet open-source

- Accorde aux utilisateurs 4 libertés
 - liberté d'utiliser
 - liberté d'étudier
 - liberté de modifier
 - liberté de redistribuer (le code)
- Rassemble une communauté de développeurs et d'utilisateurs

Hébergement du code : en enjeu de pouvoir

- Début 2009, le code source du projet Bitcoin était simplement un fichier .rar hébergé sur SourceForge. Les premiers développeurs échangeaient en fait des correctifs de code avec Satoshi par courrier électronique.
- Le 30 octobre 2009, Sirius (Martti Malmi) a créé un dépôt subversion pour le projet Bitcoin sur SourceForge.
- En 2011, le projet Bitcoin a migré de SourceForge vers GitHub.
- En 2014, le projet Bitcoin a été renommé Bitcoin Core.

De nombreuses garde-fous ont été mis en œuvre pour éviter que l'hébergement du code ne donne le moyen de le contrôler, le hacker ou le détourner :

- Moyens humains, techniques, méthodologiques
- Stratégie du "Trust No One"

Références

- [Who controls Bitcoin Core?](#)

Satoshi Nakamoto

Qui est-t-il ?

- Resté anonyme du début à la fin
- Il ne fait plus partie du projet, il a disparu de la circulation
 - Sa dernière communication publique sur un forum remonte à fin 2010
 - Son dernier message privé à un contributeur en mai 2011 :
- Il a des bitcoins non utilisés
 - le portefeuille de Satoshi hébergerait 1 million de bitcoins
 - sans aucun transferts, ni vente, ni rien depuis
- Des centaines de personnes ont cherché à trouver sa véritable identité

"I've moved on to other things and probably won't be around in the future.

-- Satoshi Nakamoto à Martti Malmi, mai 2011

-- Source : Digital Gold, Nathaniel Popper

Ce qu'on peut déduire

- Nom ou pseudonyme a consonnance japonaise
- Il est développeur (il sait manifestement coder)
- Il vient d'un milieu universitaire
 - Le whitepaper est construit de la même façon qu'un document académique
- Il est de culture anglaise ou nativement anglais
 - ...se voit à son vocabulaire (dans le whitepaper et dans ses emails)
 - L'anglais du whitepaper est particulièrement propre et typique
 - Citation de la une du Times de Londres dans la première transaction de la blockchain ("Chancellor on brink of second bailout for banks")
- Les heures auxquelles il communiquait correspondent à celle de quelqu'un qui vivrait en Angleterre ou sur la côte est américaine

Le mystère reste entier

Était-ce un individu seul ou un groupe ?

➔ Cela réduit les possibilités à une 15 aine de personnes dans le monde.

- C'est peut être Hal Finney, un des premiers contributeurs à BTC, destinataire du premier virement et décédé peu apres la "retraite" de Satoshi Nakamoto.

Comment prouver que quelqu'un est Satoshi ?

- Il suffirait qu'il utilise les premier bitcoins stockés sur la premiere adresse cryptographique que tout le monde peut surveiller
- Rien de certain n'a bougé pour l'instant (mais tout le monde surveille)

Les faketoshi

- Plusieurs personnes ont proclamé être satoshi Nakamoto.
- Dont Craig Wright - un entrepreneur australien
 - La communauté lui a demandé de le prouver (déplacer l'argent de son wallet)... ça n'est jamais arrivé :-)
 - D'autres histoires tendent à infirmer sa candidature au titre.
 - Conclusion : ce n'est PAS lui

Bien ? Mal ? Problématique ?

- Son anonymat et sa disparition sont probablement la meilleure façon pour que personne (état, entreprises, individus) ne puisse exercer de pression sur lui pour modifier ou arrêter son systeme.

Références

- [Emails de Satoshi Nakamoto](#)

Unités et nomenclature

Nomenclature

Bitcoin (avec majuscule) : le réseau

- Désigne le système de stockage et d'échange d'actifs numériques
 - un protocole réseau
 - l'ensemble des machines qui le font fonctionner
 - les données qu'elles contiennent (la blockchain Bitcoin)

bitcoin (avec minuscule) : l'unité de valeur

- Désigne l'actif numérique
 - utilisé sur la blockchain Bitcoin
 - à l'intérieur des transactions
- Les symboles de téléscripateur (ticker) utilisés pour représenter le bitcoin sont BTC[b] et XBT.
- Son caractère Unicode est `₿`.

Sous-unités

Millibitcoin and Satohis

- un BTC est divisé en plusieurs sous-unités
 - c'est l'équivalent des centimes
 - on va parler de milibitcoins (mBTC) et de satoshis (sat)

Satoshis

- nommés en l'honneur de l'inventeur du bitcoin, Satoshi Nakamoto
- unité la plus petits qu'on peut stocker dans une transaction
 - 100 millions de satoshis = un bitcoin

- 1 satoshi = 1/100000000 bitcoins
- ex: aujourd'hui ~17000 satoshis c'est \$10
- plus il sera rare de manipuler des bitcoin entiers, plus il sera pratique de parler en satoshis

References

[Although the satoshi is the finest amount that can be recorded in the blockchain *](https://en.wikipedia.org/wiki/Bitcoin)
<https://en.wikipedia.org/wiki/Bitcoin>

FRACTIONS notion : les fractions de bitcoin : les satoshis pas besoin de posséder un bitcoin complet pour faire des trucs

0, 000 000 01 BTC l'unité la plus petits qu'on peut stocker dans une transaction
 Although the satoshi is the finest amount that can be recorded in the
 blockchain[1]. [https://www.reddit.com/r/Bitcoin/comments/2wtvu1/
 question_about_the_satoshi_unit/](https://www.reddit.com/r/Bitcoin/comments/2wtvu1/question_about_the_satoshi_unit/)

1 BTC 100 000 000 Satoshi m k utilisé en pratique nommé en l'honneur de nakamoto

Architecture

La blockchain

- support pour faire des échanges,
- faire des transactions (dans le cas de bitcoin)
- objectif : enregistrer dans un historique partagé entre participants

Un historique partagé

- Des transactions proposées par les participants
- Mises en attente ...
- ... Doivent être validées (d'après certaines règles)
- Elle sont regroupées = un block

Structure des blocks

- L'identifiant du block est le "hash" de son contenu
 - Possède une référence vers le block précédent
 - Comme une "liste chaînée" (pour ceux qui ont fait de l'informatique)
 - Stocke des transactions (sur la forme d'un arbre de Merkle)
- ➔ La blockchain = l'historique des blocs qui se suivent
- ➔ On ne peut pas introduire de nouveaux blocs intermédiaires

Transactions

- Des entrées : la référence à la transaction d'où vient les BTC qui seront consommés
- Des sorties l'adresse du destinataire
- Une quantité de BTC à consommer
- Une coinbase: : un message

Fonctionnement des transactions

- pour faire une transaction il faut consommer tous les unités depuis les entrées
- il peut y avoir plusieurs entrées
- il peut y avoir plusieurs sorties

ex :

- 8 unités venant d'Alice (en entrée)
- 4 unités vont à Bob
- 4 unités allant à Alice (retour à elle-même)

transactions

Transaction spéciales

Pour la création des unités BTC (minage)

- liste d'entrée vide
- sortie (l'adresse de celui qui vient de miner le bloc)
- ne coûte rien (en BTC)

Références

- [DONE Bitcoin : Explication pour tout comprendre rapidement \(moins de 10 minutes\)](#)
- [DONE https://www.youtube.com/watch?v=s0FVHhUc7JA](https://www.youtube.com/watch?v=s0FVHhUc7JA)
- [Block: 0 | Blockchain Explorer](#)
- [Merkle Tree](#)

Genesis block

Premier bloc de la blockchain bitcoin

- Le 3 Janvier 2009
 - Premiere transaction
 - Premier block validé
 - C'est le "genesis block"

Contenu du Block #0

- Quantité: 50 BTC
- Date (2009-01-03)
- Transaction (une seule) : vide => vers le portefeuille de Satoshi
- Coinbase (message) = « Chancellor on brink of second bailout for banks »

De la théorie à la réalité

- Le concept décrit dans le whitepaper est validé
- Conséquence: le projet devient concret et utilisable

Minage et mineurs

La validation des transactions

- Il faut garantir qu'elles sont uniques
- Il faut qu'elle soient vérifiables par l'ensemble des usagers de la blockchain
- Et qu'ils ait un consensus

Le minage

- Travail de valider des blocks (c-a-d un groupe de transactions)
- Garantie du bon fonctionnement de la blockchain

Les mineurs

- L'ensemble des machines qui participent au réseau de la blockchain
- Qui font pour cet "effort"
- Par extension: les gens qui possèdent ces machines

df

Comment ça fonctionne ?

- A chaque block un challenge est posé
 - problème mathématique difficile
 - basé sur les procédés de cryptographie,
- Tous les ordinateurs cherchent en même temps
 - Opération difficile qui prend du temps (preuve de temps)
 - Forcément une seul "premier" qui trouve la solution (difficile)
- C'est celui là qui proposera son bloc
 - ... qui inclue la solution dans son bloc
 - l'identifiant du bloc dépend de son contenu (donc infalsifiable)
 - tout le monde peut vérifier que cette solution est juste (facile)
 - et accepter le nouveau bloc

- La difficulté du challenge est adaptée automatiquement
 - L'objectif est qu'un bloc soit validé toutes les ~10 minutes

No pain, no gain

- Le minage est la garantie de la confiance dé-centralisée
- Les mineurs sont essentiels pour le bon fonctionnement de la blockchain
- Comment les inciter à rejoindre le réseau ? une récompense !
 - la prime de minage : création de nouveaux bitcoin ex-nihilo
 - une "taxe" sur les transactions qu'ils ont validé

Comment les mineurs s'organisent

Comme c'est difficile mais intéressant il cherchent à augmenter leurs chances de succès

- ils se réunissent pour augmenter leurs chances (pool de minage) (ex: jouer au loto à plusieurs)
- ils achètent du matériel ultra-performant et spécialisé pour ce problème (ASIC et fermes de minage)

Les règles de création monétaire

Moitié moins de bitcoins produits tous les 4 ans (halving)

- La prime de minage de nouveaux blocs est divisée par deux tous les 210.000 blocs
 - Les mineurs reçoivent 50 % de bitcoins en moins pour vérifier les transactions.
- Une baisse programmée des récompenses (à peu près tous les 4 ans)
- Le premier bloc avait rapporté 50 BTC

Un nombre limité de bitcoins

- L'algorithme limite la quantité créée à 21 millions de BTC (arrondi)
 - 20.999.999, 9796 BTC précisément
 - pas un de plus
- Choix de Satoshi Nakamoto pour créer de la rareté

La fin de la prime de minage ?

- Non, les mineurs gagneront toujours les taxes sur les transactions

Préhistoire du bitcoin

relativement peu de gens qui s'intéressent au bitcoin s'intéressent à cette "préhistoire du bitcoin"

Références

- nakamotoinstitute.org/b-money.txt at master · NakamotoInstitute/nakamotoinstitute.org · GitHub
- [TODO GitHub - 0xb100d/manifestos: hacker/cypherpunk/etc historical writing to be included in GRINOIRE](#)
- [TODO GitHub - tombusby/cypherpunk-research](#) : This repository is essentially for compiling information about Cypherpunks, the history of the movement, and the people/events of note.
- [Wikipédia: David Chaum](#)
- [Wikipédia: Nick Szabo](#)
- [Wikipédia: Hal Finney](#)
- [CYPHERPUNKS : LA PRÉHISTOIRE DU BITCOIN](#) (avec Manuel Valente)

Contexte

Premiers ambassadeurs

- Deux communautés
 - Cypherpunk
 - Informaticiens experts
- Les gens capables de comprendre...
 - le concept de blockchain
 - les spécificités techniques du projet
 - ses enjeux

Deux possibilités pour obtenir des bitcoins

- soit en miner soi-même
- soit en obtenir auprès de gens qui en ont déjà
 - éventuellement contre de la monnaie

Une monnaie pour le DarkNet ?

Terrorisme et activités illégales

- Histoire du Bitcoin associée au Terrorisme et activités illégales
- Quelque cas d'achats/vente de choses illégales
 - drogue, sexe, armes, blanchiment d'argent...
 - surtout au début
- Aussi pour aider la liberté d'expression (ex: Wikileaks)

➔ Note: Les USD et EUR n'ont jamais empêché le terrorisme :)

BTC permet de tout tracer

- Cependant toutes les transactions sont publiques
 - chacun peut les consulter
 - ... est-ce cohérent avec la philosophie cypherpunk ?

Quid de l'anonymat ?

- si vous passez par des intermédiaires qui demande une carte d'identité.. oui
- si vous êtes sûr du 100% bitcoin (sans conversion euro/dollar)
 - là... vous êtes vraiment anonymes
 - pas forcément ceux avec qui vous faites des transactions :-)

Pizza et folklore

Premiere transaction marquante

- 22 mai 2010
- Laszlo Hanyecz propose 10000 BTC contre 2 pizzas sur un forum
- Jeremy « jercos » Sturdivant (britannique) qui lui a fait livrer 2 pizza
 - depuis le Papa John de Jacksonville, en Floride,
 - à coté de chez Laszlo

La valeur des pizza

- à l'époque entre \$20 et \$30,
- aujourd'hui \$600.000.000... (600 millions, bon deal)

Le folklore

- Première transaction « marquante » de l'histoire du BTC
- événement marquant et insolite
- fêté tous les ans par la communauté
- ... en achetant des pizzas

Références

- [Cryptoast: les deux pizza qui ont écrit l'histoire...](#)
- [Bitcoin Pizza Day: Celebrating the \\$80 Million Pizza Order](#)

Le prix du bitcoin

Historique des prix

- au début : utilité très restreinte.. ça ne vaut rien
- 5 octobre 2009 : \$0.00071
 - première évaluation du prix de production du bitcoin
 - à partir du coût de l'électricité aux USA
- 22 mai 2010 : \$0.39
 - lazlo passe commande de deux pizzas pour 10000 BTC
- fév 2011 : parité avec le dollar
- début 2020 : 8000€ / btc
- début 2021 : atteint plus de \$60k

Une très forte volatilité du BTC

- ex: en 2011 :
 - début d'année : parité avec le dollar
 - valeur maximum (ATH) à \$28,92
 - le prix s'est ensuite essoufflé, revenu à \$5
- ex: en 2021
 - début d'année : \$60k
 - juin : \$33k

Références

- [Bitcoin's Price History](#)
- [CoinMarketCap: Historique des prix BTC](#)

Une adoption massive

Historique du nombre de Wallets

- 2013: de 150k à 440k wallets
- 2018: de 22m à 31m wallets
- 2021: de 68m à 106m wallets estimés

➡ C'est un actif de plus en plus apprécié et soutenu (par une communauté d'initiés)

Une présence dans le monde réel

- 2013, Vancouver : 1er ATM (distributeur de billets)
- mai 2014, Paris : Maison du Bitcoin
 - elle fermera en juin 2018
- 2019 : VISA propose une carte de paiement bitcoin via Coinbase (conversion fiat)
- 2020 : PayPal accepte les transactions en bitcoin (wallet)
- 2021 : MasterCard propose une carte de paiement bitcoin (conversion fiat)
- 2021 : total de 17.066 ATM crypto, dans 68 pays

Références

- [106 millions d'utilisateurs](#)
- [68 millions de wallets en 2021](#)
- [Visa Grants Coinbase Power To Issue Bitcoin Debit Cards](#)

Un historique de blocs

Notion de hash

Minage et mineurs

Mécanismes de consensus

- PoW: PROOF OF WORK
- PoS: Proof of stake
- PoB: Proof of burn
- PoET: proof-of-elapsed-time
- PoI: proof-of-interaction

Références

- [Analyse et comparaison des mécanismes de consensus dans la blockchain](#)
- [Proof of Elapsed Time \(PoET\)](#)
- [Securing Proof-of-Stake Blockchain Protocols](#)
- [Proof of Interaction](#)

Dépense énergétique et énergies vertes

- Consommation énergétique
- Sources d'énergie
- GREEN ENERGY

Blockchains publiques, privées, hybrides

- Blockchain publique
- Blockchain privée & permissionnée (4 briques de base ?) (cf Hyperledger Fabric)
- Blockchain hybride

Règles de création des tokens

Différents types de transactions

070 wallets

080 private key

Mark Karpeles

CEO, 2010-2014

100 scam or hack

Forks and altcoins

Les forks donnent naissance à de nouveaux crypto actifs : les ALT coins Il existe plein d'autres blockchain, actifs, et plate-formes (ex: Litecoin, Doge, Tezos...)

les précurseurs et la communauté BTC ne reconnaissent pas les autres comme des crypto actifs valables on les appelle des bitcoins maximalistes « enjoy staying poor »

020 the need for market places

Dépasse les frontières du monde numérique L'usage s'étend de plus en plus Donne naissance à d'autres monnaies ? => Il faut des places de marché

DEX and CEX

DEX

- De-centralized
- web / non-WEB
- utilisé ainsi à l'origine

CEX

- plate-formes centralisées
- facilité d'échange contre des fiat
- opposition au concept d'origine (Re-centralisation vs P2P)

References

- <https://defiprime.com/exchanges>

040 re centralization

Fiat, coin & token

Fiat

Les monnaies sont appelées de FIAT

Une monnaie-fiat est une monnaie décrétée par l'État

- Le mot fiat est un mot latin qui signifie "qu'il en soit ainsi", c'est-à-dire décrété par l'État.
- Ca concerne les monnaies contemporaines officielles d'état

Coin

COIN = littéralement “une piece” (c'est un crypto-actif)

possède sa propre blockchain attitrée (= token principal) (ex: Ethereum, Bitcoin)
il peut être miné (ex: proof-of-work) est nécessaire au bon fonctionnement de sa blockchain important de connaître les abréviations des coins pour les échanges

Token

TOKEN = littéralement “un jeton” (c'est un crypto-actif)

un actif stocké sur une blockchain ils peuvent être natifs d'une blockchain (ex: bitcoin, ethereum) ou hébergés par une blockchain qui n'est pas la leur (ex: fonctionnent sur ethereum) ils ont des règles de création spécifiques ils ne sont pas (forcément) minés

Coin types

Assets

Commodity

Currency

Collectible

Shitcoins

Stable coins

References

<https://atas.net/crypto-trading-en/bitcoin-boom-asset-commodity-currency-or-collectible/>

Les envies post-Bitcoin

La blockchain bitcoin permet seulement de posséder des actifs et faire des transactions Mais la communauté a envie de faire plein d'autres choses en plus (d'autres actions que stocker / échanger) Penser « Blockchain as a Platform »
Ajout de règles logiques et d'automatisation (donc la possibilité de coder)
martContracts

COMMENT ON MET LES ENVIES EN PLACE POUR DE VRAI ? les gens qui veulent faire différent il leur suffit de copier du code source de bitcoin et de modifier et de trouver des utilisateurs :-) utilisable en plus de bitcoin (ou à la place de bitcoin)

Documentaires

- TODO: [Magic Money: The Bitcoin Revolution](#)
- TODO: [The Rise and Rise Of Bitcoin](#)
- TODO: [Bitcoin: The end of money as we know it](#)
- TODO: [Netflix: Explained - Cryptocurrency](#)

Youtube

- TODO: <https://www.youtube.com/watch?v=l90LfbbjQs>
- TODO: <https://www.youtube.com/watch?v=4qkrphU4AU0>
- TODO: <https://www.youtube.com/watch?v=a2ZABbMFqFU>
- TODO: <https://www.youtube.com/watch?v=epYn2uxuWEI>
- TODO: <https://www.youtube.com/watch?v=EWfGzeF3Xmw>
- TODO: <https://www.youtube.com/watch?v=tW3zHIOudgo>

People

Owen Simonon (Hashneur)

- Influenceur

FIXME: add short bio

FIXME: explain why he is relevant

Claire Blava

- Claire Blava : blockchain partners

FIXME: add short bio

FIXME: explain why he is relevant

Communities

Maître Rakoon

maitre rakoon : tres actifs sur FB et accueillants pour les débutants, bonne modération, décisions plutot démocratiques

Cryptoast

cryptoast : vulgarisation des sujets, site d'actu à jour, chaine youtube avec interview d'experts

The CoinTribune

coin tribune : magazine dédié au sujet, référence dans le secteur

Les pros des cryptos (BFM Business)

000 plan

Formation Blockchain pour non spécialistes

Appréhender la technologie Blockchain

- La présence de la Blockchain : de Facebook aux poulets d'Auvergne.
- Le Parlement va légiférer sur les usages de la Blockchain.
- Les nouveaux métiers sur le marché.
- Le cas d'usage simple : certifier un document.

Démonstration

Un site en ligne de certification de document : comment ça marche ?

Définir la technologie Blockchain et ses usages

- Le stockage de transactions métier dans un réseau (confiance, algorithme de consensus, infalsifiable).
- Les applications de la Blockchain pour le transfert d'actifs.
- Les usages de la Blockchain en qualité de registre (traçabilité des produits...)
- Les Smart Contracts pour l'infalsification des termes et conditions d'exécutions.
- Les champs d'exploitation : finance, secteur public, échanges commerciaux, startups et industrie.

Démonstration

Démonstration en ligne d'un site d'expérimentation de transactions.

Présentation d'une étude de cas dans un circuit de commercialisation avec traçabilité.

Comprendre les écosystèmes Blockchain

OK * La Blockchain et l'historique Bitcoin. OK * Le principe du Hash, de la machine à Hasher, le minage.

- Les 4 briques de base de la Blockchain privée et permissionnée Hyperledger Fabric.
- Les 3 écosystèmes : Bitcoin, Ethereum, Hyperledger Fabric.

- La technologie Blockchain et le RGPD.

Démonstration

La Bitcoin en live. Découverte en ligne de la fondation Linux autour du projet Open Source Hyperleger.

Se projeter dans la technologie Blockchain

- Les perspectives d'une nouvelle économie numérique : la « token économie ».
- La Blockchain au cœur des évolutions Web : « self-sovereign identity » et « self-managed data ».
- Le lien entre la Blockchain et les autres solutions de confiance/sécurité.
- Les autres écosystèmes Blockchain.

Réflexion collective

L'intégration dans le Système d'Information des participants.

more references

Pre-requis necessaires

Summer reading:

* Antonopoulos Andreas (2014) Mastering Bitcoin, chapter 1 and 2 ([buy](#), [source code](#)) * Guerraoui, Rachid (2018) [FR] L'algorithmique repartie : a la recherche de l'universalite perdue ([document](#)) * Guerraoui, Rachid, Kuznetsov, Petr (2018) Algorithms for concurrent systems * Internet Engineering Task Force (2014) RFC 7231 Hypertext Transfer Protocol ([document](#)) * Raymond, Eric S.(1999) The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary * Wong, David (2021) Real-World Cryptography ([livebook](#)) * Antonopoulos Andreas, Wood Gavin (2019) Mastering Ethereum ([editor](#), [source code](#)) * Corda Documentation ([link](#)) * Hyperledger Fabric Documentation ([link](#)) * Lavayssiere, Xavier (2019) Libra Compendium ([document](#)) * Nakamoto, Satoshi (2008) Bitcoin Whitepaper ([document](#)) * Song, Jimmy (2019) Programming Bitcoin * Wood, Gavin (2014) Ethereum Yellow paper

Histoire du bitcoin

FIXME: Une forme de monnaie ?

L'élément le plus important sur un billet de banque est le numéro de série car c'est ce qui permet d'identifier sa véracité.

Il fallait trouver un moyen de créer du cash numérique, c'est à dire un actif identifiable, identifiable et infalsifiable.

De plus la nature dé-centralisée de la blockchain pose des questions spécifiques :

* Théoreme CAP (consistence, disponibilité, partitionnement) * Attaque

Références

- DONE <https://www.youtube.com/watch?v=4mjYw53oe6Q>

PEER 2 PEER

Elle doit pouvoir d'échanger en P2P sans tier de confiance. Ce qui permet de donner de la valeur à un actif en tant que monnaie d'échange, c'est la confiance que l'on place en cet actif. Ce qui permet l'échange en P2P c'est la confiance entre 2 individus. Objectif, créer de la confiance dans un actif numérique en utilisant le biais de la cryptographie.

BLOCKCHAIN Spécificité : Le concept de la blockchain

4 SPECULATION

After Blockchain as a Platform (d'autres actions que stocker / échanger) ajout de règles logiques et d'automatisation (donc la possibilité de coder) SmartContracts

FORK

les gens pas content qui veulent faire différent copie du code source

ALTCOINS Les bitcoins maximalistes bitcoin VS shitcoins « enjoy staying poor »

From DEX to CEX DEX Concept : Centralized De-centralized web / non-WEB voir <https://defiprime.com/exchanges>

re-centralisation vs P2P TODO: CEX vs DEX

KYC (Know Your Customer)

Il existe plein d'autres blockchain, actifs, et plate-formes (ex: Litecoin, Doge, Tezos...) Aujourd'hui les principales crypto et plate-formes sont ETH et BTC
TODO: entourer / rendre flashy ETH et BTC

COIN BITCOIN ETHEREUM LITECOIN TEZOS un jeton (aussi) possède sa propre blockchain attitrée (= token principal) (ex: Ethereum, Bitcoin) peut être miné est nécessaire au bon fonctionnement de sa blockchain

TOKEN BITCOIN ETHEREUM LITECOIN TEZOS un "jeton" un actif stocké sur une blockchain ils peuvent être natifs (ex: bitcoin) ou hébergés ils ne peuvent pas (forcément) être minés

STABLE COIN USDT USDC BUSD DAI crypto actif "relativement stable" intérêt : ne pas convertir en fiat (notamment pour les taxes) Trois types de stable coin : Le premier est le fiat-collateralized, c'est-à-dire "garanti fiat" (le fiat est une monnaie traditionnelle comme le dollar et l'euro). Ce modèle implique que l'entité qui émet le stable coin soit détentrice d'un compte bancaire contenant en devise fiat la valeur des jetons émis. Par exemple, si elle met en circulation 1 million de coins adossés au dollar, elle doit avoir 1 million de dollars dans un compte bancaire. Le deuxième est le crypto-collateralized, un coin soutenu par une autre crypto-monnaie. Pour compenser la volatilité, le stable coin est sur-adossé. Par exemple, l'équivalent de 1 000 dollars de bitcoins peut être demandé pour émettre l'équivalent de 500 dollars de stable coins. Même si le bitcoin perd 30% de sa valeur, le stable coin reste couvert. Le troisième est le non-collateralized, le non garanti. Dans ce cas, le stable coin est soutenu seulement par sa valeur grâce à un smart contract (un contrat qui s'exécute automatiquement). Si la demande totale pour le stable coin augmente ou diminue, alors le contrat changera automatiquement le nombre de coins en circulation pour maintenir le prix stable.

NON FONGIBLE TOKEN BITCOIN ETHEREUM LITECOIN TEZOS un "jeton" un actif stocké sur une blockchain ils peuvent être natifs (ex: bitcoin) ou hébergés ils ne peuvent pas (forcément) être minés

MAXIMALIST Les bitcoins maximalistes

TRADING encore en phase expérimentale de la hype une opportunité de la demande (ou pas) achat / vente en fonction plusieurs types d'investisseurs : holder (voir aussi "hodler" dans le monde de la crypto) / trader

WHALES gros investisseurs (gros % de BTC) There are around 1,000 individuals, known as whales, who own 40% of the market. contrôlent et peuvent manipuler le marché achat en masse => le cours monte vente en masse => le cours baisse participent à la volatilité du BTC

Not your keys, not your coins. a qui appartient la clef ? (qui est propriétaire) qui controle la clef ? (qui a les clefs) ex: un appartement (aujourd'hui certains CEX ont prévu une assurance ...)

scandale / perte des fonds des usagers

SCAMS gros investisseurs (gros % de BTC) There are around 1,000 individuals, known as whales, who own 40% of the market. controlent et peuvent manipuler le marché achat en masse => le cours monte vente en masse => le cours baisse participent à la volatilité du BTC

hot & cold wallets Approche "individualiste" différents types de wallets Expliquer ce qu'est un cold wallet / hot wallet du point de vue de l'usage fréquent / moins fréquent = petites sommes / grosses sommes => le besoin d'accès à internet est une conséquence de ça

hot wallets smartphone, software etc Approche individualiste Expliquer ce qu'est un cold wallet / hot wallet du point de vue de l'usage fréquent / moins fréquent = petites sommes / grosses sommes => le besoin d'accès à internet est une conséquence de ça

FIXME: est-ce qu'on met le hot wallet ici ou ailleurs ? FIXME: changer l'illustration ?

il s'agit de copier & chiffrer des fichiers cold wallet hardware (ex: Ledger) cold wallet software

FIXME: changer l'illustration ?

5 BLOCKCHAIN

MINING

aujourd'hui consommation électrique énorme (proof of work)

la majorité des fermes de minage sont logées en chine utilisent de l'énergie verte (donc pas forcément un pb économique) => objectif : réduire le cout de l'électricité

consomme moins que les transactions bancaires classiques le futur passera probablement par une autre technologie de minage moins consommatrice voir proof of stake (voir Ethereum / Tezos)

6 FUTURE

20 999 999,9796 BTC 21 MILLIONS anecdote mathématiques vs arrondi rareté artificielle impact probable sur le cours

18 MILLIONS ici on parle du rythme 18 millions déjà minés 4 millions perdus (?)
le dernier qui sera miné sera vers 2140 (TODO: vérifier) notion de halving

DEFLATIONARY CURRENCY 1 phrase (sans détails) SYSTEME CLASSIQUE =
ARGENT DETTE 1 phrase (sans détail) création monétaire bancaire

Le pb des subprimes a été créé par les banques

=> 2/ comment on fait pour se passer des banques ? => 1/ comment on fait pour
créer un actif non-dette ? => 3/ idéalement de façon décentralisée ?

DIGITAL GOLD tout le monde n'en aura pas :D nombre de personnes sur terre
FIXME: combien en moyenne par personne ?

Michael Saylor Elon Musk Jack Dorsay 3 early adopters corporate (CEO)
connaissent l'univers numérique un changement de posture prise de risque pour
leur réputation

décision validée par leurs entreprises officialise l'entrée des institutionnels font la
promotion des crypto cours de Tesla = cours de BTC ? prise de risque pour
l'entreprise

une tendance qui se confirme Facebook Libra / Diem (?) Amazon Coin (2013) ---
split --- Europe / Euro numérique Chine / Yuan numérique

une tendance qui se confirme Facebook Libra / Diem (?) Amazon Coin (2013) ---
split --- Europe / Euro numérique Chine / Yuan numérique

une tendance qui se confirme Facebook Libra / Diem (?) Amazon Coin (2013) ---
split --- Europe / Euro numérique Chine / Yuan numérique

une tendance qui se confirme Facebook Libra / Diem (?) Amazon Coin (2013) ---
split --- Europe / Euro numérique Chine / Yuan numérique

ETHEREUM Platform smartcontracts Ether as a currency (same way as BTC for
the bitcoin blockchain) Comparaison Ether / Bitcoin

DeFi (Decentralized Finance) Approche "collective" de la gestion du risque Basé
sur Ethereum Decentralized Finance (Smart)Contrats & services financiers
Alternative au banques & assurances classiques => un vrai "danger" pour le
système traditionnel (?) => contreparties (\$++ ou en conditions) =>

Blockchain

Définitions

Une blockchain c'est quoi ? Une chaîne de blocs :D

C'est quoi un bloc ? C'est un "container" pour stocker des informations.

Exemple d'information:

- un tableau où chaque case contient 3 valeurs : source + destinataire + montant (comme dans la blockchain de bitcoin)
- un tableau où chaque case contient un numéro d'instruction exécuté, une modification de l'état mémoire, la prochaine instruction (comme dans la blockchain d'Ethereum)

Comment ça marche ?

Chaque bloc contient les informations (sous forme de Merkle-tree, mais ça on s'en fiche), ET un identifiant du bloc.

L'identifiant du bloc est unique et composé d'un numéro et d'une empreinte de son contenu (ex: la somme des contenus dudit tableau).

Cette empreinte sert de "signature" et permet ainsi vérifier si le contenu est falsifié (ou pas) pour un bloc donné.

Parmi les contenus, chaque bloc indique également le numéro du bloc précédent.

| bloc bloc préc. contenu | [2, 60, 1, 25, 2, 42, 16] | [1, 25, 0, 27, 1, 1, 23] v [0, 27, 0, 0, 12, 1, 14]

Pendant ce temps, un nouveau bloc est en cours de construction, sur chacun des membres du réseau

| bloc en cours de construction | [3, ?? 2, 60, ??, ??, ??]

Les consensus proof of work vs proof of stake

blogchain café

le blog sur la blockchain

blogchain café

Les consensus: Proof of work vs Proof of stake

powpos Share on LinkedInShare on TwitterShare on Google+

L'état du système bitcoin à un instant T est une collection de outputs de transactions non dépensées qu'on appelle UTXO.

L'argent disponible dans chacun de ces outputs est protégé cryptographiquement par le protocole de la monnaie: quiconque veuille dépenser une somme dans un UTXO doit fournir la preuve qu'il en est bien le propriétaire.

Au lieu stocker explicitement le soldes de tout le monde, bitcoin garde l'historique complet des transactions des utilisateurs et les manie dynamiquement pour déduire l'état courant. Les transactions représentent donc des échanges atomiques de monnaie qui modifient l'état interne du système.

La découverte de nouveaux blocs se fait selon un ensemble précis de règles définies dans le protocole. Ces règles doivent protéger la blockchain des attaques et atteindre rapidement un consensus lorsque par exemple apparaissent des ramifications blockchain (forks).

La Proof of work (preuve de travail) et la Proof of Stake (preuve d'enjeu ou de possession) sont les deux manières de valider les blocs les plus connues. Elles impliquent deux mécanismes de consensus très différents.

Le processus de résoudre un défi informatique imposé par une Proof of Work est appelé mining: on parle de mineurs.

Le processus de résoudre un défi informatique imposé par une Proof of Stake est appelé minting: on parle de forgeurs.

Le théorème CAP dit qu'il est impossible sur un système informatique de calcul distribué de garantir en même temps (c'est à dire de manière synchrone) les trois contraintes suivantes:

- Cohérence: tous les nœuds du système voient exactement les mêmes données au même moment ;
- Disponibilité : garantie que toutes les requêtes reçoivent une réponse;
- Tolérance au partitionnement : aucune panne moins importante qu'une coupure totale du réseau ne doit empêcher le système de répondre correctement.

Tout système de calcul distribué ne peut garantir à un instant T que deux de ces contraintes, mais pas les trois.

Les cryptomonnaies sont ainsi

1. disponibles (chaque requête reçoit toujours une réponse),
2. tolérants à la distribution (le service fonctionne encore même si quelques nœuds échouent), mais
3. il ne sont jamais cohérents.

Au fil du temps, des utilisateurs différents peuvent voir des pseudo états courants différents. Par exemple l'incohérence arrive lorsque le hash d'un bloc nouvellement découvert n'a pas encore été relayé à tous les utilisateurs du système.

Ces instabilités temporaires sont un grand obstacle lorsqu'on implémente une cryptomonnaie, puisque à la fin il faudra bien finir par obtenir une consistance finale. Les incohérences sont physiologiques, et donc tolérées, mais doivent être transitoires, mieux encore éphémères.

C'est le rôle du protocole de consensus. Pour cela il impose les exigences suivantes

1. Un utilisateur qui a découvert un bloc est encouragé à l'émettre sur le réseau immédiatement sans le retenir
2. On doit décourager l'utilisateur de découvrir les blocs des chaînes intermédiaires (il faut qu'il focalise sur les plus longues).
3. Les règles de consensus doivent être construites de manière à résoudre l'ambiguïté qui se forme à la suite d'un fork de blockchain: lors d'un fork une des branches en compétition doit prendre le contrôle sur les autres dans un temps raisonnablement court.

Proof of Work

Chaque bloc Bitcoin consiste de deux parties :

- partie de tête (header) avec les paramètres clés: timestamp de création du bloc, référence au bloc précédent, la racine de l'arbre Merkle du bloc de transactions...
- partie centrale qui contient la liste de transactions.

Pour faire référence à un bloc spécifique, on fait le hash SHA-256 de son header deux fois. L'entier résultant appartient à l'intervalle

$$[0, 2^{256} - 1]$$

Dans la Proof of Work, pour qu'un bloc soit considéré valable, cet entier ne doit pas excéder un certain seuil :

$$\text{hash}(B) \leq M/D$$

$D \in [1, M]$ représente la difficulté de la tâche.

Il n'y a aucune façon connue de prédire à l'avance quel argument B va satisfaire cette équation. La seule possibilité est de lancer une sorte d'attaque en force brute aléatoire et itératif, dans l'espoir de trouver avant les autres un minimum assez petit. Plus haute est la valeur de D, plus il faudra d'itérations avant de trouver un bloc valable.

Proof of Stake

La Proof of Stake a, elle aussi, une inégalité à satisfaire mais celle-ci concerne la quantité de monnaie qu'un utilisateur possède.

La probabilité qu'un compte parvienne à confirmer le prochain block de transactions à ajouter à la blockchain est proportionnelle à la quantité de monnaie qui est sur ce compte. Plus précisément, elle est proportionnelle au rapport entre le solde de l'utilisateur à l'instant T et le total de la monnaie en circulation.

Pour faire court, une personne possédant 5 % d'une monnaie PoS peut miner le 5 % des blocs de la même façon qu'une personne possédant 5 % de la puissance du réseau du bitcoin peut théoriquement miner le 5 % des blocs. C'est comme si une PoS tentait de copier simplement la PoW en faisant de chaque pièce de sa monnaie un simulated mining rig.

Prenons un utilisateur avec l'adresse A et un solde $\text{bal}(A)$. Une fonction de PoS commune utilisera cette condition

$$\text{hash}(\text{hash}(B_{\text{prev}}), A, t) \leq \text{bal}(A) M/D$$

· B_{prev} dénote le bloc sur lequel l'utilisateur est en train de construire, · t est le timestamp UTC courant.

Contrairement à l'équation PoW, la seule variable que l'utilisateur peut changer est le timestamp t, dans la partie gauche de l'équation.

En effet le solde est connu publiquement et on peut aisément calculer les avoirs de chaque membre en prenant par exemple les montants qui n'ont pas été déplacés pendant les dernières 24h.

Le temps pour trouver un bloc pour l'adresse u est exponentiellement distribué avec un taux

$\text{bal}(A)/D$

Ainsi, si la provision monétaire de la monnaie est fixe ou tout au plus grandit à un taux connu, la difficulté D est connue à l'avance :

$$D = 1 / \text{Tex} \sum \text{bal}(a)$$

Tex dénote le temps attendu (expectation time) entre deux blocs.

Dans la pratique, D est ajustée en dynamique en se basant sur les blocs récents afin de tenir compte du fait que tous les propriétaires de monnaie ne participent pas au minting des blocs en même temps.

Le Nothing at Stake

Dans une Pow: en contribuant aux décisions pour les validations blockchain, un mineur doit faire le choix entre toutes les fourchettes possibles (ou à défaut en commencer une nouvelle). Les options sont mutuellement exclusives. Voter double n'est pas profitable puisque on gaspille son pouvoir de mining en l'éparpillant. La stratégie payante est celle de miner exclusivement sur la fourchette que vous pensez avoir le plus de chance de gagner.

[powsec]

Avec la Pos la situation est différente: le vote est libre et ne coûte rien. Si on est en train de miner, chaque coin qu'on possède a une certaine chance par seconde d'être utilisable pour signer un bloc. Cela a un inconvénient majeur: s'il y a des forks multiples, la stratégie optimale est de voter sur tous les forks en même temps.

C'est le concept de Nothing at Stake.

[possec1]

Consensus objectif et faiblement objectif.

Un protocole de consensus est objectif si un nouveau nœud peut arriver au même état auquel arrive le reste du réseau en se basant seulement sur les règles du protocole et les messages propagés à travers le réseau.

La PoW est un exemple d'un protocole objectif: tant qu'un nouveau noeud est connecté à au moins un utilisateur honnête, il choisira un bloc valide.

La PoS par contre n'est pas objective. En effet, si nous prenons un attaquant avec assez de puissance de calcul. Pourvu que son fork soit assez longue, la difficulté sera ajustée pour favoriser le contrôle de ce fork de la part de l'attaquant. Ceci lui permet éventuellement de produire une chaîne plus longue que le vrai fork, c-à-d de celui qui aurait dû être valable.

Ce type de forks longues sont rejetées par les utilisateurs qui sont depuis un moment dans le système, mais les nouveaux arrivants, n'ayant pas de connaissance antérieure, sont poussés par le protocole même à préférer le fork de l'attaquant.

Un protocole de consensus est subjectif si le système a des états stables où des noeuds différents parviennent à des conclusions différentes. Dans ce cas il faut une grande quantité d'informations sociales externe pour participer.

Les systèmes qui utilisent des réseaux sociaux comme leur ensemble de consensus (eg. Ripple) est nécessairement subjectif. Un nouveau noeud qui ne connaît rien d'autre que le protocole et les données peut être convaincu par un hacker que ses noeuds sont dignes de confiance. Sans une informations sociale externe qui donne de la réputation il est impossible de résoudre ce type d'attaque.

C'est très différent de la PoW dans laquelle l'état actuel est toujours celui qui a fédéré la plus haute quantité de ressources de calcul.

Un protocole de consensus est faiblement objectif si un noeud a besoin d'un état récent en plus des règles du protocole et des messages propagés pour déterminer l'état actuel du système.

Un nouveau noeud venant sur le réseau sans connaissance sauf

1. les règles du protocole,
2. l'ensemble de tous les blocs + les messages « importants » qui ont été publiés et
3. un état assez récent (moins de N blocs dans le passé) qui est certainement valable

peut arriver seul à la même conclusion que le reste du réseau quant à l'état actuel.

La PoS est faiblement objective. Si il y a ambiguïté il suffira de lire le contenu d'un bloc avec au moins profondeur N , pour déterminer l'état courant du système. Un membre nouveau venu pourrait ainsi avoir accès à ce bloc d'une source fiable (par exemple, un site Web consacré à la monnaie en question).

Bien que cette méthode affaiblit la sécurité et modifie radicalement les coté décentralisation, la subjectivité faible est une bonne façon de combiner la sécurité computer-driven et celle social-driven.

Les différences PoW / PoS

Une PoS peut mettre des restrictions aux valeurs possibles de t . Par exemple, t ne doit pas différer du temps UTC sur des noeuds de réseau de plus d'une heure. Ainsi un utilisateur devra essayer au plus 3600×2 valeurs de t .

C'est la raison pour laquelle il n'y a pas de calculs particulièrement lourds dans un PoS. Les mécanismes PoS ne nécessitent pas de matériel informatique puissant et onéreux pour la maintenance de la blockchain et ne consomment pas beaucoup d'électricité. Les PoS demandent des ressources nettement plus petites par rapport aux PoW, à la louche d'un facteur 1000. C'est pourquoi on les considère comme une technologie verte.

Le PoS n'est pas sujet au risque d'attaque 51% car, pour mener une telle attaque, il faudrait posséder au moins 51% de la masse monétaire, ce qui est considéré comme impossible, sauf peut être au tout début lorsque toutefois la monnaie ne vaut forcément pas encore grand chose.

Une monnaie PoS n'a pas d'inflation. La masse monétaire est créée au début, et c'est pourquoi un système PoS garantit qu'une monnaie sera déflationniste.

Malgré ses faiblesses remplacer la preuve de travail par la preuve d'enjeu reste un objectif intéressant car un algorithme PoS consomme beaucoup moins d'énergie que l'algorithme PoW.

Toutefois si on se limite à cette seule considération, on passe à côté du fait qu'une blockchain PoS ne peut structurellement pas offrir le même niveau de sécurité qu'une PoW vu qu'elle ne demande pas de travail en contrepartie de ses validations. On pense généralement qu'une PoS est équivalente et meilleure d'un PoW, mais il n'en est rien.

Dans une blockchain PoS, si vous avez possédé assez de la monnaie à un certain point dans le passé vous pouvez faire votre propre chaîne alternative gratuitement et sans effort. Les autres membres ne pourront pas dire la différence entre la

vraie chaîne et la votre sans disposer de quelques informations supplémentaires externe.

Le problème est dans le fait que le coût production des coins PoS est pratiquement zéro car aucune énergie n'a été dépensée pour les créer. Ainsi aucune fonction de coût ne limite la quantité de coin PoS disponibles sur le marché dans le futur.

On sait que la valeur d'un réseau est fonction du carré du nombre de ses utilisateurs mais elle n'augmente pas en fonction de la quantité de coins circulant sur le réseau. La valeur réside plutôt dans le volume de transactions/paiements que le réseau est capable d'absorber.

Considérons le fait que les cryptomonnaies sont des entités numériques, divisibles à l'infini et à grande vitesse (on appelle cela la fragmentation de l'effet réseau). De toute évidence une quantité de coins illimitée dans le futur fait obstacle à la valorisation de la cryptomonnaie car il n'y a plus de lien déterministe entre la valeur présente du réseau et la valeur des coins future.

Par conséquent la valeur d'une monnaie PoS peut décroître même si le nombre d'utilisateurs augmente: une monnaie 100% PoS ne peut pas avoir valeur d'investissement. Elle aura uniquement une valeur d'usage avec sa valeur unitaire qui tend vers zéro si les offres se multiplient indéfiniment.

Une blockchain PoS véhicule donc une monnaie qui n'a qu'une valeur conventionnelle entre les participants. Ses transactions s'apparentent aux transactions Bitcoin des colored coins et comme eux devra être compensée par un transfert de valeur effectif sur un autre réseau (euro, bitcoin ou autre).

A l'inverse d'une chaîne PoS, une blockchain PoW est une infrastructure qui ne peut pas être efficacement répliquée.

La réplication du réseau Bitcoin (par exemple lorsque on a créé le réseau Litecoin) est un gaspillage du point de vue de la sécurité et ne peut se justifier que par le nombre de transactions supplémentaires qu'il permet.

Mais là aussi on peut pas considérer Litecoin comme une solution de scalabilité pérenne, vu qu'il existent des solutions de scalabilité interne au Bitcoin plus efficace qu'une blockchain flottante satellite.

Il existe une solution élégante et efficace si on combine les deux: un sidecoin PoS liée à la blockchain Bitcoin pegged sidechain. Cela évite à la monnaie PoS de converger inexorablement vers zéro tout en gardant les avantages de la faible

consommation énergétique du protocole PoS et de la pérennité de la valeur des coins PoW.

Grâce au mapping des sidecoins PoS avec la blockchain bitcoin, un acheteur ne pourra acquérir la majorité des sidecoins PoS qu'en payant le prix du marché des bitcoins. La sidechain PoS devient ainsi un registre publique annexe dont la sécurité sera directement liée à la quantité de bitcoins convertis en sidecoins PoS.

[87689]Auteur microingensPublié le mars 14, 2016mars 14, 2016Catégories bitcoin, blockchain, techniqueÉtiquettes Bitcoin, blockchain, blog, colored coins, conseil, consulting, enjeu, proof of work, pegged sidechain, POS, POW, preuve, proof of stake, travail, UTXO

2 pensées sur "Les consensus: Proof of work vs Proof of stake"

1. Ping : Les consensus: Proof of work vs Proof of stake ...
2. Ping : Slock.it: Ethereum, IoT et économie collaborative – blockchain café

Laisser un commentaire Annuler la réponse.

Votre adresse de messagerie ne sera pas publiée. Les champs obligatoires sont indiqués avec *

<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Commentaire []

Nom * []

Adresse de contact * []

Site web []

[Laisser un commentaire]

Navigation de l'article

Précédent Article précédent : Blockchains permissioned vs unpermissioned

Suivant Article suivant : Slock.it: Ethereum, IoT et économie collaborative

Recherche pour : [] Recherche AUTEUR

David TERUZZI * Consultant blockchain * Co-fondateur de blockchain-conseil.fr *
Développeur affilié du projet DECRED * Chroniqueur blockchain pour FINYEAR *

Programmeur expert en maths appliquées * Expert en IA, machine learning, data mining.

david teruzzi

contactez-moi

linkedin128 twitter128

Articles récents

• Compte rendu de la conférence Digital Contracts, Identities and Blockchains au MIT (par Marc Dangeard) juin 2, 2016 • Common Accord: le pont smart contracts / contrats papier mai 19, 2016 • Quelques stats sur le bitcoin comme moyen de paiement mai 18, 2016 • Bitcoin: la mise à jour Segregated Witness mai 13, 2016 • La mère de toutes les DAO mai 12, 2016 • Le DAO.LINK mai 9, 2016 • La programmation de smart contracts: une opération hautement délicate. mai 7, 2016 • BigchainDB: le database blockchain évolutif. mai 1, 2016 • Blockchain: la fin du big data ? avril 29, 2016 • DAO: Contractors et Curators avril 27, 2016

Commentaires récents

• Slock.it: Ethereum, IoT et économie coll... dans Slock.it: Ethereum, IoT et économie collaborative • DAO: Contractors et Curators - blockchain ... dans DAO: Contractors et Curators • La mère de toutes les DAO - blogch... dans La mère de toutes les DAO • Comprendre Ethereum (2): the Ethereum State Tra... dans Comprendre Ethereum (2): the Ethereum State Transition Function • Comprendre Ethereum (1) - blockchain caf&e... dans Comprendre Ethereum (1)

Archives

• juin 2016 (1) • mai 2016 (7) • avril 2016 (4) • mars 2016 (3) • février 2016 (5) • janvier 2016 (23)

Catégories

• bigchainDB (1) • bitcoin (19) • blockchain (22) • common accord (2) • cryptomonnaies (9) • DAO (2) • daohub (1) • Dapp (3) • decred (2) • ethereum (12) • Lisk (2) • MaidSafe (1) • maths (1) • mining (2) • news (10) • ripple (2) • safecoin (1) • smart contract (2) • technique (19) • trading (1) • tutoriel (4)

AUTRE

• Connexion • Flux RSS des articles • RSS des commentaires • Site de WordPress-FR

PARTENAIRES

blogchain café Fièrement propulsé par WordPress

Références

- <http://blogchaincafe.com/les-consensus-proof-of-work-vs-proof-of-stake>