La *blockchain* – Les défis de son implémentation

Par Ilarion PAVEL
Ingénieur en chef des mines, Conseil général de l'économie, de l'industrie, de l'énergie et des technologies et Laboratoire de physique théorique de l'École normale supérieure

Nous passerons en revue dans cet article plusieurs des difficultés techniques et défis juridiques, sociétaux ou réglementaires rencontrés dans l'implémentation de la *blockchain,* et nous suggérerons quelques pistes de solutions.

Introduction

La *blockchain* est apparue en 2008 comme partie intégrante du bitcoin [1], crypto-monnaie et système de paiement [2] qui fonctionne sans autorité centrale sur un réseau pair-à-pair, *via* des transactions cryptées. Toutes les transactions sont vérifiées par les nœuds du réseau et enregistrées dans un registre public réputé infalsifiable appelé *blockchain* [3].

Disposant de puissants moyens de calcul, certains nœuds du réseau qualifiés de « mineurs » vérifient, enregistrent et sécurisent les transactions. Celles-ci sont groupées dans des blocs, qui seront ensuite « enchaînés » l'un à la suite de l'autre pour former la *blockchain*. Le dernier bloc en date est ajouté au précédent (celui-ci étant dit « miné ») par le premier « mineur » qui réussit à résoudre un problème cryptographique difficile appelé « preuve de travail ». Ce mineur reçoit alors une certaine somme de bitcoins en récompense de sa réussite, et le nouveau bloc se propage à l'ensemble des nœuds du réseau.

Comme pour toute autre monnaie, on peut échanger des bitcoins contre de la monnaie fiduciaire, des produits ou des services en effectuant des transactions électroniques au moyen d'un logiciel installé sur un ordinateur personnel ou sur un terminal mobile, ou *via* une application *Web* [4].

Dès son lancement, le bitcoin a été imité par des systèmes de crypto-monnaies alternatives (*altcoins*) qui utilisent les mêmes techniques, mais avec diverses optimisations. De même, les techniques de la *blockchain* ont été utilisées, avec succès, pour mettre en œuvre des chaînes alternatives (*altchains*) qui permettent des applications autres que la monnaie électronique (gestion de ressources ou contrats), élargissant ainsi la sphère de la *blockchain*, qui était à l'origine consacrée exclusivement aux transactions financières. Il existe déjà quelques centaines d'*altcoins* et d'*altchains*, et ceux-ci sont en plein développement.

On appelle *blockchain* 1.0 tout ce qui concerne la monnaie électronique et ses opérations (émission, transfert, paiement), *blockchain* 2.0 l'ensemble des applications financières et économiques autres que celles liées à la monnaie (actions, obligations, contrats à terme, prêts, hypothèques, propriété intellectuelle, contrats intelligents) et *blockchain* 3.0 d'autres applications en dehors des sphères financière et économique (administration, santé, science, culture, art).

Le bitcoin est actuellement la monnaie cryptographique la plus utilisée dans le monde, avec un volume de transactions en pleine croissance [5]. Le bitcoin et ses alternatives (*altcoin, altchain*) vont probablement transformer le paysage financier et économique, mais leur implémentation risque de se heurter à plusieurs difficultés techniques, ainsi qu'à des défis de nature réglementaire, juridique et sociétale.

Les difficultés techniques

L'insuffisance de la capacité de transaction

La taille d'un bloc du bitcoin a été intentionnellement limitée à 1 Mo afin d'éviter des attaques du type « déni de service » : une personne mal intentionnée pourrait créer des blocs de grande taille et les diffuser à travers le réseau afin de provoquer des congestions, voire la paralysie du trafic.

Par ailleurs, le temps nécessaire pour miner un bloc a été fixé à environ 10 minutes. La diminution de ce laps

(1) NAKAMOTO (Satoshi), "Bitcoin: A Peer-to-Peer Electronic Cash System", https ://bitcoin.org/bitcoin.pdf
(2) Par abus de langage, on associe le terme « bitcoin » à la fois à l'unité de valeur de monnaie électronique, à la technologie sous-jacente et au réseau sur lequel cette dernière opère.
(3) De même, le terme « blockchain *» est utilisé à la fois pour désigner le registre, la technologie ou le réseau.*
(4) Les aspects techniques de la technologie bitcoin sont bien plus complexes. Il existe de nombreuses références : voir, par exemple, ANTONOPOULOS (Andreas) (2015), Mastering Bitcoin*, O'Reilly Media.*
(5) Pour des statistiques concernant le bitcoin, voir https://blockchain.info/

de temps augmenterait la fréquence du phénomène dit de « fourche » [6]. Or, plus un réseau présente des phénomènes de fourche, et plus il est vulnérable aux attaques, notamment du type 51 % qui sera décrit plus bas.

Autre effet de l'augmentation de la taille du bloc et de la diminution du délai séparant deux blocs : l'augmentation du nombre des blocs « orphelins » (minés mais point attachés à la *blockchain* [7]).

La conséquence de ces limites (taille du bloc, temps entre deux blocs) est que le bitcoin peut supporter seulement 7 transactions par seconde (tps), ce qui est bien plus faible que d'autres réseaux comme celui de la carte Visa, qui supporte 2 000 tps en moyenne, avec une capacité de surcharge ponctuelle pouvant aller jusqu'à 56 000 tps.

À terme, avec l'accroissement du nombre des transactions, le temps nécessaire à leur validation risque d'augmenter, ce qui augmentera les frais de transaction [8].

Des solutions possibles sont l'augmentation de la taille du bloc (la doubler, voire l'augmenter encore davantage), la réduction du temps entre deux blocs et la réduction du temps de latence (laquelle réduira le phénomène de fourche [9]). Ainsi, l'*altcoin* Litecoin fonctionne avec un temps entre deux blocs de 2,5 minutes, l'*altchain* Ethereum avec 17 secondes. On peut envisager des solutions plus radicales, comme la reconception du protocole bitcoin [10], mais cela demanderait un consensus entre les acteurs (notamment de la part des mineurs).

Enfin, une autre possibilité pourrait consister à construire des piles protocolaires de niveau supérieur, au-dessus du protocole bitcoin, sous la forme de contrats intelligents. Ces piles protocolaires permettraient des millions de transactions par seconde, grâce à des canaux de paiement dont seules l'ouverture et la fermeture seraient incluses dans la *blockchain* (comme c'est le cas dans les réseaux Lightning [11] et TumbleBit [12]).

Un temps de latence trop long

Le temps de latence est le temps nécessaire pour propager un bloc à partir d'un nœud du réseau vers l'ensemble des utilisateurs : il est en moyenne de 12 secondes. Après 40 secondes, en moyenne 95 % des nœuds du réseau reçoivent le bloc [13]. C'est long par rapport au réseau Visa, dont le temps de latence est de quelques secondes, et encore plus long si l'on envisage d'utiliser la *blockchain* pour sécuriser les applications pour l'Internet des objets, qui sera composé d'objets communicants en interaction permanente quasi instantanée.

La diminution du temps de latence nécessite également de modifier le protocole bitcoin ou d'ajouter des couches protocolaires de niveau supérieur.

La taille de la *blockchain*

La taille de la *blockchain* du bitcoin est actuellement de 115 Go, elle est en croissance rapide : elle a augmenté de 50 Go sur les douze derniers mois. Charger la *blockchain* sur un ordinateur demande actuellement plusieurs jours et suppose que l'on dispose de suffisamment de mémoire libre sur son disque dur [14]. Il est cependant probable que l'évolution future des performances des ordinateurs et du débit Internet permettra de faire face à l'augmentation de la taille des *blockchains*.

De plus, les utilisateurs peuvent choisir entre être un nœud complet (contenant toute la *blockchain*, ceux-ci valident les transactions et les blocs, et transmettent l'information aux autres nœuds), ou être un client léger (ne téléchargeant que les entêtes des blocs, ce qui lui permet d'avoir une taille 1 000 fois inférieure à celle du nœud complet – mais le client léger doit se reposer sur les nœuds complets pour effectuer une transaction). Par ailleurs, les utilisateurs peuvent choisir d'être clients *Web* : l'accès au réseau bitcoin se fait alors à travers un navigateur connecté à un serveur-tiers de confiance.

Le manque de liquidité

Le bitcoin a été conçu pour être une monnaie dont la masse monétaire maximale a été fixée à 21 millions d'unités. L'émission de monnaie se fait par la récompense attribuée au premier mineur ayant miné un nouveau bloc [15]. Cette récompense, initialement de 50 bitcoins, est divisée par un facteur deux tous les 210 000 blocs minés, soit environ tous les quatre ans. À l'horizon 2140, la récompense sera inférieure à la plus petite unité, le « satoshi », qui vaut 10-8 bitcoins : il n'y aura alors plus aucune émission de monnaie et les mineurs seront rémunérés exclusivement par les frais des transactions.

---

(6) Cela se produit quand deux mineurs minent en même temps deux blocs différents. En fonction des délais de propagation dans le réseau (temps de latence), ces deux blocs peuvent arriver à certains mineurs dans un ordre donné, et à d'autres mineurs dans l'ordre inverse, ce qui a pour effet de scinder la blockchain *en deux chaînes. En pratique, les deux communautés de mineurs continuent à miner des blocs pour allonger les deux chaînes jusqu'au moment où l'une d'entre elles devient plus longue que l'autre : elle sera alors considérée comme la chaîne valide (et l'autre sera abandonnée).*

(7) Par exemple, deux blocs peuvent être minés l'un à la suite de l'autre dans la même chaîne, mais arriver dans l'ordre inverse dans un nœud de réseau (le deuxième bloc est alors appelé orphelin, il est mis temporairement dans un pool dans l'attente de l'arrivée du premier).

(8) En général, l'utilisateur paie des frais pour chaque transaction, ceux-ci vont au mineur ayant réussi à résoudre le bloc contenant la transaction. Plus les frais sont élevés, plus la transaction a des chances d'être intégrée en priorité au bloc miné suivant.

(9) CROMAN (Kyle) et al.*, "On Scaling Decentralized Blockchains", http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf*

(10) EYAL (Ittay) et al.*, "Bitcoin-NG: A Scalable Blockchain Protocol", https://arxiv.org/pdf/1510.02037.pdf*

(11) POON (Joseph) & DRYJA (Thaddeus), "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments", https://lightning.network/lightning-network-paper.pdf

(12) HEILMAN (Ethan) et al.*, "TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub", https://eprint.iacr.org/2016/575.pdf*

(13) DECKER (Christian) & WATTENHOFER (Roger) (2013), "Information Propagation in the Bitcoin Network", 13-th IEEE International conference on Peer-to-Peer Computing*, Trento, www.tik.ee.ethz.ch/file/49318d3f56c1d525aabf7fda78b23fc0/P2P2013_041.pdf*

(14) Aujourd'hui, pour un nœud complet, on conseille 125 Go d'espace sur le disque dur, 2 Go de mémoire RAM et une connexion Internet d'au moins 400 kb/s, https://bitcoin.org/en/full-node

(15) La récompense attribuée au mineur ayant miné le bloc a été prévue dès la conception du bitcoin afin d'encourager les opérations de minage.

Selon certains économistes, une diminution de l'émission monétaire pourrait créer un effet déflationniste. Les porteurs de bitcoins seraient alors tentés d'utiliser cette monnaie comme valeur de trésorerie, plutôt que comme instrument d'échange. À cela s'ajoutent les problèmes des bitcoins stockés dans des portefeuilles perdus (clé privée perdue) qui resteront dormants dans la *blockchain*. En conséquence, la valeur des bitcoins augmenterait, ce qui (à masse monétaire constante) diminuerait la liquidité des transactions (surtout dans un environnement déflationniste).

On oppose à ces critiques le fait que la division du bitcoin est très fine, la plus petite unité étant le « satoshi », soit 10^{-8} bitcoin. En cas de déflation, la monnaie pourrait se décaler (d'une ou de deux décimales) vers des valeurs plus faibles. De plus, il existe des *altcoins* d'une valeur inférieure (comme le Litecoin ou le Dogecoin) vers lesquels le bitcoin pourrait se rabattre pour compléter l'offre d'échange et empêcher ainsi la déflation, ou encore des *altcoins* comme Blackcoin, NXT, Peercoin ou VeriCoin, dont la masse monétaire est illimitée.

La déflation a mauvaise réputation, car elle est associée à l'effondrement brutal de la demande et peut conduire à une crise économique majeure. Actuellement, notre système financier dispose d'une monnaie fiduciaire dont l'émission est pratiquement illimitée et, en cas de déflation, une solution est d'augmenter la masse monétaire en imprimant des billets afin de relancer la demande. Dans le système du bitcoin, la déflation ne serait pas due à un effondrement brutal de la demande, mais à une réserve monétaire limitée et établie d'avance (toutefois, cette limite supérieure sera atteinte progressivement et ne causera pas automatiquement de crise financière).

La consommation d'électricité

Pour miner les blocs et ainsi valider les transactions, les mineurs doivent résoudre des problèmes cryptographiques difficiles, ce qui demande de grands volumes de calcul, et donc une consommation importante d'énergie (pour faire fonctionner les ordinateurs et les installations de refroidissement).

La difficulté du problème cryptographique à résoudre ne dépend pas du nombre et de la valeur des transactions, mais de l'arrivée de nouveaux mineurs attirés par les perspectives de gain financier et disposés à entrer sur ce marché concurrentiel. La rentabilité de leur activité dépend du prix de l'électricité converti en bitcoins.

Une étude a montré qu'en 2014, le réseau bitcoin consommait entre 0,1 et 10 GW [16]. Actuellement, l'ASIC (*Application-Specific Integrated Circuit*) le plus performant du marché (AntMiner S9) consomme 1 300 W, pour une vitesse de hachage de 13 THash/s, soit 100 W par THash/s. L'ensemble des mineurs du réseau bitcoin effectuent en moyenne 4 millions de THash/s, ils consomment donc 400 MW, ce qui représente la moitié de la puissance d'une centrale nucléaire. En pratique, comme les mineurs utilisent aussi des outils moins performants, cette consommation serait 3 à 4 fois plus importante que la valeur précédemment calculée [17].

Ce coût énergétique considérable doit être comparé aux économies potentielles que les institutions financières pourraient réaliser en remplaçant leur système de fonctionnement centralisé par le protocole *blockchain*. Selon Santander InnoVentures, en 2022, la technologie *blockchain* pourrait réduire les coûts d'infrastructure des banques de 15 à 20 milliards de dollars par an [18].

Une critique fondée formulée à l'encontre du protocole bitcoin est le fait que l'algorithme de preuve de travail ne sert qu'à assurer la sécurité du système et qu'il serait donc plus intéressant de l'associer à la résolution d'un problème utile, comme cela a été fait dans le cas des *altcoins* Primecoin (recherche de nombres premiers jumeaux et des chaînes de Cunningham), Curecoin (recherche de repliement de protéine) ou Gridcoin (grilles de calcul de recherche scientifique).

Les problèmes de sécurité

Le plus sérieux est l'attaque du type 51 % : un mineur ou un groupe de mineurs mal intentionnés disposant d'une grande capacité de calcul pourrait prendre le contrôle de la *blockchain* et utiliser celle-ci pour créer des « doubles dépenses ». Cela consiste à payer un produit, à entrer en sa possession, puis à créer intentionnellement une fourche, dont la nouvelle chaîne invalide la transaction et utilise l'argent pour acheter un deuxième produit (double dépense). Si sa puissance de calcul dépasse 51 % de la puissance totale des mineurs du réseau, un mineur mal intentionné aura la possibilité de miner des blocs dans la nouvelle chaîne de manière à dépasser l'ancienne, qui, de ce fait, sera invalidée.

Un mineur pourrait également effectuer une attaque de déni de service contre d'autres participants du réseau bitcoin en invalidant leurs transactions. Il suffit d'identifier la transaction correspondante, puis de re-miner le bloc qui la contient, en prenant soin de l'en enlever préalablement. La transaction restera en attente aussi longtemps que l'attaquant dominera le réseau des mineurs en puissance de calcul.

Selon certains modèles probabilistes, il ne serait même pas nécessaire de disposer de 51 % de la puissance totale de calcul du réseau : 30 % suffiraient. Cependant, vu la puissance totale de calcul du réseau bitcoin, il serait très difficile pour un mineur solitaire d'atteindre ce seuil de 30 % – ce qui serait en revanche possible pour un *pool* de mineurs. Ce dernier serait géré par un chef de *pool* qui construirait les blocs à miner, puis distribuerait ceux-ci entre les membres du *pool* pour effectuer l'opération de minage. Il aurait alors la possibilité d'exclure certaines

(16) J. O'DWYER (Karl) & MALONE (David), Bitcoin Mining and its Energy Footprint*, ISSC 2014 / CIICT 2014, https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf*
(17) http://digiconomist.net/bitcoin-energy-consumption
(18) The Fintech 2.0 Paper: rebooting financial services*, www.finextra.com/finextra-downloads/newsdocs/the fintech 2 0 paper.pdf*

transactions et d'inclure des doubles dépenses à l'insu des autres membres du *pool*.

Un moyen de défense contre ces attaques pourrait consister à modifier le protocole de la preuve de travail. Si le protocole nécessitait des capacités plus importantes en termes de puissance processeur ou de mémoire vive, cela rendrait plus chers les outils de calcul, alors qu'actuellement le prix des ASIC spécialisés est abordable.

Il peut y avoir par ailleurs des attaques malveillantes dont le but n'est pas de faire des profits financiers frauduleux, mais de perturber, voire de paralyser le réseau bitcoin en compromettant massivement les opérations de minage avec du déni de service. Une telle attaque nécessiterait de grands moyens (lesquels ne seraient probablement qu'à la portée d'un État).

Néanmoins, au fur et à mesure que la puissance totale de calcul du réseau bitcoin augmentera, les attaques seront de plus en plus difficiles à mettre en œuvre.

Défis juridiques, sociétaux et réglementaires

Le changement de comportement des utilisateurs

Dans le système bancaire classique, en cas d'erreur, d'oubli de mot de passe, de perte de chéquier ou de carte bleue, les porteurs ont un interlocuteur à qui s'adresser (l'établissement bancaire). L'utilisation des bitcoins demande à l'usager beaucoup plus de discipline : perdre une clé privée équivaut à perdre l'argent disponible sur les adresses engendrées à partir de cette clé privée, et il n'existe aucun moyen de le récupérer. Plusieurs porteurs ont connu de telles mésaventures à l'occasion d'un changement d'ordinateur ou de disque dur, car ils n'avaient pas pris soin de sauvegarder préalablement leurs clés privées [19].

L'utilisation des bitcoins demande donc un changement de comportement de la part des porteurs : il faut impérativement conserver les clés privées et les mots de passe, faire des copies sur plusieurs clés USB ou sur du papier, voire les graver sur du métal et les conserver dans plusieurs endroits sûrs.

La cybersécurité

Une clé privée peut également être volée, ce qui équivaut au vol de la somme totale d'argent disponible sur les adresses du portefeuille électronique générées avec ladite clé. Dans un monde où les cyberattaques sont de plus en plus fréquentes, il faut renforcer les mesures de cybersécurité habituelles : mettre à jour les logiciels et les antivirus, ne pas répondre aux messages électroniques douteux ou ne pas cliquer sur les fichiers attachés, éviter de naviguer sur des sites *Web* suspects, ne pas télécharger des fichiers provenant de sources non vérifiées.

Il est conseillé d'éviter les bourses de change ou les portefeuilles en ligne fournissant des services client *Web*, car ils n'offrent pas encore suffisamment de garanties de sécurité pour entreposer l'argent : il est préférable d'être « client complet » afin de disposer de l'ensemble de la *blockchain*. Il est aussi recommandé d'utiliser plusieurs portefeuilles, d'effectuer les transactions de faibles montants à partir d'un terminal mobile (client léger), moins sécurisé, d'effectuer celles de montants élevés à partir d'un ordinateur fixe (client complet). Le fait d'utiliser des transactions multi-signatures à partir de plusieurs clés privées réparties sur plusieurs supports différents (ordinateur de bureau, *smartphone*) augmente également la sécurité.

La vie privée

On entend souvent affirmer que le bitcoin est une monnaie anonyme, car on peut effectuer des transactions sans donner d'informations personnelles. Effectivement, les transactions contiennent les adresses des parties impliquées, qui sont générées à partir des clés publiques, lesquelles sont elles-mêmes générées à partir d'une clé privée. À partir d'une adresse, on peut connaître, *via* la *blockchain*, toutes les transactions dans lesquelles elle a été utilisée, mais on ne connaîtra pas l'identité de la personne. Cependant, si, par un malheureux concours de circonstances, l'identité de la personne liée à cette adresse était dévoilée, toutes les transactions qu'elle a effectuées en utilisant cette adresse seraient elles aussi dévoilées. Le bitcoin est donc une monnaie pseudo-anonyme.

C'est pourquoi il est conseillé d'utiliser plusieurs adresses, voire plusieurs portefeuilles, même si cela rend plus complexe la gestion personnelle des bitcoins.

La perception par le public

Le bitcoin a été l'objet dans le passé de plusieurs scandales, vols et escroqueries. Parmi les plus retentissants, on comptait (en février 2014) la faillite de la plateforme d'échanges de bitcoins MtGox, à la suite de la « disparition » de 774 000 bitcoins (409 M$) [20], ou (en août 2016) le vol de 120 000 bitcoins (72 M$) de la plateforme Bitfinex [21].

Le bitcoin reste perçu par une partie du public comme un réseau de blanchiment d'argent sale, ce qui affaiblit la confiance des utilisateurs.

Le changement sociétal

En général, les établissements financiers ont l'habitude d'« oublier » et de pardonner certaines erreurs aux clients, après un certain délai : ils donnent une deuxième chance aux clients ayant commis une faute dans un passé lointain. En revanche, un système fondé sur la *blockchain* « n'oublie jamais rien ».

L'absence de recours en justice

Dans le cadre des « contrats intelligents » (*blockchain* 2.0), les utilisateurs sont libres de décider des règles particulières à adopter, mais les transactions sont, quant à elles,

(19) Le Britannique James Howells a jeté à la poubelle le disque dur de son ordinateur avec un portefeuille électronique contenant 7 500 bitcoins : www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site
(20) www.theguardian.com/money/us-money-blog/2014/feb/25/bitcoin-mt-gox-scandal-reputation-crime
(21) http://fortune.com/2016/08/03/bitcoin-stolen-bitfinex-hack-hong-kong/

irrévocables. Une fois choisies, ces règles doivent être respectées scrupuleusement, aucune déviation n'étant permise. Cela est renforcé par la technologie elle-même, indépendamment de la volonté des parties.

La réalisation d'un « contrat intelligent » est d'une grande efficacité et sans risque puisque l'on ne peut pas le contourner. Mais son extrême rigidité est le revers de la médaille : quelle place laisse-t-on à l'humain ? Comment procéder pour rompre un contrat intelligent ?

La taxation des transactions

Dans une économie décentralisée de partage pair-à-pair du type Uber ou Airbnb, ou faisant appel à des plateformes comme OpenBazaar pour effectuer des paiements en bitcoins, il est pratiquement impossible, pour l'État, de taxer les transactions. Par quels moyens l'État pourrait-il le faire ?

Conclusion

La *blockchain* pourrait devenir la couche économique et financière du *Web*. Elle permettra d'effectuer de façon décentralisée des paiements, des échanges, des transferts d'actifs, d'émettre et d'exécuter des contrats intelligents. Son domaine d'application peut aller au-delà des seuls aspects économiques et financiers.

Comme pour toute nouvelle technologie, l'implémentation de la *blockchain* peut connaître des obstacles et des limites. C'est à la communauté de ses acteurs qu'il revient de trouver les moyens permettant de les dépasser.

Bibliographie

ANTONOPOULOS Andreas, *Mastering Bitcoin*, O'Reilly Media, 2015.

CROMAN Kyle & *al*., *On Scaling Decentralized Blockchains,* http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf

DECKER Christian & WATTENHOFER Roger, "Information Propagation in the Bitcoin Network", *13th IEEE International Conference on Peer-to-Peer Computing,* 2013, Trento University (Italy): www.tik.ee.ethz.ch/file/49318d3f56c-1d525aabf7fda78b23fc0/P2P2013_041.pdf

EYAl Ittay & *al*., *Bitcoin-NG: A Scalable Blockchain Protocol*, https://arxiv.org/pdf/1510.02037.pdf

HEILMAN Ethan & *al*., *TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub,* https://eprint.iacr.org/2016/575.pdf

NAKAMOTO Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*", https://bitcoin.org/bitcoin.pdf

J. O'DWYER Karl & MALONE David, *Bitcoin Mining and its Energy Footprint*, ISSC 2014 / CIICT 2014, https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf

POON Joseph & DRYJA Thaddeus, *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*, https://lightning.network/lightning-network-paper.pdf

The Fintech 2.0 Paper: rebooting financial services, www.finextra.com/finextra-downloads/newsdocs/the fintech 2 0 paper.pdf