IDRAC BUSINESS SCHOOL DEVENEZ REMARQUABLE !

DELL EMC

Rapport de recherche - 4ème Année

6 Juillet 2018

Management de la stratégie commerciale
IDRAC Business School - Montpellier

Discipline : Marketing Digital

Le Bitcoin, la révolution digitale de l'économie

Rédigé en LaTeX

Par : **David VELTEN**

Sous la direction de Geoffrey PELISSIER, Consultant & Formateur - Marketing Digital

ATTESTATION DE NON-PLAGIAT

Nom : Velten

Prénom : David

Date de naissance : 31/10/1995

Résidant : 179 Rue Robert Capa, Montpellier

X J'atteste sur l'honneur que le présent dossier a été écrit de ma main, que ce travail est personnel et que toutes les sources d'informations externes et les citations d'auteurs ont été mentionnées conformément aux usages en vigueur (Nom de l'auteur, nom de l'article, éditeur, lieu d'édition, année, page).

X Je certifie par ailleurs que je n'ai ni contrefait, ni falsifié, ni copié l'œuvre d'autrui afin de la faire passer pour mienne.

X J'ai été informé(e) des sanctions prévues au Guide de l'Étudiant/Apprenant en cas de plagiat.

Cette attestation doit être insérée en page 2 de votre dossier numérique.

Remerciements

Ce rapport est le résultat d'un travail et de recherche de près de 10 mois. En préambule, je tiens à adresser tous mes remerciements aux personnes avec lesquelles j'ai échangé et qui m'ont aidé pour la rédaction de ce rapport.

En commençant par remercier tout d'abord **Geoffrey PELISSIER**, mon tuteur, pour l'accompagnement et le temps qu'il m'a accordé durant la rédaction de ce rapport mais aussi de son aide et son expérience sur le thème choisi.

Je remercie également **Ignacio MURIO** et **Pierre GAYRAUD** ainsi que **Erwan COIGNARD** et **Miguel DE LA MATA** , mes managers et mes tuteurs au sein de Dell EMC, de m'avoir accueilli au sein de leur équipe, de m'avoir fait confiance et pour le temps qu'ils m'ont consacré et tous les précieux conseils et leur soutien.

Je retiendrai aussi leur bon esprit qui m'a permis de m'intégrer facilement à l'équipe. Par la même occasion je tiens à remercier toute l'équipe TSR Private de chez Dell.

Je remercie très chaleureusement **Boris BERGEROT**, **Pierre CABRIERE**, **Paul TRAMONTIN** et **Mehdi TOUALIT** pour l'aide qu'ils ont pu m'apporter et les ouvrages qu'ils ont pu me conseiller.

Merci à **Valérie MOHR** et **Olivier GRIZIAUX**, ma responsable pédagogique et mon responsable relation entreprise, qui m'ont suivi tout le long de l'année en s'assurant du bon fonctionnement de mon alternance et du déroulement de ce rapport.

Je tiens à remercier toute l'équipe pédagogique de l'IDRAC ainsi que le secrétariat.

Ce rapport a été rédigé en LaTeX, langage de programmation, utilisé pour la rédaction de document dans des domaines scientifique et technique. J'ai pu utiliser les moteurs de compilation PdfTeX et XeTex pour la création de mes documents PDF. Ainsi, je tiens à évoquer et faire une mention particulière au concepteur, récompensé du prix Turing en 2013, Leslie LAMPORT.

Enfin, je tiens à adresser mes plus sincères remerciements à toutes les personnes ayant pris le temps de lire ce mémoire.

Résumé

Le Bitcoin est devenu en quelques mois la une des actualités économiques et technologies. Véritable révolution dans le domaine des crypto-monnaies et très peu connu il y a quelques années alors qu'il a quand même 10 ans d'existence, qu'est-ce que le Bitcoin réellement, comment fonctionne-t-il ? Et quel rapport a-t-il avec les monnaies d'aujourd'hui et d'avant ?
Nous verrons ensemble les origines de la monnaies, du troc aux orfèvres jusqu'à nos banques d'aujourd'hui. Nous aborderons la vie cachée des Crypto-anarchistes et voir que leurs philosophie n'est pas si incohérente que ça en a l'air. Et enfin, le Bitcoin, ça peut paraitre plus complexe que ça en a l'air, mais il repose sur une technologie de stockage que l'on appelle la « Blockchain » qui va révolutionner l'ère de la data, nous parlerons également des « Hash » qui permettent d'assurer l'intégrité et la sécurité de la Blockchain et donc du Bitcoin. Nous évoquerons l'activité des « mineurs », les chasseurs de Bitcoin et nous terminerons en expliquant comment fonctionne les paiement avec le Bitcoin. Alors, suivez le guide !

The Bitcoin became in a matter of few months the hottest topic in the news. A true revolution in the cryptocurrency field but still very unknown few years ago, what is the Bitcoin really in the end ? How does it work ? How is it related to the real currencies ?
We will see together the origins of the currencies, from silversmiths bartering to our current banks. We will tackle the hidden life of the crypto anarchists and see how their philosophy is not as incoherent as it seems. Though the Bitcoin can look more complex than it is actually, it lies on a storage technology called the “Blockchain” which is revolutionizing the data era. We will also deal with the “Hash”, which allows to ensure the integrity and security of the Blockchain and consequentially the Bitcoin. We will raise the topic of the activity of “minors”, the Bitcoin hunters and then conclude by explaining the operation of paying with the Bitcoin. So, follow the guide !

Introduction

Cela fait quelque temps que l'on entend parler, dans les informations, sur les réseaux sociaux ou même dans nos discussions, de monnaie virtuelle, de crypto-monnaie ou encore plus précisément, du Bitcoin et du concept de la « Blockchain ».

Il y a quelques mois désormais, il ne se passait pas une semaine sans que le Bitcoin ne fasse les titres de l'actualité économique. Quand on en parle, on entend systématique les mêmes mots : la bulle, valeur nulle, danger, effondrement, … D'autres personnes vont même jusqu'à affirmer que c'est une fraude.
Au fil de l'actualité et quand vous avez commencé à vous y pencher, et, commme moi, vous n'avez rien compris.

Qu'est-ce qu'une crypto-monnaie, qu'est-ce que le Bitcoin, quel est son rapport avec la Blockchain ? Et qu'est-ce qu'une Blockchain d'ailleurs ? Peut-on réellement acheter des choses avec une monnaie « virtuelle », alors qu'on ne peut la toucher physiquement … Et pourquoi parle-t-on de « Bulle » ?

Alors, curieux, j'ai commencé à me renseigner sur le sujet. Au fur et à mesure que je me documentais, j'ai découvert un univers complexe, technique mais captivant, au-delà de l'aspect purement financier, le Bitcoin est basé sur une technologie révolutionnaire qui dépasse l'aspect économique et simplement pécuniaire.

Dans ce mémoire, nous allons découvrir les concepts du bitcoin, des crypto-monnaies et de la Blockchain. Concrètement, comment ça marche ? Qui est derrière cette technologie ?

Après avoir présenté une brève histoire de la monnaie, nous allons voir qui et que sont les crypto-anarchiste pour enfin expliquer comment est né le Bitcoin. Enfin, nous allons voir ce qui se cache derrière le concept de la Blockchain, et comment celle-ci fonctionne et fait fonctionner le Bitcoin.

Je vous propose de rentrer dans cet univers, aussi passionnant que mystérieux, celui du Bitcoin et de la Blockchain. Alors … Suivez le guide !

Table des matières

Première partie

Analyse Stratégique de l’entreprise

Chapitre 1

L’histoire de Dell

1984, au Texas, Michael Dell, encore étudiant en médecine, créé une entreprise « PC’s Limited » avec un capital de 1000 dollar US. Il assemblait lui-même les premiers ordinateurs pour l’entreprise, le premier était un « Dell TURBO » équipé d’un Microprocesseur Intel 8088 à 8 mégahertz. La philosophie de Michael Dell était de proposer des ordinateurs montés sur mesure afin de satisfaire le besoin du client, ce qui a rapidement démarqué la société et fait connaitre un réel succès. Suite à l’ampleur de PC’s Limited, Michael Dell arrête ses études à 19 ans pour se consacrer à son activité. En 1987, l’entreprise est rebaptisée « Dell Computer Corporation ».

Année 1992, la compagnie est classée dans les 500 premières entreprises américaines. Cinq années plus tard, alors que la société de Michael Dell n’est « que » 7ème constructeur mondial de PC, il décide d’encourager le succès du fournisseur Intel en proposant des PC plus puissants grâce à leurs processeurs « Pentium » et ainsi, s’attaquer au marché moins concurrentiel des petits et moyens serveurs. C’est en 2003 que « Dell Computer Corporation » adopte son nom de marque connu de tous à ce jour : « Dell, Inc »

La marque propose des solutions pour les entreprises comme des serveurs, des systèmes de sauvegarde mais aussi du stockage et du matériel spécifique relatif au réseau (« networking » : switch, routeur, câbles, firewall, etc). Afin de proposer des solutions complètes aux clients, Dell commercialise des solutions software partenaires externes comme Microsoft, VMware, Citrix ; hardware comme Intel, AMD et même physique comme Sonicwall.

C’est en 2011 que Dell affirme ses ambitions en rachetant Compellent Technologies, constructeur spécialisé de baies SAN / NAS. Mais c’est en 2016 que Michael Dell annonce un grand coup dans le milieu de la « tech » : le rachat d’EMC, le spécialiste mondial du stockage de données, pour 67 milliards de dollars avec un objectif en vue : « Nous allons être le fournisseur des infrastructures de la prochaine révolution industrielle. Nous disons à ceux qui construisent leur futur numérique et transforment leur informatique : venez chez nous » - Michael Dell. Suite à ce rachat, Dell devient alors « Dell Technologies » qui se compose de 7 leaders technologiques et qui n’ont qu’un

seul objectif : la transformation digitale de A à Z. Dell Technologies comprend alors : Dell, Dell EMC, Pivotal, RSA, Secureworks, Virtustream et vmware.

Chapitre 2

L'organisation de Dell

2.1 Les équipes et services

Comme toutes multinationales, Dell est divisé en multitude de services, eux même divisées en plusieurs équipes. Parmi les services on retrouve les services Marketing, Support, Ressources humaines, Commerciales, Informatique, Appel d'offres, etc.
Un service est lui-même segmenté selon la stratégie de Dell. Par exemple le service commercial est divisé en plusieurs sous-services selon le statut du client, eux même divisé en sous-sous-service selon le potentiel du portefeuille client :

- Entreprise : GCCS (Grand compte)
- Private :
    - Large Commercial
        - Large Commercial Ile de France
        - Large Commercial Sud
        - Large Commercial Nord
    - Mid Market
        - Mid Market Ile de France
        - Mid Market Régions
    - Acquisition
- Public :
    - High Education
    - Healthcare
    - Collectivités Territoriales
- Channel : toutes les relations avec les partenaires Dell

Ceci n'est qu'un exemple du service commercial, et de la segmentation des services. Au sein même de chaque service il existe une multitude d'équipe et de métier différents. Suite à la fusion avec EMC, de nouveau métiers ont été créé, voici des exemples :

- **ISR** : Inside Sales Representative, c'est le commercial sédentaire.
- **ISM** : Inside Sales Manager
- **TSR** : Technical Sales Representative, ce sont les avant-ventes infrastructure. Chaque équipe commerciale a un ou deux TSR attribué.
- **TSM** : Technical Sales Manager

- **AE** : Account Executive, ce sont les commerciaux terrains des ISR, AE et ISR travaillent souvent en binomes.
- **CSE** : Ce sont l'équivalent des AE pour les TSR.
- **IDCSE** : Rattaché à EMC, ce sont les spécialiste stockage (Inside Data Center Sales Executive)

La liste des métiers et des équipes et longue. Au sein de Dell il y a également plusieurs personnes employées par les partenaires mais présent sur site afin d'assurer l'intermédiaire Dell/Partenaires. Ainsi, on retrouve des employé Microsoft, APC Schneider, VMware, Intel, Nutanix, etc

2.2 La gamme Dell

L'idée là n'est pas de lister toutes les gammes et produit de Dell mais de proposer un aperçu des champs d'actions. Dell Technologies est présent sur le marché des :

- PC, Workstation : XPS, Inspiron, Precision, …
- Ecran, périphérique, souris, clavier, …
- Stockage : Compellent, Isillon, Unity (pour le unified-storage)
- Serveurs : PowerEdge, chassis VRTX, …
- Appliances : Hyperconvergence (VxRail)
- Networking : Switch, routeurs, firewall, …
- Licences : Microsoft, Nutanix, VMware
- Kits : Disque dur, mémoire, cables, carte PCIe, carte réseaux, …

Sans en faire une liste détaillée, voici une liste résumant l'ensemble des produits Dell :

Chapitre 3

La stratégie de Dell

3.1 Environnement interne

Forces

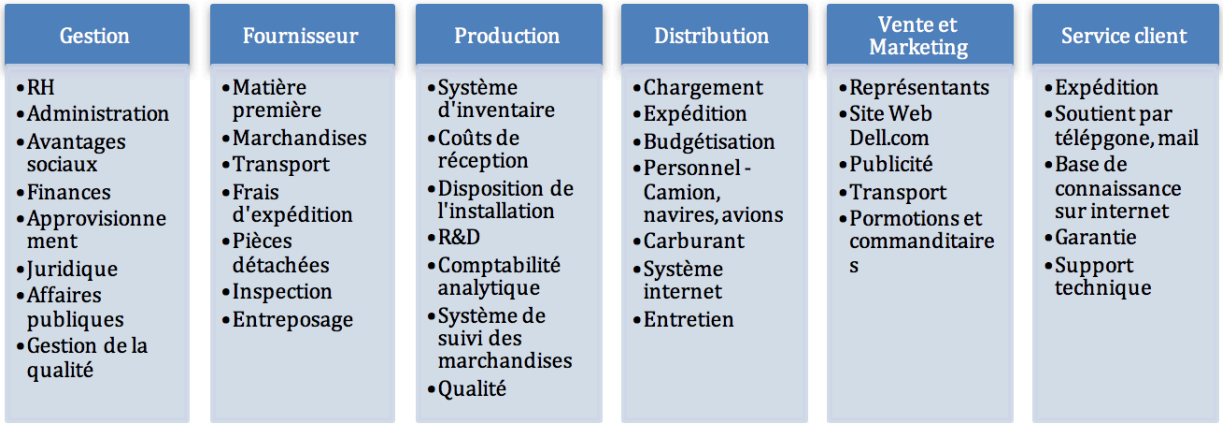
Dell est une marque connue, qui a fait sa réputation. Aujourd'hui Dell peut se reposer sur sa bonne image de marque. Son business model sur la vente directe la personnalisation de l'offre en fonction du client a su la démarquer du marché.
Dell a su s'appuyer sur de nombreux partenaires de renom comme Microsoft, Citrix, Vmware, Nutanix, APC Shneider, Aerohive, Mellanox, AMD, etc ….
Grâce à ses nombreux partenaires et implantations dans le monde entier, Dell propose des solutions pour les entreprises de A à Z sur leurs transformations digitale et infrastructure.
Avec un budget de 5 milliards par an dans la R et D, Dell est l'entreprise qui détient de plus de brevets.
Comme vu plus tôt, Dell possède une multitude de services, spécialistes, équipes, qui accompagnent le client.

Faiblesses

Ayant adopté une stratégie de vente directe, Dell ne propose un SAV uniquement téléphonique et en ligne pour les produits de vente au particulier.
Particulier comme professionnels, Dell ne possède pas de point de vente, tout doit passer par le site, par les partenaires (Atos, SC-DAM, Axians, etc), par téléphone, …
Le rachat d'EMC est une vision à long terme mais qui oblige Dell aujourd'hui à rembourser la dette.

Chaine de valeur

La chaine de valeur de Dell ressemble à la norme dans l'industrie, en revanche elle a su mettre en avant ses atouts. Delle fonctionne sur un cycle de conversion de trésorerie négative.



3.2 Environnement externe

Opportunités

Le rachat d'EMC a permis à Dell de se positionner comme un réel leader sur le marché du stockage, marché qui est en hausse. Le marché de la virtualisation et la mode du « Software Defined » prend beaucoup de place avec de nombreuse entreprises qui se mettent à l'hyperconvergence, Dell possède un point d'avance par rapport à la concurrence.
Dell sait se développer dans les pays émergent.
Le large domaine d'activité de Dell (sécurité, cloud, infrastructure, computer) permet de se positionner sur une multitude d'offres.

Menaces

Malgré la popularité de la marque, dans le section PC pour les particuliers, du fait de n'avoir aucun point de vente physique, HP, Lenovo, ASUS est en avance sur la vente d'ordinateur aux particuliers, ce qui rend la marque moins connue dans la culture populaire.
Une montée en puissance de Apple et MacOS peut faire craindre Dell sur leur vente de computeur.
Dell n'a pas conquis le monde du smartphone, là où ASUS, HUAWEI commencent à fortement attirer de client.

Analyse PEST

Politique

Le facteur politique représente un impact et une menace majeure auprès de DELL. L'utilisation d'Internet est de plus en plus contrôlée, notamment avec la « neutralité du net » qui n'est plus d'actualité aux Etats-Unis depuis cette année. Comme toutes les sociétés travaillant à l'international, les acteurs mondiaux doivent faire faces à de diverses pressions politiques.
Les activités mondiales de Dell sont régies par plusieurs environnements juridiques. Les règlements comprennent les lois sur l'environnement, l'emploi et la protection des consommateurs, les lois antitrust, l'exportation et l'importation, les règlements sur la sécurité des produits, la protection des investisseurs et les activités de réglementation des marchés financiers, pour n'en nommer que quelques-uns.

Economique

Au sein d'entreprises commerciales et internationales, le facteur économique est le plus important, en effet, il engage à la fois les vendeurs et les clients (acheteurs), le facteur économique d'un pays en particulier jouera en grand partie sur les ventes de Dell au sein de ce pays même.
Comme l'industrie électronique connaît une croissance rapide, elle est confrontée à un nombre croissant de demandes axées sur la réduction de l'impact environnemental de la conception, de la fabrication, de l'utilisation et de la gestion des produits en fin de vie. Preuve de politiques d'approvisionnement " vert ", le marché mondial exige de plus en plus d'informations environnementales sur les produits. Les ventes et le marketing de Dell ciblent les besoins changeants de leurs clients. Leur modèle commercial direct permet à Dell de communiquer directement avec ses clients, ce qui leur permet d'affiner leurs produits pour des groupes de clients spécifiques.

Sociologique

Les facteurs socioculturels ont une grande influence sur la demande pour les produits Dell. Il y a des différences dans la demande en fonction du niveau financier et éducatif d'un pays.
Le potentiel est élevé dans les marchés émergents. L'influence des PC, des ordinateurs portables, des tablettes et des smartphones sur la vie quotidienne des gens est essentielle et presque impossible à ignorer.
Les produits Dell s'adressent à toute la famille, étant fonctionnels pour le travail, l'école et le divertissement et personnalisables en fonction des besoins individuels.

Dell coopère avec l'Université du Texas à Austin, à la recherche d'étudiants universitaires avec des idées novatrices pour résoudre des problèmes sociaux ou environnementaux, avec un prix en espèces de plus de 100,00 dollars à l'intention de soulever des idées sur la façon d'améliorer les problèmes sociaux et environnementaux.
Les employés de Dell sont engagés dans leur communauté, qu'il s'agisse d'activités caritatives ou d'engagement politique, le personnel de Dell est impliqué dans les décisions qui affectent leur entreprise. Dans une lettre ouverte de Michael Dell pour présenter "The Dell 2020 Legacy of Good", il prévoit de donner 5 millions d'heures de bénévolat (Dell, 2013).

Technologique

Dell s'appuie sur sa technologie pour rester à la pointe des ventes ; elle doit constamment améliorer sa technologie, au même rythme ou à un rythme plus rapide que ses concurrents.
Parce que Dell est une entreprise qui se concentre beaucoup sur le fait d'être « vert », ils développent de nouvelles façons de le rester. Dell a obtenu le premier programme de recyclage gratuit de l'industrie à l'échelle mondiale.
Dell s'associe également avec « The conservation fund » et « carbonfund.org », des organisations à but non lucratif qui utiliseront les fonds pour planter des arbres dans des forêts gérées de manière durable, absorbant le dioxyde de carbone libéré dans l'atmosphère sous forme d'électricité produite. L'entreprise a déclaré que 100% des dons reçus par le programme " Planter un arbre pour moi " seront utilisés par les partenaires pour faciliter la plantation d'arbres.

Forces de PORTER

Produits de remplacement - MOYEN

Les téléphones commencent à remplacer un peu les ordinateurs dans certaines utilisations. En revanche sur la partie infrastructure, Dell EMC est à la pointe de la technologie avec toutes les nouveautés qui se font aujourd'hui. Hyperconvergence, « Software Define », Virtualisation, VDI, …

Acheteurs - ÉLEVÉ

Les clients préfèrent avoir des solutions sur mesure, pc custom, serveurs custom, etc. C'est pour ça aussi qu'ils ont choisis Dell.
La concurrence par les prix est forte sur le marché.
Les consommateurs recherchent un bon rapport qualité-prix et ont tendance à acheter

des produits moins chers, car les cycles de vie des ” gadgets ” sont de plus en plus courts.
Préférences élevées du client

Nouveaux concurrents potentiels - ÉLEVÉ

Comme il n’y a presque pas de fidélité à la marque, n’importe qui pourrait entrer sur le marché avec une marque convaincante. Sur le marché du PC, HP, Lenono, ASUS sont de réelles menaces. Sur le marché de l’infrastructure, Huawei, Cisco, HPE, Lenovo le sont également.

Fournisseurs - MOYEN

132 fournisseurs différents, AMD, Intel, Microsoft, Toshiba, Toshiba, Samsung, etc. En entretenant des relations étroites à long terme avec de multiples fournisseurs, Dell est en mesure d’obtenir des prix plus bas pour les pièces détachées.
Les monopoles de fournisseurs comme Intel rend incapable le remplacement du matériel (disque dur, disque dur, processeurs, RAM, etc.)
Certains produits sont monopolisés par Microsoft et Intel.
Coût élevé de changement de fournisseur

Rivalité entre les concurrents - ÉLEVÉ

Forte concurrence de HP, Lenovo, Asus, Apple, Huawei, Cisco.
Un grand nombre de concurrents actuellement sur le marché avec des ventes en baisse, la saturation du marché augmente. Il y a peu de place sur le marché pour la différenciation. Le prix est un facteur déterminant.
La rivalité concurrentielle est forte sur les principaux marchés de DELL. En tant que troisième plus grand fournisseur de PC au monde après HP et Lenovo (acquisition de l’activité PC d’IBM en 2005) et avant Acer, DELL fait face à une forte concurrence de la part de divers concurrents.

Marketing Mix

Les produits Dell consistent à offrir des avantages tangibles et intangibles aux exigences des clients. Pour se faire, Dell fournit une large gamme de produits, couvrant tous les domaines d’activité relatifs à la transformation digitale, adaptée aux besoins et aux demandes des clients individuels, petites, moyennes et grandes entreprises.
La stratégie des prix de Dell changent en fonction du cycle de vie du produit, bien que l’objectif principal soit de fournir le meilleur produit au meilleur prix.

Le client, en fonction des besoins, des demandes et de l'abordabilité, peut configurer le produit, qui est ensuite facturé en conséquence. Pour gagner continuellement des parts de marché, DELL réduit au maximum les prix des concurrents.

Conclusion

Dell a su rapidement devenir une entreprise leader sur le marché de son domaine d'activité. Leur modèle économique et leur philosophie leur ont permis de maintenir une longueur d'avance par rapport à la concurrence.
L'image de marque de Dell est toujours positive

Rapidement, DELL est rapidement devenue une entreprise incroyablement prospère dans ses premières années de croissance, passant d'une start-up à l'un des leaders du marché. Leur modèle d'affaires et leur philosophie, ainsi que leur système sophistiqué de gestion de la chaîne d'approvisionnement, leur ont permis pendant longtemps de maintenir leur avantage concurrentiel en fournissant des produits à bas prix tout en offrant une qualité élevée.
Cette image de marque est toujours vivante bien que l'entreprise ait eu des années difficiles au milieu des années 2000. La concurrence se renforce et les marges bénéficiaires diminuent. Tandis qu'Apple grandissait rapidement avec ses iPods, iPhones et iPads prisés, et les services associés, DELL manquait le point de sauter dans ce train et comptait toujours sur les ordinateurs de bureau, les ordinateurs portables et les serveurs.

De nos jours, nous cherchons en permanence des solutions pour satisfaire le client, mais aussi pour devenir novateur sur le marché. Peut-être que le paiement en crypto-monnaie serait un moyen d'élargir le périmètre client à l'avenir.

Deuxième partie

Revue de littérature

Chapitre 4

L’origine de la monnaie

Le Bitcoin … C’est une nouvelle monnaie. Peu connu encore dans le domaine financier, le bitcoin est une monnaie virtuelle, une monnaie que l’on ne peut pas saisir dans ses mains comme des vraies pièces de monnaie mais qui existe bel et bien dans l’ordinateur et qui pourtant, a de la valeur. Pour certains, c’est même le futur de la monnaie.
Avant de comprendre comment marche le Bitcoin, il est important d’introduire ce qu’est la monnaie, les euros, les dollars. Vous avez tous des pièces et des billets dans votre porte-monnaie. Mais savez-vous vraiment ce que ça signifie ? Pourquoi est-ce qu’on les a créés ? Et pourquoi ça a de la valeur ? C’est ce que l’on va découvrir dans ce chapitre.

Le Troc

Bien avant d’utiliser la monnaie, les échanges de biens et de produits étaient basés sur « le troc ». Par exemple, si l’on possède 2 chiens et qu’on veut les échanger à une personne qui possède un perroquet. On prend les 2 chiens et on les échanges contre le perroquet.

> Mais alors sur quoi étaient fondés ces échanges ? Comment déterminait-on la valeur des produits échangés ?

Les gens négociaient entre eux, et se mettaient d’accord, partant de la maxime : « Tout ce qui est rare est cher ». Comme un perroquet est plus rare qu’un chien, alors les gens échangeaient plusieurs chiens afin d’obtenir un perroquet.
Sauf qu’avec ce système, on arrive vite à une contradiction. Imaginons que la personne souhaite un seul chien et qu’elle n’a qu’un seul perroquet … Elle ne va pas couper son perroquet en deux.
C’était bien le problème avec l’époque du troc !

Alors très vite, on a envisagé d’autres « éléments » qui étaient en fait les embrayons des monnaies.

Les monnaies primitives

Les premières traces de la monnaie se font voir assez tôt dans le temps, quelques centaine d'années avant J.C, on utilisait des objets comme des couteaux comme équivalent de monnaie. Puis vient l'époque Romaine où l'or a commencé à être utilisé et il est vite devenu l'outil de base pour s'échanger de l'argent. En effet, l'or est un métal rare, si l'on reprend la dernière maxime énoncée, il est donc devenu précieux et il a pris de la valeur. D'autres éléments ont aussi été utilisés comme monnaie d'échange. Pour l'anecdote, les légionnaires Romain été payé en Sel, c'est d'ailleurs de là que vient le mot « Salaire ».
Dans la Grèce antique, l'or n'était pas le seul métal utilisé, l'argent faisait parfois office de monnaie car il est lui aussi, un métal précieux. De nos jours le terme « argent » se rapporte autant à la monnaie que l'on utilise qu'au métal.
Il fallait savoir que l'or n'était pas toujours très pratique. Vu que l'or avait de la valeur, si on perdait l'or, on perdait l'argent.
C'est là qu'on a commencé à confier notre « or » à des personnes de « confiance » qui deviendront les prémices des banquiers.

Les orfèvres

L'orfèvre récupérait l'or, ou les pièces d'or et le plaçait dans un coffre-fort. En échange de l'or déposé dans le coffre, l'orfèvre rendait un « bon » à la personne qui indiquait la somme récupérée et ainsi, le bon valait cette somme. La personne repartait donc avec son bon qui correspondait à la somme déposée, et il pouvait revenir voir l'orfèvre récupérer ses pièces d'or. Les gens se sont servis alors de ces bons afin de payer des objets. Ces bons étaient les ancêtres des pièces de monnaies et des billets tels qu'on les connait aujourd'hui.
Dès lors, les orfèvres se sont rendu compte que les personnes ne venaient que rarement chez eux récupérer leur or étant donné que les gens se payaient avec les bons en circulation. Les gens n'allaient chez l'orfèvre que pour récupérer de l'argent.
Ils ont alors commencé à distribuer plus de bons qu'il n'y avait réellement d'offres dans leurs coffres.
Par exemple, on a une tonne d'or dans un coffre, un bon pour une tonne d'offre, et bien ils créés un deuxième bon pour une tonne d'or que l'on va donner à quelqu'un d'autre. En suivant cet exemple, ça voulait dire qu'il y avait 2 tonnes d'or sur papier en circulation alors qu'en réalité, dans le coffre, il n'y avait qu'une seule tonne d'or.

Cette pratique a permis de créer de la liquidité sur le marché. Donc les gens pouvaient continuer à s'échanger de l'argent même s'il n'y avait pas exactement l'équivalent en or

dans le coffre-fort. Les orfèvres ont commencé à devenir les « banquiers » actuels en prêtant de l'argent qu'ils n'avaient pas. C'est comme ça que fonctionne les banques aujourd'hui, elles ont distribué beaucoup plus de billets et de pièces qu'elles ne possèdent en réalité dans leurs réserves.

> Mais alors vous vous dites, « Ce n'est pas normal ..! », « Ca peut pas marcher … »

Et c'est vrai, en théorie, ça ne peut pas marcher, mais dans la pratique ça fonctionne **SI** tout le monde ne vient pas récupérer son argent en même temps. C'est ce qu'il se passe lorsque l'on parle de **« Bank-run »**, où toutes les personne d'un pays ses ruent vers les distributeurs pour récupérer leurs argent. Si tout le monde fait ça en même temps, il n'y aura pas assez d'argent pour tout le monde.

Faisons maintenant un rapide saut dans le temps :

- 1914, les monnaies nationales sont convertibles en or
- 1944, accords de « Bretton Woods » : seul le dollar est convertible en or.
- 1971, arrêt de la convertibilité de l'or. Désormais, un dollar n'est plus directement égal à une quantité d'or. Ce qui permet d'imprimer plus de billet qu'il n'y a véritablement d'or. C'est le fonctionnement de notre monnaie aujourd'hui. C'est le cas de notre monnaie aujourd'hui. Bien qu'elle ne soit plus convertible en or, elles le sont dans d'autres monnaies. On appelle ça des cours flottant. La valeur de la monnaie ne dépend plus de l'or.

Nos banques aujourd'hui

Faisons un lien entre les orfèvres et les banques d'aujourd'hui.
Lorsque vous voyez écrit 500€ sur votre compte en banque, vous pensez peut-être qu'il y a 500€ qui vous attendent dans le coffre-fort de la banque, et bien, réellement ce n'est pas ça. C'est 500€ correspondent à une somme que la banque vous doit. Une somme qu'elle a peut-être dans son coffre-fort, mais peut-être qu'elle ne l'a pas. Simplement, ces 500€ indiquent une dette que la banque a envers vous. Cela veut dire que l'argent représenté sur votre compte n'est qu'une ligne en base de données et ne correspond donc pas à un élément matériel précis. C'est simplement une reconnaissance de dette de la banque envers vous.

En résumé

Alors bien sûr il s'agit là d'un bref historique de l'histoire de la monnaie, mais ça permet de bien comprendre pourquoi le Bitcoin a été créé et qu'elle est son lien avec la monnaie actuelle.
Le système actuel fonctionne, on utilise des pièces de monnaie, bien qu'elles ne soient pas en or, les pièces et billets représentent une valeur.
Elles ont de la valeur car elle est distribuée par un état en qui nous avons confiance (la plupart du temps) qui a décidé que telle pièce valait telle valeur. On parle de monnaie fiduciaire.
Ce système est beaucoup débattu et ne fait pas l'unanimité. Beaucoup de personnes ne croient pas en ce système. Notamment car ils ne supportent pas savoir que les banques et l'état puisse « contrôler » notre argent. Avec le Bitcoin, nous entrons dans le monde des crypto-monnaies et des crypto-anarchistes.

Chapitre 5

Les crypto-anarchistes

Le bitcoin est originaire du mouvement des crypto-anarchiste. Avant de s'intéresser au fonctionnement du Bitcoin, je pense qu'il est intéressant de comprendre le raisonnement qui a amené à la création du bitcoin.

Les origines

Décomposons le mot, dans crypto-anarchiste il y a deux mots :

— **Crypto**, ou Cryptage se réfère au chiffrement et à la modification de certaines données pour ne pas être lues par d'autres.

— **Anarchiste**, en référence au mouvement anarchiste, des personnes qui souhaitent une société où il n'y a pas de régulations et ou lois particulières (pas d'école, pas d'états, pas de banques).

> Mais alors, dans la pratique, qui sont-ils réellement ?

Ce sont généralement les rois du chiffrement, ce sont des personnes qui ne veulent pas être espionnés. Quel que soit leurs sur un support numérique, elles vont faire en sorte de chiffrer toutes leurs données et donc de les rendre illisibles pour quiconque essaie de les espionner.
Elles n'ont pas forcément de choses à cacher, mais au contraire elles veulent tout cacher de leurs vies pour que personne ne puisse savoir ce qu'il s'y passe.
Alors, qu'est-ce qui les poussent à tout chiffrer ? Ils se méfient dans le cas où quelqu'un souhaite exploiter leurs données. Ils ne veulent pas que, plus tard, une personne, une société, un état, pourrait avoir accès à toutes leurs informations. Alors « dans le doute, chiffrons tout, comme ça, c'est sur ».
Plusieurs éléments historiques ont poussés les crypto-anarchiste à tout chiffrer.

Le dernier évènement récent, Edward SNOWDEN. Ancien consultant pour la NSA, il s'est rendu compte que la NSA espionnait beaucoup plus les américain et le monde entier que ce qui était dit et l'a fait savoir en diffusant l'information. Les gens ont pu se rendre compte de l'ampleur de la surveillance de masse. Ça a motivé beaucoup de personnes et notamment les crypto-anarchiste à rejoindre une philosophie où l'on préfère

tout chiffrer pour éviter que des super-sociétés soit au courant de tout ce qu'il s'y passe.

Autre évènement, plus parlant et pourtant pas si vieux que ça, depuis la seconde guerre mondiale, il existe un réel traumatisme en France qui fait qu'on a décidé d'interdire les bases de données globales. En effet, l'état possédait des centaines de données papier avec comme informations qui possédait quoi, qui habitait où, ou qui était de quelle religion, par exemple, qui était juif. Avec la montée du nazisme en France, les nazis ont pu mettre la main sur ces données et vous imaginez bien le problème que ça a été.

Ces évènements parmi tant d'autres ont poussé les crypto-anarchiste à chiffrer leurs données et à en diffuser le moins à l'extérieur.

Comment s'équipent-ils ?

Un crypto-anarchiste est avant tout une personne qui connait très bien le fonctionnement de l'ordinateur. Il s'y connait bien en développement et en programmation. De plus, ils utilisent des logiciels choisis avec soin :

- Il utilisera **UNIX**, système d'exploitation libre, le roi des OS. Notamment une distribution LINUX : Tails, qu'utilise également Edward Snowden. Cette distribution a pour particularité de chiffrer un maximum de données et de ne jamais rien retenir au sein de la mémoire de l'ordinateur.
- Il utilisera un **VPN**, un réseau privé virtuel qui lui permettra de chiffrer toutes les données qui circulent sur internet. C'est notamment ce qu'utilise les personnes qui téléchargent illégalement par utilisation de torrent.
- UNIX oblige, il utilisera des **logiciels libres**, comme Firefox. Etant donné qu'il peut fouiller dans le code source, il a beaucoup plus confiance. Il regardera dans le code qu'il n'y a pas de programme espion.
- Il naviguera sur des réseaux comme **TOR**, le réseau internet anonyme. Réseaux informatique superposé mondial qui a la particularité d'être décentralisé. En anonymisant les connexions du protocole TCP, il permet de ne pas être espionner. TOR a également développé un navigateur basé sur le code source de Firefox, Tor Browser afin de préserver l'anonymat des usagers qui veulent naviguer sur internet.
- Il installera des **plug-ins**, pour bloquer toutes sortes de publicités, bloquer des scripts, ou même chiffrer ses emails.
- Et pour finir, les crypto-anarchiste vont avoir tendances à utiliser des **crypto-monnaies**, comme le Bitcoin, qui est la première crypto-monnaie qui a réellement été créée. D'ailleurs sur le « Deep Web » et plus particulièrement dans le

« Dark Web », il n’est possible de payer qu’en crypto-monnaie afin de ne pas être tracé.

Pour résumé la philosophie et la motivation des crypto-anarchistes, ils ont horreur de toute ce qui est centralisé. Les immense data-center des multinationales, les banques, qui font l’intermédiaire entre nous et notre monnaie. Ils ont horreur de ça, et ils veulent s’en débarrasser. Dans cette optique-là, depuis quelques années, ils se penchent sur un moyen qui permettrait de créer une nouvelle monnaie. Ainsi, je vais vous parler de l’histoire de Satoshi NAKAMOTO...

Chapitre 6

Le Bitcoin

2008, un mystérieux Satoshi Nakamoto publie un WhitePaper de moins d'une dizaine de pages sur internet qui va révolutionner le monde des crypto-anarchistes.
Ce papier décrit une nouvelle monnaie, le Bitcoin. Document encore disponible sur internet et présent en annexe. C'est le document officiel sur le fonctionnement du Bitcoin.
Pour commencer, Satoshi Nakamoto est un pseudonyme, personne ne sait qui il est. Ce qui a suscité de nombreuses rumeurs, informations et démentis. Laissons de côté la paternité et Satoshi Nakamoto pour l'instant et intéressons-nous plutôt au fonctionnement même du Bitcoin.

La Blockchain

A l'intérieur du fonctionnement du Bitcoin, il y a beaucoup d'innovations et de nouveauté, et l'une d'entre elle, la Blockchain.

> Alors qu'est-ce que la Blockchain ?

En réalité, il s'agit d'un immense livre de compte. Dans ce livre de compte est répertorié qui donne combien à qui et à quel moment. Et bien le Bitcoin fonctionne de la même manière, c'est un immense livre de compte. Pas sous format papier mais sous forme d'un gros fichier informatique qui contient l'historique de toutes les transactions.
Grâce à cette technologie, on peut retrouver qui a donné un bitcoin à qui, à n'importe quel moment depuis sa création.

> Mais alors comment peut-on savoir de combien chacun dispose ?

Tout est écrit dans le livre. Si Toto donne 2€ à Tata, que Tata donne 1€ à Titi et que Titi donne 6€ à Toto, on sait combien d'argent possède Tata, Toto et Titi au fur et à mesure que l'on suit les opérations. Ainsi est fait le Bitcoin.
On regarde simplement la circulation de l'argent et on en déduit combien d'argent dispose chacun.
Alors vient un problème. Reprenons notre livre de compte au format papier, que se

passe-t-il quand il n'y a plus de place ? Et bien on en rajoute un au fur et à mesure qu'un livre est complet.
Dans l'univers du Bitcoin, on appelle ces livres des blocs. Un livre correspond à un bloc. Et comme ils s'enchainent pour respecter la chronologie, on a appelé ça la « Blockchain ». Chaque livre est la suite du livre précédent.
En plus de ça, chaque livre possède un résumé du livre précédent. Dans le langage Bitcoin, chaque « Bloc » possède un résumé du « Bloc » précédent au début du bloc suivant.
Ainsi, au début du livre B ou bloc B, nous aurons un résumé du livre A ou bloc A, pareil pour le livre C avec le livre B.
Les blocs s'enchainent ainsi avec ce système de résumé. Ce système permet d'assurer la continuité et l'intégrité du livre de compte qu'est le Bitcoin.
Ce système-là, c'est le concept même de la Blockchain, c'est l'innovation majeure derrière le Bitcoin, mais ça n'est pas la seule.
Alors avec ce système de résumé et de bloc, comment le bloc B peut-il contenir TOUT le contenu du bloc A ? En reprenant l'exemple de nos livres, comment faire tenir un livre entier au début d'un autre livre …

C'est là que le terme de « Hash » arrive dans le monde du Bitcoin.

Les Hash

Si vous avez programmé et êtes développeur et notamment utilisé le système de versionning de code Git et son réseau GitHub, vous avez certainement déjà entendu parler de « Hash ».
Un Hash est tout simplement une fonction mathématique. Comme toute fonction mathématique, on lui donne des données, elle exécute sa fonction et elle nous sort un résultat en sortie. Ainsi, on fait passer notre livre A à la fonction de hash et la fonction nous donne une longue suite de caractère alphanumérique qu'on appelle « le hash ».
Grâce aux fonctions de hash, on peut hacher un grand livre comme « Guerre et Paix » et le faire tenir sur une simple suite de caractère.

La famille de fonction de hachage utilisé par le Bitcoin est le SHA-2 (Secure Hash Algorithm version 2) et conçue par la NSA.

Alors quel est l'intérêt puisqu'il s'agit juste d'une suite de caractère et non d'un réel résumé ?
La taille du hash ne dépend pas de la taille du livre ou du bloc. Un livre de 50 pages

comme un livre de 1500 pages tiendra sur la même suite. Et c'est le concept de la fonction mathématique de hachage.

Cette suite de caractère, on ne peut pas retrouver le contenu du livre/bloc haché. En revanche, ça permet d'assurer l'intégrité de la donnée.
C'est à dire que si une tierce personne arrive avec un livre qu'il prétend être « Guerre et Paix » il suffit de le hacher et comparer les résultats avec l'original.
L'intérêt de cette fonction, c'est que si l'on change ne serait-ce qu'un accent dans le livre, alors le hash final n'a rien à voir et en conclure que le contenu a été modifié.

Et dans la blockchain ?

Et bien on souhaite s'assurer que personne ne peut modifier le contenu précédent. Par exemple si Toto se manifeste en disant que Tata ne lui a pas envoyé 6€ mais 1000€. Grâce au Hash, on s'assure que personne ne modifie le contenu d'origine. Car si je modifie cette valeur de Toto à Tata, alors le résumé du livre B va changer et par conséquent le résumé du livre C qui contient lui-même le contenu du livre B avec le résumé du livre A va lui aussi être modifié.
C'est comme ça que l'on assure l'intégralité des données, afin de s'assurer que même au livre 200, si quelqu'un modifie le livre numéro 4, alors l'ensemble des hash serait erroné et on serait au courant qu'une personne a essayé de tricher.
Historiquement, le premier bloc du Bitcoin a été créé par Satoshi Nakamoto au début de l'année. À ce jour, la Blockchain comprend des centaines de milliers de blocs et ça ne fait qu'augmenter.

Voyons maintenant un point essentiel au Bitcoin et si important aux yeux des crypto-anarchistes : où est stockée la Blockchain ?

Chapitre 7

Le stockage et le minage

Le stockage

Le concept du Bitcoin est de créer une monnaie non-centralisée, et Satoshi Nakamoto a pensé à tout. Alors, il a pensé que chaque ordinateur sur le réseau possédant un certain logiciel serait un nœud qui communiquerait l'intégralité de la Blockchain avec les autres ordinateurs sur le réseau mondial. Pour ça, ils utilisent un système que vous connaissez déjà, le système de P2P (« Peer to peer » ou « Pair à pair »), comme lorsque l'on s'envoie des torrents. Ce système permet de s'envoyer des fichiers de manière décentralisé.
Chaque ordinateur va alors récupérer une copie de l'intégralité de la Blockchain, son travail alors sera de vérifier que celle-ci est valide en testant les hashs un par un dans tous les blocs pour confirmer que jusqu'au premier bloc, aucun bloc n'a été modifié.
Il faut savoir que les ordinateurs du réseau vérifient constamment l'intégralité de la Blockchain, en continu, ils vérifient que les hash correspondent à ce qui a été indiqué dans le bloc précédent et donc que tous les blocs sont les mêmes que depuis le début. Que personne n'a essayé de tricher.

Venant-en maintenant à la création des blocs, comment sont créé les nouveaux blocs ?
Un nouveau concept du Bitcoin dont on va parler est « le minage ».

Le minage

C'est là que l'on va parler de « Proof of work » ou « preuve de travail ». La validation par preuve de travail est une mesure de sécurité permettant d'éviter sur un réseau des attaques par déni de services. Il est très couteux en temps et en énergie. Souvenez-vous de tous les ordinateurs reliés entre eux, formant un nœud et qui se partagent l'ensemble de la Blockchain. Et bien ces ordinateurs vont faire quelque chose de plus, en plus de posséder la Blockchain, ils vont faire un très grand nombre de calculs, pour tenter de résoudre un problème mathématique. Ainsi, le premier mineur qui parvient à résoudre ce problème va ainsi gagner le droit d'écriture sur le réseau et créer le prochain bloc de la Blockchain. Si un mineur tente de déposer un bloc à la Blockchain sans

présenter sa preuve de travail sera rejeté.
Le système de PoW utilisé dans le monde du Bitcoin est le « Hashcash », conçu par Adam Back. Le problème mathématique, défini par le système Hashcash, est de trouver « le nombre qui, hashé, donne un nombre commençant par une longue série de 0 ».

Les principales tâches du mineur sont donc les suivantes :

— Ecouter les transactions du réseaux (et nouveaux blocs)
— Maintenir une liste à jour des blocs
— Tenter de construire le prochain bloc valide acceptable par l'ensemble du réseau en respectant le protocole.

Il est important de noter que les mineurs ne travaillent pas sur exactement les mêmes blocs, ce qui rajoute une compétition entre les mineurs. La preuve de travail à effectuer est de trouver le chiffre dit « nonce » qui vérifie la propriété suivante :
Hash (nonce || prev_hash || transactions du bloc) < difficulty target Le hash du nonce concaténé avec la valeur du hash précédent concaténé avec l'ensemble des transactions du bloc doit être inférieur à un chiffre que l'on appelle « difficulty target ». L'épreuve consiste donc, pour une chaîne alphanumérique donnée, à y ajouter une chaîne alphanumérique aléatoire jusqu'à ce que le hash de l'ensemble soit inférieur à un seuil donné.
Prenons un exemple. « Pour trouver une preuve de travail sur la chaine de caractères « Hello world ! » on pourrait calculer des hashs successifs avec la fonction de hachage sha256 en ajoutant à chaque fois un nombre supérieur jusqu'à obtenir un hash qui commence par 000. Il s'agit d'un travail de puissance brute, car il n'y a aucun moyen mathématique de déduire quel nombre pourrait permettre d'obtenir un tel résultat. » (Source : https ://bitcoin.fr/preuve-de-travail-proof-of-work/)

« Hello world ! 0: 3f6fc92516327a1cc4d3dca5ab2b27aeedf2d459a77fa06fd3c6b19fb609106a
Hello world ! 1 : b5690c48c2d0a09481186aaa99e4e090901ff2ac4d572e6706dfd30eefc22a27
Hello world ! 2 : 5b6fd9c27fcb54ca23404d9428f081b7c9280ba6370e33a6a20b16f40ce76320
Hello world ! 3 : 9c5d769416aa0ca894abf22bd17bd30fbb6959291423ae1903a9f86a1fe7ce78
Hello world ! 4 : 4efc65df7933e4f5cc21947c61d5cc6bd11d644794bfa210603b0547c4b1cc3e
Hello world ! 5 : 441b15b67d791620cd50ea537144e3115422e33bdb1b1b9b110d3265f7a9199b
Hello world ! 6 : d368331386f0cf773ad53910fefcef4bdceeb526e408d3fbc9408d6f6e481ca4
Hello world ! 7 : 013cc9722f38d2eb6186b75e2e7cbe6e7818e0612a2774d4400416b17ae03b87
Hello world ! 8 : 3a92631799b478c3bcc554df8401b09900fbdb58cc0e58efe711cc475ee097b3
Hello world ! 9 : 66658881696164fcb04f32ec505bb5e515000a85baf691beb63fc9d3f4d0fee2
....
Hello world ! 88 : 80d009db72c6ad35241bb3dbac77cbe177c6a803fe67527c159dbfaf2cbf9f5c
Hello world ! 89 : a5b1e789f691f9793f8a84f8ebae3d8e28d49cbe0eeea2da621cd409e3bdee2b
Hello world ! 90 : 4eba5b2459caac3d9ff3b787aaa5cac481aaa4a0232fbbe02a8ee4d1101c2ca2
Hello world ! 91 : c811722c68b53614d58d37dcad9d540c2bce9f85b5ccae94424ff4716eea1765
Hello world ! 92 : e30c716fccda22f394a8e80a2670b97968b5416b8b39e2061a7b7d1a9f41e0a9
Hello world ! 93 : 965425c39d4e24c532721d7f7b77a00b31b0c0d0e316d46240c4e6bec9c09f65
Hello world ! 94 : 7090a0e5d88cff635e42ea33fcd6091a058e9cdd58ab8cd5c21c1c70421e35c6
Hello world ! 95 : b74f3b2cf1061895f880a99d1d0249a8cedf223d3ed061150548aa6212c88d43
Hello world ! 96 : 447ca2fa886965af084808d22116edde4383cbaa16fd1fbcf3db61421b9990b9
Hello world ! 97 : **000**ba61ca46d1d317684925a0ef070e30193ff5fa6124aff76f513d96f49349d »

Le travail a été trouvé après 98 calculs.

> Alors pourquoi les mineurs font ça ?

Pour prouver qu'ils travailler et également rester allumé. Et c'est le mécanisme de base qui permet d'assurer l'intégrité du réseau. En faisant ça, on fait travailler les ordinateurs sur la planète et on s'assure qu'ils sont tout le temps connectés et donc qu'ils possèdent la Blockchain et on les récompenses pour leur travail en leurs offrant des bitcoin par consensus si quelqu'un trouve une solution à ce problème.
Une fois qu'un mineur a trouvé la solution au problème, il pourra le soumettre et tout le monde va pouvoir vérifier que c'est bien le cas. Les gens du réseau vont ainsi pouvoir dire que c'est bien cette personne Toto située à Montpellier qui a trouvé le résultat et on l'accrédite ainsi de par exemple 12.5 BTC et on continue à essayer de chercher une solution au problème pour pouvoir créer le prochain bloc.

Soyons clair, les mineur et leurs ordinateurs essayent de trouver une solution à un problème théorique. En réalité, ça ne sert à rien dans l'absolu, on la jette et on passe à la suite, mais cela permet de faire travailler les ordinateurs pour prouver qu'ils sont allumés et qu'ils testent constamment l'intégrité de la Blockchain.

Une fois que la personne a trouvé une solution au problème, on considère que c'est elle qui crée le bloc suivant, on l'accrédite d'un certain nombre de Bitcoin (définie dans le code bitcoin) et on passe à la recherche du bloc suivant.

> Mais alors, peut-on devenir riche en laissant tourner mon ordinateur ?

Et bien en théorie …. Oui ! Mais dans la pratique, les mineurs sont des personnes bien plus équipées que vous et moi avec des ordinateurs bien plus puissants que nos simples PC et Mac. Il existe même des fermes de minage et on les trouve souvent dans les pays du nord où l'électricité y est moins cher.

Terminons par le plus gros défi du Bitcoin, la « double dépense ».

Chapitre 8

La double dépense

En fait c'est un problème qui existe aussi dans notre système bancaire actuel. Le fait de faire croire que l'on possède plus d'argent que l'on en a en réalité.
Par exemple, si je dis « Voici 50€ pour acheter un jeu » et en même temps je dis à quelqu'un d'autre « Voici 50€ pour acheter un aspirateur » et bien à ce moment, les deux commerçants vont consulter la banque et la banque va leur dire que je ne possède pas plus de 50€ et qu'il faut faire un choix, soit le jeu, soit aspirateur. La banque sert donc « d'intermédiaire de confiance » pour veiller à ce que que la même quantité d'argent ne soit dépensée deux fois.

Dans le cas du Bitcoin, on a le même problème, à l'exception qu'il n'y a pas de banque, donc personne pour vérifier ce problème. Heureusement, Satoshi Nakamoto a pensé à tout et a trouvé une solution pour ça. Dans la pratique, vous pouvez tout à fait dépenser deux fois la même quantité d'argent, si strictement et exactement en même temps si vous dites par exemple « avec 1BTC j'achète ça, et en même temps je donne 1BTC à Toto ». Ça sera écrit dans le livre de compte. Seulement à un moment donné, les choses ne vont pas fonctionner dans le livre de compte que les gens vont consulter et on verra que vous n'aviez pas l'argent laquelle des deux versions ont prend, généralement la première version. On dira que cette personne a dépensé des bitcoins dans le jeu mais pas dans l'aspirateur et elle va rejeter la dépense que vous avez essayé de faire.

Maintenant que l'on sait comment est stocké la Blockchain, intéressons-nous au fonctionnement des paiements. Comment ça se passe lorsque je veux payer quelqu'un en Bitcoin ?

Chapitre 9

Les paiements en Bitcoin

Comme évoqué plus haut, le Bitcoin n'est pas une monnaie physique, tout est écrit dans la Blockchain, mais alors, qu'écrit-on dans cette Blockchain ?

Rappelons-nous que nous somme dans l'univers de la Crypto, donc on n'écrit pas nos noms, fini les Toto et les Tata. On écrit des suites de caractères qui nous correspondent. C'est pour ça que l'on ne parle pas de chaine anonyme quand on évoque la Blockchain mais qu'on la qualifie de « pseudonyme ».
Alors, qu'est-ce qui empêche n'importe qui d'aller modifier cette Blockchain puisque toute le monde peut posséder cette Blockchain ? Alors c'est vrai que pour les blocs du passé le problème ne se pose pas car grâce au système de hash, on s'assure que personne n'a changé l'historique. Mais que se passe-t-il pour le dernier bloc ? En effet, je pourrai dire au mineur qui vient de créer le bloc « Et bien, Toto m'a donné 450BTC ».
Heureusement notre ami Satoshi y a pensé, il a fait en sorte que l'on ne puisse pas dire que quelqu'un nous envoie de l'argent à sa place.

Concrètement, qu'essai-t-on de faire ? On essaie d'éviter que je puisse dire « Toto m'a donné 450BTC », grossièrement, que je me fasse passer pour Alice et que je dise « j'ai donné 450BTC ».

Le chiffrement asymétrique

Le Bitcoin utilise un concept de cryptage, de chiffrement, que l'on appelle le chiffrement asymétrique. Concept déjà utilisé depuis des dizaines d'années sur internet et qui correspond au fameux « s » sur les sites en https ://. C'est un composant de base utilisé un peu partout sur internet.
Dans ce concept, chaque personne possède une paire de clé différente. Une clé privée et une clé publique.
Ainsi, pour pouvoir signer une transaction et dire que c'est bien Toto qui m'a donné 450BTC, Toto utilise sa clé privée qu'il ne communique à personne pour chiffrer l'information et pour pouvoir dire « et bien j'ai donné 450BTC ». Personne n'a accès à sa clé

privée, par contre tout le monde a accès à sa clé publique. Et c'est grâce uniquement à cette clé publique qu'on peut bien vérifier que c'est bien Toto qui a chiffré l'information et donc que c'est bien lui qui a donné les 450BTC.
Voilà comment ça marche : chacun possède une paire de clé privé / publique et tout le monde peut vérifier que c'est bien cette personne grâce à ce système de doubles clés.

Dans le cas du Bitcoin, Toto utilise sa clé privée pour chiffrer l'information et dire j'ai donnée 450BTC et le reste du réseau connait la clé publique et peut l'utiliser pour déchiffrer l'information. Donc évidemment il y a un sens et il faut que la clé privée reste bien protégée par Toto. Parce que si jamais un pirate mettait la main sur la clé privée et bien là il pourrait se faire passer par Toto et dire « J'ai donnée 600BTC » et là, il y aurait un problème.

Alors, comment sont générés les adresses où chacun peut se payer dans le monde du Bitcoin ?

La graine

Il s'agit en fait d'un dérivé de la clé publique. La clé publique étant envoyé à tout le monde, elle est et devient le moyen pour tout le monde de se faire payer. Une fois qu'on connait la clé publique d'une personne, on peut dire « ok, j'envoie de l'argent à Tutu » et tout le monde sait que c'est bien Tutu qui récupère l'argent.

Chaque personne ne possède pas une paire de clé mais …. plusieurs. Pourquoi fait-on ça ? Pour éviter que l'on puisse se faire pister. Si j'utilisais la même paire de clé tout le temps, on pourrait savoir combien d'argent je possède, on ne saurait pas que c'est moi « Toto », mais on saurait que quelqu'un avec telle adresse possède une certaine somme de Bitcoin, ce qui pourrait être dangereux parce que si quelqu'un arrive à savoir que je possède beaucoup d'argent, je pourrai avoir un souci à me faire ….

C'est donc pour ça que chaque personne génère une grande quantité de paires de clés et qu'elle est normalement censé utiliser chaque paire pour une seule transaction à la fois.
Ces paires de clés sont générés lors de la création d'un portefeuille électronique de Bitcoin.
On créé ce qu'on appelle une graine (seed en anglais), la graine va générer un arbre et chaque branches va générer une paire de clés. Pour générer cette graine, on va utiliser en général une série de mot de la langue française ou de la langue anglaise, qui,

combinées, vont permettre de générer une infinité de paires de clé dont on a besoin. Grâce à cette liste de mot, on peut donc retrouver les paires de clé publique et privée et donc c'est ce qui représente notre portefeuille électronique de Bitcoin. Grâce à ça, on a accès à toutes les informations, tous les Bitcoin que l'on nous a envoyé.

Au final, il faut retenir une chose : La graine (cette série de mot qui permet de générer les clés privées et les clés publiques) est une chose à garder en sécurité. Quand vous allez créer votre portefeuille en Bitcoin, notez là sur une feuille de papier et surtout pas sur un logiciel dans votre ordinateur qui pourrait être piraté. Cette liste de mot permet de recréer toutes les clés privées et publiques et donc d'avoir accès à l'argent !

Chapitre 10

Conclusion

Ça y est, vous êtes incollables sur le Bitcoin, vous souhaitez en acquérir, devenir des crypto-anarchistes ?

En réalité et en lien avec l'actualité, c'est peu plus compliqué, il y a des rebondissements, des coups bas, les médias en parlent dans tous les sens, il grimpe, il chute … Il faut s'intéresser à l'actualité du Bitcoin pour se rendre compte que ça n'est pas si simple.

Les enjeux

Le premier, il correspond à son histoire, le Bitcoin n'a pas de parent. On dit qu'un certain Satoshi Nakamoto a créé le Bitcoin, mais personne ne connait véritablement son identité. Pourquoi c'est important ? Et bien parce que dans un premier temps, ne pas connaitre le propre fondateur de ce qu'on utilise, ça peut poser des problèmes pour le futur. On peut penser à une théorie du complot derrière, quelque chose nous est caché.
Ça, c'est un petit souci. L'autre soucis, c'est que cette personne, possède de très nombreux Bitcoin, vu qu'elle a créé le Bitcoin, elle a été propriétaire des premiers Bitcoin qui ont été émis. Et au cours actuel, elle possèderait plusieurs milliards de dollar en Bitcoin. Donc elle serait vraiment très riche. Mais, on ne connait toujours pas son identité. Voilà le premier enjeu.

Pourtant le principal enjeu du Bitcoin, n'est pas tant de savoir qui est le père du Bitcoin, mais du problème de la taille des blocs. Les blocs qui nous permettent de stocker le Bitcoin dans la Blockchain sont limités à la base à 1 Mégaoctet. Avec 1Mo, on ne peut pas stocker énormément d'informations par secondes. Et donc on est limité, et donc les transactions mettent de plus en plus de temps à être validés sur le réseau. Ce qui fait que quand je veux payer quelque chose en Bitcoin, il faut attendre parfois plusieurs dizaine de minutes avant que le réseau me confirme que j'ai bien pu faire le paiement.

— Ceux qui ne souhaitait pas modifier la taille des blocs qui ont accepté quand

même quelques concessions pour libérer un peu d'espace avec plusieurs manipulations, pour qu'on puisse faire un peu plus de transactions par secondes.
— Et ceux qui ont décidés de créer une nouvelle monnaie, le Bitcoin Cash, dans laquelle les blocs sont portés à plusieurs mégaoctets et qui permettent beaucoup plus de transactions par secondes.

Aujourd'hui il existe donc deux monnaies à base de Bitcoin.

Viabilité du Bitcoin

Un autre problème avec le bitcoin qui a récemment fait l'actualité, c'est qu'il est très volatile. Il suffit de regarder les graphes de l'évolution du bitcoin pour s'en rendre compte. Et par ce fait, rien ne garantit que le Bitcoin sera encore là demain. Les choses variant et avançant régulièrement, on peut tout à fait imaginer qu'une autre crypto-monnaie va prendre le dessus et que le Bitcoin ne vaudra plus rien.
Enfin, il faut savoir que le Bitcoin est peut être le « Père » des crypto-monnaies, mais que à sa suite de nombreuses autres monnaies électroniques ont été créés aujourd'hui c'est impressionnant. Il existe des centaines de monnaies alternatives qu'on appelle les « Altcoins ».

Les Altcoins

Le bitcoin n'est plus la seule monnaie électronique. C'est surement la première à être lancée. Mais aujourd'hui à sa suite, de nombreuses autres monnaies ont été créés, les « Altcoins ». Si même aujourd'hui, Bitcoin reste la principale crypto-monnaie, il faut considérer que c'est important de connaitre les autres crypto-monnaies qu'on peut trouver sur le marché.

La première qu'il faut connaitre : le Bitcoin cash, elle est dérivée du Bitcoin d'origine. Comme évoqué plus haut, dans le bitcoin classique on est limité à 1Mo par bloc, ce qui limite le nombre de transaction qu'on peut faire par secondes. Le bitcoin cash lui permet plus d'espaces dans chaque bloc. Du coup le Bitcoin classique et le Bitcoin cash partagent le même historique, ils ont la même Blockchain d'origine mais un jour, au milieu de l'été 2017 il y a eu une scission qui s'est faite, le bitcoin classique a continué dans sa voie, et le Bitcoin cash a été créé où on pouvait mettre plus de transactions par secondes.

L'Ethereum est probablement l'une crypto-monnaie qui connait une popularité forte derrière Bitcoin. Cette monnaie, que l'on appelle l'Ether permet aussi d'acheter et de

vendre des objets. Mais elle va beaucoup plus loin, elle intègre un concept que l'on appelle les « Smart Contracts ». Littéralement ce sont des contrats électroniques qui sont stockés sous forme de programme informatique dans la Blockchain d'Ethereum. Il faut s'imaginer que pour chaque transaction en Ethereum, on peut intégrer des programmes qu'on peut stocker dans le réseau et ces programmes indiquent des règles qui peuvent notamment dire « Sous telle condition, on va envoyer telle somme d'argent à Toto ». Et ça, c'est codé dans un programme informatique dans Ethereum. C'est réellement un changement très profond qui peut avoir à terme de grosses implications dans le fonctionnement même de la société puisqu'avec ça on pourrait potentiellement à terme se passer des contrats papier.

Il existe également d'autres monnaies alternatives qui vont un peu plus loin dans le concept de l'anonymat, par exemple, Zcash est une monnaie qui se veut véritablement anonyme avec beaucoup d'algorithmes et de programmes complexes … Mais on peut citer un concept qu'utilise le Zcash qui est le « Zéro Knowledge proof » qui dit que on peut prouver qu'une transaction a eu lieu sans forcément montrer la transaction.

Et puis il en existe encore une centaine et une centaine de monnaies alternative.

Le Bitcoin a aujourd'hui conquis le monde de l'informatique et de l'économie, ne cessant de faire l'actualité des médias ces derniers mois, il a provoqué une réelle révolution de l'utilisation des crypto-monnaies aujourd'hui. Serions-nous prêts à acheter une monnaie « virtuelle », que l'on ne peut pas toucher et tout reposer sur la confiance d'une personne sans savoir sa véritable identité ? Là est tout l'enjeux du Bitcoin. Alors … **Le Bitcoin, une révolution digitale de l'économie ?**

Bibliographie

— http ://presse-citron.net
— http ://openclassrooms.com
— http ://bitcoin.info
— http ://sudouest.com
— http ://bitcoin.org
— http ://altcoins.com
— http ://coinmarketcap.com
— https ://cryptoencyclopedie.com/Blockchain
— http ://larevolutionBlockchain.com
— https ://bitcoin.fr/preuve-de-travail-proof-of-work/
— https ://medium.com/JB_Pleynet/le-minage-expliqué-aux-non-initiés-b511b5a33117
— https ://fr.wikipedia.org/wiki/Bitcoin#Minage
— https ://fr.wikipedia.org/wiki/Preuve_de_travail
— Bitcoin : A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto

Troisième partie

Annexes

CERTIFICAT DE RÉUSSITE

David Velten

né(e) le 31/10/1995

a validé et obtenu le certificat :

Comprendre le Bitcoin et la Blockchain

Mathieu Nebra,
Co-fondateur d'OpenClassrooms

Certificat n° 1147942930 - Délivré le 5 janvier 2018

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

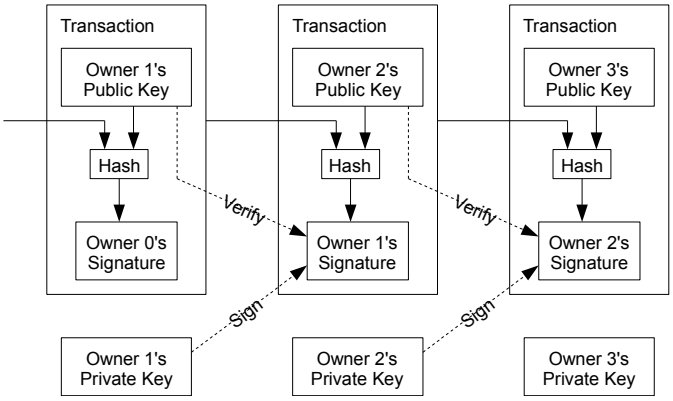
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

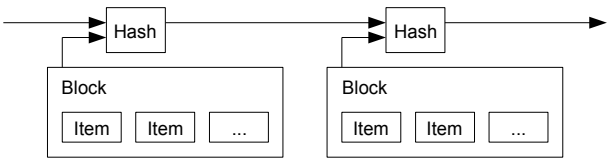


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

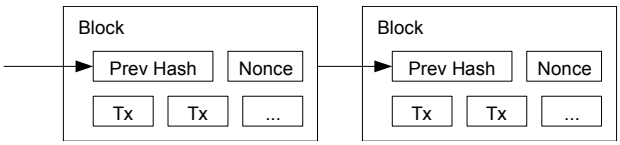
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

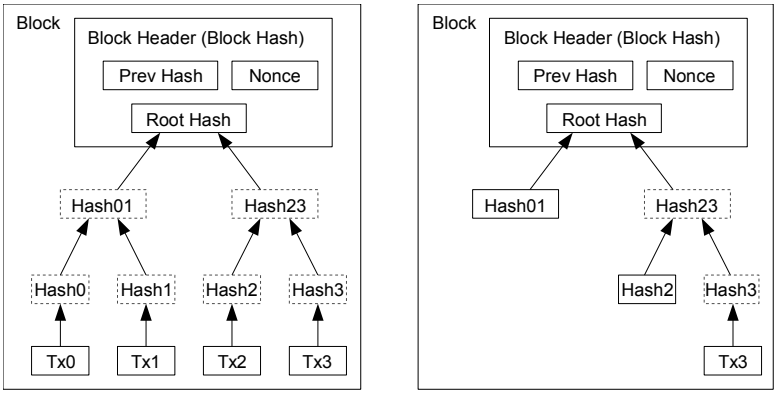
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



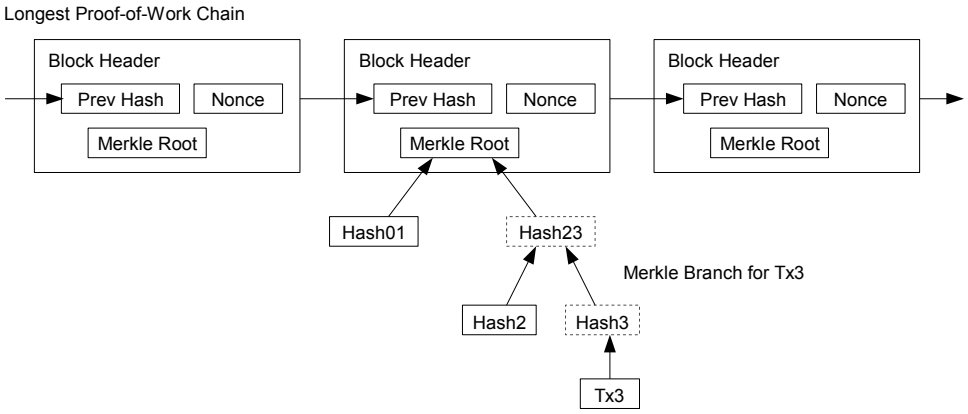
Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

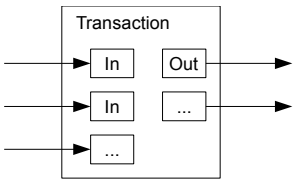
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

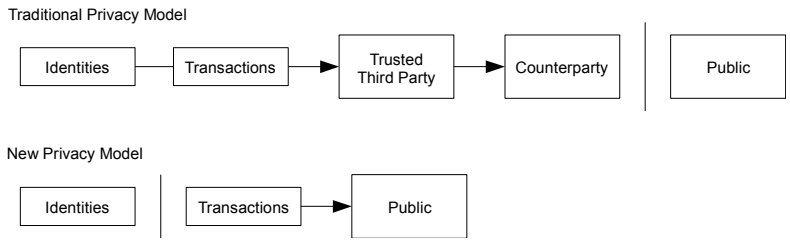
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.