



Méthodes Informatiques Appliquées à la Gestion de l'Entreprise

Mémoire Master 2 Classique

---

# Comment intégrer les blockchains dans les transactions bancaires ?

---

*Auteur :*

Sokhna Maimouna SOW

*Encadrant :*

Mme Marie-Pierre GERVAIS

Année scolaire  
2017 - 2018



# 1 Remerciements

MERCIIIIIII.

MERCIIIIIII.

# Table des matières

1	Remerciements . . . . .	2
2	Introduction . . . . .	4
3	Glossaire . . . . .	5
4	Fonctionnement de la blockchain . . . . .	6
	4.1 Historique . . . . .	6
	4.2 Architecture de la blockchain . . . . .	7
	4.3 Les types de blockchain . . . . .	9
5	Système des transactions bancaires . . . . .	11
	5.1 Les transactions par carte bancaire physique . . . . .	12
	5.2 Le monde du E-commerce . . . . .	12
	5.3 Les transactions sur papier . . . . .	13
	5.4 Les transferts d'argent . . . . .	14
	5.5 Prêts bancaires . . . . .	15
	5.6 Pré-autorisation . . . . .	15
	5.7 Vente à distance . . . . .	15
6	Blockchain dans les transactions . . . . .	16
7	Conclusion . . . . .	20
8	Webographie . . . . .	22
9	Annexes . . . . .	23

## 2 Introduction

Notre monde évolue au rythme des innovations et des nouvelles technologies. Aujourd'hui, nous sommes témoins d'une nouvelle révolution mondiale avec une portée assez difficile à mesurer mais mettant en avance des possibilités d'applications infinies. Cette révolution est marquée par le phénomène "**blockchain**". Elle est née du croisement d'une technologie cryptographique de pointe basée sur les registres distribués et d'un contexte sociologique opportun. Le cas de la blockchain est juste *phénoménale*. En effet la rapidité de son développement technologique coïncide avec un contexte sociologique favorable, ce qui augmente les chances de tirer profit des grandes innovations technologiques en les transformant en un vrai usage.

Derrière ce concept de blockchain se cachent les cryptomonnaies qui se démarquent des monnaies traditionnelles sur différents plans. Non seulement elles sont dématérialisées, anonymes, sécurisées mais ces devises peuvent s'échanger entre elles et permettent de faire des transactions bancaires. Et pendant ce temps, nous avons un système bancaire avec un réseau trop organisé, encadré et centralisé qui est bien construit et trop hiérarchisé avec des dirigeants qui contrôlent tout le système et ont toujours le dernier mot.

Face à cette situation, il me semble opportun de s'interroger sur la performance et l'avenir des banques. Puisque c'est assez difficile de contourner les banques, cela me pousse à chercher comment procéder à mettre en place en place les blockchains afin de faciliter le monde monétaire de demain? Comment intégrer les blockchains dans les transactions bancaires ? Quels sont les acteurs à impliquer ? Tellement de questions qui me motivent à faire à faire une étude approfondie et dans la mesure du possible trouver une solution pour faire cohabiter les banques et les blockchains.

A travers ces lignes je vais d'abord expliquer ce que c'est la blockchain en partant de sa création jusqu'à son processus final en détaillant son architecture et voir les différentes blockchains qui existent de nos jours. Ensuite j'étudierais l'impact des blockchains dans l'actualité économique sans oublier de mettre en évidence les faiblesses de cette nouvelle technologie et répondre aux questions posées précédemment..... QUOI RAJOUTER OU COMMENT REFORMULER

### 3 Glossaire

KEY	Value
Subprimes	Prêts immobiliers accordées aux américains ne remplissant pas les conditions pour un prêt classique
BTC	Symbole utilisé pour représenter l'unité de compte du bitcoin
Cyber-marchand	Commerçant proposant ses services via un site de e-commerce
FEVAD	Fédération du e-commerce et de la vente à distance
TPE	Terminal de paiement électronique
Coin	Terme utilisé pour désigner les monnaies bitcoin
GBP	Code qui signifie : livre sterling, la monnaie du Royaume-Uni
USD	United States dollar, code de la monnaie des États-Unis
EUR	Code qui désigne : Euro, la monnaie européenne
QR	Acronyme de Quick Response et qui est un code barre 2D
IBM	International Business Machines Corporation, est une société multinationale américaine
C2C	Consumer to Consumer, regroupe les activités entre consommateurs
P2P	Peer-to-Peer, modèle de réseau où chaque client est aussi un serveur
B2B	Business to Business, entreprise qui vise une clientèle d'entreprises
B2C	Business to Consumer, entreprise qui vise une clientèle de consommateurs

## 4 Fonctionnement de la blockchain

PHRASE OU PAS PHRASE

### 4.1 Historique

Tout a commencé par un groupe de 'geek' auto-organisé, sans hiérarchie et sans État qu'on appelle des **crypto-anarchistes**. Ces crypto-anarchistes savaient coder les données de façon à ce que personne d'autre que le destinataire ne puisse les déchiffrer. Ils se sont mis à "crypter des monnaies" d'où la naissance des **monnaies virtuelles** appelées aussi **cryptomonnaie**. Si ces cryptomonnaies remontent aux années 70, ce phénomène devient célèbre qu'en début de 2009 avec la création de la blockchain et du bitcoin.

En effet vers 2008, il y a eu une crise financière des subprimes. Les banques déclenchent alors la planche à billet afin de créer des euros et des dollars pour maintenir le système bancaire à flots. Et c'est vers cette même période précise qu'un certain **Satoshi Nakamoto**, un pseudo qui lui est attribué, publie un livre blanc de 10 pages, dans un forum de discussion, appelé ***Bitcoin - A Peer to Peer Electronic Cash System*** qui va révolutionner le monde monétaire. Par la suite, plusieurs personnes ont prétendu être Nakamoto mais nous n'avons jamais pu découvrir le vrai cerveau qui se cachait derrière avec une fortune estimée à **980.000 token** soit **5.473.465.943 euros**. Il est resté actif jusqu'à mi 2010 pour ensuite disparaître des radars. C'est ainsi qu'on assiste à la naissance de la première monnaie virtuelle décentralisée, qui fonctionne principalement avec la blockchain.

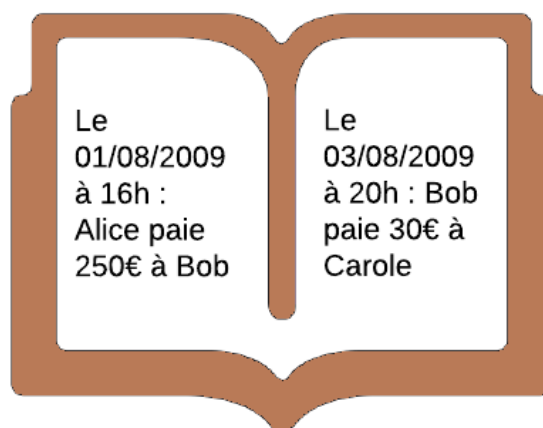
De ce fait la première blockchain est apparue avec la monnaie numérique bitcoin. Aussitôt le marché virtuel se met à utiliser la technologie de la blockchain et plusieurs activités ont tourné autour de cette technologie naissante. Des plateformes, des sites Internet et même des applications ont été mis en place pour la gestion des monnaies virtuelles et une utilisation permanente des blockchains.

## 4.2 Architecture de la blockchain

Qu'est que la blockchain? Certains diront que c'est juste une écriture comptables d'opérations numériques qui sont partagées entre de multiples parties prenantes. D'autres diront c'est un ensemble de réseau maillé d'ordinateurs reliés entre eux. Tellement de définitions lui sont attribuées. Mais quand est-il réellement de ce nouveau fléau? Comment est elle structurée? Quelles sont ses composantes? Essayons plutôt d'expliquer le mécanisme de la blockchain pour en sortir une définition adéquate.

Prenons un livre où nous allons écrire toutes les dépenses que chacun a réalisé avec les montants et les dates.

- Le 01/08/2009 à 16h : Alice paie 250 euros à Bob
- Le 03/08/2009 à 20h : Bob paie 30 euros à Carole
- Le 03/08/2009 à 22h : Alice paie 15 euros à Carole
- Le 04/08/2009 à 19h : Carole paie 20 euros à Clara
- etc.

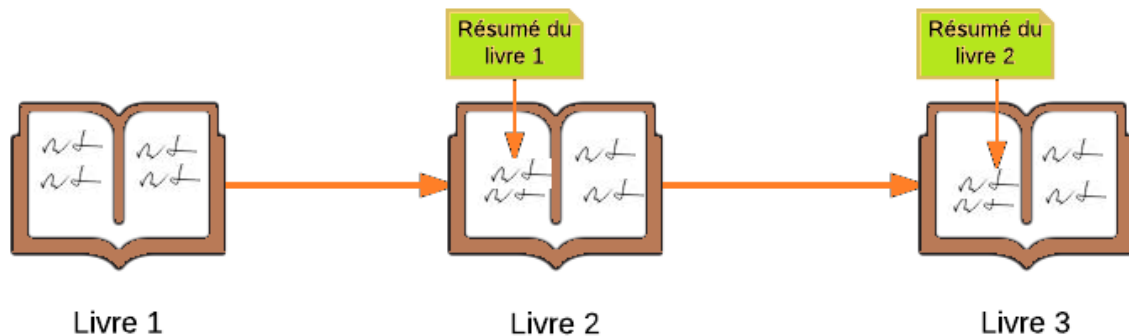


Livre de compte

Nous avons ici un grand livre qui dit qui a payé qui. Il n'est dit nulle part de combien d'argent vous disposez, mais nous le savons bien car nous avons toutes les échanges, leurs détails et le contenu du compte initial, donc il suffit juste de faire ses déductions. Par contre nous pouvons avoir des centaines d'échanges alors que le nombre de ligne d'un livre est limité. Comment faire dans ce genre de cas alors? C'est très simple il faut prendre un nouveau livre et continuer à remplir. Et



pour ne pas se perdre les livres sont numérotés. Chaque livre contient le résumé du précédent, ce qui permet de les relier entre eux et d'avoir une continuité. Nous obtenons ainsi un enchaînement de livres remplis de toutes les échanges.



### Enchaînement des livres

Et dans le monde de la cryptomonnaie, à la place de ces livres, nous avons des fichiers appelés **blocs**. Ces blocs sont construits les uns à la suite des autres, formant ainsi une **chaîne de blocs**. D'où le nom de **Blockchain**.

Mais comment est ce possible de résumer les informations du bloc précédent dans le bloc suivant? Ils utilisent ce qu'on appelle les **Hash** qui sont des fonctions mathématiques permettant de transformer n'importe quelles données en entrée en un grand nombre hexadécimal composé de lettres et de chiffres en sortie. Ces fonctions nous permettent non seulement de relier nos blocs mais aussi d'avoir la garantie que le contenu du bloc n'a pas été changé. En effet les fonctions de hachage ne marchent que dans un seul sens, ce qui assure la sécurité des blockchains. Si vous modifiez l'historique, cela ne correspondrait plus avec le hash du 1er bloc qui est dans le 2ème bloc et ainsi de suite.

Ainsi ce sont les transactions effectuées entre les utilisateurs du réseau qui sont regroupées en blocs. Chaque bloc sera validé par les noeuds du réseau, on les appelle les **mineurs**, en fonction des techniques qui dépendent du type de blockchain. Dans la blockchain du bitcoin, la cryptomonnaie la plus populaire, cette technique s'appelle le **Proof-of-Work**, ce qui signifie **preuve de travail**. Elle consiste en la résolution de problèmes algorithmiques. Et dès que le bloc est validé, il est horodaté et est ajouté à la chaîne de blocs, ce qui implique que la transaction est visible aussi bien pour le récepteur que pour l'ensemble du réseau.



### Les transactions dans une blockchain

Ce concept de **minage** fait qu'il n'existe pas de banque centrale qui produit ou gère les monnaies. En effet ce sont les ordinateurs appartenant au même réseau qui font tous le travail. Ce qui fait que tout est sécurisé par le procédé cryptographique. Et c'est la difficulté pour quiconque de résoudre les preuves de calcul qui assure la sécurité de toutes les transactions.

Ainsi je définirais plutôt la blockchain comme une technologie de transmission d'informations et de stockage. Elle a une base de données très sécurisée et dont la gestion est traitée par un ensemble de réseau d'ordinateurs connectés entre eux et qui stockent ces données de manière distribuée. Cette base contient toute l'historique de toutes les transactions entre les utilisateurs depuis sa création et est en même temps partagée sans intermédiaire. Ce qui donne la possibilité à chaque utilisateur de vérifier la validité de la chaîne.

## 4.3 Les types de blockchain

Nous avons différents types de blockchain en fonction des secteurs.

### 1. Blockchain publique

La blockchain publique est caractérisée par le fait que tous les noeuds du réseau d'échange sont contrôlés par le fameux réseau peer-peer. Pour y accéder, il y a aucune permission à demander et aucune barrière d'entrée. N'importe qui peut faire une transaction ce qui veut dire que tous les acteurs sont égaux dans leur participation du réseau. C'est le cas des monnaies virtuelles **bitcoin** et **ethereum** pour lesquels chacun a libre accès au registre et participe au même titre au processus d'approbation, celui qui permet de décider lequel des blocs doit être ajouté ou pas à la chaîne et qui définit l'état actuel du système.

## 2. Blockchain privée

la blockchain privée a son propre réseau privé dont l'accès est strictement confié au gérant qui, lui seul peut faire des modification dessus. Donc personne ne peut y accès sans y être autorisé. Cette blockchain est beaucoup utilisée par les banques grâce à sa gouvernance simplifiée, ses coûts réduits, sa rapidité, sa confidentialité surtout et du fait que les acteurs sont connus. Par contre cette blockchain perd tout son charme du moment qu'elle est privée. En effet comme l'a si bien dit **Juge David Teruzzi**, expert en bitcoin, je cite "Cette blockchain n'est pas très intéressante. Elle est certe scalable à l'infini, contrairement à la blockchain publique, mais son intérêt est limité puisqu'elle ne fait pas le lien entre différents acteurs".

## 3. Blockchain hybride

Nous avons aussi les blockchains hybrides. Vous avez les droits d'écritures et de modifications et certains noeuds peuvent êtres rendus publics et d'autres privés. C'est le cas du **consortium** qui est une blockchain regroupant plusieurs acteurs mais n'est ni publique ni ouverte à tout le monde. Les acteurs ont certains droits d'accès mais les décisions sur la blockchain sont prises par la majorité d'entre eux. Cette blockchain est plutôt adaptée aux contextes régulés et est utilisée à l'international comme IBM.

Tous ces types de blockchains, publiques, privées et consortium, pourraient finir par cohabiter. Chacune est spécialisée sur des applications adéquates. Et comme le dit **Luca Comparini**, un blockchain leader chez IBM France, je cite "La blockchain publique est idéale pour les marchés C2C et P2P, tandis que les blockchains privées et les consortiums sont davantage adaptés au B2B. Pour le B2C, cela dépendra des contraintes du secteur". Ce qui pousse aux mineurs de prévoir des passerelles entre les différentes blockchains afin d'assurer leur une possibilité de communication entre les systèmes.

## 5 Système des transactions bancaires

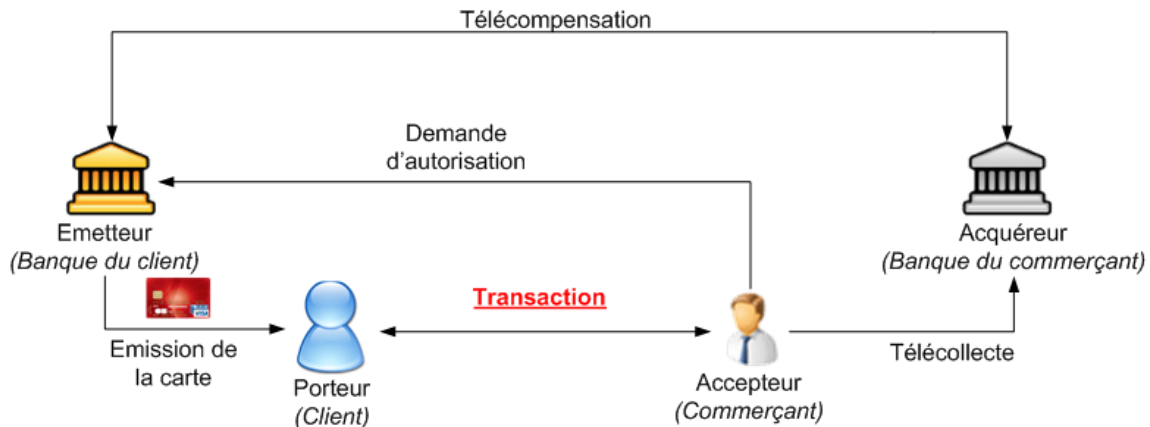
Avant la mise en place des premières cartes de paiement, la plupart de la population gardait leurs fonds sur eux ou à leur domicile. Ce qui veut dire que ces sommes pouvaient être dérobées et quand ça arrivait ils n'étaient pas remboursés. Donc faire des achats n'était pas sans risque pour l'intégrité de l'acteur et de ses économies. De plus il fallait avoir la totalité de la somme du montant au moment d'un achat pour effectuer l'opération, ce qui rendait les transactions un peu compliquées. Il était aussi facile de faire des erreurs de calculs dès que la monnaie était échangée et les transactions bancaires n'étaient pas répertoriées directement.

Pour faciliter les transactions bancaires, ils ont mis en place un système appelé la **monétique** qui regroupe l'ensemble des processus nécessaires à la création d'une carte, la lecture des informations associées et la gestion des transactions monétaires. Ces transactions monétaires ont toutes des processus différents et spécifiques. Nous allons prendre comme exemple le processus d'une transaction par carte bancaire qui est très courant. Il met en jeu plusieurs acteurs tels que :

- Un **émetteur**, qui peut être la banque du client
- Un **porteur** de carte, c'est à dire le client
- Un **accepteur** du moyen de paiement qui est très souvent le commerçant
- Un **acquéreur** de données de transaction dont la banque émettrice

Ces principaux acteurs communiquent indirectement mais de façon coordonnée et sécurisée. En effet:

- il y a d'abord le client qui crée son compte dans une banque. La banque lui envoie une carte associée au compte et qui lui permettra de faire tous les achats par la suite.
- Dès lors le client est libre de faire ses transactions chez un commerçant. Parfois il peut y avoir des demandes d'autorisation afin de vérifier la solvabilité du compte ainsi que la validité de la carte.
- Après la transaction le commerçant obtient un TPE qui va lire la carte et transmettre les données de la transaction. Cette étape est appelée la **télécollecte**.
- Une fois cette télécollecte effectuée, la banque du client et celle du commerçant communiquent entre elles afin d'effectuer ce qu'on appelle la **télécompensation** qui va permettre de débiter le compte du client et créditer celui du commerçant.



Processus d'une transaction bancaire

## TROUVER UNE PHRASE POUR INTRODUIRE LES TRANSACTION

Ce système monétique .....

### 5.1 Les transactions par carte bancaire physique

La carte bancaire est le moyen de paiement le plus utilisé en France. Elle représente presque **50%** des paiements en 2014 avec **9,49 milliards** de paiements effectués par cartes. Cette carte est d'une utilisation simple que ce soit pour un paiement ou pour un retrait et est acceptée presque par tous les commerçants. A CONTINUER.....

Cependant la carte nous impose un coût annuel assez élevé en fonction des banques ainsi que des frais sur certains retraits et paiements avec des assurances sur les achats effectués. De même il exige très souvent un montant minimum d'utilisation chez les commerçants. Ils ont mis en place des plafonnements de dépenses par mois ou par semaine en fonction des banques, ce qui est très embarrassant à cause du manque de flexibilité. Avec cette carte vous n'avez pas non plus la possibilité de faire des paiements entre particuliers.

### 5.2 Le monde du E-commerce

Le e-commerce est l'ensemble des transactions commerciales s'opérant à distance via des interfaces électroniques et digitales. Aujourd'hui les achats et ventes se

passent le plus souvent par le biais du numérique au détriment des marchés physiques traditionnels. L'e-commerce prend de plus en plus d'ampleur. en effet, une étude de la Fevad montre un chiffre d'affaire qui s'élève à **72 milliards d'euro** en 2016 pour un total de plus de **200 000 sites marchands**. Nous avons environ **2000 euro par année** dépensé par un e-acheteur pour **28 transactions**. En 2016 l'e-commerce représentait **8%** du commerce de détail. Par contre ces e-commerçants investissent beaucoup sur des plate-formes qui jouent le rôle d'intermédiaire entre eux et les acheteurs. Ce qui les pousse parfois à augmenter le prix de leurs marchandises pour en tirer bénéfice.

### 5.3 Les transactions sur papier

Nous faisons différentes transactions basées principalement sur les documents telles que:

- **Billet à ordre**: C'est un écrit par lequel le client s'engage à payer une certaine somme avec une échéance déterminée à son fournisseur.
- **Chèque**: C'est un écrit par lequel une personne donne l'ordre de payer une certaine somme, prélevable immédiatement sur les fonds portés au crédit de son compte, à lui même ou à un tiers.
- **Lettre de change** : C'est un écrit par lequel un créancier d'origine donne à un débiteur l'ordre de payer avant l'échéance fixée, une certaine somme à une troisième personne appelée qui est le bénéficiaire.
- **Traite** : C'est un titre qu'on peut négocier et qui présente, au profit du porteur, une créance d'une certaine somme et sert à son paiement. Il doit suivre un formalisme très rigoureux pour sa validité et son efficacité. Contrairement au chèque, il n'est pas encaissable immédiatement et ils sont beaucoup plus utilisés que les billets à ordre.

Ces moyens de transaction bancaires sont quotidiennement utilisés en France, particulièrement les chèques, grâce à leur gratuité d'acquisition. Avec une transaction par "papier", vous avez la possibilité de garder une trace du paiement. De plus les paiements sont gratuits ainsi que leurs acquisitions. Cependant certains commerçants n'acceptent pas les chèques à partir de certains montants, par mesure de sécurité et à cause des nombreux chèques impayés. Effectivement vous n'avez aucune garantie que les chèques encaissés ne sont pas sans provisions. En plus de tout ça il y a beaucoup de fraudes sur les fraudes aujourd'hui

Nous pouvons mettre ici aussi en avant les smart contracts qui sont très puissants. Ils ne s'appliquent pas seulement dans le e-commerce. La même logique avec le même procédé décrit dans les e-commerces peut également s'appliquer sur les transactions par billet à ordre, sur les lettres de change ainsi que sur les traites.

REQ, permet à l'utilisateur d'effectuer des transactions de manière transparente, sécurisée et à moindre coût, via la blockchain. Leur livre blanc estime actuellement les frais de 0,05 à 0,5pcent par transaction, les frais diminuent à mesure que le volume du réseau augmente puisqu'une partie des frais perçus sont brûlés et partiellement utilisés pour financer le réseau.

## 5.5 Prêts bancaires

## 5.6 Pré-autorisation

## 5.7 Vente à distance

Au niveau de l'international, le processus de la transaction change. Les cartes de paiement acceptées sont de type EMV (Europay Mastercard Visa) ou AmericanExpress.

Ces cartes utilisent les réseaux bancaires internationaux pour effectuer les traitements monétaires. Par exemple, si un porteur achète un produit aux Etats Unis, le traitement s'effectuera en empruntant le réseau Automated Clearing House avant de rejoindre la plate forme nationale Français qui est le Groupement des Systèmes Interbancaires de Télécompensation.

A chaque achat effectué en dehors de l'euros, une opération de change est effectuée. Cette opération est facturée et un pourcentage de la transaction est reversé à la banque pour rembourser le coût de traitement.

Pour les transactions effectuées au sein de l'U.E., le projet SEPA va bientôt permettre d'améliorer l'organisation des systèmes de paiement européen. —————

Conclusion de 5 ————— De ce fait depuis toujours nous vivons avec cette monétique qui nous permet d'effectuer des transactions bancaires, des transferts de fonds... Cependant ce système commence à semer les doutes dans l'esprit des utilisateurs. Il coûte de plus en cher et présente des failles de sécurité surtout avec la présence des cyberattacks sur le marché. Pour résoudre et faire face à ces problèmes, nous pouvons chercher d'autres méthodes pour assurer ces transactions. Et aucune autre technologie ne me vient en tête à part les blockchains. C'est vrai que c'est une nouvelle technologie, mais a déjà montré ses prouesses et semble avoir un avenir assuré. Je vais donc essayer de voir comment mettre en place les blockchains dans le monde monétaire et voir le rôle qu'elle peut jouer dans les différentes transactions.



## 6 Blockchain dans les transactions

**CARTE BANCAIRE** Le système de la blockchain pourrait faire disparaître ces contraintes et nous offrir ainsi une meilleure gestion de nos transactions. Et quoi de plus beau que de pouvoir dépenser ses *coins* dans la boulangerie en bas de chez soi? Pourtant c'est bien possible en mettant en place des cartes bancaires en cryptomonnaie. Cette carte est relié à votre portefeuille, qui stocke "votre richesse". Et afin d'effectuer des transactions de manière décentralisée, le portefeuille doit en sorte être "multi-cryptos". C'est à dire donner accès à plusieurs devises virtuelles dans différentes chaînes de blocs, afin de ne pas imposer aux utilisateurs une unique monnaie.

Et comment faire pour retirer en espèce? Obtient-on des euros ou des cryptomonnaies une fois devant le distributeur de banque? Cela ne pose pas de problème majeur. La carte cryptomonnaie est avant tout une carte prépayée. Ce qui veut dire qu'elle peut être créditée qu'avec les devises actuelles comme EUR, USD ou GBP. Donc même si vous détenez des bitcoins cette monnaie sera convertit à la devise de votre choix au moment des retraits.

Cette carte permettra aussi de dépenser ses cryptomonnaies chez les commerçants qui, à priori, n'a pas à y voir un quelconque inconvénient. En effet pour lui c'est comme une carte bancaire normale puisqu'il recevra son argent en euro. Tout simplement parce que la conversion crypto en euro est instantanée. Comment ça marche? Lorsque vous effectuez un paiement chez le commerçant, une vente instantanée du même montant en crypto est donc initiée. La carte est ensuite chargée du montant en euro, sans laisser de trace et sans que le commerçant même sans aperçoive.

La carte sera transparente aussi pour tout ce qui est frais bancaire, donc pratiquement pas de frais du tout, même si une transaction en bitcoin coûte de plus en plus chère. Il faut afficher le continuellement les cours auxquelles les cryptomonnaies seront vendus en se basant sur sur plusieurs échanges afin de proposer le meilleur taux. Mais à vrai dire, un paiement sans frais n'existe pas, donc qui doit payer les frais? Sur ce point il n'y aura pas de changement car ce sera le marchand qui paie comme dans les transactions bancaires actuelles.

Cependant Le processus de mise en place des outils nécessaires pour le marchand du quartier afin d'accepter les cryptomonnaies est assez simple mais un peu

complexe . Un autre point bloquant, qu'il ne faut surtout pas oublier, est la sensibilisation des commerçants à accepter une monnaie dont le cours varie subitement d'une minute à l'autre.

—————-Brouillon—————- Recevoir un paiement avec Bitcoin est presque instantané. Toutefois, il y peut y avoir un délai de 10 minutes avant que le réseau ne commence à confirmer votre transaction en l'incluant dans un bloc et avant que vous ne puissiez dépenser les bitcoins que vous recevez.

Une confirmation signifie qu'il existe un consensus dans le réseau pour considérer que les bitcoins que vous avez reçus n'ont été envoyés à personne d'autre et sont désormais votre propriété. Une fois que votre transaction est incluse dans un bloc, elle continuera d'être enfouie sous chaque bloc après celui-ci, ce qui consolidera exponentiellement ce consensus et diminuera le risque d'une transaction renversée. Chaque utilisateur est libre de déterminer à quel moment il considère une transaction confirmée, et 6 confirmations est souvent considéré comme étant aussi sécurisé et irréversible qu'une attente de 6 mois pour une transaction par carte de crédit.

Evidemment on adaptera le délai de sécurité à l'importance de la transaction effectuée. Quelques minutes suffiront généralement pour un micro-paiement sans enjeu qui peut se contenter d'une —————-Fin—————-

### **E-commerce**

La blockchain serait un grand atout pour ces e-commerçants. En effet la mise en place de cette technologie dans ce secteur supprimerait tous les intermédiaires entre vendeurs et acheteurs. Les e-commerçants pourront proposer des transactions se passant d'intermédiaires, donc ne plus verser de commissions aux plate-formes, aux organismes bancaires. Prenons un exemple sur Shopify et Paypal, qui sont des sociétés de paiement en ligne très populaires de grandes plate-formes de commerce. Elles prennent une commission de 1,5% à 6%. Cette redevance est transmise au client, ce qui rend les achats en ligne beaucoup plus chers.

D'après **Thomas France**, co-fondateur de la Maison du Bitcoin à Paris, ce système pourrait faire économiser 3% à 4% des chiffres d'affaires des e-commerçants qui réalisent beaucoup d'opérations depuis de l'étranger. Effectivement, les transactions internationales sont souvent réalisées par l'intermédiaire des plate-formes tierces, les obligeant à déboursier beaucoup de frais. Alors que les paiements en bitcoins ne génèrent aucun frais de transactions pour le vendeur. Ceci est un grand avantage pour les e-commerçants en quête de rentabilité absolue.

L'inexistence des frais de transaction est assurée grâce au protocole de la

blockchain dont le code source a la caractéristique d'être un open source. De même avec son fonctionnement sur le réseau de pair à pair, il n'y a pas d'autorité centrale ou intermédiaire. Ce qui fait que tout le monde peut contrôler ou posséder les bitcoins. Donc, quand une transaction est réalisée entre deux parties la monnaie ne passe par aucun intermédiaire et est échangée, comme presque un échange liquide. Ce qui fait que rien ne justifie des frais de transactions. De même une fois le paiement effectué, il devient irréversible, donc l'e-commerçant est aussi protégé contre des frais d'annulation de paiement de la part de l'acheteur. Par contre pour tout mécontentement de l'acheteur le cyber-marchand peut toujours le rembourser contre le retour du produit acheté.

Nous avons aussi un élément clé qui peut vraiment révolutionner le e-commerce. On l'appelle les **contrats intelligents** plus connus sous le nom de **smart contracts**, en anglais qui peuvent être une grande force pour le e-commerce. Ces contrats sont la véritable application derrière la technologie blockchain. Nous entrerons pas en détails sur là-dessus car il faudra tout un article entier pour vous en parler. Mais je peux vous dire que ces contrats sont en résumé des accords numériques entre des parties qui s'exécutent automatiquement quand les obligations ont été respectées et remplies. Si un acheteur valide son panier il envoie le prix fixé d'un produit en cryptomonnaie au contrat. Une fois le contrat reçu, le vendeur envoie la preuve de propriété au smart contract et en même temps il va lier ce contrat au transporteur du produit vendu. Dès que toutes les obligations sont remplies, le contrat enverra automatiquement l'argent au porte-monnaie du vendeur qui pourra les récupérer et utiliser à tout moment. Ainsi ces contrats permettent de faire des transactions directes entre les acheteurs et les vendeurs sans frais et avec une simplicité remarquable.

### METTRE IMAGE SI JAI LE TEMPS

Par conséquence mettre en place le paiement par les crypto-monnaies n'est pas sans présenter certains risques pour les professionnels de la vente en ligne. En effet le système est très volatile. La monnaie est soumise à la loi de l'offre et de la demande, ce qui fait que le prix augmente quand la demande est forte et diminue lorsque la demande est faible. Donc son cours est très instable et évolue de manière imprévisible, en témoignent les fortes fluctuations de son prix ces derniers mois, à des périodes très rapprochées. Le montant perçu lors d'une vente peut varier entre le moment de l'achat et celui de la réception du paiement.

Les cryptomonnaies ont donc la capacité de fournir des solutions aussi bien pour le e-commerçant que pour l'acheteur en supprimant le besoin d'un tiers. Ces

monnaies peuvent également être meilleures que les services de portefeuille numérique de nos jours car la blockchain nous permet:

- De faire des transactions instantanées avec des frais peu élevés
  - A n'importe qui d'en bénéficier
  - De ne pas fournir ses informations personnelles et financièrement sensibles aux tiers.
-

## 7 Conclusion

La blockchain est devenue un sujet incontournable cette année. Grâce au réseau et à la cryptographie, elle a un système sécurisé qui pousse les particuliers et les entreprises à l'utiliser sans besoin de faire appel à des intermédiaires. Les seuls frais possibles à payer sont la maintenance et la sécurisation du réseau. Pour un acheteur et un vendeur, techniquement il y a aucun frais à dépenser puisque les plates-formes du e-commerce seront des applications blockchain. Ainsi les utilisateurs détermineront le développement et le fonctionnement de la plate-forme car les blockchains sont décentralisées, pas de partie centrale ou de société qui décide ou définit les règles.

---

Un défaut majeur dans la façon dont nous stockons actuellement les données est qu'elles sont stockées dans un endroit central et contrôlées par une partie centrale. Les données sont le nouveau pétrole et les cybercriminels sont désireux de voler ces énormes bases de données. La cybersécurité nécessite d'importants investissements en capital et des réglementations strictes, ce qui décourage les flux de revenus. Puisque les blockchains sont décentralisées, les données sont également décentralisées. Oui, les cybercriminels peuvent pirater des individus, mais ils ne voleront que les informations de l'individu qu'ils piratent. Il est pratiquement impossible de pirater une blockchain entier.

Le grand public est encore peu familiarisé avec cette monnaie alternative, dont le fonctionnement tranche résolument avec les devises monétaires habituelles. Sa démocratisation demeure encore hypothétique et il est difficile d'évaluer l'importance qu'elle pourrait prendre dans les années à venir.

La technologie blockchain actuelle présente un problème de scalabilité, analyse Frédéric Dalibard, responsable du digital de la banque de grande clientèle de Natixis, filiale du groupe BPCE. Imaginer un équivalent de Visa sur la blockchain est pour l'instant impossible." Le Bitcoin, par exemple, ne peut enregistrer qu'une dizaine de transactions par seconde, contre 20 000 pour Visa

Malgré le coût potentiel d'implémentation, la blockchain dispose tout de même d'avantages incontestables en termes de rapidité et de sécurité.

Aujourd'hui, les systèmes de paiement fonctionnent plutôt bien, renchérit de son

côté Grégory Chenue, du Crédit Agricole. Tout casser pour remplacer par des systèmes blockchain prendrait beaucoup de temps car on ne part pas de zéro, les infrastructures de réseau sont très complexes.”

Outre les barrières culturelles et d’expérience utilisateur déjà mentionnées plus haut, mais qui peuvent donc être levées en étant ingénieux, plusieurs limites techniques rendent cependant aujourd’hui la blockchain Bitcoin difficilement utilisable à grande échelle pour des paiements, rendant sa menace pour les banques a priori assez limitée à court terme. En particulier, seules 7 transactions par seconde maximum sont aujourd’hui possibles sur toute la blockchain Bitcoin, loin des milliers du réseau Visa. Ce chiffre est modifiable, mais avec l’accord de la communauté Bitcoin, au sein de laquelle les débats sur ces sujets sont vifs. Du fait de la gouvernance complexe du bitcoin, il faudra sans doute un peu de temps avant que ces restrictions ne soient assouplies – ou, plus probablement, avant que des méthodes de contournement apparaissent (pensons par exemple aux sidechains et au Lightning Network).

Le caractère décentralisé de cette nouvelle technologie, couplé avec sa sécurité et sa transparence, fait des prouesses aujourd’hui.

Depuis, de nombreuses institutions bancaires s’y intéressent et réalisent des transactions mais le débat reste entier : doit-on réguler ces monnaies virtuelles ? Comment contrôler la fluctuation de celles-ci ? Retour sur l’histoire des crypto-monnaies en 17 dates clés.

## 8 Webographie

## **9 Annexes**