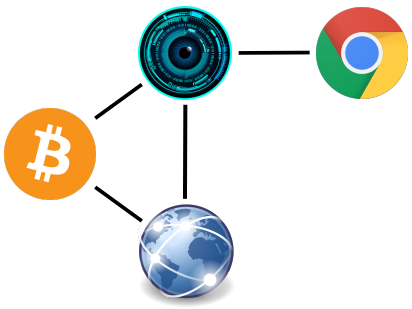


Olivier Ricou

Géopolitique de l'Internet

Version 3.0α du 25 juillet 2023

Table des matières

Chapitre 6

Payer en ligne

Qui dit commerce électronique dit paiement et de préférence un mode de paiement qui dépasse les frontières. Devenir le mode de paiement de référence peut être hautement lucratif aussi tous les acteurs financiers ont essayé à un moment de pousser leur solution sur Internet et de nombreuses startups sont nées [1]. Les vainqueurs sont pour l'instant PayPal et les crypto-monnaies.

On sait que l'argent, sous-jacent aux modes de paiements, est intrinsèquement source de pouvoir. Contrôler les transactions permet de prélever un pourcentage mais celui qui contrôle les moyens de transfert, les comptes bancaires, voire la monnaie peut en tirer d'autres avantages économiques et politiques nettement plus importants. Par exemple Paypal peut surveiller l'activité de ses usagers voire bloquer leur compte, vendre des données relative à ses clients, permettre de les contacter, faire des statistiques... Lors de la crise de 2008, les banques ont bien fait comprendre que si elles meurent, toute l'économie s'effondrerait. Avec tant de pouvoir, il semble naturel de confier cet outil de base de notre économie à l'État ou au moins que l'État puisse contrôler cette activité [2]. C'est le cas pour les monnaies nationales. Pour les institutions financières aussi mais partiellement, le contrôle étant limité par l'influence qu'ont les banques sur les politiques. Il existe aussi des monnaies et systèmes de paiement alternatifs et suivant les cas, l'attitude de l'État varie à leur égard. Ainsi les systèmes d'échange locaux (SEL) et les crypto-monnaies ont été interdits, tolérés ou encouragés suivant les lieux et époques.

Du point de vue purement financier, les revenus que peut générer un moyen de paiement ou une monnaie sont très importants. Les prélèvements sur les paiements avec les cartes de

1. qui se souvient de Mondex, eCash, e-gold ou S.E.T. ?
2. Depuis 2007 Paypal Europe est devenu une institution financière. Cela peut limiter les dérives spécifiques de PayPal mais les banques n'ont pas réellement cédé de pouvoir malgré la crise qu'elles ont générée.

paiement ont généré un revenu de 2,6 milliards pour les banques françaises en 2009 [3]. En 2012 Visa a dégagé un bénéfice de plus de 2 milliards de dollars et MasterCard un peu moins de 3 milliards. Alors bien sûr devenir le système de référence pour des milliards d'internautes fait rêver.

Mais le chemin est difficile. Il faut convaincre les internautes avec toute leur diversité, les sites marchants et surtout les institutions financières si on désire se relier au système monétaire physique. Il faut aussi satisfaire aux critères des États, stricts pour la création d'un mode de paiement, quasiment impossibles pour la création d'une monnaie [4], la monnaie étant un symbole fort considéré par de nombreux états comme relevant de la souveraineté nationale. Pourtant certains économistes sont pour une séparation de la monnaie et de l'État. L'Europe avec la Banque Centrale Européenne indépendante va dans ce sens. La porte n'est donc pas totalement fermée. On constate que les institutions observent toujours avant éventuellement d'interdire ou de valider. Dernièrement ce sont les bitcoins et plus largment les crypto-monnaies qui sont au cœur des préoccupations des banques centrales et de pays.

Dans cette partie nous allons donc regarder l'histoire et l'avenir des modes de paiement avec leur application à Internet ainsi que l'arrivée de nouvelles monnaies et leur impact dans notre monde physique.

6.1 La théorie

La première monnaie a été le grain d'orge, utilisé 3000 ans avant notre ère. Les cauris, des coquillages qui ont l'avantage d'être imputrescibles, ont été utilisés depuis -1300 av. JC jusqu'au 18e siècle. Les pièces de monnaie ont plus de 25 siècles. Puis est arrivé l'ère de la monnaie papier. Les lettres de changes date du 13e siècle, les billets de banque du 18e en Europe [5], les chèques du 19e. Enfin les cartes bancaires et les virements en ligne sont apparus au 20e siècle. Aujourd'hui les modes de paiement les plus usuels dans le monde physique sont :

1. le liquide ;
2. les chèques ;
3. les cartes bancaires ;
4. les versements.

Ils font tous intervenir un payeur, un bénéficiaire et leur banquiers respectifs mais de façons différentes. De plus chaque méthode a ses avantages et inconvénients. L'idéal serait d'avoir une monnaie électronique qui garde les avantages sans les inconvénients.

3. source : L'avenir de moyens de paiement en France par G. Pauget et E. Constans, mars 2012
4. Des simili-monnaies sont acceptées comme les Miles des compagnies aériennes, certes très limité à l'usage, mais dont la masse monétaire dépasse celle des dollars (The Economist 2005).
5. La Chine a utilisé des billets de banque autour de l'an 1000.

Le paiement en liquide permet de sauvegarder l'anonymat du payeur tout comme celui du bénéficiaire. Il permet les transactions entre particuliers. Enfin il est bien adapté à de petites sommes et permet aux parents d'envoyer leur enfant acheter le pain.

Son inconvénient principal est l'impossibilité d'annuler l'argent perdu ou volé pour pouvoir être remboursé. Cela le rend peu pratique pour le paiement de grosses sommes. On peut aussi lui reprocher sa divisibilité peu aisée, à savoir la difficulté pour faire la monnaie.

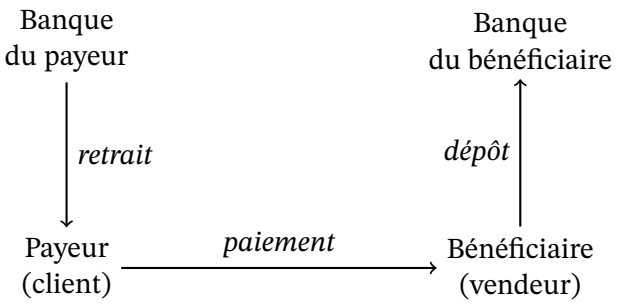


FIGURE 6.1 – Paiement en liquide

Les chèques suivent le même schéma que le liquide avec l'avantage de laisser une trace et de pouvoir toujours payer la somme exacte. Ils permettent les transactions entre particuliers et peuvent être annulés lorsqu'on les perd.

Le paiement par carte est très largement utilisé à travers le monde. Le nombre de carte de paiement Visa est de 3,4 milliards en 2019 (2,1 milliards en 2012). Celui de MasterCard est équivalent par contre UnionPay, le système chinois, avec ses 7,5 millards de cartes en circulation correspond à Visa + MasterCard [6].

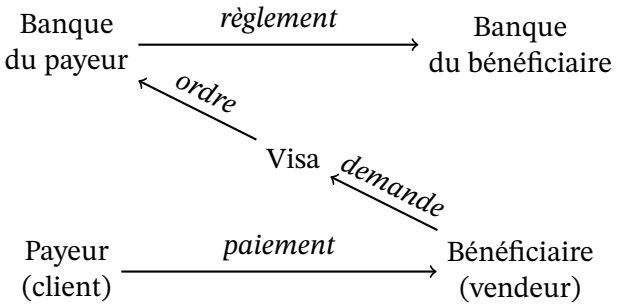


FIGURE 6.2 – Paiement par carte bancaire

Son fonctionnement permet d'avoir toujours l'appoint et garantit la sécurité grâce à la puce qui empêche un autre de l'utiliser.

Mais la carte peut être utilisée sans la puce. Cela permet la fraude sur Internet puisque le marchand dispose de toutes les informations pour faire des prélèvements. Il peut donc prélever de façon abusive, donner les informations à des personnes tierces ou se les faire voler. Notons enfin que la carte de paiement ne permet pas à des particuliers d'échanger de l'argent.

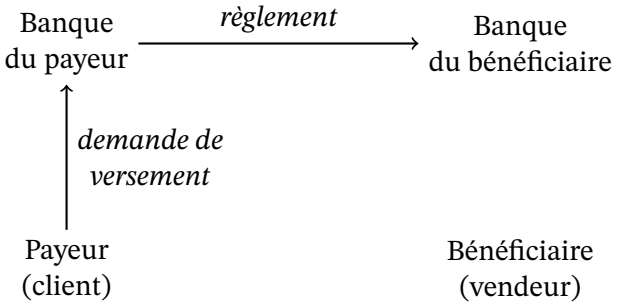


FIGURE 6.3 – Versement interbancaire

Les versements sont normalement le type de paiement le plus sûr. Ils sont dédiés aux sommes importantes et surtout adaptés au monde professionnel que ce soit pour payer les employés ou payer une autre société. Ils peuvent aussi être utilisés par les particuliers sur Internet pour payer un magasin ou un ami.

On peut les trouver trop lourds pour le paiement de petites sommes.

6. https://www.lesechos.fr/finance-marches/banque-assurances/le-chinois-unionpay-vient-defier-visa-et-mastercard-en-europe-1025

Ces exemples permettent d'établir une liste des avantages potentiels d'un moyen de paiement :

— la simplicité d'utilisation ;
— l'anonymat ou à l'inverse l'enregistrement de la transaction ;
— l'intégrité de ses économies si on perd le moyen de paiement ;
— la transaction entre particuliers ;
— la divisibilité ou la possibilité d'avoir toujours la somme exacte ;

À cette liste on peut ajouter les qualités nécessaires pour un moyen de paiement sur Internet :

— la garantie de l'intégrité de la transaction : soit le client est débité et le vendeur crédité, soit rien ne se passe,
— la sauvegarde des transactions afin de pouvoir retrouver l'état des comptes en cas de panne du système,
— la sécurité aux attaques de pirates, à la création de fausse monnaie, à la copie des billets électroniques...,
— la portabilité qui permet à tous les systèmes (ordinateurs, tablette, téléphone...) de communiquer,
— la convertibilité qui permet d'être changé en un autre type de monnaie (vers de la monnaie papier, vers une autre monnaie électronique...).

Notons que parmi ces caractéristiques, une seule est souhaitable ainsi que son contraire à savoir l'anonymat. Cela mène à deux catégories :

— les paiements anonymes, pour les petites sommes le plus souvent donc appelés les micro-paiements ;
— les paiements nominatifs ou vérifiables pour les sommes plus importantes.

À l'usage on retrouve bien ces deux catégories avec les autres caractéristiques qui se rattachent naturellement. Ainsi la simplicité d'utilisation est nécessaire pour les micro-paiements mais non nécessaire pour les paiements important où on accepte plus facilement de subir des étapes de vérifications. De même on peut accepter de perdre un porte-monnaie électronique qui a 10 euros, mais on n'acceptera pas que les traces du virement de son loyer aient disparues alors que l'argent a été débité.

En pratique on constate que les solutions développées ne suivent pas obligatoirement cette dichotomie. Ainsi les paiements avec téléphone sont souvent micro mais nominatifs alors que ceux avec des bitcoins peuvent être importants et anonymes.

6.2 Les micro-paiements

Le but est de développer un système pouvant remplacer le liquide. Des solutions s'appuient sur des porte-monnaies électroniques, d'autres réalisent des versements, enfin certaines sont purement logicielles et vont avec le développement de nouvelles monnaies. Ces dernières seront étudiées dans la section **??** sur la monnaie électronique.

Les solutions basées sur un porte-monnaie électronique se retrouvent dans de nombreux pays, mais ne traversent pas les frontières. Une solution française a été Monéo, héritière de la solution allemande Geldkarte. Elle permettait de payer un trajet de bus, un café rapidement, sans vérification comme pour du liquide. Elle a échoué et été remplacée par le paiement sans contact des carte bleues.

Sur Internet, une solution immatérielle a rencontré un véritable succès : Paypal. Ce système de versement est devenu de fait la référence du paiement en ligne même si les cartes bancaires restent plus utyilisée.

Enfin la véritable innovation en matière de paiement en ligne est la crypto-monnaie dont Bitcoin est l'initiateur et encore la référence.

Quelle que soit la mécanique développée, on sent que la difficulté liée aux micro-paiements électroniques réside dans la facilité avec laquelle on peut recopier une pièce de monnaie digitale puisqu'il ne s'agit que de 0 et de 1. Pour éviter les problèmes de fausse monnaie tout en gardant la facilité d'usage du liquide, différentes approches se dégagent :

— le porte monnaie électronique avec un support physique, une carte par exemple avec un lecteur,
— la solution logicielle avec sa sécurité intégrée au code (en utilisant la cryptographie),

Bien sûr, si on retire l'anonymat, qui est une des caractéristiques principales des micro-paiements, alors il existe une solution simple : le versement inter-comptes (ce que fait Paypal).

6.2.1 Le porte monnaie électronique

La carte à mémoire, brevetée en 1975 par Roland Moreno, a fait ses premiers pas en tant que carte téléphonique. Avec le temps elle a évolué pour devenir la carte à microprocesseur que l'on retrouve partout, de la carte bancaire à la carte Vitale en passant par les cartes SIM, Navigo, jusqu'aux cartes programmables comme les JavaCards. Chaque année, des milliards de cartes à puce sont fabriquées à travers le monde.

La sécurité de ces cartes est basée sur la difficulté à violer la puce avec un mécanisme de protection qui s'active en cas de tentative d'infraction. Ainsi la puce d'une carte bleue se bloque si l'on ne donne pas le bon code trois fois de suite.

Mais comme tout coffre fort, la sécurité n'est jamais totale comme cela a été démontré dernièrement lorsque la clé privée d'authentification de la véracité d'une carte bleue a été diffusé sur Internet, rendant possible la création de fausses vraies cartes (cf l'affaire Humpich et le dossier de Parodie.com).

D'un point de vue pratique, le point faible des cartes à puce à contact est le besoin de lec-

teurs pour communiquer. Cet aspect interdit les transferts d'argent entre particuliers [7] et rend caduque la sécurité de la puce lors des paiements sur Internet. Notons que cet aspect est nettement moins vrai pour les cartes à puce radio, il existe déjà des ordiphones qui peuvent communiquer avec de telles cartes.

Malgré ces inconvénients, la carte à puce est très largement utilisée ce qui en a fait un bon candidat pour un porte-monnaie électronique physique.

La Geldkarte (1996–2025) a été introduite en Allemagne en 1996. Ses principaux succès semblent être comme mode de paiement pour les transports en commun et pour les parcmètres. L'année la plus faste a été en 2007 avec une transaction moyenne qui a fortement chutée pour remonter doucement à 3 euros. Mais l'utilisation de la carte est en chute constante depuis 2007, cf figure 6.4, aussi en 2018 la Deutsche Bank annonce l'abandon de ce type de carte. En 2020 d'autres banque se retirent et la fin de la Geldkarte est prévue pour 2024/2025.

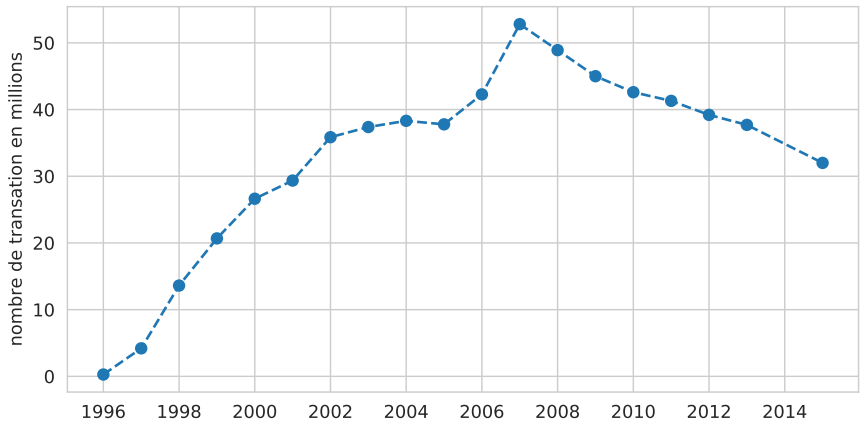


FIGURE 6.4 – Évolution de l'utilisation de la Geldkarte entre 1996 et 2015
source : bankenverband – Union des banques allemandes et Wikipedia

Le coût d'utilisation de la carte est de 0,3% de la transaction avec un minimum d'un centime. Le coût d'acquisition de la carte auprès de sa banque est en général nul mais peut être payant si la banque le décide.

Il est possible d'utiliser sa Geldkarte pour effectuer des paiements sur Internet avec un lecteur de carte à puce connecté à son ordinateur (prix : 60 euros).

Monéo (1999–2017) était l'application française de la Geldkarte. Elle a été créée par BMS, un consortium de banques françaises [8]. Son déploiement, lancé à Tours en 1999, est arrivé à Paris et sa région fin 2002 et a couvert l'ensemble du territoire en 2003.

7. ce qui de toute façon n'est pas au goût de la Banque de France qui craint des fraudes et son utilisation pour le blanchiment de l'argent sale

8. le Crédit Agricole, la BNP (28,5 % chacun), les Banques Populaires, le Crédit Lyonnais, le Crédit Mutuel (10 %), le CCF (7 %) et le CIC (6 %)

Elle permettait à l'utilisateur de payer des petites sommes, inférieures à 30 , € simplement et rapidement mais elle coûtait cher tant aux particuliers qu'aux commerçants.

En 2005 l'UFC [9] indiquait :

«*Moneo demeure un produit sans grand intérêt pour les consommateurs, et cela tant qu'il ne sera pas gratuit et totalement indépendant des banques.*»

En 2013 l'échec de Moneo est pattant. La BNP, la Poste et la Caisse d'Épargne se désengagent. Le groupe BMS-Moneo se reconvertit dans les cartes de restauration pour étudiants et vise le marché des tickets restaurants. En 2017 c'est la fin, Monéo-Resto est racheté par Edenred (tickets restaurants).

Techniquement, Monéo utilisait l'algorithme de chiffrage triple DES pour valider les cartes, probablement suivant le même principe de *défi* que les cartes bleues mais avec une clé plus longue. Le SCSSI [10] a certifié les composants de Monéo.

Pour des raisons de simplicité et de rapidité lors du paiement seule la vérification de l'authenticité de la carte était faite. Aucune vérification n'était faite pour vérifier que le porteur est bien le propriétaire de la carte. Il n'y avait pas de code à taper.

Il était possible de recharger sa carte sur Internet, après avoir acheté un lecteur de carte à puce, mais pas de l'utiliser pour faire des paiements a priori.

6.2.2 La carte radio

L'un des inconvénients de la carte à puce est le besoin d'avoir un lecteur et d'y insérer la carte pour effectuer une transaction. Ces lecteurs sont encombrant, coûtent chers et, à l'usage, la transaction est plus lente que s'il suffit de passer sa carte à proximité du lecteur. La carte radio [11], ou carte NFC du nom de la norme, répond à ces problématiques :

— un lecteur NFC tient dans une puce et son coût est négligeable. De nombreux ordiphones intègrent un tel lecteur.
— la communication radio se fait sans contact, rapidement et simplement.

Parmi les applications les plus connues de telles cartes, citons

— Navigo utilisées par la RATP dans le métro parisien,
— la carte à tout faire FeliCa développée et commercialisée par NTT DoCoMo et Sony au Japon,
— la carte de paiement PayPass de MasterCard et Motorola déjà utilisée dans plusieurs états des États-Unis.
— les cartes de paiement française qui, en plus de la puce électronique, disposent de plus en plus de la technologie NFC pour les paiements sans contacts.

9. L'Union fédérale des consommateurs (UFC-Que Choisir)
10. remplacé depuis par l'ANSSI (Agence nationale de la sécurité des systèmes d'information)
11. La carte communique par ondes radio. Pour pouvoir émettre, elle puise son énergie dans le champ électromagnétique généré le lecteur.

La norme NFC (Near Field Technology)

Comme pour la communication filaire, il existe une infinité de façon de communiquer via les ondes. Comme pour la communication filaire, il n'y a pas d'interconnexion sans norme, aussi trois acteurs majeurs, Nokia, Philips et Sony ont développé une norme pour les cartes radio, la *Near Field Technology* qui permet :

- une connexion seulement à courte distance sur 13.56 MHz (moins de 20 cm) qui garantie la connexion volontaire [a]
- le transfert de données à 106, 212 ou 424 kbit/s,
- une communication active ou passive suivant qu'on désire utiliser sa propre énergie ou celle de l'autre appareil (au moins un des deux doit être actif),
- un système d'amorçage permettant de s'authentifier puis rediriger la communication radio vers le Bluetooth ou le Wifi (d'autres protocoles radio au débit plus important)

Une extension de cette norme, la *Secure NFC*, ajoute par dessus la NFC un système d'authentification basé sur la cryptographie.

a. enfin normalement, des tests ont permis de lire une carte à plus de 10 mètres...

Ajoutons que de nombreux ordiphones intègrent la technologie NFC et disposent d'applications qui peuvent remplacer la carte Navigo par exemple ou stocker des tickets de métro. Il est également possible de payer sans contact avec son téléphone plutôt qu'avec la carte bleue.

Il ne reste plus qu'a pouvoir payer sur Internet avec sa carte NFC et donc à avoir des claviers avec lecteur NFC (la marque Cherry en propose) et des sites marchants qui permettent un tel paiement.

6.2.3 Le téléphone mobile – L'Afrique innove

Le téléphone portable étant un outil de plus en plus répandu, il n'est pas surprenant que des solutions de paiement l'utilisent. Ainsi les systèmes de paiement par carte ont couplé le paiement sur Internet avec une validation par SMS [12] pour améliorer la sécurité.

Durant les années 2000, Bouygues avait essayé de développer sa solution assez proche qui fonctionnait aussi dans le monde réel :

1. le client donne son numéro de portable au vendeur,
2. le vendeur l'entre dans son terminal relié à Bouygues ainsi que le montant de la transaction,
3. Bouygues envoie un SMS sur le portable du client et lui demande de confirmer l'achat en entrant son code secret,
4. le vendeur reçoit la confirmation de la vente et le terminal imprime le ticket.

Mais ce système n'a pas pris et n'existe plus.

12. au moment de payer votre achat, vous devez entrer sur le site web le code que vient de vous envoyer votre banque par SMS

À l'inverse, en Afrique des systèmes de paiement par téléphone sont largement utilisés. Ainsi M-Pesa au Kenya et en Tanzanie, et Zaad au Somaliland, remplacent l'argent liquide pour de nombreuses personnes avec les avantages de sécurité et de liquidité évidents.

Le paiement d'un achat avec Zaad suit la procédure suivante :

1. faire le `*888#`
2. entrer son code secret
3. indiquer que l'on désire payer un marchant : `4`
4. entrer l'identifiant du marchand
5. entrer le montant
6. confirmer
7. le marchant et le client reçoivent alors un SMS qui confirme le paiement.

Donner de l'argent à une personne suit la même procédure si ce n'est qu'on indique le téléphone de la personne et non l'identifiant du magasin. On peut aussi retirer de l'argent liquide avec son téléphone, voir son relevé "bancaire", payer des factures... Notons aussi que ce système permet de payer à distance, par exemple la glace de votre enfant alors que vous êtes au travail, puisqu'il suffit que vous sachiez le code du marchand et le montant. Dès lors le passage à l'e-économie est simple et il existe naturellement des sites web qui acceptent ce mode de paiement.

L'opérateur téléphonique Safaricom, propriétaire de M-Pesa, indique que 15 millions de kenyans utilisent M-Pesa et qu'un tiers du PNB du Kenya passe par son système de paiement (chiffres 2012). Statista indique 30 millions d'utilisateur en 2017 et 40 millions en 2020.

Notons enfin que ces systèmes alternatifs rencontrent du succès là où les offres bancaires sont réduites ou bien pour les populations qui n'ont pas accès au système bancaire. Cela place M-Pesa en situation de monopole dans ces cas, ce qui peut générer des abus comme des commissions excessives.

6.3 Les macro-paiements

Le système de macro-paiements les plus utilisés sur Internet reste la carte de débit. PayPal est second. En dehors de ces deux systèmes, on trouve les virements interbancaires et des systèmes plus marginaux. Parmi les systèmes marginaux, les bitcoins sont intéressants car anonymes, ce qui ressemble plus aux micro-paiements qu'aux macro-paiement, avec des frais d'usage importants qui en font plus une monnaie pour macro-paiements. Ils seront étudiés à la section suivante.

Alors que reste-t-il ? Pas grand chose. Regardons néanmoins le système de paiement SET qui montre que l'on peut proposer une solution techniquement bien, moralement tout aussi bien, supportée par les plus grands noms du monde du paiement, de l'informatique et même par l'Europe, sans pour autant trouver le succès.

6.3.1 SET (1996–2001)

La création en 1996 du protocole SET, Secure Electronic Transaction, est le résultat de la fusion de divers projets et de l'union des grandes sociétés du domaine que sont Visa, MasterCard, CyberCash, Netscape, IBM, Microsoft et DigiCash. Elle aurait du être un succès et ce d'autant plus qu'il s'agissait d'un protocole ouvert, donc pas de jaloux, une pérennité et intercompatibilité garantie.

Les spécifications de SET précisent chaque étape de la procédure (les spécifications "Business" sont assez précises pour comprendre en détail les différentes procédures) :

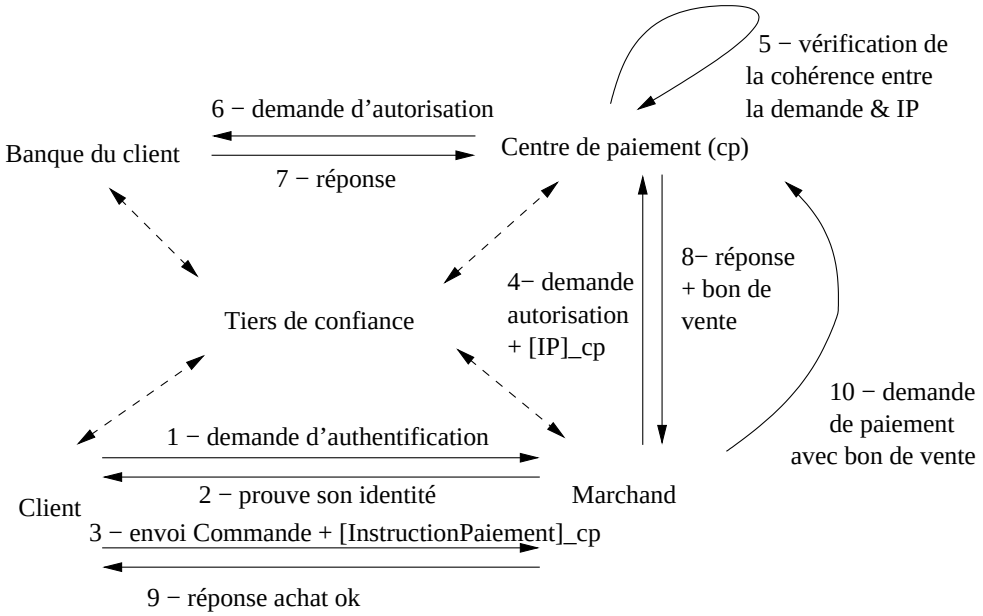


FIGURE 6.5 – Fonctionnement de SET
Les vérifications auprès du tiers de confiance sont faites
lors de la réception de chaque message pour en vérifier l'auteur

D'un point de vue technique, SET fait intervenir en plus du client, de sa banque et du vendeur, une autorité de certification (ou tiers de confiance) pour valider l'identité des partenaires et une passerelle de paiement qui centralise les demandes de paiement SET de la part des vendeurs pour décrypter l'identité bancaire du client et faire la demande à sa banque.

Du point de vue moral, la présence de la passerelle de paiement permet d'éviter que le vendeur puisse connaître les coordonnées bancaires du client. De même elle protège la vie privée du client vis-à-vis de sa banque en cachant le contenu de la commande et vis-à-vis du marchand en cachant l'identité de sa banque (cf le schéma figure 6.5).

En France l'application la plus importante de SET a été menée par le GIE Carte Bleue qui à travers sa société Cyber-COMM a promu ce système de paiement, d'autant plus intéressant pour le GIE que 60% des plaintes des porteurs de Cartes Bleues étaient alors liées à des achats

faits sur Internet.

Si SET est passé en mode de production et a été utilisé par des grands sites web comme celui de la Redoute, il n'a jamais atteint la masse critique nécessaire. Aussi courant 2001, VISA et MasterCard ont décidé d'abandonner le déploiement de SET. La nécessité pour l'acheteur de devoir disposer d'un lecteur de carte à puce relié à son ordinateur est probablement la cause principale de l'échec.

SET a finalement été remplacé par le système 3-D Secure [13] qui est utilisé tant par Visa que par MasterCard. On note que, là encore, la simplicité a gagné.

Notons aussi que l'arrivée des cartes NFC et des lecteurs dans les ordiphones n'ont pas relancé le projet.

6.4 PayPal

En tant que solution leader créée pour le paiement sur Internet, PayPal mérite sa section.

PayPal est un système lourd d'usage qui offre la traçabilité des transactions, donc plutôt pour les macro-paiements. Cependant PayPal vise aussi les micro-paiements, en particulier des micro-paiements pour biens numériques, comme un mp3 ou un article de presse [14].

L'innovation

Comment PayPal a réussi là où les autres ont échoué ? L'explication est dans la figure 6.6 extraite de leur site web. La réussite de PayPal n'est pas technique mais marketing : vous pouvez donner de l'argent à tout le monde avec PayPal, même à ceux qui n'ont pas de compte PayPal. Il suffit d'une adresse mail ou d'un numéro de téléphone. Si le destinataire n'a pas de compte PayPal, il se verra offrir le choix entre avoir un compte PayPal avec l'argent dessus ou donner un RIB pour que l'argent soit versé sur son compte bancaire. Bien sûr, comme il s'agit de petites sommes en général, le destinataire choisit d'avoir un compte PayPal. Ainsi en moins d'un an, PayPal a dépassé le million de comptes ouverts. Bien sûr ce point n'est probablement pas la seule raison du succès de PayPal. Le fait qu'un grand nombre de sites web l'accepte comme mode de paiement est certainement un élément important, ne serait-ce que pour conserver son argent sur PayPal.

Le succès initial ne s'est pas démenti comme le montrent les chiffres de la figure 6.7.

En octobre 2002 eBay a acquit PayPal pour 1,5 milliards de dollars. Une véritable synergie a pu se développer entre ces deux sites complémentaires. Lors de l'achat, les revenus de PayPal étaient d'environ 53 millions de dollars alors que ceux d'E-Bay étaient de 266 millions de dol-

13. vérification par un autre canal, SMS en général, que vous êtes bien à l'origine du paiement.

14. La commission appliquée alors est de 5 centimes + 0,6 % pour les paiements nationaux inférieur à 10 € et utilisant les codes QR, donc adaptée au commerce en ligne. Source : https://www.paypal.com/fr/webapps/mpp/merchant-fees

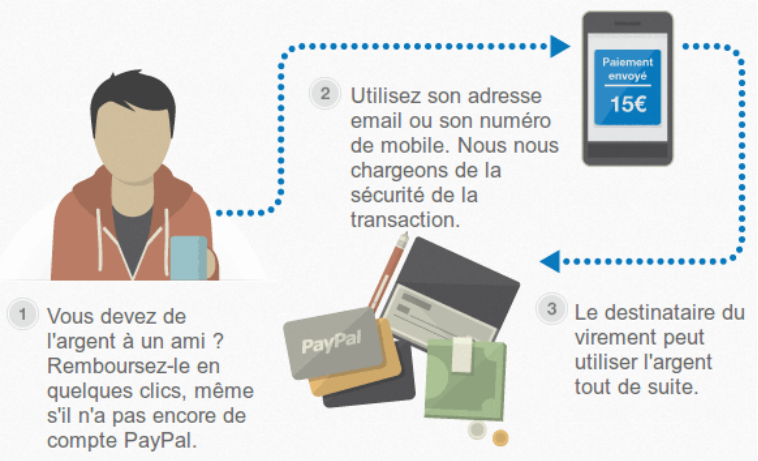


FIGURE 6.6 – Enrolement à la PayPal

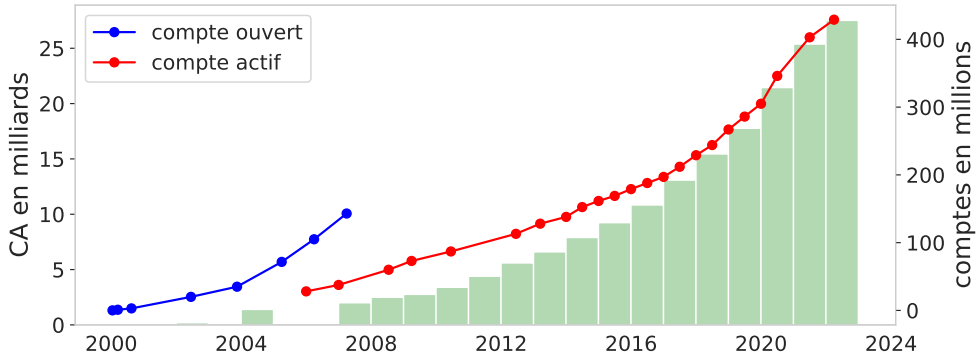


FIGURE 6.7 – Nombre de comptes et chiffre d'affaire de PayPal

Compte actif = au moins une transaction par trimestre

lars. Fin 2012 les revenus générés par PayPay ont représenté 39% des revenus de la nouvelle entreprise. En 2014 PayPal est devenue une spin-off de eBay à savoir qu'elle devient indépendante, chaque actionnaire d'eBay recevant autant d'actions de PayPal qu'il a d'actions d'eBay. En 2022 PayPal a fait un chiffre d'affaire de 27,5 G$ et un bénéfice de 2,4 G$.

Fonctionnement

D'un point de vue technique, PayPal n'est qu'un système de virements entre comptes. Aucune innovation mais un système simple qui passe par le site web de PayPal pour s'authentifier et initier ou valider le paiement. Pour des macro-achats sur Internet c'est tout à fait satisfaisant.

Le même manque d'innovation est en train d'être appliqué à une solution de paiement avec son compte PayPal dans le monde physique. Mais dans ce cas il n'est pas certain que le succès soit au rendez-vous, la procédure étant plus lourde qu'avec une carte de paiement (il faut entrer

dans le terminal du magasin son numéro de téléphone ainsi que son code secret [15]). Comme les tarifs de PayPal sont aussi plus élevés, la bataille n'est pas gagnée.

Tarifs

PayPal prend entre 3 et 4 % des montants qui transitent par son système de paiement. C'est un coût nettement supérieur à celui des cartes bleues. C'est aussi nettement plus cher que le coût des transferts interbancaires en France, en général gratuit, mais nettement moins que le coût de transfert vers l'étranger hors Europe, voir table 6.1.

Système	particulier en France	magasin en Europe (€)	magasin hors Europe
PayPal (2023)	0	0,35 € + 2,9 %	~ 0,35 € + 4,9 % + ? de change
TransferWise (2019)	0,8 €	0,8 €	1 € + 0,41 % + 0.35 % de change ($)
Carte Bleue Visa	impossible	~ 1 % (⋆)	1 € + 2,7 % (†)
Virement interbancaire (Société Générale 2019)	0	0	9 à 33 € (•) + ? de frais de change

TABLE 6.1 – Tarifs de PayPal comparé à d'autres

(⋆) varie fortement suivant les accords avec sa banque

(†) tarif 2015 Visa via la Société Générale

(•) 9 à 29 € si < 500 €, 13 à 33 € si < 4000 €, sinon ?

PayPal est surtout intéressant pour échanger entre particuliers, ensuite il faut faire attention. Si PayPal, comme les Cartes Bleues, fait porter les frais bancaires sur le vendeur, les frais de changes restent pour l'acheteur. Pour les paiements en devise étrangère, TransferWire [16] ou la carte Ultim de Boursoma sont préférables.

Pour un magasin, le choix des modes de paiement acceptés n'est pas seulement lié aux frais bancaires mais aussi à leur popularité. Aujourd'hui PayPal est assez populaire pour s'imposer de plus en plus auprès des magasins sur Internet mais pas dans le monde physique (même s'il y vient).

6.5 Les monnaies complémentaires

Si on appelle système de paiement tout système organisé permettant de rémunérer un service rendu ou l'achat d'un objet, alors il existe déjà de nombreux systèmes de paiement alternatifs mis en place de façon autonome.

Ces systèmes peuvent être limités géographiquement ou dans leur utilisation. Dans ce dernier cas on trouve Les Miles et les tickets restaurant.

15. cf http://venturebeat.com/2012/03/14/paypals-new-pos-service-is-a-piece-of-sht/
16. La néobanque N26 s'appuie sur TransferWire pour son offre en devises étrangères.

Mais les systèmes de paiement alternatifs ou complémentaires qui ont le plus marqué les esprits sont les monnaies locales, de par leur capacité à remplacer, localement, la monnaie officielle. Parmi les plus connues, citons les bons vieux Systèmes d'Echange Locaux, SEL dont la première expérience date de 1932. Cette année là, la ville de Wörgl en Autriche avait alors émis sa monnaie avec succès mais celle-ci a été interdite au bout de 9 mois par la Banque Nationale. En 1956 la même chose se produit en France à Lignières en Berry. Puis le rythme a accéléré durant les années 80 pour entrer dans les mœurs durant les années 90, voir figure 6.8.

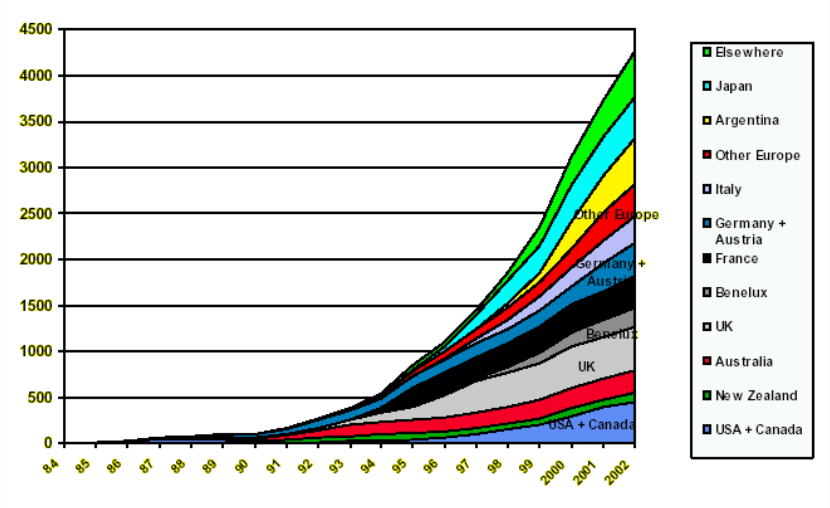


FIGURE 6.8 – Nombre de systèmes monétaires complémentaires dans 12 pays
source : Bernard Lietaer, The Future of Digital Money, 5e Digital Money Forum

Initialement le but de ce type de monnaie était d'aider les plus défavorisés, les exclus, en leur donnant une unité d'échange abordable afin de pouvoir continuer à exercer une activité. Mais elles offrent d'autres avantages. Elles garantissent que la richesse reste dans une zone géographique délimitée, ce qui favorise ses utilisateurs et donc les commerçants qui les acceptent. Elles peuvent être rattachées à la monnaie officielle ou pas. Elles peuvent augmenter la masse monétaire ou pas. Elles ont une souplesse qui les rend à même de répondre aux besoins qu'elles visent. Par exemple en Bavière, le Chiemgauer, une monnaie à parité avec l'Euro, permet de financer les associations locales en leur versant 3% des échanges Chiemgauer vers Euro [17]. Autre exemple, après la crise de 1929, des entrepreneurs suisses ont créé le WIR à parité avec le francs suisse. Il sert de relai lorsque l'argent officiel vient à manquer. Le WIR est toujours utilisé par un quart des entreprises suisses et permet de réduire fortement l'impact des crises financières. On a retrouvé cet effet d'amortisseur avec d'autres monnaies locales lors de la crise asiatique de 1997. Aussi on comprend que les États puissent voir d'un bon œil ces initiatives locales. Les États vont même parfois jusqu'à les encourager. De fait, le poids économique de ces monnaies a crû régulièrement durant les années 2000, cf figure 6.9.

En 2009, le Brésil a créé 5 banques communautaires afin de relancer l'économie dans des quartiers. Ces banques qui reposent sur des militants locaux, connaissent bien leurs *clients* et obtiennent des remboursements très satisfaisants tout en incitant les habitants à reprendre

17. cf http://www.recit.net/Le-Chiemgauer-une-monnaie

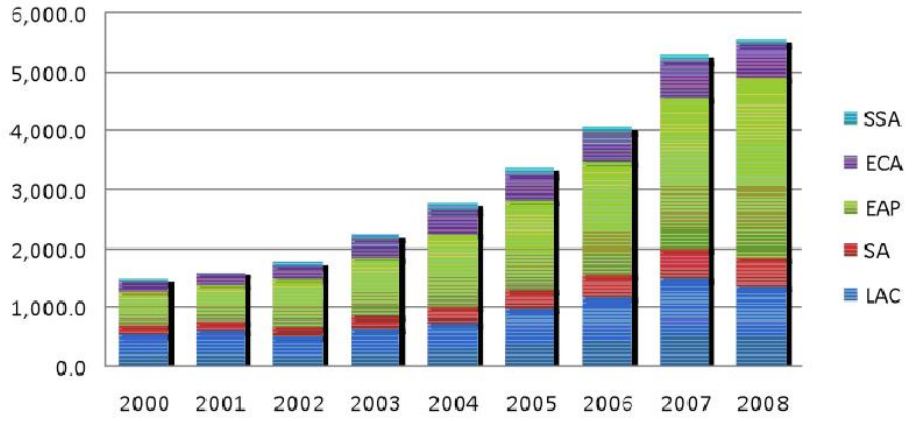


FIGURE 6.9 – Valorisation des monnaies locales par région (en millions de dollars)
Légende : EAP : East Asia, LAC : Latin America
ECA : Eastern Europe, SA : South Asia, SSA : Sub-Saharab Africa
source : Heiko Hesse, Ismail Dalla, voxeu.org, 2009

des activités et à dépenser localement.

Le Vénézuela a été plus loin en inscrivant le principe dans la loi et comptait plus de 5000 banques communautaires en 2011 (pour 100 au Brésil).

Mais ces monnaies parallèles aux monnaies fiats [18] sont le plus souvent en dehors des systèmes de taxations sur les biens, TVA, et sur le travail. Elles peuvent donc avoir un impact négatif si elles deviennent trop importantes et détruisent des activités économiques existantes.

On voit donc que la création de monnaies complémentaires n'est pas une nouveauté et qu'elles sont déjà largement intégrées dans nos sociétés. Aussi il n'est pas si surprenant de voir de telles monnaies apparaître sur Internet sans être directement contrées par les gouvernements [19].

6.6 Création de monnaies sur Internet

Pour créer du liquide sur Internet, une solution naturelle consiste à avoir des pièces numériques que les utilisateurs puissent s'échanger. Il est bien sûr nécessaire de respecter toutes les qualités demandées à une monnaie de micro-paiement (l'anonymat par exemple). Une autre solution consiste à utiliser la cryptographie pour effectuer des virements rendus publics pour vérification mais brouillés, là encore pour protéger l'anonymat.

Dans tous les cas la cryptographie est utilisée pour garantir au propriétaire de garder le contrôle de son argent et pour protéger son anonymat. Elle doit aussi prévenir

— la création de fausses pièces,

18. Une monnaie fiat est une monnaie contrôlée par un État.
19. Pour plus d'information sur les monnaies complémentaires, on pourra lire le rapport de Jean-Michel Cornu : http://www.club-jade.fr/images/jean-michel-cornu-l-innovation-monetaire.pdf

— la copie des pièces,
— l'espionnage des transactions d'un client par sa banque ou des tiers.

6.6.1 DigiCash (1993–2002)

La technologie de l'eCash a été mise au point dès 1993 par David Chaum au sein de sa société DigiCash. Cette monnaie a été mise en production par différentes banques mais elle n'a jamais pris. En Europe, la Deutsche Bank a fait une tentative en 2000.

Tout commence par la création des pièces. Il s'agit de créer de véritables pièces sans que la banque puisse savoir à qui elles appartiennent.

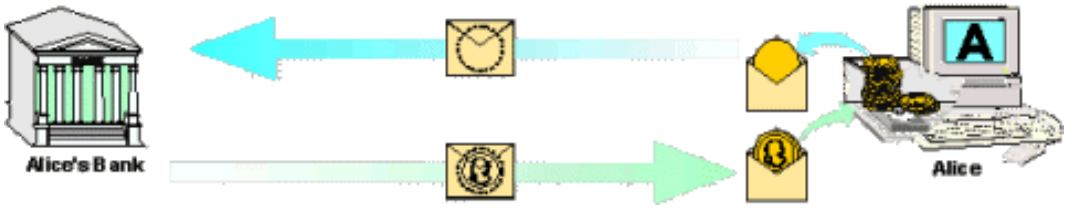


FIGURE 6.10 – Créations "anonyme" de pièces eCash

Pour cela Alice crée une pièce vierge avec un numéro de pièce unique qu'elle cache dans une enveloppe avant de l'envoyer à sa banque en lui demandant de donner à cette pièce une valeur déterminée. La banque débite la valeur désirée du compte d'Alice, marque la pièce de cette valeur sans ouvrir l'enveloppe. Elle renvoie le tout à Alice qui extrait la pièce marquée et la range dans son ordinateur.

Bien sûr la pièce, l'enveloppe et le marquage de la banque sont des images qui représentent l'identifiant numérique généré par Alice et l'opération de cryptographie qui brouille l'identifiant et celle de la banque qui valide l'identifiant brouillé.

Lorsqu'Alice veut payer Bob, elle lui envoie les pièces qui font le montant demandé.

FIGURE 6.11 – Alice donne des pièce à Bob qui les vérifie auprès de la banque d'Alice

Bob fait alors suivre les pièces à la banque d'Alice, laquelle vérifie qu'il s'agit de pièces qu'elle a validées (la banque ne peut pas savoir qu'il s'agit de pièces d'Alice). Elle vérifiera aussi que les pièces n'ont pas déjà été utilisées.

Finalement, Bob peut demander à la banque d'Alice des pièces neuves de la même somme ou demander un virement sur son compte.

Parmi les points faibles de cette méthode, notons la difficulté d'avoir l'appoint (sauf à avoir des millions de pièces d'un centime mais alors le coût de la transaction sera lourd) et l'obligation de devoir être connecté aux banques pour chaque transaction. Il est aussi probable que l'infrastructure du web 1.0 n'était pas adaptée à la diffusion d'une solution aussi lourde techniquement.

6.6.2 Le Bitcoin

Contrairement à l'eCash, les bitcoins sont simples à utiliser. Il n'y a pas de création de pièce pour l'utilisateur lambda donc pour en avoir, il faut en recevoir. Verser de l'argent revient à lire un code QR le plus souvent. Il est aussi possible indiquer le numéro de compte du vendeur (appelée adresse) et la somme à verser. Vous pouvez faire cela depuis votre ordiphone ou ordinateur. Le destinataire verra la somme arriver sur son logiciel.

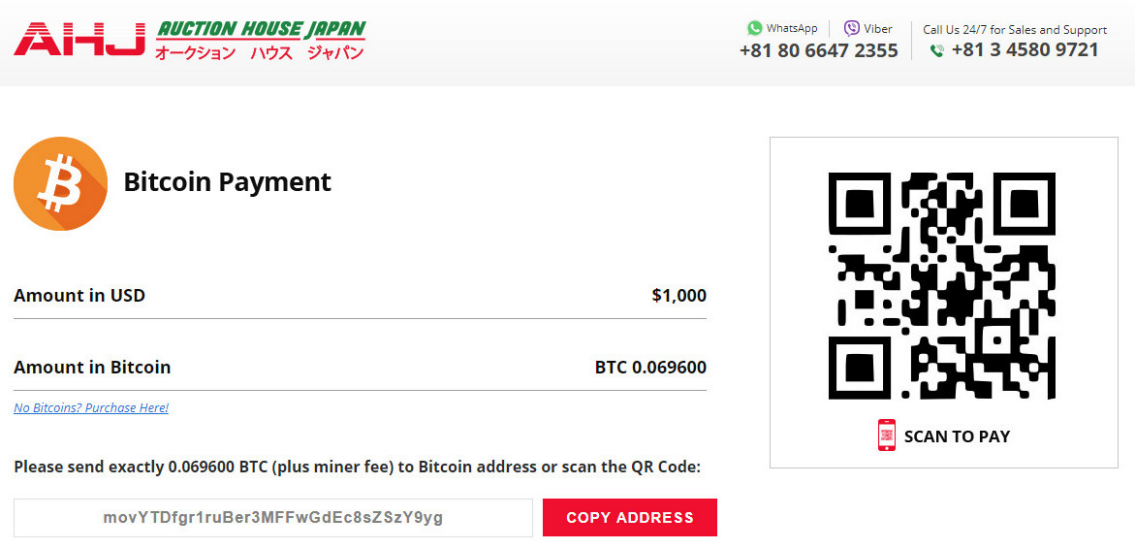


FIGURE 6.12 – Magasin qui présente la note en Bitcoin

Pour recevoir de l'argent, vous générez une adresse que vous transmettez. Vous pouvez générer autant d'adresse que vous le souhaitez, un par client, un par achat ou un seul pour tout. Cette adresse est écrite sur le grand livre de compte du Bitcoin [20] ainsi que la somme qui lui a été versée. Celui qui contrôle cette adresse peut y prendre l'argent pour le verser à une autre adresse.

Comme on a vu, il est également possible de générer un code QR qui comprend toutes ces informations.

20. Ce grand livre de compte que chacun peut recopier localement (attention, ce livre fait 300 gigaoctets en 2020) s'appelle la *blockchain* pour des raisons qu'on verra dans la partie technique ci-dessous.

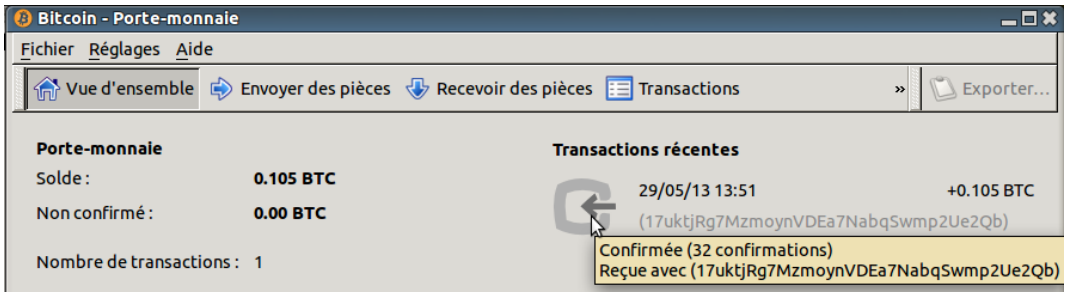


FIGURE 6.13 – Réception de premiers bitcoins dans ce (vieux) porte-monnaie
L'adresse 17uktjR... a été généré par ce porte-monnaie et transmis au payeur

Mise en œuvre

Installer une application qui permet de manipuler ses bitcoins sur son ordinateur peut être stressant pour certains, surtout lorsque les sommes sont importantes. Il faut savoir que si on perd le mot de passe associé à son compte, on perd ses bitcoins sans possibilité de les récupérer (c'est déjà arrivé plusieurs fois). Aussi pour certain il peut être préférable d'utiliser une plateforme d'échange qui ressemble à une banque [21]. C'est la solution la plus simple Lorsqu'on désire acheter des crypto-monnaies avec des euros.

— Binance est la plus grande plateforme de crypto-monnaie en terme de volume, elle propose des centaines de cypto-monnaies. Attention, elle a eu régulièrement des problèmes avec les autorités de différents pays et devrait quitter certains pays européen en 2023 [22].
— Coinbase est une entreprise américaine créée en 2012 pour les crypto-monnaies. Elle est en seconde position en terme de volumes échangé.
— eToro est une ancienne plateforme israélienne de finance qui a pris le virage des crypto-monnaies dans les années 2010. Elle est plus chère et moins populaire que Binance mais mieux intégrée dans le système financier des États,
— de très nombreuses autres plateformes existent, ainsi que des comparateurs.

Binance France et eToro sont enregistrées auprès de l'autorité des marchés financiers en tant que prestataires de services en actifs numériques, PSAN [23].

Il est possible d'avoir un compte sur une telle plateforme d'échange pour acheter et vendre des bitcoins puis de les rapatrier sur sa machine une fois la transaction faite. Cela a un coût mais vous êtes protégé contre une mésaventure qui pourrait arriver à la plateforme.

Pour suivre les transactions, pour visualiser le marché des crypto-monnaies, il existe des sites dédiés :

— CoinMarketCap permet de comparer les monnaies et d'avoir une description précise de

21. Comme une banque, une plateforme d'échange peut se faire voler ou disparaitre avec la caisse, c'est déjà arrivé.
22. https://www.cointribune.com/crypto-bientot-la-fin-de-binance-en-europe/
23. L'explication de ce status et la liste des plateformes enrgistrées sont ici : https://www.amf-france.org/fr/espace-professionnels/fintech/mes-relations-avec-lamf/obtenir-un-enregistrement-un-agrement-psan

chacune.
— Blockchain ou BlockChair permettent d'explorer la *blockchain* et de tracer les échanges.

Pour gérer ses bitcoins en local, il existe de nombreuses applications qui sont présentées dans la section choisir son porte-monnaie du site bitcoin.org. Pour une sécurité renforcée, il est possible d'utiliser un coffre fort physique à savoir une clef usb qui intègre de la cryptographie et garde votre clef privée au sûr. Parmi les plus connues citons les clefs de Ledger ou de Trezor.

Techniquement

La complexité du Bitcoins est cachée dans la mécanique. Là encore on utilise la cryptographie massivement mais celle à base de courbes elliptiques et non celle présentée dans le premier chapitre qui s'appuie sur les nombres premiers. Sans entrer dans le domaine des courbes elliptiques, regardons comment le Bitcoin fonctionne.

Le principe fondamental est un livre de compte dans lequel on écrit tous les transferts. La notion de pièce n'est pas présente. Si j'ai reçu un transfert de 1 bitcoin (transaction A, ancienne) et que je dépense 0,2 bitcoins, alors tout le monde doit pouvoir voir que ces 0,2 bitcoins proviennent du bitcoin que j'avais reçu. On s'appuie sur les transactions passées pour permettre les nouvelles.

L'émetteur signe ses paiements avec sa clef privée afin de pouvoir utiliser ses bitcoins. Il utilise la clef publique de son destinataire pour déposer la somme afin que ce dernier soit le seul à pouvoir la revendiquer (avec sa clef privée). En pratique la clef publique du destinataire est intégrée dans l'adresse de transaction.

Ainsi cela donne pour une transaction C (Courante) :

— `entrée` : l'adresse de la transaction A de 1 btc (bitcoin) que l'émetteur avait reçu
— `sortie 1` : l'adresse donnée par le destinataire et la somme de 0,2 btc
— `sortie 2` : l'adresse de l'entrée et la somme de 0,8 btc (il se donne ce qui reste)

L'émetteur signe le tout avec sa clef privée et voilà. Sa signature est obligatoire car la transaction A de 1 btc était signée avec sa clef publique.

Après la transaction C, la transaction A n'est plus utilisable car elle a un fils.

Dans le cas où on ne dispose pas d'une transaction précédente avec assez d'argent, il est possible de combiner plusieurs transactions reçues afin d'atteindre le montant voulu. La transaction décrite ci-dessus aurait alors eu plusieurs entrées.

Double dépense Afin que je ne puisse pas utiliser une seconde fois la transaction A pour payer quelqu'un d'autre, la transaction C est incorporée dans un bloc de transactions (lequel regroupe toutes les transactions des 10 dernières minutes en moyenne, cf Blockchain.info).

Lorsque ce bloc est publié, tout le monde est au courant de la transaction C, y compris le destinataire qui, alors, se considère payé. Bien sûr aucune autre transaction avec la transaction

A en entrée sera acceptée. Si durant la création du bloc j'avais utilisé 2 fois la transaction A, alors une seule des 2 transactions aurait été acceptée et seul un destinataire aurait pu voir qu'il a été payé.

La force du Bitcoin est que les blocs sont créés par tout le monde en résolvant un problème mathématique difficile, mais simple à vérifier lorsqu'on a la solution. Ainsi lorsqu'une personne indique qu'elle a la solution dans son bloc, les autres peuvent valider cette solution et tout le monde passe à la création du bloc suivant. Chaque bloc est lié à sont précédant ce qui crée une chaine de blocs, cf encart page 26.

Annuler la transaction Une autre façon de tricher est de créer un bloc menteur qui ne comprend plus la transaction C pour remplacer le bloc qui la comprenait. Ainsi le destinataire a cru être payé, et donc a livré l'achat, mais finalement son argent disparaît et comme la transaction A n'a plus de fils, le payeur récupère l'argent. Pour éviter cela, on considère que seule la plus longue chaine de blocs est la bonne. Aussi si je crée un bloc menteur pour remplacer le bon bloc, il va aussi falloir que je recrée tous les blocs suivant créés depuis. Or la construction d'un bloc est difficile à cause des problème mathématiques à résoudre et pour faire la chaîne de bloc la plus longue je dois aller plus vite que tous les autres mineurs réunis.

Faiblesses du système

Les créateurs de blocs, les mineurs, sont récompensés par 6,25 bitcoins par bloc créé [24] plus un pourcentage sur les transactions enregistrées [25]. Avec le temps, la récompense fixe baisse afin de ne pas créer trop de monnaie et le pourcentage augmente. Ce système motive les mineurs et fournit la puissance de calcul nécessaire au bon fonctionnement général.

Ce système génère des problèmes :

— plus la valeur du bitcoin est élevée, plus il est intéressant de miner, ce qui garantit la sécurité mais ce qui génère une consommation électrique démesurée comme on le verra.
— plus il y a de transactions, et plus les frais de transactions augmentent puisque les mineurs choisiront d'intégrer dans leur bloc les transactions les plus rémunératrices. Ainsi le prix moyen à payer pour que sa transaction soit intégrée devient bien trop important pour des micro-paiments (le prix varie de quelques dollars à quelques dizaines de dollars, cf figure 6.14).
— plus il y a de transaction et plus on doit attendre pour que sa transaction passe (problème de passage à l'échelle).

Lightning Network Pour répondre à ces problèmes, le *Lightning Network* et été crée. Il s'agit d'un réseau de niveau 2 qui se rattache de temps en temps à la chaîne du Bitcoin. Il permet

24. après la division par 2 de la récompense en mai 2020. Des divisions par 2 sont prévues tous les 4 ans par le protocole.
25. le pourcentage est choisi par le payeur mais plus il est important, plus les mineurs ont envie d'inclure la transaction dans leur bloc

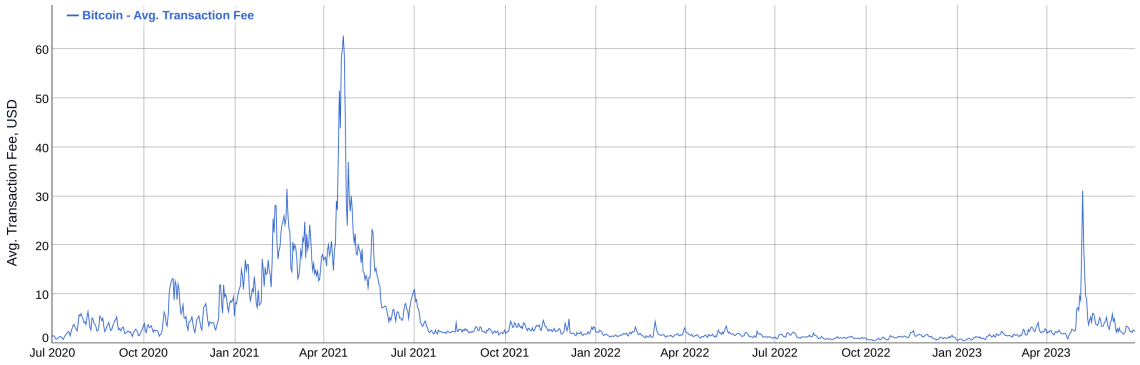


FIGURE 6.14 – Frais moyens pour une transaction en bitcoins

des paiements très rapides (en dessous de la minute voire de la seconde) et des frais de transaction très faibles (0,003 % soit 1000 fois moins cher que Visa). De plus il résout le problème de passage à l'échelle en permettant des billions de transaction par seconde. On a donc une solution miracle qui a néanmoins un coût : une perte de sécurité par rapport au Bitcoin.

Ce réseau est intéressant seulement pour effectuer un nombre significatif de paiements afin d'amortir les frais de transaction liés au dépôt et au retrait de bitcoins sur ce réseau (transactions écrites sur la chaîne du Bitcoin).

Voici comment fonctionne le *Lightning Network* :

- on ouvre un canal avec une autre personne
- pour chaque canal (entre 2 personnes) :
  - chacun dépose une somme de bitcoin prise sur la chaîne du Bitcoin
  - on choisit la durée et nombre d'échanges possible, éventuellement infinis.
  - lorsqu'on ferme le canal, on écrit la balance sur la chaîne du Bitcoin.
- payer revient à modifier la valeur de chacun dans le canal (cela ne génère pas de trace sur la chaîne du Bitcoin d'où la perte de sécurité mais aussi la possibilité de frais très faibles).

L'astuce est qu'on peut rebondir de personne en personnes pour payer son destinataire. Ainsi il est possible d'échanger avec tous les membres du réseau. Chaque personne intermédiaire (nœud du réseau) prend au passage une petite commission. Aussi il est intéressant d'être un nœud central. C'est ce que font certains services qui offrent une application pour payer sur le *Lightning Network* en créant initialement une connexion, entre l'utilisateur et leur nœud [26].

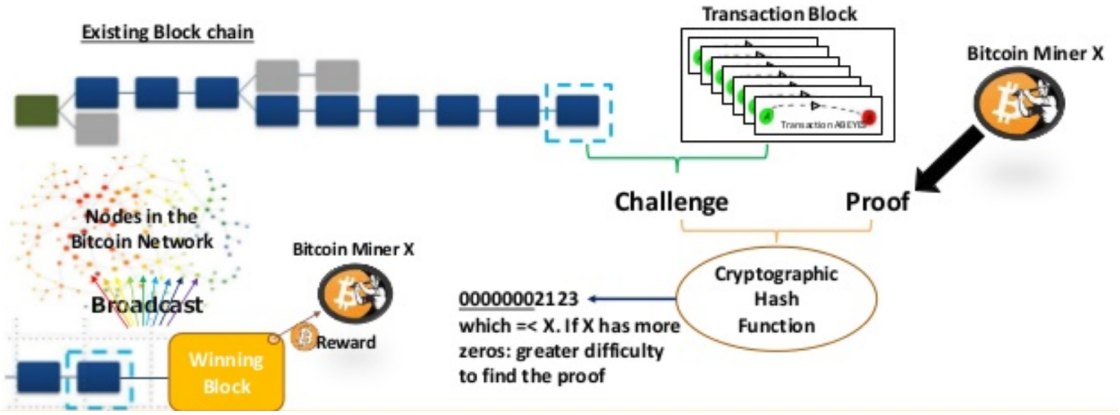
Notons qu'il est possible d'ouvrir soit même plusieurs canaux, en particulier si on a plusieurs partenaires avec lesquels on a des échanges commerciaux. L'application BitBanana offre un contrôle total sur ses connexions et donc permet cela.

26. C'est le cas de Breez ou de Phoenix.

La *blockchain*

La blockchain est souvent considérée comme la merveille de l'article de Satoshi Nakamoto qui présente le bitcoin [a].

L'idée de base est d'avoir un livre ouvert où on (les mineurs) écrit les pages (blocs) à la suite, chaque page étant liée de façon incassable à la précédente. La seule façon de casser le système est de repartir d'une ancienne page et de créer plus de nouvelles pages que le livre en a actuellement car le livre de compte de référence est celui qui a le plus de pages. Sachant qu'il y a vraiment beaucoup de personnes (ordinateurs) qui écrivent le livre, il faut être plus rapide que tous les autres réunis. A priori c'est impossible [b]. On a donc un système sans contrôleur qui garantit que personne ne triche en imposant au tricheur potentiel d'avoir une puissance de calcul supérieure à celle de toute la communauté (on appelle cela la preuve de travail ou *proof of work*).



En pratique, un mineur va prendre un groupe de transactions dans la file d'attente publique des transactions (il peut choisir celles qui paient le plus pour être validées). Il les range dans un bloc, le *Transaction Block*, avec le condensat du dernier bloc validé. Maintenant il faut qu'il trouve un nombre, *Proof*, qui combiné à ce bloc sera passé à une fonction dont le résultat doit commencer par X zéros. Pour trouver ce nombre *Proof* le mineur en essaie plein jusqu'à ce que ça marche. Il n'y a pas d'autres façons de faire. C'est cela qui est gourmand en puissance de calcul.

Une fois le nombre *Proof* trouvé, le mineur annonce publiquement son résultat qui est validé par les autres mineurs [c] et ainsi le nouveau bloc est ajouté à la *blockchain*. Si le temps nécessaire pour valider le bloc avec son nombre *Proof* a été inférieur a 10 minutes, on augmente X afin que le calcul soit plus long la prochaine fois, sinon on diminue X.

Ce mécanisme de la *blockchain* peut être appliqué à d'autres cas à tel point qu'une économie se construit sur les applications possibles de la *blockchain* (pour les notaires par exemple).

Pour plus de détails, voir Blockchain 101 - A Visual Demo.

a. https://bitcoin.org/bitcoin.pdf

b. Avec le système de regroupement de mineurs pour se distribuer les récompenses, on pourrait imaginer que cela arrive, mais cela devrait se voir.

c. Exécuter une fois la fonction est rapide, c'est le faire des milliards de fois pour trouver le bon nombre qui prend du temps.

Moralement

La grande force du Bitcoin est qu'il n'appartient à personne, donc à tout le monde. Le Bitcoin est une monnaie décentralisée. Il n'y a pas d'entreprise ou de banque derrière le Bitcoin ni même d'État. Le réseau Bitcoin est géré par tous les serveurs qui collaborent, ces derniers étant rémunérés pour cela à un prix prédéterminé par de la création de monnaie.

Une autre force du Bitcoin est qu'il s'agit d'un logiciel libre. Cela implique que la sécurité du système peut être analysée par n'importe qui et surtout que tout le monde peut développer des applications liées au Bitcoin. Ainsi on trouve de nombreuses applications pour ordinateurs et ordiphones mais aussi des applications au monde physique (il existe des pièces physiques Bitcoin).

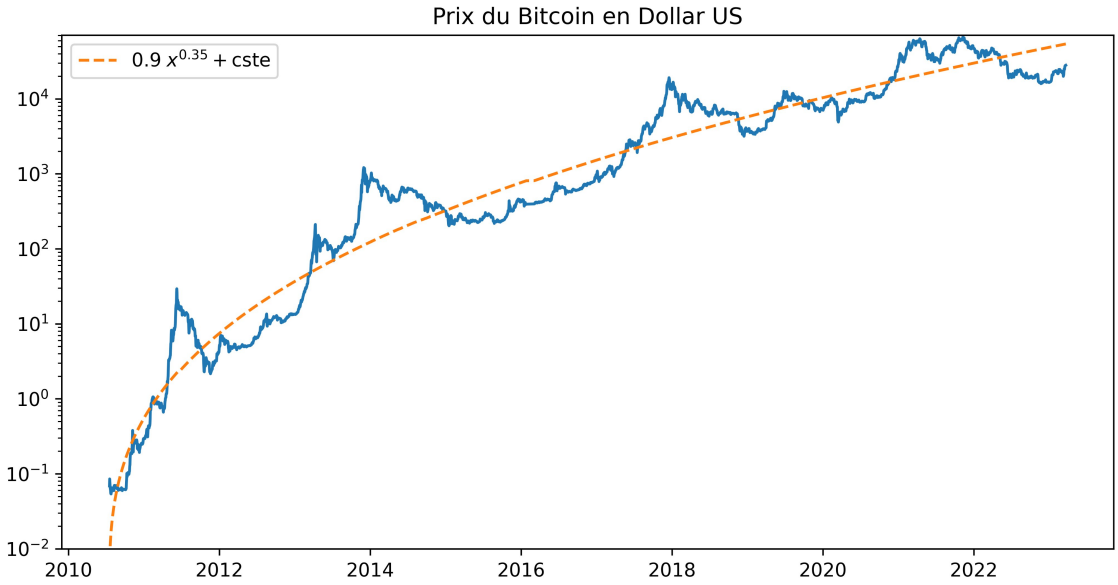


FIGURE 6.15 – Bitcoin par rapport au dollars depuis 2010

Notons enfin que la valeur du Bitcoin est celle du marché de l'offre et de la demande. Actuellement cette valeur est hautement volatile aussi il est déconseillé d'y investir plus que ce que l'on peut se permettre de perdre. On peut néanmoins constater qu'elle progresse régulièrement à long terme, cf figure 6.15, et penser qu'elle se stabilisera avec le temps.

D'ici là, sa popularité grandissante et certains événements géopolitiques ou simplement techniques en font régulièrement exploser le cours. La valorisation du Bitcoin a ainsi dépassé les 600 milliards de dollars en 2021 ce qui est 100 fois plus que l'ensemble monnaies complémentaire non étatiques en 2008, cf figure 6.9. À titre de comparaison, le dollars US, qui a la plus grosse masse monétaire du monde, pèse 1 800 milliards en 2019 [27].

Une des raisons de l'augmentation des cours est la limitation du nombre de bitcoins, nombre limité à 21 millions de par son protocole. Aussi la seule façon de répondre à la demande est d'augmenter la valeur du Bitcoin puisqu'il n'est pas possible d'émettre plus de bitcoins. Cet

27. https://www.federalreserve.gov/paymentsystems/coin_data.htm

aspect peut pousser certains à conserver leurs bitcoins en attendant que sa valeur monte, ce qui raréfie l'offre et donc pousse à la hausse. On peut donc y voir un placement spéculatif plutôt qu'une monnaie, surtout que le nombre de magasins acceptant les bitcoins reste limité.

Tous ces points rendent possible une intervention des États, ce qui aurait évidemment un impact sur le cours du Bitcoin. En août 2013 l'Allemagne a reconnu le Bitcoin comme une monnaie de transaction légale alors qu'en juillet la Thaïlande l'interdisait. En mars 2014 le fisc des États-Unis a déclaré que les bitcoins sont un bien et non une monnaie, et, en tant que tel, sont imposables sur les plus values. L'approche de la BCE est équivalente, le Bitcoin est un placement et non pas une monnaie [28].

Autre aspect moral concerne l'impact écologique du Bitcoin. La validation des transactions demande la résolution de problèmes mathématiques dont la difficulté croît avec la puissance de calcul mise en œuvre pour les résoudre. Cela implique un coût énergétique croissant avec le succès du Bitcoin et/ou le renouvellement des serveurs. Le fait que la difficulté soit liée à la puissance de calcul devrait mener à un équilibre puisqu'à partir d'un moment la part de gâteau pour chacun sera trop petite pour être rentable. Cela étant cet équilibre ne semble pas encore atteint comme le montre la courbe 6.16.

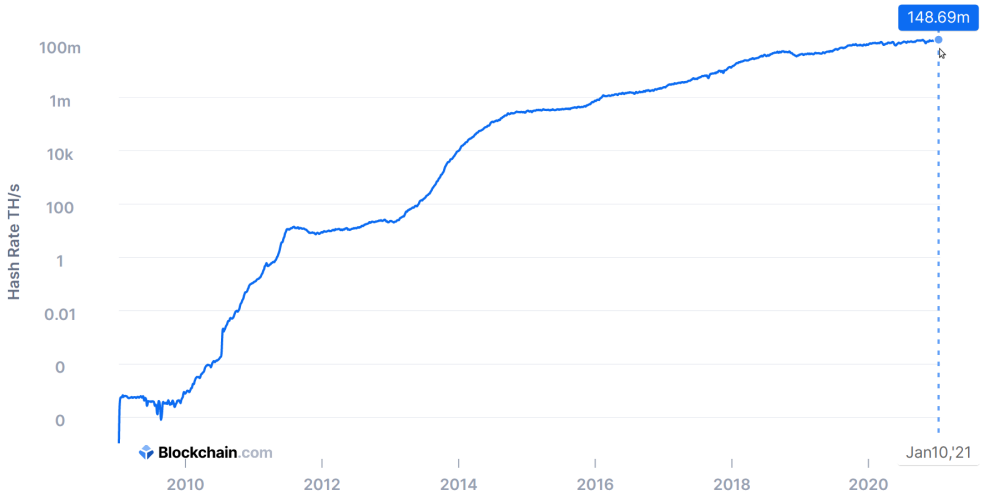


FIGURE 6.16 – Évolution de la puissance de calcul des serveurs Bitcoin

Cette puissance nécessaire pour faire fonctionner le système a donné lieu à de nombreux articles sur le gaspillage énergétique du Bitcoin. Le calcul de la consommation électrique liée au Bitcoin est délicat. S'il est possible de mesurer le nombre de cycles d'horloges il est difficile de connaître la consommation électrique, tous les ordinateurs n'ayant pas la même efficacité pouvant aller de 0,001 W-s par giga hash/s (GH/s) pour du hardware spécialisé à 19 W par GH pour un classique Raspberry Pi (chiffres de 2013). Une machine spécialisée la plus classique est l'ASIC que de nombreux mineurs utilisent. La version 2015 consomme 0,2 w/GH. Aussi une autre façon de calculer est d'évaluer le modèle financier des mineurs.

Fin novembre 2017, le gain journalier pour les mineurs est d'environ 20 millions de dollars.

28. Pour plus d'information sur la légalité du Bitcoin suivant les pays : https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory

Cela permet de consommer beaucoup d'électricité tout en dégageant des bénéfices. Pour avoir un ordre de grandeur, 1 MW.an coûte environ 1 million de dollars en consommation de base. Certains annoncent que les mineurs dépensent 60% de leurs revenus en électricité ce qui permet au rythme d'aujourd'hui de dépenser 12 millions par jours soit 4,4 G$ par an donc 4,4 GW.an ou 38,5 TWh, soit presque la consommation annuelle de la Hongrie (40 TWh d'après le rapport 2017 de l'IEA).

Le site dédié de Cambridge qui affiche arrive à des chiffres similaires [29] et annonce une consommation annuelle de 130 TWh à la mi-2023 (les Pays-Bas consomment 110 TWh / an).

Il y a donc un véritable problème écologique qui n'existe que pour garantir que personne ne puisse fausser les transactions et non pas pour réaliser les transactions. D'autres crypto-monnaies basées sur d'autres systèmes de validation des transactions qui n'ont pas ce problème.

6.6.3 L'Éthereum

Dans le monde des crypto-monnaies, la plus importante après le Bitcoin est l'Éther, la monnaie du réseau Éthereum.

La technologie Éthereum se base sur un ordinateur virtuel, l'EVM [30], qui permet d'exécuter des contrats dit intelligents, *smart contract*, écrits en langage informatique. Ces contrats sont la grande idée de l'Éthereum. Il s'agit de contrats financiers, ou ayant un aspect financier, qui s'appuient sur la monnaie de l'Éthereum. On peut citer comme exemple de contrat une enchère qui remettra automatiquement la plus haute enchère au vendeur, une caution qui rend l'argent si les termes du contrat sont respectés, un ticket d'entrée qui donne le code dès qu'il reçoit l'argent etc. Les possibilités sont infinies. Pour garantir le bon fonctionnement des contrats, ils sont écrits dans la *blockchain* d'Éthereum sans possibilité de les modifier. L'ordinateur virtuel d'Étherum exécute les contrats tout comme les mineurs du Bitcoin enregistrent les transactions. Ainsi il n'est plus nécessaire d'avoir des tiers de confiances (avocat, banque, intermédiaire...) puisqu'on a un système automatique inviolable.

Mais s'il est possible d'exécuter du code sur l'infrastructure d'Éthereum, pourquoi se limiter à des contrats financiers et pourquoi ne pas exécuter de véritables programmes informatiques, des jeux par exemple ? C'est possible mais avec deux limites :

— Le code d'un contrat est exécuté sur l'EVM qui est une machine très lente car fortement redondante (pour des raisons de sécurité). Éthereum annonce que l'EVM est 1 million de fois plus lente que sur une machine classique. Le stockage aussi coûte cher.
— Une erreur de programmation dans un contrat peut coûter une fortune, le code est visible et les pirates adorent exploiter les erreurs dans les contrats [31].

Aussi il existe les *dapps* ou *decentralized applications* qui mettent le début de leur programme (ou l'API) dans la chaîne d'Éthereum avec un lien vers le cœur du programme qui tourne sur

29. Cambridge Bitcoin Electricity Consumption Index : https://ccaf.io/cbeci/
30. L'*Ethereum Virtual Machine*
31. cf cette liste de failles : https://ventral.digital/posts/2022/12/15/ethereum-smart-contract-auditors-2022-rewind

un serveur quelque part sur Internet. Ainsi les frais d'exécution sont limité au lancement du programme et une erreur dans le programme n'a d'impact que sur le serveur, ce qui peut être corrigé facilement. Il en est de même pour les données, une *dapps* peut choisir de stocker ses données sur son serveurs et certaines données importantes dans la chaîne, ce qui mène aux fameux NFT dont on parlera.

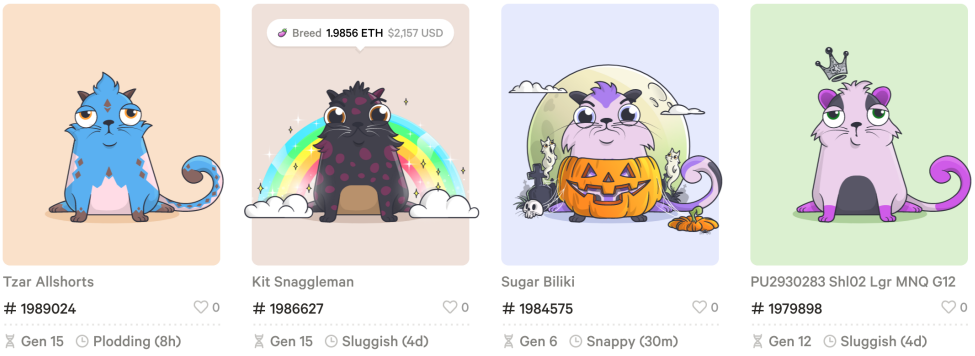


FIGURE 6.17 – CryptoKitties
Une *dapps* pour acheter et faire un élevage de chats.
L'ADN de chaque chat et son propriétaire sont stockés dans la chaîne.

En pratique les contrats sont exécutés lorsqu'ils sont intégrés au sein d'un bloc de la chaîne. Il est également possible d'indiquer qu'on désire exécuter un contrat déjà enregistré dans la chaîne. Par exemple on peut enchérir sur une enchère en donnant l'adresse du contrat et la somme qu'on propose. Cette action est elle-même un contrat, un contrat qui appelle un autre contrat (l'enchère).

Il est également possible de programmer des actions dans le futur en s'appuyant sur un contrat comme l'Ethereum Alarm Clock [32] qui déclanchera notre contrat à la date voulue [33].

Enfin, le contrat le plus simple est un versement d'Éther. L'Éther étant à la base des contrats financiers, il est devenu une monnaie d'échange voire de spéculation comme le Bitcoin. Il est aussi très volatile, comme le Bitcoin.

Comme tous les contrats n'ont pas la même taille ni la même complexité, est il logique que leur exécution sur l'EVM génère des calculs plus ou moins importants. Aussi chaque opération d'un contrat a un coût exprimé en gaz (cf l'encart sur le gaz page 32 pour plus de détails). On a donc deux coûts : celui pour que sa transaction soit prise, c.a.d. que son contrat soit lancé, et celui de l'exécution du contrat. Ces deux coûts sont fusionnés en un : le prix du gaz. Ainsi une personne qui veut lancer un contrat à 21 000 gaz (un versement en éther) indique qu'il est prêt à payer 30 nano-éther pour 1 gaz. Si ce prix est plus cher que le prix du marché, alors son contrat sera exécuté en priorité.

32. https://github.com/ethereum-alarm-clock/ethereum-alarm-clock
33. En octobre 2023 une faille a été découverte dans l'Ethereum Alarm Clock et elle n'a pas été corrigée depuis. Il est possible que Chrono Logic, l'entreprise qui avait développé ce système, soit morte.

Les contrats intelligents ou *smart contracts*

Ces petits programmes informatiques sont la réussite d'Éthereum. Inscrits dans la chaîne et exécuté sur l'EVM (*Éthereum Virtual Machine*), ils sont :

— transparents, tout le monde peut lire leur code
— immuables, il sont gravés dans la chaîne et ne peuvent être effacés ou modifiés → ils peuvent être réutilisés (appelés)
— déterministes
— de taille maximale de 24 kB (contournable)

Les contrats sont écrits dans des langages dédiés comme Solidity ou Vyper[a]. Voici un exemple de système d'enchère avec une limite temporelle :

Solidity

```
pragma solidity ^0.4.25;

contract OpenAuction {

    address public beneficiary;
    uint public auctionStart;
    uint public auctionStop;
    bool public ended;
    uint public highestBid;
    address public highestBidder;

    constructor (address _beneficiary, uint _biddingTime) public {
        beneficiary = _beneficiary;
        auctionStart = now;
        auctionStop = auctionStart + _biddingTime;
    }

    function bid() public payable {
        assert(now < auctionStop);
        assert(msg.value > highestBid);
        if (highestBid != 0) {
            highestBidder.transfer(highestBid);
        }
        highestBid = msg.value;
        highestBidder = msg.sender;
    }

    function endAuction() public {
        assert(now >= auctionStop);
        assert(!ended);
        ended = true;
        beneficiary.transfer(highestBid);
    }

}
```

Vyper

```
# Open Auction contract

beneficiary: public(address)
auctionStart: public(timestamp)
auctionStop: public(timestamp)
highestBid: public(wei_value)
highestBidder: public(address)
ended: public(bool)

# constructor
@public
def __init__(_beneficiary: address, _bidding_time: timedelta):
    self.beneficiary = _beneficiary
    self.auctionStart = block.timestamp
    self.auctionStop = self.auctionStart + _bidding_time

# create function for bidding
@public
@payable
def bid():
    assert block.timestamp < self.auctionStop
    assert msg.value > self.highestBid
    if not self.highestBid == 0:
        send(self.highestBidder, self.highestBid)
    self.highestBid = msg.value
    self.highestBidder = msg.sender

# end auction and send the highest bid to the beneficiary
@public
def endAuction():
    assert block.timestamp >= self.auctionStop
    assert not self.ended
    self.ended = True
    send(self.beneficiary, self.highestBid)
```

La partie violette déclare les variables que l'on pourra consulter et qui donne l'état de l'enchère, en jaune le constructeur puis les fonctions en vert. Ce code est ensuite compilé pour donner deux parties :

— une description lisible pour utiliser le service, l'ABI ou *Application Binary Interface*
— le code, bytecode, qui sera exécuté sur l'EVM.

Il ne reste plus qu'à les déployer, payer le coût en gaz et c'est parti, chacun peut faire des enchères.

a. Solidity est le langage initial des contrats, il est proche de JavaScript. Vyper, proche de Python, est arrivé par la suite avec une volonté de réduire le risque de produire du code avec une faille de sécurité.

Du Gaz dans l'Éther

Pour faire exécuter un contrat dans l'Éthereum, il faut payer les mineurs dont les ordinateurs vont effectuer les calculs. Le prix est défini en Gaz avec un prix fixe pour différentes opérations. Le prix du Gaz s'exprime en GWei c.a.d. 10^9 Wei, un Wei étant la plus petite unité de l'Éther à savoir 10^{-18} ETH.

Opération	Prix en Gaz
une addition	3
une multiplication	5
une comparaison	3
état d'un compte	700
charger un *mot* de la mémoire	800
sauver un *mot* en mémoire	20 000
transférer des ETH	21 000

TABLE 6.2 – Exemples de prix des opérations sur l'Éthereum

Le cours du Gaz est variable et suit l'offre et la demande. Si vous désirez que votre contrat s'effectue rapidement, vous indiquez que vous êtes prêt a payer cher le Gaz, à l'inverse s'il n'y a pas urgence, vous pouvez payer moins cher (cf https://etherscan.io/gastracker pour le prix courant à payer suivant l'urgence). Début 2021 le prix du Gaz est cher, il a décuplé en 2020 pour atteindre 100 GWei ce qui fait le Gaz à 0,01 centime d'euro avec un éther à 1000 €. Un transfert d'éther coûte donc 2,1 € en janvier 2021. Été 2023, le prix du gaz est à 33 GWei et le cours à 1700 €, donc le transfert d'éther est à 1,2 €. Dans les deux cas, c'est bien trop cher pour les micro-paiements.

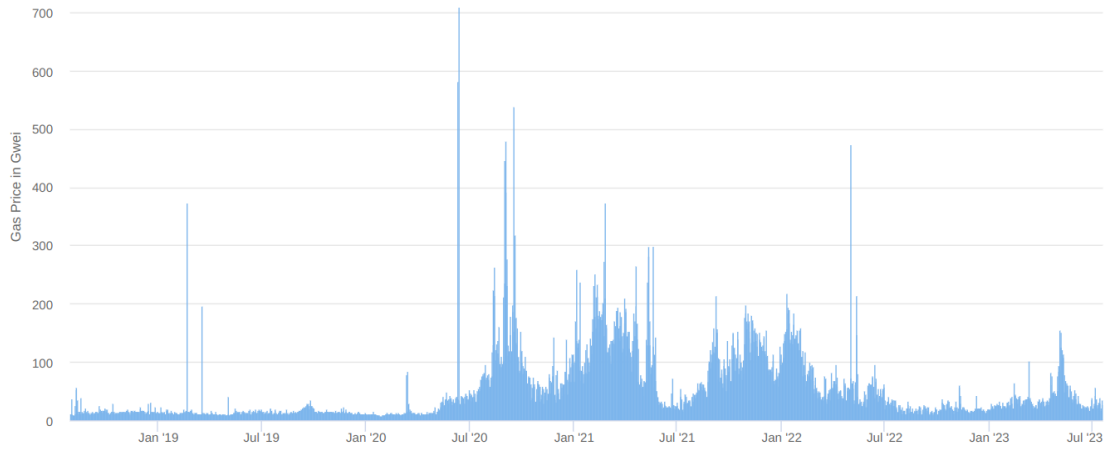


FIGURE 6.18 – Prix moyen du Gaz
source : Etherscan

La finance dématérialisée – DeFi

Comme on l'a vu la force de l'Éthéreum est ses contrats intelligents qui permettent de programmer des opérations financières (entre autres). Aussi un nouveau type de finance s'est développé en dehors des banques, salles de marché et autre entités financières. Il a néanmoins ses propres acteurs et une infrastructure complexe que ce schéma résume :

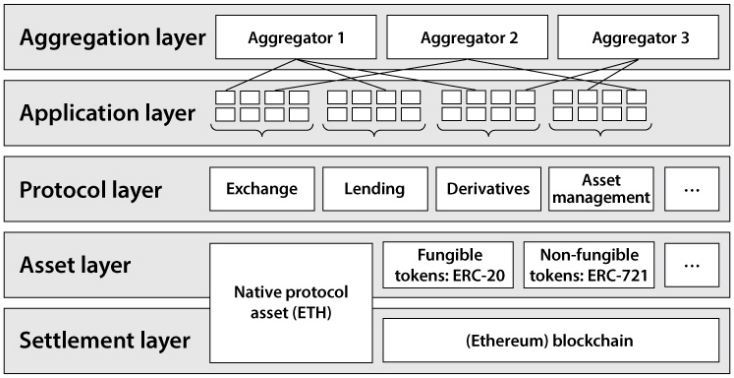


FIGURE 6.19 – Schéma en couches de la DeFi
auteur : Fabian Schär

La base est la chaîne Éthereum. Ce n'est pas une obligation mais de fait c'est la chaîne la plus utilisée. Vient ensuite la couche des biens avec le jetons fongible ou pas. Puis les protocoles présentent en filigrame les contrats. Au dessus on trouve les applications web ou sur ordiphones qui utilisent ces contrats. Enfin les aggrégateurs fusionnent plusieurs services de base en services financiers complets.

Au niveau des biens on trouve deux normes fondamentales. L'ERC-20 est à la base de milliers de jetons de toutes sortes. Il y a des jetons qui sont d'autres crypto-monnaies, d'autres sont des jetons de votes, des jetons de jeux, de lotteries... En juillet 2023, on recense [34]

— 12 jetons ERC20 dont la masse monétaire > 1 G$
— 96 jetons ERC20 dont la masse monétaire > 1 M$

Le jeton ERC-721 plus connu sous le nom de NTF, *Non Fungible Token*, est la références pour enregistrer les œuvres numériques. Parmi les plus célèbres, citons les cryptopunks et les *Bored Apes* qui représentent de petites images qu'on peut utiliser comme avatar. Chacune vaut des dizaines voire des centaines de milliers d'euros en 2023. On peut en acheter sur OpenSea, une des plateformes d'enchère pour les NFT.

Au niveau supérieur, voici quelques exemples de contrats financiers :

— La monnaie stable (*stable coins*) peut utiliser des contrats pour garantir la parité avec une autre monnaie (souvent le $).
— Le contrat permettant d'emprunter des euros en mettant en caution une crypto-monnaie.
— Le contrat gardien qui redistribue l'argent entre les parties que si elles sont d'accord sur la répartition.

34. https://www.coinlore.com/token-types/erc20

Les monnaies stables Les *stable coins* joue de rôle de stabilisateur afin de pouvoir faire de la finance dématérialisée sans les risques liés à la variabilité des crypto-monnaies. Leur rôle est donc très important.

La mécanique qui permet de lié un jeton à une monnaie fiat comme le dollar, peut être basée sur une crypto-monnaie de référence ou une monnaie fiat. Dans le premier cas la technique consiste à demander une caution de la crypto-monnaie de référence nettement supérieure à la somme considérée afin de pouvoir vendre la crypto-monnaie si elle baisse trop et récupérer la somme considérée. Le second cas est plus simple, puisqu'en cas de vente du jeton stable, on prend l'équivalent dans les stocks de monnaie fiat (sauf si l'émetteur du jeton a émis plus qu'il n'a de réserves...). Ainsi on a parmi ces monnaies stables :

- jeton avec caution dans la chaîne (la crypto-monnaie de réféence) :
  - le DAI est cautionné en ETH (1 DAI = 1 $ avec une caution = 150 % de la somme désirée en DAI)
  - le WBTC est cautionné en bitcoin (1 WBTC = 1 btc)
- jeton avec caution hors chaîne :
  - les USDT et USDC sont cautionné en $ dans une banque (1 USDx = 1 $)
  - le PAXG est cautionnés en or (1 PAXG = 1 once d'or)

La somme des cautions, pour les monnaies stables mais aussi pour d'autres opérations, est une façon de mesurer l'activité de la DeFi :

FIGURE 6.20 – Total des sommes en caution de la DeFi et valorisation des monnaies stables
source : DEfiLlama

Le crash de mars 2022 est lié à la chute de la chaîne Terra et de ses monnaies Luna et UST. UST était une monnaie stable arrimée au dollar et Luna était sa crypto-monnaie de référence (caution). La mécanique était qu'on pouvait toujours échanger x Luna pour leur valeur en UST et inversement. Aussi si l'UST baisse à 0,99 $, on peut acheter 100 UST pour 99 $, puis avec on achète x Luna que l'on revend pour 100 $ et on gagne 1 $. Le fait d'avoir acheter des UST fait remonter son cours.

En mai 2022, la monnaie stable UST a décroché suite à des ventes importantes et plutôt que d'en profiter comme on vient de voir, les investisseurs ont eu peur ce qui a entrainé une panique qui a fait chuter Luna de 80 $ à 0,01 cents, ce qui achevé l'UST qui s'est totalement effondré. Sachant que l'UST était une monnaie stable majeure, le total de sommes en caution dans la DeFi a été divisé par deux.

En 2023, la DeFi ne s'est pas remise de ce crash et la question de la confiance qu'on peut avoir en des monnaies stables basées sur des crypto-monnaies est toujours d'actualité (notons que le DAI qui a un fonctionnement différent n'a pas bougé, y compris durant cette crise).

Reconstruire Wall Street

La DeFi a besoin de certaines infrastructures financières de la TradFi [35].

Les plateformes d'échange Étant donné le nombre de crypto-monnaies et d'autres actifs, il est important de pouvoir les échanger sans devoir repasser par des dollars ou des euros à chaque fois. Aussi il existe des plateformes d'échanges centralisées, un site web usuel où on achète ses crypto-monnaies et où on peut passer d'une crypto à un autre, et des plateformes d'échange décentralisées qui utilisent des contrats pour échanger des cryptos. La force des premières est leur simplicité d'accès, leur faiblesse est que si elles meurent, leurs clients perdent leurs avoirs.

Les DEX [36] à l'inverse ne possèdent pas les avoir des échanges, par contre elles disposent de réserves qui permettent justement d'effectuer ces échanges. Un des fonctionnements des DEX est d'avoir une cagnotte avec 2 monnaies qui s'équilibre automatiquement en liant les cours aux réserves :

Soit x et y les reserves des 2 monnaies. On veut avoir toujours $x\,y = k$ avec k une constante. Donc si je donne Δx alors je reçois en échange Δy ainsi calculé :

$$(x + \Delta x)\,(y - \Delta y) = k \quad \Longrightarrow \quad \Delta y = y - \frac{k}{x + \Delta x}$$

Si je mets autant que la réserve de la première monnaie, $\Delta x = x$ alors je ne récupère que la moitié de la réserve de la seconde monnaie $\Delta y = y/2$. Pour tout prendre, $\Delta y = y$, il faut mettre une infinité, $\Delta x = \infty$. Le système est fait pour des échanges Δx petits par rapport à la taille de la réserve, sinon les prix s'envolent. Ce comportement permet une triche connue pour générer des prix anormaux dans l'espoir de récupérer ses gains ailleurs (cf ci-dessous). Bien sûr un tel prix anormal sera rapidement corrigé par d'autres investisseurs qui feront une bonne affaire en équilibrant cette DEX avec une autre, cf figure 6.22.

Les oracles Une des grandes faiblesses de la chaîne Éthereum est qu'elle ne sait rien du monde. Pourtant ce qui se passe dans le monde physique est très important pour la finance. Comment faire de la finance sans son flux Bloomberg? Si je veux construire un contrat qui enregistre les paris d'un tournois sportif, il faut que mon contrat sache de façon certaine qui a gagné tel match pour distribuer les gains.

Aussi on a construit les oracles dont le travail est d'enregistrer dans la chaîne des informations de l'extérieur [37], ce qui permet ensuite aux contrats de prendre en compte la donnée pour agir. Bien sûr, il faut avoir confiance en l'oracle pour être certain que le contrat fonctionne bien. Si l'oracle triche, ou si des personnes assez riches génèrent un micro-crash sur un DEX qu'utilise un oracle comme référence, alors le contrat se trompera (probablement en faveur des

35. Finance Traditionnelle
36. Decentralized EXchange
37. un oracle peut aussi sortir des informations de la chaîne comme des statistiques sur certains usages.

tricheurs). Aussi il est préférable d'utiliser plusieurs oracles pour travailler en toute confiance. Ainsi pour connaître le cours de l'ether dans un contrat, on regarde les valeurs entrées par un ensemble d'oracle et on prend la moyenne, cf figure 6.21.

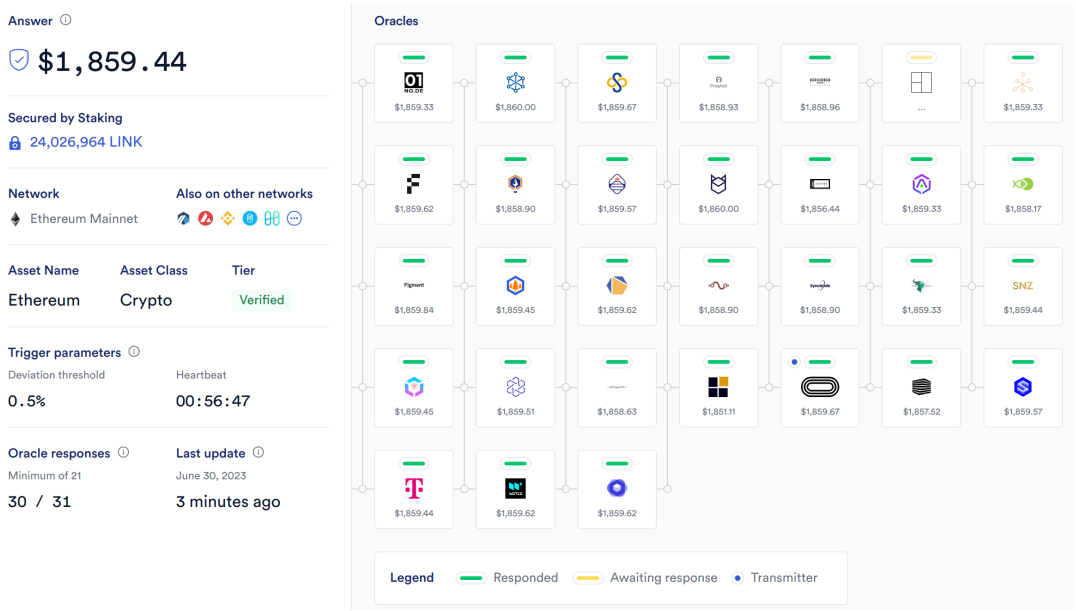


FIGURE 6.21 – Prix de l'Ether en dollars auprès d'un ensemble d'oracles
https://data.chain.link/ethereum/mainnet/crypto-usd/eth-usd

Equilibrer les DEX Parmi les contrats existants, les contrats d'emprunts sont bien utiles pour emprunter de la monnaie fiat en mettant en caution de la crypto-monnaie [38].

Dernièrement l'emprunt flash a été crée pour emprunter sans caution et rembourser en même temps, ou disons au sein du même bloc. Cela permet d'avoir l'argent pour faire une opération financière très rapide, prendre le bénéfice et rembourser. Ainsi on peut dans un seul bloc, emprunter, acheter sur une DEX, vendre sur une autre et rembourser, cf figure 6.22. Le bon coté pour le système est que cela permet que tous les DEX affichent les mêmes valeurs de change.

Il est également possible de refinancer une crypto dette avec un emprunt flash. Il suffit de faire un emprunt flash, rembourser sa dette, récupérer la caution et ainsi pouvoir faire un nouvel emprunt à un meilleur taux puis rembourser l'emprunt flash avec la somme empruntée. Tout cela au sein d'un bloc.

38. Pour ce type d'emprunt, la caution est supérieure à la somme empruntée et le contrat vend automatiquement la caution pour rembourser le prêteur si le cours de la crypto-monnaie baisse assez pour que la caution ne vaille que la somme empruntée.

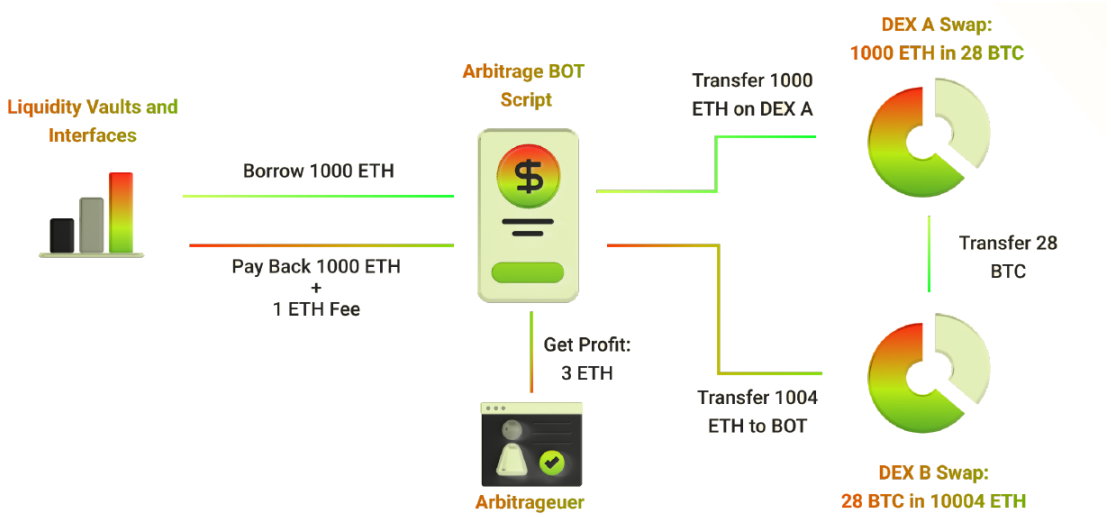


FIGURE 6.22 – Emprunt flash pour équilibrer deux DEX

Éthereum 2.0

Le fonctionnement du choix des transactions à valider ainsi que le mécanisme de preuve était les mêmes que pour le Bitcoin, à savoir qu'on utilisait la preuve par travail. Depuis fin 2022, Éthereum a choisi de passer à la preuve par enjeux (*proof os stakes* ou PoS).

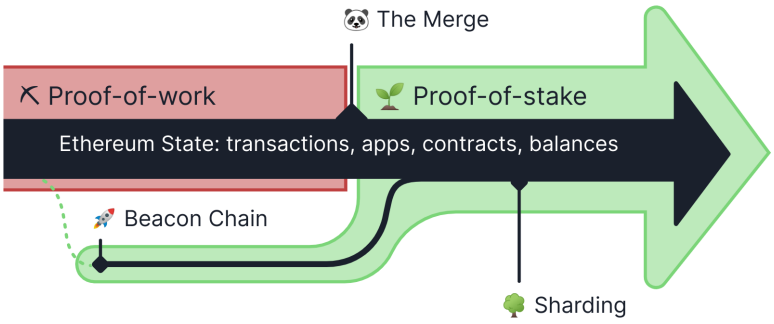


FIGURE 6.23 – Changement de méthode de preuve pour l'Éthereum

L'équivalent des mineurs s'appelle les validateurs dans la preuve par enjeux. On devient validateur en bloquant 32 éthers et en ayant un ordinateur qui participe au travail de validation.

Le principe de base de la preuve d'enjeu consiste à tirer au sort qui, parmi les validateurs, va valider le prochain bloc. L'idée est que les validateurs n'ont pas envie de détruire le système qui leur appartient, donc que le validateur écrira de façon honnête le prochain bloc. Il sera rémunéré pour ce petit travail ce qui revient à rémunérer l'argent mis en dépôt pour avoir le droit de valider les blocs (bien plus faible que la rémunération des mineurs du Bitcoin car il n'est plus besoin de rémunérer une consommation électrique folle).

Cela étant il y a des failles dans ce système si on l'applique tel quel. Le mineur peut vouloir optimiser ses gains et pour cela valider des blocs de différentes branches de la *blockchain*, les fausses comme la vraie, avec l'idée que si une fausse devient la plus longue, sa participation sera rémunérée. Aussi pour lutter contre cette stratégie, valider un bloc d'une mauvaise branche sera puni et entraînera une amende. Ainsi valider toutes les branches n'est plus rentable et il vaut mieux se focaliser sur le bonne.

D'autres types d'attaques ont été imaginé, comme l'achat d'assez de possesseurs pour les convaincre de tricher ensemble et donc avoir le poids pour écrire une fausse *blockchain*. Normalement Éthereum a pensé à tout mais seul l'avenir pourra le dire.

Du point de vue écologique, ce nouveau système est un véritable succès comme le montre le comparatif figure 6.24. En passant de la preuve par le travail à la preuve par enjeux, le système de validation de l'Éthereum a fait passer sa consommation de 78 TWh / an à 2,6 GWh / an. On est passé de la consommation de la Belgique (2022) à celle de 500 foyers français.

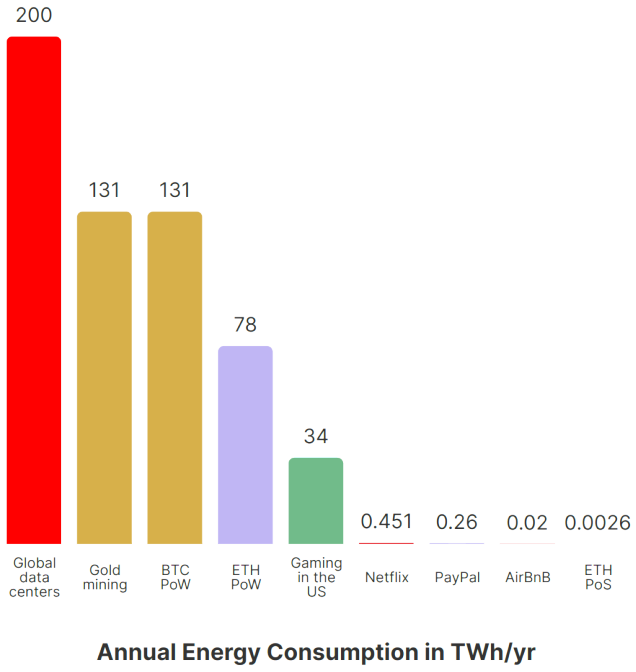


FIGURE 6.24 – Comparaison de la consommation électrique de l'Éthereum (PoW et PoS).

Des réseaux de niveau 2 (L2)

Comme pour le Bitcoin, l'Éther n'est pas adapté aux micro-transactions à cause du coût trop élevé des transactions. Aussi on applique la même solution avec des réseaux de niveau 2 qui travaillent dans leur coin et viennent inscrire des données dans la chaîne de l'Éthereum de temps en temps pour profiter de la sécurité qu'elle offre. Cela permet de résoudre le trilème des chaîne de bloc à savoir :

Une chaîne de bloc ne peut résoudre simplement 2 de ces 3 points mais le troisième sera

toujours très difficile :

— la sécurité
— la décentralisation (pas de nœud central, pas de chef qui choisit)
— le passage à l'échelle (accepter toujours plus de transactions)

Éthereum remplit les 2 premiers mais plafonne à 1 M transactions / jour.

D'autres réseaux, de niveau 2, s'appuient sur la *blockchain* d'Ethereum pour sa sécurité et peuvent ainsi remplir les 2 autres critères.

Optimism, Arbitrum ou Polygon en sont des exemples. Les 3 sont aussi des EVM mais avec des coûts (gaz) nettement inférieurs.

Rollup Une façon de baisser les coûts s'appelle le *rollup*. Cela consiste à

1. faire 100 transactions sur un réseau de niveau 2,
2. enregistrer la trace sur Ethereum (presque 100 fois moins cher).

Il existe 2 manières de faire cela.

Optimiste	Zéro connaissance
— L2 publie les transactions (supposées correctes) — une compression est enregistrée sur L1 — un délais permet à quiconque de montrer une faude — si fraude, alors on annule et on punit le tricheur — sinon, c'est validé	— L2 enregistre les transactions — une preuve de leur validité est envoyée dans L1 Fabriquer la preuve est un calcul difficile et donc faire une EVM compatible (zkEVM) est compliqué.

La méthode optimiste est simple à mettre en œuvre mais elle oblige à surveiller ce qu'on n'a pas tous envie de faire. De plus le délais pour dénoncer une tricherie, délais d'une semaine par exemple, ralentit nettement les transactions.

Aussi la méthode zéro connaissance est préférable si elle marche. Des évolutions prometteuses de zkEVM laissent à penser que le *rollup* zéro connaissance pourrait prendre son envol en 2023.

L2 + jetons + NFT = jeux On sent qu'on a un combo gagnant. Un niveau L2 offre la vitesse nécessaire et des frais assez faibles pour permettre des transactions fluides dans un jeux en ligne. Les jetons peuvent être une monnaie qui permet d'acheter dans le jeu et en dehors du jeu, quand aux NFT ils sont le support naturel pour les objets voire les personnage du jeu. On peut ainsi imaginer un joueur monter un personnage à un niveau 10 et le revendre, avec les jetons, à un autre joueur. Tout ce qui peut se construire, s'acheter et se vendre dans un jeu produit une économie dont les concepteurs du jeu contrôlent les rouages et peuvent prendre

une commission sur les transactions. Ainsi vous avez un jeu à l'entrée libre mais lucratif tant pour les concepteurs que pour les meilleurs joueurs.

On retrouve cette mécanique dans le jeu Axis Infinity qui a été un énorme succès jusqu'en mars 2022 lorsque le jeu s'est fait voler l'équivalent de 620 M$ en ether et USDC. Cela a fait chuter la valeur du jeton du jeu de 99% et le nombre de joueur est passé de 2,7 millions à environ 250 000.

Pour certains, le fait que les nouveaux joueurs achètent des personnages à des joueurs plus avancés et donc que le système a besoin de nouveau entrants pour que l'économie fonctionne, est proche d'une pyramide de Ponzi.

6.6.4 Les bébés Bitcoin

Le succès du Bitcoins, ses faiblesses et le désir de créer la crypto-monnaie qui offre les bonnes spécifications, ont poussé à la création de monnaies alternatives basées sur les principes du Bitcoin. Il existe aussi beaucoup de crypto-monnaies créées simplement pour enrichir ceux qui les lancent (c'est simple à faire puisque le code du bitcoin est ouvert).

Le site CoinChoose liste les monnaies vivantes (134 début 2020). On peut choisir une monnaie en fonction de sa popularité et donc de la possibilité de l'utiliser réellement comme monnaie, en fonction de ses caractéristiques avec le désir de promouvoir la « bonne » monnaie ou en fonction du rendement espéré pour spéculer. Le site Coin Market Cap présente chaque monnaie de façon complète ce qui permet aussi de se faire un avis.

Voici une présentation rapide de quelques monnaies alternatives au Bitcoin et à l'Éther et leurs spécifications :

— Le Ripple (XRP) est une des premières crypto-monnaies rattachée à une entreprise qui veut interagir avec les banques. Un procès pour création abusive de pièces est probablement une des raisons de sa baisse depuis 2018.
— Le Bitcoin Cash (BCH) est le fruit d'une scission majeure du Bitcoin en août 2017 pour amméliorer les transactions. En tant que scission il reprend le livre de compte des Bitcoins au 1er aout 2017 et donc tous les possesseurs de Bitcoins à cette date sont automatiquement possesseurs de Bitcoin Cash. Le succès initial est passé et la baisse régulière.
— Les Litecoin (LTC) est une copie du Bitcoin avec des transactions plus rapides et une masse monétaire finale plus grande.
— les Monero (XMR) est une monnaie qui désire offrir le plus grand anonymat possible.
— Le Dogecoin est initialement présenté comme une blague avec l'image du mème Doge. L'intérêt déclarée par Elon Musk pour cette monnaie lui a fait prendre un envol inattendu avant de retomber sèchement.
— Le Tether (USDT) est une crypto-monnaie stable ancrée au dollar US : 1 USDT = 1 $.

L'entreprise Tether Limited permet cette stabilité en garantissant qu'elle peut racheter tout tether avec des dollars. Cependant avec le temps on s'est rendu compte que cette affirmation est fausse, que non seulement Tether Limited n'a pas les fonds le permettant mais en plus rien ne l'oblige de rembourser contractuellement. Quoi qu'il en soit, le Tether a tenu et est stable.

— Le Dai est une autre crypto-monnaie stable dont la valeur est toujours 1 $. Plus précisément il s'agit d'un contrat Éthéreum dans lequel l'utilisateur qui fabrique des Dais met en gage des crypto-monnaies pour assurer la stabilité (laquelle est garantie tant que le système ne craque pas).

Notons que certaines monnaies très populaires ont vu leur cours s'effondrer voire tomber à zéro. En 2022, le cours de Luna est ainsi a chuté de 80 $ à rien en une semaine, générant 60 milliards de dollars de perte.

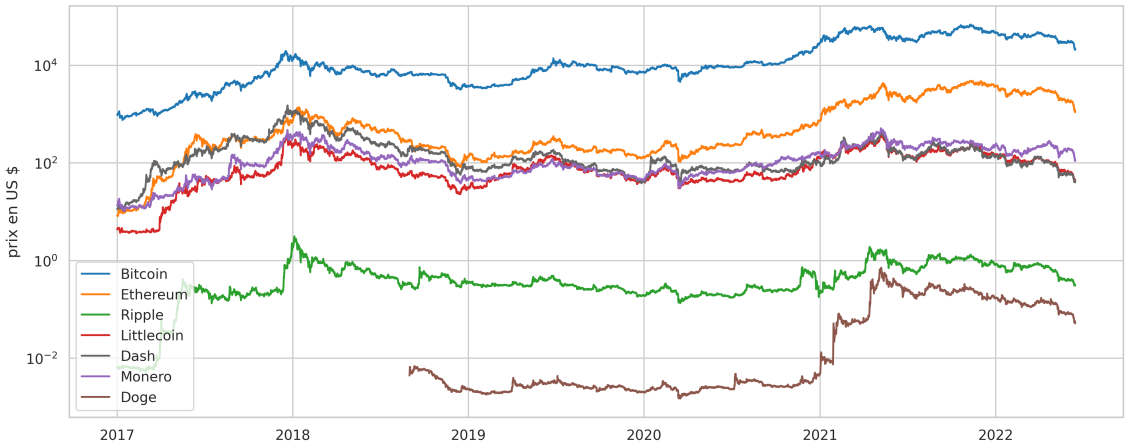


FIGURE 6.25 – Cours en dollars de quelques crypto-monnaies

De nouvelles monnaies sont régulièrement crées. Il est toujours tentant d'y participer au début en comparant aux débuts du Bitcoin et des autres monnaies qui ont "réussi" mais attention aux risques que la monnaie soit abandonnée et que votre investissement disparaisse dans la poche de ceux qui l'ont créée.

Plus

Pour en savoir plus sur les crypto-monnaies :

— le blog de Jacques Favier la voie du Bitcoin regarde avec son œil d'historien cette nouvelle monnaie et les réactions qu'elle suscite.
— le site web d'Éthereum est riche et bien écrit,
— les sites web d'information sur les crypto-monnaies : CoinDesk et le CoinTelegraph pour suivre l'actualité.