mon livret C

Formation crypto-actifs

Cryptographie, Web3 et Monnaies numériques:

Aux origines des crypto-actifs.

Novembre 2022

I - La monnaie et la cryptographie : des destins liés

À l'origine, la cryptographie est définie comme la discipline permettant la transformation, au moyen d'un algorithme de chiffrement, d'un message dit clair en un message chiffré.

Concrètement, **l'objectif est de s'assurer de l'authenticité, de l'intégrité et de la confidentialité de tout échange d'informations entre un groupe défini de personnes.** Chaque donnée transmise devient donc incompréhensible et inexploitable pour autrui.

Si la plupart de ses évolutions datent du XXème siècle, ses premières applications remontent à l'antiquité. Jules César avait ainsi créé sa propre règle de chiffrement (le fameux "chiffre de César") pour anonymiser ses correspondances privées, tandis que d'autres recherches, plus anciennes, témoignent du chiffrement d'une recette de… poterie, dès le XVIème siècle av. J.-C.

Comme souvent, c'est ensuite sur le terrain militaire que la technologie se développe. Au cours de la Seconde Guerre mondiale, elle devient une composante importante de l'attirail technologique allemand via notamment la machine Enigma, à laquelle le scientifique britannique Alan Turing apportera une réplique décisive pour la victoire des Alliés.

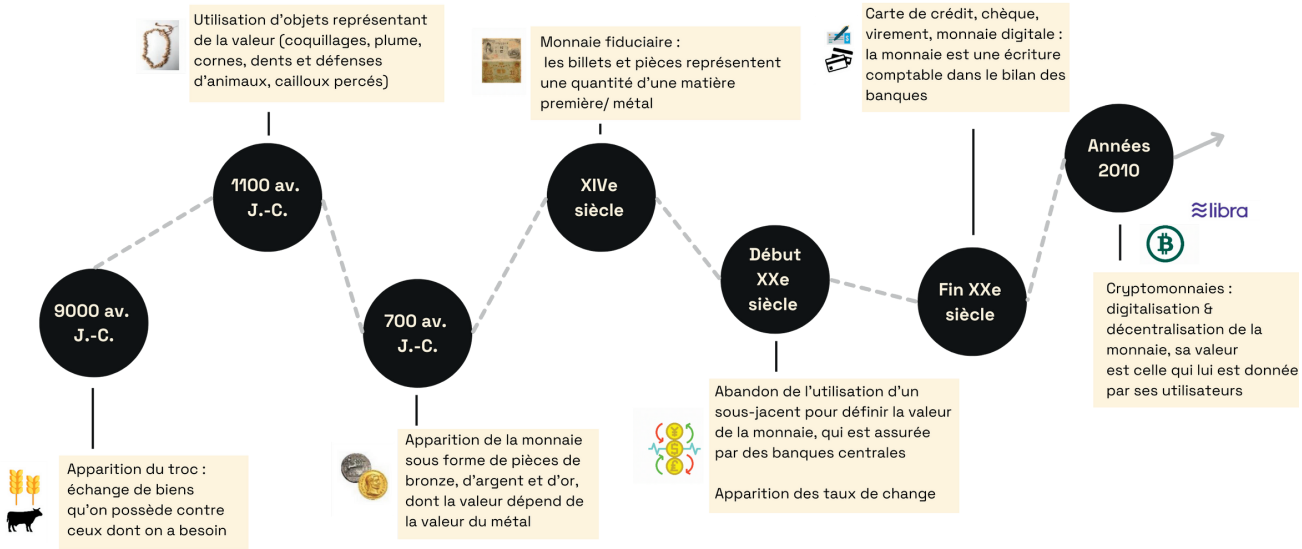
En parallèle, **la monnaie, elle aussi, se révolutionne au fil des époques.**

Du troc aux coquillages et des pièces d'or aux billets, tout bascule en 1971 lorsque ces derniers, auparavant indexés sur des réserves d'or, ne reposent alors plus sur… rien du tout, à la fin des accords de Bretton Woods.

La monnaie devient une simple écriture comptable dans le bilan des banques, et surtout, se centralise par l'intermédiaire de puissants établissements financiers eux-mêmes dépendants des Banques Centrales, seules responsables de l'émission ou non de liquidités financières.

Un mouvement économique néolibéral, l'École autrichienne, se développe alors sous l'impulsion de Friedrich August von Hayek. Celui-ci prône le développement de monnaies privées, soumises à la loi du marché et au principe de libre-concurrence. Des caractéristiques qui leur permettraient, selon lui, de devenir rapidement plus stables et fiables que les monnaies étatiques. Avant lui, l'industriel belge Ernest Solvay allait jusqu'à préconiser la suppression pure et simple de la monnaie et son remplacement par un registre rigoureux de tenue des transactions.

Chronologie de l'évolution de la monnaie



Mais en l'absence d'infrastructures techniques permettant leur concrétisation, ces mouvements de pensée restent encore à l'état d'idées.

Cryptographie et monnaie demeurent donc séparées… jusqu'à l'avènement d'Internet.

Enregistrée auprès de l'AMF en tant que Prestataire de Services sur Actifs Numériques n°E2022-035

II - Internet, cypherpunks et premières monnaies numériques

Dans les années 1990, la généralisation de l'informatique et le développement commercial d'Internet marquent un tournant majeur de notre histoire. Il devient possible pour tout individu d'accéder à une infinité de contenus, hébergés sur une première version du Web.

Mais les perspectives déjà palpables de cette révolution amènent leur lot de problématiques, et notamment celle du respect de la vie privée. **Le mouvement cypherpunk, qui réunit alors quelques activistes voyant en la cryptographie une manière de préserver leur anonymat en ligne, émerge rapidement.**

Ceux-ci perçoivent en Internet la possibilité de construire, enfin, l'infrastructure technologique qui servira de base pour leur projet ultime de bâtir une monnaie numérique universelle et décentralisée.

En 1995, un système de paiement électronique et décentralisé, Digicash, voit le jour, mais le projet ne convainc pas le grand public et s'effondre trois ans plus tard. D'autres initiatives, encore trop immatures ou limitées, suivent sa trajectoire : BitGold, B-money, E-gold...

De premières recherches sont menées sur la technologie blockchain, mais celle-ci demeure inexploitée à grande échelle.

Dans le même temps, la bulle Internet explose et laisse place à de nouveaux business models : les internautes peuvent désormais interagir entre eux, rédiger et publier du contenu... **C'est l'avènement du Web2.** Celui-ci donne naissance à des sociétés plus puissantes que des États, enrichies grâce à la monétisation des données de leurs utilisateurs.

Enregistrée auprès de l'AMF en tant que Prestataire de Services sur Actifs Numériques n°E2022-035

III - Bitcoin et Ethereum : la blockchain en action

En plein coeur de la crise financière de 2008, alors que le système monétaire mondial est au bord du précipice, un mystérieux internaute connu sous le pseudonyme de Satoshi Nakamoto publie le livre blanc d'un **système monétaire élctronique de pair-à-pair : Bitcoin.**

Celui-ci marque **la première application aboutie de la blockchain et permet de transférer en quelques secondes de la valeur à n'importe qui, n'importe quand, via une simple connexion internet**. C'est une première révolution.

En 2010, le premier achat en bitcoins est effectué, et tout s'accélère. Le bitcoin, qui vaut désormais plusieurs centaines de dollars, gagne en popularité et inspire de nouveaux projets. Beaucoup viennent se placer en concurrents mais d'autres, plus visionnaires, confèrent à la technologie blockchain de nouvelles applications.

C'est le cas d'**Ethereum qui, en 2015, crée une seconde révolution**. Âgé de 21 ans seulement, Vitalik Buterin démocratise alors la notion de contrats intelligents, ou smart contracts, des programmes informatiques irrévocables exécutant des clauses contractuelles prédéfinies, et ce de façon automatique.

La blockchain devient alors un gigantesque ordinateur décentralisé, sur lequel des milliers d'autres projets peuvent être développés.

En 2020, grâce à cette architecture technologique d'un genre nouveau, émergent les premières applications de la Finance Décentralisée. **N'importe qui peut désormais accéder à des services financiers de base, en quelques secondes, sans intermédiaire et à moindre coût.**

Les crypto-actifs, qui connaissent une grande vague d'adoption, deviennent une classe d'actifs à part entière, tandis que la blockchain laisse entrevoir des milliers d'applications dans des domaines aussi variés que la traçabilité des flux, l'art, la conservation des données, la gouvernance ou le gaming.

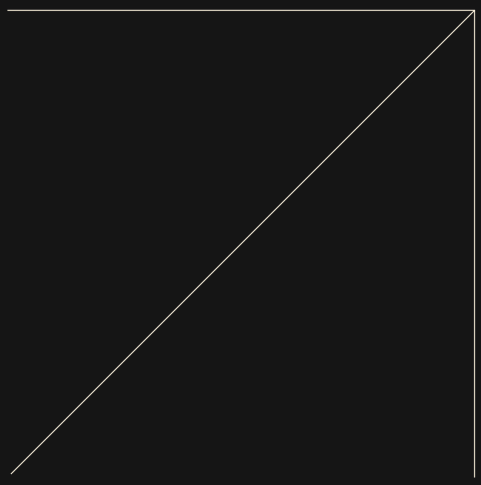
Le Web3, adossé à ces technologies, émerge alors. Avec lui, la perspective pour les internautes de se réapproprier leurs données et de rester seuls décisionnaires de leur éventuelle commercialisation.

Une nouvelle ère commence, une ère axée sur la décentralisation et la création d'interactions d'un genre nouveau.

L'évolution du Web et ses trois phases

EN BREF

- La cryptographie, qui existe depuis des millénaires, a connu ses principales évolutions à partir de la Seconde Guerre mondiale ;
- Les premières monnaies numériques, développées par des cryptographes, se sont développées dans les années 1990 avec l'avènement d'Internet ;
- Bitcoin a été en 2008 la première application concrète de la blockchain ;
- D'autres applications ont émergé depuis, et notamment le Web3, une version du Web plus décentralisée que les précédentes.



mon
livret C

monlivretc.com

contact@monlivretc.com