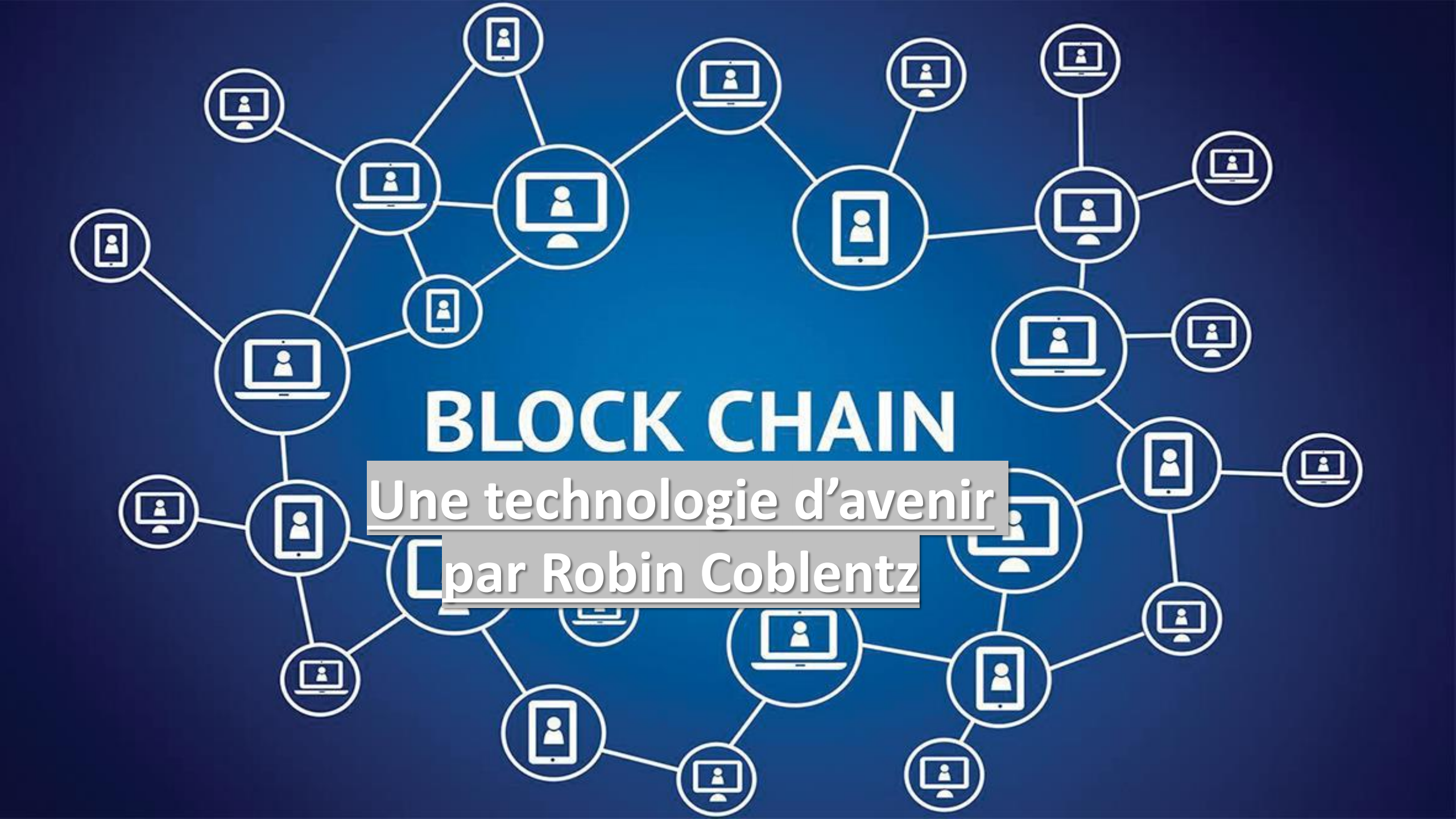



# Une technologie d'avenir

par Robin Coblentz

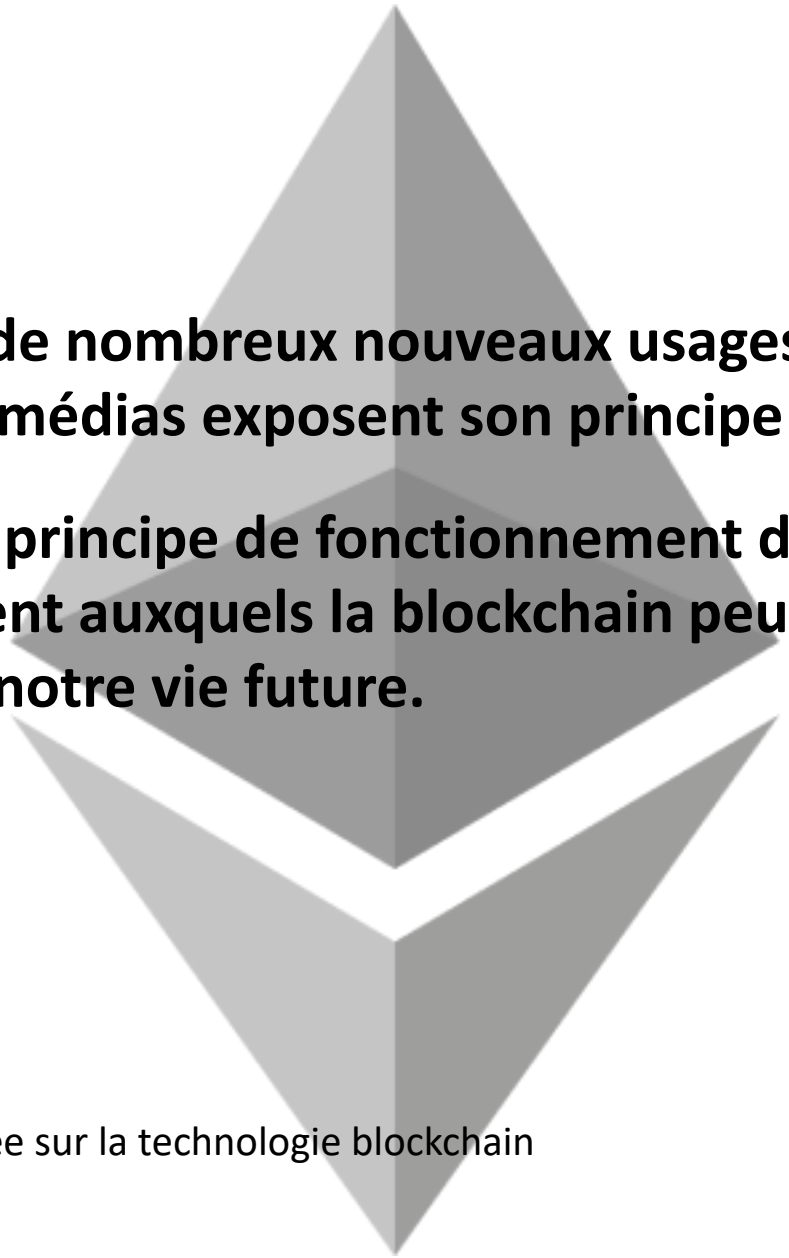
# Présentation :

- **Depuis 5 ans, les médias traitent de nombreux services décentralisés faisant appel à de nouveaux services basés sur une technologie appelée blockchain. Le service dont l'engouement médiatique fut le plus élevé et qui démocratisa aux yeux du grand public cette technologie est bien évidemment le BitCoin dont la valeur à exploser au fur et à mesure. La capitalisation de celui-ci a atteint les 50k€ en 2021.**

Logo bitcoin, une cryptomonnaie basée sur la technologie blockchain

# Présentation :

- **Cette technologie offre de nombreux nouveaux usages dont on entend bien moins parler et peut de médias exposent son principe de fonctionnement.**
- **Nous allons donc voir le principe de fonctionnement de cette technologie, les applications concrètement auxquels la blockchain peut répondre, et comment pourra-t-elle influencer notre vie future.**



Logo etherum, une cryptomonnaie basée sur la technologie blockchain

# Objectifs :


Les objectifs de cette veille sont de déterminer la place qu'occuperont les applications issues de la technologie de la blockchain dans les années à venir.

# Organisation :

- Cette présentation aura pour but d’exposer ma veille technologique.
- Les thèmes à traiter seront listés dans un sommaire.
- Un dossier de sources sera disponible en fin de présentation.

# Thème à traiter :

→Nous verrons d’abord le principe de fonctionnement de la blockchain.

→Nous verrons les avantages qu’elle offre.

→Nous verrons les inconvénients actuel de cette technologie.

→ Nous verrons pourquoi cette technologie a connu un tel essor.

→Nous verrons les usages qui pourraient se démocratiser dans l’avenir et les problématiques.

# Acteurs à surveiller :

- **Plateforme financière**

Les acteurs à surveiller sont principalement les plateformes de finances liées au crypto-monnaies qui participent à l'essors de la finance liée à ce domaine, au financement de nouveaux projets basé sur la blockchaine.

- **Plateforme de minage/stack**

Ce sont les plateformes qui permettent de mettre en commun la puissance ou les services de fonctionnement du réseau blockchain.

- **Plateforme de lancement de projet**

Ce sont les plateformes qui permettent de mettre en avant de nouveaux projets liés à la blockchain.

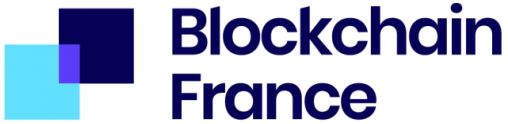
- **Plateforme d'informations**

Ce sont les plateformes qui permettent d'informer les utilisateurs et les passionnés des évolutions globales des principaux réseaux/applications disponibles.

# Sources à surveiller :

- **Plateforme financière :** www.binance.com, www.crypto.com
- **Plateforme de minage/stack :** www.just-mining.com, www.binance.com
- **Plateforme de projet :** www.cryptocompare.com , www.hackster.io
- **Plateforme d'informations :** www.journalducoin.com, www.blockchainfrance.net, www.cryptoast.fr

***Ces plateformes sont des acteurs majeurs du milieu grand publique de la blockchain***





# Méthode de collecte :

- ***Mode pull :***

***(mode de recherche où l'utilisateur recherche activement l'information)***

*- Recherche via différant moteur de recherche (google, duckduckgo, bing)*
*- Utilisation de services de formations (binance-academy)*

- ***Mode push :***

***(mode de recherche où l'utilisateur met en place un système afin que l'information arrive à l'utilisateur.)***

*-Inscription au mailing des plateformes citées précédemment.*
*-Utilisation de flux RSS*

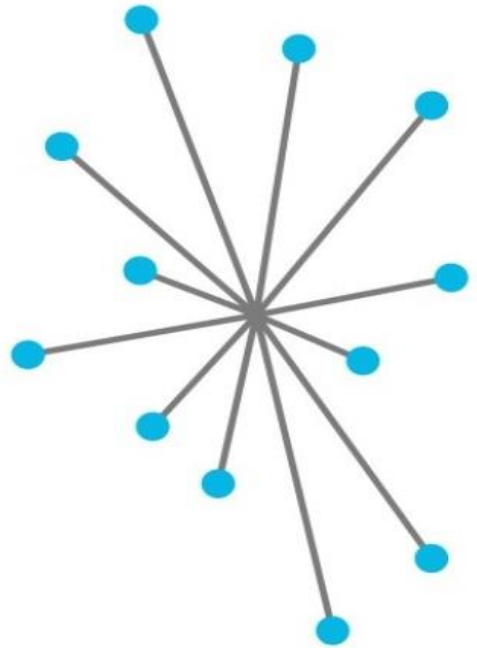
# Suivi :

- Cette veille sera suivie afin de me permettre de voir quelle orientation prend cette technologie et quels nouveaux usages ou à quelles problématiques la blockchain pourrait répondre.

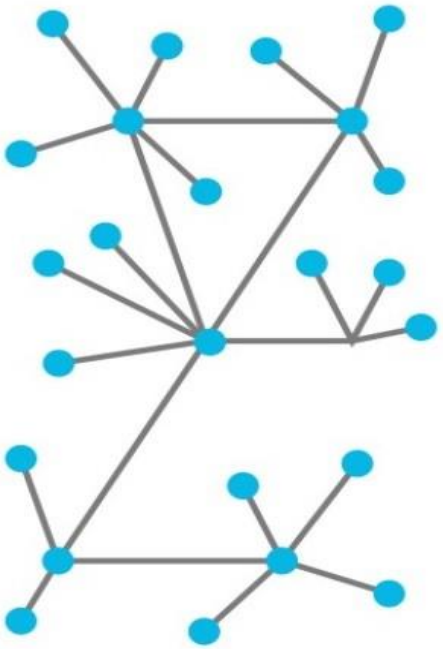
- Le but est également de trouver des marcher futures en tant qu’entrepreneur dans le milieu de l’informatique.

# Fonctionnement :

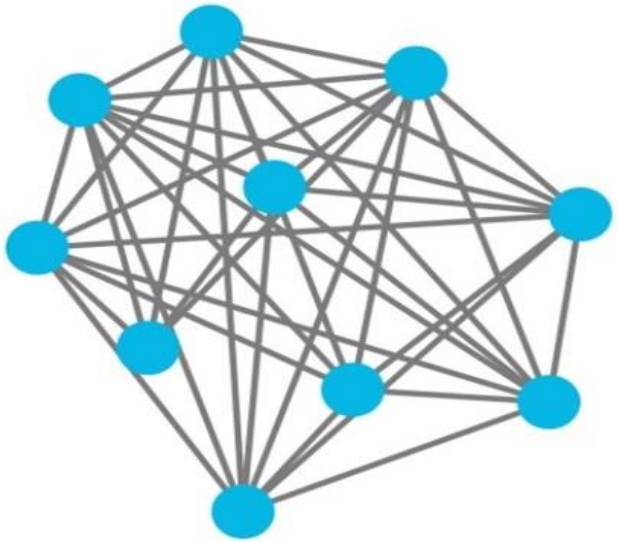
Le principe de la blockchain est de mettre en commun l'intégralité des transactions ayant eu lieu sur un réseau entre les membres utilisateurs de celui-ci. Il faut voir ça comme un réseau paire à paire, en opposition avec les réseaux classiques qui sont des réseaux centralisés.



Centralisé



Décentralisé



Distribué

# Fonctionnement :

- Exemple :

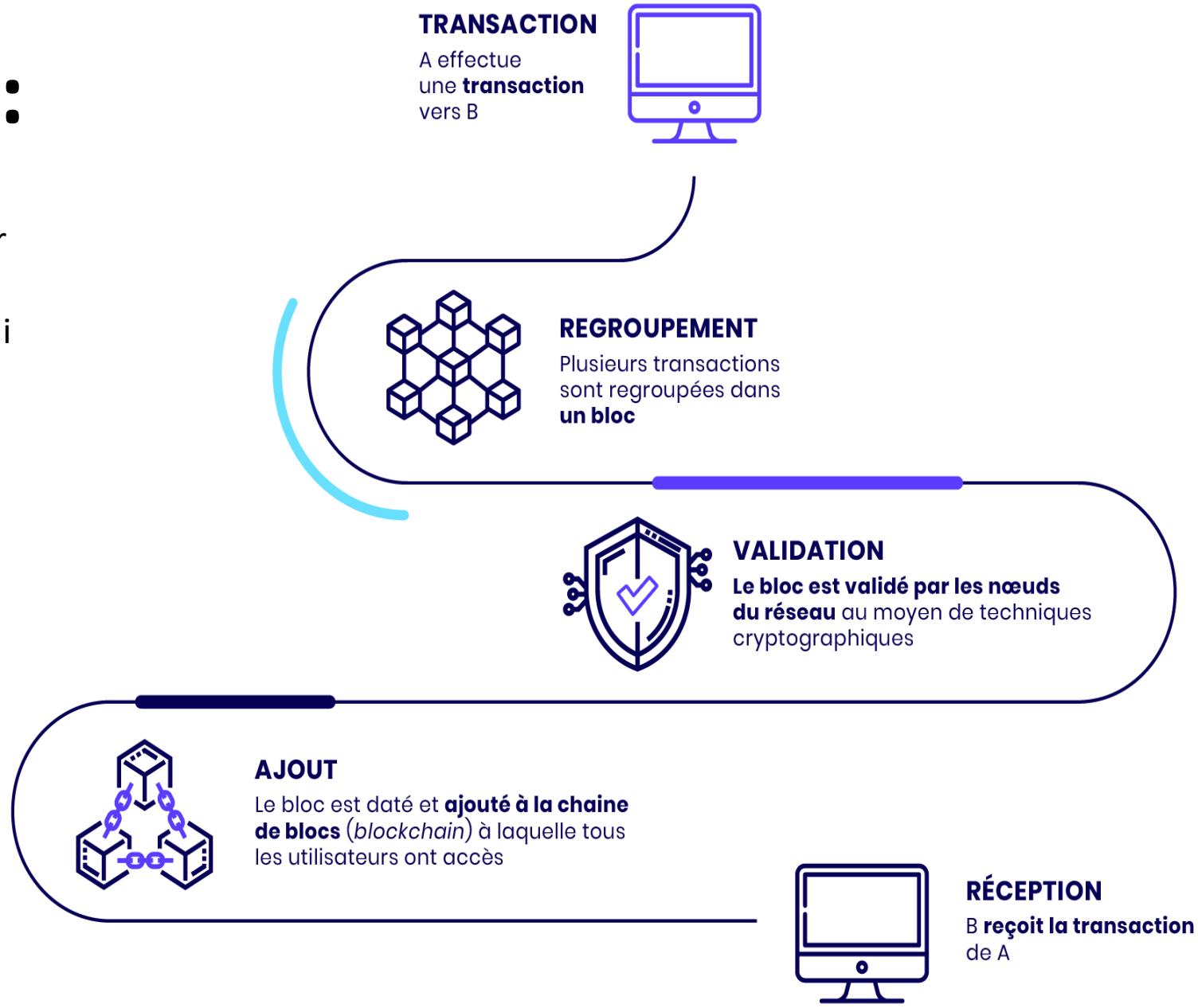
→Réseau bancaire = centraliser (le réseau Swift gère l'ensemble des transactions effectuées)

→Réseau google = décentraliser (un ensemble de serveurs répliquent leurs informations des différentes plateformes et les compare en permanence afin d'être à jour)

→Blockchain = décentraliser (chaque utilisateur détient l'intégralité des transactions)

# Fonctionnement :

Le principe de fonctionnement repose sur la validation et la mise en commun de l'information via des blocs de données qui une fois rassemblés et partagés entre les différents utilisateurs forment une chaine d'information.



# Fonctionnement :

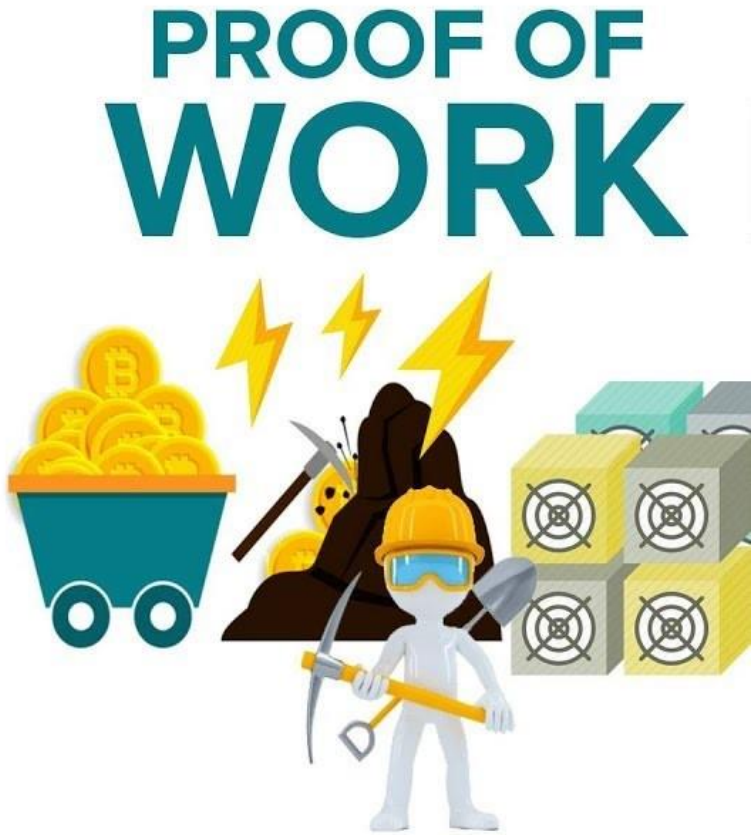
Validation d’une transaction (vérification de la légitimité)

PoW (Proof of Work)

*Preuve de travail*

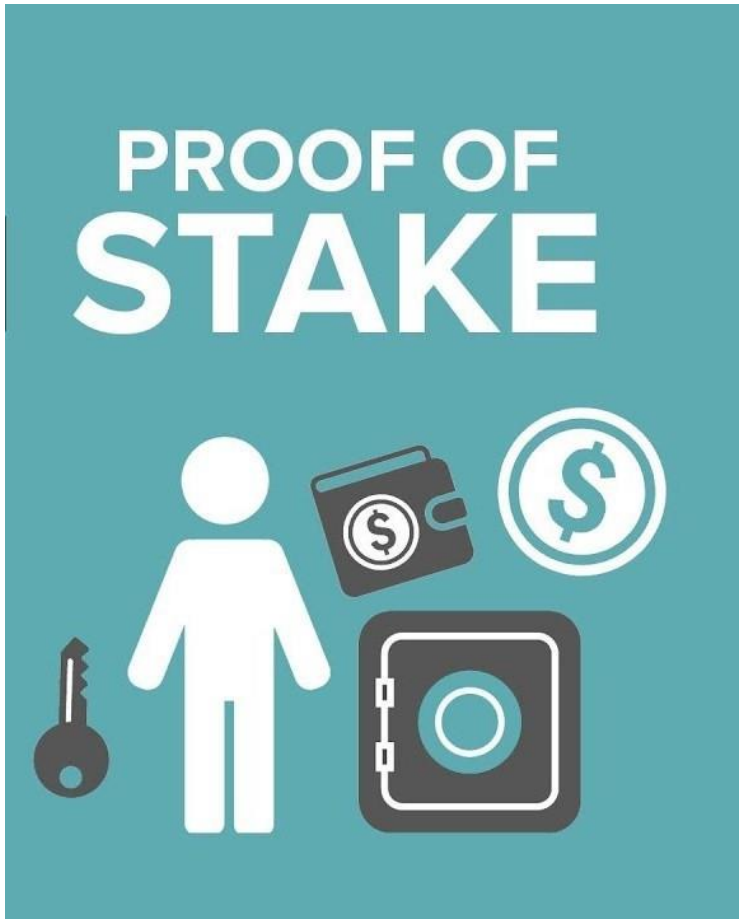
*La preuve de travail consiste en la vérification de blocs (groupe de transactions) par des algorithmes en vérifiant pour chaque bloc sa validité : une équation doit être résolue afin de valider le bloc. Les différents acteurs appelé « mineurs » mettent en commun le résultat successivement dans la chaine. Ils touchent une commission proportionnelle à la puissance de calcul fourni.*

*Le travail des machine sert de preuve*



# Fonctionnement :

Validation d’une transaction (vérification de la légitimité)




## PoS (Proof of Stake)

*Preuve d’enjeux*

*La preuve de stockage correspond à garder des tokens (unité de valeur d’un réseau donné) sur un espace de stockage dédié. Les jetons ont une variable de preuve d’ancienneté qui détermine depuis quand le jeton n’a pas été déplacé. Des jetons sont sélectionnés par afin de vérifier un bloc et le détenteur du jeton touche donc une commission.*

*Ici c’est le stockage des utilisateurs qui sert de preuve*

# Avantage :

- Absence d’intermédiaire

(l’absence d’intermédiaire limite les frais d’utilisation et offre une meilleure vie privée)

- Transparence et traçabilité

(chacun a librement accès aux transactions de l’intégralité du réseau donc pas de fraude)

- Sécurité

(infalsifiable car sécurisé par différents systèmes de vérification de bloc en temps réel)

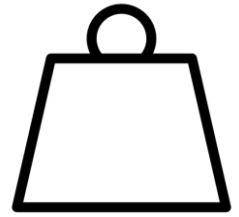
# Inconvénient :

- Consommation Energétique :

L’infrastructure (notamment pour le proof of work) consomme beaucoup d'énergie

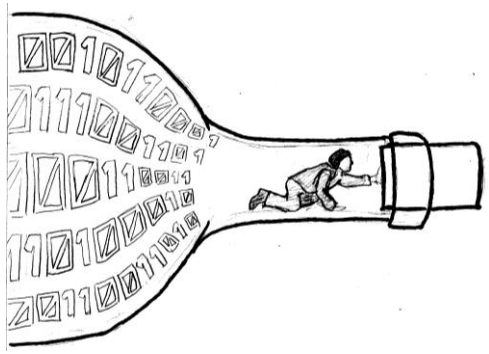
- Lourdeur du réseau

Le réseau peut devenir très lourd car toutes les transactions sont stockées dans un fichier.



- Réactivité

Ce type de réseaux peut suivant son utilisation présenter des lenteurs car la vérification / synchronisation des transactions n’est pas instantanée.

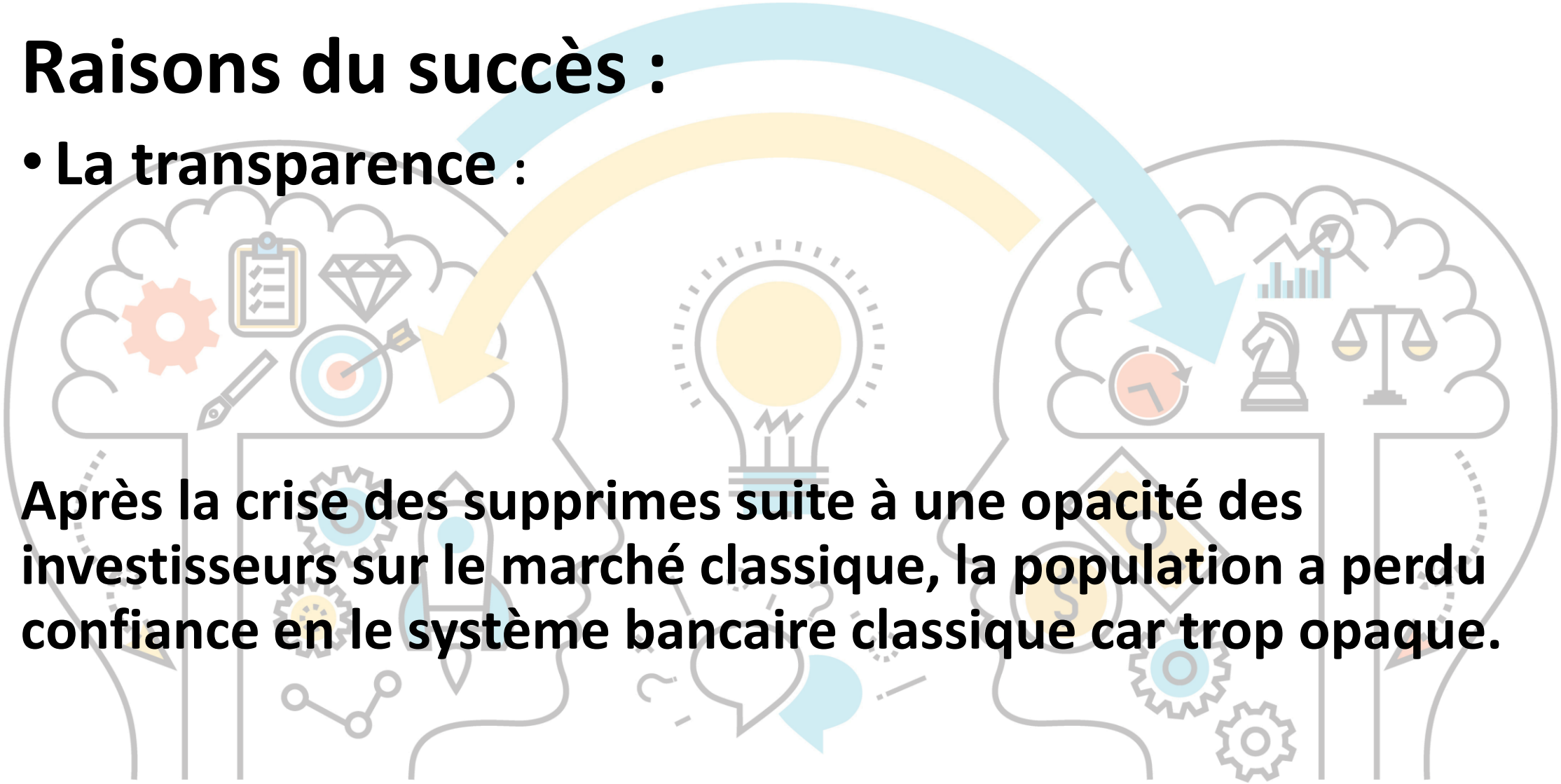


# Raisons du succès :

Cette technologie a connu un essor au cours des 10 dernières années suite à plusieurs facteurs. En effet depuis environ 2010, cette technologie s'est retrouvée mise en avant par des développeurs et des passionnés, gagnant en crédibilité (bien que cette technologie fut inventée en 1991, à la base simplement pour horodater des fichers).

# Raisons du succès :

- **La transparence :**



**Après la crise des supprimes suite à une opacité des investisseurs sur le marché classique, la population a perdu confiance en le système bancaire classique car trop opaque.**

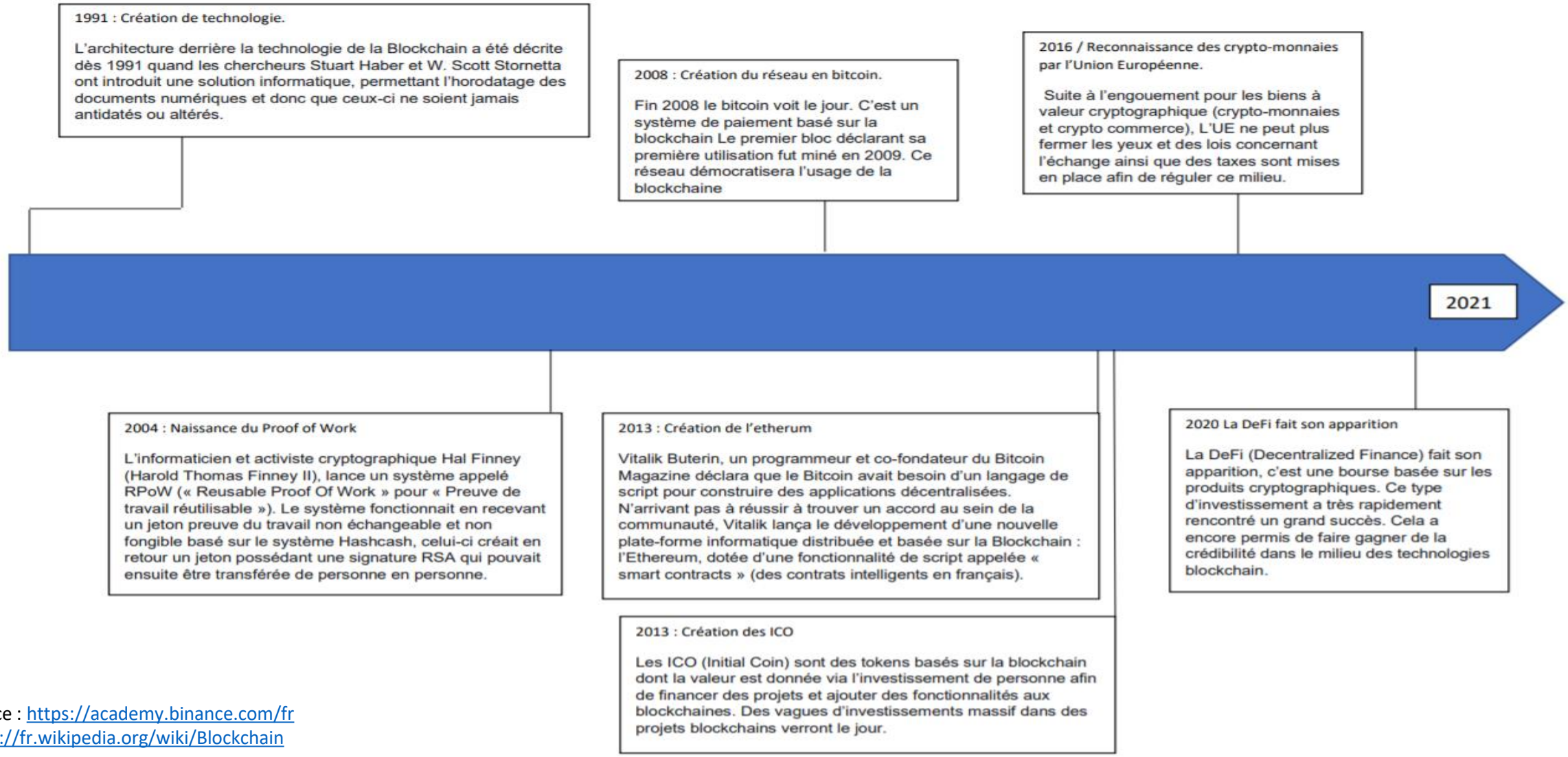
# Raisons du succès :

- La sécurité :

Une vague de piratage a eu lieu suite à l'expansion fulgurent de l'e-commerce, et la sécurité dans les systèmes de paiements est devenue primordiale. La blockchain offre cette sécurité de par son principe de fonctionnement de base, tout est inscrit, traité puis validé après vérification mathématique. De plus l'anonymat est garnetie car la blockchaine n'a pas de verification d'identité. Ainsi une personne souhaitant resté anonyme peut le resté (à noter que la notion d'anonymat diffère d'un système de blockchain a un autre).

# Raisons du succès :

La blockchain connait de nombreuses évolutions au fil du temps et renforcent ses fonctionnalités au fil du temps : elle est évolutive.




Source : https://academy.binance.com/fr
https://fr.wikipedia.org/wiki/Blockchain

# Evolution :

- Certification d’appartenance de bien numérique


Une nouvelle notion de NFT (Jeton non fongible, Non-fungible token) permettent de certifier l’appartenance d’un bien numérique et donc cela permet de créer une notion de rareté d’un bien numérique et donc de valeur entre l’offre et la demande. Cela pourrait révolutionner le commerce de produits numériques, permettre l’authentification de bien dématérialisé et la sécurité des licences d’exploitations.

https://opensea.io

# Evolution :

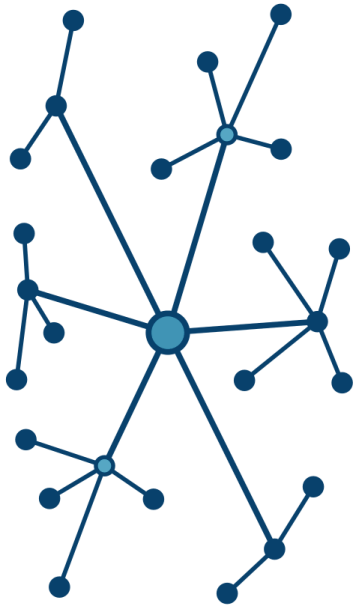
- Certification d’appartenance de bien numérique

On observe déjà une application concrète des NFT dans l’achat d’œuvre d’art dématérialisé, on pourrait donc imaginé dans le future l’achat de licences d’exploitation via des NFT pour l’utilisation de biens numériques. A grande échelles cela résoudrais les problèmes de copyrights non respecté, de propriétés intellectuels de ressources etc… Car aujourd’hui les entreprises, les états et les particuliers déploies de gros moyens sans réel efficacité afin de faire respecté leurs copyrights.

Image original du « nyancat », emblème d’internet dans le milieu geek fut vendu 500k$ en équivalent etherum au enchère. L’anonymat qu’a souhaiter l’acquéreur est garantie par la blockchain.
Sources : https://www.theverge.com/2021/2/18/22287956/nyan-cat-crypto-art-foundation-nft-sale-chris-torres

# Evolution :

#DeFi



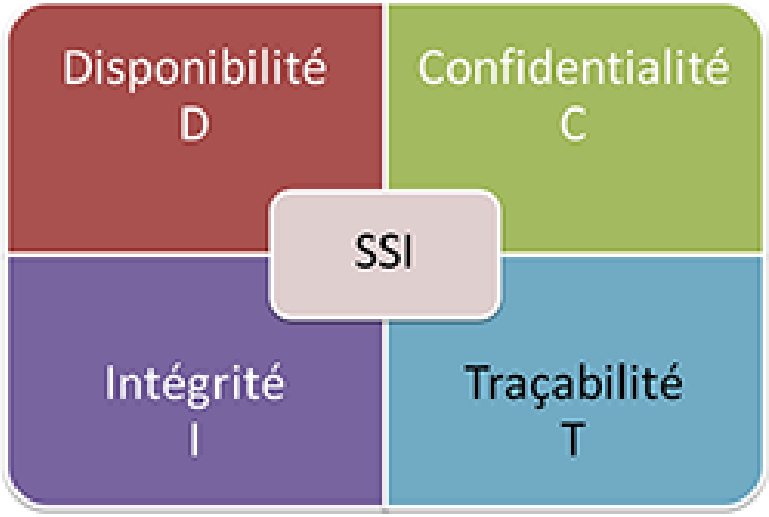
- Finance

La DeFi et les cryptomonnaies pourraient permettre une fois utilisé par des institutions financières de fluidifier les échanges de capitaux et d'améliorer la transparence. De plus cela peut être un nouveau moyen d'obtenir des fonds que des institutions classiques n'aurait pas débloqués pour des projets. Cela permet donc d'ouvrir de nouvelles portes aux investisseurs, aux entrepreneurs et au secteur de la finance via des méthodes alternatives d 'échanges de capitaux.

# Evolution :

- Traçabilité de l’information

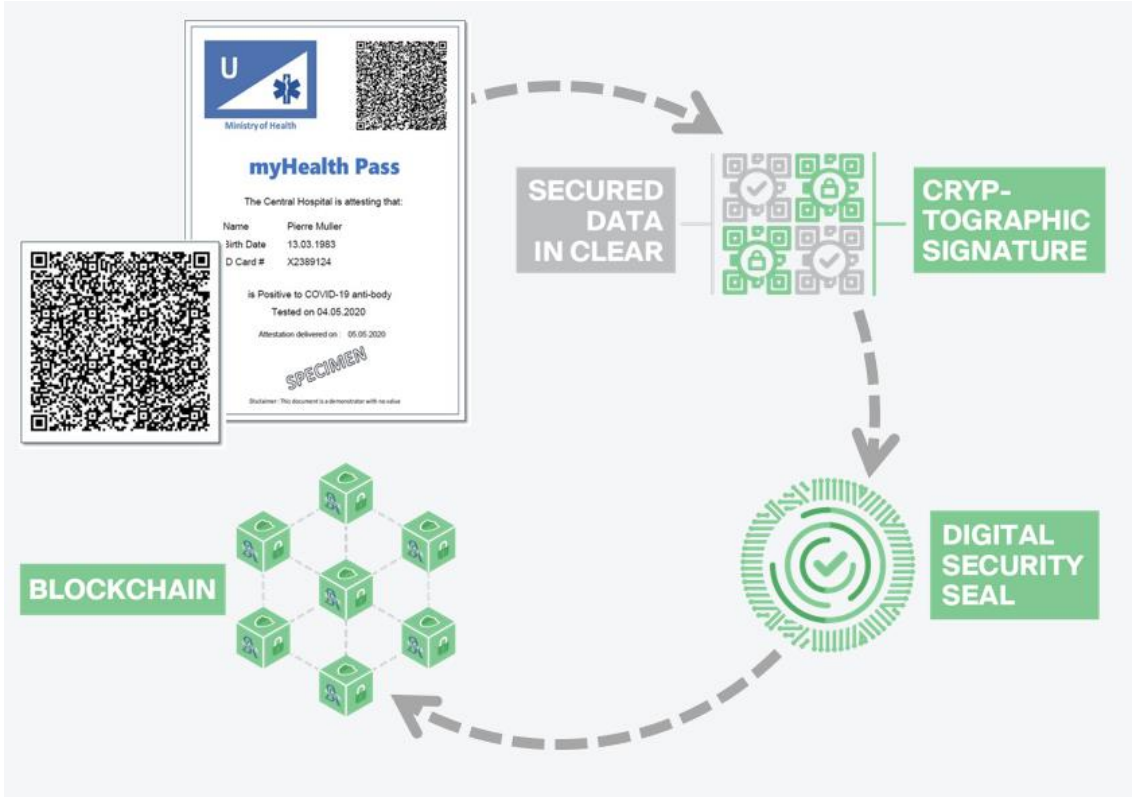
De plus en plus de services pourraient se baser sur la blockchain pour la sécurité et la traçabilité de leur donnée. Cette technologie pourrait s’ajouter aux bases de données classiques, et augmenter la robustesse de la disponibilité de l’information. De plus on pourrait également vérifier l’authenticité des informations via des techniques de comparaisons de blockchain.



# Evolution :

- Traçabilité de l'information

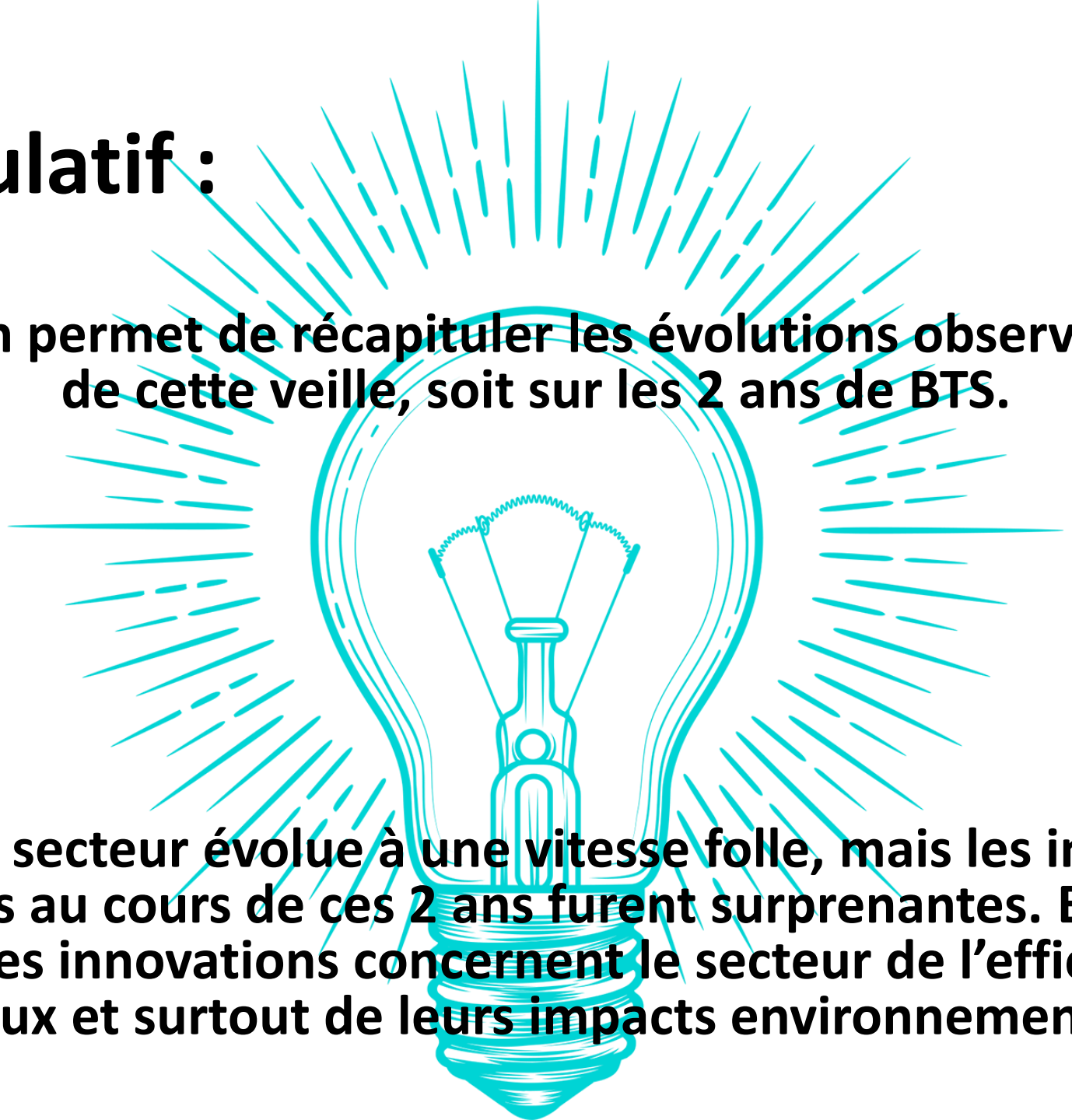
On pourrait par exemple créer une blockchain pour les passeports, ainsi la vérification serait beaucoup plus simple : un numéro de série permettrai d'authentifier le passeport. Tout les pays du monde synchroniserai leur passeport via la blockchain. Ainsi les faux seraient impossible, de même pour l'usurpation car le passeport serait instantanément bloqué. Le tout sans avoir à géré des facteurs humains car la blockchain se charge automatiquement de tout synchroniser instantanément.




Ici on peut voir un projet français de passeport médical pour répondre à la problématique du covid. Il est donc anonyme et infalsifiable.

Source : https://www.sicpa.com/fr/news/un-passeport-sante-covid-19-securise-par-blockchain-pour-accompagner-le-deconfinement

# Récapitulatif :



**Cette section permet de récapituler les évolutions observées au cours de cette veille, soit sur les 2 ans de BTS.**

**En effet ce secteur évolue à une vitesse folle, mais les innovations observées au cours de ces 2 ans furent surprenantes. En effet la plupart des innovations concernent le secteur de l'efficacité des réseaux et surtout de leurs impacts environnementaux.**

# Récapitulatif :

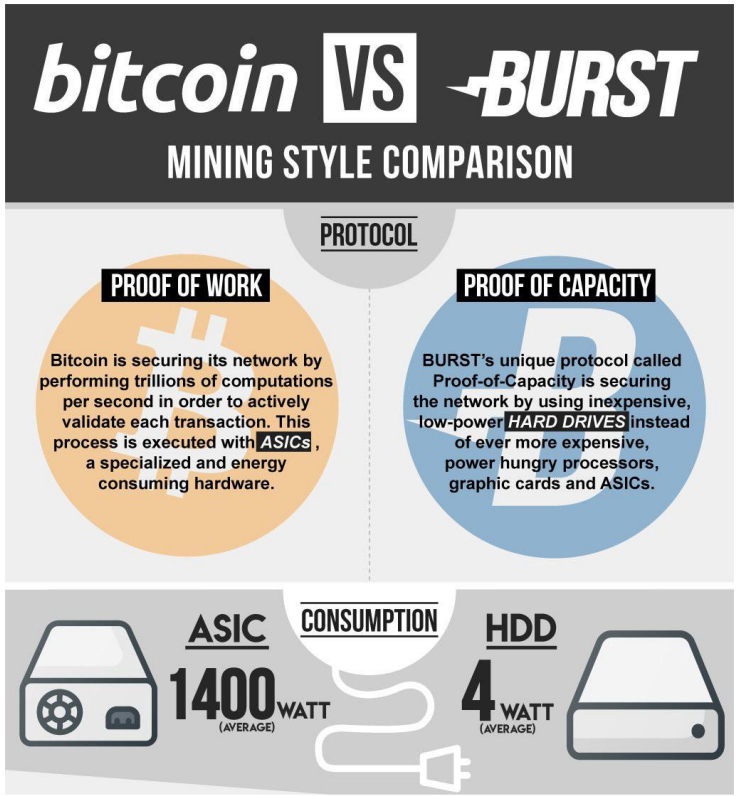
- Smart-contract :

La blockchain etherum à exploser au point d'être parfois totalement congestionnée pendant plusieurs heures. L'apparition de nombreuse sous blockchaines fonctionnant via des smart-contracts (permettant d'exécuter du code au sein de la blockchaine) ont vu le jour. Cela montre que l'intérêt porter au smartcontracts explose, mais que les technologies actuelles sont inadaptées à la demande croissante. La démocratisation de langage de programmation comme Solidity spécialiser dans les applications blockchaine pousse les développeurs à innover.


https://fr.wikipedia.org/wiki/Solidity

# Récapitulatif :

- Aspect environnemental :




BURSTCoin

chia

Un nouveau type de blockchaine c'est démocratiser, suscitant un fort intérêt à vu le jour via une nouvelle méthode de vérification moins onéreuse et plus respectueuse de l'environnement : le proof of storage dont le but proche du proof of stacke se base sur le stockage des informations via des disques durs, moins énergivores et qui dispose d'une meilleure longévité que les gpu /asic utilisés pour le proof of stacke. Cela prouve que les technologies s'adaptent aux besoins rapidement.

Les pionniers sont les projets chia-network et burst.

https://www.chia.net , https://www.burst-coin.org

# Récapitulatif :

- Aspect environnemental :

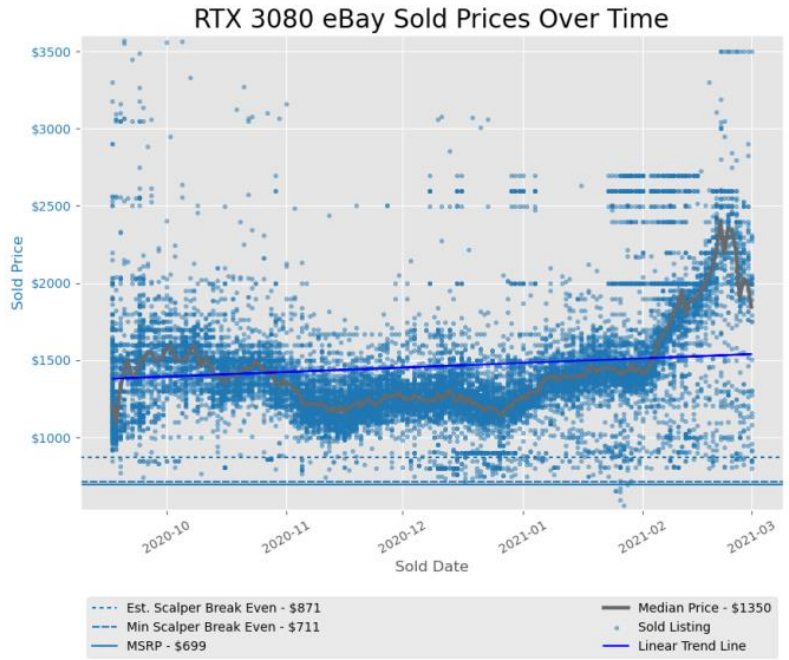
Le réseau etherum a annoncé la mise en place de etherum 2.0 d'ici à 2 ans, un fork (mise à jour profonde) du système etherum dans le but d'abandonner le proof of work pour du proof of stake, ce qui réduirai d'au moin 99% la consommation énergétique de ce dernier. De nombreux autres réseaux blockchains cherchent des solutions afin de limiter l'impact écologique via des algorithmes plus efficients énergétiquement.

https://cryptoactu.com/economie-energie-ethereum-2-futur-de-la-blockchain/

# Récapitulatif :

- Impactes négatifs:

On n’a observé que le besoin de composants croissant à entrainer (avec les retards de productions liés au COVID) une pénurie de composant. La demande ayant dépassée l’offre de manière exponentielle, le prix des composants neuf et d’occasion a mondialement doublé sur le secteur haut de gamme pour particulier/semi-pro. De plus l’optimisation énergétique ne rattrape pas la croissance des réseaux.


https://www.lesnumeriques.com/pro/composants-electroniques-une-penurie-au-dela-de-2022-n162699.html

# Sources


- https://www.toutsurlebitcoin.fr/quest-ce-qui-differencie-preuve-de-travail-et-preuve-denjeu.htm
- https://cryptoast.fr/defi-finance-decentralisee/
- https://www.theverge.com/2021/2/18/22287956/nyan-cat-crypto-art-foundation-nft-sale-chris-torres
- https://www.coinhouse.com/coinhouse-academy/blockchain/what-is-decentralized-finance-defi/
- https://fr.wikipedia.org/wiki/Blockchain
- https://academy.binance.com/fr
- https://www.amf-france.org/fr/quest-ce-quune-cryptomonnaie
- https://fr.wikipedia.org/wiki/Cryptomonnaie

# Sources


- https://www.ledger.com
- https://opensea.io
- https://www.phonandroid.com/bitcoin-le-minage-consomme-plus-delectricite-que-largentine-dapres-une-etude.html
- https://fr.wikipedia.org/wiki/Preuve_d%27enjeu
- https://en.wikipedia.org/wiki/Proof_of_work
- https://www.bearingpoint.com/fr-fr/blogs/blog-digital-strategy/la-blockchain-la-garantie-dune-traçabilité-transparente/#:~:text=La%20technologie%20Blockchain%20au%20service,acteurs%20sont%20parfois%20très%20nombreux.
- https://www.crowdlending.fr/la-blockchain-va-revolutionner-le-crowdfunding-deja/