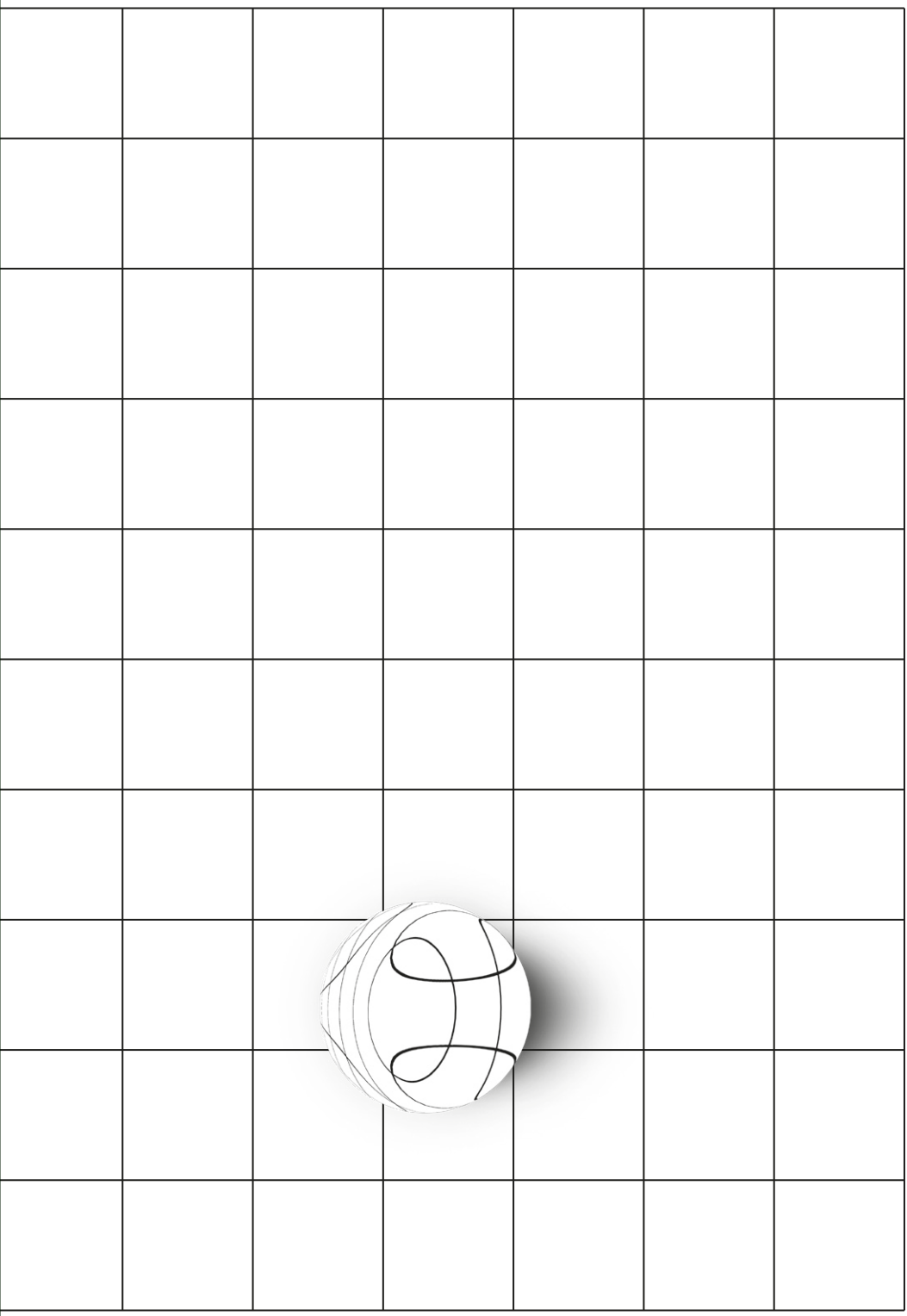
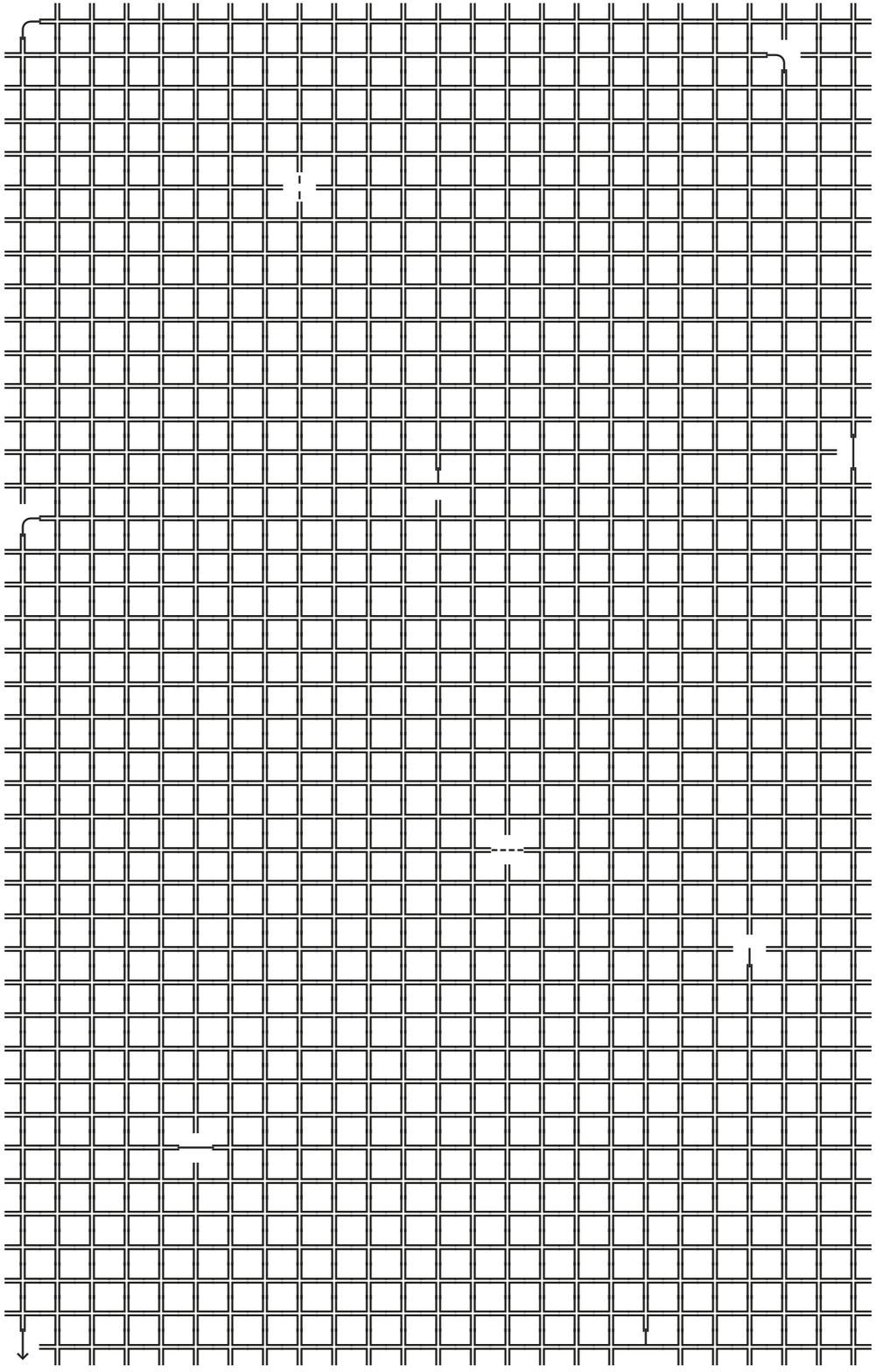
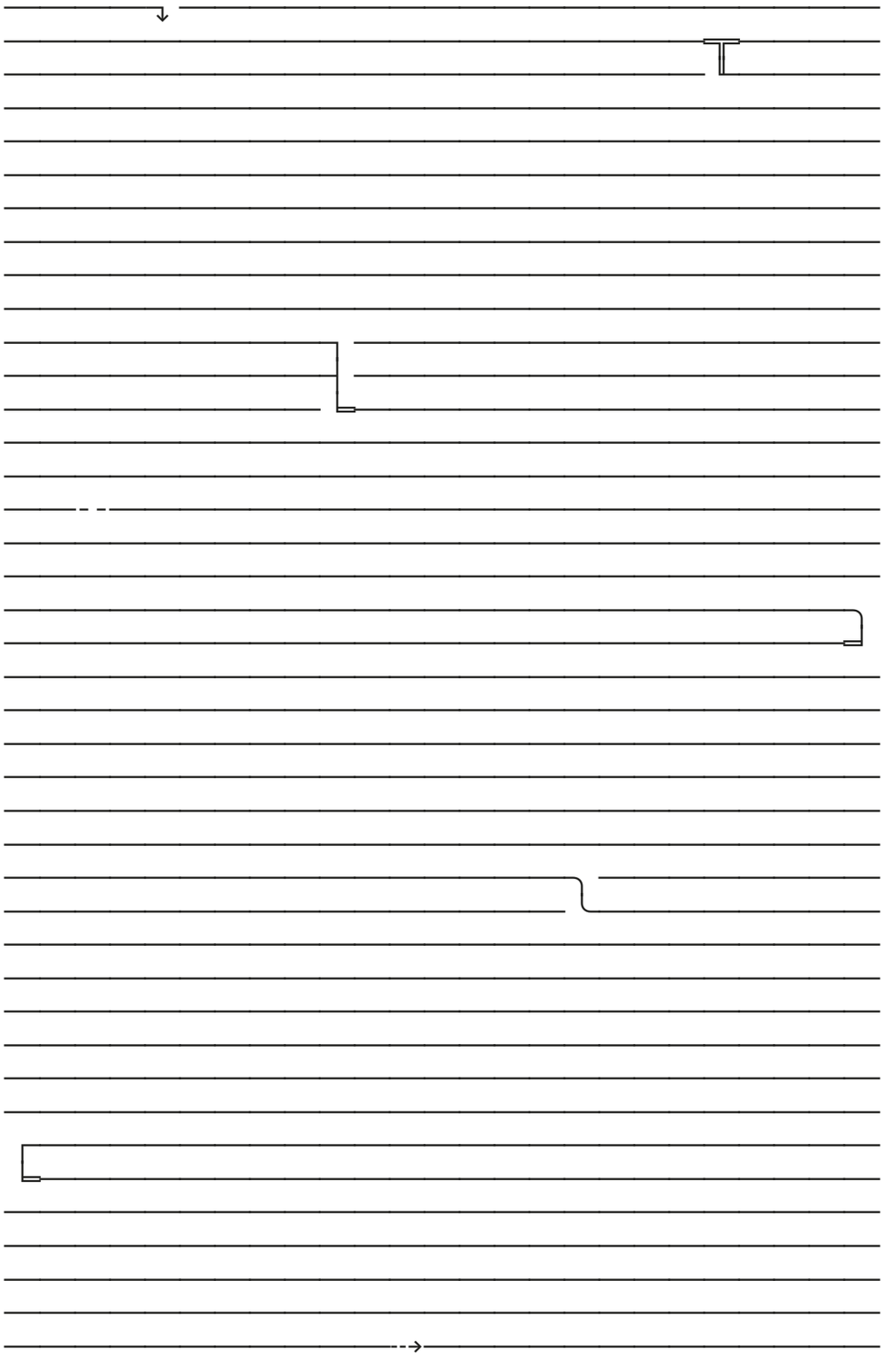
CRYPTOKIT



UNE HISTOIRE DE LA BLOCKCHAIN

A HISTORY OF BLOCKCHAIN





SUMMARY

SOMMAIRE

Blockchain, for a non-initiated public, is often an obscure and incomprehensible subject. In a didactic approach far from the several related polemics, CryptoKit is a set of pictograms and graphic symbols that represents the key concepts of **blockchain** technology.

La **blockchain**, pour un public non initié, reste un sujet obscur et difficile à comprendre. Dans une visée didactique et à distance des polémiques, le projet CryptoKit propose un ensemble de symboles graphiques représentant les concepts clés de cette technologie.

A HISTORY OF BLOCKCHAIN: PROTECT PRIVACY AND RECLAIM THE MONETARY SYSTEM

Whether one is a 'crypto-enthusiast' or a neophyte, rare are those of us who have not heard of **Bitcoin** and the (mostly) financial gibberish that surrounds it. But few people know that a group of people, the **cypherpunks**, are the creators of what would become the **Bitcoin protocol** (2009) and its associated technology, **blockchain**. The term "**cypherpunk**" combines the words "cypher," which refers to the use of **cryptography** to secure communication, and "**punk**", which connotes a rebellious attitude stemming from the counterculture.

The **cypherpunk movement** began in the 80-90's, with the development of **encryption** technologies and the growth of the **Internet** (1974). **Cypherpunks** are strong advocates of the use of **encryption** technologies to protect against surveillance and the erosion of privacy in the digital age. In 1983, the computer scientist and **cypherpunk** David Chaum proposed an anonymous, untraceable electronic money system. A few decades later, thanks to the combination of several technical bricks, this concept became a reality with the creation of **crypto-currencies** operating thanks to the **blockchain**.

At its core, a **blockchain** is a decentralized and immutable **ledger** of a database (structure through a data register) a system that allows for secure and transparent record-keeping and transfer of data or value. It takes the form of a **chain** of **blocks** (hence the name, **blockchain**). This makes it well-suited for use cases such as financial **transactions** (as David Chaum proposed) but also supply chain management and identity verification, among others. If it was the monetary aspect that initially drew the general public's attention to **blockchain** in the 2010s, it would subsequently manifest a much broader potential to revolutionize a wide range of industries.

The first **blockchain** and the most well-known crypto-asset is **Bitcoin** ("B" for the **protocol**) and its eponymous currency **bitcoin** (with a small "b"). Both were detailed in October 2008 in a **whitepaper** (a technical document published to highlight the characteristics

UNE HISTOIRE DE LA BLOCKCHAIN : PROTÉGER LA VIE PRIVÉE ET SE RÉAPPROPRIER LE SYSTÈME MONÉTAIRE

Que l'on soit « crypto-enthousiaste » ou néophyte, rares sont les personnes n'ayant pas entendu parler de **Bitcoin** et du charabia (essentiellement) financier qui l'entoure. Mais peu savent qu'un groupe de personnes à mouvance anarchiste, les ***cypherpunks***, est à l'origine de ce qui allait devenir le **protocole Bitcoin** (2009) et la technologie qui y est associée, la **blockchain**. Le terme « ***cypherpunk*** » combine les mots « *cypher* », qui fait référence à l'utilisation de la **cryptographie** pour sécuriser les communications, et « ***punk*** », qui connote une attitude rebelle issue de la contre-culture.

Le **mouvement cypherpunk** a vu le jour dans les années 1980-1990, avec le développement des technologies de **chiffrement** et l'essor d'**Internet** (1974). Les **cypherpunks** défendent ardemment la protection de la surveillance et combattent l'érosion de la vie privée à l'ère numérique. En 1983, l'informaticien et **cypherpunk** David Chaum propose un système de monnaie électronique, anonyme et intraçable. Quelques décennies plus tard, grâce à l'association de plusieurs briques techniques, ce concept se concrétise par la création de **crypto-monnaies** fonctionnant grâce à la **blockchain**.

Une **blockchain** est un **registre de comptes** décentralisé et immuable d'une structure de base de données (par le biais d'un registre de données) qui permet le transfert de données ou de valeurs de manière sûre et transparente. Ce système se présente sous la forme d'une **chaîne** de **blocs** (d'où son nom, « **blockchain** »). La **blockchain** permet d'effectuer des **transactions** financières sur le réseau (comme l'avait proposé David Chaum), mais est aussi adaptée, entre autres, à gérer des chaînes d'approvisionnement et à vérifier des identifiants numériques. Si c'est l'aspect monétaire qui a initialement attiré l'attention du grand public sur la **blockchain** dans les années 2010, celle-ci va manifester un potentiel bien plus large dans sa capacité à révolutionner un large éventail d'industries.

of a service) written under the pseudonym **Satoshi Nakamoto** — whose identity as an individual or group remains a constant source of speculation. **Bitcoin** was created in response to the 2008 global financial crisis (the subprime crisis) as a way to challenge the **centralized system** on which banks are based. The relation to the crypto-anarchist movement was most clearly demonstrated in the first **bitcoin transaction**, included in the **Genesis Block**, dated January 3rd, 2009, where **Nakamoto** quote in the metadata, with a hint of irony, a headline from the Times newspaper of the day: "Chancellor on brink of second bailout for banks."

BITCOIN PROTOCOL: A PUBLIC AND DECENTRALIZED LEDGER OF MONETARY TRANSACTIONS

One of the key features of **blockchain** is its decentralized nature. This decentralization is made possible by the use of the **Internet** which, unlike a **centralized system**, is not controlled by any central authority or organization. Among those **interrelation system**, a **polarized system** also rely on a third-party verification (TPV). Only the **distributed system** (**peer-to-peer**) infrastructure of the **Internet** makes it possible for the **blockchain** to function by networking computers that participate in the maintenance and validation of the **ledger** to ensure secure and transparent recording and

La première **blockchain**, et la plus connue, **Bitcoin** (« B » majuscule pour le **protocole**) possède sa monnaie éponyme, le **bitcoin** (avec un petit « b »). Les deux ont été détaillées en octobre 2008 dans un **livre blanc** (un document technique publié pour mettre en évidence les caractéristiques d'un service) rédigé sous le pseudonyme de **Satoshi Nakamoto** – dont l'identité en tant qu'individu ou groupe reste à ce jour inconnue. **Bitcoin** a été créé, en réaction à la crise financière mondiale de 2008 (celle des *subprimes*), comme un moyen de défier le **système centralisé** sur lequel les banques reposent. La relation avec le mouvement crypto-anarchiste est énoncée dans la première **transaction bitcoin** (incluse dans le **bloc originel** (*Genesis Block*) du 3 janvier 2009) où **Nakamoto** , avec ironie, cite dans les métadonnées du **bloc** une manchette du journal *Times* du même jour : « Le ministre des Finances au bord d'un second plan de sauvetage des banques » (« *Chancellor on brink of second bailout for banks* »).

LE PROTOCOLE BITCOIN : UN REGISTRE DE TRANSACTIONS MONÉTAIRES PUBLIC ET DÉCENTRALISÉ

L'une des principales caractéristiques de la **blockchain** est sa nature décentralisée, rendue possible par l'utilisation d'**Internet** qui, contrairement à un **système centralisé**, n'est contrôlé par aucune autorité ou organisation. Parmi ces **systèmes d'interrelations**, les **systèmes polarisés** reposent également sur une vérification par un tiers. Seule l'infrastructure du **système distribué** (*peer-to-peer*) de l'**Internet** permet à la **blockchain** de fonctionner. Celle-ci s'organise par un réseau d'ordinateurs qui participent à la maintenance et à la validation d'un **registre de comptes** pour assurer un enregis-

transfer of data.----------
Bitcoin takes the form of a bank registry based on the client/**server** architecture of the **Internet**: it is a **public blockchain** where anyone can consult all the **transactions** or participate in the smooth running of the **protocol** by becoming a **node** (provided they have the appropriate hardware).----------
---

The **incrementation** process unique to **blocks** of data means that they cannot be changed, but only added to the register. Therefore, no one can falsify the **transaction** history, because it is—metaphorically—"carved in stone." **Bitcoin**'s public **ledger** lists all **transactions** made on the network, i.e. the transfer of ownership of **bitcoins** from one entity to another. This mechanism, unlike the banks' **economy** of debts, makes it impossible to have a negative balance.

As with most traditional currencies, such as the **euro** of the **dollar** (commonly called **FIAT money**), the "materiality" of **bitcoins** resides in their registration in the registry, which is not a representation of the value but the value itself: **bitcoins** do not exist elsewhere than in their registration in the **blockchain**. The value of **bitcoins** (their **FIAT money** equivalent) is still volatile, giving rise to much speculation. This instability has led to the development of a new type of currency, **stablecoins**. A **stablecoin** is a digital **cryptocurrency** whose value is based on that of a traditional currency like the **dollar**, making it less unstable.----------
---

Moreover, in an effort to modernize, **FIAT money** also got their digital version issued and regulated by the country's central bank. These are called **Central Bank Digital Currencies (CBDC)**. They share one characteristic of **stablecoins** as they are pegged 1:1 to the value of the traditional currency and can be used for **transactions** and as a store of value. **CBDCs** are not to be confused with **cryptocurrencies**, though, as they're centralized and regulated by governments, which could allow for an unprecedented surveillance of money **transactions** as federal officials have full control over the money going into—and coming out of—every person's account. As a result, **CBDCs** are the direct opposition to the original purpose of **Bitcoin**. The same is true of **private blockchains**, which do not rely on decentralization to maintain authority over the **protocol**.

trement et un transfert de données sécurisé et transparent.----------
Plus concrètement, **Bitcoin** prend la forme d'un registre bancaire basé sur l'architecture client/**serveur** d'**Internet** : c'est une **blockchain publique** où n'importe qui peut consulter l'ensemble des **transactions** ou participer au bon fonctionnement du **protocole** en devenant un **nœud** (*node*) (à condition de posséder le matériel technique adéquat). ----------
---

Le processus d'**incrémentation** propre aux **blocs** de données signifie que celles-ci ne peuvent pas être modifiées, mais seulement ajoutées au **registre**. Par conséquent, personne ne peut falsifier l'historique des **transactions** car ce dernier est – métaphoriquement – « gravé dans la pierre ». Le **registre** public de **Bitcoin** liste toutes les **transactions** effectuées sur le réseau, c'est-à-dire le transfert de propriété de **bitcoins** d'une entité à une autre. Ce mécanisme, à l'inverse de l'**économie** de la dette propre aux banques, a pour conséquence de rendre impossible l'obtention d'un solde négatif. ----------
---

Comme pour la plupart des monnaies traditionnelles, telles que l'**euro** ou le **dollar** (communément appelées **monnaies fiduciaires**), la « matérialité » des **bitcoins** réside dans le **registre**, lequel n'est pas une représentation de la valeur, mais la valeur même. Autrement dit, les **bitcoins** n'existent pas ailleurs que dans leur inscription dans la **blockchain**. La valeur des **bitcoins** (leur équivalent en **monnaie fiduciaire**) est encore volatile, ce qui donne lieu à de nombreuses spéculations. Cette instabilité a conduit au développement d'un nouveau type de monnaie, les ***stablecoins*** (littéralement « monnaie stables »). Un ***stablecoin*** est une **crypto-monnaie** numérique dont la valeur est basée sur celle d'une monnaie traditionnelle comme le **dollar**, ce qui la rend moins fluctuante.----------
---

En outre, dans un souci de modernisation, les **monnaies fiduciaires** ont obtenu leur version numérique émise et réglementée par une banque centrale. Celles-ci sont appelées **monnaies numériques de banques centrales** (*Central Bank Digital Currencies*, CBDC). Elles présentent une caractéristique similaire aux ***stablecoins*** puisqu'elles sont un double numérique 1:1 des monnaies traditionnelles, et peuvent être utilisées pour des **transactions** et comme

This type of **blockchain** is often used by companies to improve the efficiency and security of their internal processes.

ANONYMITY IN BITCOIN: EXAMINING THE ROLE OF CRYPTOGRAPHY IN BITCOIN TRANSACTIONS

In opposition to governments-owned **CBDCs** or banks, **Bitcoin** operates by the pseudonymization of individuals. This partial anonymity (contrary to the popular belief of full anonymity) makes use of **asymmetric cryptography**, also known as **public key cryptography**, a type of **encryption** that uses two different keys: a **public key** and a **private key**. While the **public key** is available to anyone, the **private key** is known only to the recipient. This means that anyone can send an encrypted message to the recipient, but only the recipient will be able to read it.

One of the fundamental tools of **cryptography** is the **hash function**—a mathematical algorithm that takes any amount of data as input and produces a fixed-size output. Known as a **hash**, this output can be used to create a digital **signature** for a piece of data and allows others to verify its authenticity and integrity. In the context of **bitcoins**,

réserve de valeur. Les **CBDC** ne doivent cependant pas être confondues avec les **crypto-monnaies** car elles sont centralisées et réglementées par les gouvernements, ce qui pourrait permettre une surveillance des **transactions** sans précédent dès lors que les fonctionnaires fédéraux ont un contrôle total sur l'argent des individus. Par conséquent, les **CBDC** vont à l'encontre de l'objectif initial de **Bitcoin**. Il en va de même des **blockchains privées**, qui ne s'appuient pas sur la décentralisation afin de maintenir une autorité sur le **protocole**. Ce type de **blockchain** est souvent utilisé par les entreprises pour améliorer l'efficacité et la sécurité de leurs processus internes.

L'ANONYMAT DANS BITCOIN : LE RÔLE DE LA CRYPTOGRAPHIE DANS LES TRANSACTIONS

En opposition aux **CBDC** et aux banques contrôlées par des gouvernements, **Bitcoin** opère par la pseudonymisation des individus. Cet anonymat partiel (contrairement à la croyance populaire de l'anonymat total) fait appel au **chiffrement asymétrique**, également connu sous le nom de **chiffrement** à **clé publique**, un type d'encodage qui utilise deux clés différentes : une **clé publique** et une **clé privée**. Alors que la **clé publique** est accessible à tous, la **clé privée** n'est connue que de la personne destinataire. Cela signifie que n'importe qui peut envoyer un message crypté à quelqu'un, mais que seule cette personne sera en mesure de le lire.

Un des outils fondamentaux de la **cryptographie** est la **fonction de hachage** – un algorithme mathématique qui prend n'importe quelle quantité de données en entrée et produit une valeur fixe en sortie. Appelé **condensat cryptographique** (ou *hash*), le résultat de la

a specific type of **hash function** # known as **Secure Hash Algorithm 256 bits (SHA-256)** is used in conjunction with the **Merkle tree** data structure, a tree-like data structure which allows for efficient verification of large amounts of **transaction** data on the **Bitcoin** network.

All this taken into account, **Bitcoin** is a pretty secure way to send money to someone. Some services can further increase the privacy of **transactions** by mixing them together. For instance, one might send funds to a **coin mixer**, which will in turn send the funds back to another **address** (controlled by the **user**), mixed with other **users'** funds. That way, it makes it difficult to determine which funds belong to which **user**, as the funds (mixed together) are not easily traceable. This method can be useful for people who want to keep their financial activities private or who want to protect themselves from being targeted by attackers.

④ ④

EXPANDING THE LIMITS: THE ISSUE OF SCALABILITY IN BLOCKCHAIN TECHNOLOGIES

The development of **blockchain** technologies and the increase in the price of **bitcoins** have made this type of **protocol** increasingly popular with the general public. However, because of this increasing popularity, one of its biggest challenges today is **scalability**, which is the ability of a system to handle a growing number of **transactions** without experiencing delays or performance issues. As more

fonction peut être utilisé pour signer numériquement un ensemble de données et permettre à d'autres de vérifier son authenticité et son intégrité. Dans le contexte des **bitcoins**, un type spécifique de **fonction de hachage** # connu sous le nom de **Secure Hash Algorithm 256 bits** (SHA-256) est utilisé conjointement avec une structure d'**Arbre de Merkle**, une structure de données arborescente qui permet de vérifier efficacement de grandes quantités de données de **transaction** sur le réseau **Bitcoin**.

Tout bien considéré, **Bitcoin** est un moyen assez sûr d'envoyer de l'argent à quelqu'un. En sus, certains services peuvent encore accroître la confidentialité des **transactions** en les combinant. Par exemple, on peut envoyer des fonds à un **mixeur de crypto-actif** (*coin mixer*), qui renverra à son tour les fonds à une autre **adresse** (contrôlée par l'**utilisateur**) après les avoir « mélangés » aux fonds d'autres personnes. De cette façon, il est difficile de déterminer ce qui appartient à qui. Cette méthode peut être utile pour les personnes qui veulent garder leurs activités financières privées ou qui veulent se protéger contre des attaques.

④ ④

REPOUSSER LES LIMITES : L'EXTENSIBILITÉ DES TECHNOLOGIES BLOCKCHAIN

Le développement des technologies **blockchain** et l'augmentation du cours des **bitcoins** ont rendu ce type de **protocole** de plus en plus populaire auprès du grand public. Cependant, en raison de cette célébrité croissante, l'un des plus grands défis auxquels est confrontée cette technologie est celui de son **extensibilité**. L'**extensibilité** (*scalability*) est la capacité d'un système à gérer

people join a **blockchain** network, the ability of the system to handle **scalability** is increasingly tested, leading to issues such as slow **transaction** speeds and high fees.

One solution that has been proposed to address this issue is the use of **sidechains**. A **sidechain** is a separate **blockchain** that runs parallel to the parent **blockchain**. It allows for **transactions** to occur off of the **main chain** to reduce the strain on it as the **sidechain** can process **transactions** at a faster rate.

An example of a **sidechain** is the **Lightning Network**. It operates as a "layer 2" solution to the **Bitcoin** **main chain** and enables fast and low cost micro transactions. It is implemented by creating channels between **users** which enables them to transact directly with each other, as to reduce the load on the **main chain** and increase the **scalability**.

Another example is the **Interplanetary File System (IPFS)**, which is a **peer-to-peer** method of storing and sharing media in a distributed file system. It relies on the peer **node** to keep the files instead of depending on central **servers** or cloud solution.

A last example is **off-chain** solutions (as opposed to **on-chain**), that allows the handling of **transactions** and data outside of the **main chain**, that is without being written directly onto the **blockchain**.

Sidechains, the **IPFS** **protocol** and **off-chain** solutions push the boundaries of **blockchain** technology to ensure a wider variety of applications and usage scenarios. While **on-chain** **transactions** provide greater security, **sidechains** allow for new rules and **off-chain** solutions allow for lower **transactions** costs.

un nombre croissant de **transactions** sans subir de ralentissement ou de problèmes de performance. Quand le nombre de personnes qui utilisent un réseau **blockchain** augmente, le système est de plus en plus mis à l'épreuve, entraînant des problèmes tels qu'une diminution de la vitesse des **transactions** et des frais élevés.

Une solution proposée pour remédier à ce problème est l'utilisation de **blockchain secondaires**. Une **blockchain secondaire** (*sidechain*) est une **blockchain** distincte, qui fonctionne parallèlement à la **blockchain** d'origine. Elle permet aux **transactions** d'avoir lieu en dehors de la **chaîne principale** (*mainchain*) afin de réduire la pression sur celle-ci, car la **blockchain secondaire** peut traiter les **transactions** à un rythme plus rapide. Le ***lightning network*** est un exemple de **blockchain secondaire**. Il fonctionne comme une solution de « niveau 2 » (*layer 2*) par rapport à la **chaîne principale** de **Bitcoin** et permet des microtransactions rapides et peu onéreuses. Il est mis en œuvre par la création de canaux entre **utilisateurs** permettant d'effectuer des **transactions** « directes » afin de réduire la charge sur la **chaîne principale**.

Un autre exemple d'**extensibilité** est le **système de fichiers interplanétaire** (IPFS), une méthode **pair-à-pair** de stockage et de partage des médias qui fonctionne de manière décentralisée et repose sur chaque **nœud** pour stocker les fichiers au lieu de dépendre de **serveurs** centralisés ou de solutions en ***cloud***.

Un dernier exemple est celui des solutions à l'extérieur de la chaîne (***off-chain***) qui, à l'inverse de celles à l'intérieur de la chaîne (***on-chain***), autorisent la prise en charge de **transactions** et de données en dehors de la **chaîne principale**, c'est-à-dire sans les inscrire directement dans la **blockchain**.

Les **blockchain secondaires**, le **protocole** **IPFS** et les solutions à l'extérieur de la chaîne repoussent les limites de la technologie **blockchain** pour assurer une plus grande variété d'applications et de scénarios d'utilisation. Alors que les **transactions** ***on-chain*** assurent une plus grande sécurité, les **blockchain secondaires** permettent d'appliquer de nouvelles règles et les solutions ***off-chain*** permettent de réduire les **frais de transaction**.

HOW TRANSACTIONS WORK: THE ROLE OF ASYMMETRIC CRYPTOGRAPHY

Public blockchains are often used for **decentralized finance (DeFi)** applications, which allow for financial **transactions** to take place without the need for a central authority. **Decentralized exchanges (DeX)** are a type of **exchange platform** that allows the trading of assets using **DeFi protocols**.

In the context of **cryptocurrencies**, a **transaction** typically refers to the transfer of property of **bitcoin** from one **address** (a unique string of characters that is used to identify a specific location on a network) to another. As we've seen before, **Bitcoin** operates by the pseudonymization of individuals through **asymmetric cryptography** by making use of a **public key** and/or a **private key**. The process of using a **private key** is called '**signing**' and allows the recipient to add a digital signature (a cryptographic code) to a piece of data in order to verify that it came from a specific sender and has not been altered. This is an important security measure, as it helps to ensure that only the intended recipient can access the data and that the data has not been tampered with. A **multi-signature**, also known as a 'multi-sig', is a type of digital signature that requires multiple **private keys** to sign a **transaction**. This is used as an additional security measure, as it means that a **transaction** can only be approved if a certain number of authorized individuals all sign it.

To send and receive a **transaction**, and more specifically **cryptocurrencies** such as **bitcoins**, it is necessary to have a **crypto wallet** or a **Web3 wallet**. That is, a software program that allows to store, send and receive **cryptocurrencies**. It usually contains one or more **addresses**, and uses the associated **private keys** to enable one to manage their **cryptocurrencies**. Contrary to popular beliefs, one cannot *"lose their bitcoin,"* on a lost hard drive for instance, as **bitcoins** (and other cryptos) are registered on a **blockchain** in a decentralized way. It is more accurate to say that this person has misplaced their **private key** or their seed, also referred to as **mnemonic phrase**, which is a set of words (typically a string

FONCTIONNEMENT DES TRANSACTIONS : LE RÔLE DU CHIFFREMENT ASYMÉTRIQUE

Les **blockchain publiques** sont souvent utilisées dans le cadre d'applications de **finance décentralisée** (DeFi), qui permettent d'effectuer des **transactions** financières sans avoir recours à une autorité centrale. Les **bourses décentralisées** (DeX) sont un type de **plateforme d'échange** qui permet le ***trading*** d'actifs à l'aide des **protocoles DeFi**.

Dans le contexte des **crypto-monnaies**, une **transaction** fait généralement référence au transfert d'un actif numérique d'une **adresse** (une chaîne de caractères unique qui est utilisée pour identifier un emplacement spécifique sur un réseau) à une autre. Comme nous l'avons vu précédemment, **Bitcoin** fonctionne par la pseudonymisation des individus par le biais du **chiffrement asymétrique**, en utilisant une **clé publique** et/ou une **clé privée**. Le processus d'utilisation d'une **clé privée** permet à la personne destinataire d'ajouter une **signature** numérique (un code cryptographique) à un élément (message, transaction, etc.) afin de vérifier qu'il n'a pas été modifié. Il s'agit d'une mesure de sécurité majeure, car elle permet de s'assurer que seule la personne destinataire concernée peut accéder aux données et que celles-ci n'ont pas été altérées. L'usage de **multi-signatures**, également appelée « *multi-sig* », est un type de **signature** numérique qui nécessite plusieurs **clés privées** pour signer une **transaction**. Elle est utilisée comme mesure de sécurité supplémentaire, car elle signifie qu'une **transaction** ne peut être approuvée que si un certain nombre de personnes autorisées la signent.

Pour envoyer et recevoir une **transaction**, et plus particulièrement des **crypto-monnaies** comme les **bitcoins**, il est nécessaire d'avoir un **portefeuille crypto** (*crypto wallet*) ou un **portefeuille Web3** (*Web3 wallet*), c'est-à-dire un logiciel qui permet de stocker, d'envoyer et de recevoir des **crypto-monnaies**. Il contient généralement une ou plusieurs **adresses**, et utilise les **clés privées** associées pour permettre d'accéder aux **crypto-monnaies**. Contrairement aux idées reçues, une personne ne peut pas « perdre ses **bitcoins** », par

of 12-24 words that are generated at the creation of a new **crypto wallet**) used as a backup of the **private key**. This wallet is to be imagined as a bank account for which you have lost the connection access: your money is still there, at the bank, but you cannot use it or transfer it. Since the bank doesn't really exist in a decentralized registry, you simply can't request a new password.----------
----

If **blockchain** technology has revolutionized the way we think about financial **transactions** and organizational structures, we've yet to tackle one other important aspect of this technology which is the use of **protocols** to govern the way information is recorded, verified and shared on a **blockchain** network.----------------------
----

----

⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥

CONSENSUS MECHANISM: FROM MINING TO STAKING

Bitcoin **transactions** are not recorded one after another, but rather 'page by page,' in **blocks** which hold a set of **transactions** that have been validated by the network at time T. The workforce allowing for the validation and inscription of the chains of **blocks** is constituted by '**miners**.' A **miner** is a person who contributes to the **Bitcoin** network by downloading the open-source registry software and allocating some of the computational power of their computer. The **miners** can at any moment submit their version of a new **block** (along with other **miners**) to insert into the registry. To write their

exemple sur un disque dur égaré, car les **bitcoins** (et autres cryptos) sont enregistrés sur une **blockchain** de manière décentralisée. Il est plus juste de dire que cette personne a égaré sa **clé privée** ou bien sa **phrase mnémotechnique** (*seed*) (généralement une chaîne de 12 à 24 mots générée lors de la création d'un **portefeuille**), utilisée comme sauvegarde de la **clé privée**. Ce **portefeuille** est à imaginer comme un compte bancaire dont vous avez perdu l'accès de connexion : votre argent est toujours là, à la banque, mais vous ne pouvez pas l'utiliser ou le transférer. Comme la banque n'existe pas vraiment dans un registre décentralisé, vous ne pouvez tout simplement pas demander un nouveau mot de passe.--------------------------------
----

Si la technologie **blockchain** a révolutionné la façon de concevoir les **transactions** financières et les structures organisationnelles, il reste à aborder un autre aspect important de cette technologie, à savoir l'utilisation de **protocoles** pour régir la manière dont les informations y sont enregistrées, vérifiées et partagées.---------------------
----

----

⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥⑥

MÉCANISME DE CONSENSUS : DU MINAGE À L'ÉPARGNE

Les **transactions** en **bitcoins** ne sont pas enregistrées l'une après l'autre, mais plutôt « page par page », dans des **blocs** qui contiennent un ensemble de **transactions** validées par le réseau à un instant T. La main-d'œuvre permettant la validation et l'inscription des chaînes de **blocs** est constituée de « **mineurs** ». Un **mineur** est une personne qui contribue au réseau **Bitcoin** en téléchargeant le **registre** et en allouant une partie de la puissance de calcul de son ordinateur. Les **mineurs** peuvent, à tout moment, soumettre leur version d'un nouveau **bloc** (avec d'autres **mineurs**) à insérer dans

block, **miners** will select which pending **transactions** waiting in the **memory pool** to include in their **block**. The most recent inclusions are sorted and classified by **transaction fee**, a small amount of money measured in **satoshi**., the smallest unit of **bitcoin** used to represent the average cost of a **transaction** (in january 2023, 1 **satoshi**. is equal to $0.0002309 USD and 0.00000001 BTC).-------

---

Since new versions of a **block** can vary from one **miner** to another, the **protocol** must make an appeal to a **consensus** to avoid '**double spending**' (the act of spending digital currency twice as the same **transaction** could be recorded in the two different **blocks**) or fraudulent activity. To avoid such issues, **Bitcoin** rests on **Proof-of-Work** (PoW) technology, which requires **miners** to 'validate' their **blocks** before submitting them. The **miner** must therefore exercise a sort of 'transformation' of their **block** via a 'hash operation.' As we've seen before, **Bitcoin** uses a specific type of **hash function** (**SHA-256**), which allows for the transformation of any set of numerical data into a product (following alphanumeric characters), called a '**hash**,' which constitutes the 'footprint' (or 'cryptographic condensate') of the original data and allows others to verify its authenticity and integrity.---------

---

This operation is irreversible and allows for the verification of a unique set of data corresponding to a specific **hash** (any modification would result in a different **hash**). This exercise consists of finding a new number (**nonce**) integrated into the new **block**, which contains a set of **transaction** waiting for **confirmation**, such that it produces a result (**hash**) that respects certain characteristics of the network. The difficulty of this operation, which only depends upon computational power and time allocated on the network, automatically adjusts according to accumulated total power. This difficulty is called a **target** and defines the minimum number of zeros that the **hash** must have in its header to be valid. It is automatically adjusted by the network so that the average time for a person on the network to find a valid **hash** is about 10 minutes. This is why the **blocks** are edited at this period of time: it is not a technical choice but a **protocol** choice in order to ensure better security. Because new **blocks** are edited at a regular rate, a **transaction** with 6 **confirmations** means that if the **transaction** is in the 6th block from the last; **transaction**

le **registre**. Pour écrire leur **bloc**, les **mineurs** sélectionnent les **transactions** en attente dans la **mémoire temporaire** (*memory pool*) à inclure dans leur **bloc**. Les inclusions les plus récentes sont triées et classées par **frais de transaction**, une petite somme d'argent mesurée en **satoshi**., la plus petite unité de **bitcoin** utilisée pour représenter le coût moyen d'une **transaction** (en janvier 2023, 1 **satoshi**. est égal à 0,0002309 USD et 0,00000001 BTC).----------

---

Étant donné que les nouvelles versions d'un **bloc** peuvent varier d'un **mineur** à l'autre, le **protocole** doit faire appel à un **consensus** pour éviter le problème de la « **double dépense** » (le fait de dépenser deux fois de la monnaie numérique, la même **transaction** pouvant être enregistrée dans deux **blocs** différents) ou les activités frauduleuses. Pour cela, **Bitcoin** repose sur le principe du *Proof-of-Work* (PoW, « **preuve de travail** »), qui exige des **mineurs** qu'ils « valident » leurs **blocs** avant de les soumettre. Le **mineur** doit donc exercer une sorte de « transformation » de son **bloc** via une « opération de hachage ». Comme nous l'avons vu précédemment, **Bitcoin** utilise un type spécifique de **fonction de hachage** (**SHA-256**), qui permet de transformer n'importe quel ensemble de données numériques en un produit (suivant des caractères alphanumériques), appelé « **condensat cryptographique** » , qui constitue l'empreinte des données d'origine et permet à d'autres de vérifier leur authenticité et leur intégrité.----------

---

Cette opération est irréversible et permet de vérifier un ensemble de données correspondant à un **hash** spécifique (toute modification entraînerait un **hash** différent). Cet exercice consiste à trouver un nouveau nombre (***nonce***) intégré au nouveau **bloc**, qui contient un ensemble de **transactions** en attente de **confirmation**, de telle sorte qu'il produise un résultat (le **hash**) qui respecte certaines caractéristiques du réseau. La difficulté de cette opération, qui ne dépend que de la puissance de calcul et du temps alloué sur le réseau, s'ajuste automatiquement en fonction de la puissance totale accumulée. Cette difficulté est appelée la **cible** (*target*) et définit le nombre minimum de zéros que le **hash** doit avoir dans son en-tête pour être valide. Elle est automatiquement ajustée par le réseau de sorte que le temps moyen pour une personne sur le réseau de trouver un **hash** valide est d'environ 10 minutes. C'est pourquoi

was mined one hour ago (6 × 10 minutes). This state can be easily verify through a **blockchain explorer**.

Let's explore a simple way to illustrate this: Alice (representing the **protocol**) thinks of a number between 1 and 100 and asks a group of ten people (representing all the **miners**) to find the number she has in mind. There is no specific calculation or method to find this number more easily; the group will have to enumerate them one after the other until they find the right number, whether by increasing the number (1, 2, 3, 4, etc.) or randomly selecting one (23, 9, 15, 74, etc.). Each method would be valid and with the same success rate. Now let's assume that each member of the group can only say a number every second so it will take 10 seconds for the probability of finding the number to be 1. If Alice now thinks of a number between 1 and 10,000 it will take 1,000 seconds or (16.6 min) to get the same result.

On **Bitcoin**, the **protocol** will adjust the **target** (the difficulty) according to the number of **miners** and their computing power: the **hashrate**. The **hashrate** refers to the number of **hashes** that the entire network is able to calculate per second. This computational work is referred to as **mining** and is often done on dedicated—and powerful-computer hardware, the **mining rigs**. To operate this hardware, and have it run complex calculations, it requires energy. The **transaction fee** one has to pay to operate a **transaction** helps pay for the energy needed to confirm it, however, the ecological impact of thousands of computers competing against each other in the **Proof-of-Work protocol** is harder to solve.

In the **Ethereum blockchain**, which we'll explore more deeply in the following part, **transaction fees** are measured in **gas**: a unit of measurement that represents the amount of computational work required to execute a particular action on the **Ethereum blockchain**. The price of **gas** is measured in a smaller unit of **Ethereum**'s native currency, the **ether**, called **gwei**. Because of the amount of power needed to operate a **consensus** mechanism based on **Proof-of-Work**, **Ethereum** operated, on the 15th of September 2022, the then long-awaited "Merge": the transition of **Ethereum** from a **Proof-of-Work protocol** to a **Proof-of-Stake (PoS) protocol**.

les **blocs** sont édités à cette période de temps : ce n'est pas un choix technique, mais un choix protocolaire afin d'assurer une meilleure sécurité. Comme les nouveaux **blocs** sont édités à un rythme régulier, une **transaction** avec 6 **confirmations** signifie que si la **transaction** se trouve dans le 6e bloc à partir du dernier, elle a été minée il y a une heure (6 × 10 minutes). Cet état peut être facilement vérifié à l'aide d'un **explorateur de blockchain**.

Voyons une façon simple d'illustrer cela : Alice (représentant le **protocole**) pense à un nombre entre 1 et 100 et demande à un groupe de dix personnes (représentant tous les **mineurs**) de trouver le nombre qu'elle a en tête. Il n'y a pas de calcul ou de méthode spécifique pour trouver ce nombre plus facilement ; le groupe devra les énumérer les uns après les autres jusqu'à ce qu'il trouve le bon nombre, que ce soit en augmentant le nombre (1, 2, 3, 4, etc.) ou en en choisissant un au hasard (23, 9, 15, 74, etc.). Chaque méthode serait valable et aurait le même taux de réussite. Supposons maintenant que chaque membre du groupe ne puisse dire un nombre que toutes les secondes, il faudra donc 10 secondes pour que la probabilité de trouver le nombre soit de 1. Si Alice pense maintenant à un nombre entre 1 et 10 000, il faudra 1 000 secondes ou (16,6 min) pour obtenir le même résultat.

Sur **Bitcoin**, le **protocole** ajuste la **cible** (la difficulté) en fonction du nombre de **mineurs** et de leur puissance de calcul : le **taux de hachage** (*hashrate*). Ce **taux de hachage** désigne le nombre de **condensats cryptographique** que l'ensemble du réseau est capable de calculer par seconde. Ce travail de calcul est appelé « **minage** » et est souvent effectué sur du matériel informatique dédié et puissant, les « **installations de minage** » (*minning rig*). Pour faire fonctionner ces machines et leur faire exécuter des calculs complexes, il faut de l'énergie. Les **frais de transaction** aident à payer l'énergie nécessaire à leur traitement, mais l'impact écologique de milliers d'ordinateurs en concurrence les uns avec les autres propre au **protocole** ***Proof-of-Work*** (PoW) est difficile à estimer et potentiellement problématique.

Dans la **blockchain Ethereum**, que nous allons étudier plus en détail dans la partie suivante, les **frais de transaction** sont mesurés en **gaz** (*gas*) : une unité de mesure qui représente la quantité de travail de calcul nécessaire pour exécuter une action particulière.

Proof-of-Stake is considered a more ecological alternative to **Proof-of-Work** as it avoids any overconsumption of energy (the **Ethereum** Foundation estimates a reduction of energy consumption of 99.95%). Indeed, it does not involve any type of **mining**, where the **miner** has to invest in hardware, but relies on **staking**. To participate in the **consensus** mechanism of a **PoS** **blockchain**, the **miner** needs to have accumulated ("staked") a sufficient amount of relevant **tokens**. The more **tokens** you have, the more important the security of the network will be considered to be for you and you will have a better chance to see your **block** added to the **blockchain**. In short, this solution requires you to invest in the **blockchain** instead of investing in hardware. However, if a "staker" is found to have made a fraudulent **transaction**, they may be punished by having their stake slashed (potentially losing a lot of money) or being ejected from the network altogether.----------
---

In a decentralized **blockchain**, if not all **miners** upgrade at the same time (for a change in **protocol**), whether due to miscommunication or active resistance, the market could split. This is what happened in 2017, when a dispute between **Bitcoin** **miners** caused the **blockchain** to split in two and the minority became a new **crypto-currency** called Bitcoin Cash. A potential split on a **blockchain**, also called a **fork**, could result in a loss of **governance**, security and funds as well as create uncertainty and divide among communities.----------
---

Le prix du **gaz** est mesuré dans la plus petite unité de la monnaie native d'**Ethereum** (l'**ether**), appelée **gwei**. En raison de la quantité d'énergie nécessaire pour faire fonctionner un mécanisme de **consensus** basé sur la preuve de travail (**PoW**), **Ethereum** a opéré, le 15 septembre 2022, la transition tant attendue d'**Ethereum** vers un **protocole** de *Proof-of-Stake* (PoS, « **preuve d'enjeu** »).---
---

La **preuve d'enjeu** (PoS, *Proof-of-Stake*) est considérée comme plus écologique que la **preuve de travail**, car elle évite la surconsommation d'énergie (la Fondation **Ethereum** estime une réduction de l'ordre de 99,95 %). En effet, elle n'implique aucun type de **minage** (où le **mineur** doit investir dans du matériel), mais repose sur l'**épargne** (*staking*). Pour participer au mécanisme de **consensus** d'une **blockchain** à **preuve d'enjeu**, le **mineur** doit avoir accumulé (« épargné ») une quantité suffisante de **jetons** concernés. Plus vous avez de **jetons**, plus la sécurité du réseau sera considérée comme importante pour vous et plus vous aurez de chances de voir votre **bloc** ajouté à la **blockchain**. En bref, cette solution vous oblige à investir dans la **blockchain** au lieu d'investir dans du matériel. Toutefois, si d'autres personnes découvrent qu'un « *staker* » (une personne possédant une **épargne**) a effectué une **transaction** frauduleuse, il peut être sanctionné en voyant son **épargne** réduite (perdant alors potentiellement beaucoup d'argent) ou en étant carrément éjecté du réseau.---------
---

Dans une **blockchain** décentralisée, si tous les **mineurs** ne se mettent pas à niveau en même temps (pour un changement de **protocole**), que ce soit en raison d'une mauvaise communication ou d'une résistance active, le marché peut se diviser. C'est ce qui s'est passé sur **Bitcoin** en 2017, lorsqu'un différend entre **mineurs** de **bitcoin** a provoqué la **scission** (*fork*) de la **blockchain** en deux : la minorité est devenue une nouvelle **crypto-monnaie** appelée Bitcoin Cash. Une **scission** sur une **blockchain** pourrait entraîner une perte de **gouvernance**, de sécurité et de fonds, et créer de l'incertitude en divisant la communauté.----------
---

ETHEREUM: THE SWISS ARMY KNIFE OF BLOCKCHAINS

While it was the monetary aspect that initially brought **blockchain** to the attention of the general public, it will manifest a much broader potential to revolutionize a wide range of industries. Indeed, while **Bitcoin** still is the focus of media attention, it is only one of 1,500 crypto-assets (or **altcoins**) that have been developed since its launch in 2009. Some are particularly notable in terms of their technology as they are no longer developed to create yet another **cryptocurrency**, but rather to provide new functionalities, linked for example to **governance**.

Initially developed by Vitalik Buterin as an update to **Bitcoin**, the **Ethereum** Platform (2015) proposes new **protocols** such as **smart contracts**, **decentralized application (dApp)**, and **tokens**. These three new concepts allow for a diversity of new use cases.

Smart contracts

Smart contracts are like 'intelligent contracts' which automatically generate **scripts** under specific conditions. By allowing for the shipment of all kinds of metadata in the **blockchain**, **smart contracts** allow for the autonomization of predefined actions by the parties putting a contract into place, for example, reimbursement for a ticket for a flight that has been canceled. In this fictitious case, a person only needs to buy (with ethers) his ticket in the **decentralized application (dApp)** of the given airline. That ticket can later be materialized as a **token** specifically designed for this usage. The funds harvested by the **application** will be blocked through a **smart contract**. This same **dApp**, by means of an **Oracle** service (charged with entering the external data into the **blockchain**), connected to the airport's network will automatically trigger, via the **smart contract**, a specific action defined by the signee(s).

ETHEREUM : LE COUTEAU SUISSE DES BLOCKCHAIN

Si c'est l'aspect monétaire qui a initialement attiré l'attention du grand public sur la **blockchain**, celle-ci va manifester un potentiel bien plus large pour révolutionner un large éventail d'industries. En effet, bien que **Bitcoin** reste au centre de l'attention médiatique, il ne représente pourtant qu'une des 1 500 **crypto-actifs** (ou ***altcoins***) qui ont été développés depuis 2009. Certains se distinguent particulièrement, car ils ne sont pas pensés pour créer une énième **crypto-monnaie**, mais pour offrir de nouvelles fonctionnalités liées par exemple à la **gouvernance**.

Initialement développée par Vitalik Buterin comme une actualisation de **Bitcoin**, la plateforme **Ethereum** (2015) propose ainsi de nouveaux **protocoles** tels que les **contrats programmables** (*smart contracts*), les **applications décentralisées** (dApps), et les **jetons** (*tokens*). Ces trois concepts permettent une diversité de nouveaux cas d'usage.

Contrats programmables (*smart contracts*)

Les **contrats programmables** (*smart contract*) permettent de générer automatiquement l'exécution de **scripts** en fonction de certaines conditions. En envoyant toutes sortes de métadonnées dans la **blockchain**, les **contrats programmables** automatisent le déclenchement d'actions prédéfinies dans des contrats, comme par exemple le remboursement d'un billet pour un vol qui a été annulé. Dans ce cas fictif, il suffit qu'une personne achète (avec des **ethers**) son billet dans l'**application décentralisée** (dApp) de la compagnie aérienne donnée. Ce billet peut ensuite être matérialisé sous la forme d'un **jeton** spécialement conçu pour cet usage. Les fonds récoltés par l'**application** seront bloqués par un **contrat programmable**. Cette même **dApp**, par le biais d'un service « **oracle** » (chargé d'importer les données externes dans la **blockchain**, en l'occurrence l'annulation du vol) connectée au réseau de l'aéroport, déclenche automatiquement, via le **contrat programmable**, une action spécifique définie par le ou les signataires.

dApps

A **decentralized application (dApp)**, is a type of software **application** that runs on a **blockchain** and is not controlled by any single entity. Compared to the usual centralized **applications** (like on the App Store), **dApps** are more resistant to censorship and malfunctions.

Tokens

A **token** is a unit of value that is issued and managed on a **blockchain** network. **Tokens** can represent assets such as **cryptocurrencies**, commodities, or even assets that are not traditionally considered to be digital, such as real estate or art. There are two main kinds of **tokens**: **fungible tokens** and **non-fungible tokens** (**NFTs**). **Fungible tokens** are interchangeable and have a uniform value, such as **cryptocurrencies** like **bitcoin** or **ether** and follow the **ERC-20** standard. **NFTs**, on the other hand, are unique and have a distinct value, such as digital art or collectibles; they follow the **ERC-721** standard.

NFTs have gained fame because of their appropriation by the art world in which they triggered their own controversies, largely discussed—or fought—when some big sale made the headlines: in 2021, the digital artist known as Beeple sold an **NFT** of his work for $69 million at Christie's. This sale placed Beeple, who had never sold a print for more than $100, among the most valuable living artists in the world. As an **NFT** is a **token** associated with a digital artwork and not the artwork itself, you may think that buying a **NFT**, apart from the bragging rights you get over a digital entity, is quite absurd (the purchase of a work in **NFT** is not necessarily associated with the right to exploit it commercially). However, the accusation of uselessness is more related to the overall allegations expressed about art in general. Most importantly, **NFTs** do not only apply to the art world, which is only a fraction of it. For instance, a **NFT** concert ticket could be a unique digital asset that represents ownership of a specific seat at a concert. In this fictional case, the ownership of the **NFT** ticket is recorded on a **blockchain** network, making the ticket's authenticity verifiable and secure. Additionally, the **NFT** ticket may have

Applications décentralisées (dApps)

Une **application décentralisée** (dApp, *Decentralized Application*), est un type d'**application** fonctionnant sur une **blockchain** et qui n'est, dès lors, pas contrôlée par une seule entité. Par rapport aux habituelles applications centralisées (comme sur l'App Store), les **dApps** sont plus résistantes à la censure et aux dysfonctionnements.

Jetons (*tokens*)

Un **jeton** (*token*) est une unité de valeur émise et gérée sur un réseau **blockchain**. Les **jetons** peuvent représenter des **crypto-monnaies**, des marchandises, ou même des actifs qui ne sont pas traditionnellement considérés comme numériques, tels que l'immobilier ou l'art. Il existe deux principaux types de **jetons**: les **jetons fongibles** et les **jetons non fongibles** (*non-fungible tokens*, **NFT**). Les **jetons fongibles** sont interchangeables et ont une valeur uniforme, comme les **crypto-monnaies** telles que le **bitcoin** ou l'**ether** et suivent la norme **ERC-20**. Les **NFT**, en revanche, sont uniques et ont une valeur distincte, comme l'art numérique ou les objets de collection ; ils suivent la norme **ERC-721**.

Les **NFT** sont devenus célèbres en raison de leur appropriation par le monde de l'art, notamment à partir du moment où une vente importante fit la une des journaux : en 2021, l'artiste Beeple cédait un **NFT** d'une œuvre pour 69 millions de **dollars** chez Christie's. Cette vente a placé Beeple, qui n'avait jamais vendu d'œuvre pour plus de 100 dollars, parmi les artistes vivants les plus valorisés au monde. Comme un **NFT** est un **jeton** associé à une œuvre d'art numérique et non l'œuvre elle-même, on peut penser que l'achat d'un **NFT**, hormis le droit de se vanter de ses droits sur une entité numérique, est assez absurde (l'achat d'une œuvre en **NFT** n'est pas forcément associé au droit de l'exploiter commercialement). Cependant, l'accusation d'inutilité des **NFT** mériterait d'être corrélée à celle de l'art en général, et plus précisément du marché de l'art contemporain. Surtout, les **NFT** ne s'appliquent pas uniquement au monde de l'art qui n'en est seulement qu'une fraction. Par exemple, un billet de concert en **NFT** représenterait la propriété d'une place spécifique à un concert. Dans ce cas fictif, la propriété du billet **NFT** est enregistrée sur un

additional features such as the ability to transfer ownership or access special perks at the concert, which can increase its value.

REWARDING PARTIES: CREATING VALUE AND REVENUE

We could wonder why anyone would want to participate in a **blockchain** other than being a simple **user**? Like **cypherpunks**, it can be because of one's ideology and their will to change the current systems. But values don't always pay the bills: we'll dig more into the financial aspect of it which drives a lot of **miners**.

Indeed, participating in a **blockchain** as an active party can be financially rewarding. One type of reward is the **block reward**, which is a fixed amount of **cryptocurrency** that is given to the **miner** who successfully mines a **block**. This reward is a key component of a **mineable blockchain protocol**, such as **Bitcoin** that uses computing power to validate **transactions**. Because **mining** can require expensive equipment in order to have hardware powerful enough to find the **nonce**, **miners** can join a "**mining pool**" in order to combine their computational resources to strengthen their probability to find a **block**. In a **mining pool**, the **block reward** is then split amongst all **miners** in the pool according to the amount of work they contributed to the collective effort.

réseau **blockchain**, ce qui rend l'authenticité du billet vérifiable et sûre. En outre, le billet **NFT** peut avoir des caractéristiques supplémentaires telles que la possibilité de transférer la propriété ou d'accéder à des avantages spéciaux lors du concert, ce qui peut augmenter sa valeur.

RÉCOMPENSER LES ACTEURS : CRÉER DE LA VALEUR ET DES REVENUS

On pourrait se demander pourquoi quelqu'un souhaiterait contribuer à une **blockchain** autrement que comme simple **utilisateur**. Au même titre que les **cypherpunks**, cela peut relever de l'idéologie et de la volonté de faire évoluer les systèmes existants. Cependant, les valeurs ne paient pas toujours les factures : nous allons nous pencher sur l'aspect financier qui est le moteur de nombre de **mineurs**.

Il est vrai que contribuer à une **blockchain** de façon active peut se révéler lucratif. Un type de gain est la **récompense de minage** (*block reward*) qui est un montant fixe de **crypto-monnaies** donné à la personne qui réussit à **miner** un **bloc**. Cette récompense est un élément-clé d'un **protocole** comme **Bitcoin**, qui utilise la puissance de calcul pour valider les **transactions**. Étant donné que le **minage** peut nécessiter un équipement coûteux afin de disposer d'un matériel suffisamment puissant pour trouver le ***nonce***, les **mineurs** peuvent rejoindre un groupe de **minage collaboratif** (*mining pool*) afin de combiner leurs ressources de calcul pour renforcer leur probabilité de trouver un **bloc**. Dans une *mining pool*,

A **coin** can therefore be referred to as "**mineable**", if its **blockchain** implements a **protocol** where its emission is done block by block. To create new **tokens** (**minting**) on **Ethereum** (such as a **cryptocurrency**, a **Decentralized Autonomous Organizations (DAOs) token** membership, a **NFT**) you would have to *mint it*: that is to design the **token** (its specifications such as its total supply, its symbol and any features it may have), write a **smart contract** designed to automatically create and distribute the new **token** based on certain conditions, such as a specific date or the completion of a fundraising campaign and deploy this **smart contract** on the **blockchain** by uploading the code and paying the **transaction fee**. The **smart contract** will then automatically create and distribute new **tokens** if the conditions set in the code are met.

Tokens can be created during an **initial coin offering (ICO)**, in which a new **blockchain project**, announced by a **whitepaper**, sells a portion of its **tokens** to early investors in exchange for money. This money is typically used to fund the development of the **project** and bring it to market. After the **ICO**, the **tokens** are typically traded on marketplaces, allowing people to buy and sell them just like they would any other **cryptocurrency**. Another way to create value and gather communities around new **cryptocurrencies** is through **airdrops**, where a certain amount of **tokens** is given away for free to a specific group of **users** or holders that have been previously **whitelisted**. These **rewards** can help to increase awareness and adoption of a new service.

As we've seen before, **cryptocurrencies** value can fluctuate, and some processes allow for a better control of their value. On **Bitcoin**, the **block reward** decreases by 50% over time (every four years) in a process known as **halving**. This is done to control the inflation rate of the currency and to ensure that there's a limited amount of **bitcoins** (21 million at most) as rarity creates value. Following this idea, a **token** **burn** can also create value by decreasing the supply of a **token**, by permanently destroying it or making it unavailable for use thus increasing its scarcity and potentially causing the value of the **token** to rise. While demand stays the same, the supply drops.

la **récompense de minage** obtenue est répartie entre les **mineurs** du groupe en fonction de leur quantité de travail fournie.

Un **crypto-actif** (*coin*) peut donc être qualifié de ***mineable*** (exploitable) si sa **blockchain** met en place un **protocole** où son émission se fait bloc par bloc. Pour créer de nouveaux **jetons** (processus de ***minting***) sur **Ethereum** (comme une **crypto-monnaie**, une adhésion à des **organisations autonomes décentralisées**, un **NFT**), vous devez les *minter* : concevoir le **jeton** (ses spécifications telles que le stock disponible, son symbole et toutes les caractéristiques qu'il peut avoir), écrire un **contrat programmable** (*smart contract*) conçu pour créer et distribuer automatiquement le nouveau **jeton** en fonction de certaines conditions, telles qu'une date spécifique ou la réalisation d'une campagne de collecte de fonds, et déployer ce **contrat programmable** sur la **blockchain** en téléchargeant le code et en payant les **frais de transaction**. Le **contrat** créera et distribuera alors automatiquement de nouveaux **jetons** si les conditions définies dans le code sont remplies.

Les **jetons** peuvent être émis lors d'une **levée de fonds en crypto-monnaies** (ICO), dans laquelle un **projet**, annoncé par un **livre blanc** (*whitepaper*), met en vente une partie de ses **jetons** aux primo-investisseurs. Après la levée de fonds, les **jetons** sont généralement échangeables sur des places de marché comme pour n'importe **crypto-monnaie**. Un autre moyen de créer de la valeur et de rassembler des communautés se fait au travers de récompenses (***airdrops***), où une certaine quantité de **jetons** est donnée gratuitement à un groupe spécifique de personnes qui ont été préalablement inscrits sur la **liste blanche** (*whitelist*). Les **récompenses** peuvent contribuer à accroître la notoriété et l'adoption d'un service.

Comme nous l'avons déjà vu, si la valeur des **crypto-monnaies** peut fluctuer, certains processus permettent de mieux la contrôler. Sur **Bitcoin**, la **récompense de minage** diminue de 50 % au fil du temps (tous les quatre ans) dans un processus connu sous le nom de ***halving*** (littéralement : « réduction de moitié »). Celui-ci est fait pour contrôler le taux d'inflation de la monnaie et pour s'assurer qu'il y aura toujours une quantité limitée de **bitcoins** (21 millions au maximum),

In fine, blockchain-powered **tokens** and shared ownership addresses the fundamental issue with centralized networks where value is accumulated by a single organization. Thanks to decentralization, **users** become the content owner of their data and have an equal opportunity to participate in the **project**. Until now, even though decentralization has helped create the stable, robust infrastructure on which the **World Wide Web** lives, it has at the same time allowed a handful of centralized entities (the GAFAM – Google, Amazon, **Facebook/Meta**, Apple, Microsoft) to have a stronghold on large swathes of cyberspace. Many early crypto adopters therefore felt that the **Web** required too much trust. That is, most of the **Web** that people know and use today relies on trusting a handful of private companies to act in the public's best interests. The question then arises as to whether **blockchain** could usher in a third age of the **Web**, the **Web3**.

WEB3: A NEW WEB ERA

From the first version of the **Web**, retrospectively called "**Web 1.0**", developed in the early 1990's, which was primarily used for accessing and sharing information on personal webpages, it evolved in the early 2000's into "**Web 2.0**", which refers to the more interactive and dynamic version of the **Web**, that we still know today in the early 2020's. **Web 2.0** services, such as social media, blogging platforms,

car la rareté crée de la valeur. En suivant cette idée, le processus de **destruction de jetons** (*burn*), de façon permanente ou en le rendant indisponible pour l'utilisation, augmente sa rareté et fait potentiellement augmenter sa valeur. Alors que la demande reste la même, l'offre diminue.

In fine, les **jetons** pilotés par la **blockchain** et la propriété partagée du réseau répondent au problème fondamental des réseaux centralisés où la valeur est accumulée par une seule organisation. Grâce à la décentralisation, les personnes possèdent leurs données et ont une chance égale de participer au projet. Jusqu'à présent, même si la décentralisation a contribué à créer l'infrastructure stable et robuste sur laquelle vit encore le **World Wide Web** contemporain, elle a en même temps permis à une poignée d'entités centralisées (les GAFAM : Google, Amazon, **Facebook/Meta**, Apple, Microsoft) d'avoir la mainmise sur de larges pans du cyberespace. En effet, la majeure partie du **Web** que les gens connaissent et utilisent aujourd'hui repose sur la confiance donnée à une poignée d'entreprises privées d'agir dans le sens de l'intérêt public. Se pose alors la question de savoir si la **blockchain** pourrait ouvrir un troisième âge du **Web**, le **Web3**.

WEB3 : UNE NOUVELLE ÈRE DU WEB

Depuis la première version du **Web**, rétrospectivement appelée « **Web 1.0** », développée au début des années 1990 et qui était principalement utilisée pour accéder et partager des informations sur des pages **Web** personnelles, le **Web** a évolué au début des années 2000 vers le « **Web 2.0** », qui fait référence à une approche plus dynamique et participative encore en vigueur au début des années 2020.

and user-generated content have revolutionized the way we communicate, access information, and do business. It has also raised issues regarding concepts of privacy, ownership and security as the digital age allowed for new forms of surveillance and piracy, creating the need for new data-encryption technologies.

In this respect, the term "**Web3**" was coined by Gavin Wood in 2014 to name the next generation of **Web** where decentralization is key. **Web3** proposes an all-in-one ecosystem: a monetary system (**Bitcoin**) within an economic system (**DeFi**) to exchange digital properties (**NFT**), all managed by a new **governance** systems such as **Decentralized Autonomous Organizations (DAOs)** through **decentralized identifier (DID)**.

A **Decentralized Autonomous Organizations (DAOs)** operates based on a set of predetermined rules encoded into **smart contracts**. **DAOs** work through the use of a **decentralized identifier (DID)** which ensures the secure and private management of member identities and voting power.

A **decentralized identifier (DID)** is a unique identifier that is owned and controlled by the individual rather than a central authority thus opposing **Web 2.0**'s tendency toward the monetization of data and invasion of privacy. **Web3** allows with this **Web3 identity** for a more "self-designed" identity that would allow **users** to fully immerse themselves in the **metaverse**, a virtual world where **avatars** and **virtual reality** intersect.

This new era of the **Web** offers a wide range of possibilities for both individuals and businesses. As people gain the ability to own and control their own identity, new opportunities can open up for commerce, communication, and even entertainment. However several artists have highlighted the paradoxes endemic to **blockchains** and **NFTs**, with, on the one hand, its promise of equity and responsibility, and, on the other, implementations that are often quite capitalistic in nature. One example of this is the **play-to-earn** model.

Through the years, it seems that the true economic potential of **NFTs** might emerge not in the realm of art which, until now, has garnered

Les services du **Web 2.0**, tels que les médias sociaux, les plateformes de blogs et les contenus créés par les **utilisateurs** ont révolutionné la façon de communiquer, d'accéder à l'information et de faire des affaires. Ils ont également soulevé des questions concernant les concepts de vie privée, de propriété et de sécurité, car cette ère numérique a engendré de nouvelles formes de surveillance et de piratage, créant ainsi le besoin de nouvelles technologies de chiffrement des données et de protection de la vie privée.

Dans cette optique, le terme de « **Web3** » a été inventé par Gavin Wood (cofondateur d'**Ethereum**) en 2014 pour préfigurer la prochaine génération du **Web** où la décentralisation est clé. Le **Web3** propose un écosystème tout-en-un : un système monétaire (**Bitcoin**) au sein d'un système économique (**DeFi**) pour échanger des propriétés numériques (**NFT**), le tout géré par un nouveau système de **gouvernance** (**DAO**) grâce aux **identifiants décentralisés** (**DID**).

Une **organisation autonome décentralisée** (**DAO**) fonctionne sur la base d'un ensemble de règles prédéterminées encodées dans des **contrats programmables**. Les **DAO** utilisent des **identifiants décentralisés** (**DID**) pour assurer la gestion sécurisée et privée de l'identité des membres et des votations.

Un **identifiant décentralisé** (**DID**) est détenu et contrôlé par un individu plutôt que par une autorité centrale, s'opposant ainsi à la tendance du **Web 2.0** à la monétisation des données et à l'invasion de la vie privée. Le **Web3** autorise potentiellement la production d'une identité virtuelle mieux contrôlée et auto-définie (**identité Web3**) où se croisent **avatars** et **réalité virtuelle**.

Cette nouvelle ère du **Web** offre un large éventail de possibilités tant pour les particuliers que pour les entreprises. À mesure que les gens acquièrent la capacité de posséder et de contrôler leur propre identité, de nouvelles possibilités s'ouvrent pour le commerce, la communication et même le divertissement. Cependant, plusieurs artistes ont souligné les paradoxes endémiques des **blockchains** et des **NFT**, avec d'une part une promesse d'équité et de responsabilité, et d'autre part des mises en œuvre qui sont souvent capitalistes – dont le modèle du ***play-to-earn*** (« jouer-pour-gagner ») est un exemple.

the most media attention, but rather that of video gaming. One of the most well-known games using the **play-to-earn** economic model is **Axie Infinity**, launched in 2018, which offered the chance to purchase and collect, trade and battle **NFTs** of digital Pokemon-like creatures called Axies in order to gain revenue. The **play-to-earn** paradigm has given rise to "guilds'' which play an intermediary role between the "managers" (owners of **NFTs**), and players: if they cannot purchase the **NFTs** in the game (like Axies) because they are too expensive, players—called **scholars** in that context—can "rent" them in order to gain revenue: this is referred to as a **scholarship**. This activity has grown to be a new economic model, quite representative in how **Web3** could work by allowing people to transfer data across platforms and which brought about major social transformations in the countries in which the players are based.----------

---

The case of **play-to-earn** shows that it is difficult to know whether the problems that **Web3** is supposed to solve (those of GAFAM) will not be replaced by the emergence of new areas of control (increased inequality, censorious voting, insecurity related to individual management of digital identifiers, complexity of access, etc.) potentially more harmful. The **cypherpunk ideology** is an echo to the one of the tech-idealists (such as John Perry Barlow) who saw in the early days of the **Web** the possibility for a space independent from government control and free of privilege and prejudice—but which instead became predominantly owned and operated by capitalistic-oriented companies. At this stage, it is still difficult to know if **Web3** and its sometimes utopian ideologies will not be just a repetition of history.---

---

L'un des jeux vidéo les plus connus utilisant le modèle économique du ***play-to-earn*** est **Axie Infinity** (2018), qui propose d'acheter, de collectionner, d'échanger et de combattre des **NFT** de créatures numériques ressemblant à des Pokemons, les **Axies**, afin d'en tirer des revenus. Le paradigme du ***play-to-earn*** a donné naissance à des « guildes » qui jouent un rôle d'intermédiaire entre les « managers » (propriétaires des **NFT**), et les joueurs : s'ils ne peuvent pas acheter les **NFT** du jeu (comme les **Axies**) car ceux-ci sont trop chers, les joueurs – appelés ***scholars*** (locataires) dans ce contexte – peuvent les « louer » afin de gagner des revenus : on parle alors de ***scholarship*** (contrat de location). Cette activité est représentative de la façon dont le **Web3** peut fonctionner en permettant aux gens de transférer des données d'une plateforme à l'autre, et a entraîné des transformations sociales majeures dans les pays dans lesquels les joueurs sont basés.----------

---

Le cas du ***play-to-earn*** montre qu'il est difficile de savoir si les problèmes que le **Web3** est censé résoudre (ceux des GAFAM) ne seront pas remplacés par l'apparition de nouvelles zones de contrôle (accroissement des inégalités, vote censitaire, insécurité liée à la gestion individuelle des identifiants numériques, complexité d'accès, etc.) potentiellement plus néfastes. L'**idéologie cypherpunk** à l'origine de **Bitcoin** est un écho à celle des « tech-idéalistes » (tels que John Perry Barlow) qui voyaient dans les premiers jours du **Web** la possibilité d'un espace de liberté, indépendant du contrôle gouvernemental, et affranchi de privilèges et de préjugés –, qui est pourtant devenu majoritairement exploité par des entreprises capitalistes. À ce stade, il est encore difficile de savoir si le **Web3** et ses idéologies parfois utopiques ne seront pas qu'une répétition de l'histoire.----------

---

 Punk	 Punk (Left)	 Punk (Right)	 Cryptography	 Cypherpunk (Symbol)	 Cypherpunk	 Cypherpunk (Left)
 Cypherpunk (Right)	 Satoshi Nakamoto	 Bitcoin	 bitcoin	 Protocol	 Project	 Whitepaper
 Internet	 Web	 Web 1.0	 Web 2.0	 Web3	 Interrelation System	 Centralized System
 Polarized System	 Distributed System	 Chain	 Main chain	 Sidechain	 On-chain	 Off-chain
 InterPlanetary File System (IPFS)	 Fork	 Lightning Network	 Blockchain Protocol	 Blockchain Symbol	 Consensus	 Private Blockchain
 Public Blockchain	 Node	 Trading	 Exchange	 Decentralized Exchange (DEX)	Transaction	Decentralized Finance (DeFI)
Governance	Decentralized Autonomous Organization (DAO)	Avatar #1	Avatar #2	Decentralized Identifier (DID)	Web3 Identity	Decentralized App (dApp)
Smart contract	Initial Coin Offering (ICO)	Staking	Airdrop	Whitelist	Asymmetric Cryptography	Public Key
Private Key	Seed (Mnemonic Phrase)	Signing	Address	Ledger	Crypto Wallet	Web3 Wallet
Multisignature	Block	Block Explorer	Memory Pool (Mempool)	Scalability	Genesis Block	Nonce

Target	Halving	Mining	Mineable	Block reward	Minteable	Burn
Encryption	Double Spending	Merkle tree	Hash Function	Secure Hash Algorithm 256 bits (SHA-256)	Hash	Ethereum
Ether	Fungible	ERC-20	Non-Fungible	ERC-721	None-Fungible Token (NFT)	Transaction Fee
Gas	Gwei	Satoshi	Coin Mixer	Coin	Altcoin	Cryptocurrency
Stablecoin	Central Bank Digital Coin (CBDC)	FIAT Money	Token	Token #1	Token #2	Token #3
Token #4	Token #5	Token #6	Pound Sterling	New Sheqel	Dollar	Dollar (CBDC)
Dollar Stablecoin (USDC)	Euro	Euro (CBDC)	Euro Stablecoin (EUROC)	Yuan	Yuan (CBDC)	Yuan (Stablecoin)
Hashrate	Mining Rig	Mining Pool	Proof-of-Work (PoW)	Proof-of-Stake (PoS)	Miner (Front)	Miner (Left)
Miner (Right)	Cloud	Confirmation	Play-to-Earn	Virtual Reality	Metaverse (Front)	Metaverse (Left)
Metaverse (Right)	Scholarship	Scholar	Axie Infinity	Axie Infinity Shards (AXS)	Ronin (RON)	Smooth Love Potion (SLP)

Script	Application	Database	Server	Oracle	Data Register	Incrementation
Economy	FIAT Money Stack	Binance	Binance Coin (BNB)	Tether	Tether (USDT)	Tezos
Tezos (TZS)	Ripple	Ripple (XRP)	Investor #1	Investor #2	User #1	User #1 Neg.(Front)
User #1 (Left)	User #1 (Right)	User #2 (Front)	User #2 Neg. (Front)	User #2 (Left)	User #2 (Right)	Team
Company	Coinbase	Discord	Metamask	Meta	Twitter	Instagram
Circled Digit One	Circled Digit One (Negative)	Circled Digit Two	Circled Digit Two (Negative)	Circled Digit Three	Circled Digit Three (Negative)	Circled Digit Four
Circled Digit Four (Negative)	Circled Digit Five	Circled Digit Five (Negative)	Circled Digit Six	Circled Digit Six (Negative)	Circled Digit Seven	Circled Digit Seven (Negative)
Circled Digit Eight	Circled Digit Eight (Negative)	Circled Digit Nine	Circled Digit Nine (Negative)	Circled Digit Zero	Circled Digit Zero (Negative)	Plus Sign
Minus Sign	Multiplication Sign	Division Sign	Equals Sign	Check	Cancel	Power on
Timer Clock	Percent Sign	Download	Exchange (Arrow)			

CREDITS

RESEARCH TEAM

→ Anthony Masure (applicant), associate professor, dean of research, Geneva University of Art and Design (HEAD – Genève, HES-SO), co-founder of Hint3rland

→ Guillaume Helleu, associate researcher at Geneva University of Art and Design (HEAD – Genève, HES-SO), co-founder of Hint3rland

→ Océane Juvin, graphic designer, author of the typeface Cryptokit

FUNDING

Bureau de la stratégie numérique of HES-SO Genève and Geneva University of Art and Design (HEAD – Genève, HES-SO), 2022-2023.

GRAPHIC DESIGN → E+K — Élise Gay & Kévin Donnot

TYPEFACE → IBM Plex Sans

PRINTING → Lulu (Raleigh, NC, USA)

MAY 2023

HEAD Genève

CRÉDITS

ÉQUIPE DE RECHERCHE

→ Anthony Masure (requérant du projet), professeur associé, responsable de la recherche, HEAD – Genève (HES-SO), cofondateur de Hint3rland

→ Guillaume Helleu, chercheur associé à la HEAD – Genève (HES-SO), cofondateur de Hint3rland

→ Océane Juvin, designer graphique, autrice du caractère Cryptokit

FINANCEMENT

Bureau de la stratégie numérique de la HES-SO Genève et HEAD – Genève (2022-2023)

CONCEPTION GRAPHIQUE → E+K — Élise Gay & Kévin Donnot

CARATÈRE TYPOGRAPHIQUE → IBM Plex Sans

IMPRESSION → Lulu (Raleigh, NC, États-Unis)

MAI 2023

WWW.CRYPTOKIT.CH

Hes·so Genève