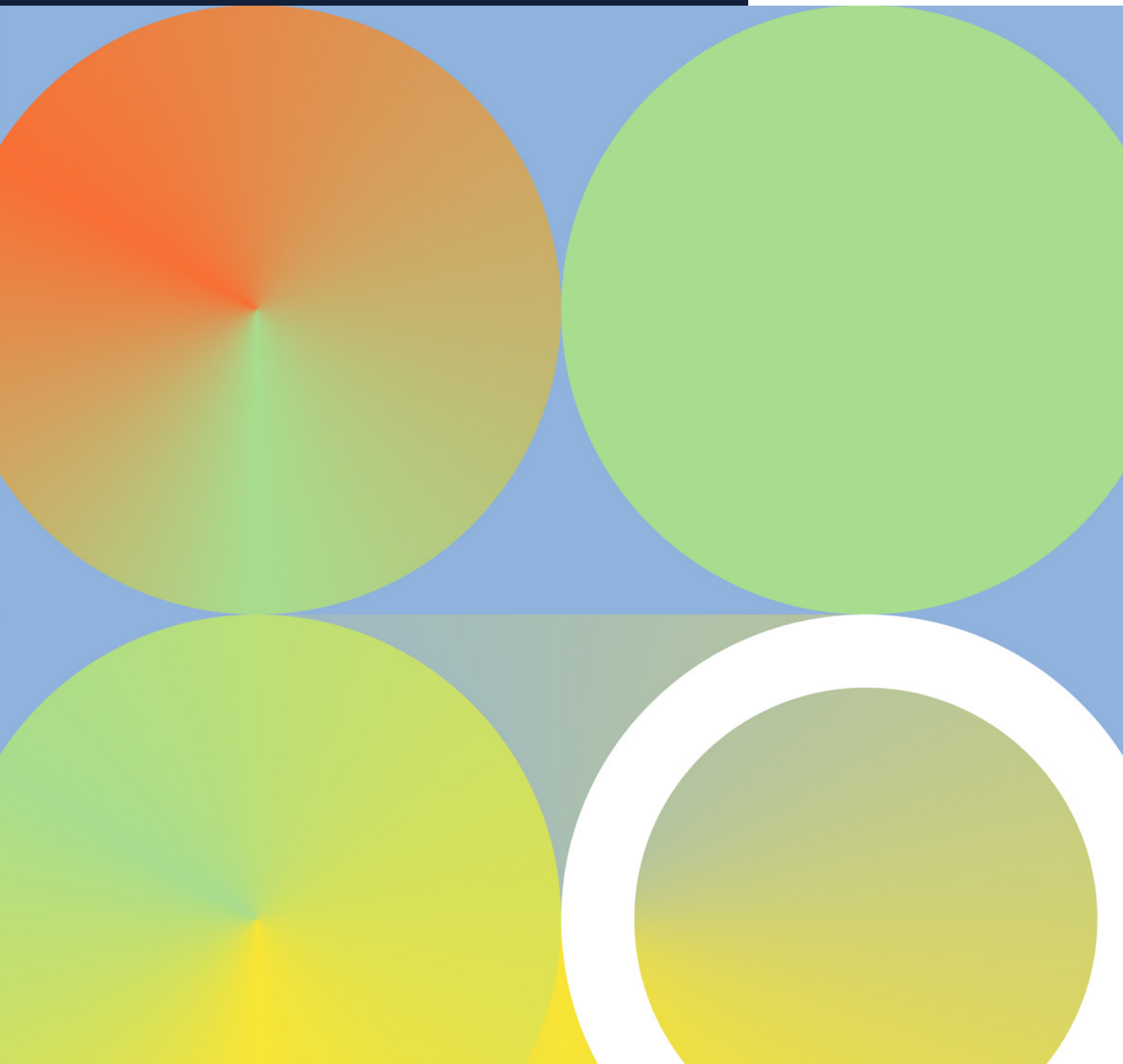
La blockchain peut-elle (vraiment) remplacer le DNS ?

DOSSIER THÉMATIQUE

afnic

Internet
made in France



Sommaire

DNS – Présentation rapide

Un espace de nommage est un espace dans lequel stocker des noms, un contenant dans lequel chaque nom est unique. Les deux principaux espaces de nommage d'Internet sont aujourd'hui les adresses IP et les noms de domaine.

Le DNS est le service de nommage historique d'Internet.[1] Il permet d'associer une adresse IP (identifiant unique de tout périphérique connecté au réseau) composée d'une combinaison de chiffres, à un nom de domaine facilement mémorisable et plus stable dans le temps. Par exemple, www.afnic.fr est associé vers l'adresse IP 2a00:e00:0:5::2.

Le DNS assure la fonction d'annuaire téléphonique pour Internet. Il permet également d'assurer le service de résolution de ces noms, qui revient à « appeler » ces numéros depuis votre répertoire téléphonique.
Le DNS conçu dans les années 80, vise à assurer une gestion dynamique, évolutive et hiérarchique de son espace de nommage. C'est une pierre angulaire d'Internet puisque la plupart des applications en réseau utilisent cette technologie pour se connecter à Internet.

Le nombre de requêtes DNS réalisé chaque jour est considérable. Il faut comptabiliser l'ensemble des utilisateurs de l'Internet ainsi que les services et applications. Quelques chiffres : plus de 100 milliards de requêtes par jour reçues par les serveurs dits « racines » de l'Internet[2] ; plus de 2 000 milliards sur les infrastructures de CloudFlare[3], opérateur notamment de services distribués de serveur de noms de domaine ; plus de 2 milliards sur nos infrastructures à l'Afnic reçues chaque jour.

Cette puissance fait du DNS un vecteur d'attaques intéressant et a été, souvent et de manière incorrecte, identifié comme un point de défaillance unique (SPOF, *Single Point of Failure*) d'Internet, nécessitant d'être remplacé. Au cours des quarante dernières années, de nombreuses tentatives ont été lancées pour remplacer le DNS, dont dernièrement les systèmes de nommage basés sur la blockchain (ou chaîne de blocs).

La blockchain pour remplacer le DNS

Substituer au DNS un système de nommage basé sur la blockchain revient à remplacer la monnaie par de la cryptomonnaie. A l'instar de cette dernière qui doit encore surmonter des obstacles tels que l'aspect pratique, l'évolutivité et l'acceptation avant de devenir le moyen d'échange principal, le système de nommage basé sur la chaîne de blocs en est à ses balbutiements et ne peut être considéré à l'heure actuelle comme le concurrent du DNS.

Penchons-nous sur les arguments avancés par les partisans du remplacement du DNS par la chaîne de blocs.

Les arguments mis en avant pour remplacer le DNS

Les arguments en faveur du remplacement du DNS sont multiples. Sa structure poserait des problèmes de tolérances aux pannes et vulnérabilités face aux cyberattaques, ainsi qu'un risque de censure et des vulnérabilités en termes de confidentialité.

Le DNS, par conception, est une architecture distribuée (comme un arbre inversé). Elle suit un modèle de gouvernance hiérarchique qui fonctionne à partir d'une racine centrale unique, avec la racine[4] en haut et les TLD[5] (*Top-Level Domains* ou Domaines de premier niveau, comme « .FR » ou « .COM ») en-dessous. L'ICANN, en sa qualité d'organisation de coordination permettant l'établissement des règles de fonctionnement et les opérateurs de noms de domaine déterminent ce qui peut être ajouté ou retiré de la zone racine (via sa filiale PTI[6]) et des noms de domaine de premier niveau.

Les pays qui ont la gestion de leur domaine de premier niveau ont la possibilité de poser leurs propres règles quant à l'enregistrement de noms de domaine et ainsi autoriser, ou non, l'enregistrement de certains termes. Ils ont également la possibilité de mettre en place des règles de filtrages d'accès aux noms de domaine[7] limitant l'accès à certaines adresses, ces demandes s'adressant aux opérateurs de résolveurs (les fournisseurs d'accès principalement) et non aux opérateurs de noms de domaine de premier niveau.

Le DNS subit des attaques, comme le déni de service distribué (DDoS, *Distributed Denial of Service*), le spoofing DNS ou l'amplification. Parce qu'elles sont nombreuses et que leurs répercussions sont potentiellement très importantes, certains disent du DNS qu'il est un SPOF d'Internet – (un SPOF se définissant par la défaillance généralisée d'un système provoquée par une seule source). Cette notion reste toutefois théorique et erronée : même si le DNS a été impliqué dans certaines pannes importantes[8,9], jamais depuis le début d'Internet, le monde n'a connu de panne généralisée de la résolution DNS. Son modèle hiérarchique, réparti et délégué est au contraire une force qui permet aux ressources d'infrastructures DNS de continuer à fonctionner alors que d'autres sont victimes d'abus sur leurs infrastructures.

Des extensions de sécurité du DNS, comme DNSSEC[10] (Domain Name System Security Extensions), réduisent en grande partie ces attaques. Mais le déploiement de DNSSEC à l'échelle mondiale reste problématique, car souvent jugé complexe sur les plans administratif et technique. C'est le cas de la plupart des composants permettant de renforcer le niveau de sécurité d'une ressource d'infrastructure. Le DNS ne doit pas faire exception. On estime ainsi aujourd'hui le pourcentage de validation DNSSEC à seulement environ 30 %[11] au niveau mondial.

Si DNSSEC assure l'intégrité de la réponse à une requête DNS, encore aujourd'hui, la majorité des requêtes et réponses DNS ne sont pas réalisées via des protocoles chiffrés. Selon son positionnement dans la chaîne de résolution, cela peut permettre d'analyser les informations relatives aux données de navigation des utilisateurs. Afin de renforcer et protéger les données de navigation accessibles via le DNS, diverses solutions pour renforcer la confidentialité des requêtes ont été implémentées et déployées. Parmi ces solutions, les protocoles de chiffrement DoT[12] (DNS over TLS) et DoH[13] (DNS over HTTPS). Ces solutions représentent environ un quart[14] des requêtes DNS et leur part ne cesse d'augmenter.

Dernier point sujet à de nombreux débats : les données des titulaires et leur visibilité. Les informations d'un titulaire de nom de domaine peuvent être consultées publiquement avec des services d'interrogation comme le WHOIS ou RDAP. Les pratiques des registres gestionnaires de domaine de premier niveau divergent encore mais si des données personnelles sont accessibles par défaut, pour beaucoup d'autres, elles sont par défaut anonymisées et ne permettent pas d'identifier un titulaire depuis ces services. Aujourd'hui la vaste majorité des bureaux d'enregistrement ont adopté les règles des registres ou mis en place des solutions pour anonymiser les données personnelles de ces bases accessibles publiquement, y compris pour des registres ne proposant pas ce masquage par défaut.

30%

C'est l'estimation du pourcentage de validation DNSSEC.

20%

C'est la quantité de requêtes DNS qui utilisent les protocoles de chiffrements comme DoT et DoH.

Systèmes de nommage basés sur la blockchain

Depuis quelques années, plusieurs projets développent leur propre système de nommage basé sur la blockchain pour tenter de remplacer le DNS. Si certains le conservent néanmoins comme infrastructure de base pour créer un protocole de nommage décentralisé, comme Handshake[15] ; d'autres en revanche cherchent à être totalement indépendants du DNS à l'instar de Namecoin[16].

Les systèmes de nommage basés sur la Blockchain sont souvent utilisés pour nommer des portefeuilles *(wallets)* et d'autres objets comme les NFT (*non-fungible tokens* ou jetons non fongibles).

De la même manière que le DNS est utilisé pour résoudre un nom de domaine, c'est-à-dire trouver son adresse IP correspondante, les systèmes de nommage basés sur la blockchain, comme ENS (Ethereum Name Service[17]), doivent assurer le mappage entre des noms et des adresses de wallets. Ainsi, « alice.eth », correspond à « e32fre43f584bnf2784b3 ».

Plusieurs systèmes de nommage basés sur la blockchain sont actuellement utilisés :

- BitDNS
- Solana Name Service
- EmerDNS
- Diode
- Ethereum Name Service
- RIF Name Service
- Handshake
- Namecoin
- Unstoppable domains
- PeerName
- Emercoin
- Et bien d'autres

Blockchain : une solution possible

Étudions maintenant les avantages d'un système de nommage basé sur la blockchain par rapport au DNS : décentralisation, sécurité, protection contre la censure et confidentialité.

L'objectif premier de la blockchain dans ce contexte serait de se libérer de l'organisation de gouvernance de la racine du DNS, l'ICANN, mais également des registres et des bureaux d'enregistrement. La blockchain propose une architecture décentralisée où les mêmes informations sont stockées et distribuées entre plusieurs nœuds, évitant le recours à toute autorité centrale.

En répartissant les données sur tout le réseau plutôt que dans un emplacement central, la blockchain ne peut être définie comme un SPOF et est donc immunisée contre les attaques DDoS. La falsification des données de la blockchain est également plus complexe car si une copie tombait entre des mains malveillantes, seule cette copie serait compromise, et non l'intégralité des copies dans la chaîne.

Avec le DNS, nous avons vu que la censure est possible, soit en bloquant la résolution d'un domaine, soit en prenant le contrôle du domaine en lui-même, par voie légale ou administrative. Avec la décentralisation offerte par la chaîne de blocs, il devient quasiment impossible de bloquer ou de prendre le contrôle[18] d'un espace de noms, les noms étant diffusés sur l'ensemble du réseau et non plus stockés sur une base de données centrale.

Enfin, la blockchain permet une protection de la vie privée. Les propriétaires de noms dans la blockchain peuvent enregistrer et gérer leurs noms via un pseudonyme. La propriété des noms est protégée par de la cryptographie à clé publique. Et même si les transactions (création, suppression ou modification des informations rattachées à un nom) sont accessibles au public, il est difficile de déduire des informations relatives à l'utilisateur qui les a réalisées.

Toutefois, si un utilisateur a transmis une identité à une plateforme dédiée pour acquérir des cryptomonnaies par exemple, avant de les envoyer sur un portefeuille décentralisé, il sera tout à fait possible de croiser ces informations via ce tiers. La confidentialité ne serait donc pas assurée à 100%. Cette dernière dépend, non pas de la technologie elle-même, mais des règles établies par les organisations qui la déploient. Ici, pas de différence essentielle avec le système DNS.

La blockchain peut-elle remplacer le DNS ?

Si les systèmes de nommage basés sur la chaîne de blocs peuvent combler certaines lacunes du DNS, leur viabilité comme alternative au DNS reste discutable. Plusieurs raisons expliquent cela :

Décentralisation et censure

Les systèmes de nommage basés sur la blockchain sont pensés pour être indépendants de toute autorité centrale, ce qui signifie qu'aucun groupe ou autorité ne devrait pouvoir en prendre le contrôle.

Or, les systèmes de nommage basés sur la blockchain présentent eux aussi une certaine forme de centralisation. Par exemple, dans le cas d'ENS (Ethereum Name Service), un équivalent du DNS pour la blockchain : Amazon héberge plus de deux tiers des nœuds du réseau (cf. figure ci-contre), et près de 50 % d'Ethereum est hébergé aux États-Unis[19]. Cette forme de consolidation de l'architecture pourrait laisser craindre une prise de contrôle par l'une ou l'autre de ces deux parties prenantes majoritaires.

Autre exemple possible de risque de centralisation et faisant l'objet de débats visibles au sein de la communauté cryptomonnaie : l'importance de Lido et les risques[20]. Lido est un protocole décentralisé d'Ethereum qui permet de déposer ses ETH en jalonnement (« staking ») sans pour autant les verrouiller. Lors du dépôt d'ETH, l'utilisateur récupère des jetons stETH, qui représentent le dépôt.

Ce système de jalonnement se base sur un mécanisme de consensus appelé preuve d'enjeu « Proof of Stake » qui permet de garantir que les transactions sont vérifiées et sécurisées sans l'intervention d'une banque ou d'un intermédiaire.

Néanmoins, la croissance rapide de Lido fait craindre une centralisation. Lido a une pénétration du réseau proche d'un tiers du total des preuves de jalonnement, soit le montant de la participation qui relève d'une seule entité. Cela signifie que si Lido atteint 33 % et que survient une attaque ou un bug sur Lido, cela pourrait empêcher le réseau Ethereum de parvenir à un consensus, 66% pour la blockchain Ethereum. Cela signifie qu'Ethereum cesserait de fonctionner correctement.

Adéquation aux besoins des utilisateurs et des entreprises

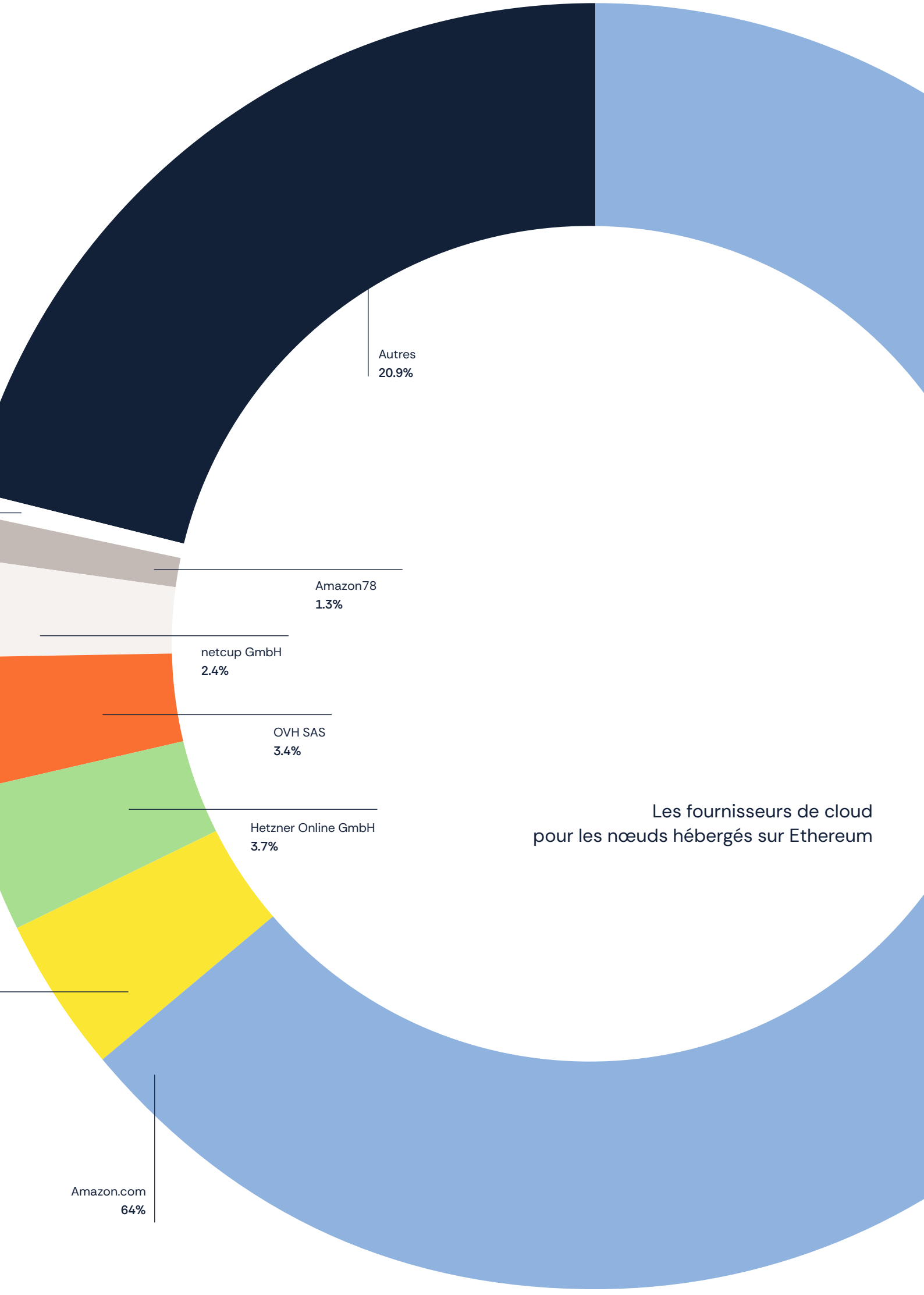
L'objectif des systèmes de nommage est d'associer des noms à des valeurs. Mais aujourd'hui, le DNS est devenu plus qu'une simple solution de mappage pour former une infrastructure pesant des milliards de dollars[21].

Le DNS permet d'associer des noms à des personnes morales et, grâce à son caractère centralisé, il garantit aux parties prenantes de disposer de mécanismes de régulation et de résolution de litiges pour la protection de leurs actifs immatériels[22] (marques et noms de domaine associés).

Plus largement, les acteurs du système des noms de domaine sont très majoritairement encadrés par des règles d'utilisation transparentes, soit élaborées dans le cadre multi-acteurs de l'ICANN (pour les extensions génériques) soit, tout en prenant en compte ce cadre multi-acteurs au niveau national, par un cadre juridique et réglementaire. C'est le cas en France à travers les articles L45 et suivants du code des postes et communications électroniques[23].

Les systèmes de nommage basés sur la blockchain, de par leur nature décentralisée, ne proposent pas à notre connaissance ce type de solution. L'élaboration de systèmes de gouvernance ouverts et transparents permettant l'évolution tout comme l'encadrement de ces systèmes n'a pas à notre connaissance commencé. Ainsi, même si certaines entreprises ont fait l'acquisition de noms[24] dans ces systèmes afin d'éviter le cybersquattage, elles restent dans l'ensemble prudentes[25] et adoptent une position attentiste.

Les fournisseurs de cloud pour les nœuds hébergés sur Ethereum



Les fournisseurs de cloud
pour les nœuds hébergés sur Ethereum

Facilité d'utilisation

Les systèmes de nommage basés sur la blockchain disposent d'intéressantes fonctionnalités mais restent encore complexes à exploiter pour un utilisateur moyen.

Un domaine basé sur la blockchain est une chaîne de hachage. Le hachage est le processus qui consiste à convertir un ensemble de données numériques en un hash, c'est-à-dire en une courte suite binaire qui lui est propre. Chaque bloc possède son propre hash ainsi que celui du bloc précédent, et chaque bloc correspond à une entrée dans la chaîne. Ainsi, le site web d'un domaine (c'est-à-dire les pages) est stocké sous forme de données binaires et l'utilisateur a encore besoin de logiciels ou plugins spécialisés pour pouvoir accéder au contenu du site. Le navigateur Chrome par exemple nécessite un plugin externe pour parcourir les données binaires de la blockchain et afficher le code HTML dans le navigateur. L'intégration de clients pouvant interroger des blockchains n'est pas encore généralisée.

Dans le cas de plusieurs systèmes de nommage basés sur la blockchain, des techniques d'interconnexion sont nécessaires pour accéder correctement à l'information[26]. Cette multiplication des systèmes de nommage les rend enclins aux collisions de noms[27] et, faute de coordination, il est fort probable qu'une application résolvant un nom (par ex. « alice.eth ») obtienne des résultats inattendus. Cette collision de noms est impossible avec le DNS qui est un espace où chaque nom est unique.

Consommation énergétique

Le mécanisme de consensus historique, encore en vigueur pour le Bitcoin par exemple, pour ajouter un bloc dans la blockchain est la preuve de travail (PoW, *Proof of Work*). Ce processus consomme d'importantes quantités d'énergie et de puissance de traitement pour résoudre des énigmes cryptographiques complexes.

Un autre mécanisme de consensus, la preuve d'enjeu (PoS, *Proof of Stake*), utilisé dorénavant sur Ethereum par exemple, consomme beaucoup moins d'énergie mais son utilisation nécessite dans une certaine mesure de centraliser la blockchain, comme nous avons pu le décrire plus haut avec le cas de Lido, ce qui peut aller à l'encontre des principes de base de la blockchain.

Il reste difficile d'avoir une vision globale de l'émission de CO_2 générée par les centaines ou milliers de nœuds différents dans le réseau. Selon les données collectées[28] et évaluées par le Cambridge Centre for Alternative Finance, incluant une estimation de la consommation de ces nœuds, la consommation annuelle du réseau Ethereum est estimée à environ 7 GWh (avec un minimum à 2,28GWh et un maximum à 1922 GWh).

Pour référence, le bilan Carbone 2022 de l'Afnic[29], calculé au 1er trimestre 2023, s'élevait à 690 tCO_2, pour la gestion administrative et technique du registre.
Ramené au nom de domaine, les émissions sont de 153g (calculs réalisés par l'Afnic dans le cadre d'un groupe de travail de registres[30]). Cette valeur inclut non seulement les émissions liées aux serveurs, mais aussi celles des employés et de l'infrastructure immobilière nécessaires à l'hébergement d'un nom de domaine en .fr.

Selon les experts[31], une *transaction* Ethereum, utilisant la preuve d'enjeu représente environ 10g d'émissions de CO_2. Actuellement, on compte en moyenne environ 1 million de transactions Ethereum par jour.

Sur son infrastructure DNS, l'Afnic traite chaque jour environ 1,8 milliard de requêtes DNS sur ses serveurs, dans le cadre de ses services DNS liés au .fr et aux autres extensions que l'association gère techniquement (21 TLDs en tout).

La méthodologie de mesure développée et implémentée par l'Afnic a permis d'évaluer la consommation énergétique de ses serveurs DNS faisant autorité et de son nuage anycast. La consommation énergétique reste très stable, quel que soit le nombre de requêtes reçu. La charge d'utilisation du processeur du serveur, qu'elle soit élevée ou faible, ne fait pas varier la courbe de consommation. Au total, cela représente 15 768 kWh d'électricité par an – soit la consommation énergétique annuelle qu'un peu plus de 3 foyers français en moyenne.

Il convient de souligner que bien qu'une transaction Ethereum et une résolution DNS soient très différentes en termes de fonctionnalités et d'objectifs, elles constituent des services essentiels et très demandés au sein de ces infrastructures.
Il semble déterminant de pouvoir évaluer et expliciter les niveaux de consommation d'énergie et les émissions de CO_2 associées à ces opérations.

Conclusion

Le système de nommage basé sur blockchain suscite un débat passionné quant à sa pertinence pour remplacer le DNS ; il peut apparaître sur certains aspects plus décentralisé que le DNS, et ainsi théoriquement moins exposé à des pannes de disponibilité. Néanmoins, il lui reste de nombreux défis à relever avant d'en devenir une alternative sérieuse, d'autant que les problèmes « résolus » par la blockchain restent théoriques sur le DNS, dont la conception a permis de démontrer une résilience tout à fait exceptionnelle.

Conçu pour être entièrement décentralisé, résistant aux cyberattaques et à la censure, nous avons vu que le système de nommage basé sur la blockchain ne garantit pas dans les faits l'abandon total de centralisation.

La multiplicité des systèmes de nommage de la blockchain les rend sources de confusions lors de la résolution des noms, et leur facilité d'utilisation reste à ce jour discutable.

Enfin, le système de nommage basé sur la blockchain présente deux préoccupations majeures : le cybersquattage, et plus généralement l'absence de règles transparentes prenant en compte les droits des utilisateurs, et l'efficacité énergétique, avec une consommation très importante due aux calculs complexes nécessaires au mécanisme de consensus.

Le DNS bénéficie quant à lui d'une infrastructure solide, amenée à perdurer en tant que protocole à la fois pratique, efficace, évolutif et facile à utiliser.

Il pourrait être utile de s'inspirer des avantages des systèmes de nommage de la blockchain pour les appliquer au DNS.

L'objectif : limiter la censure, davantage le décentraliser, et continuer à renforcer sa sécurité, même si des extensions telles que DNSSEC et les protocoles DoT/DoH montrent toute leur efficacité pour renforcer la sécurité du système existant.

Il est encore difficile de se projeter quant au développement du système de nommage basé sur la blockchain dans les prochaines années, et son adoption dépendra des compromis que la communauté Internet est prête à faire.

Il sera cependant nécessaire, dans les prochaines discussions, d'avoir une approche globale et de prendre en compte l'aspect pratique, l'évolutivité, la facilité d'utilisation, la régulation et l'efficacité énergétique.

Sources

1. https://www.ietf.org/rfc/rfc1034.txt
2. https://blog.apnic.net/2023/02/08/the-root-of-the-dns-revisited/
3. https://blog.cloudflare.com/application-security-report-q2-2023/
4. https://www.icann.org/root-server-system-en
5. https://www.cloudflare.com/learning/dns/top-level-domain/
6. Public Technical Identifiers (PTI) est une filiale de l'ICANN dont la responsabilité est de gérer techniquement la « fonction IANA » : « *PTI is responsible for the operational aspects of coordinating the Internet's unique identifiers and maintaining the trust of the community to provide these services in an unbiased, responsible and effective manner.* » cf : https://www.iana.org/about
7. https://www.afnic.fr/observatoire-ressources/actualites/le-conseil-scientifique-de-lafnic-partage-sur-le-filtrage-Internet-par-dns/
8. https://blog.avast.com/ddos-attack-on-dyn-took-down-the-bulk-of-the-Internet-on-friday
9. https://techcrunch.com/2021/07/22/a-dns-outage-just-took-down-a-good-chunk-of-the-internet/
10. https://datatracker.ietf.org/doc/rfc9364/
11. https://stats.labs.apnic.net/dnssec
12. https://www.rfc-editor.org/rfc/rfc7858
13. https://www.rfc-editor.org/rfc/rfc8484
14. https://stats.labs.apnic.net/edns
15. https://handshake.org/
16. https://www.namecoin.org/
17. https://ens.domains/
18. https://beincrypto.com/learn/51-attacks-explained/
19. https://ethernodes.org/countries
20. https://www.datawallet.com/crypto/ethereum-staking-statistics-and-trends
21. https://www.forbes.com/sites/roslynlayton/2021/03/23/mit-researchers-estimate-the-value-of-domain-name-system-dns-at-8-billion/
22. https://www.icann.org/en/help/dndr/udrp/policy
23. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000028727656
24. https://nftnewstoday.com/2022/02/24/puma-follows-nike-and-adidas-into-the-nft-space-registering-a-puma-eth-address/
25. https://protos.com/are-blockchain-domains-really-immutable-and-what-does-this-mean-for-brands/
26. Challenges with Alternative Name Systems – ICANN OCTO-34, 27th April 2022
27. « Managing the Risks of Top-Level Domain Name Collisions Findings for the Name Collision Analysis Project (NCAP) Study 1, » https://www.icann.org/en/system/files/files/ncap-study-1-report-19jun20-en.pdf.
28. https://ccaf.io/cbnsi/ethereum/methodology
29. https://www.afnic.fr/wp-media/uploads/2023/07/Rapport-RSE-Afnic-2022.pdf
30. https://www.dnsbelgium.be/en/news/carbon-footprint
31. https://digiconomist.net/ethereum-energy-consumption

DOSSIER THÉMATIQUE

Internet
made in France

À propos de l'Afnic :

L'Afnic est le registre des noms de domaine .fr (France), .re (Île de la Réunion), .yt (Mayotte), .wf (Wallis et Futuna), .tf (Terres Australes et Antarctiques), .pm (Saint-Pierre et Miquelon).

L'Afnic se positionne également comme fournisseurs de solutions techniques et de services de registre. L'Afnic – Association Française pour le Nommage Internet en Coopération – est composée d'acteurs publics et privés : représentants des pouvoirs publics, utilisateurs et prestataires de services Internet (bureaux d'enregistrement). Elle est à but non lucratif.

www.afnic.fr
contact@afnic.fr