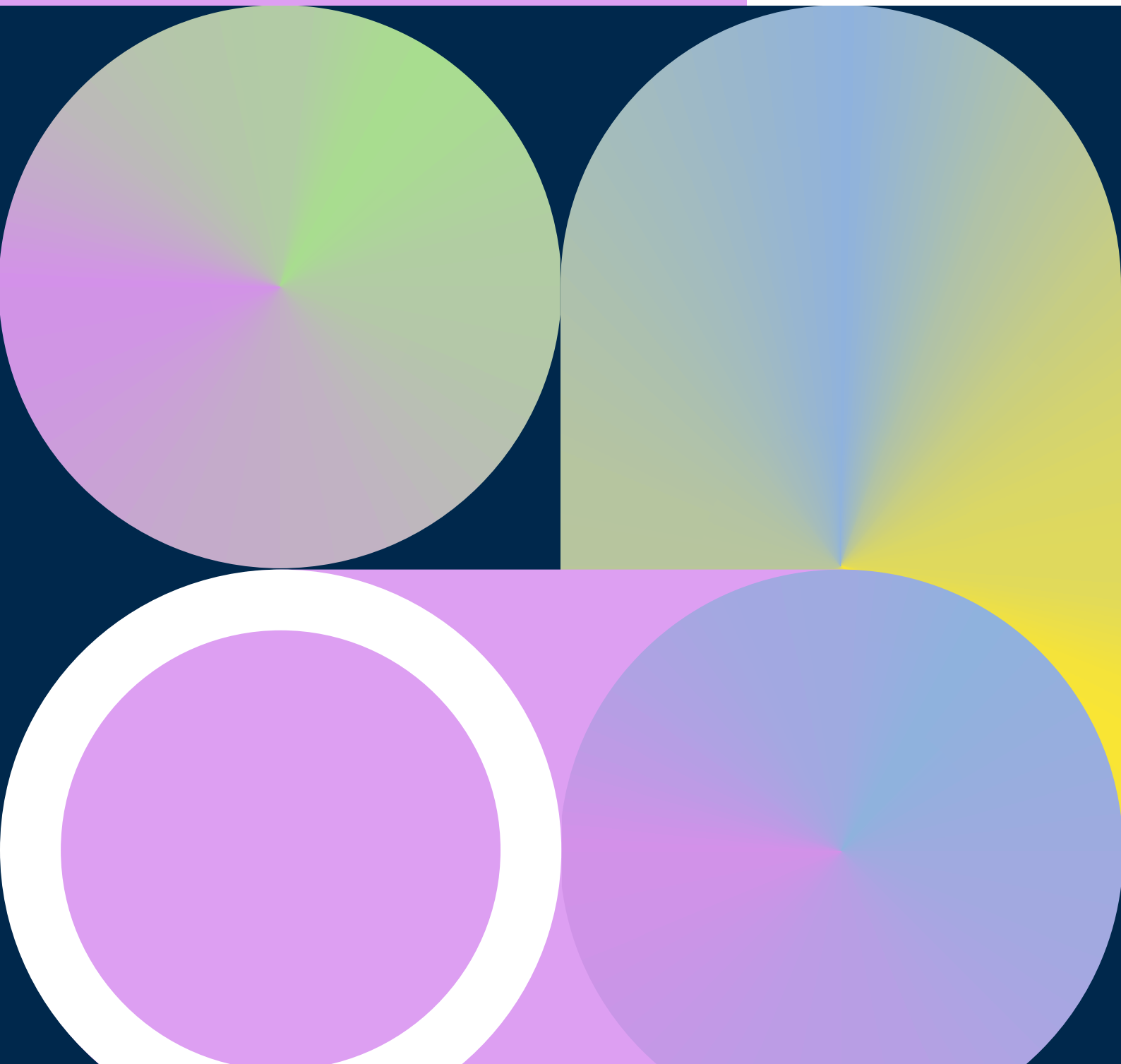
Peut-on faire mieux que le DNS ?

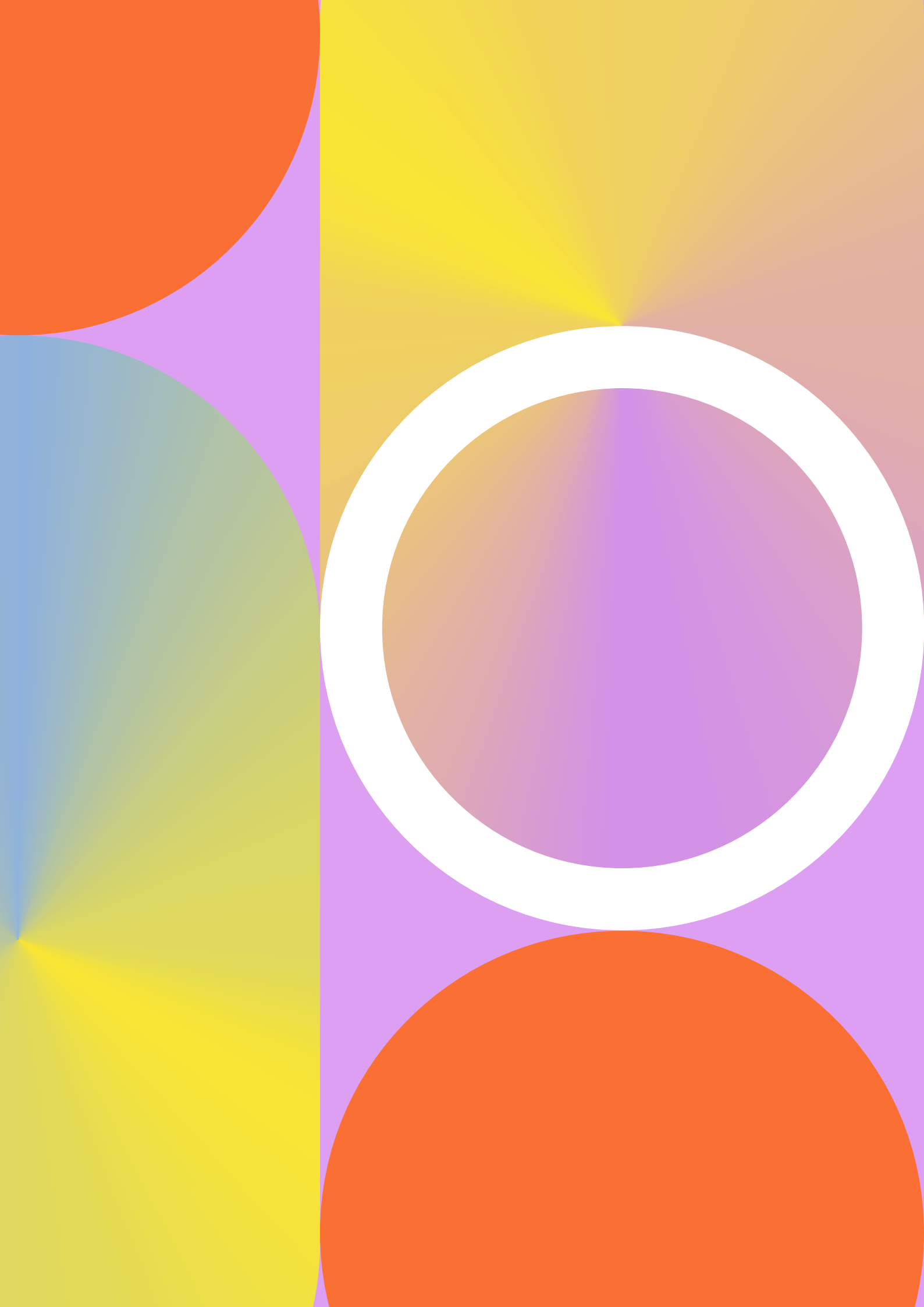
Analyse comparative de la sécurité des identifiants blockchain

LES DOSSIERS THÉMATIQUES

afnic

Internet made in France





Sommaire

Introduction

Le DNS (*Domain Name System*) constitue aujourd'hui l'infrastructure de référence pour l'enregistrement et la résolution des noms de domaine sur internet. C'est un système éprouvé, standardisé, déployé à l'échelle mondiale. Mais depuis plusieurs années, des initiatives de systèmes de noms alternatifs basés sur la *blockchain* émergent et cherchent à se positionner en explorant d'autres modèles que celui du DNS.

Dans un précédent dossier, nous avions étudié la possibilité pour la *blockchain* d'effectivement remplacer le DNS. Dans cet article, nous allons explorer les différences en matière de sécurité qu'offrirait un système de « noms de domaine » reposant sur une *blockchain* publique.

Si nous utilisons ici des guillemets pour « nom de domaine » en évoquant l'approche *blockchain*, c'est qu'il ne s'agit pas, à proprement parler, de noms de domaine. Ces identifiants en ont l'apparence, mais ne s'inscrivent pas dans le système des noms de domaine tel que défini par le DNS. Ils ne sont pas encadrés par les mêmes autorités de régulation, ni intégrés aux infrastructures racines reconnues par l'IANA (*Internet Assigned Numbers Authority*). Il est donc plus rigoureux de parler d'identifiants *blockchain*.

Les espaces de nommage basés sur la *blockchain*, qui s'écartent du modèle DNS, amènent à s'interroger : la *blockchain* permet-elle réellement d'améliorer la sécurité pour les détenteurs de noms de domaine ? Est-elle plus résiliente ? Offre-t-elle une meilleure confidentialité ?

Pour répondre à ces questions, nous commencerons par comparer le DNS et la *blockchain* à travers les deux principaux services qu'assure aujourd'hui le DNS : l'enregistrement des noms de domaine, qui garantit l'unicité des noms dans l'espace de nommage ; et la résolution des noms de domaine, qui permet à chacun d'accéder de manière fiable aux données associées à un nom, tout en assurant autant que possible la confidentialité. Ensuite, nous verrons comment le DNS et la *blockchain* répondent à ces services et quels sont les avantages et les inconvénients de chacun. Enfin, nous analyserons pourquoi la *blockchain* ne constitue pas forcément une solution miracle.

L'enregistrement d'identifiants dans la *blockchain* offre-t-il les mêmes garanties que les noms de domaine dans le DNS ?

Le DNS et la *blockchain* offrent des fonctionnalités d'espaces de nommage, permettant de stocker des noms et les données associées. Mais ces systèmes diffèrent fortement dans la manière dont ils garantissent l'unicité des noms, définissent la titularité, assurent la confidentialité des données des titulaires, ou encore dans leur résilience face aux attaques. Cette section examine ces différents aspects pour comprendre si la *blockchain* peut réellement offrir les mêmes garanties qu'un enregistrement via le DNS.

Une unicité des noms assurée dans le DNS, relative dans la *blockchain*

Le DNS et la *blockchain* utilisent deux méthodes distinctes pour garantir l'unicité des noms dans leur espace de nommage.

Le DNS repose sur une architecture hiérarchique et un système de délégation. L'unicité des noms est assurée par un système de gouvernance coordonné par l'ICANN (*Internet Corporation for Assigned Names and Numbers*), qui supervise la racine du DNS via sa fonction technique IANA (*Internet Assigned Numbers Authority*), opérée par sa succursale PTI[1] , et les registres ensuite qui gèrent, de manière déléguée, chaque TLD (*Top-Level Domain*). L'existence d'une racine unique, acceptée par tous, garantit qu'aucun nom ne peut être enregistré deux fois dans le même espace de nommage. C'est cette organisation qui assure la cohérence globale du DNS.

Dans le cas des *blockchains*, l'espace de nommage est généralement géré par des « *smart contracts* », qui définissent les règles d'enregistrement et de résolution des identifiants *blockchain*. En théorie, ces contrats garantissent l'unicité des noms au sein d'un même *smart contract*, et plusieurs *smart contracts* peuvent coexister sur une même *blockchain*. Cependant, il n'existe pas de gestion centralisée de l'unicité des identifiants à l'échelle de toutes les *blockchains*. Il est donc possible que plusieurs *blockchains* concurrentes attribuent le même identifiant, entraînant des collisions.

Ce problème s'est déjà produit avec certaines extensions *blockchain*, comme dans l'affaire .wallet, où Unstoppable Domains et Handshake ont chacun proposé une extension .wallet, entraînant un conflit sur l'attribution des noms (voir l'analyse du conflit et la décision judiciaire) ; ou encore l'affaire .coin, où Unstoppable Domains a dû arrêter la vente des noms de domaine en .coin après avoir découvert qu'une autre *blockchain*, Emercoin, attribuait déjà cette extension (voir le détail de l'affaire). D'autres extensions, comme .free ou .visa, posent également problème car elles existent déjà dans la racine DNS officielle, ce qui accroît le risque de confusion entre identifiants *blockchain* et noms de domaine classiques. La dernière étude de la DNSRF[2] réalisée avec le soutien de l'Afnic montre des chevauchements préoccupants à tous les niveaux. Ces collisions sont susceptibles d'augmenter avec l'introduction de nouvelles applications de gTLD, en particulier dans des catégories telles que la finance (.wallet, .coin), l'identité/sécurité (.verify, .identity) et les actifs numériques (.crypto, .nft, .blockchain). Parmi les fournisseurs examinés, Freename avait le plus de conflits directs avec des

gTLD existants (8), suivi de DecentraName (4) et Handshake (1). Afin d'évaluer également les risques de collisions du point de vue d'un registre ccTLD comme l'Afnic, nous avons également croisé les données récoltées par la DNSRF et avons trouvé des centaines de collisions directes entre les identifiants de *blockchain* de second niveau et les noms de domaine .fr existants.

Cette coexistence non coordonnée peut aussi entraîner une fragmentation de l'espace de nommage : par exemple, le navigateur Brave reconnaît certaines extensions comme .eth ou .brave[3] en dehors du DNS, ce qui permet à un utilisateur de partager un lien en .brave mais qui ne fonctionnera pas chez un destinataire utilisant un autre navigateur.

En conclusion

Contrairement au DNS, où l'ICANN et les registres jouent un rôle d'autorité, il n'existe pas de consensus global sur quelle *blockchain* et quel *smart contract* doivent être considérés comme faisant foi. Chaque utilisateur choisit quelle *blockchain* il préfère utiliser. Cette absence de gouvernance unifiée pose un vrai défi pour l'adoption généralisée des identifiants sur la *blockchain*.

> Chaque utilisateur choisit quelle *blockchain* il préfère utiliser. Cette absence de gouvernance unifiée pose un vrai défi pour l'adoption généralisée des identifiants sur la *blockchain*.

De la délégation à l'autonomie : deux visions opposées de la titularité

Nous parlons bien ici d'être titulaire d'un nom de domaine ou d'un identifiant *blockchain*, et non pas propriétaire. La différence est importante car nous ne sommes pas propriétaire d'un identifiant, nous en avons la jouissance uniquement si nous payons les frais associés et respectons la politique du registre tout au long de son utilisation. La manière dont la titularité est définie et gérée diffère profondément entre un nom de domaine et un identifiant *blockchain*.

Dans le modèle classique du DNS, notamment avec le modèle 3R (*Registry, Registrar, Registrant*) (RFC 8499), l'enregistrement d'un nom de domaine repose sur un contrat à durée déterminée, renouvelable sans limite par le titulaire, dès lors qu'il respecte ses obligations contractuelles. Ce système est souvent critiqué, car plusieurs acteurs — autres que le titulaire lui-même — peuvent modifier le statut de titularité d'un nom de domaine :

- **Le bureau d'enregistrement (BE)**, qui peut transférer un nom de domaine à un autre titulaire en réponse à une décision judiciaire ou en cas de non-respect des conditions générales d'utilisation.
- **Le registre**, qui peut également intervenir selon ses propres règles et obligations.

Ce modèle n'est pas immune aux cyberattaques, les BE et les registres étant ciblés. Certains BE ont déjà été compromis, permettant à des attaquants de transférer ou de modifier illégalement des noms de domaine. Dans ce genre d'attaque, le système est suffisamment résilient et remis en place rapidement grâce aux sauvegardes et autres plans de reprise d'activité (PRA). Il est donc essentiel de bien comprendre les conditions spécifiques à chaque TLD et à chaque bureau d'enregistrement pour protéger ses droits sur un nom de domaine.

Dans le cas de la *blockchain*, la gestion de la titularité est fondamentalement différente. Ici, un identifiant est généralement représenté par un *token*, généré par un *smart contract*, détenu par un portefeuille cryptographique. En théorie, seul le portefeuille propriétaire du *token* peut transférer ou modifier l'identifiant. Toutefois, plusieurs points doivent être pris en compte :

La fiabilité du *smart contract*.
Un *smart contract* reste un programme qui peut contenir des *bugs* (avec des impacts plus ou moins critiques), rendant les identifiants *blockchain*s vulnérables. L'un des exemples les plus célèbres est le *hack* de *The DAO*, qui a révélé des failles majeures dans certains contrats Ethereum.

Certains systèmes, comme ENS (*Ethereum Name Service*), garantissent que leur *smart contract* ne sera jamais modifié[4]. Cependant, d'autres peuvent autoriser des mises à jour, censées corriger d'éventuelles vulnérabilités, mais qui pourraient aussi être détournées pour modifier les règles d'enregistrement et compromettre la confiance dans le système.

La sécurité des clés privées.
Contrairement au DNS, où un registre centralisé gère l'association entre nom de domaine et titularité, la *blockchain* repose sur la possession de la clé privée du portefeuille. Si cette clé est perdue ou compromise, l'identifiant peut être définitivement inaccessible ou volé.

Certains services centralisés, comme les plateformes d'échange de cryptomonnaies, hébergent des portefeuilles pour leurs utilisateurs. Or, une grande partie des actifs en cryptomonnaies (environ 85 % des *bitcoins*, par exemple) sont détenus par des plateformes centralisées comme Binance ou Coinbase, qui regroupent les fonds de milliers d'utilisateurs sous une poignée d'adresses *blockchain* dont elles sont les seules titulaires[5]. Cela signifie que, dans de nombreux cas, le véritable titulaire d'un identifiant *blockchain* est l'exchange lui-même, et non l'utilisateur final. De nombreux *hacks* ont visé les *exchanges*, compromettant les actifs de leurs utilisateurs. Par exemple, l'attaque récente contre Bybit a entraîné le vol de millions de dollars en cryptomonnaies[6]. Dans ce cas, une fois les *tokens* transférés sur un autre portefeuille, il est impossible de les récupérer.

En conclusion :

Que ce soit avec le DNS ou la *blockchain*, la gestion de la titularité d'un nom de domaine ou d'un identifiant *blockchain* nécessite une vigilance accrue. Pour le DNS, il est crucial de bien comprendre les règles du registre et du bureau d'enregistrement afin de minimiser les risques de litiges ou de pertes. Pour la *blockchain*, il est essentiel de s'assurer du bon fonctionnement du *smart contract* et de sécuriser rigoureusement la clé privée du portefeuille.
La propriété décentralisée offerte par la *blockchain* semble séduisante, mais elle s'accompagne de nouvelles responsabilités et de risques qu'il ne faut pas sous-estimer. Car si la *blockchain* est décentralisée, il n'en reste pas moins que des utilisateurs passent par des plateformes pour simplifier la gestion de leurs identifiants, en faisant ainsi des facteurs de centralisation du système. De plus, ces plateformes peuvent, elles aussi, être sujettes à défaillance (technique, économique) et mettre à risque la possibilité pour un titulaire de récupérer la gestion de ses identifiants, par exemple en cas de perte de clés privées gérées via cette plateforme.

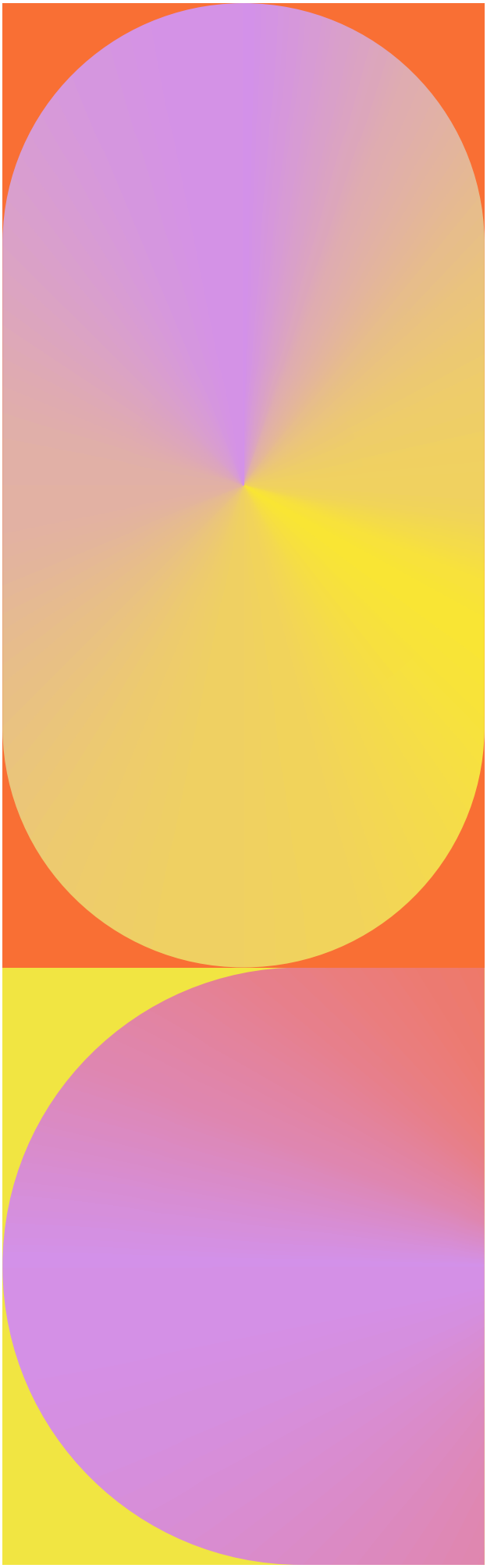
Confidentialité : l'identité des titulaires protégée dans le DNS, traçable sur la *blockchain*

Lorsqu'on enregistre un nom de domaine (NDD), c'est généralement pour héberger un site web ou des services accessibles publiquement sur internet. Toutefois, certains titulaires peuvent souhaiter préserver leur anonymat, notamment pour des raisons commerciales ou économiques (lancement d'une nouvelle marque ou d'un nouveau produit, par exemple), politiques ou simplement pour la protection de données personnelles pour une personne physique.

Dans le DNS, la confidentialité dépend principalement de la politique du registre, qui décide quelles informations sont publiées via RDAP (remplaçant du Whois). Pour certaines extensions, comme le .fr, les informations des personnes physiques sont anonymisées par défaut, tandis que celles des personnes morales restent publiques. D'autres extensions appliquent des règles différentes selon le registre, souvent en fonction des lois locales (notamment pour les ccTLD). Le choix du TLD devient donc stratégique, car il faut tenir compte des politiques de confidentialité du registre, mais aussi de celles du bureau d'enregistrement (BE).

À première vue, la *blockchain* semble garantir une confidentialité absolue, car elle repose sur des adresses cryptographiques de portefeuilles électroniques (appelés communément *wallet*), qui apparaissent comme des suites aléatoires de caractères. Cependant, cette perception est trompeuse. En réalité, la *blockchain* ne garantit pas l'anonymat. Toutes les transactions sont publiques et traçables. Contrairement au DNS, où seules certaines informations sont accessibles via RDAP ou le Whois, la *blockchain* fonctionne sur un registre ouvert et consultable par tous.

Toute opération réalisée avec un portefeuille électronique peut en compromettre l'anonymat et permettre de remonter à l'identité de son propriétaire. C'est notamment vrai pour l'achat de cryptomonnaies sur une plateforme d'échange, qui peut exiger une vérification d'identité (*KYC : Know Your Customer*) ou le paiement d'un service avec des cryptomonnaies sur une plateforme associée à une identité connue. Des techniques avancées de désanonymisation existent et permettent d'identifier des utilisateurs en croisant diverses sources de données[7]. Certaines attaques exploitent même ces failles pour compromettre



le pseudonymat des utilisateurs, comme par exemple l'attaque par « *dusting* » où une petite quantité de cryptomonnaie (« dust » ou « poussière » en français) est envoyée à un grand nombre d'adresses. Lorsque ces fonds sont utilisés, il devient possible de lier plusieurs adresses ensemble et de remonter à un utilisateur. Un exemple de cette technique est discuté ici.

En conclusion

Dans le cas du DNS, il est crucial de bien choisir son registre et son bureau d'enregistrement en tenant compte de leur politique de gestion des données personnelles. Dans tous les cas, le registre et/ou le BE ont connaissance de l'identité du titulaire. Dans le cas de la *blockchain*, la confidentialité repose entièrement sur l'utilisateur. Il doit être extrêmement vigilant dans l'utilisation de son portefeuille pour éviter de révéler involontairement son identité. La *blockchain* n'est donc pas un moyen infaillible d'anonymisation, contrairement à ce que l'on pourrait penser.

Résilience : deux architectures robustes, chacune avec ses fragilités

Le DNS repose sur une architecture hiérarchique et déléguée, ce qui lui confère une très bonne résilience face aux pannes. Grâce à son système de délégation, il est facile de vérifier et propager les informations. La redondance des serveurs racines, des TLDs et des serveurs de noms secondaires garantit une disponibilité élevée. Les mécanismes comme la DNSSEC ajoutent une couche supplémentaire de protection contre la modification des réponses ou l'empoisonnement de cache par des acteurs mal intentionnés, bien que leur adoption ne soit pas systématique.

Comme tout système, le DNS peut être vulnérable à des attaques ciblées, via par exemple une compromission du registre ou bien une compromission technique d'un bureau d'enregistrement, même si des mécanismes comme le *Registry Lock* ou *Registrar Lock* existent et ont fait leurs preuves pour les noms de domaines les plus sensibles.

Sur ce point, la *blockchain* démontre une forte robustesse contre la modification des données associées à un identifiant. L'association d'un registre distribué avec une signature cryptographique garantit que tous les participants peuvent vérifier la véracité des informations contenues dans la *blockchain*. Tant que les algorithmes cryptographiques utilisés restent résistants aux différentes attaques existantes, la *blockchain* peut être considérée comme sûre et fiable.

> **Amazon héberge à lui seul plus de 50% des nœuds actifs d'Ethereum.**

Les attaques cryptographiques sur la *blockchain* nécessitent souvent une puissance de calcul colossale (ex : attaque des 51 %), ce qui rend leur exécution coûteuse et difficile sur des *blockchain*s bien établies. Cependant la distribution des infrastructures utilisées par le registre peut être remise en question quand on sait, par exemple, que la majorité (69 %) des 4 653 nœuds actifs d'Ethereum sont hébergés par trois grands fournisseurs de services *cloud*, dont Amazon Web Services (AWS) qui en héberge à lui seul plus de 50 %. Cela montre que la *blockchain* n'est pas aussi distribuée qu'on pourrait le penser (voir le précédent dossier blockchain).

En conclusion

Le DNS et la *blockchain* ont chacun des atouts en matière de résilience. Le DNS est fiable grâce à sa structure déléguée et redondante, mais peut être vulnérable à certaines attaques visant les infrastructures de registres ou les bureaux d'enregistrement. La *blockchain* repose sur un modèle décentralisé et « *crypto by design* », rendant les falsifications presque impossibles tant que la cryptographie sous-jacente demeure robuste. Toutefois, la résilience ne se limite pas à la seule disponibilité des données. Il faut aussi considérer d'autres aspects comme la gouvernance, la mise à jour des protocoles et la gestion des litiges, qui peuvent poser problème sur la *blockchain*.

En matière d'enregistrement, la *blockchain* ne fait pas mieux, elle fait autrement et cela implique d'autres risques

L'enregistrement d'un identifiant sur la *blockchain* n'apporte pas nécessairement plus de sécurité que l'enregistrement d'un nom de domaine classique via le DNS. Si la *blockchain* permet d'éliminer certains tiers de confiance tels que les registres ou les BE, elle transfère aussi l'entière responsabilité de la sécurité au propriétaire du domaine. La gestion des clés privées, la compréhension du *smart contract* sous-jacent et la protection contre les attaques sur les portefeuilles deviennent alors critiques.

À l'inverse, le DNS repose sur un modèle délégué, où la sécurité dépend des registres et bureaux d'enregistrement. Ce modèle offre des garanties en matière de récupération et de gouvernance, mais introduit aussi des risques de blocage d'accès, de confiscation ou de modification par des acteurs tiers.

Sécurité et résolution des identifiants : la *blockchain* fait-elle aussi bien que le DNS ?

Après avoir identifié les différences entre la *blockchain* et le DNS en matière d'enregistrement, intéressons-nous maintenant à la seconde étape, plus technique : la résolution des noms de domaine et des identifiants *blockchain*.

Les enjeux de disponibilité dans la résolution DNS et *blockchain* : continuité, autonomie et accessibilité à grande échelle

Le service de résolution du DNS n'est pas un *Single Point of Failure* (SPOF) comme cela peut être parfois évoqué. En effet, il existe 13 noms de serveurs racines ([a-m].root-servers.net.) répartis sur 1 900 serveurs physiques, gérés par plusieurs organismes différents, qui assurent ce service à l'échelle mondiale grâce à la technique *anycast*[8].

1 900
serveurs physiques rendent disponible le DNS

Cette architecture répartit la charge, améliore la résilience et réduit les délais de réponse du DNS. Pour rappel, les serveurs racines contiennent les informations nécessaires pour localiser les serveurs de noms de domaine de premier niveau (appelés TLD pour *Top-Level Domain*). L'ensemble des TLD est disponible ici. Une grande majorité des TLD eux-mêmes mettent en œuvre, eux aussi, la technologie *anycast* pour assurer la résilience de leur TLD.

Pour les noms de second niveau (comme monnomdomaine.fr, par exemple), la responsabilité de la résilience repose sur le titulaire du domaine. Celui-ci peut alors choisir d'héberger et gérer ses propres serveurs DNS (comme il hébergerait son site internet), utiliser les services d'hébergement DNS généralement fournis par son bureau d'enregistrement ou un service de DNS as a Service (DNSaaS), qui exploitent également l'*anycast* pour assurer une haute disponibilité. En combinant plusieurs prestataires d'hébergement ou de DNSaaS, il est ainsi possible (et recommandé) d'améliorer la redondance et de réduire les risques de panne. Les techniques pour rendre le DNS résilient sont aujourd'hui connues et bien maîtrisées.

En théorie, une *blockchain* est infaillible pour la résolution des identifiants *blockchain*, puisque toutes les transactions sont inscrites dans des blocs et que le mécanisme de consensus garantit qu'au bout d'un certain temps, tous les participants ont la même vision de la chaîne. Ainsi, chaque acteur pourrait simplement interroger sa propre copie de la *blockchain* pour résoudre un identifiant *blockchain*.

Mais en pratique, cette vision idéale est difficilement réalisable car maintenir un nœud complet d'une *blockchain* requiert un espace disque conséquent, ce qui limite le nombre d'acteurs capables d'héberger leur propre copie. Si certaines techniques permettent de réduire la taille du stockage nécessaire (comme utiliser un « *pruned node* »), cela

ne résout pas pour autant le problème plus large de la fragmentation des *blockchains*. Contrairement au DNS qui repose sur une infrastructure ayant un unique point d'entrée (la racine), il existe plusieurs *blockchains* attribuant elles-mêmes leurs propres identifiants dans leur système d'identification. Un acteur souhaitant résoudre tous les identifiants disponibles devrait donc maintenir une copie de chaque *blockchain* pertinente, ce qui complexifie encore le processus.

Il faut également souligner que la résolution de noms dans la *blockchain* est particulièrement efficace lorsqu'elle reste confinée à des usages internes à l'écosystème *blockchain* lui-même. Tant que les applications évoluent dans cet environnement, par exemple des *smart contracts* interagissant entre eux, la résolution repose sur des mécanismes fiables, cohérents et bien intégrés. En revanche, dès que l'on cherche à utiliser ces identifiants dans des contextes extérieurs à la *blockchain* (comme l'accès à des contenus web classiques), des difficultés apparaissent. L'utilisateur n'a plus toujours accès direct à la chaîne, la résolution repose alors sur des passerelles ou des services tiers, et la promesse d'une résolution fiable, décentralisée et de confiance s'effrite.

En conclusion

Bien que la *blockchain* puisse théoriquement offrir une alternative décentralisée et résiliente, elle soulève de nombreux défis techniques qui freinent son adoption à grande échelle.

> **Dès que l'on cherche à utiliser ces identifiants dans des contextes extérieurs à la *blockchain*, des difficultés apparaissent.**

Intégrité et authenticité des réponses : dans le DNS comme dans la *blockchain*, tout repose sur la confiance

Un autre aspect fondamental de la sécurité est d'assurer l'intégrité et l'authenticité des réponses à des interrogations par les utilisateurs ou les services. Il est crucial de garantir que la réponse n'a pas été altérée par un attaquant ou falsifiée par le serveur qui la fournit.

À l'origine, le DNS ne comportait aucun mécanisme de sécurité garantissant l'intégrité ou l'authenticité des réponses. Cette faiblesse a conduit à plusieurs types d'attaques, comme l'empoisonnement de cache (*DNS cache poisoning*), où un attaquant injecte de fausses réponses dans le cache d'un résolveur – une vulnérabilité rendue célèbre en 2008 par le chercheur Dan Kaminsky. On peut également citer les attaques de type Homme du milieu (ou MITM pour *Man-In-The-Middle*), où un acteur malveillant intercepte et modifie les réponses DNS en transit.

Ces vulnérabilités ont été partiellement résolues grâce à DNSSEC (RFC 4033, 4034 et 4035). DNSSEC signe les enregistrements DNS, garantissant leur authenticité (via une chaîne de confiance) et leur intégrité. Si un domaine est signé, il est possible de vérifier la légitimité de la réponse en suivant la chaîne de signatures DNSSEC. Cependant, DNSSEC reste encore peu déployé : environ 35 % des requêtes DNS sont résolues avec DNSSEC[9] et un grand nombre de noms de domaine ne sont pas signés (par exemple, seulement ≃19,8 % des domaines en .fr sont signés[10]).

Un autre problème est que l'utilisateur doit faire confiance à son résolveur DNS. C'est ce dernier qui valide les signatures DNSSEC et indique si la réponse est authentique via le bit AD (*Authenticated Data*). Cependant, cette architecture est parfois exploitée pour rendre inaccessibles des contenus considérés comme illégaux ou problématiques (voir la section *Filtrage*).

Bien que cette architecture repose sur un modèle de confiance, elle présente des avantages pratiques qui expliquent sa large adoption. Il convient notamment de souligner que cette délégation permet de décharger les utilisateurs des calculs cryptographiques nécessaires à la validation des réponses DNSSEC, ce qui est particulièrement utile pour les dispositifs aux ressources limitées, comme les objets connectés. De plus, le partage du cache de résolution entre les utilisateurs d'un même réseau améliore la rapidité des réponses DNS. Enfin, le choix du résolveur peut être guidé par des critères fonctionnels, comme le filtrage de sites malveillants ou l'activation d'un contrôle parental.

En matière d'intégrité des réponses, la

blockchain est en théorie plus robuste sur ce point. Il suffit d'interroger directement la copie locale de la *blockchain* pour obtenir une réponse non altérable, car toutes les transactions sont immuables et vérifiables. Mais en pratique, très peu d'utilisateurs possèdent une copie locale de la *blockchain* sur leur machine. Aujourd'hui, les *blockchains* atteignent des tailles considérables (560 Go pour Bitcoin, 1 To pour Ethereum), héberger un nœud complet est donc une contrainte majeure.

Pour éviter cette complexité, la majorité des utilisateurs passent par des passerelles API fournissant un accès simplifié aux *blockchains*. Certains services d'identifiants sur la *blockchain* recommandent même officiellement cette approche, comme Freename[11].
Cependant, cette solution revient exactement au même problème qu'un résolveur DNS : l'utilisateur fait confiance à un service tiers pour obtenir la réponse. Rien ne garantit que la réponse n'ait pas été altérée par ce service.

≃19%

C'est le pourcentage des domaines en .fr qui sont signés par DNSSEC

En conclusion

Dans la réalité, la résolution via *blockchain* n'apporte aucun avantage significatif par rapport au DNS sur le plan de l'intégrité et de l'authenticité. Tant que les utilisateurs continueront à s'appuyer sur des passerelles tierces, ils devront faire confiance à un intermédiaire, que ce soit pour la *blockchain* ou pour le DNS.

Une promesse de confidentialité des requêtes à relativiser

Comme mentionné précédemment, le DNS n'a pas été conçu pour garantir la confidentialité des requêtes. À l'origine, toute requête DNS était envoyée en clair, ce qui permettait à n'importe quel acteur sur le réseau d'intercepter les requêtes et d'en déduire des informations sensibles sur l'utilisateur. Heureusement, plusieurs protocoles ont depuis été développés pour chiffrer les communications entre les clients et les résolveurs DNS : DNS *over* HTTPS (DoH – RFC 8484), DNS *over* TLS (DoT – RFC 7858) et DNS *over* QUIC (DoQ – RFC 9250). Ces mécanismes empêchent l'interception des requêtes DNS par un attaquant intermédiaire.

Logiquement, un résolveur DNS, utilisant un canal de communication chiffré ou non, connaît toujours l'intégralité des requêtes effectuées par l'utilisateur. Cela signifie que l'on doit faire confiance au résolveur utilisé car il peut collecter et analyser les requêtes, ce qui soulève des enjeux en matière de vie privée.

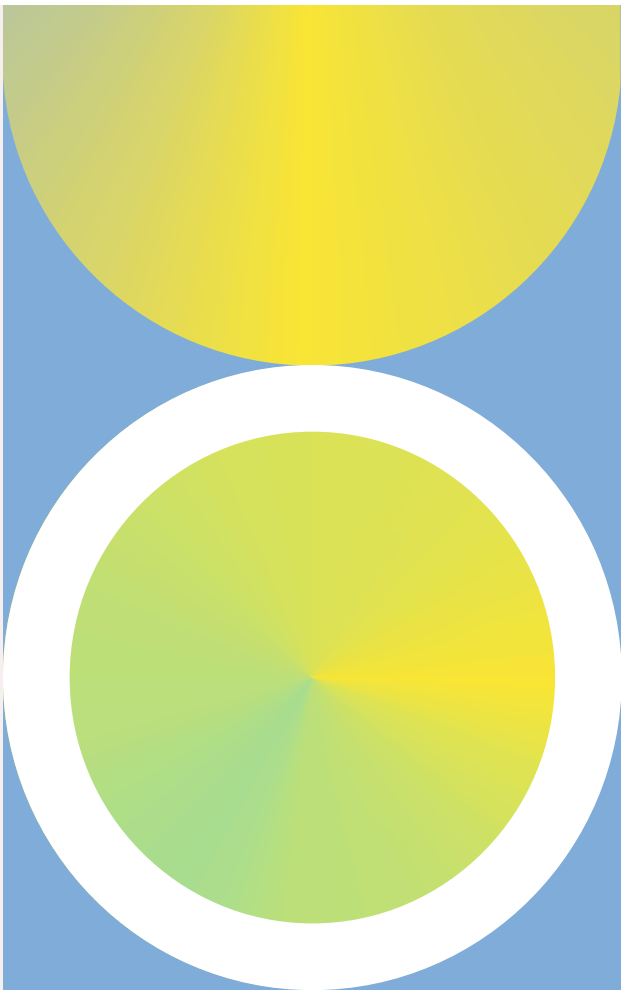
De plus, lorsque le résolveur ne connaît pas la réponse, il interroge les serveurs DNS faisant autorité qui, eux aussi, peuvent observer certaines informations sur les requêtes des utilisateurs. Ce problème a été partiellement résolu grâce à la technique du *QName minimisation* (RFC 7816), qui permet à un résolveur d'envoyer uniquement la partie nécessaire d'une requête au serveur faisant autorité. Cela limite la quantité d'informations divulguées à chaque niveau de la résolution DNS.

La *blockchain* propose une approche différente. L'utilisateur pourrait en théorie interroger directement un nœud *blockchain* local, sans interagir avec un service tiers. Cela garantirait une confidentialité totale car les requêtes resteraient sur la machine de l'utilisateur. Cependant, comme pour l'intégrité, la majorité des utilisateurs ne gèrent pas un nœud *blockchain* complet. Ils passent par des passerelles API (*gateways*) qui interrogent la *blockchain* à leur place. Il est cependant important de noter, même si ce n'est pas une pratique répandue, qu'un utilisateur peut également supprimer l'intermédiaire que représente le résolveur DNS de son FAI ou un résolveur DNS public en hébergeant lui-même un résolveur local – l'utilisateur ayant dans ce cas directement des interactions directes avec les serveurs faisant autorité.

Pour revenir au cas de l'utilisation d'un service de passerelle *blockchain*, seule cette passerelle connaît les requêtes de l'utilisateur. Cela implique donc toujours une dépendance à un service tiers, qui pourrait enregistrer ou analyser les requêtes. C'est par exemple le cas avec le navigateur Web Brave qui permet de résoudre des identifiants *blockchain* en passant par la plateforme infura.

En conclusion

Le problème de confidentialité touche aussi bien le DNS que la *blockchain*. Avec le DNS, des solutions comme DoH, DoT, DoQ et le *QName minimisation* réduisent la fuite d'informations. Avec la *blockchain*, la confidentialité dépend du fait que l'utilisateur interroge directement un nœud local (ce qui est rare) ou utilise une passerelle tierce (ce qui pose les mêmes problèmes qu'un résolveur DNS public). Ainsi, aucun des deux systèmes ne garantit une confidentialité absolue, sauf si l'utilisateur prend des mesures spécifiques pour minimiser son exposition, comme installer son propre résolveur DNS ou une copie de la *blockchain* chez lui.



Dans le DNS comme dans la *blockchain*, le filtrage reste possible

La résolution d'un nom de domaine ou d'un identifiant *blockchain* est une étape essentielle pour de nombreuses applications, qu'il s'agisse d'accéder à une page web ou d'interagir avec divers services. Rares sont les applications qui n'utilisent pas, directement ou indirectement, un tel identifiant. Cela en fait donc un point de contrôle privilégié, qu'il soit exercé par des entreprises ou des gouvernements.

Comme mentionné dans la section *Intégrité*, un résolveur DNS peut modifier ou bloquer une réponse, car son fonctionnement repose sur la confiance de l'utilisateur. Cette capacité est souvent exploitée pour mettre en place des mécanismes de blocage de l'accès à certains contenus. Dans de nombreux pays, les fournisseurs d'accès à internet (FAI) sont contraints de rediriger ou bloquer certaines requêtes DNS à la demande des autorités. Cette méthode est relativement facile à contourner en utilisant un résolveur DNS public alternatif qui ne filtre pas les requêtes (ex. : Quad9, DNS4EU, Cloudflare…) ou bien un résolveur personnel qui interroge directement les serveurs faisant autorité. Cependant, cette action reste efficace, car la plupart des utilisateurs utilisent les résolveurs fournis par leur FAI par défaut.

À première vue, une *blockchain* publique pourrait sembler incensurable, puisqu'elle est décentralisée et que toutes les transactions sont enregistrées de manière immuable. Cependant la majorité des utilisateurs n'hébergent pas eux-mêmes un nœud *blockchain*. Ils passent souvent par des passerelles API pour interroger la *blockchain*, et ces passerelles peuvent choisir de bloquer certaines requêtes de la même manière qu'un résolveur DNS.

> **La majorité des utilisateurs n'hébergent pas eux-mêmes un noeud blockchain.**

Un exemple notable de blocage dans l'écosystème *blockchain* est celui du blocage des utilisateurs iraniens sur OpenSea en raison des sanctions américaines.

Cet événement montre bien que certains acteurs clés peuvent refuser d'interagir avec certaines adresses ou identités.

Il est toujours possible de contourner ces restrictions en déployant son propre nœud *blockchain*, mais cela reste complexe et hors de portée pour la plupart des utilisateurs.

En conclusion

En matière de blocage d'accès, le DNS et la *blockchain* sont tous deux susceptibles de le rendre possible. En pratique, aucun des deux systèmes ne rend techniquement totalement impossible de tels blocages. Cependant, les règles de gouvernance du DNS étant dans la majorité des cas transparentes et accessibles, le DNS offre davantage de garanties, par sa gouvernance elle-même, que la *blockchain* dans ce domaine.

Les promesses de résolution de la *blockchain* ne tiennent pas face à la maturité et la résilience du DNS

Aucun des deux systèmes de résolution n'est infaillible. Dans les deux cas, les problèmes de confidentialité et de filtrage sont présents, principalement à cause de l'utilisation d'intermédiaires de confiance (résolveur pour le DNS et *gateway* pour la *blockchain*). Le DNS offre toutefois un système de résolution efficace, facile à mettre en place et surtout mature et mondialement utilisé, avec plusieurs décennies de fonctionnement stable à grande échelle ; là où la *blockchain*, en revanche, peine à s'imposer à cause de sa complexité et de sa dépendance aux intermédiaires.

Conclusion : entre promesse de rupture et réalité d'usage

Dans ce dossier, nous avons exploré les différences entre le DNS et les identifiants *blockchain*. Présentés comme une alternative décentralisée, ces derniers proposent un modèle qui s'éloigne des logiques de gouvernance et d'infrastructure du DNS. Mais si la *blockchain* introduit des mécanismes différents en matière d'enregistrement d'identifiants – notamment sur le plan de l'autonomie individuelle –, elle déplace aussi les risques et les responsabilités vers l'utilisateur, sans pour autant résoudre les problématiques de sécurité de façon systématique.

Côté résolution, elle n'est pas au niveau du DNS. Les promesses initiales de la *blockchain* se heurtent encore à des contraintes techniques et pratiques, là où le DNS bénéficie d'une maturité, d'une interopérabilité et d'un déploiement mondial difficile à égaler.

En définitive, la *blockchain* ne « fait pas mieux » que le DNS – elle fait autrement et est encore en développement. Et cet « autrement » soulève autant d'opportunités que de questions et de risques. Reste à observer dans quelles conditions ces deux modèles pourraient, à terme, coexister ou s'influencer mutuellement dans les futurs usages d'internet.

Sources

1 · « Public Technical Identifiers (PTI) » https://pti.icann.org

2 · « How much will blockchain identifiers clash with traditional DNS domains? » par Nathan Alan consultable sur https://dnsrf.org/blog/how-much-will-blockchain-identifiers-clash-with-traditional-dns-domains/index.html

3 · « Brave » · https://brave.com/blog/brave-tld/

4 · « The Registry (Ethereum Name Service) » https://docs.ens.domains/registry/ens/

5 · « Understanding 460 Million Bitcoin Addresses and Economic Activity » consultable sur https://www.chainalysis.com/blog/bitcoin-addresses/

6 · « Bybit frappé par le pire vol de l'histoire : Lazarus blanchit 70% des fonds sous le nez du FBI » par Renaud H. consultable sur https://journalducoin.com/exchanges/bybit-pire-vol-histoire-lazarus-blanchit-fonds-sous-nez-fbi/

7 · « Data-Driven De-Anonymization in Bitcoin » par Nick et Jonas David consultable sur https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/155286/eth-48205-01.pdf

8 · « Root-Servers » · https://root-servers.org/

9 · « DNSSEC Validation Rate » consultable sur https://stats.labs.apnic.net/dnssec

10 · « Le .fr en 2024 » par l'Afnic consultable sur https://www.afnic.fr/wp-media/uploads/2025/03/Le-FR-en-2024.pdf

11 · « Freename API Resolution » https://docs.freename.io/freename-api-resolution

LES DOSSIERS
THÉMATIQUES

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 fournisseur 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