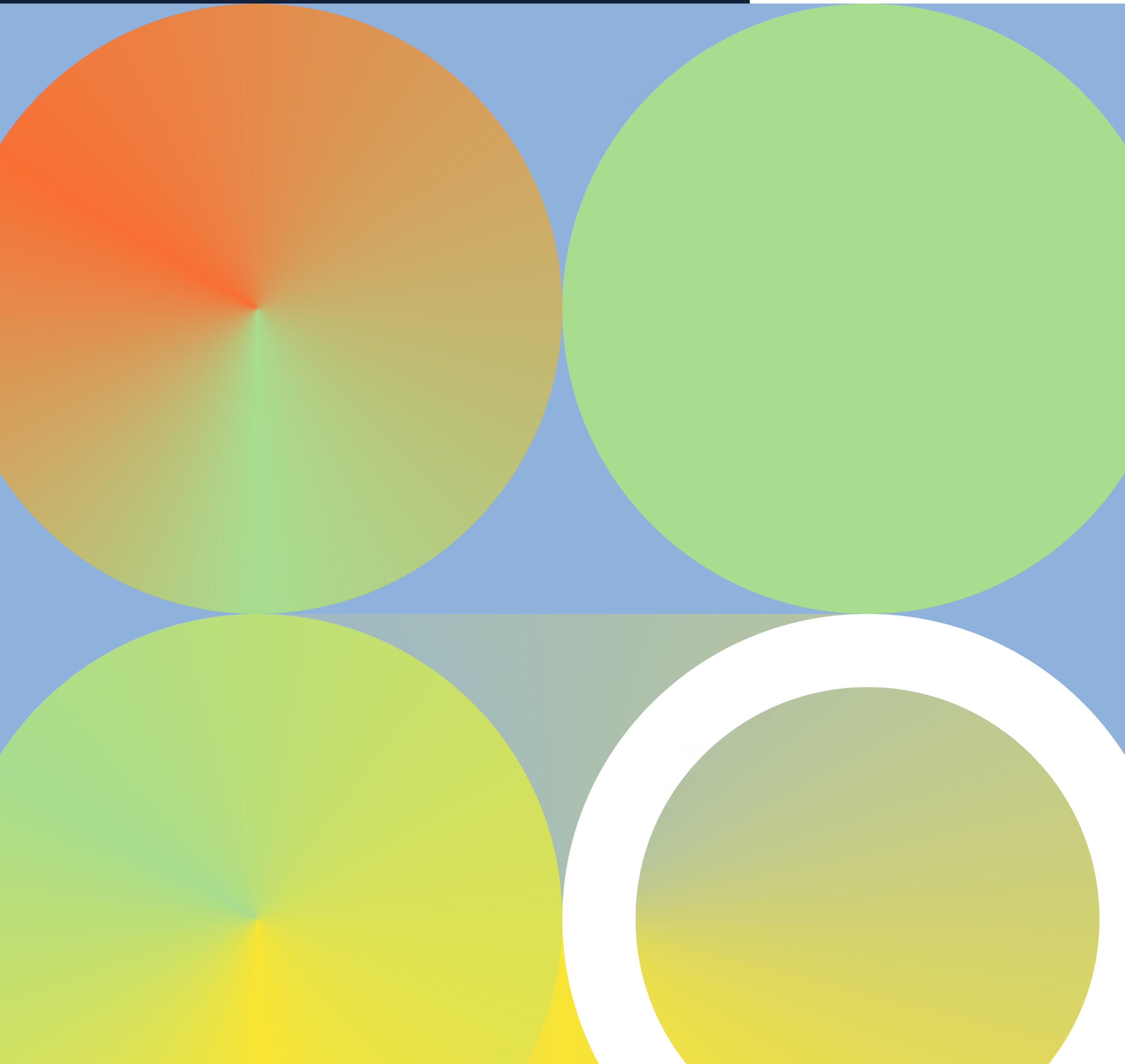
Could blockchain (really) replace DNS?

ISSUE PAPER

afnic

Internet
made in France



Summary

DNS – Quick overview

A naming space is a space in which to store names, a container in which each name is unique. The two main Internet naming spaces today are IP addresses and domain names.

DNS is the historical Internet naming service.[1] DNS (Domain Name System) allows an IP address (the unique identifier of every peripheral device connected to the Internet) consisting of a combination of figures, to be associated with a domain name which is both easy to remember and more stable over time. For example, www.afnic.fr is associated with the IP address 2a00:e00:0:5::2.

DNS acts as a telephone directory for the Internet. It also provides the resolution service for these names, which means it "calls" these numbers from your telephone directory. Designed in the 1980s, DNS aims to provide dynamic, scalable and hierarchical management of its naming space. It has become the cornerstone of Internet technology, used by the majority of online applications to connect to the Internet.

The number of DNS requests made every day is huge. All Internet users and all services and applications have to be taken into account here. A few figures: more than 100 billion requests a day received by Internet "root" servers[2]; more than two trillion requests on the infrastructure of CloudFlare[3], a domain name server distributed services operator, and more than two billion requests a day received on our infrastructure here at Afnic.

This predominance makes DNS an obvious target for cyber-attacks and has often, though wrongly, been pointed to as the Internet's Single Point of Failure (SPOF), needing to be replaced. Over the past forty years, numerous attempts have been made to replace DNS, most recently with blockchain-based naming systems.

Blockchain as a replacement for DNS

Replacing DNS with a blockchain-based naming system is akin to replacing a currency with crypto-currency. Like crypto-currency, which still has to overcome obstacles such as the practical aspect, its ability to evolve and, more generally, be accepted before it can become the main medium of exchange, the blockchain-based naming system is in its infancy and cannot yet be seen as a serious rival to DNS.

Let us consider the arguments put forward by those in favour of replacing DNS with blockchain.

The arguments put forward for replacing DNS

The arguments in favour of replacing DNS are many and varied. Its structure is seen as being prone to breakdowns and vulnerable to cyber-attack, as well as posing a risk of censorship and being vulnerable in terms of confidentiality.

By design, the DNS architecture is distributed (like an upside-down tree). It follows a hierarchical governance model which works on the basis of a single central root, with the root[4] on top and the (Top-Level Domains[5] such as ".FR" or ".COM") below. ICANN, in its capacity as coordinating organisation, setting the operating rules for domain name operators, determines what can be added to or taken away from the root zone (via its subsidiary PTI[6]) and the TLDs.

Countries that manage their own TLDs can make their own rules on the registration of domain names and thus decide whether or not to authorise the registration of certain terms. They can also put in place filters on access to domain names[7], restricting access to certain addresses, these requirements being imposed on resolver operators (mainly ISPs) rather than on the TLD operators.

DNS suffers attacks, such as distributed denial of service (DDoS), DNS spoofing and DNS amplification. Because these weaknesses are numerous and their consequences potentially serious, some people say that DNS is an Internet SPOF, meaning a single source that can lead to the generalised failure of a system. However, this idea is purely theoretical and furthermore mistaken : although DNS has been involved in certain major breakdowns[8],[9], since the birth of the Internet, the world has never seen a generalised failure of DNS resolution. On the contrary, its hierarchical, distributed, delegated model is a strength that allows DNS infrastructure resources to continue working even though others are victims of abuse on their infrastructure.

DNSSEC[10] (Domain Name System Security Extensions) go a long way towards reducing these attacks. However, deployment of DNSSEC on a global scale is not without its problems, given that DNSSEC is often seen as complex in administrative and technical terms. This is the case with most components that reinforce the level of security of an infrastructure resource. In this regard, DNS is no exception. The current global estimate of the degree of DNSSEC validation is around 30%[11].

Although DNSSEC ensures the integrity of responses to DNS requests, the majority of DNS requests and responses are still not carried out through encrypted protocols. Depending on its positioning in the resolution chain, this can allow an analysis of information on users browsing habits. Various solutions to strengthen the confidentiality of requests have been implemented and deployed with a view to strengthening and protecting the browsing data accessible via DNS. These solutions include the DoT[12] (DNS over TLS) and DoH[13] (DNS over HTTPS) encryption protocols. These solutions are currently applied to a quarter[14] of all DNS requests, a proportion that is constantly increasing.

Finally, a much debated point concerns holders: data and their visibility. Information on a domain name holder can be consulted publicly through directory services like WHOIS and RDAP. Registries managing TLDs have divergent practices in this regard. For some, personal data are accessible by default, while for many others they are anonymised by default and do not allow holders to be identified from these services. Nowadays, the vast majority of registrars have adopted the registries rules or put in place solutions to anonymise the personal data of these publicly accessible databases, including for registries that do not offer this masking by default.

● 30%

This is the current global estimate of the degree of DNSSEC validation.

● 20%

These solutions are currently applied to a quarter of all DNS requests, a proportion that is constantly increasing.

Blockchain-based naming systems

For some years now, several projects have been developing their own blockchain-based naming system in an attempt to replace DNS. While some, like Handshake[15], retain DNS as the basic infrastructure on which to create a decentralised naming protocol, others, like Namecoin[16], seek on the contrary to be totally independent of DNS.

Blockchain-based naming systems are often used to name wallets and other objects such as NFTs (non-fungible tokens).

Just as DNS is used to resolve domain names, i.e. to find its corresponding IP address, so blockchain-based naming systems such as ENS (Ethereum Name Service[17]) are used to provide the mapping between names and wallet addresses. For example "alice.eth" corresponds to "e32fre43f584bnf2784b3".

Several blockchain-based naming systems are currently in use:

- BitDNS
- Solana Name Service
- EmerDNS
- Diode
- Ethereum Name Service
- RIF Name Service
- Handshake
- Namecoin
- Unstoppable domains
- PeerName
- Emercoin
- And many more...

Blockchain: a possible solution

Let us look now at the advantages of a blockchain-based naming system compared with DNS: decentralisation, security, protection from censorship, and confidentiality.

The first objective of the blockchain in this context is to break free from ICANN, the DNS root governing organisation, but also from registries and registrars.
Blockchain offers a decentralised architecture in which the same information is stored and distributed among several nodes, avoiding recourse to any central authority.

By spreading the data over the whole network rather than having it all in a central site, blockchain cannot be defined as a SPOF and is therefore immunised against DDos attacks. Falsification of blockchain data is also more difficult since, if a copy were to fall into malevolent hands, only this copy would be compromised, as opposed to all copies in the chain.

With DNS, we have seen that censorship is possible, whether by blocking the resolution of a domain or by taking control of the domain itself, legally or administratively.
With the decentralisation offered by blockchain, it becomes virtually impossible to block or to take control[18] of a naming space as the names are spread over the whole network as opposed to being stored in a central database.

Lastly, blockchain allows privacy to be protected. With blockchain, name owners can register and manage their names through pseudonyms. Ownership of these names is protected by public-key cryptography. And although the operations (create, read, update and delete) on information associated with a name may be accessible to the public, it is difficult to deduce ownership from the information on the user carrying them out.

However, if a user has transmitted an identity to a dedicated platform to acquire crypto-currency for example, before sending it to a decentralised wallet, it will be entirely possible to cross-check this information via this third party. So confidentiality would not be 100% guaranteed. This depends not on the technology itself but on the rules established by the organisations using it. Therefore, in this respect, there is no basic difference from the DNS.

Could blockchain replace DNS?

While blockchain-based naming systems may remedy some shortcomings left by DNS, their viability as an alternative to DNS is nonetheless debatable. There are several reasons for this:

Decentralisation and censorship

Blockchain-based naming systems are designed to be independent of any central authority, which means that no group or authority should be able to take control of them.

The problem is that blockchain-based naming systems are themselves prone to a certain form of centralisation. For example, in the case of ENS (Ethereum Name Service), a blockchain-based equivalent to DNS, Amazon hosts more than two-thirds of the nodes in the network (see figure below), and nearly 50% of Ethereum is hosted in the USA[19]. This form of architectural consolidation could lead to fears of control being taken by one or other of these two majority stakeholders.

Another possible example of the risk of centralisation which is much debated in the crypto community is the importance of Lido and the associated risks[20]. Lido is a decentralised protocol of Ethereum that allows users to "stake" ETHs (units of the crypto-currency "ether"), without locking them in. On staking the ETH, the user receives stETH tokens representing the stake.

This staking system is based on a consensus mechanism called Proof of Stake, which guarantees that the transactions are verified and secured without the involvement of a bank or intermediary.

Nonetheless, the rapid growth of Lido gives rise to fears of centralisation. Lido has a network penetration that is close to one-third of the total stakes, the amount of participation corresponding to a single entity. This means that if Lido reaches 33% and there is an attack on Lido or it is infected by a bug, this could prevent the Ethereum network from reaching a consensus, which is 66% for the Ethereum blockchain. This in turn means that Ethereum would no longer work correctly.

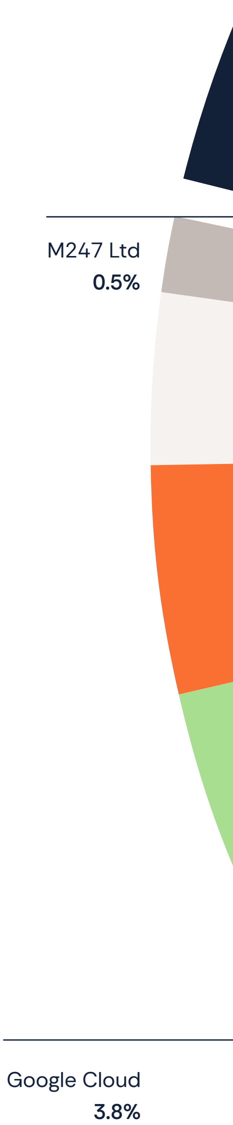
Alignment with the needs of users and businesses

The purpose of naming systems is to associate names with values. But DNS has evolved from being a simple mapping solution into an infrastructure representing billions of dollars[21].

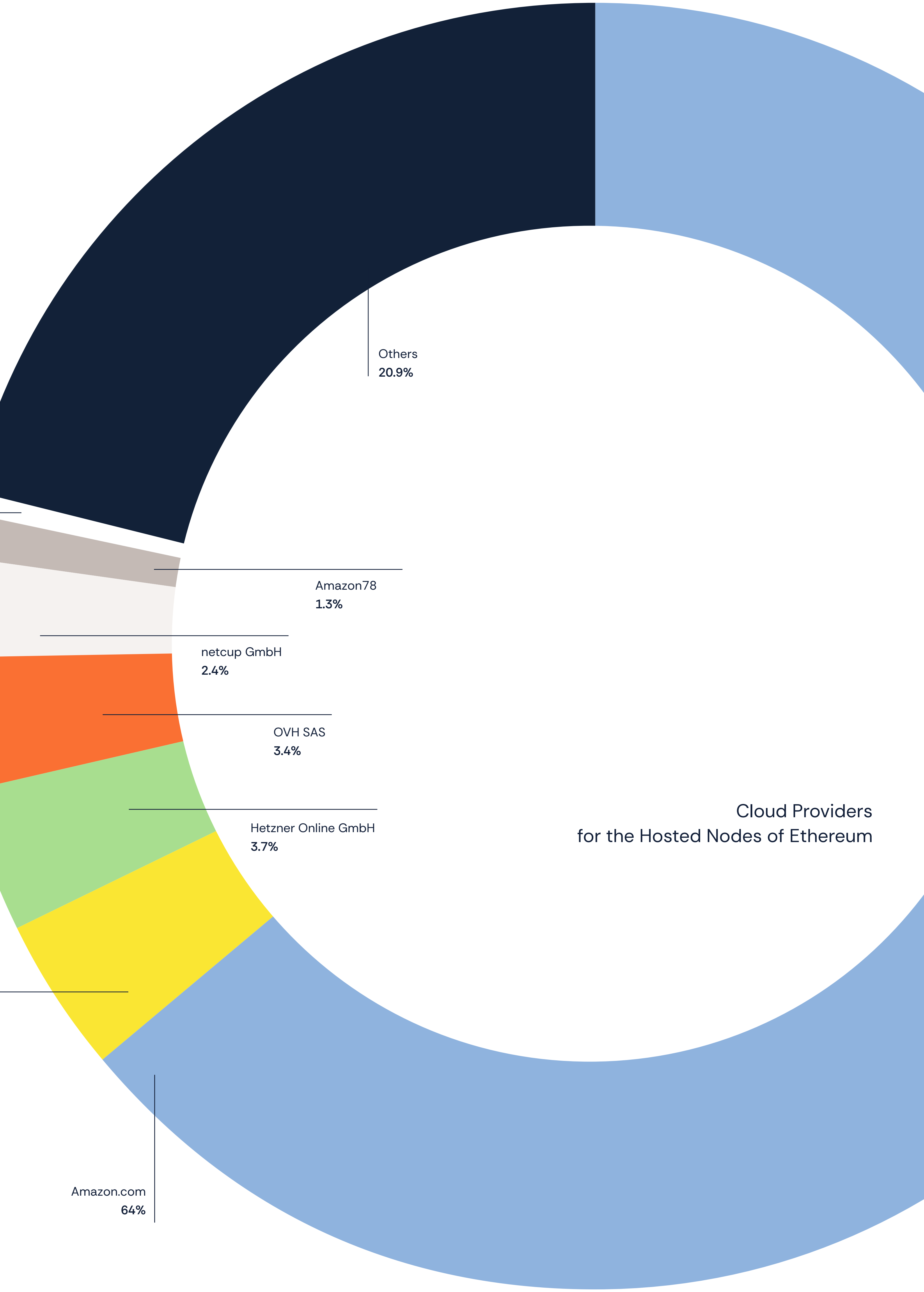
DNS allows names to be associated with legal persons and, thanks to its centralised nature, it guarantees stakeholders that it has mechanisms for resolving and settling disputes for the protection of their intangible assets[22] (trademarks and associated domain names).

More broadly, the vast majority of actors in the domain name system are governed by transparent rules of use, either drawn up in the multi-actor context of ICANN (for gTLDs) or by a national legislative and regulatory framework that also takes account of this multi-actor context. Such is the case in France, with Articles L45ff. of the Postal and Electronic Communications Code (CPCE).[23]

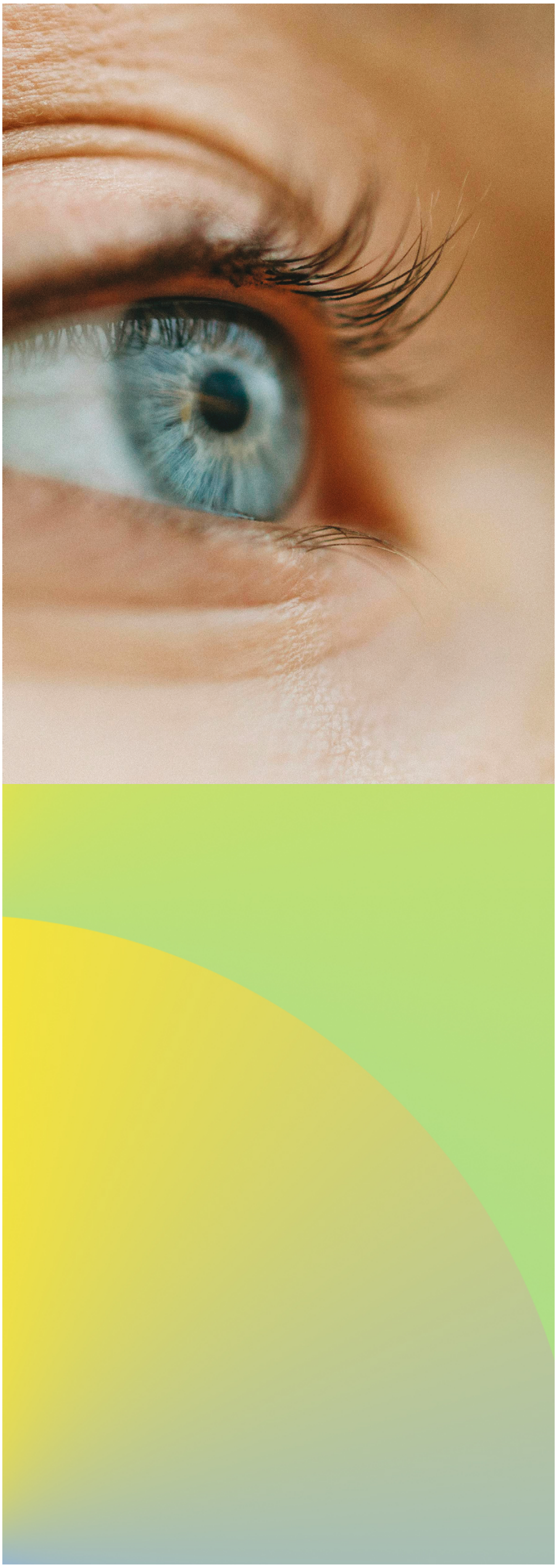
Given their decentralised nature, blockchain-based naming systems do not offer this type of solution as far as we are aware. As far as we know, the preparation of open and transparent systems of governance allowing these systems to evolve and be given tangible form has yet to begin. So although some businesses have acquired names[24] in these systems to avoid cybersquatting, most companies remain cautious[25] and are adopting a "wait and see" attitude.



Cloud Providers
for the Hosted Nodes of Ethereum



Cloud Providers
for the Hosted Nodes of Ethereum



Ease of use

Blockchain-based naming systems have some attractive functionalities, but are still difficult to operate for the average user.

A domain based on blockchain is a hash chain. Hashing is the process of converting a string of digital data into a hash, in other words into a short binary sequence that is unique to it. Each block has its own hash plus that of the block before it, and each block corresponds to an entry in the chain. So, for example, the website of a domain (i.e. the pages) is stored in the form of binary data and the user still needs software applications or special plug-ins to be able to access the website content. For example, the Chrome browser needs an external plug-in to be able to read the binary data of the blockchain and display the HTML code in the browser. The integration of clients that can query blockchains is still far from generalised.

In the case of several blockchain-based naming systems, inter-connection techniques are necessary to be able to access the information correctly[26]. This proliferation of naming systems makes them more prone to name collisions[27] and, in the absence of coordination, it is quite likely that an application resolving a name (e.g. "alice.eth") will obtain unexpected results. This name collision is impossible with DNS, which is a space in which each name is unique.

Energy consumption

The historical consensus method, still in force for Bitcoin, for example, for adding a block to the blockchain is the Proof of Work (PoW). This process consumes considerable quantities of energy and processing power to resolve complex cryptographic puzzles.

Another consensus mechanism, the Proof of Stake (PoS), now used on Ethereum for example, consumes much less energy but its use requires a degree of centralisation of the blockchain which, as we described above in the case of Lido, may run counter to the basic principles of blockchain.

It is difficult to form a global view of CO2 emissions generated by the hundreds or thousands of nodes in the network. According to data collected and assessed by the Cambridge Centre for Alternative Finance, including an estimate of the consumption of these nodes, the annual consumption of the Ethereum network is estimated at around 7 GWh (minimum 2.28 GWh and maximum 19.22 GWh).

For reference, Afnic's carbon balance sheet for 2022[29], calculated in Q1 2023, was 690 metric tons of CO2, for the administrative and technical management of the registry. In terms of the domain name, emissions stood at 153 g (calculations made by Afnic as part of a working group of registries[30]). This value includes not just emissions linked to servers, but also those of employees and the premises needed to host .fr domain names.

> According to the experts[31], one Ethereum transaction using the PoS represents about 10 g of CO2 emissions. There are currently around one million Ethereum transactions a day.

On its DNS infrastructure, Afnic handles roughly 1.8 billion DNS requests a day on its servers, as part of its DNS services linked to the .fr TLD and the other TLDs for which the association is the back-end registry operator (21 TLDs in all).

The measurement methodology developed and implemented by Afnic has allowed us to evaluate the energy consumption of its authoritative DNS servers and of its Anycast cloud. Energy consumption remains very stable, irrespective of the number of requests received. The load rate of the server processor, whether high or low, does not affect the consumption curve.
In all, this represents 15,768 kWh of electricity per year – just over the average annual energy consumption of three French households.

We should stress that although one Ethereum transaction and one DNS resolution are very different in terms of functionalities and objectives, they constitute essential services that are much in demand in these infrastructures. It seems that being able to evaluate and explain the levels of energy consumption and associated CO_2 emissions will be the determining factor.

Conclusion

The blockchain-based naming system has led to lively debate as to its pertinence as a replacement for DNS; it may seem more decentralised than DNS in certain respects and thus theoretically less exposed to breakdowns and unavailability. Nevertheless, there remain numerous challenges to overcome before it can become a serious alternative, the more so as the problems "resolved" by blockchain remain theoretical on DNS, the design of which has allowed it to demonstrate quite exceptional resilience.

Designed to be fully decentralised, resistant to cyber-attacks and to censorship, we have seen that blockchain-based naming systems do not in fact guarantee the complete abolition of centralisation.

The proliferation of blockchain naming systems makes them prone to confusion when resolving names, and their ease of operation so far remains debatable.

Lastly, there are two major concerns regarding the blockchain-based naming system: cybersquatting, and more generally the lack of transparent rules that take account of users' rights, and energy efficiency, with its very substantial consumption due to the complex calculations needed for the consensus mechanism.

DNS has a solid infrastructure, made to last as a protocol that is practical, effective, scalable and easy to use.

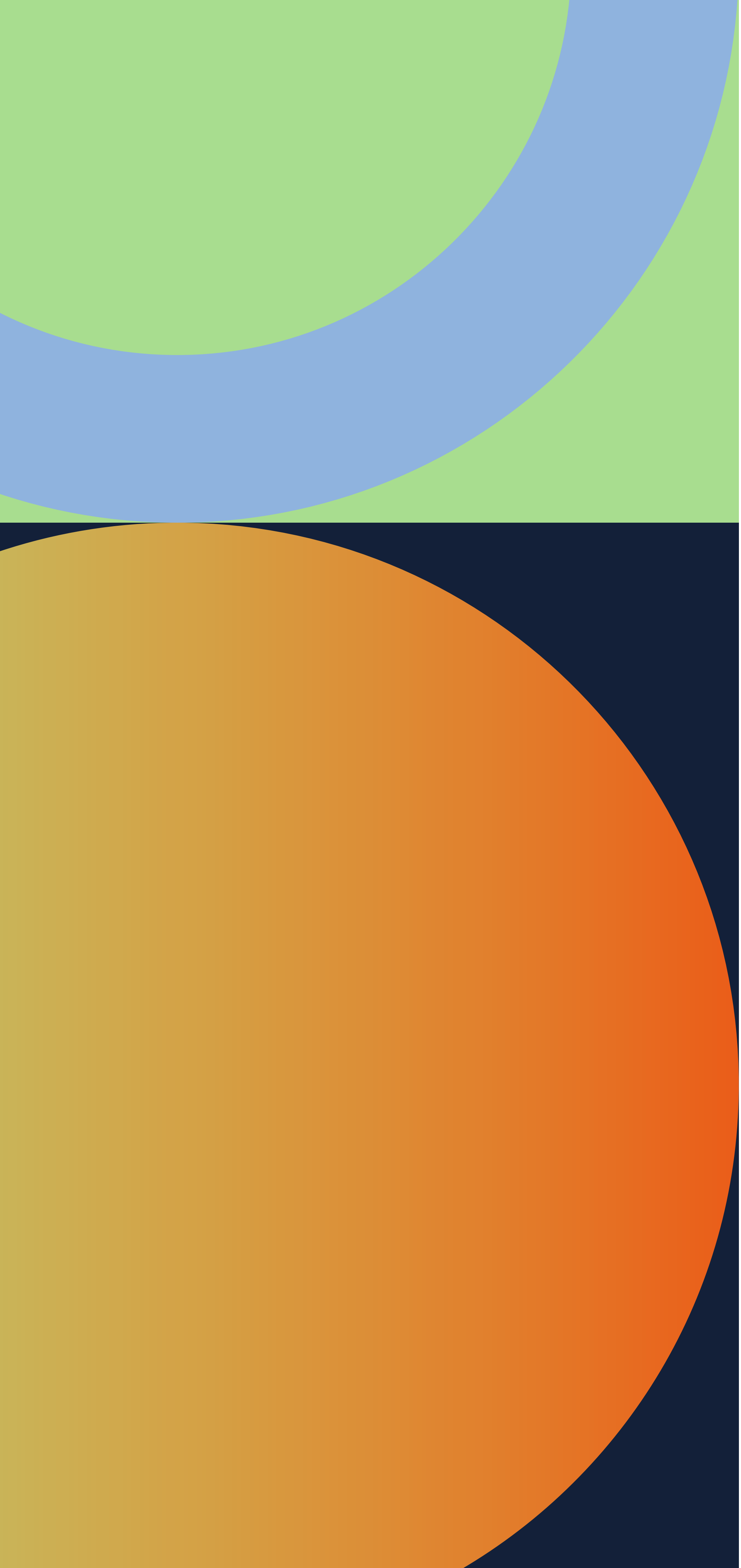
It could be useful to take the advantages of blockchain-based naming systems and use them as inspiration for application to the DNS. The aim: to limit censorship, to decentralise more, and to continue to strengthen security, even though extensions such as DNSSEC and the DoT/DoH protocols are highly effective in strengthening the security of the existing system.

It is difficult to predict the development of the blockchain-based naming systems in the coming years. Its adoption will depend on the compromises that the Internet community is prepared to make.

In any case, it will be important in upcoming discussions to take an overall approach and take account of the practical aspect, scalability, ease of use, regulation and energy efficiency.

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) is a subsidiary of ICANN responsible for the technical management of the "IANA function" (IANA stands for Internet Assigned Numbers Authority) *"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."* See: https://www.iana.org/about
7. https://www.afnic.fr/en/observatory-and-resources/news/the-afnic-scientific-council-shares-its-report-on-dns-based-Internet-filtering/
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/Afnic-2022-Corporate-Social-Responsibility-CSR-Report.pdfhttps://www.dnsbelgium.be/en/news/carbon-footprint
30. https://www.dnsbelgium.be/en/news/carbon-footprint
31. https://digiconomist.net/ethereum-energy-consumption



ISSUE PAPER

afnic

Internet
made in France

About Afnic:

Afnic is the registry for domain names in the following TLDs: .fr (France), .re (Réunion), .yt (Mayotte), .wf (Wallis and Futuna), .tf (French Southern and Antarctic Lands), and .pm (Saint Pierre and Miquelon).

Afnic also positions itself as a provider of back-end and registry solutions and services. Afnic – Association Française pour le Nommage Internet en Coopération,the French Network Information Centre – is composed of public and private actors: representatives of the public authorities, Internet users and service providers (registrars). It is a non-profit association.

www.afnic.fr

contact@afnic.fr