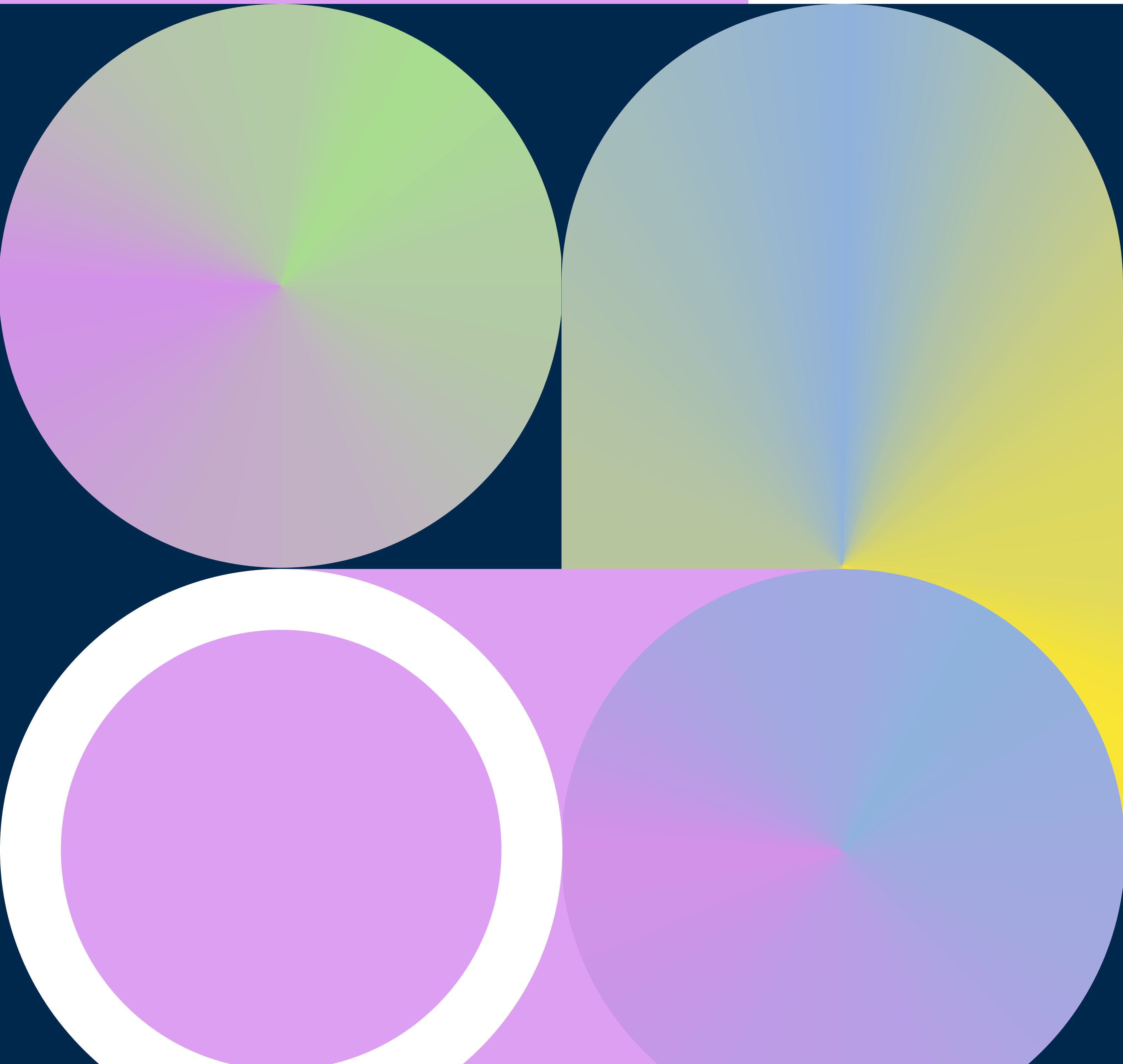
Can we do better than the DNS?

A comparative analysis of the security of blockchain identifiers

ISSUE PAPER

afnic
Internet
made in France



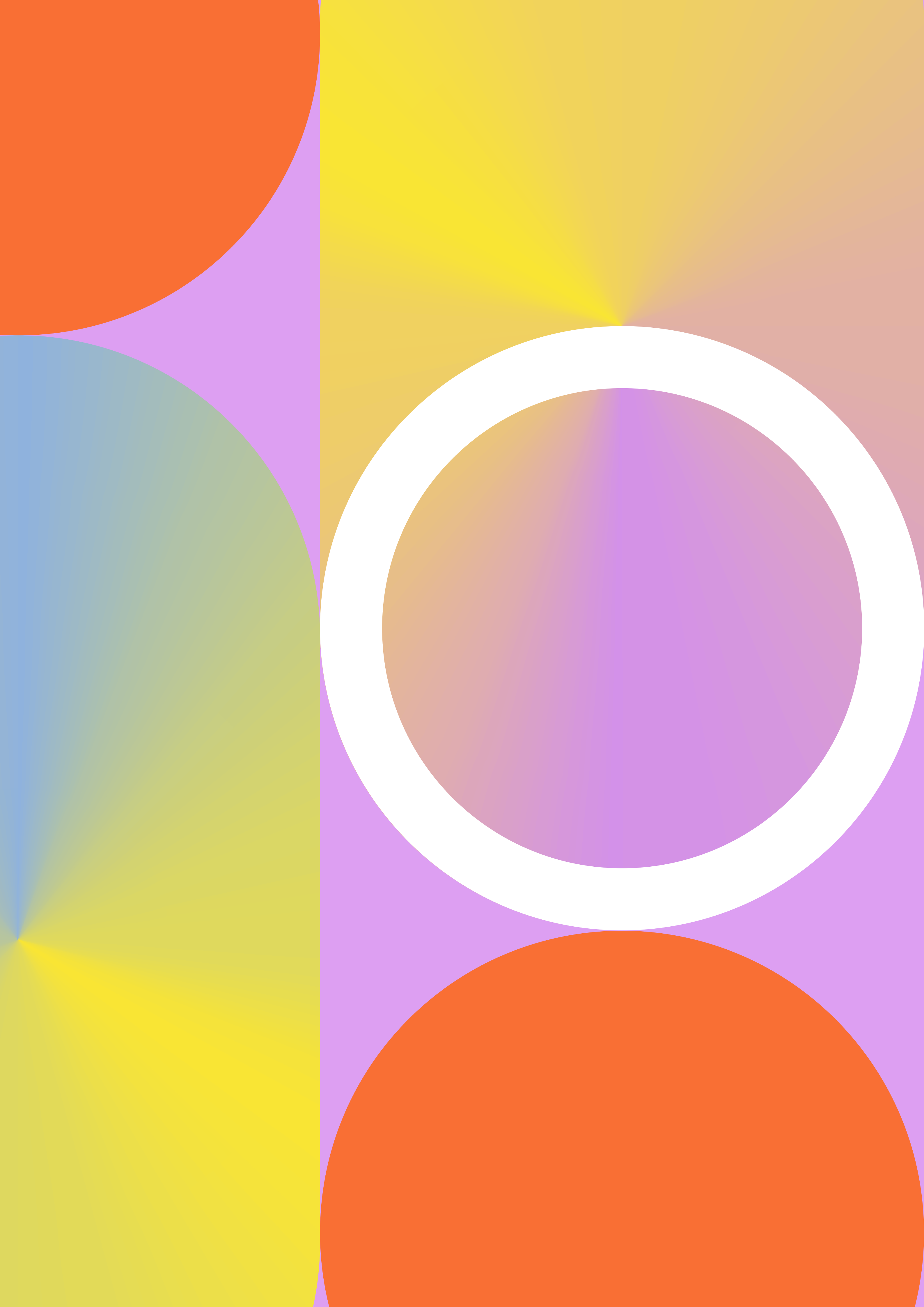


Table of Contents

Introduction

The DNS (Domain Name System) currently constitutes the reference infrastructure for recording and resolving domain names on the Internet. The system is tried and tested, standardised, and deployed worldwide. But in the past few years, initiatives for alternative naming systems based on blockchain have emerged and are seeking to establish themselves by exploring models other than the DNS.

In a previous paper, we studied the possibility of blockchain actually replacing the DNS. In this article, we explore the differences in terms of security that a "domain name" system based on a public blockchain would offer.

We put "domain name" in inverted commas when referring to the blockchain approach because, strictly speaking, they are not domain names. These identifiers may be similar in appearance, but they are not actually domain names as defined by the DNS. They are not governed by the same regulatory authorities or integrated with the root infrastructures recognised by the Internet Assigned Numbers Authority (IANA). So we should refer to them more correctly as blockchain identifiers.

Naming spaces based on blockchain, which are different from the DNS model, raise several questions: does blockchain really improve security for domain name holders? Is it more resilient? Does it offer greater confidentiality?

To answer these questions, we will start by comparing the DNS and blockchain through the prism of the two main services currently provided by the DNS: the registration of domain names, which guarantees uniqueness of the names in the naming space; and the resolution of domain names, allowing each user to access the data associated with a name reliably and as confidentially as possible. We will then look at how the DNS and blockchain handle these services and the pros and cons of each. Finally, we will analyse why blockchain does not necessarily constitute a miracle solution.

Does the registration of identifiers in blockchain offer the same safeguards as domain names in the DNS?

Both the DNS and blockchain offer naming space functionalities allowing names and associated data to be stored. But these systems differ widely in terms of how they guarantee the uniqueness of names, how they define holding, how they ensure the confidentiality of holders' data and their resilience to attacks. In this section we examine these various aspects with a view to understanding whether blockchain can really offer the same safeguards as a DNS registration.

The uniqueness of names ensured by the DNS is not absolute in blockchain

The DNS and blockchain use two different methods to safeguard the uniqueness of names in their naming space.

The DNS relies on a hierarchical architecture and a system of delegation. The uniqueness of names is ensured by a governance system coordinated by ICANN (Internet Corporation for Assigned Names and Numbers), which supervises the root of the DNS through its technical function, the IANA (Internet Assigned Numbers Authority), operated by its affiliate PTI[1] , and the registries that then manage each TLD (Top-Level Domain) on a delegated basis. The existence of a single root, accepted by all, ensures that no name can be registered twice in the same naming space. It is this organisation that ensures the global consistency of the DNS.

In the case of blockchains, the naming space is generally regulated by 'smart contracts', which define the rules for registration and resolution of the blockchain identifiers. In theory, these contracts ensure the uniqueness of all the names under a given smart contract, and several smart contracts can exist on the same blockchain. However, the uniqueness of the identifiers is not centrally managed at the global level of all blockchains. So it is possible for the same identifier to be allocated by more than one blockchain, leading to duplication.

This problem has already arisen with certain blockchain TLDs, such as in the .wallet saga where Unstoppable Domains and Handshake each offered a .wallet TLD, leading to a dispute on name allocation (see the analysis of the dispute and the judge's decision); or the case of .coin, in which Unstoppable Domains had to cease marketing .coin domain names after discovering that another blockchain, Emercoin, had already allocated this TLD (see details of the case). Other TLDs, such as .free and .visa, also pose problems in that they already exist in the official DNS root zone, thus increasing the risk of confusion between blockchain identifiers and traditional domain names. The latest DNSRF study[2] conducted with the support of Afnic reveals worrying overlaps at all levels. These clashes are likely to become more frequent with the introduction of new gTLDs, particularly in such categories as finance (.wallet, .coin), identity/security (.verify, .identity) and digital assets (.crypto, .nft, .blockchain). Of the providers studied, Freename had the highest number of direct conflicts with existing gTLDs – eight –, followed by DecentraName with four and Handshake with one. In order to include an assessment of the risk of clashes from the point of view of a ccTLD registry such as Afnic, we also cross-referenced the data collected by DNSRF and found hundreds of direct clashes between second-level blockchain identifiers and existing .fr domain names.

This uncoordinated coexistence may also lead to fragmentation of the naming space: for example, the Brave[3] browser recognises certain TLDs such as .eth and .brave which are not in the DNS, allowing users to share a .brave link that will not work, however, if the recipient uses a different browser.

Conclusion

in contrast with the DNS, where ICANN and the registries exercise authority, there is no global consensus as to which blockchain or which smart contract is to be considered authoritative. Each user chooses their preferred blockchain. This absence of unified governance poses a real challenge for the widespread adoption of blockchain identifiers.

> Each user chooses their preferred blockchain. This absence of unified governance poses a real challenge for the widespread adoption of blockchain identifiers.

From delegation to autonomy: two opposing visions of holding

Here we are talking about being the holder of a domain name or a blockchain identifier, which is not the same thing as being the owner. The difference is important: we do not own an identifier, we just have the enjoyment of it as long as we pay the associated costs and comply with the registry's policy throughout the time we use it. There is a profound difference between a domain name and a blockchain identifier as regards how holdership is defined and managed.

In the classic DNS model, particularly with the 3R model (Registry, Registrar, Registrant) (RFC 8499), registration of a domain name is based on a fixed term agreement, indefinitely renewable by the holder providing it fulfils its contractual obligations. This system is often criticised, since several actors — other than the holders themselves — can amend the holdership status of a domain name:

- **The registrar**, which can transfer a domain name to another holder in application of a court decision or in the event of non-compliance with the general conditions of use.
- **The registry**, which can also intervene in accordance with its own rules and obligations.

This model is by no means immune to cyberattacks, registrars and registries both being targeted. Certain registrars have already been compromised, allowing attackers to illicitly transfer or alter domain names. With this kind of attack, the system is sufficiently resilient and quickly restored thanks to safeguards and other disaster recovery plans. It is therefore essential to obtain a good understanding of the conditions specific to each TLD and each registrar in order to protect your rights to a domain name.

In the case of blockchain, holdership is managed in a fundamentally different way. With blockchain, the identifier is generally represented by a token, generated by a smart contract, held in a crypto portfolio.

In theory, only the portfolio owning the token can transfer or alter the identifier. However, there are several points to be borne in mind:

The reliability of the smart contract. A smart contract is a program, and as such it may contain bugs (with impacts of varying criticality), making the blockchain identifiers vulnerable. One of the most famous examples was the hack of The DAO, which revealed major failings in certain Ethereum contracts.

Some systems, such as ENS (Ethereum Name Service), guarantee that their smart contract will never be altered[4]. Others, however, can authorise updates supposedly to correct possible vulnerabilities, but which might also be misused to alter the registration rules and compromise trust in the system.

The security of the private keys. Unlike the DNS, where a centralised registry manages the association between domain name and holdership, blockchain is based on the possession of the private portfolio key. If this key is lost or compromised, the identifier may be definitively inaccessible or stolen.

Certain centralised services, such as cryptocurrency exchange platforms, host portfolios for their users. A large proportion of cryptocurrency assets (approximately 85% of bitcoins, for example) is held by centralised platforms such as Binance and Coinbase, which amalgamate the funds of thousands of users under a handful of blockchain addresses of which they are the sole holders[5]. This means that, in many cases, the real holder of a blockchain identifier is the exchange itself, not the end user. Numerous hacks have targeted exchanges, compromising their users' assets. For example, the recent attack on Bybit resulted in the theft of millions of dollars in cryptocurrencies[6]. In such a case, once the tokens have been transferred to another portfolio, it is impossible to recover them.

Conclusion :

Whether you use the DNS or blockchain, managing holdership of a domain name or a blockchain identifier requires constant vigilance. For the DNS, it is crucial to have a clear understanding of the rules of the registry and the registrar in order to minimise the risks of disputes or losses. For blockchain, it is essential to make sure the smart contract functions correctly and to carefully secure the private portfolio key. The decentralised holdership offered by blockchain may seem attractive, but it comes with new responsibilities and risks that must not be underestimated. While blockchain is indeed decentralised, users nonetheless go through platforms to simplify management of their identifiers, and this gives the platforms a centralising function. Furthermore, these platforms are themselves subject to the possibility of failure, whether technical or economic, and may jeopardise holders' chances of recovering the management of their identifiers, for example if the private keys managed via a platform are lost.

● Confidentiality: the identity of holders, protected by the DNS, is traceable with blockchain

Domain names are generally registered in order to host a website or publicly accessible services on the Internet. However, some holders may wish to remain anonymous, particularly for commercial or economic reasons (launch of a new brand or product, for example), political reasons, or simply to protect the personal data of a natural person.

With the DNS, confidentiality depends mainly on the policy of the registry, which decides what information is published via RDAP (replacing WHOIS). For some TLDs, such as .fr, information on natural persons is anonymised by default, while that of legal persons remains public. Other TLDs apply different rules depending on the registry, often in accordance with local laws (particularly ccTLDs). The choice of TLD thus becomes strategic, since account must be taken of the registry's confidentiality policy but also that of the registrar,

At first glance, blockchain seems to ensure absolute confidentiality, being based as it is on cryptographic addresses of electronic portfolios (commonly referred to as wallets) which appear as random sequences of characters. However, this perception is deceptive. In reality, blockchain does not ensure anonymity. All transactions are public and traceable. Unlike the DNS, where only certain information is accessible via RDAP or WHOIS, blockchain works on an open registry that can be consulted by anyone.

Any transaction carried out on a wallet can compromise its anonymity and allow the identity of its holder to be tracked down. This is particularly the case for the purchase of cryptocurrency on an exchange platform, which may require identity to be verified (KYC: Know Your Customer) or payment for a service with cryptocurrency on a platform associated with a known identity. There are advanced de-anonymisation techniques in existence which allow users to be identified by cross-referencing data from several sources[7]. Some attacks even exploit these weaknesses to compromise users' pseudonymity, such as for exavmple 'dusting' attacks in which a small amount of cryptocurrency ("dust") is sent to a large number of addresses. When these funds are used, it becomes possible to link several addresses together and to identify the user. An example of this technique is discussed here.

● Conclusion

In the case of the DNS, it is crucial to choose your registry and registrar carefully, taking account of their personal data management policies. In all cases, the registry and/or the registrar know the holder's identity. In the case of blockchain, confidentiality relies entirely on the user. Users need to be extremely vigilant in using their wallet so as to avoid involuntarily revealing their identity. So blockchain is not an infallible means of anonymisation, contrary to what one might think.

● Resilience: two robust architectures, each with its own weaknesses

The DNS is based on a hierarchical, delegated architecture, making it highly resilient to breakdowns. Thanks to its system of delegation, it is easy to verify and disseminate information. The redundancy of the root servers, the TLD and secondary name servers, ensures a high degree of availability. Mechanisms such as DNSSEC add a layer of protection against alteration of responses or cache poisoning by malicious actors, although their adoption is not systematic.

Like any system, the DNS may be vulnerable to targeted attacks, such as those compromising the registry or technically compromising a registrar, even though mechanisms such as 'Registry Lock' and 'Registrar Lock' exist and have been shown to work for the most sensitive domain names.

On this point, blockchain has proven to be very robust in the face of alteration of the data associated with an identifier. The association of a distributed registry with a cryptographic signature ensures that all participants can verify the information contained in the blockchain. To the extent that the cryptographic algorithms used remain resistant to the various kinds of attacks, blockchain can be considered safe and reliable.

Cryptographic attacks on blockchain often require colossal calculation power (e.g. 51% attacks), making them expensive and difficult to carry out against well-established blockchains. However, the distribution of the infrastructure used by the registry may be called into question, for example in light of the fact that the majority (69%) of the 4,653 active Ethereum nodes are hosted by three large cloud services providers, one of which, Amazon Web Services (AWS), hosts over 50%. This shows that blockchain is not as well distributed as one might think (see previous blockchain paper).

> Amazon alone hosts over 50% of Ethereum's active nodes.

Conclusion

The DNS and blockchain each have their strong points in terms of resilience. The DNS is reliable thanks to its delegated and redundant structure, but may be vulnerable to certain attacks aimed at registry or registrar infrastructure. Blockchain is based on a decentralised, ‘crypto by design’ model, making falsification almost impossible as long as the underlying cryptography remains robust. However, resilience is not confined to the availability of data. Consideration must also be given to other aspects such as governance, the updating of protocols and the management of disputes, which may pose problems on blockchain.

As far as registration is concerned, blockchain does not work better, it works differently, and that implies other risks

Registering an identifier on blockchain does not necessarily provide any more security than a classic domain name registration via the DNS. While blockchain eliminates certain trusted third parties such as registries and registrars, it also transfers all responsibility for security to the holder of the domain. This means that management of the private keys, understanding of the underlying smart contract and protection against attacks on wallets are all critical.

Conversely, the DNS is based on a delegated model in which security depends on the registries and registrars. This model offers guarantees as regards recovery and governance, but also introduces risks of access blocking, confiscation or alteration by third parties.

Security and resolution of identifiers: does blockchain work as well as the DNS?

Having identified the differences between blockchain and the DNS as regards registration, let us turn now to the second, more technical, stage: the resolution of domain names and blockchain identifiers.

Availability issues in DNS and blockchain resolution: continuity, autonomy and large-scale accessibility

The DNS resolution service is not a Single Point of Failure (SPOF) as may sometimes be suggested. There are in fact 13 root server names ([a-m].root-servers.net) spread over 1,900 physical servers, managed by several different bodies that provide this service on a global scale thanks to "Anycast" technology[8].

1,900
physical servers make the DNS available

This architecture distributes loads, improves resilience and reduces DNS response times. By way of reminder, the root servers contain the information needed to locate the top-level domain (TLD) name servers. All the TLDs are available here. The vast majority of TLDs themselves make use of "Anycast" technology to ensure their resilience.

For second-level names (such as mydomainname.fr, for example), responsibility for resilience rests with the domain holder. The holder can choose to host and manage its own DNS servers (as it would host its website), or use the DNS hosting services generally provided by its registrar or a DNSaaS (DNS as a Service) provider, which also make use of "Anycast" to ensure high uptime. By combining several hosting or DNSaaS providers, it is thus possible (and recommended) to improve redundancy and reduce the risks of outages. The techniques for making the DNS resilient are currently well-known and mastered.

In theory, a blockchain is infallible for the resolution of blockchain identifiers, since all transactions are entered in blocks and the consensus mechanism ensures that, after a certain time, all the nodes have the same view of the blockchain. So each actor would simply be able to query their own copy of the blockchain to resolve a blockchain identifier.

But this ideal notion is difficult to achieve in practice, since maintaining a full node of a blockchain requires considerable disk space, which limits the number of actors capable of hosting their own copies. Certain techniques allow the necessary storage space to be reduced (such as use of a "pruned node"), but this does not solve the wider problem of blockchain fragmentation. Unlike the DNS, which is based on an infrastructure with a single point of entry (the root), there are several blockchains, each allocating their own identifiers in their identification system. An actor wishing to resolve all the available identifiers therefore needs to maintain a copy of each relevant blockchain, which complicates the process still further.

It must also be stressed that name resolution in blockchain is particularly effective when confined to use within the blockchain ecosystem itself. As long as applications evolve in this environment, for example through the interaction of smart contracts, resolution is based on reliable, consistent, well-integrated mechanisms. On the other hand, as soon as we seek to use these identifiers in contexts outside blockchain (such as access to classic web content), difficulties arise. Users no longer always have direct access to the chain, resolution is then based on gateways or third-party services, and the promise of reliable, decentralised, trustworthy resolution is eroded.

● Conclusion

Although blockchain can theoretically offer a decentralised, resilient alternative, it poses a number of technical challenges which hinder its widespread adoption.

> As soon as we seek to use these identifiers in contexts outside blockchain, difficulties arise.

Integrity and authenticity of responses: in the DNS as in blockchain, everything depends on trust

Another fundamental aspect of security is ensuring the integrity and authenticity of responses to the queries of users or services. Guaranteeing that the response has not been altered by an attacker or falsified by the server providing it is crucial.

Originally, the DNS did not have a security mechanism ensuring the integrity or authenticity of responses. This weakness led to several types of attacks, including DNS cache poisoning, where an attacker injects false responses into the resolver's cache – a vulnerability made famous in 2008 by the researcher Dan Kaminsky. Other types of attack include MitM, or Man-in-the-Middle, where a malicious actor intercepts and alters DNS responses in transit.

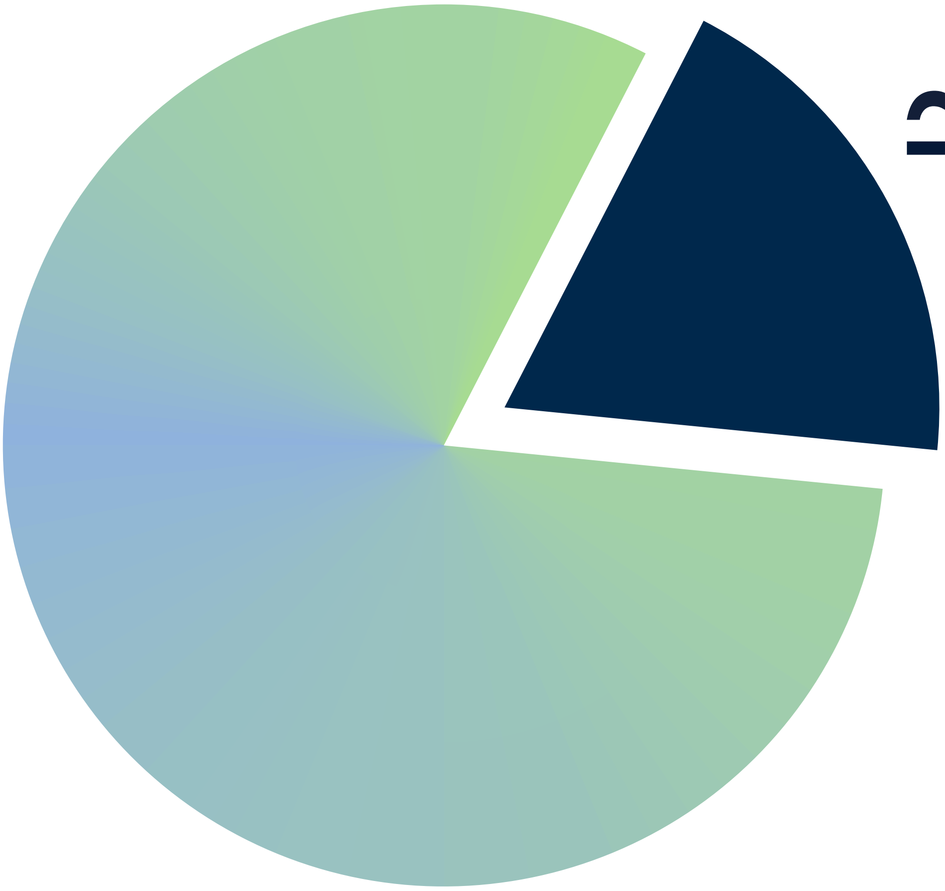
These vulnerabilities have been partly resolved thanks to DNSSEC (RFC 4033, 4034 and 4035). DNSSEC signs DNS registrations, guaranteeing their authenticity (via a 'chain of trust') and their integrity. If a domain is signed, it is possible to verify the legitimacy of the response by following the chain of DNSSEC signatures. However, DNSSEC is still not widely deployed: only about 35% of DNS queries are resolved with DNSSEC[9] and a large number of domain names are not signed (for example, only around 19.8% of .fr domains[10]).

A further problem is that users have to trust their DNS resolver. It is the DNS resolver that validates DNSSEC signatures and indicates whether the response is authentic via the AD (Authenticated Data) bit. However, this architecture is sometimes exploited to block access to content that is considered illegal or problematic (see section on Filtering).

Although this architecture is based on a trust model, it has certain practical advantages which explain its widespread adoption. It should be noted in particular that this delegation relieves users of the cryptographic calculations necessary to validate DNSSEC responses, which is especially useful when resources are limited, as in the case of connected objects. Furthermore, sharing the resolution cache among users of the same network improves the DNS response speed. Lastly, the choice of resolver may be guided by functional criteria such as the filtering of malicious sites or the activation of parental controls.

When it comes to the integrity of responses, blockchain is theoretically more robust. We only have to query the local copy of the blockchain directly to obtain an unalterable response, since all transactions are unalterable and verifiable. In practice however, very few users have a local copy of the blockchain on their computer. Blockchains have now reached a considerable size (Bitcoin 560 GB, Ethereum 1 TB), so hosting a full node is a major constraint.

To avoid this complexity, most users use API gateways which provide simplified access to blockchains. Some blockchain identifier services such as Freename[11] even officially recommend this approach. However, this solution poses the same problem as a DNS resolver, namely that the user has to rely on a third-party service for the response. There is no guarantee that the response has not been altered by this third party.



≃19%

is the percentage of .fr domains that are signed with DNSSEC.

Conclusion

In reality, resolution via blockchain does not provide any significant advantage over the DNS as regards integrity and authenticity. As long as users continue to rely on third-party gateways, they will have to trust an intermediary, whether for blockchain or for the DNS.

A promise, but not an absolute one, of query confidentiality

As previously mentioned, the DNS was not designed to guarantee the confidentiality of queries. Originally, all DNS queries were sent in clear text, so any actor on the net could intercept them and deduce sensitive information on the user. Fortunately, several protocols have since been developed to encode communications between clients and DNS resolvers: DNS over HTTPS (DoH - RFC 8484), DNS over TLS (DoT - RFC 7858) and DNS over QUIC (DoQ - RFC 9250). These mechanisms prevent the interception of DNS queries by intermediate attackers.

Logically, a DNS resolver, whether or not it uses an encrypted communication channel, always sees all the queries made by the user. That means the resolver used has to be trusted since it can collect and analyse queries, raising issues of privacy.

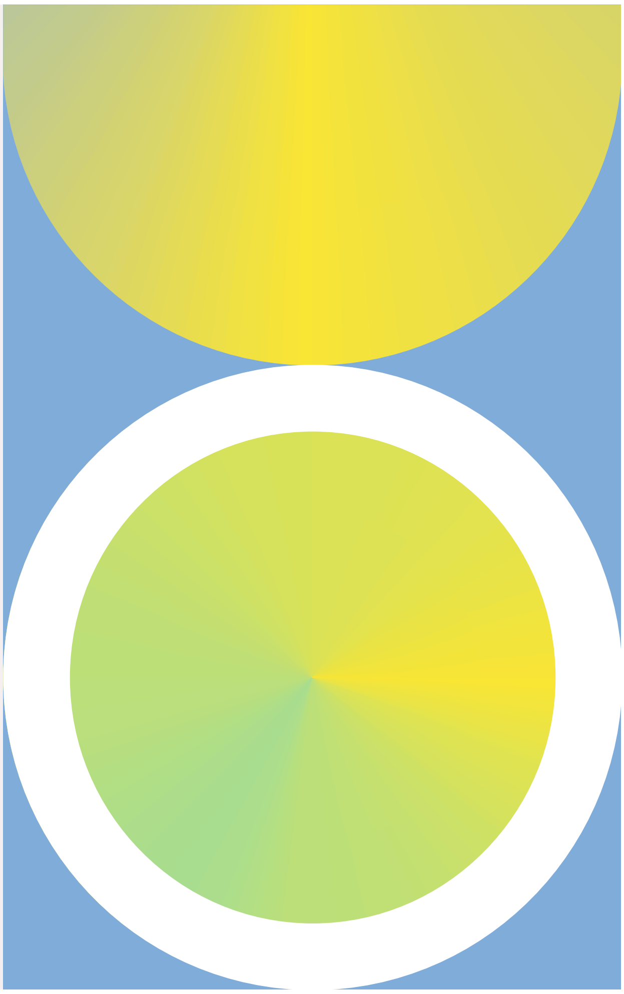
Furthermore, when the resolver does not know how to respond, it queries the authoritative DNS servers, which can also observe certain information on users' queries. This problem has been partly resolved thanks to the QName minimisation technique (RFC 7816), which allows a resolver to send only the necessary part of a query to the authoritative server, thus limiting the amount of information disclosed at each level of DNS resolution.

Blockchain takes a different approach. In theory, the user could directly query a local blockchain node without interacting with a third-party service. This would guarantee complete confidentiality, since queries would remain in the users' computer. However, just as with integrity, most users do not have a full blockchain node. They use API gateways which query the blockchain in their place. It is however important to point out, although this is not a widespread practice, that a user can also eliminate the intermediary represented by its Internet service provider's (ISP) DNS resolver or a public DNS resolver by hosting a local resolver itself, in which case the user interacts directly with the authoritative servers.

Returning to the use of a blockchain gateway service, the user's queries are known only to this gateway. Therefore this still implies reliance on a third-party service which could record or analyse the queries. Such is the case, for example, with the Web Brave browser, which allows blockchain identifiers to be resolved via the infura platform.

Conclusion

The issue of confidentiality affects the DNS and blockchain equally. With the DNS, solutions such as DoH, DoT, DoQ and QName minimisation reduce the leakage of information. With blockchain, confidentiality depends on users directly querying a local node (which they rarely do) or using a third-party gateway (which raises the same problems as a DNS public resolver). So, neither system guarantees complete confidentiality unless users take specific measures to minimise their exposure, such as installing their own DNS resolver or a copy of the blockchain.



● Filtering remains possible both in the DNS and in blockchain

The resolution of a domain name or of a blockchain identifier is an essential step for numerous applications, whether to access a web page or to interact with various services. Applications that do not use such an identifier directly or indirectly are few and far between. This makes them a preferred point of control, whether commercial or governmental.

As mentioned in the section on integrity, a DNS resolver can alter or block a query, since its workings rely on the user's trust. This ability is often exploited in order to put access blocking mechanisms in place for certain content. In many countries, Internet service providers (ISPs) are obliged by the authorities to redirect or block certain DNS queries. This method is relatively easy to circumvent by using an alternative public DNS resolver that does not filter queries (e.g. Quad9, DNS4EU, Cloudflare, etc.) or a personal resolver that directly queries the authoritative servers. However, this action remains effective since most users use the resolvers provided by their ISP by default.

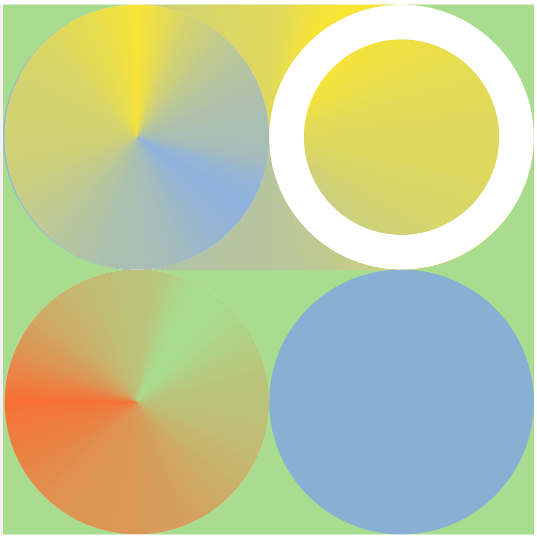
On the face of it, a public blockchain might seem impossible to censor, since it is decentralised and all transactions are unalterably registered. However, most users do not host a blockchain node themselves. They often use API gateways to query the blockchain, and these gateways may choose to block certain queries in the same way as a DNS resolver does.

> “Most users do not host a blockchain node themselves”

A notable example of blocking in the blockchain ecosystem is that of the blocking of Iranian users on OpenSea due to U.S. sanctions. This is a clear example of how key actors can refuse to interact with certain addresses or identities. You can circumvent these restrictions by deploying your own blockchain node, but that remains a complicated and impracticable option for most users.

Conclusion

Access blocking is possible on both the DNS and blockchain. In practice, neither system makes such blocking technically impossible. However, the rules of governance of the DNS being in most cases transparent and accessible, the DNS offers more safeguards, by its very governance, than blockchain in this area.



Blockchain's resolution promises do not hold up against the maturity and resilience of the DNS

Neither resolution system is infallible. In both cases, confidentiality and filtering are problems, largely due to the use of trusted intermediaries (resolver for the DNS and gateway for blockchain). The DNS however offers an effective resolution system that is easy to implement and above all mature and very widely used, with several decades of steady large-scale operation behind it, whereas blockchain is struggling to gain a foothold due to its complexity and its reliance on intermediaries.

Conclusion: between the promise of revolution and the reality

This paper has explored the differences between the DNS and blockchain identifiers. Presented as a decentralised alternative, blockchain identifiers propose a model far removed from the governance and infrastructure logic of the DNS. But while blockchain introduces different mechanisms for the registration of identifiers – particularly as regards individual autonomy –, it also shifts the risks and responsibilities onto the user, without systematically resolving security issues.

In terms of resolution, it is no match for the DNS. Blockchain's initial promises are still coming up against technical and practical constraints, whereas the DNS benefits from its maturity and unrivalled worldwide interoperability and deployment.

In short, blockchain does not "work better" than the DNS – it works differently and is still a work in progress. And this "differently" gives rise to opportunities as well as questions and risks. It remains to be seen how these two models might coexist or influence one another in future Internet practices.

Sources

1 · “Public Technical Identifiers (PTI)”
https://pti.icann.org

2 · “How much will blockchain identifiers clash with traditional DNS domains?” by Nathan Alan available at 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” available at 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” by RenaudH. available at https://journalducoin.com/exchanges/bybit-pire-vol-histoire-lazarus-blanchit-fonds-sous-nez-fbi/

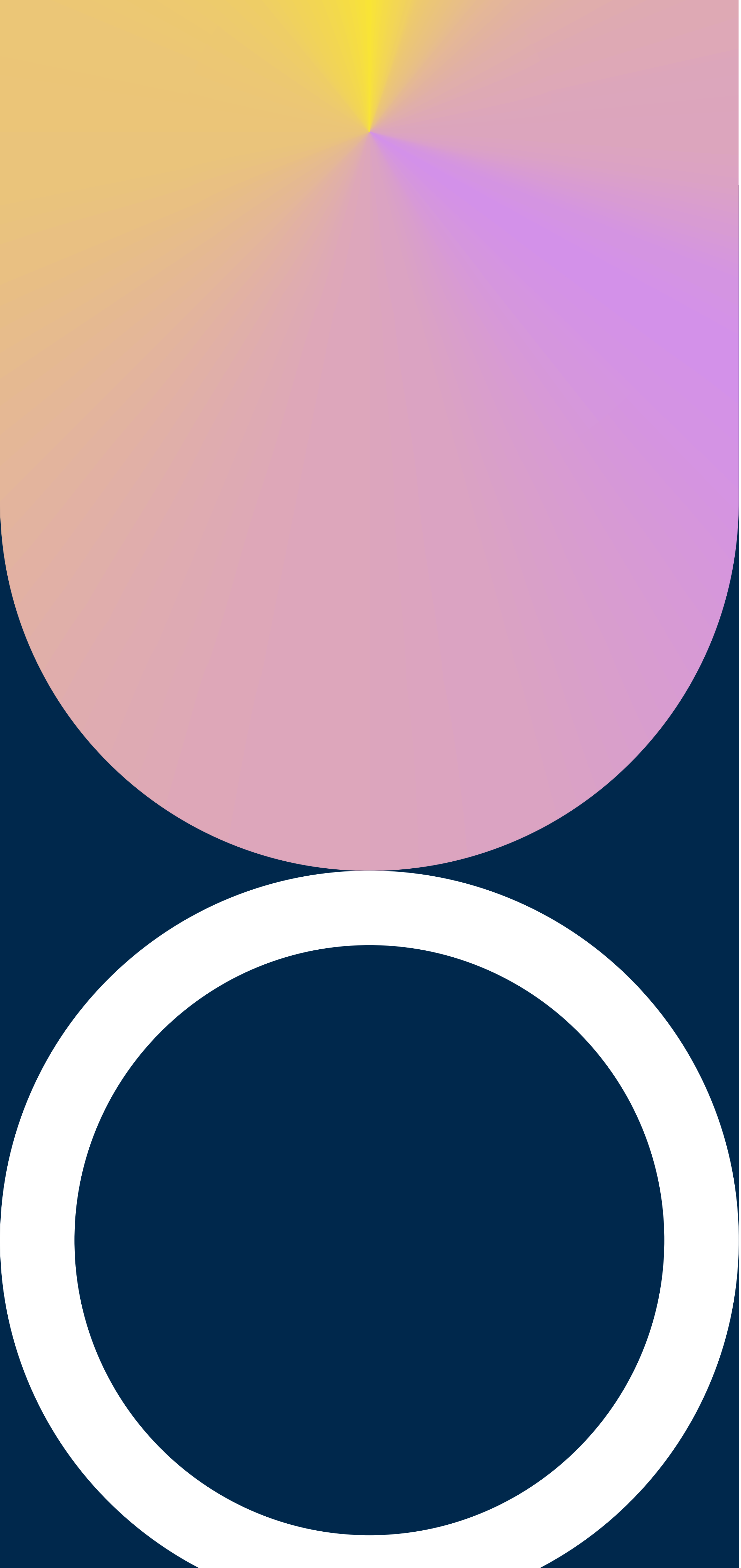
7 · “Data-Driven De-Anonymization in Bitcoin” by Nick and Jonas David available at https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/155286/eth-48205-01.pdf

8 · “Root-Servers” · https://root-servers.org/

9 · “DNSSEC Validation Rate” available at
https://stats.labs.apnic.net/dnssec

10 · “The .Fr in 2024” by Afnic available at
https://www.afnic.fr/wp-media/uploads/2025/04/The-FR-in-2024.pdf

11 · “Freename API Resolution” available at
https://docs.freename.io/freename-api-resolution



ISSUE PAPER

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/en/

contact@afnic.fr