# Internet of Universal Resources

White Paper

Jonathan J. Attia, Thibault Verbiest

September 2020 v0.2

# Abstract

First published in 1974 by V. Cerf and R. Kahn under the title "*A Protocol for Packet Network Intercommunication*[1]", the TCP/IP protocols, the basis of the Internet, have known a worldwide success since the invention of the World Wide Web in[2] 1989 by Tim Berners-Lee.

Thirty years later, the Internet Society is sounding the alarm about the extraordinary concentration of power that now prevails in the digital economy[3].

A handful of companies hold a virtual monopoly of the Internet in the critical areas of services (search engines, e-mail, etc.), infrastructures (global transit, content distribution networks, cloud computing services, etc.) and even, to some extent, Internet standardization (IETF,[4]5ICANN/IANA[6]7, W3C, etc.).

Parallel to this evolution of the Internet, blockchain technology appeared in 2008 under the name Bitcoin[8] and is based on the theoretical decentralization of its infrastructure (P2P[9]) and governance (PoW[10]).

As a consequence of this double decentralization, the blockchain introduces an innovative concept of autonomous trust: it is no longer necessary to use a *trusted third party to* execute and control a valuable computer transaction between 2 or more identified or pseudonymized (or even anonymized) parties.

It is in this context that the authors of this white paper have formulated a technical-legal proposal to create "universal" Internet services. These services will be operated by a greater diversity of actors and will attempt to respond to the challenges outlined by the Internet Society.

This will involve coupling for the first time the current Internet protocols with blockchain technology.

This "merger" will foster a more open, resilient and plural Internet that is capable of natively offering essential services such as information search, decentralized domain name management, digital identity, electronic messaging, data storage, computing power (AI), confidentiality, traceability and electronic signature.

[1] V. Cerf and R. Kahn, "A Protocol for Packet Network Intercommunication," in IEEE Transactions on Communications, vol. 22, no. 5, pp. 637-648, May 1974, doi: 10.1109/TCOM.1974.1092259.
[2] The birth of the Web https://home.cern/science/computing/birth-web
[3] Global Internet Report 2019, Consolidation in the Internet Economy https://future.internetsociety.org/2019/
[4] Internet Engineering Task Force https://www.ietf.org/
[5] Internet Corporation for Assigned Names and Numbers https://www.icann.org/
[6] Internet Assigned Numbers Authority https://www.iana.org/
[7] World Wide Web Consortium https://www.w3.org/
[8] https://bitcoin.org/bitcoin.pdf
[9] Peer to peer https://bitcoin.org/fr/vocabulaire#p2p
[10] Proof of work : https://en.wikipedia.org/wiki/Proof_of_work

By relying on new internationally standardized protocols, this innovation has the potential to make the Internet a true "common" for humanity, a network that is more respectful of fundamental rights and freedoms and in line with the sustainable development objectives set by the United Nations. It will also make it possible, for the first time, to program a digital territory and effectively combat "fake news".

This white paper outlines the proposal for a new Internet Protocol (*Internet of Universal Resources* - IOUR) combining the TCP/IP suite and blockchain technology, and some of the fundamental consequences of this marriage in terms of services, effective decentralization of services, diversity, societal impact, human rights, democracy and digital sovereignty[11].

# Acknowledgements

We thank Gabriela Salah and Ali El Broudi very warmly for their valuable help in the preparation of this whitepaper. Our thanks also go to Etienne Wéry, Philippe Vogeleer as well as to the whole IOUR Foundation team for their support and advice: Jean-Michel Amor, Georges Ataya, Dan Gavartin, Michel de Kemmeter, Christophe Boeraeve, Nelly Cornejo, Mhamed Dalla, Bruno Fedrici, Luc Jarry-Lacombe, Caroline Lequesne-roth, Lisa Loud, Jacques Marceau, Frédéric Marty, Céline Moille, Louis Pouzin, Paul Bougnoux and Tilen Cuk.

[11] The authors invite the interested readers to refer to their book « Un nouvel internet est-il possible ?» for a more detailed analysis of the current state of the Internet and its current (concentrated) economy, as well as of the blockchain technology, its deployment and its potential : https://www.larcier.com/fr/un-nouvel-internet-est-il-possible-2020-9782802766339.html

# Table of content

## 1. Is the right to access the Internet a human right ?

The United Nations General Assembly[12], as well as various UN agencies[13], have repeatedly stressed the critical importance of guaranteeing access to the Internet as a means of realizing the human rights recognized in international texts[14]: freedom of expression[15] and association, privacy, cultural participation, equality between women and men, and security and rights related to education, employment and well-being.

The Council of Europe, guarantor of the respect of the European Convention on Human Rights, shares the same analysis[16].

This observation is self-evident. However, the debate does not stop there. Since the World Summit on the Information Society (WSIS), organized under the aegis of the International Telecommunication Union (ITU),[17]more and more voices have been raised to go further and enshrine a new human right: the right of access to the Internet[18].

The right of access to the Internet means both the right not to be deprived of access to the Internet (non-interference) and the right to have access to the Internet infrastructure without discrimination.

An academic study has revealed that UN agencies, over the last fifteen years, have massively referred to the right to access the Internet, conceived as a "derivative" of freedom of expression and the "right to development"[19].

---

[12] See in particular the report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue : https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf . Recommendation 85 : " 85. Given that the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States. Each State should thus develop a concrete and effective policy, in consultation with individuals from all sections of society, including the private sector and relevant Government ministries, to make the Internet widely available, accessible and affordable to all segments of the population."

[13] Notably UNESCO, in its 2018 report on the Universality of the Internet: "The Internet is much more than just a digital technology. It is a network of interactions and economic and social relations. As such, the Internet has great potential for defending human rights, empowering individuals and communities, and supporting sustainable development", https://fr.unesco.org/internetuniversality.

[14] Universal Declaration of Human Rights (UDHR) and international rights agreements such as the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR), the Conventions on the Elimination of All Forms of Racial Discrimination (ICERD) and Discrimination Against Women (CEDAW), and the Convention on the Rights of the Child (CRC)

[15] Freedom of expression is one of the rights set out in the Universal Declaration of Human Rights most affected by the emergence of the Internet as a means of communication. Individual freedom of expression is defined in Article 19(2) of the ICCPR as including "the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media of his choice.

[16] https://www.coe.int/en/web/freedom-expression/guide

[17] https://www.itu.int/net/wsis/index-fr.html

[18] This recognition is subject to debate: https://en.wikipedia.org/wiki/Right_to_Internet_access

[19] Internet Access as a New Human Right? State of the Art on the Threshold of 2020 , https://www.researchgate.net/publication/328290234_Internet_Access_as_a_New_Human_Right_State_of_the_Art_on_the_Threshold_of_2020 , Prawniczy Uniwersytetu im Adama Mickiewicza, September 2018, in Przegląd

This study concludes that a process of consecration of the right of access to the Internet as an autonomous human right is indeed at work. It also proposes to strengthen it by relying on Article 15(1)b of the International Covenant on Economic, Social and Cultural Rights (ICESCR), which establishes the right to "enjoy the benefits of scientific progress and its applications"[20].

A parallel can be drawn in this respect with the "right to water", which was finally recognized as a fully-fledged human right after having been emancipated from the "right to an adequate standard of living" (art. 11 of the ICESCR)[21].

Let us note that in France, during its partial censorship of the Hadopi law, the Constitutional Council enshrined the right of access to the Internet as a fundamental right, as a component of freedom of expression[22].

## 2. The Internet: a « common » of humanity

Historically, the Internet is defined by reference to the TCP/IP protocol suite. It is therefore a strictly technical definition, centered on data transport, and not on services[23].

Today, it is hardly questionable that the Internet is conceived above all as a network offering a set of services, without which the Internet would be useless, namely:

- Naming and addressing (domain names)
- Search engine
- Digital identity
- Electronic messaging
- Digital data storage
- Confidentiality of electronic communications (traditional or post-quantum encryption)

Thus, for example, the ability to benefit from Internet access would make little sense nowadays without access to a possibility to search for available content (which is the obligatory entry point for any Internet user) or without the possibility of peer-to-peer communication (messaging).

[20] See also the Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind: https://www.ohchr.org/FR/ProfessionalInterest/Pages/ScientificAndTechnologicalProgress.aspx

[21] https://en.wikipedia.org/wiki/Human_right_to_water_and_sanitation

[22] Decision No. 2009-580 DC of June 10, 2009: https://www.conseil-constitutionnel.fr/decision/2009/2009580DC.htm https://www.numerama.com/magazine/13113-le-conseil-constitutionnel-fait-d-internet-un-droit-fondamental.html#hkyHrMoXimjkh7bB.99

[23] See in particular the definition given in October 1995 by the US *Federal Networking Council:* https://www.nitrd.gov/fnc/internet_res.pdf

These services have become "universal resources" of the Internet, and as such should be natively provided by the network and managed as "commons"[24].

These resources would form the fundamental components of the human right of "access to the Internet".

To this first category of "universal resources" can be added a second category of "critical" services for the planet's scientific, economic and industrial activity:

- Traceability and signature of electronic transactions
- Algorithmic capacity (artificial intelligence, *deep learning, etc.*)
- Distributed computing (e.g. for decoding the human genome[25])
- Digital currencies (e.g. the digital currencies of central banks or CBDCs[26])

Today, it is clear that these resources, whether "universal" or "critical", are offered by a handful of ultra-powerful companies. Many users do not really care because they believe that these services are free, while they pay the price, some would say the full price, by sacrificing their individual freedoms.

This is the case with the search engine or e-mail, which is offered free of charge in return for the massive collection and exploitation of users' personal data.

We are therefore confronted with a paradox: today's Internet requires us to give up some of our freedoms in order to access a digital space of rights and freedoms.

This paradox is therefore a threat to the very survival of Internet access as a human right.

It is precisely to resolve this paradox that we propose a new protocol: *Internet of Universal Resources* (IOUR).

[24] https://en.wikipedia.org/wiki/Commons
[25] https://en.wikipedia.org/wiki/Distributed_computing
[26] https://en.wikipedia.org/wiki/Central_bank_digital_currency

## 3. Internet Of Universal Resources (IOUR)

The equation to be solved is enabling the Internet to offer access to the above-mentioned universal resources while facilitating a greater diversity of operators. In other words, it is a question of avoiding (or reducing) the concentration of actors monopolizing services that should be natively available to all network users.

So what is meant by "a network that natively provides universal resources"?

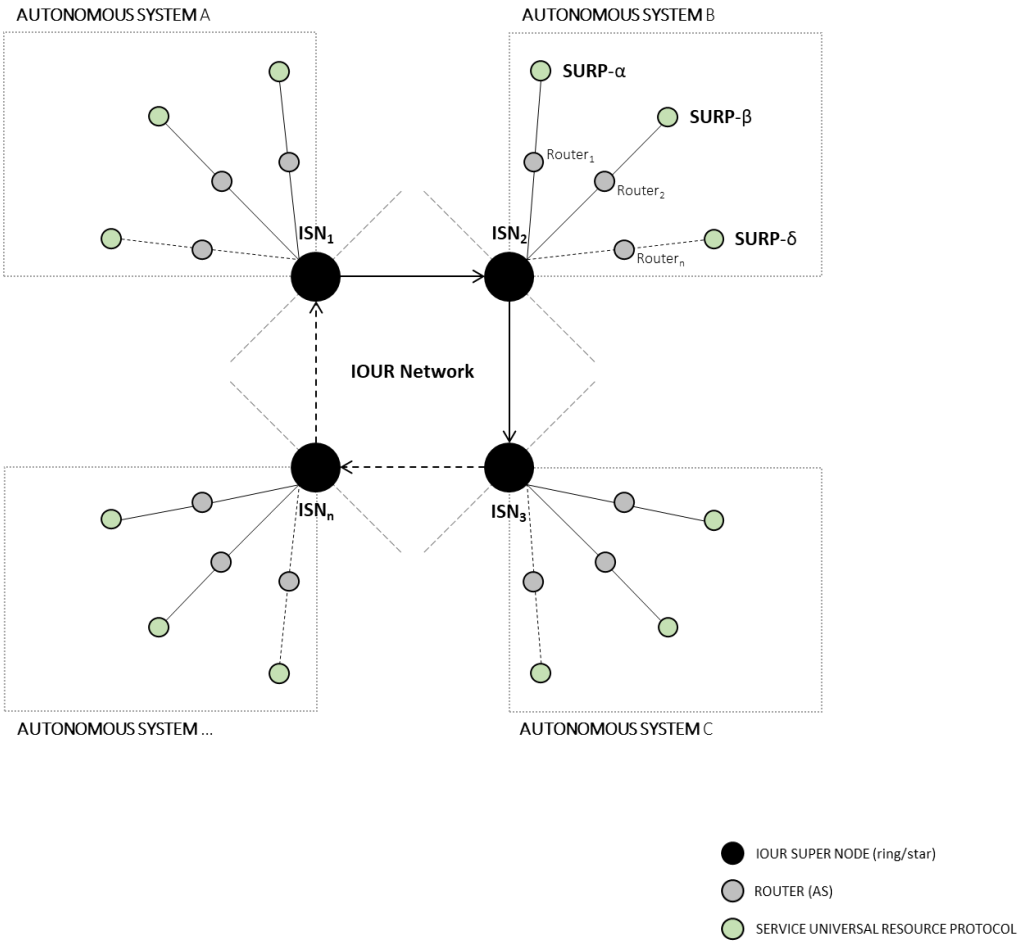
In technical terms, the challenge is to combine the data packet transport (TCP/IP) functionality with "intelligence" that allows packets to encapsulate a service "marker".

This service marker will be read and interpreted by all components of the network infrastructure (routers, *switches,* servers).

In doing so, services (universal or critical) are brought back to the protocol level of the Internet. Indeed, the packet (routed according to the rules of the protocol) "activates" access to these services from a dedicated "node" server.

This node is part of a decentralized network of nodes. The operators of these nodes can be either existing Internet service providers, specialized companies (software publishers, data centers, etc.) or public authorities. Ownership of these nodes could also be hybrid, shared between these different actors.

## Chart 1: IOUR network topology




*Source: Authors*

## Comments on Chart 1

The IOUR network topology was strongly inspired by the existing interconnections between the Autonomous Systems (AS) of the Internet network.

For the most part, AS are operated by ISPs, Tier 1/2/3 or IXPs[27] allowing IOUR a **native, progressive and inclusive deployment** among operators.

[27] https://www.internetexchangemap.com/

Just as ASN edge routers[28] run the BGP protocol[29] to connect to the Internet network, ISNs (at the[30] edge of autonomous systems) will eventually be deployed in all ASNs on the Internet network.

Each ISN node will be connected to SURP resources[31]. These resources will be distributed and decentralized due to their colocation with ASNs. Thus, it will become possible to access resources via the ISN nodes and thus by extension via the Internet network. This ISN/internet interoperability will be made possible by a double IOUR property of the IP datagram.

---

In doing so, we are "merging" the TCP/IP suite with blockchain/DLT technology,[32]and giving birth to a new, "augmented" Internet protocol, which we have named "IOUR" for "*Internet of Universal Resources*".

It should be noted that we could also do the same crossover with other alternative protocols to TCP/IP, such as RINA[33].

The technological crossover between TCP/IP protocols and blockchain protocol brings out a new fundamental property of the Internet network, with multiple consequences.

Each packet[34] becomes capable of contextualizing its purpose in terms of services, and the network becomes capable of processing the information contained in the packet.

---

[28] This is known as an "Autonomous System Number" (ASN). See https://www.iana.org/assignments/as-numbers/as-numbers.xhtml Here is an example with the Orange operator: https://awebanalysis.com/fr/ipv4-as-name-directory/France+Telecom+-+Orange/

[29] https://fr.wikipedia.org/wiki/Border_Gateway_Protocol

[30] For "IOUR Super Node

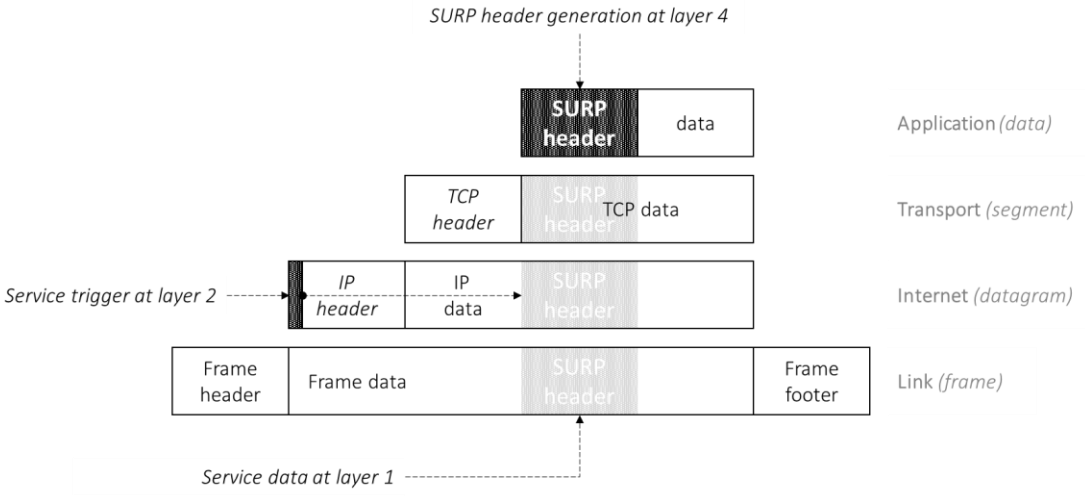
[31] For "Service Universal Resource Protocol

[32] The blockchain protocol that will operate this network will be specifically defined by consensus and will materialize in an open source standard.

[33] https://en.wikipedia.org/wiki/Recursive_InterNetwork_Architecture_(RINA)

[34] More precisely, each datagram

## Chart 2: SURP & TCP/IP




*Source: Authors*

## Comments on Chart 2

One of the possible approaches adopted by IOUR to establish native interoperability between ISNs and TCP/IP[35] is to integrate a double property in the IP datagram.[36]

This involves entering a **specific code** (or trigger code) in the datagram header field provided for this purpose to indicate to the router the existence of SURP information " or *SURP header " in the data* field.

The router will be able to detect the presence of the "trigger code" without processing overload and route the packet to the nearest ISN node.

The ISN will then be able to read and execute the SURP data and redirect the request to the nearest SURP nodes. The latter will return the processing result directly to the customer via the ASN's network infrastructure or the Internet.

---

An example of a universal resource offered by this new "augmented" protocol is digital data storage, hereinafter referred to as SURP-D[37].

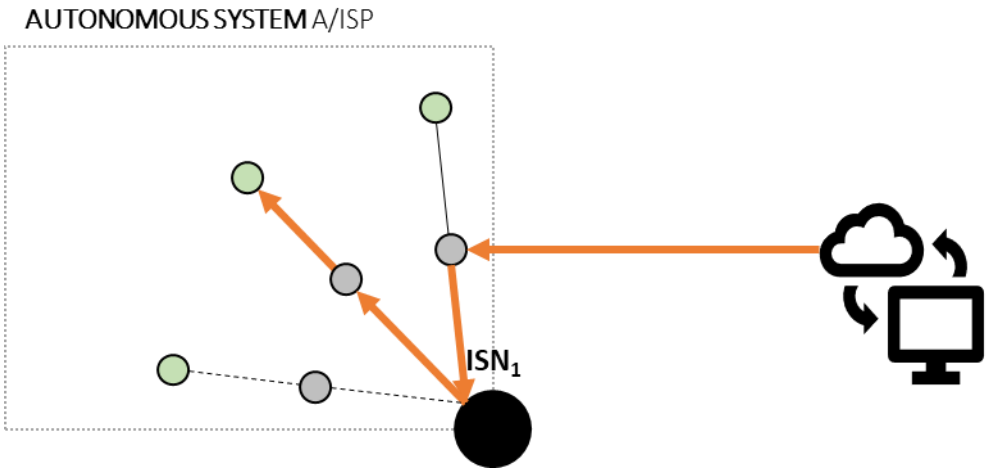
[35] https://fr.wikipedia.org/wiki/Transmission_Control_Protocol
[36] https://fr.wikipedia.org/wiki/Datagramme
[37] Acronym for "universal" services proposed by IOUR: SURP-D for Service Universal Resource Protocol - Data

This essential activity for Internet users is today extremely concentrated in that a handful of technology companies concentrate global storage capacity through their own infrastructure (data centers, submarine cables, etc.).

**The sequence would be as follows:**

1. The user calls the universal data storage service through their browser (or a specific "client[38]") by entering the SURP-D internet address,[39]which enables the service to be activated at the protocol level.
2. This request generates, via the browser,[40] "intelligent" packets that encapsulate the SURP-D service request.
3. These intelligent packets will be read and processed by the routers of the user's Internet Service Provider (ISP). These routers will have been updated beforehand in order to be able to read and interpret these SURP-D packets correctly.
4. ISP routers will redirect packets to the IOUR service server(s) (hereinafter *IOUR Super Node*, or ISN). The ISNs have the function of identifying the transported SURP service (in our example SURP-D) and redirecting it to the specific IOUR service.
5. The ISN[41] returns a page to the user's browser inviting the user to load the file to store[42].
6. The file is then stored, in a decentralized manner, by the SURP-D servers coupled to the Internet infrastructure.

## Chart 3 : Client-ISN Communication




*Source : Authors*

[38] https://fr.wikipedia.org/wiki/Client_(computer science)
[39] For example surpd:iour
[40] And via the network interface of the terminal (PC, tablet, smartphone etc.).
[41] The ISN is therefore, technically, a recursive services server, interoperable with the TCP/IP suite.
[42] For the sake of simplicity, we have excluded the authentication/identification phase, assuming that the file is intended to be public.

In summary, the ISN servers and the SURP-D server form the nodes of the IOUR network, natively interoperable with the Internet.

## 1. IOUR and domain name management

IOUR allows decentralized management of domain names and extensions (called *gTLDs*[43] in ICANN's traditional DNS, such as .com and .net).

As a reminder, the current DNS is managed centrally and hierarchically, between root servers and DNS servers. This infrastructure, through a directory, allows a unique correspondence to be established between a domain name and an IP address.

In the IOUR proposal, the correspondence between a domain name and an IP address is done through a registry administered and governed in a decentralized manner. We have named this service "SURP-N".

By way of illustration, here is what would be a common request from an Internet user using the "SURP-N":

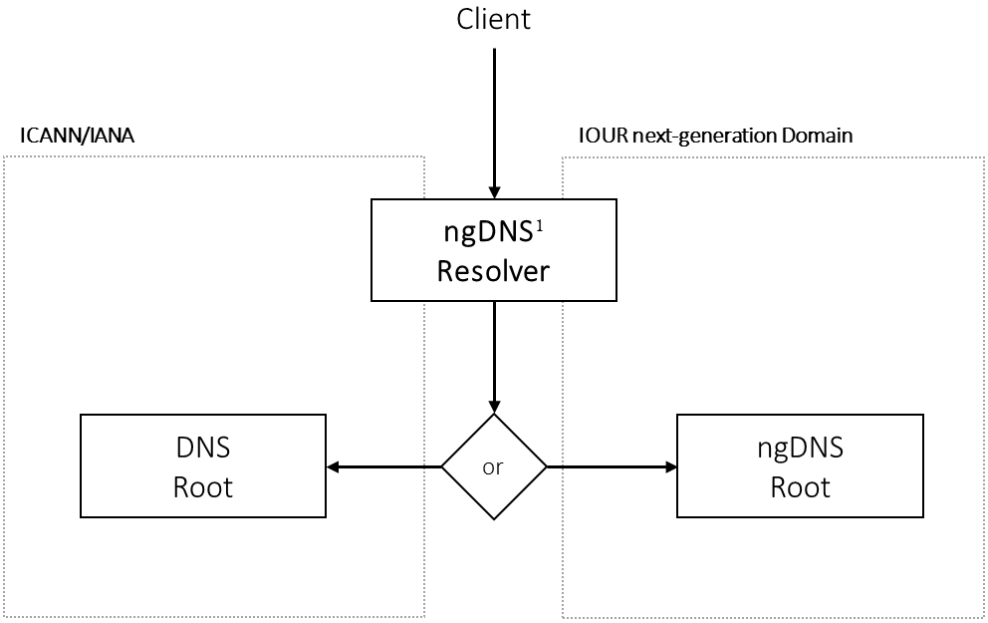
1. The user enters the desired domain name via their browser (or specific client), indicating a separator character distinct from the one imposed by the traditional DNS (for example, iour:org instead of iour.org).
2. This request generates, via the browser, "intelligent" packets that encapsulate the SURP-N service request.
3. These intelligent packets will be read and processed by the routers of the user's ISP.
4. The routers of the ISP will redirect the packets to the ISN server(s).
5. ISNs query the "domain names/IP addresses" mapping table. This mapping table is administered in a decentralized manner by the SURP-N nodes/servers.
6. ISNs return the IP address to the browser.

One of the advantages of this system is that it allows cohabitation with the traditional DNS, since the user can choose, within the same browser, to query the traditional DNS or the IOUR DNS (SURP-N).

---

[43] *Generic Top Level Domain*

## Chart 4: DNS & ngDNS




*Source: Authors*

### Comments on Chart 4

Domain names as well as the allocation of IP addresses are administered and managed by ICANN and the IANA function. No Internet resource would be accessible by machine or human without these two functions[44].

The need for a single registry is therefore necessary to avoid any conflict of accessibility or network blockage: two distinct resources with the same IP address or a domain name referring to two distinct IP addresses would create a serious malfunction in cyberspace.

In the IOUR proposal, we believe it is critical, even essential, to preserve the integrity of the current registry administered by ICANN.

IOUR's ambition is to extend the possibilities offered by blockchain technology to the existing domain name system. SURP-N (with ngDNS) will therefore be able to coexist with traditional DNS and will be natively compatible with the TCP/IP suite. This interoperability is based on the generic principle of the double property of the IP datagram. Thus, SURP-N will be a totally decentralized and distributed application, like other SURP services, and will benefit from (quasi-) non-hierarchical decentralized governance.

[44] The machine could use only numeric IPv4 addresses, or alphanumeric for IPv6 addresses.

Such a system makes it possible to deploy governance that is itself decentralized (as opposed to the traditional DNS), and as a result, to give a greater number of players the possibility of defining, by consensus, the TLDs and their assignment.

This governance could be exercised under the control or responsibility of the ICANN or another international governing body[45].

**This governance includes :**

1. The definition and assignment of first and second level extensions and geographical extensions[46]. The existing model will naturally provide inspiration for this area of governance.
2. The rules and obligations for the maintenance of the registry by the designated *registrars* ("*registrars"*).
3. The rules relating to the life cycle of an extension or domain name (creation, modification, deletion).
4. The mechanisms for resolving disputes related to the above management of domain names or extensions. (Of course, the governing body could simply associate the new DNS system with existing mechanisms (UDPR[47])).

The entire governance will be implemented via *smart contracts.* These will also be subject to governance rules (who can write/modify/call a *smart contract* linked to the SURP-N). This aspect is essential because it conditions the operationality of decentralized governance.

For the sake of clarity, let's take the following fictitious scenario: the registration of a "usurped" domain name within the extension :com[48]. The governing body[49] decided to entrust the WIPO, rather than a private company, with the task of registering the domain names of the ":com", because they considered that the generic top level domain names were "common goods" of humanity.

An individual registers a domain name that violates someone else's trademark. The trademark owner applies to WIPO to challenge the disputed registration by entering the SURP-N :claim address via his browser, which activates the *ad hoc* procedure provided for by the SURP-N protocol.

The user communicates via the interface all the information relating to their complaint. The protocol automatically redirects the complaint to the competent authorities of WIPO, which in turn initiates the appropriate UDPR procedure. This procedure has been translated into a *smart contract* attached to the SURP-N. The UDPR body judges that the domain name has indeed been usurped. It transmits its decision, via the SURP-N protocol, to the *smart contract,* which automatically proceeds to the execution of the decision (cancellation or transfer).

[45] It could be, for instance, the International Telecommunication Union (ITU) or a new entity.
[46] Example: who is entitled to the extensions :fr or :uk ?
[47] *Uniform Domain-Name Dispute*, see in particular WIPO's UDPR: https://www.wipo.int/amc/fr/domains/
[48] And not .com, because it is indeed a "SURP-N" extension.
[49] We could also have chosen ICANN or ITU. This is ultimately a political issue.

We could push the exercise even further by imagining that the condemned party would be required to pay the costs of the proceedings. These procedural costs are automatically relayed to another *smart contract* linked to a SURP-P protocol (P for "payment") which sends a request for payment in digital currency. The individual in question will then be able to pay with their electronic wallet (see 3.10 *below*).

This scenario assumes that the parties involved have a native identity (SURP-ID[50]), which will be discussed below.

---

## 2. The "search engine" service

There is little debate about the importance of the "search" function within a network as vast as the Internet. It is a function as essential as it is concentrated[51].

**Today's search engines raise three fundamental questions:**

1. Lack of transparency and neutrality of the search engine algorithm (indexing and query mode).
2. Incompleteness of the indexing, for at least two technical reasons: on the one hand, the indexing is performed at more or less long intervals by the robot, and on the other hand, not all available content can be indexed (e.g. databases[52]).
3. The centralization of personal data related to the research and indexing activity. This last point is the most sensitive. In the current reality, the dominant search engines literally own the privacy of Internet users, which[53] leads to a fundamental problem in terms of democracy and digital sovereignty.

The SURP-S (S our "search") protocol provides a relevant answer, by changing paradigm. Indexing is performed in "*bottom-up"* mode, rather than "*top-down*". In fact, all newly created content is self-indexed[54] and distributes the result of this indexing to the SURP-S, which in turn is responsible, in a decentralized (and distributed[55]) manner, for optimizing the general index.

---

[50] Including for payment in digital currency because the electronic wallet is attached to the SURP-ID, see 3.3 and 3.10 *below*.

[51] In April 2020, Google had 86% market share, compared to 6% for Bing and 3% for Yahoo! https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/.

[52] The visible part of the internet is estimated at 0.03%! : https://oedb.org/ilibrarian/invisible-web/

[53] The history of searches actually makes it possible to draw up an extremely precise profile of Internet surfers, and even of the community, and to monetize it.

[54] This auto-indexing feature requires the installation of a client within the content server and will allow its administrator to fine-tune the indexing properties, especially for databases.

[55] The processing of this indexing and its optimization can be distributed to the nodes of the SURP-S network, or even the SURP-C network (see *below* 3.5).

Let's take the following example:

1. The user enters, via browser, the name of the protocol followed by their query (example: surp-s: what is today's weather?).
2. This query generates, via the browser, "intelligent" packets that encapsulate the SURP-S service request.
3. These intelligent packets are read and processed by the routers of the user's ISP.
4. ISP routers redirect packets to the ISN server(s).
5. The ISNs forward the request to the SURP-S nodes, which return the response to the ISNs[56].
6. ISNs return the search result to the user's browser.

This is indeed a paradigm shift because:

1. The indexing and querying algorithm will be defined by consensus since it is an *open source* protocol. Internet standardization bodies (IETF, W3C, ISO) will therefore be able to become involved in the definition of the protocol, ensuring transparency and neutrality.
2. Indexing will be significantly more complete because content server administrators will be able to make “invisible” content accessible[57].
3. There is no longer any processing of personal data by a technology company since all research-related data will be anonymized, under the protocol, in strict compliance with the GDPR.
4. The “right to be forgotten” linked to content indexing[58] is natively implemented in the SURP-S protocol. The Internet user enters surp-S :claim and can request, under legal conditions, the deletion of the data they indicate. This requires that the user be identifiable, according to the SURP-ID protocol (see *below* 3.3).

5. The continuous indexing of SURP-S makes it possible to create a complete archiving of the web according to a decentralized architecture, which has never been achieved in the history of the Internet. This archiving will function according to a dedicated protocol SURP-A ("A" for archive). The “right to be forgotten” will also be implemented from within SURP-A :claim.

This last feature is aligned perfectly with the Charter on the Preservation of Digital Heritage adopted by UNESCO in 2013, and for the first time allows it to be fully implemented. Indeed, UNESCO warns States against the "loss of digital heritage" and urges them to take legal, economic and technical measures to preserve this heritage[59].

[56] In some cases, the SURP-S can also deliver the result directly to the user's browser.
[57] By default, all new content will be indexed, unless otherwise set.
[58] https://en.wikipedia.org/wiki/Right_to_be_forgotten
[59] Charter on the preservation of digital heritage: http://portal.unesco.org/fr/ev.php-URL_ID=17721&URL_DO=DO_TOPIC&URL_SECTION=201.html

## 3. Digital Identity

There are as many digital "identities" as there are applications.

The term "identity" rarely corresponds to an official identity as defined by national legislation.

In practice, digital identity is composite, in that it is made up of a set of elements (usually personal data in the sense of the GDPR[60]) that contribute to establishing an online identity (identifiers, passwords, credit card numbers, cell phone numbers, etc.).

The digital identity "market" is growing rapidly and is dominated by the Internet giants. This is quite logical insofar as the identities they deliver are linked to their services, which are dominant. This dominant position is reinforced by the fact that other online service providers offer, for the user's convenience, authentication based on these digital identities ("*single sign-on"* or SSO[61]).

This situation has two major disadvantages:

- Elements relating to the digital identity of Internet users are centralized with service providers. Their control is therefore beyond the control of Internet users. In addition, this centralization makes the data more vulnerable to computer attacks.
- The data forging digital identity is uncertain in terms of proof of that identity. They do not have the seal of competent authorities to attest to a certain identity.

The SURP-ID protocol provides a solution by allowing Internet users (as well as legal entities) to be identified by the competent authorities who issue a digital identity linked to the SURP-ID protocol. This requires each authority to define its own digital identity standard. Such "official" identification is certainly not essential for the creation of a SURP-ID (and therefore for the use of other SURP services) but may be required for certain online services subject to enhanced identification requirements (e.g. opening an online bank account[62]).

Here is an example of an "official" SURP-ID creation sequence:

1. The user enters the SURP-ID :registration address in their browser.
2. A form from the competent authority appears and the user fills in the necessary data. Eventually, if required by the authority, the user will have to go to the authority for identification purposes.
3. The identity is generated in the form of an electronic certificate, signed by the competent authority via the SURP-S electronic signature function (see 3.7 *below*).
4. Each time the user will have to access his digital identity (via his browser), they will have to authenticate their identity. The level of this authentication will be defined by

[60] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

[61] For example, Facebook Connect and Google Identity Platform

[62] These are known as KYC ("Know Your Customer") requirements for the purpose of combating money laundering.

consensus, and could be based on existing authentication standards[63], in particular the strong authentication standard of the second directive on payment services ("PSD2"[64]).

5. This "official" digital identity can be enriched with other identifying data (e.g. a certificate of residence, recent bills, etc.) in order to comply with certain regulations[65]. The user will simply have to "load" these documents via their administration interface ("SURP-ID:admin").
6. Via this administrator interface, the user authorizes (or revokes) the sharing of their identification data, with the desired granularity. For example, a user could share only their date of birth, or even allow a calculation of their adult status without communicating the date of birth (*zero knowledge proof*[66]).
7. All SURP-ID communications will be encrypted and the storage of identification data will also be encrypted and distributed (SURP-D).

SURP-ID therefore provides an environment that addresses the above concerns:

- The data remains under the control of the user and is stored in a decentralized manner ("*self-sovereign identity*").
- Digital identity becomes certain and unique

In order to preserve the privacy of users, they will be able to issue a command to pseudonymize or even anonymize their identity when they associate their SURP-ID to another SURP service. For example, a user will be able to anonymize their internet research carried out from SURP-S.

## 4. The electronic messaging system

We find the same concerns with respect to email service: a handful of dominant technology companies[67], centralized data, and questionable security[68].

[63] For example: the Auth0 standard: https://auth0.com/learn/how-auth0-uses-identity-industry-standards/ , or the FIDO standard: https://fidoalliance.org/

[64] https://ec.europa.eu/commission/presscorner/detail/fr/QANDA_19_5555 ;

[65] For example, in the case of a banking KYC

[66] It is also known as *blind computing* or *trusted execution environment* (TEE): https://en.wikipedia.org/wiki/Trusted_execution_environment . This function will be native to the SURP-ID protocol.

[67] Gmail, Hotmail, Office 365 etc.

[68] See for example the computer fraud that hit Twitter in July 2020: https://www.nytimes.com/2020/07/17/technology/twitter-hackers-interview.html More than 1,000 Twitter employees had access to all social network accounts before the fraud: https://mobile.reuters.com/article/amp/idUSKCN24O34E Such a fraud could hit any other centralized service provider.

It is certainly possible to create your own mail server, but it will then be operated via a "cloud" whose governance will necessarily be centralized[69].

We propose here the SURP-M ("M" for "mail") protocol to offer a native Internet protocol e-mail:

1. The user enters, via the browser, the command to create an e-mail address ("SURP-M:registration") and configures it via the interface that appears.
2. The messaging system parameters can be modified via the SURP-M administration interface :admin. These parameters will concern in particular:
    - The association to the SURP-ID (in order to link the e-mail to the user's digital identity)
    - Location of e-mail storage. In the IOUR proposal, the storage is by default decentralized. However, the user can specify a location for this data (for example, specify that the data will be stored on European SURP-D servers in order to comply with the requirements of the GDPR).
    - The level of confidentiality (encryption) of the data[70]
    - Management of access rights to archives (also decentralized)

Once again, the SURP-ID association with SURP-M can be declined under a real, pseudonymized or anonymized identity, at the user's choice. The user will thus be able to create several email addresses, some coupled with their "real" identity, others not.

## 5. Confidentiality of electronic communications

This service is transversal to all the above-mentioned SURP services (data storage, search history, digital identity, e-mail). We have named it SURP-C ("C" for "confidentiality").

SURP-C will bring the "encryption" dimension to the protocol level and will be called whenever encryption is required. All the usual encryption modes will be available natively (AES[71], RSA[72], ECC[73]) as well as the post-quantum encryption protocols currently under study (notably within the American NIST[74]). Post-quantum encryption is defined as encryption that is known to be resistant to the power of a quantum computer[75]. Indeed, we are entering an era where a new generation of computers (called "quantum") will, in theory, be able to break current cryptographic protocols, which is an existential threat for entire industries, such as the financial sector.

In addition, the SURP-C protocol will, where the communication infrastructure permits, enable end-to-end quantum communication. Quantum communication refers to electronic

[69] Example: Microsoft Office 365

[70] The SURP-M and SURP-D protocols, which are natively interoperable, can apply an advanced confidentiality strategy by fragmenting the encryption key (symmetric or asymmetric) and/or fragmenting the encrypted data. Such a strategy may be required in cases where security is critical (e.g. government applications).

[71] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[72] https://en.wikipedia.org/wiki/RSA_(cryptosystem)

[73] https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

[74] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

[75] In other words who is resistant to Shor's algorithm: https://fr.wikipedia.org/wiki/Algorithme_de_Shor

communications that are completely tamper-proof, ensuring the exchange of cryptographic keys without the possibility of interception. This mechanism is called QKD[76].

## 6. Traceability of electronic transactions

Traceability is natively available since all SURP services are deployed from a blockchain infrastructure (the ISN and SURP nodes).

It is therefore up to the user to activate this feature to apply it to the service of his choice.

Let's take the following example: a user sends an e-mail, with an attachment, to several recipients. The message is likely to have significant legal effects. From his SURP-M interface, the user activates the SURP-T function ("T" for "traceability"). The traceability of this message will be ensured by the SURP-B blockchain ("B" for "blockchain"), through the digital fingerprints ("hash") of the various elements of the communication (sender, recipients, message and attachment).

The user may also wish to store this sensitive message on SURP-D servers located in Europe (to be GDPR compliant) and prove it with the SURP-T traceability functionality. It is even possible to guarantee storage in Europe even if the recipients are outside the European zone. They will then be able to access the content of the e-mail but without being able to store it locally.

It is important to remember that the identity associated with the SURP-T can be, at the user's choice, declined on a real, pseudonymized or anonymized identity. This association can be symmetrical or asymmetrical. For example, a whistleblower will be able to anonymize his real identity while ensuring the real identity of his recipient and the traceability of the message content. This is an example of asymmetrical traceability of the identity.

## 7. The electronic signature

Electronic signatures have been around for more than 30 years and have been subject to European regulations since 1999, updated in 2014 by the eIDAS regulation[77].

The electronic signature is an essential brick of the digital economy because TCP/IP protocols do not natively implement this function.

The electronic signature has two functions:

- It guarantees the integrity of the electronic document with legal value (e.g. a contract).
- It identifies the signatories.

[76] https://en.wikipedia.org/wiki/Quantum_key_distribution
[77] https://en.wikipedia.org/wiki/EIDAS

In this respect, the regulations establish a hierarchy within the technologies used to sign electronically. At the bottom of this hierarchy are the so-called "simple" electronic signatures, which only "weakly" identify the author and guarantee the link between the signature and the document.

For example, it will be a login and a password, or the simple acceptance of online terms and conditions. These signatures benefit, logically, from a degraded legal recognition, i.e. they will only be "admissible" in court. In order to be accepted as proof (and be assimilated to a handwritten signature), the judge will still have to be convinced of the "reliability" of the system.

At the top of this hierarchy are the so-called advanced electronic signatures (level 3 in the eIDAS regulation), which involve a trusted third party in the system: a certification authority, which must be accredited by the competent local body. These signatures benefit from a presumption of validity, so that the judge will be able to assimilate them, without any further examination (unless the opposing party seriously contests them) to a handwritten signature.

In practice, these advanced signatures are rarely used because they usually require a face-to-face identification (KYC) for delivery[78]. In addition, blockchains, even if they are based on a cryptographic signature system, do not allow a level 3 signature to be implemented natively[79].

The SURP-SIG ("SIG" for "signature") protocol provides a relevant solution by associating a signatory's native digital identity (SURP-ID) with the SURP-C confidentiality function and the SURP-T traceability function. The result is therefore ipso facto equivalent to the advanced electronic signature of the eIDAS regulation, without recourse to a certification authority[80].

Any SURP process can be signed using the SURP-S function with an effect equivalent to level 3. This is the case for data stored within the framework of SURP-D (a copyright protected work, an archive, etc.), an application using the algorithmic capacity and computing power functions of the IOUR network (see 3.8 and 3.9 *below*). This will be the case for the full content of a videoconference session, which may be signed (as proof of a vote for example).

As for the other SURP services, the signatory will be able to sign in a pseudonymous way, knowing that SURP-T will be able to prove that this signature is linked to the real identity of the SURP-ID.

[78] It is possible to use remote identification by videoconference if the system is approved by competent authorities, but to date, such a system is little used. See for example Esign from IDnow and Docusign: https://www.idnow.io

[79] It is however possible to associate an advanced electronic certificate with a *smart contract* of a blockchain but this function is not native: https://deepai.org/publication/authsc-mind-the-gap-between-web-and-smart-contracts

[80] This will probably require an update of the eIDAS regulation in the long term...

## 8. Algorithmic capability

More and more common activities require significant algorithmic resources: videoconferencing system, *deep learning*[81], online text editors, etc.

These services can be offered natively via the SURP-ALG protocol ("ALG" for "algorithm").

For example, by typing the SURP-A :office command from the browser, the user will activate an *open source* text editor. The file will then be stored, in a decentralized way, via the SURP-D protocol, encrypted if necessary by SURP-C, and traceable by SURP-T.

## 9. Distributed computing

Numerous applications require significant computing power. Examples include medical imaging, 3D animations, scientific calculations, prototyping, and finite element method,[82] among others.

The SURP-X protocol will natively offer computing power associated with an algorithm and a *dataset*.

As an example, a user will be able to classify images by designating a type of algorithm available via SURP-A, associate a collection of images previously loaded on SURP-D, and allocate a calculation resource (SURP-X) that will execute the above-mentioned algorithm.

In our example, the number of images to be classified being large (several million), in order for the processing time to be reasonable (a few hours at most), significant computing power will be required. Currently, such computing power can only be offered by a handful of dominant players.

SURP-X will enable distributed computing, potentially without limitation, and available to all users.

In addition, the protocol will be compatible with the quantum computer, offering humanity unprecedented computing power.

## 10. Digital currencies

Today, each (public) blockchain protocol generates its own native cryptocurrency (and in some cases allows the protocol to create other "tokens")[83].

[81] https://en.wikipedia.org/wiki/Deep_learning
[82] https://fr.m.wikipedia.org/wiki/M%C3%A9thode_des_%C3%A9l%C3%A9ments_finis
[83] There are more than 1500 cryptocurrency registered in the world : https://www.cryptoencyclopedie.com/crypto-monnaies

It is therefore not surprising that one of the major challenges of the blockchain ecosystem is the interoperability of protocols[84].

In addition, governments are beginning to look at blockchain technology to issue "digital central bank currencies" (CBDCs[85]). From the States' point of view, the advantages of these digital currencies are obvious: reduction of the costs of issuing currency, traceability of transactions and real-time control of the economy.

From a user perspective, CBDCs enable the emergence of a means of payment that is both legal[86] and interoperable with "Industry 4.0".

The FIAT currency (euro, dollar) is not "compatible" with decentralized applications (especially financial) and new services such as AI and IoT which, more and more, will be operated via blockchains (examples: the shared autonomous cars of the future, or remote control of a 3D printer).

Of course, the associated risks are equally obvious, especially in terms of invasion of privacy (the Big Brother spectre), and the guarantees provided to citizens will depend on the political systems involved.

For CBDCs, the question of the choice of blockchain is even more acute.

Is it realistic for a central bank to deploy a state currency on a public blockchain, whose governance is not under its control and which could be exposed to the risk (even theoretical) of a "hard fork"?

And even if the central bank in question has chosen a blockchain (proprietary) protocol, how can it ensure interoperability with other CBDCs? The example of China is eloquent in this regard[87].

In this field too, the giants of the Internet are wielding their weapons, as we have seen with the announcement of the Libra stablecoin by Facebook[88].

Therefore, to make the large-scale deployment of digital currencies realistic, central banks will need the following key safeguards:

---

[84] See the report of the European Blockchain Observatory, Scalability, interoperability and sustainability of blockchains, March 2019, https://www.eublockchainforum.eu/reports .

[85] https://en.wikipedia.org/wiki/Central_bank_digital_currency

[86] Bitcoin type cryptocurrency is not a "legal tender" currency, at least in Europe, where only the Euro has this status. From an economic point of view, the debate continues to rage about the real status of Bitcoin-type cryptocurrency. The discussion has become classic. Money fulfills three functions: a means of exchange, a unit of account and a store of value (savings).
We can quibble indefinitely about whether these three criteria are present in the case of Bitcoin (and other global cryptocurrencies). It is true that more and more merchants are accepting Bitcoin (medium and unit of account), but it is also true that the "store of value" function has become predominant. Moreover, cryptocurrencies are subject to speculative movements (notably through exchange platforms), bringing it closer to the nature of a (risky) investment.

[87] S. Haig, China Could Roll Out Its CBDC Without Anyone Realizing, 14 juin 2020, https://cointelegraph.com/news/china-could-roll-out-its-cbdc-without-anyone-realizing

[88] Jonathan J. Attia, Thibault Verbiest, Blockchain, A Four-Time Waltz: Bitcoin, Ethereum, Libra & the CBDCs – The Need for a New Balance, 12/09/2019, , https://www.crowdfundinsider.com/2019/12/154949-blockchain-a-four-time-waltz-bitcoin-ethereum-libra-and-the-cbdcs-the-need-for-new-balance/

1. A universal blockchain, whose protocol has been standardized by a broad consensus of stakeholders, including States,
2. Rational governance, which excludes the hypothesis of a "hard fork", and in which the States participate,
3. A protocol that allows the identification of node operators, and
4. An infrastructure that is not under the control of a State or group of States.

In other words, this blockchain should be operated by all States, in a decentralized manner.

**The SURP-B protocol makes this equation possible in the following ways:**

- The protocol will be *open source* and should be defined by a broad consensus (IETF, W3C, ISO, ITU, central banks).
- In such a governance framework, the risk of a hard fork would be excluded[89].
- In the IOUR proposal, the nodes will be known, and operated by well-identified legal entities.
- As the SURP-B protocol is not based on a consensus mechanism requiring computing power (and therefore leading to node rallies), it can be deployed by all the nodes, individually, without risk of concentration. In addition, the very principle of the IOUR proposal, which is to "merge" TCP/IP and blockchain, naturally favours the deployment of the IOUR network by Internet operators (ISPs, IXPs[90] or their local partners).

[89] In theory, a *hard fork* would not be impossible, but would not be in the interest of any of the stakeholders. Central banks would thus have no interest in ending up with distinct and non-interoperable blockchains, except to make them interoperable, which demonstrates the absurdity of a *hard fork* in this case.
[90] https://fr.wikipedia.org/wiki/Internet_Exchange_Point

**To illustrate the power of the proposal, let's take the example of the creation of a digital bank under the SURP protocol:**

1. When creating its SURP-ID identity, the bank (or Fintech) will have to comply with the conditions imposed by the regulations and justify in particular the required authorizations. The competent regulator, via its own SURP-ID identity, will certify the bank's compliance with the regulations by means of a SURP-S electronic signature.
2. Each new client will be identified by its SURP-ID ("KYC" native).
3. The new bank (or Fintech) will create individual "accounts" for its customers based on its SURP-ID primary identity as a[91] legal entity identified and regulated by the competent authorities.
4. Each SURP-ID is associated with a native *wallet,* which can receive and send CBDCs (or other digital currencies issued by regulated operators using the[92] SURP protocol).
5. All transactions will be recorded (and therefore auditable) on the blockchain via SURP-B.
6. All personal data relating to customers, and shared with the bank, will be stored on SURP-D (with the possibility to define that they will be stored only in Europe) and traced on the SURP-B blockchain to meet compliance obligations.
7. As a result, the scheme is natively compliant not only with the legal anti-money laundering obligations but also with the GDPR (see *infra* 4.1).

In short, the future digital bank will be able to benefit from a natively compliant and interoperable technological infrastructure, allowing it to focus on its core business (the originality of the product and the creation of a community of users).

## 4. Implications of the IOUR proposal

Today, all online services (including blockchains) operate from the top "layer" of the Internet[93].

Simply put, the IOUR proposal presents a suite of protocols (SURPs) that brings these services "down" to the lower layer of the Internet.

Such a proposal has fundamental implications on the Internet's physiognomy. We have already mentioned several of them (notably decentralized governance, interoperability of services, native traceability and confidentiality).

It is impossible to foresee all the consequences of such a proposal if it is implemented on a large scale, just as it has been impossible to anticipate all the evolutions or mutations of any disruptive technologies (internet, blockchain, AI, and more recently quantum computing).

[91] It is possible to use the "HD wallet" technique in this respect: https://www.investopedia.com/terms/h/hd-wallet-hierarchical-deterministic-wallet.asp .
[92] These would be payment service providers within the meaning of PSD2 or electronic money institutions.
[93] Layer 4 and more of the TCP/IP model

Although the exercise is uncertain, we can nevertheless foresee certain fundamental consequences:

## 1. Effective implementation of the GDPR

In the IOUR proposal, the servers (nodes) of the network are identified. They may therefore be qualified, where applicable, as data processors within the meaning of the GDPR, bearing in mind that the data controllers will also be identifiable, via their SURP-ID.

On the (thorny) question of the right to be forgotten, personal data (public keys and other personal data hashed on the blockchain[94]), we propose a radically innovative system of a double level blockchain operated by the SURP-B protocol:

- A "high" level registry, which would be the registry recording all transactions related to IOUR native services.
- A "low" level register which would be the control and traceability register of all modifications made on the high-level register.

Thus, any deletion - by the person authorized and identified by his SURP-ID - of data on the top part (example: a public key linked to a transaction) will be controlled, recorded and traced by the low-level registry. In other words, the SURP-B blockchain "tolerates" the break in cryptographic integrity of the high-level register.

It will therefore be the first "correlated multiple register blockchain" protocol, making it possible to achieve "by design" compliance with the GDPR.

It would also be possible to deploy a *zero knowledge proof* style of blockchain (which encrypts the transaction data) via the SURP-B with an auditability function at the request of the competent authorities (identified again via their SURP-ID), following the example of certain existing protocols[95].

[94] On the question of compatibility between GDPR and blockchain : https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf
[95] For example, BEAM : https://beam.mw/, DUSK: https://dusk.network/ and Zcash: https://z.cash/

## 2. Anonymity, identity and neutrality

Regarding the apparent paradox between anonymity and identity, IOUR creates an "augmented internet" by amplifying both the possibilities of anonymity and of transparency of the network.

Indeed, the user can choose to be anonymous (as well as all the SURP services they would activate) and SURP-T (traceability) will allow them to prove that this anonymization is effective. For example, a user wishes to pay anonymously for the purchase of a consumer good (a legitimate transaction not subject to a legal obligation of identification) in a digital currency.

In this case, the consumer will activate the "anonymization" function in their SURP-ID so that they will appear anonymously in the transaction. The user will then be assured that they have been anonymized thanks to the traceability of this transaction operated by SURP-T. This is a major innovation.

There is also the possibility of making the transaction content confidential at the user's discretion, thanks to the SURP-C function (confidentiality). In fact, the content cannot be discriminated against by the network, and will therefore benefit from effective neutrality in its treatment. In other words, the encrypted content will not be filtered, and thanks to SURP-T it will be possible to prove that there was no filtering.

If the transaction requires reinforced identification (banking operations for example), SURP-T will guarantee the traceability of the transaction with the use of the real identities (verified and official) of the parties involved.

These functions can be combined: anonymization of identities coupled with unencrypted content and vice versa, anonymization and encryption etc.

## 3. The "blockchain of blockchains".

Currently all blockchains operate predominantly in isolation from each other. It is not possible for a user to centralize and trace all their interactions with these different blockchains within the same blockchain[96]. For example, if a person has crypto-assets from different blockchains, they will have to manage as many wallets as crypto-assets.

With the IOUR proposal, the SURP-B blockchain would become the default entry point for other blockchains because of its native TCP-IP character and associated SURP services.

For example, from the wallet associated with the SURP-ID, it will become possible for a user to initiate a transaction on the Bitcoin blockchain, without having to worry about managing

[96] Note that initiatives exist to create interoperability between blockchains, such as the Cosmos, Fusion and Polkadot projects. See: https://news.bitcoin.com/best-defi-interoperability-solutions-exploring-fusion-vs-cosmos-vs-polkadot/

their wallets and while benefiting from the recording and traceability of this transaction, auditable from SURP-B.

## 4. Decentralization to the rescue of digital democracy

Over the last twenty years, the State and its organs have been increasingly required to be transparent. A myriad of laws has been adopted to this effect, both at the national and European levels.

However, there is one area where this transparency is not sufficiently guaranteed: that of the computer processing of citizens' data. There is the GDPR, which is also applicable to public authorities. However, these legal safeguards are insufficient to guarantee, in concrete terms, to citizens that the rule of law is preserved.

We saw it during the Covid-19 crisis, when the debate was raging about the use of a mobile *contact tracing* application launched by governments. The issue was not only to agree on rules of the game (in line with the GDPR) but also, and more fundamentally, to ensure that they were respected by the “responsible” State bodies. The citizen has no means of controlling the State's effective compliance with its commitments, which leads to a trust issue.

With the IOUR proposal, it would become possible to trace (SURP-T), in a certain way, all the processing carried out by the State and its various emanations, identified via their SURP-ID. It would therefore become possible to have a real "right of audit" of "public" data processing by citizens or their representative associations (in addition to the supervisory authorities)[97].

Furthermore, when it comes to digital democracy, the IOUR proposal opens up a vast field of possibilities for many "e-government" applications that are currently controversial (in terms of cybersecurity), such as electronic voting.

## 5. Digital Sovereignty

For the first time, it would become possible to define a digital territory, not only in terms of formal regulations, but also in terms of computer programming.

There is already the system of IP addresses which makes it possible, to a certain extent, to locate a machine connected to the network. However, this technique is insufficient to allow the actual definition of a digital territory. In theory, the sum of IP addresses should make up the territory, but nobody has this information.

[97] In the same vein, see the proposals of the TFC19.tech collective, which advocates the use of a public blockchain to trace and audit the treatments made by the State in the case of a contact tracing application. J. Attia and T. Verbiest, C. Lequesne-Roth, Les dix commandements du contact tracing, L'Echo, April 14, 2020: https://www.lecho.be/dossiers/coronavirus/les-10-commandements-du-contact-tracing/10220409.html

The SURP suite allows authorities to precisely define a digital territory. It's a real paradigm shift. Thus, it becomes possible to define a territory where data (personal or not, sensitive or not) will have to be processed and stored[98].

The applications will obviously be very numerous: implementation of the GDPR[99], hosting of health data, cyber-regulation (e.g. in terms of VAT[100]), outsourcing of critical activities in third countries in the banking sector,[101]etc.

## 6. Diversity of actors

**The IOUR proposal introduces diversity on two levels:**

- At the level of protocol standardization, which will have to involve a set of stakeholders (existing standardization bodies, European Commission, UN, States, central banks, etc.).
- At the level of protocol deployment, which can only be done with the involvement of access providers (ISPs) and new players at the local level. Indeed, the SURP suite assumes:
    - An update of ISP routers
    - Servers operating as nodes (ISNs and SURPs), which may be owned by ISPs or other players (existing *data centers*[102], public blockchain nodes or new companies) wishing to make it a new business, in partnership with ISPs[103]. So a whole ecosystem, both local and global, will have to be set up.

## 7. Sustainable development

Fundamentally, the IOUR proposal creates an ecosystem of decentralized *data centers, which* will reduce overall energy consumption by pooling resources,[104]and increase service availability and therefore the overall resilience of the system.

---

[98] SURP-D (data storage), SURP-T (traceability) and SURP-B (blockchain) protocols will be used.
[99] Data transfer outside the EU. The issue is all the more topical since the annulment (judgment of 16 July 2020) by the Court of Justice of the European Union of the Privacy Shield: https://edps.europa.eu/press-publications/press-news/press-releases/2020/edps-statement-following-court-justice-ruling-case_en
[100] Thanks to the SURP suite, it would be possible to implement and automate the collection of VAT at the source of each electronic transaction (associated with a "CBDC" and another authorized digital currency).
[101] It is currently very difficult for a regulator to monitor compliance with the rules on outsourcing critical banking activities to third countries, which are mostly IT-based, and based on data that may be stored in high-risk countries without the regulator's knowledge. The European Banking Authority's "Guidelines on outsourcing arrangements": https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements .
[102] The current nodes operating the various public block chains could participate in the deployment of the IOUR infrastructure, without giving up their core business.
[103] The ISN and SURP nodes will indeed have to be hardware "colocated" with the Internet infrastructure, i.e. ISPs. In other words, they will be in close proximity to the routers and switches of the ISPs.
[104] An IOUR node can manage several instances of ISN or SURP type.

Mathematical and economic models have shown that a complex system is only sustainable if the right balance is struck between efficiency and resilience.

The well-known example is that of the forest: a "monoculture" forest (of pine wood, for example) will be very "efficient" (profitable) but not very resilient (resistant), because it will be susceptible to disease and fire, whereas a forest composed of a wide variety of trees will be more resistant but less "efficient".

Professor Bernard Lietaer has shown that the same applies to the monetary system[105]. The current system works like a monoculture, it is very efficient (money being created out of nothing) but also very vulnerable. There have been more than 600 monetary crashes since 1970.

The Internet, as a complex system, is no exception to this law. It has become too centralized, in search of efficiency and profitability. It is now controlled by a handful of companies[106]. On the other side of the coin, it has also become too fragile, due to a lack of resilience.

One of the fundamental ingredients of resilience is diversity. In fact, UNESCO has made it one of the founding principles of the Universality of the Internet and sustainable development[107].

The IOUR proposal also contributes to some of the sustainable development goals defined by the United Nations, under the SDG (*sustainable development goals*), in particular goal #9 "Industry, innovation and infrastructure"[108].

[105] Money and Sustainability: The Missing Link / A report from the Club of Rome (avec Christian Arnsperger, Sally Goerner et Stefan Brunnhuber), Triarchy Press Ltd, 30. May 2012,
[106] https://wiki.threefold.io/#/true_decentralized_internet_system?id=curve-of-life-efficiency-vs-resilience

[107] UNESCO has identified four principles as essential to the Universality of the Internet. These are the so-called "D-OA-M" principles. They are fundamental to the development of the Internet in that they must promote the achievement of sustainable development goals. These principles are the following: D - the Internet is based on Human Rights O - it is Open A - it should be Accessible to all, and M - it is powered by the participation of Multiple actors. https://fr.unesco.org/internetuniversality/about

[108] Objective 9: "Investing sustainably in infrastructure and innovation is a key vector for economic growth and development. With more than half of the world's population now living in cities, public transport and renewable energies are becoming increasingly important, as is the growth of new industries and information and communication technologies". See: https://www.undp.org/content/undp/fr/home/sustainable-development-goals/goal-9-industry-innovation-and-infrastructure.html

| Sustainable Development Goals (SDGs) | IOUR Impacts |
|---|---|
| 9 - Industry, innovation and infrastructure | 100% |
| 16 - Peace, justice and effective institutions | 67% |
| 10 - Reduced inequalities | 50% |
| 8 - Decent work and economic growth | 33% |
| 11 - Sustainable Cities and Communities | 30% |
| 12 - Responsible consumption and production | 18% |

## 8. An elegant answer to "fake news".

Fake news[109] is perceived as one of the major wounds of the current Internet. There is no solution offered by the network to combat them except to make the intermediaries of the Internet (social networks etc.) bear the responsibility of filtering them.

This trend is at work (we saw it in particular when Twitter censored President Trump's comments) but it poses a serious problem in terms of compatibility with the principle of neutrality of the Internet and the texts that govern the liability regime of Internet intermediaries.[110]

Here we offer an elegant answer by not filtering the content itself, but by associating a native digital identity and traceability to online content.

Any content could indeed be associated with a SURP-ID and a SURP-T, so that any non-identifiable, non-traceable content would be uncertain content, and therefore subject to doubt.

The "standard" would consist in signing content via SURP-S (based on SURP-ID), making it traceable (SURP-T), where the digital identity offered by the main current social networks is largely insufficient to authenticate content.

In addition, it would also be possible to trace the chronology of propagation of a content to determine with extreme precision the origin of a piece of information.

Concretely, we find all the properties of an advanced electronic signature (level 3) associated with a content broadcast online (regardless of the medium, Twitter, Facebook, LinkedIn, blog, e-mail ...) and immediately verifiable from SURP-T.

[109] Understanding Media and Misinformation in the Digital Age https://mitpress.mit.edu/books/fake-news
[110] Internet intermediaries https://www.coe.int/fr/web/freedom-expression/internet-intermediaries

## 9. The spatial internet

Designed for areas without ADSL or fiber optics, satellite internet allows a two-way connection between a fixed satellite dish (preferably located in a white zone) and a ground station connected to the internet network.

Since the recent and progressive deployment of constellations of satellites in orbit, the question of a space-based Internet infrastructure arises with respect to the terrestrial Internet infrastructure. Indeed, the OneWeb[111], Starlink[112] and Kuiper[113] projects alone represent the deployment of several thousand satellites in orbit over time.

In other words, in addition to offering Internet connectivity to any point on the globe, the terrestrial[114] network infrastructure could be gradually replaced by a space-based infrastructure offering bandwidth equivalent to or even greater than our current infrastructures.

In addition, the Kuiper project, led by Amazon, potentially heralds the emergence of a new kind of *cloud*: a "spatial cloud" offering computing resources in orbit for Internet users on Earth and in space (from the Moon, for example). From then on, everything needs to be rethought, both technologically and in terms of space law.

The IOUR approach will adapt to the evolution of the space internet by proposing, like colocation for terrestrial operators, an integration of ISN and SURP nodes in the satellite payload: IOUR services will thus be directly addressable from space communication protocols and natively interoperable with the terrestrial network infrastructure.

## Conclusion

The IOUR proposal is ambitious. It proposes a model of unification, by bringing together not only technologies, but also people.

It embodies the values of universality, sharing and collective responsibility.

It will only become a reality through the involvement of all stakeholders, in the spirit of the multi-stakeholder governance and co-regulation model advocated by the European institutions[115].

---

[111] https://www.oneweb.world/

[112] https://www.starlink.com/

[113] The U.S. authorities have authorized Amazon to deploy and operate 3,236 satellites that will form a constellation dedicated to broadband Internet. Called Kuiper, this project aims to provide Internet coverage to the greatest number of people. See https://blog.aboutamazon.com/company-news/amazon-receives-fcc-approval-for-project-kuiper-satellite-constellation

[114] https://global-internet-map-2018.telegeography.com/

[115] Under a co-regulation model, the European Union defines legislative standards that are then implemented by the private sector. It thus reflects new governance features. These include (i) participation and power sharing, because power is not monopolized but shared; (ii) a preference for diversity and decentralization, because the impossibility of uniform regulation is recognized; and (iii) multi-stakeholder deliberation, because the European Union cannot effectively regulate in isolation. See the own-initiative opinion of the European

It is not a question of fighting anyone, but of enabling the transition to a new stage in the development of a more open, resilient and pluraldigital society[116].

Powerful organizations, States, innovative companies, users; everyone will be able to find their place.

It is to support this proposal that we created the "IOUR Foundation[117]", with a group of experts, including Louis Pouzin, one of the fathers of the Internet[118].

Its main objectives will be to initiate the technical proposal of IOUR, to sensitize and mobilize the various stakeholders around this suite of protocols.

The Foundation will file patents, which will be available in *open source* or in Frand[119]mode, in order to protect the innovation against attempts to appropriate it, which would slow down its development.

This white paper is only the beginning of a series of publications dedicated to the IOUR proposal and its various services.

**Jonathan. J. Attia**, Associate Researcher, Executive Vice President IOUR Foundation - jonathan@iour.org

**Thibault Verbiest**, Attorney at the Paris and Brussels Bars (Yellaw) and President of the IOUR Foundation - thibault@iour.org

Economic and Social Committee "Self- and co-regulation in the legislative framework of the European Union", 22 April 2015, OJ C 291, 04.09.2015, p. 29: https://www.eesc.europa.eu/fr/our-work/opinions-information-reports/opinions/autoregulation-et-coregulation
https://www.eesc.europa.eu/resources/docs/auto_coregulation_fr--2.pdf

[116] We are in phase with other projects or initiatives that share the same objective. For example: "Web Futures: Inclusive, Intelligent, Sustainable The 2020 Manifesto for Web Science" https://www.webscience.org/wp-content/uploads/sites/117/2020/07/main.pdf; FreeFlow Nation: https://www.freeflownation.org/

[117] . The Foundation was recognized on September 13, 2020 by the King of the Belgians as a foundation of public utility.

[118] Louis Pouzin is also a supporter of the RINA protocol and creator of Open-Root: https://www.open-root.eu/.

[119] https://en.wikipedia.org/wiki/Reasonable_and_non-discriminatory_licensing