POST PLATFORMS FOUNDATION

postplatforms.org

Whitepaper

The Technology of Web 3.0 Data Space

Author: Alex Tourski, alex.tourski@postplatforms.org

v3

1 Jan 2024

Public link (read only):
https://izi.synology.me:792/d/s/wMkgrqx5qCTXE54ecrepzeVFZW8T7S63/cIF3lm8sjtdSWr2GlclC5NhcEBd6QCFl-lbUg83_c9wo

Please contact the author if you would like to comment on this text and see others' comments.

Table of Content

Security Audit

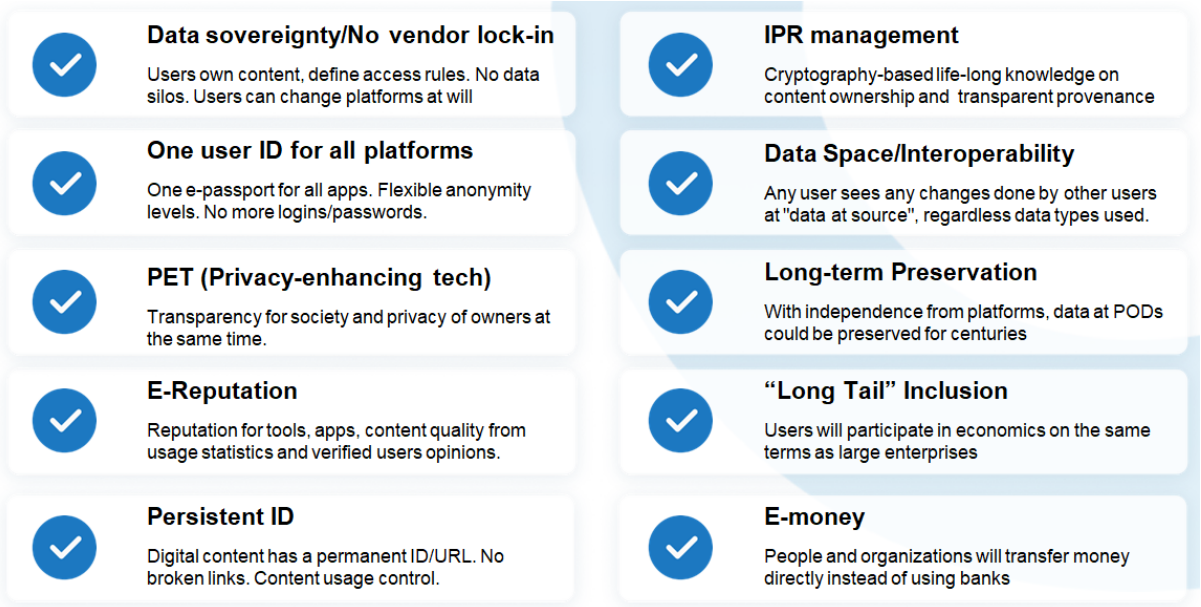
Insurance

Legal support/prosecution

Acceptance of e-Reputation

Executive Summary

This document offers a comprehensive description of the Web 3.0 Data Space, a very specific architecture for solving most of problems of modern Internet and platforms: monopoly of platforms, data ownership, IPR control, long-term preservation etc.
A number of leading projects have been working on this problem for a decade (European Data Space, IDSA, Solid, Gaia-X, MyData and many others), but so far none of them have achieved tangible results or presented a sustainable/scalable architecture and solution.
We have to admit that even articulation of a clear definition of the Data Space is a challenge for most of those projects. Given this unclear situation, we decided to start the whitepaper by defining what is a Data Space. The best way to do this was to create a series of business cases that would describe the main problem areas common to all industries. This is done in section Challenges and Biz-cases of the document. We have defined the following blocks (this list is not complete):

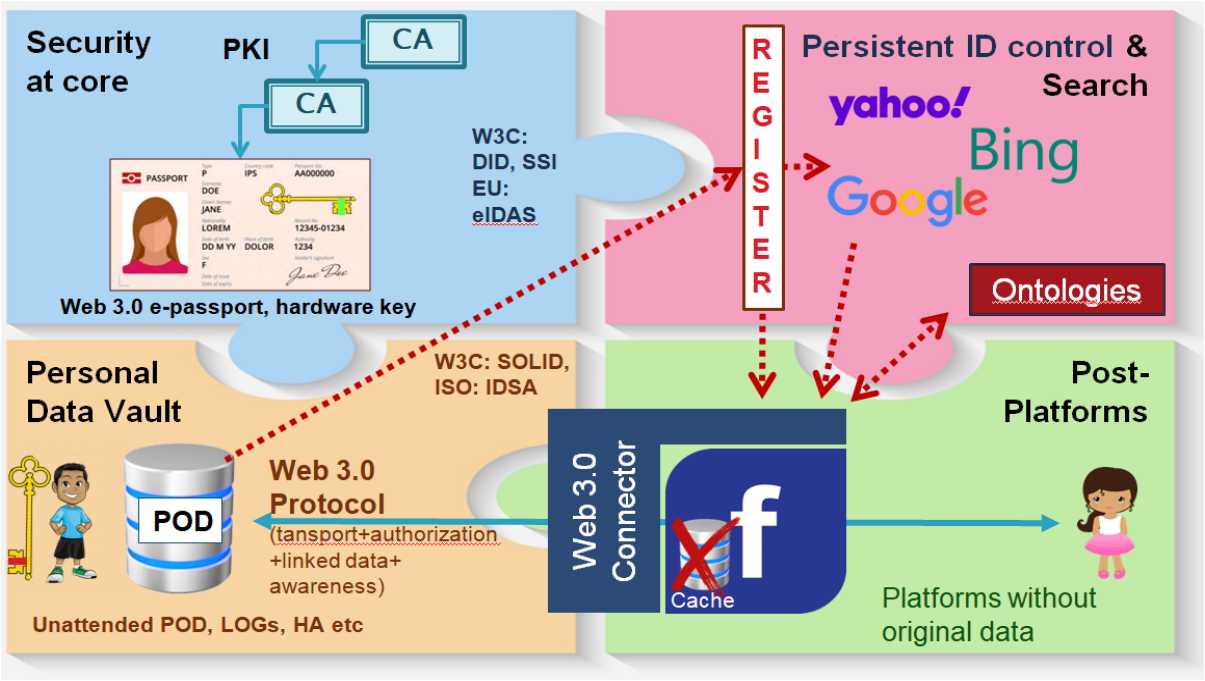


In each of these blocks we offered several specific biz-cases from different domains. Biz-cases are high-level functional business requirements. E.g., museums may ask for "*Long-term preservation for centuries for all data*", railways demand "*Passengers can get a multi-modal route with ANY app of their choice*", governments need "*Peoples' spending data without violating privacy*" and citizens need "*Simple yet secure e-voting*" and "*One e-passport to get all services*". Biz-cases will be the starting point for any architecture and technical discussion.
We decided to start from biz-cases as we see a number of initiatives which discuss protocols and even standards without any attempt to answer simple WHY questions at the business level.
We discussed it with many reps of Solid and IDSA communities, and we got initial support for this approach. Also, biz-cases will allow us to avoid direct confrontation in the discussion on "which protocol is better". We suggest that first we agree on the biz-cases and then the protocol requirements and implementation will follow. This is the most natural way to develop any technology.
We propose the Data Space community (united within the IDSA project) to develop the biz-cases further in the process of discussion with specific industries.
Thus, a set of such biz-cases defines the ***Data Space landscape*** and ***is*** the definition of Data Space.
With the biz-case landscape ready, we invite any project, from blockchain to Mastodon, from Solid to MyData, to review it and indicate which of these biz-cases it can solve. This will allow us to see

all projects on one common “Data Space map”. This solves a major problem for customers – from enterprises to governments – who simply don't understand, e.g. “whether MyData is better than DSNP?”. Biz-cases will be a simple tool for comparing Data Space architectures and developing common standards and approaches.
Further in this whitepaper we describe the specific approach and architecture of the Web 3.0 Data Space, proposed by the Post-Platforms Foundation. The Web 3.0 Data Space is a further development of the concepts promoted by the Solid and IDS projects.
For the convenience of the reader, we have divided the document into 3 blocks, which we call Levels. There are 3 of them. Each of them describes the same Web 3.0 Data Space ecosystem, but does so at an increasingly deeper level:
Level 1. Here we introduce the concept of Web 3.0 Data Space at the highest level, define the terms of ***Web 3.0*** and ***Data Space*** separately, and briefly introduce the landscape of projects around Data Space with clear positioning of our Post-Platforms Foundation among them.
Here we present the core idea of the Web 3.0 Data Space project: the separation of data and platforms, which leads to effective resolution of all biz-cases presented above.
The Level 1 is intended for C-level managers working on strategic solutions in data management.
Level 2. Here we discuss the basic principles of the ecosystem design and conduct an in-depth analysis of the organizational innovations which are crucial for this project. At this level we discuss step-by-step the Web 3.0 Data Space-based solutions for all the challenges and biz-cases presented at the beginning of the document. Then we reflect on the essence of the new Internet and the role of Web 3.0 Data Space in the development of the AI. Indeed, instead of being a media to transfer data, with Web 3.0 Data Space the Internet will become a media to access everything in this world (from people to companies and things) and to store data safely for centuries. We also will discuss the governance of Web 3.0 Data Space, which is mostly based on the Web 1.0 governance (with institutions like ICANN and W3C) and typical industry associations. It will allow to keep Internet independent from governments and corporations, decentralized and human-centric. Finally, we discuss possible commercial and non-commercial ways of launching Web 3.0 Data Space in several domains.
This level is intended for product managers and Analysts
Level 3. Here we analyse the architecture of the Web 3.0 Data Space, possible technological problems and solutions. We start with a 4-part architecture, which is based on:

- Secure PODs for citizens, corporations and things (IoT)
- Platforms which become post-platforms after agreeing to keep data on PODs
- The Register which combines the role of former DNS, with extra tasks like managing Persistent IDs. Search engines here help platforms to find PODs and data.
- Advanced security and e-Passport (key management) sub-system, based on PKI.

This picture provides a high level view on the architecture of Web 3.0 Data Space. Please refer to Level 3 for details.



Then we demonstrate how all these elements help to deliver all biz-cases described in the beginning of the document.
This level is intended for product managers and architects.
Please refer to our web site postplatforms.org and Post-Platforms youtube channel for more information on the Post-Platforms Foundation and its Web 3.0 Data Space project

Definitions

POD - Personal Online Datastore. A universal storage of data, similar (yet more advanced) to a Web site. Introduced by Tim Berners-Lee within the Solid project
Platform - Any information system which serves numerous users online and keeps their data inside. Examples: Facebook, SAP, Uber.
Post-platform - any former Web 2.0 platform which joins the ecosystem of Web 3.0 Data Space, learns how to keep data at PODs, adopts use of security mechanisms of Web 3.0 Data Space etc.
PET - privacy enhancing technologies, which allow to get statistically reliable data without exposing the IDs and actual data of data owners. E.g. e-Voting
E-Voting - a reliable on-line voting which guarantees privacy and security, free and open, as part of Web 3.0 Data Space
E-Money - a money transferring and money-keeping service which can totally replace the current banks and e-banks, free and open, as part of Web 3.0 Data Space.
E-Reputation – the reputation of a person, certain digital assets, IoT, a post-platform, calculated by specialized e-Reputation post-platforms on the input from all reactions (likes, comments etc) left by users, used the assets or post-platforms at question. Most probably e-Reputation will depend on context and will be a vector.
Private key - a private cryptographic asymmetric key. In Web 3.0 Data Space it is always stored at the specialized hardware, so-called crypto-engine, which could be based on the SIM card (MobileID), USB fob or inside a smartphone.
Public key - is derived from the private key. It is a one-way function, therefore it is impossible to derive a private key from the public key
PKI - Public Key Infrastructure, an infrastructure of notaries (CA - certificate authorities) who issue e-Passports.

IoT - Internet of Things.
ACL - Access Control List, a set of data which defines who and how can access and change certain assets.
Web 3.0 Data Space - the ultimate ecosystem which will address all the modern challenges with data and Internet.
Web 3.0 Protocol - Either Solid protocol or IDSA Protocol or similar protocol which connects post-platforms and PODs. See section Web 3.0 Protocol to access POD
Web 3.0 e-Passport – the Verifiable Credential (private key + certificate, which links the ID of the user with the user's open key), used within Web 3.0 Data Space, based on Persistent IDs. Most probably meets eiDAS (CEN) and VC & DID (W3C) standards.
NB! It is totally different from Web ID, currently used in Solid.
Web 3.0 Connector - (former Solid Adapter) a module which helps any platform to get connected to the Web 3.0 Data Space and become a post-platform without much efforts.
Persistent ID – the identifier, a long number which identifies the object globally. For the avoidance of doubts, it does not bear any authentication functionality. It is a long number like 7436503242457345736452 (actually, its range is unlimited). It is totally independent from any platform or service. It will be created and distributed via the Register. The object could be located by any post-platform at a URL like e.g. Web3://7436503242457345736452 via the Register.
Authorship – the result of establishing the original creator of a digital asset. In the context of this document: it is not enough just to sign the asset (everyone can do it), we need to establish who was the FIRST (e.g. with the timestamp service)
Provenance – the result of establishing the origin, history and changes made to an object. It is based on the Authorship and then tracks down all transactions when the object changed hands.
IPR – a set of rights, defined by the current owner, about copyright (e.g. the right to commercially exploit a work), and rights that can be transferred or licensed, and about moral rights that cannot be transferred.
Organizational Innovation – a special type of innovation which usually follows a technical one, and required in very large systems and projects. It is about finding new ways of doing business instead of technical contraptions, protocols and new technologies. Examples: PPP (public-private partnerships) in infrastructure projects, which limits corruption in infrastructure projects, or introduction of containers in transport industry.

Introduction

This document represents at the TRL Level 2 the current version of the Web 3.0 Data Space architecture and technologies, starting from the definition of challenges and biz-cases which define the nature of the Data Space. We will also briefly cover strategies of the ecosystem deployment, social impact, etc. As the whole community is evolving its understanding of the Web 3.0 Data Space with every step it makes, this document is a work-in-progress and we apologize in advance for any inaccuracies or inconsistencies that may arise with time.

The structure of this document

We begin this document with the definition of Data Space, which in our case is a rather difficult task, as over the past 10 years none of the projects that deal with this topic have been able to deliver a clear definition, including the European Commission, which launched the European Data Space program and allocated a billion euros to it.
Since it is quite difficult to define Data Space, we will start by defining the Challenges of the modern world and defining the biz-cases that describe the desired future (in the section Challenges and Biz-

cases). This set of biz-cases can be considered our initial “definition” of the problem.
When the problem defined, we dive into the solution in three levels, taking a gradual dive into the Web 3.0 Data Space, from (1) the general concept, through (2) analysis, to (3) the architectural level:
Level 1. Here we introduce the concept of Web 3.0 Data Space at the highest level, define the terms ***Web 3.0*** and ***Data Space*** separately, and briefly introduce the landscape of projects around Data Space.
Level intended for strategic managers
Level 2. Here we discuss the basic principles of system design and conduct an in-depth analysis of the organizational innovations which are crucial for this project. At this level we discuss step-by-step the solutions for all the challenges presented at the beginning of the document. Then we reflect on the essence of the new Internet and the role of Web 3.0 Data Space in the development of AI. At the end we will discuss the problems of governance and launching Web 3.0 Data Space.
This level is intended for strategic and product managers
Level 3. Here we analyse the architecture of Web 3.0 Data Space, possible technological problems and solutions.
This level is intended for product managers and architects.

Challenges and Biz-cases

For about 10 years already we have been observing a number of initiatives in the field of Data Space, from IDS and blockchain to Solid and MyData. We'll talk briefly about them below, in the Data Space projects Strategic Landscape section.
Yet, despite so many initiatives and substantial funding, after a decade of development, we not only do not have any working ecosystem, but not even a clear definition of what we are building here. Moreover, we don't even have the exact name of this ecosystem. What is it? New Internet? Web 3.0 (or Web3)? Data Space? Metaverse? There is no established name. A good candidate is the ***Data Space***, suggested by the EC. Yet, neither EC nor projects that explicitly state that they have been building Data Space provide a clear definition for this Data Space.
In our Post-Platforms team we do have both the term and the definition (see Level 1. The Solution: Web 3.0 Data Space), yet, before we discuss our approach, it would be better to discuss here the problems, challenges and reasons WHY do we need any Data Space at all.
Therefore we decided to structure this chapter in the following way:

- We will list some of the major challenges of the modern world, which potentially could be addressed by the Data Space.
- For every challenge
  - we will very briefly state its current state-of-art
  - we will present (in grey boxes) so-called "biz-cases", that represent in a concise way demands from certain stakeholders.

Later on, in the section Level 2. Web 3.0 Data Space Analysis we will address exactly the same set of challenges with the clear explanations on how exactly our concept of Web 3.0 Data Space resolves them. But we specifically delayed presentation of our solution till the chapter Level 2. This split between challenges in one chapter and solutions in another allows us to discuss with other projects (mostly IDSA and Solid) different approaches to Data Space:

- firstly, we would like all stakeholders to agree on the challenges and biz-cases (without any discussions on technologies);
- then we can discuss particular solutions, architecture and technologies which meet the demands of the biz-cases.

The main reason for choosing this 2-step approach is: we found that most of the discussions on particular protocols (like Solid or IDSA Protocol) and specific solutions on the market are too technical and missing the biz-cases step and the WHY questions, including a clear definition of Data Space. As a result they are trying to develop a solution without defining the problem.
This section resolves this omission.
We will spend significant efforts in this section in definition of the Problem, and biz-cases are very instrumental here.
Speaking about biz-cases we would like to state that the biz-cases you see here are exemplary and in no way they do not pretend to be complete. Yet, there are enough of them to provide a holistic view on every challenge. If you (or we) find some sets of biz-cases incomplete, please inform us and together we will fill in gap.
A special note on the wide range of challenges, presented below.
When you read the list of challenges below, you may be surprised by their broad scope, and you may think that it is impossible to create a Data Space technology that covers all these problems. However, we would like to assure you that this document contains only those challenges that are solved by the Web 3.0 Data Space architecture, presented in Layers 2 and 3 of this document. Even more: the whole variety of biz-cases is addressed with the only one silver bullet at origin: we separated data from platforms, as discussed in Level 1 below.

Now, please find below our list of Challenges:

Data Silos

Nowadays users' personal data is scattered in many copies across many platforms, with no control over it, with no trace of the original. Every platform considers their copy of our data as "my precious" value to keep their monopoly and they actively avoid/oppose sharing it.
At the same time, large corporations have hundreds of platforms in use and suffer from data silos issue and version control of numerous copies at every platform even more than individuals. And these numbers grow with every new platform introduced.
The whole Internet, public, and corporations all suffocate under the massive data silos with "rotten" data.

Biz-case 1:
As a user I would like that any element of my information - photo, text, my address etc – exists in one – and the original – copy. And whoever I allow to use it will use only this copy
Biz-case 2:
As a corporate CTO I would like to keep all my corporate data in one – and the original – copy. All platforms in our company should operate with these originals

We address this challenge and the biz-cases in the Level 2 section when discussing the Data @ Source principle and in the No Data Silos subsection.

Data Sovereignty

Currently users and companies have little control over their data which they upload to platforms. Even when these platforms illegally sell/use it, we cannot know it. We hardly can even get a copy of it our of platforms (e.g. Facebook), even though GDPR demands it explicitly.

Biz-case 1:
As a user, I would like to own all my data and control who, how and on what conditions (including price) access it via any platform
Biz-case 2:
As a patient I would like to keep all my medical data in one place and keep control (or even sell to big pharma) over the usage of my data by hospitals and researchers
Biz-case 3:
As a company, I would like to share certain data with partners, suppliers and clients, yet I would totally control who exactly has certain access, and the usage of my data

We address this challenge and the biz-cases in the Level 2 section below, subsection Data Sovereignty

Monopoly of Platforms

Platforms quickly monopolize their market niches. Citizens and companies suffer from vendor lock-in effect. We get a lot for free with platforms simply because we became product ourselves.

Biz-case 1:
As a user I would like not to depend on monopoly of any platform. E.g. if I prefer Facebook to post my photo, I want "my friends" who use LinkedIn or Instagram be able to see and comment on it. I also would like to define the group "my friends" independent from any platform.
Biz-case 2:
As a corporate CTO I would like not to depend on vendor lock-in. I would like to be able to change platforms overnight or even use several simultaneously if I find them complementary in their functionality.

Biz-case 3:
As a professional, I would like to use the tools I'm used to, not those suggested by my employer. For example, if I work professionally with SAP, I don't want to switch to Oracle, which is used in my new company.
Biz-case 4:
As a new platform on the market, I would like to immediately access all potential users just like the leading platforms. I also would like not to manage user IDs and profiles.
We address this challenge and the biz-cases in the Level 2 section below, when discussing the Competition instead of Monopoly principle and in the Eliminating Monopoly of platforms subsection.

Advanced Security

Security is a concern since the invention of Internet because the Internet itself (as TCP/IP), email, Web, FTP, and many other systems were designed without any security in mind. Yet later on we tried to add security to all of them, without (in case of IPSec or email/PGP) or with partial (in case of SSL for Web, which works halfway only) success only. We got used to insecure internet and to hundreds of logins and passwords, but this is far, far away from the “normal”. It’s time to change this approach and put the security at the core of the Data Space.
Biz-case 1:
As a user, I would like to have a secure environment, where I do not have to worry about any threats, and I am always supported by numerous security services.
Biz-case 2:
As a corporate CTO, I would like to have a military grade security environment for all my corporate data, with proper logs, audit and traceability of what, who, when, how and why questions answered. I do not want to depend on proprietary security of specific platforms on that.
We address this challenge and the biz-cases in the Level 2 section below, subsection Advanced Security, and in the Level 3, subsection Security.

Strong identity management

As we are creating a new profile/account with every new platform, we ended up with hundreds of logins/passwords. It doesn’t make our access to services truly secure and convenient. Most people suffer from it, forgetting passwords. Some of them use one password for many systems, which is a serious issue, etc etc.
This whole situation with huge mass of logins and passwords is not normal at all, and millions of people would be surprised to learn that we could have one e-Passport for all services, from logging into platforms to opening a hotel room or renting a scooter.
Yet, instead of addressing the core issue, all current solutions assume that hundreds passwords is a normal situation, and our browsers and phones suggest to save these passwords inside. Or, systems like Facebook or Google suggest their own “passport” (Single Sign-On) which will allow them to trace our every move wherever we go. While it partially mitigates the problem, these solutions violate user's privacy and ultimately make us depend even more on platforms.
Biz-case 1:
As a user, I would like to use one e-Passport for all transactions, access to all platforms and services, getting money from ATM, unlock the office doors, access to rental cars, hotel rooms, voting for president etc.
Biz-case 2:
As a user I would like to control the level of anonymity for every transaction. E.g. I would like to use my real name when buying a house, my (protected) pen name for an article, no name when I buy anything in a shop. Yet, when I buy wine, I would like to share the info with the shop that I am above

21.

Biz-case 3:
As a user, when I lost my e-Passport, I would like to get a new one, just like I get a new bank card (and block my previous e-Passport)

Biz-case 4:
As a bank CEO, I would like to introduce a new service, “issuing e-Passports”, leveraging our vast network of offices.

Biz-case 5:
As a mobile operator CEO, I would like to sell Mobile ID (crypto engine on a SIM card), which we have invented but have not found the use yet.

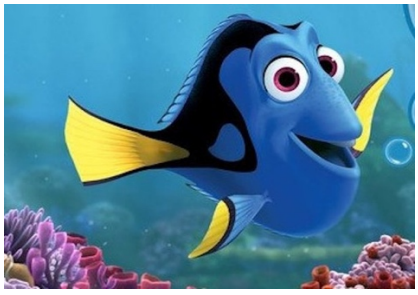
Biz-case 6:
As a Web shop CEO, I would like to avoid managing identities and profiles of my clients, and I would prefer to share them with other (competing) Web shops.

We address this challenge and the biz-cases in the Level 2 section below, subsection Strong identity management (e-Passports & e-Keys), and in the Level 3, subsection Key management is at the foundation of security.

Long-term preservation

Few people can find 20-years old photos, as most of it gone with “one of those HDD crashes”. Nowadays we keep stuff on platforms, yet we lose data every time a platform is gone. Indeed, life expectations of any platform is within 20-40 years (who remembers Yahoo who once had a world like Google now?). We have serious doubts that personal, corporate and government data will survive more than 50 years in the world of platforms (Web 2.0). If we continue to store our data like this, then in 5000 years our descendants will still be finding records of ancient Egypt, but little will remain of our digital-savvy civilization.

Indeed, the humanity as a whole now looks more like a Dory fish from the “Finding Nemo”



Biz-case 1:
As a user I would like to be assured that any data I put via any platform will be stored for a 100 years and more, without any efforts from my side. I would like to see Internet as a safe place to keep data forever.

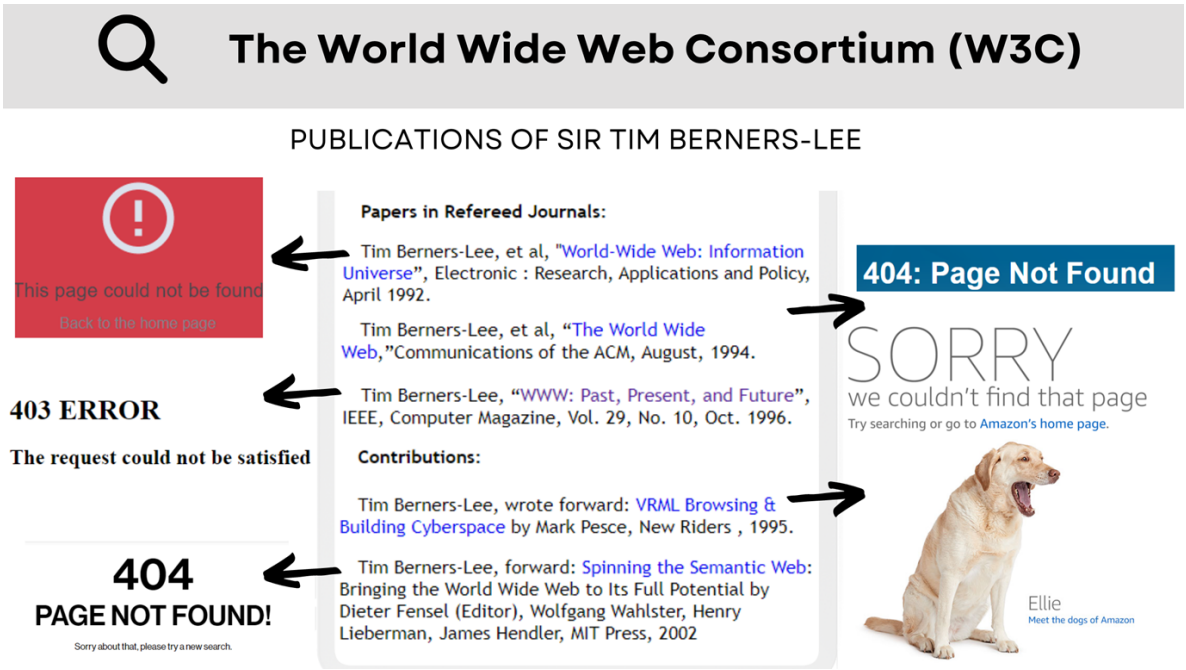
Biz-case 2:
As a museum curator I would like to be assured that any digital data I upload to my professional platforms will stay for 500+ years, far beyond the life expectations of these platforms, and the museum will still work and maintain this data. I would like it to be done automatically, as I am not a specialist in long-term preservation.

Biz-case 3:
As a platform I would like to assure the user that he data will be stored forever if she upload this data to my platform.

We address this challenge and the biz-cases in the Level 2 section below, subsection Long-term preservation of all our data

Persistent IDs (no broken links)

If you try to open any old article or link to a photo older than 20 years, most likely you will end up with a broken link, like demonstrated below on the examples of articles written by Sir Tim Berners-Lee, the father of Web 1.0, Linked Data and Web 3.0 Data Space. Yet, unfortunately, we perceive this issue as a natural state-of-the-art. But there is nothing natural about this: links to the digital assets are an important part of our knowledge network, and loosing them is like loosing the data itself. We definitely need Persistent IDs that are much more versatile and reliable than the well-known DOI system, and free. Digital Assets with Persistent ID will be reachable even if the owner of the assets moved them many times to other locations. We also assume (see above) that the data itself will be safe for centuries, otherwise it does not make sense to require longevity of IDs.



Biz-case 1:
As a creator, I would like my asset (doc, photo) to get (or even generate) an ID which allows to find it centuries later, even if it changed hosting many times.

Biz-case 2:
As a word processor, I would like to get a Persistent ID for a new document for free (or very reasonable price) any time the user clicks File/New command.

Biz-case 3:
As an owner of a digital asset, I would like to be assured that my asset ID is unique and no one else used (or will use) it for another asset, a person or a company.

Biz-case 4:
As a book writer I would like to insert the link to a document into my book, expecting it to be available and resolvable for centuries.

Biz-case 5:
As an owner of a digital asset I would like to know full statistics of its usage via any platform for the last century, as well as the amount of links to it from any type of media.

We address this challenge and the biz-cases in the Level 2 section below, subsection Persistent IDs (no broken links)

IoT (Internet of Things)

The current landscape of IoT is rather balkanized: every equipment manufacture provides its own platform/system to control its equipment. It results in companies having hundreds of systems to control hundreds of types of equipment.

Biz-case 1:
As a company which has different types of equipment, I would like to use one Digital Twin platform which simulates/controls all machinery as one system.

Biz-case 2:
As a construction company I would like all my partners (service company, insurance, suppliers of materials and all other affected) to be aware when my bulldozer fails and be able to act accordingly, even if they use their own platforms and systems.

We address this challenge and the biz-cases in the Level 2 section below, subsection IoT.

e-Reputation

We already see how the reputation mechanism works on platforms through reactions (e.g. likes of different kinds), ratings and reviews. E.g. we check a reputation of a hotel at booking.com before taking it. Yet such reputation stays with certain platforms and we cannot carry it with you when migrating to another one.

We can consider reputation as a special type of data, a very important one. If so, just like with data, we require sovereignty of our reputation.

Biz-case 1:
As a user, I would like to develop and maintain my e-Reputation from numerous likes and feedback I get from users of all platforms I used. I would like to keep it in one place under my full control.

Biz-case 2:
As a user, I would like to maintain e-Reputation for my documents, works (e.g. academic papers), products in similar way to help me sell and promote them at any platform.

Biz-case 3:
As a bank I would like to know the reputation of my client (KYC) without knowing any details about her personal life, as long as my client allows me.

Biz-case 4:
As a professional e-Reputation service (e.g. Michelin) I would like to calculate e-Reputation for any clients.

Biz-case 5:
As a user, I would like to have a choice of e-Reputation calculation services, so that I could chose those with the best e-Reputation of their own. For example, I would like to use a service that can identify and counteract collective bullying or cancel culture, and punish those who organize and participate in collective bullying by lowering their e-Reputation.

Biz-case 6:
As a mobile user who often lives in different countries, I would like to carry on my reputation across state and cultural borders so that in a every new country or city I would not have to prove to citizens, businesses and officials that I am a good citizen with a good e-Reputation.

We address this challenge and the biz-cases in the Level 2 section when discussing the Trust principle and in the Trust & e-Reputation subsection.

IPR and provenance

Private property is a backbone real-world institution, and it is surprising how long we have tolerated the lack of a reliable IPR mechanism on the Internet. Indeed, currently we do not have convenient and reliable mechanisms to prove the authorship of digital assets, as well as tools to track assets changing hands (Provenance). Systems like NFP are more indicator of high social need than

solution, as in reality it does not work and has significant security issues.

Biz-case 1:
As a photographer, I would like to claim Authorship for the photo I took, using my (the only) e-Passport.

Biz-case 2:
As a Canon camera product manager, I would like the camera to claim the authorship for the photographer at the moment the shutter runs. The photographer should be able to disable this feature when camera is lost or not in use.

Biz-case 3:
As an Adobe Photoshop product manager, I would like the Photoshop App to provide a button to claim the authorship for the photographer when the picture is ready.

Biz-case 4:
As a owner of a digital asset (e.g. photo), I would like to sell my rights in such a way that this deal becomes a part of the official provenance.

Biz-case 5:
As a owner of a digital asset (e.g. photo), I would like to set up the IPR (rights to use the asset, incl commercial use) and the shares of ownership, if there are several owners, in such a way that from this moment the co-owners can set up their own IPR scheme.

Biz-case 6:
As a user, I would like to be able to claim ownership to XV century painting exhibited in a museum, and I would like such claim to be visible to anyone who deals with this painting or checks its provenance.

Biz-case 7:
As a user, I would like to easily check the provenance of any digital asset with any IPR platform of my choice and see (a) the chain of provenance, (b) the author, (c) all claims attached to it and other relevant information .

We address this challenge and the biz-cases in the Level 2 section below, subsection IPR and Provenance

Data interoperability

We know that there are many different data formats, structures and ontologies in this world, created and maintained by millions of different platforms. Yet we do not see many systems understanding each other. Interoperability is a holy grail in the data science.

Biz-case 1:
As a user (even if I am a corporate CTO), I do not want to be troubled with data structure, format or ontology issues. I just want to deal with information in a convenient way, via any platform. Yet, as discussed above, I cannot afford many data silos, therefore I expect all these platforms to deal with ONE and original copy of my data.

Biz-case 2:
As a platform I would like to understand the data created and maintained by another platform. From my side, when writing down data to the ORIGINAL I am ready to make efforts to explain my data structures and ontologies for other platforms to interpret it well, otherwise I will lose competition.

Biz-case 3:
As a user I would like to use data from different industries without any hurdles. In this context I need One Data Space, not many domain-specific Data Spaces.

We address this challenge and the biz-cases in the Level 2 section below, subsection Data interoperability, and the Level 3 section, subsection Providing Interoperability of Data Types & Structures.

Privacy protection with PET

On the one hand, society, scientists, and the state need to know basic social statistics (for example, how many people have bought diesel cars last year). On the other hand, people would not want their names to be visible in these statistics.
Theoretically, this challenge could be addressed with help of new area of cryptography, called PET, privacy enhancing technologies.

Biz-case 1:
As a user I understand the need for researchers, governments and other actors to get statistics which includes my personal data. I do not mind them to get it as long as my identity could be totally hidden on my request. Yet, I would like to be able to explicitly provide my consent.

Biz-case 2:
As a researcher I would like to receive statistics based on the actions and purchases of millions of citizens. At the same time, on the one hand, I don't need their names, on the other hand, I want to receive related statistics when I know that this car was bought by the same person who graduated from a specific university and likes to read Jack London.

We address this challenge and the biz-cases in the Level 2 section below, subsection PET (privacy enhancing technologies)

Inclusion and empowerment for people and SMEs

Every person has many capacities. But the modern world offers him/her only one job, 8 hours a day. The reason is the dominance of companies that have resources, reputation, and markets, and they use people as elements of their businesses. The well-being of companies depends on their brand and reputation. People do not have such protection mechanisms and lose competition to companies. It's a clear lack of economical inclusion.

Biz-case 1:
As a legal professional who left a large law firm I would like to work as one-person-company and build up my own reputation based on fair opinion of my clients. At the same time I would like my clients to be able to provide anonymized ratings, yet their own e-Reputation should be included pro-rata into such a feedback.

Biz-case 2:
As a solo repair specialist, I would like all search systems used by people in search for home repair services to list my name together with my cumulative and fair e-Reputation, so that I do not have to spend funds on advertising. I would like to compete with large home repair firms with established reputation.

We address this challenge and the biz-cases in the Level 2 section below, subsection Economic Inclusion

Eliminating fakes

Fake news divide societies and lead to wars (like the one we have in Ukraine). Fake data harms businesses. Fake parts ruin the reputation of brands. Fakes causes significant costs for society. We would like to change it.

Biz-case 1:
As a news agency (e.g. BBC) I would like to know the full origin (provenance) of every particular news as well as the reputation of the author of the news in order to make a decision on putting it to the air.

Biz-case 2:

As a jet engine maker I would like to know whenever my engine gets fake parts installed (e.g. the fan blade) at the service anywhere around the globe.

We address this challenge and the biz-cases in the Level 2 section below, subsection Eliminating fakes

e-Money

Transferring money through banks is no longer convenient. Too many troubles with KYC checks, with opening accounts in banks etc. Cryptocurrency turned out to be expensive, risky, unstable and not very secure, failing to deliver its promise. Central banks are considering e-Money which go directly via central banks (skipping private banks). Yet, it raises issues with big brother control.

Biz-case 1:
As a user, I would like to have ability to transfer/receive money instantly and for free between me and other people or organizations directly, without use of any (central) bank accounts

Biz-case 2:
As a tax authority, I would like to get taxes controlled and paid, based on all such transactions.

Biz-case 3:
As a citizen, I do not mind paying taxes, but I do not want tax office to know what items I buy in online shops.

Biz-case 4:
As police, I would like to be sure that no illegal transactions are done (e.g. drugs or weapon sales). We need to see related invoices and even contracts and emails, when needed.

Biz-case 5:
As a citizen, I would like to be able to prove that I do not have illegal transactions without disclosing any extra private information

We address this challenge and the biz-cases in the Level 2 section below, subsection e-Money

Reducing Bureaucracy

Bureaucracy is not only expensive for society, it creates many problems and complications.
5000 years ago governments created a large strata of bureaucrats who register deals, houses, companies, marriages etc. As paper and handwriting was the only data management technology available then, we fully accepted those registers.
When we invented computers 50 years ago, instead to re-engineering the whole system on the foundation of new technologies, we just re-applied computers to the paper-based architecture, invented 5000 years ago, and we still consider it “normal”.
We do not accept it as normal, as computers allow us to create something better than hundreds of nation-wide overlapping data silos registers, expensive and inaccurate.
If we do it right, it will be faster, cheaper, more accurate and convenient.

Biz-case 1:
As a citizen I would like to set up a company with a notary and then skip all government registrations. With my e-Passport I can register it myself. At the same time I want my company to be officially accepted by the government and be visible to all who may concern as an official business.

Biz-case 2:
As a Cadastre CTO I would like to have 100% (and I mean 100%, not 99.999999% or so) updated data on all parcels and buildings in the country, updated automatically by all those who change their status: construction companies changing the roof type, city authorities changing the street name or notary changing the ownership. In a way, I would like to use their resources to keep the data up-to-dated and reduce my stuff, getting more value with less efforts.

We address this challenge and the biz-cases in the Level 2 section below, subsection Reducing

Bureaucracy: No more government registers

Transparency/Ideal capitalism

Economists know the model of ideal capitalism with perfect competition. Its characteristic features are the absence of monopolies and availability of all information to all participants. We have already discussed monopoly above. Here we would like to address the challenge of complete market transparency. If there is a small new pencil factory in Bangladesh, we expect millions of Web shops (platforms) around the world will start selling those pencils the next day.

Biz-case 1:
As an owner of the new pencil factory in Bangladesh, I expect millions of Web shops around the world discover our products instantly when we release this info. We do not need middle-men here.
Biz-case 2:
As an owner of the new pencil factory in Bangladesh, I expect clients of Web shops to rate my products thus helping me to build e-Reputation of my products and the factory.
Biz-case 3:
As an owner of the new pencil factory in Bangladesh, I do not want to spend money on marketing. I strongly believe that clients should make educated decisions on the feedback of other clients instead of my advertising. It is more fair.

We address this challenge and the biz-cases in the Level 2 section below, subsection Transparency and Ideal Capitalism

e-Voting

There are times when a community needs to vote for something, from the president of the country to “what type of benches to put on our street”. This is usually very expensive and difficult and totally corrupted in authoritarian countries.
We want a simple and reliable voting system that can be used every day.

Biz-case 1:
As a citizen I would like to be able to vote with my e-Passport in such a way that nobody knows who I voted for, while I can easily check that my voice was counted. I would like to use any platform of my choice to do it.
Biz-case 2:
As a community manager/activist I would like to organize a voting on a subject which concerns us all. It should be (almost) free and simple, and I would like to use any available platform to set it up.
Biz-case 3:
As a citizen I would like to be able to check the results of elections with the help of any platform of my choice and even compare results using different platforms.
Biz-case 4:
As a society we would like to be assured it is all reliable and safe, meaning that people were not exposed.
Biz-case 5:
As the organizer of the specific local voting (e.g. on the new layout of a crossing in our city) I would like to add special (and rather significant) weight to those citizens who have special knowledge (confirmed by their e-Reputation) in city planning and road safety. I believe that in this way we get a better decision.

We address this challenge and the biz-cases in the Level 2 section below, subsection e-Voting

Improving/protecting Democracy

Just like capitalism (discussed above), democracy was hacked in many countries, from developed to underdeveloped cases:

- In USA Trump literally challenged the democracy institutions with his claims on “unfair elections”.
- In Poland the leading PiS party corrupted low-income citizens with public money to win their votes and stay for another term
- In Russia Putin mimicry elections to fool the society with the image of “elected” president.

It all is far from “normal”. We need mechanisms to improve and protect democracy.

Biz-case 1:
As citizens of USA we would like to have reliable elections
Biz-case 2:
As a president of USA I would like to launch long-term project like Apollo which goes beyond my term in the office, yet I would like to get credits for it while I am in the office
Biz-case 3:
As citizens of Poland we would like not to allow PiS to use public funds to corrupt low income citizens.
Biz-case 4:
As citizens of Russia we would like to organize an alternative elections to demonstrate that Putin cannot win fair elections
Biz-case 5:
As citizens of Russia we would like to be able to get organized in protected groups in such a way that (a) names of group members are not disclosed (b) such groups can discuss any projects in a protected way

We address this challenge and the biz-cases in the Level 2 section below, subsection Improved Democracy

Environmental (green) impact

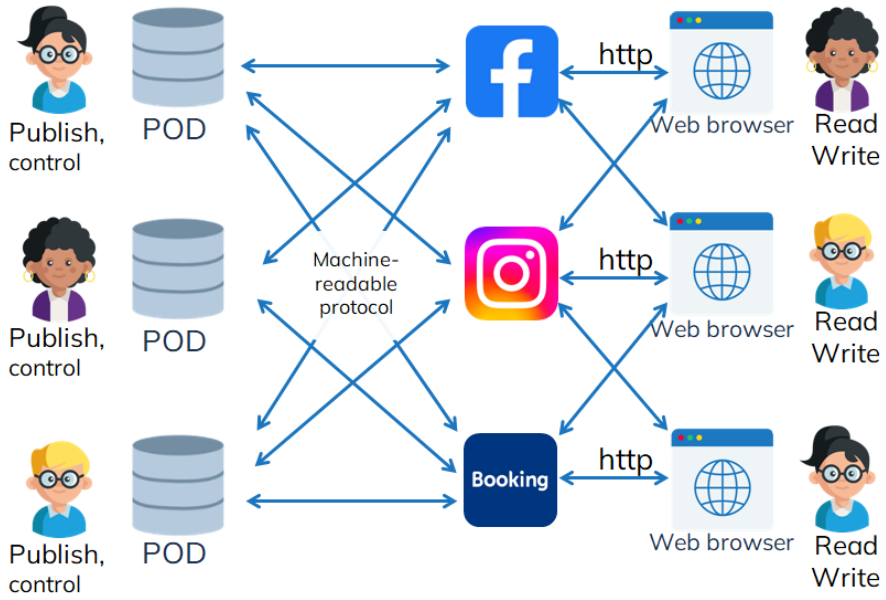
Internet and related services represent significant proportion of the global Carbon footprint production, and it became an issue for modern society.

Biz-case 1:
As a concerned citizen I expect Data Space to reduce Carbon footprint at least two times

We address this challenge and the biz-cases in the Level 2 section below, subsection Environmental (Green) impact.

LEVEL 1. Web 3.0 Data Space for C-level

Our concept is dead simple: most systemic issues of today's IT systems are caused by data being de-facto controlled by platforms. Therefore, the solution is to decouple data from platforms. Our vision of a decentralized Web 3.0 Data Space is an open ecosystem where people, organizations, and devices own their data and control access rights, whereas platforms and services access it on par with each other.



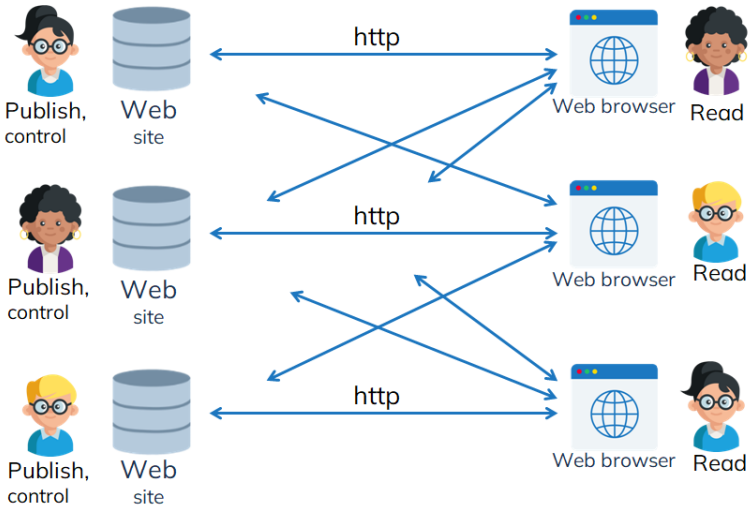
We call this concept the **Web 3.0 Data Space**. The name consists of two elements and requires some explanation: why do we call it Web 3.0 and why do we call it Data Space?

Why do we call it Web 3.0?

The best way to explain the name Web 3.0 is to start with the history of the Web, that is, Web 1.0, which we have known for 30 years:

- an owner of the content publishes it on the website
- an owner has the only (original) copy and has complete control over it
- a user needs a web browser to access content at any web site
- a user can (usually) only read the content

WEB HISTORY: WEB 1.0

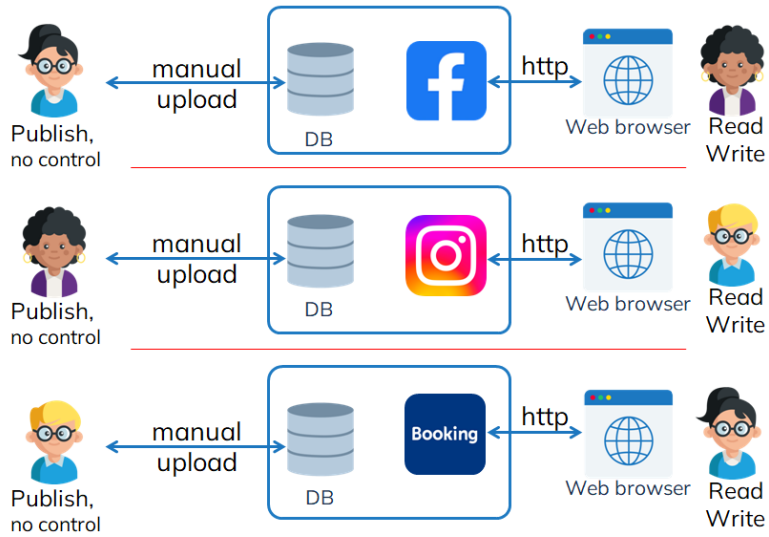


Web 1.0 was a huge step forward compared to any other systems. However, over time we began to feel its limitations. And the main limitation was the lack of data aggregation: if we wanted to book a hotel in Rome, we had to check and compare the websites of hundreds of hotels in Rome, and this is very difficult, because all websites are different.

That's why 20 years ago the first platforms (we call it Web 2.0), for example booking.com in the case of hotels, began to appear, which gave us such aggregation. At the same time platforms demanded to give up the natural advantages of Web 1.0, such as the owner's control over his/her information. Below we will summarize the essence of Web 2.0 for the hotel case, but the same applies to any other platform or domain:

- all hotels are presented in one platform
- it’s convenient to compare information about hotels
- users can leave comments about the hotel, and other users will be able to use it
- users can book the hotel at the platform, i.e. we can not only read the information, but also write it down
- as a rule, platforms provide their service for free

WEB HISTORY: WEB 2.0



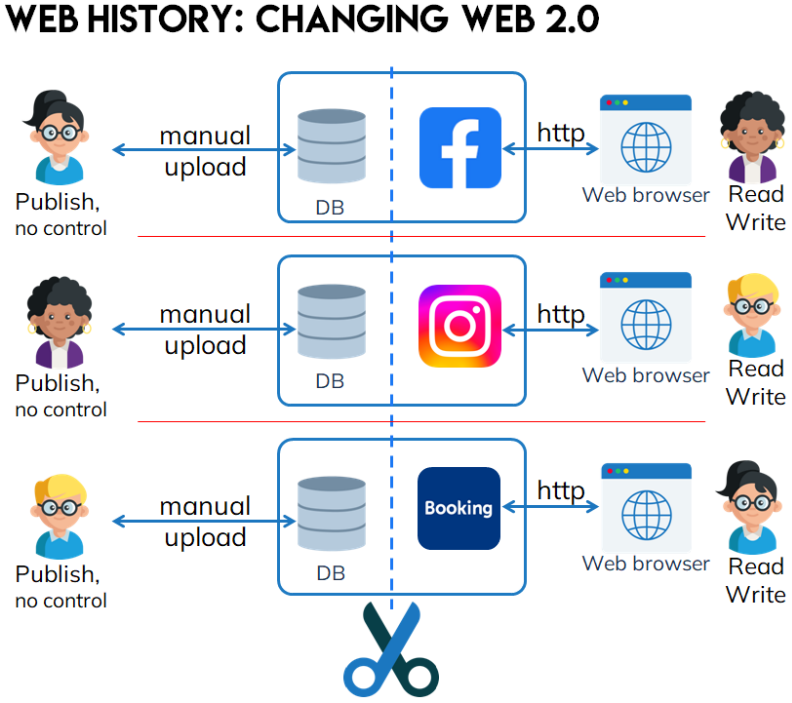
Along with all these benefits, we also received a number of problems that did not bother us much from the very beginning, but have become really big in the last 5 years:

- We have lost control of our information, and platforms can do whatever they want with it, and

this violates our rights.

- We discovered that there is (and cannot be) no communication between the platforms (after all, they are competitors). We have marked this with red lines in the picture above.
- We found that we were creating multiple profiles of ourselves on each platform, and posting the same information over and over again on different platforms, forgetting which version was the most current. It's called Data Silos.
- Most platforms are free, but their capitalization is huge. The reason is that "*if they give you something for free, then you yourself have become the product.*"

It turned out that along with a lot of benefits we also got a lot of problems. It does not take much time to figure out that ALL these issues have one reason: we allowed platforms to take and keep our data in their internal databases. Therefore if we want to get rid of all these issues, we need to decouple data from platforms, just like the next picture suggests:



If we do it, all the data from platforms comes back to the data owners (on the left), just like it was in Web 1.0 world. You will see the result on the next picture: all users' data returns to them in a form of PODs (Personal Online Datastore), which reminds good old web sites. Actually, PODs ARE the websites, just a little bit more advanced: while Web 1.0 websites were designed by Tim Berners-Lee (the father of Web 1.0) to be rad by people (via browsers), the PODs will be consumed by platforms. Web 1.0 websites were human readable. Web 3.0 PODs will be machine readable, and this is the only difference. BTW, PODs, and the new protocol Solid (instead of http) were invented by the same person, Tim Berners-Lee.

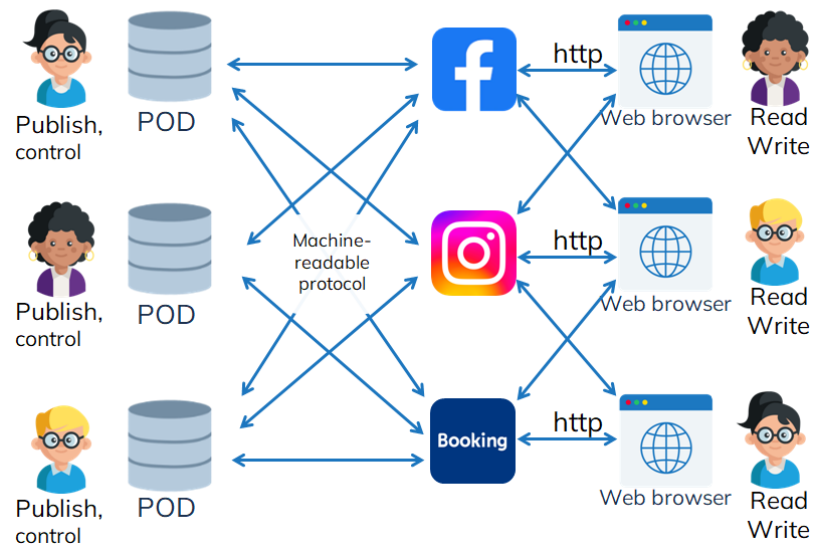
Please note that in Web 3.0 world all the platforms will continue to work as usual. Their users (on the right) will not notice much difference.

Yet, they will notice certain benefits:

- All platforms work with the same data, so we do not have any data silos and any confusion about numerous versions of the same bit of data. E.g. a user can publish a photo on one platform and her friends will see and discuss it on other platforms
- User can switch between platforms. If a user does not like one platform, he can start using another one, but he will continue the same discussions and work with the same information
- When Alice sends message to Bob, this message will land on the Bob's POD, and Bob will decide himself which messenger to use to read it. BTW it is exactly the way the ordinary e-mail works!

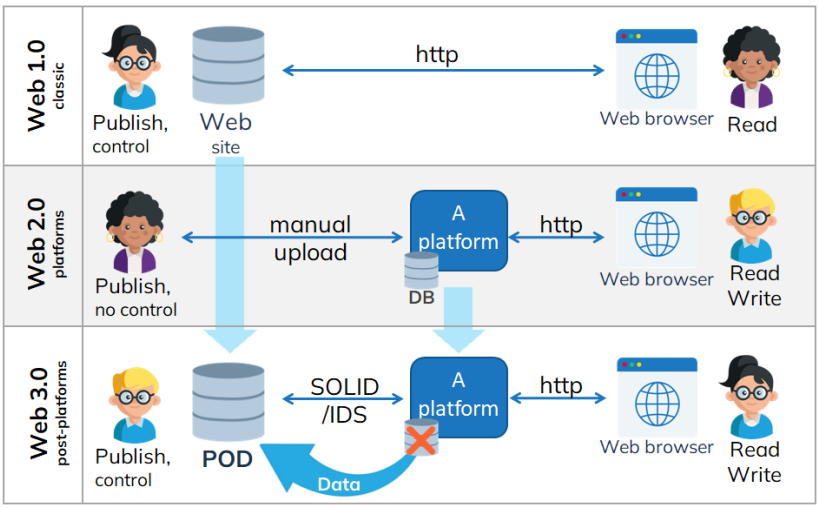
We will call these platforms without data as post-platforms, for convenience of further communication.

WEB HISTORY: WEB 3.0



To sum it up, Web 3.0 is a natural name for the ecosystem we are building, as it inherits the best from Web 1.0 (convenience of data access control on personal web-servers) and from Web 2.0 (aggregating power of platforms). Our vision of Web 3.0 is also perfectly compatible with the Semantic Web concept and with the Solid project by Tim Berners-Lee, the father of the Web 1.0, which is a one more reason to call it Web 3.0.

WEB HISTORY OVERVIEW



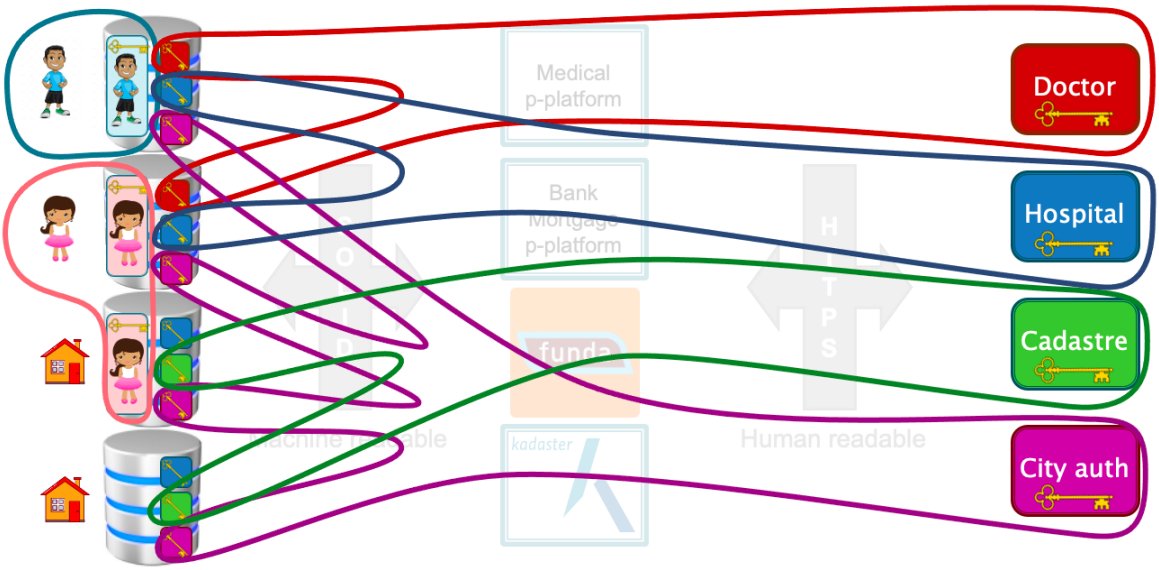
Why do we call it Data Space?

The second part of the name – Data Space – does require some explanation. The term ***Data Space*** became widely known after it was introduced by the European Commission in 2021, and since then many different visions of the Data Space concept were suggested (e.g. International Data Spaces (IDS), Gaia-X, MyData or Solid). Yet all these projects fail to provide a very clear definition/example of Data Space. For most of them Data Space is just a vague “general concept”.

In this section we are going to present a definition of Data Space, which is very clear and specific. We call it the Web 3.0 Data Space.

Before we provide such a definition, let’s dive into a couple of use-cases of a citizen who has a

personal POD and who has a house with the house's POD.



Here is the description of the case #1:

- A doctor may write down a prescription at the user's POD. It is the doctor (not the citizen) who can create, change and delete such a prescription, which means that the doctor OWNS it.
- A hospital may review such a prescription, and write down to the citizen's POD a MRI scan.
- Please note that:
  - both the doctor and the hospital are free to use any post-platform to read/write data (this is why we blurred the names of platforms on the picture)
  - they will be able to do it only if the citizen authorizes them.

Conclusion #1: As a result we see a doctor, a hospital (and, possibly, a pharmacy, an insurance, a ministry, a researcher, a pharmaceutical company) keeping all patients data on his/her POD and exchanging this data via POD, using all kind of platforms they wish. It looks like a giant shared Google document.

And now comes a more advanced use case #2:

- A Cadastre may decide to keep copies of their records at PODs of houses which belong to citizens (why not?)
- City authorities may decide to keep copies of the address information at the very same PODs of houses.
- At one day a certain authority may decide to change the name of a street where the citizen lives. Then they will change the address info at the POD of affected houses.
- At the very same moment it will change the address at the Cadastre records at the same POD due to Linked Data which connects records from Cadastre and City office at the POD.
- And now we have a situation when the Cadastre own database is outdated: it's records have outdated address information on a range of houses

Conclusion #2: the Cadastre does not need its database at all: the most updated information is kept at the houses' PODs, and many organizations (notaries, construction companies, city authorities etc) are busy with updating it, so that Cadastre can save a lot of costs. Also, it makes the Cadastre data 100% correct, which was never the case before. The same refers to the use-case #1 above: the hospital and the doctor do not need their own databases. They are better off keeping their data at the patients' PODs and reviewing it via any post-platform of their choice. We discussed the case with the Dutch Cadastre specialists, and this situation seams very feasible (yet, of course, it needs further investigation, and this whitepaper will serve it)

Conclusion #3: citizens' PODs will keep not only personal data but also the data from organizations (e.g. hospitals) and public authorities (e.g. Cadastre). It means that:

- people are responsible to keeping public information, and they cannot turn their PODs off
  - it means that the PODs require advanced level of security.
- we may need less public registers and less bureaucracy.

Now we are ready to define the Data Space as we see it at the Post-Platforms Foundation.
This Data Space is formed of billions, and at some point in the future, of trillions of independent PODs for every person, company, or object, where all the data by and about them is stored at source, in one and original copy. They all constitute a gigantic decentralized machine-readable Data Space, where every element is always up to date and every data transaction is identified and secure. This new ecosystem of trillions of “data at source” PODs has rather unusual consequences. In the world of the Web 3.0 Data Space, governments and corporations won’t need databases. Individual PODs keep all the information originated by a person via their online activities, including sent messages, posts, transactions, various files they created, etc. The same storage also keeps track of all messages, comments, and reactions they or their content ever received. Last but not least, organizations and public authorities also record on the POD every piece of information about its owner's identity and legal liabilities, and this data cannot be changed or deleted by anyone but their authors.
Every legal entity also stores all the information related to its business and legal interactions on its POD. Just like individual ones, their PODs become unique focal points for their data. The Web 3.0 Data Space concept also implies that sooner or later, every real estate, vehicle, device, or even many parts of them will have their own separate PODs. All information regarding their history (ownership, origin, modifications, adjustments etc.), their future (resource left, maintenance scheduled), and their interactions with other subjects and objects will become available to their owners, manufacturers, regulators, partners etc.

In a certain sense, the Data Space brings us back to the natural non-digital interaction with information. When we are interested in the name of a person and where she works, we turn to her directly, not to the municipality or to the tax authority. And if we are interested in what color the house is and what it is built of, we just come and have a look, instead of calling the Cadastre.

Data Space projects Strategic Landscape

Our Web 3.0 Data Space project is not alone. It is surrounded by a number of similar projects, and, of course, we need to understand how Web 3.0 Data Space relates to them.
This is why we started the document with a description of Challenges and Biz-cases in order to create a landscape of problems that are solved by certain projects. Below we will very briefly describe the main relevant projects and the positioning of the Web 3.0 Data Space project in relation to them.

Existing Web 3.0/Data Space Concepts

Here we will very briefly reflect the most interesting concepts relevant to Data Space.

Blockchain

In the past years, the Web3 term has been widely used by the blockchain and crypto communities. However, if we examine their products from the standpoint of the core Web 2.0 challenges they are supposed to solve, we quickly find a lot of serious issues, including, among other, low scalability, re-centralization, poor security, lack of privacy, etc. There is no way we can rely on blockchain in building Data Space. For more details why blockchain totally fails the challenges of Data Space, read our separate whitepaper here. If you prefer video, please use this one. If you also need a quick tour on the basic cryptography, you can watch it here.

Solid project

Another interesting project is the Solid project from Tim Berners-Lee, the father of Web 1.0. He proposed a new vision of the Web 3.0, where each user has his/her own Personal Online Datastore (POD), with data stored as Linked Data. Surprisingly there is not much room in this concept for platforms, which makes the entire architecture hardly scalable. The security is based on Web ID which is also rather weak SSO (single sign-on) solution. Indeed, security in classic Solid is rather limited, which is a serious issue. It probably explains why Solid was not implemented in large scale after a decade since the inception.
Yet we like the idea of POD, as it represents a powerful concept of Data @ Source.
Indeed, most specialists explore Solid as a Protocol, and discuss its pro/con. We specifically would like to draw your attention not to the protocol, but to the two elements, connected by this protocol:

- on one side there is data @ source, at the POD
- on the other side there is an app (or we call it a platform)

We believe that this is the major innovation, brought in by Solid: separation of data from platforms. If we start from this maxim, we end up with Web 3.0 Data Space, adding a lot of missing elements to Solid along this road: Persistent ID, advanced security, the Register etc etc etc.
Therefore we consider Solid project as a solid foundation for Web 3.0 Data Space.

European Data Space

Another prominent approach to Web 3.0, called Data Spaces, was launched by the Fraunhofer Society and is currently promoted by numerous European organizations, including IDS, DSSC, MyData, iSHARE etc. Their vision is to connect platforms together via a standard API, called IDSA Protocol. It looks like a quick fix to the issue of having 800 (which is a typical number for large corporations) platforms in corporations like BMW, but it has certain limitations:

- it does not recognize people behind platforms which leads to limited capacity to cover most of our biz-cases
- it also does not cover IoT biz-cases for the same reason
- as a result it has to provide keys to organizations instead of people, which creates fundamental security issue with building trust
- it is not scalable, as it is virtually impossible to interconnect 800 platforms with APIs (it means ~800x800/2=320’000 connections)

In a way, just like Solid, IDS puts the focus on the Protocol, without paying attention what exactly the protocol connects. Usually it connects platforms, and here is the issue: interconnecting platforms does not resolve the issue of data silos at all, it just makes silos little bit more synchronized.
Yet, if we connect best of IDS (platforms) and Solid (PODs) together, we will get something usable, like Web 3.0 Data Space.

A special role of IDSA in European Data Space

It is important to add that IDS is not only about IDS architecture, protocol and standard. There is also an IDS Association (IDSA), the purpose of which is to unite all Data Space projects. We are happy to be part of this large family, within which different approaches to the implementation of Data Space are being developed. We believe that IDSA is a very important and necessary association that should unite all Data Space participants. Therefore, we set the task to involve the Solid community in the IDSA orbit, and combine IDS and Solid architecture. We hope that the result of this merger will be Web 3.0 Data Space or similar technology. Such a merger is a complex project that can only be completed based on the work on the biz-cases described above. It can probably be seen as a natural evolution of the IDS architecture over time.

European Digital ID program

This program does not promise to build Data Space, yet it is important for us. It develops the perfect cryptographic ID, in our case, the Web 3.0 e-Passport.
At the moment these two European programs are not interconnected, therefore they have to overlap:

- The Data Space program re-invents the identities
- The Digital ID program re-invent the POD in a form of a “Wallet”

We clearly need to interconnect them.
The European ID program develops the eIDAS standard, which we will use.

Other open source projects

In the social media industry, some other initiatives and protocols, such as Fediverse/ActivityPub or BlueSky keep trying to create platform-independent distributed databases, but they all lack semantic specs, have weak authorization schemes, and still have some remaining issues around data ownership and data control to solve.

Gaia-X

We mentioned Gaia-X here only because most of Data Space professionals ask to comment on this project. In order to provide the answer we have reviewed a lot of materials (papers, presentations, video) from Gaia-X.
Finally, we have decided to refrain from discussing Gaia-X in this document.

Post-Platforms Foundation Strategic Positioning

Post-Platforms Foundation (NL) is an open non-for-profit community, which has 5 major goals, presented below. 4 of them (except #3) require business experience in so-called ***organization innovation***, therefore most of our specialists are business developers and entrepreneurs with MBA degrees and experience in large projects, or engineers with profound business and strategic experience.

1. **Engaging co-opetition among Data Space projects with help of shared Biz-Cases**

As we discussed earlier in this chapter, there are many Data Space-related projects (mostly) in Europe that have little to no communication with each other and know little about each other. They speak different languages. This creates problems for buyers of such systems, because they do not understand why Gaia-X is, say, better than Solid.
In December 2023, together with IDSA and the Solid community, we launched an initiative to unite Data Space projects. We suggested starting with a common language, which is Biz-Cases, the high level functional requirements, presented above in the section Challenges and Biz-cases. These Biz-cases will allow:

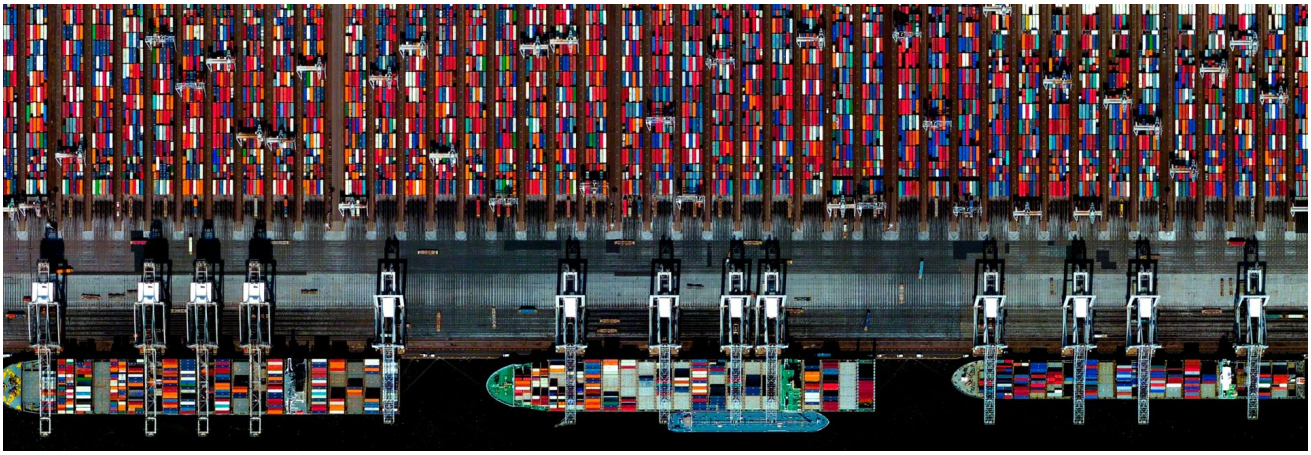
- Data Space projects themselves to understand how they relate to each other on the Data Space landscape, and where they have the potential for cooperation and knowledge exchange.
- Buyers (corporations, governments and citizens) to understand which projects address the biz-cases they need.

We do not expect that as a result all projects will immediately merge into one. We expect creative co-opetition between competing architectures, using this common language.
We carry out this work within the framework of the IDSA association, as one of the members of this association. We believe that IDSA is the ideal community for this kind of unification, and we play a facilitating role here.

2. **Leading the Organizational Innovation in the Data Space field**

As discussed above in this section, most Data Space projects approach the problem from an engineering point of view, and develop protocols, standards, data structures, clearing centers, App stores, etc.

Yet the Data Space project is too huge to be done with just technological innovation. Large projects are carried out only in a balance of technological and so-called ***organizational innovation***. For example, in transport it was not enough to invent a truck or an airplane, but an organizational innovation called a “container” was needed: it required cooperation and trust between large ports, ship makers, railway systems and truck makers to get a simple container to be delivered around the globe. At the same time, from the technical point of view, a container is just a box.



In automotive it was not enough to come up with a diesel engine, and it took Henry Ford's assembly line and Toyota's Just-in-time innovation to make cars affordable.

As a member of IDSA, the Post-Platforms Foundation is developing exactly this aspect to ensure that we all work together to create a coherent and working system. This includes activities such as:

- support in development the Governance ecosystem around Web 3.0 Data Space, including launch of Post-Platforms Association, the Register NGO etc.
- maintaining the balance between organizational and technological innovation (for example, in creating a PKI system)
- maintaining the balance of commercial and non-commercial participants (for example, the Register should be non-commercial, while the search engines around it should be commercial)
- maintaining the balance between the role of business and states/politicians (for example, in deciding who should issue e-passports)
- participation in the development of governance systems and complementary legal frameworks
- maintaining the balance between large corporations and startups, investors and grants
- assistance for participants in developing roll-out scenarios and business plans for corporations and startups
- etc

3. Suggesting our own Data Space architecture, called Web 3.0 Data Space

Our Web 3.0 Data Space concept takes the most promising ideas and technologies from several projects above (mostly Solid and IDS), and incorporates them into a single Web 3.0 Data Space vision, as we will present below. We also make sure that the final ecosystem addresses ALL the Challenges mentioned above.

We would like to specifically stress that we do not see Post-Platforms Foundation as an inventor of any technology. We believe that all technologies were invented long time ago and Web 3.0 Data Space just re-arrange them in a new way, which, IS the organizational innovation.

4. Launching commercial spin-offs in the Web 3.0 Data Space ecosystem

The world of Web 3.0 Data Space cannot be built by states and corporations alone. We need to attract startups to it. We all understand that it is very difficult for startups to build such a system on their own, and they need help from investors, accelerators, and universities. We intend to provide

such assistance, and even launch similar startups ourselves or share our business plans with them. At the moment, we have business plans to launch startup projects in the areas of accommodation, education, mobile operators, and real estate.

5. R&D in Social Impacts of Web 3.0 Data Space

Web 3.0 Data Space will have a huge social impact, for example:

- it will allow the development of a very complex ecosystem of electronic reputation of people, companies, products and any digital assets.
- it will change the political life of many states, from developed democracies to autocracies, from electronic voting and the first experiments with meritocracy to the possibility of organizing resistance to dictators
- it will develop new types of electronic money without the participation of banks
- it will make capitalism flat and almost “ideal”, which will undermine the foundations of all current monopolies
- high transparency will require serious systems for protecting people from surveillance, probably through the use of PET technologies
- it will give AI systems access to huge amounts of data that AI developers never dreamed of. This will require new regulations regarding rights to derivative data created with the help of AI

All of these changes require coordinated exploration, and the Post-Platforms Foundation intends to play an important role in this effort.

LEVEL 2. Web 3.0 Data Space for Analysts

In this section, we will take the Web 3.0 Data Space exploration to the next level, where we discuss specific solutions, analytics, and reflections. Specifically, we will review:

- Basic principles on which the ecosystem is built
- The Importance of Organizational Innovation
- Specific solutions for all Challenges and Biz-cases stated at the beginning of the document.
- The essence of the Internet
- Governance of Web 3.0 Data Space
- Possible strategies for deploying the system

Later on, in the Level 3, we will discuss the Architecture and relevant technologies.

Basic principles of Web 3.0 Data Space

After two years of work in this area, we were able to identify the most important principles that define the essence of the Web 3.0 Data Space system

Most Important: Data @ Source

In fact, the remaining principles are much less important. Indeed, all the variety of amazing opportunities that Web 3.0 Data Space will give us is based on only one basic principle: The data must be with the owner, and in only one copy, the Original one. As a person, I would like to have one birthday, one current address, one set of phone numbers, and not many (mostly outdated) copies of them on different platforms.

As soon as we follow this simple principle, a Pandora's box opens, from which answers to all the questions posed in the Challenges section appear. And the first challenge we answer is that we totally get rid of Data Silos, as there will be no more numerous copies of the same data at different platforms, only one and original data @ source.

Actually, in Web 3.0 Data Space architecture we execute this principle by splitting platforms from their data and returning it to owners in a form of PODs.

As we'll discuss further in the New Essence of the Internet section, this principle does reflect the reality. E.g. if you want to know how many floors this building currently has, you don't have to go to the Cadastre. All you have to do is ‘ask’ the building itself. It’s POD will have the right answer.

Indeed, despite its apparent simplicity, this principle will completely change the world as we know it. This is the foundation of Web 3.0 Data Space.

In large networks connections are more important than nodes

With the advent of Web 30 years ago, we have learned to appreciate the world of hyperlinks. But we know that hyperlinks are unreliable and often break. Typically, most links will be broken 20 years after publication. We discussed this issue in the Persistent ID biz-case in the Challenges and Biz-Cases section above. With the Persistent ID, connections will become reliable and begin to play as important a role as the data itself. For example, e-Reputation, in fact, is 100% based not on data, but on connections, because the phrase “I like your hotel” is nothing more than a link between you and the hotel with a positive rating being a parameter of this link. Or, educational services will appear that assemble a course specifically for you from a huge number of related pieces of completely different courses.

But here we would like to note another feature of connections: their number in a large system. Indeed, to connect 2 objects, you need 1 connection, 3=>3, 4=>6, 5=>10, 1000=>499’500 and so

on. The number of connections between objects grows as $N^2/2$. It is obvious that in a large system, which will be Web 3.0 Data Space, connections will play a dominant role over the data objects themselves. And then, when discussing any information problems, we will have to remember about connections. For example, when discussing long-term Preservation, we will have to think about how we will preserve relationships between objects over centuries, which will require a Persistent ID.

Fuzzy structures instead of strict structures

All participants in the Data Space discussion understand that the interaction of all participants, all data and all platforms will require ***ultimate data interoperability***. And the obvious next step is to demand the development of common standards for data structures and ontologies.
And this may be a strategic mistake.
The fact is that it is impossible to create the same data structures for all hotels, ships, astronomers and museums. One may be thinking that it is possible to divide the entire world into 14 Data Spaces, as the EC did with the European Data Space program, and define data structures within each of the 14 domains. But the problem is that even if it were possible to define uniform data structures for one domain (which, of course, is also impossible), how would you define the boundaries between these 14 domains? Where does the world of museums end and the world of tourism begins? Where does tourism end and transport begins? Of course, there are no clearly defined boundaries between domains. Therefore creation of a single set of data structures for the entire world is completely impossible. Moreover, this world of data is constantly changing over time, and old structures or ontologies become outdated.
What should we do then?
Correct answer: nothing.
There is no need to create uniform data structures. Let each platform keep the data in the format it wants. Later, at the Level 3, we will discuss how Linked Data & LLM technologies will help us solve the problem of data interoperability. Here we would just like to point out that the world of rigid structures is ending. Yes, for the last 50 years data could only be stored in rigid databases. In similar way, 20-50 years ago programs also could be written only in well-structured algorithmic languages, starting with FORTRAN and PASCAL. The programs have changed since then. Nowadays we often see neural networks that work without any pre-built logic. Similar change we expect in the world of data, which will go away from rigid formats and universal data structures. The real world consists of millions of types of data, and Web 3.0 Data Space suggests learning to live with it, as Web 3.0 Data Space should reflect the real world, as we will discuss in the section New Essence of the Internet.

Thus, we come to one of the most important principles of Web 3.0 Data Space: we move away from strict structures and begin to live in a world of fuzzy data structures. People have been living in such a world for millions of years. It's time for computers to learn how to do this too.

Trust. Reputation

The success of human civilizations in the real world is mostly built on our ability to maintain trust and reputation. Trust and reputation mitigates risks and damages, allowing us to cooperate effectively within society and create value.

As Web 3.0 Data Space is just an extension of the real world (see the New Essence of the Internet section), its e-Reputation mechanism is extremely important.

We know how it partially works already even with conventional Web 2.0 platforms: while booking a hotel, you read reviews from other customers about that hotel. Unfortunately nowadays all these reviews are spread across many platforms, which reduces their value. Also, we are not sure that those reviews are fair, as these people are not properly authenticated.

Therefore, if the Web 3.0 Data Space doesn't allow platforms to own our data, why should we allow them to own our reputation (likes and comments)? Both likes and comments must belong to us, the owners of the information, that is, they must land on our PODs.

When we get all likes and comments on our POD, we can calculate what we call e-Reputation, a set of parameters (a vector of, e.g. 17 parameters) which sum it all up. We need to say that:

- it should be many post-platforms which calculate such e-Reputation in a competitive manner
- the owner of a POD cannot change (or delete) these comments, as they will be signed by authors
- the owner (or the requesting party) will decide which reputation calculator to use and whom to share the result with
- e-Reputation could be calculated for people, organizations, things, documents, products and even post-platforms.

Some people do not feel comfortable with idea of recording people’s opinion on our PODs in the future. We say that we should feel uncomfortable right now, as nowadays similar e-Reputation is collected either by commercial players like facebook in the Western world or by governments in countries like China, and it is done totally without keeping us informed. Within the Web 3.0 Data Space concept we just suggest to take it under our ***own*** control. Nothing more.

Many valuable services will be built with help of e-reputation: economical inclusion, fake news control, job search and many others.

No fake names. Just Real IDs

The basis of trust and reputation should be the belief that you are talking to a real person with a real ID (e-Passport). This is especially important in times of deep fakes, when your voice or even video image can be faked. The only thing a thief cannot fake is your e-Passport and your private key. Therefore, the e-Passport is becoming the most important basis for trust and reputation in the Web 3.0 Data Space. It is also the basis of "***security at design***". Modern security is based not only on encryption algorithms and security protocols but mostly on key management. Key management is the Achilles heel of modern security. E.g. this is why you have several hundred logins and passwords for different platforms.
By the way, we will show below that in Web 3.0 Data Space, security based on reliable e-Passport management is not so much a burden for the entire system, but rather an inspiring source of completely new services, such as e-Reputation, e-Voting, e-Money, IPR management , PET etc. And, of course, if you need to hide your identity in certain situations, this should be possible. Yet, the system should know that you are the real person with the real e-Reputation. We will demonstrate in Level 3 below how to make it possible.

Large System approach

When we discuss Web 3.0 Data Space, we must remember that we are talking about a system of enormous size. Size matters in the sense that a large system has capabilities that its elements do not have.
Accordingly, Data Space solutions must take system size into account. For example, when creating a security system or solving an interoperability problem, we will have to make decisions that take into account the enormous size of the Web 3.0 Data Space.

Competition instead of Monopoly

This is a pretty obvious principle. However, its correct use may not be so obvious.
Here are two examples:

- **Calculation of e-Reputation.**
  e-Reputation is the most important mechanism of self-regulation of society. But who will calculate it? Should we create a single standard for calculating e-Reputation based on likes and comments? Obviously, this is the path to a monopoly. It is important that many ***e-Reputation calculators*** appear on the market, and that in the competition they develop increasingly complex calculation methods. For example, it is necessary to learn how to deal with attacks on e-Reputation, like mass bullying or cancel culture,
- **Data interoperability**
  We will discuss below that we are solving the problem of data interoperability not by creating a "single standard," but in a completely opposite way: by inviting all platforms to write data on the PODs in the format they are comfortable about. At the same time, with the help of special technologies (Linked Data, LLM etc), platforms will learn to understand each other. And competition here will be the most important mechanism for the development of these technologies. The best and brightest platforms will better understand other platforms and leapfrog ahead, raising the bar for interoperability ever higher. Competition, not data standards, will drive the solution to this critical problem. See Providing Interoperability of Data Types & Structures

Decentralization vs. Centralization

Most experts agree that decentralization is good.

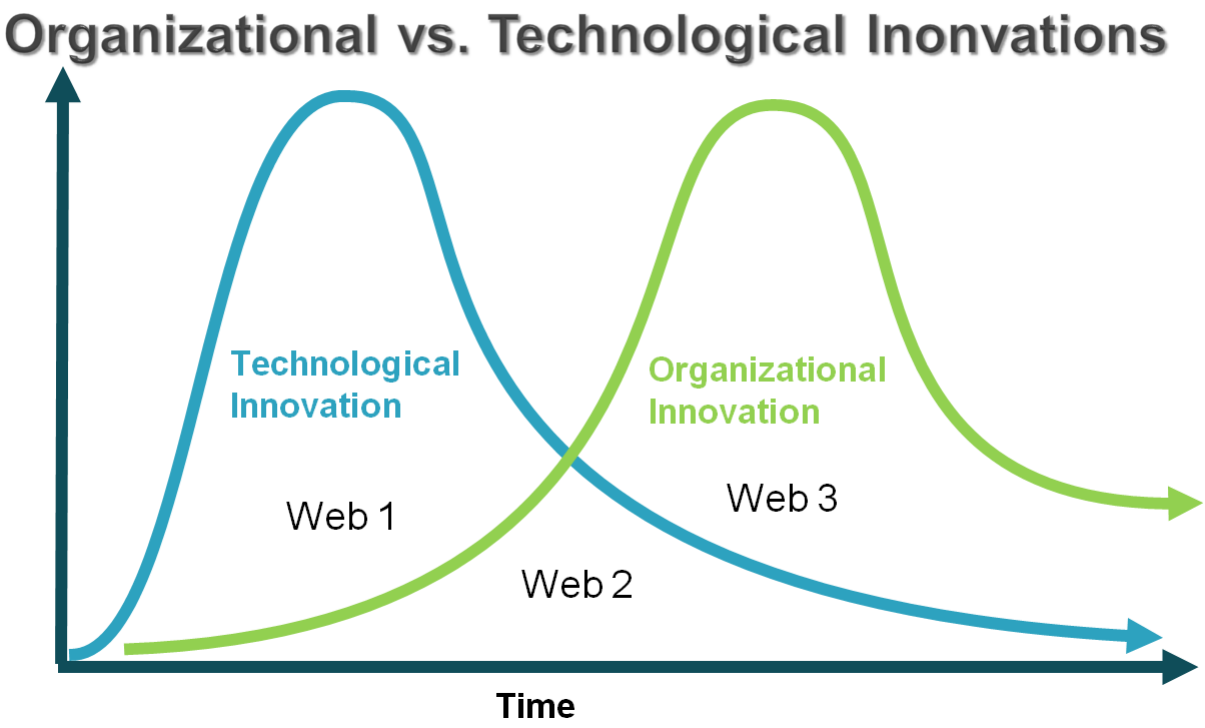
At the same time, we must remember one rule, promoted by our partner Fabien Gandon from INRIA.fr: "*You push Centralization out of the door and it gets back through the window.*"
This is a really serious problem. In addition, it is not always possible to distinguish centralization from decentralization. For example, blockchain adherents claim that this system is decentralized. And only if you take a closer look at the blockchain, you will discover that it is a strictly centralized system that works with a single ledger. The fact that this ledger has a million copies does not make it decentralized. BTW, the DNS looks exactly the same: it is centralized in essence, but decentralized in the sense of many copies. And yet it is a centralized system.
Web 3.0 Data Space will face the problem of centralization many times, and each time we will have to make serious strategic decisions, for example:

- Do we prefer to issue e-passports with the help of a centralized state or shall we outsource this to notaries and banks?
- Will we choose centralized Persistent ID or decentralized?
- Do we need centralized or decentralized ontological vocabularies?
- Can we afford a centralized standard for calculating e-reputation, or is it better to have many competing calculation methods?

In most cases we will strive for decentralization to avoid any monopolies. But with Persistent ID, we may, like DNS, have to agree to a single ID space for the entire world. And perhaps this should be considered not as centralization, but as an open market place.
We have a lot to discuss as we develop the Web 3.0 Data Space project, and we invite everyone to the conversation within IDSA.

Organizational Innovation

In the Level 3 section you will see, that despite the rather complex technical architecture of the Web 3.0 Data Space, there is not a single major technological innovation that you had not heard about before. Yes, we probably configure data and access to it somewhat unusually, but we do not offer any technical innovations.
However, implementing Web 3.0 Data Space does not promise to be easy. And this complexity lies not in Web 3.0 Data Space technologies, but in the so-called organizational innovation.
It is known from the industrial history that ***organizational innovation*** always follows the technological one. For example, in transport, the introduction of the container (organizational innovation) followed the invention of the train, plane, and truck. In the automotive industry, the organizational innovation of *Toyota Just in Time* and the *Assembly Line* from H.Ford followed the invention of the internal combustion engine. And, of course, these organizational innovations were much more powerful in their impact than the technological innovations that preceded them.



We see the same thing in the development of the Internet and web technologies. While TCP/IP and Web 1.0 and 2.0 can be classified as technological innovations, Web 3.0 Data Space is almost entirely in the area of organizational innovation.
Indeed, launching a Web 3.0 Data Space system requires the interaction of a huge number of platforms, enterprises, support of legal infrastructure and the launch of a global PKI. It also requires the development of a number of standards. And it seems that no commercial company on its own can launch such an ecosystem.
Organizational innovation of this magnitude requires the support of public funds and state-owned enterprises.
Thus, Web 3.0 Data Space will be the largest organizational innovation in the development of the Internet, which will determine its development for centuries to come.

Addressing the Challenges and Biz-cases

In this section, we are going to apply the Web 3.0 Data Space concept introduced in Level 1 onto the challenges and biz-cases presented at the beginning of the document, and show how all of these challenges can be solved in a holistic and effective manner.
In fact, Web 3.0 Data Space is capable of solving a much wider range of biz-cases, especially in the area of social impact. We address them in a separate whitepaper.
We will discuss the issues below in exactly the same order as they were presented in Challenges and Biz-cases section.

No Data Silos

The solution to this problem in the world of Web 3.0 Data Space is most obvious:
If your data is not spread among tens or hundreds of platforms, but securely stored in one place on your own POD (according to the Data @ Source principle), then the problem of data silos disappears automatically. All platforms around the world will deal with a single original copy of data, and change it directly on the POD.
Of course, only authorized users can make changes, regardless the platform/service they use, and their authorization is control by the owner in one place, at the same POD.
Also, old versions of data will be saved on the same POD, too, much like Google Doc saves

versions of your document.
Some specialists may be concerned as the Data @ Source principle creates a risk of ***single point of failure*** for PODs. We address this issue via creation of numerous synced PODs, as discussed below in the section Long-term preservation .

Data Sovereignty

Within Web 3.0 Data Space Individuals (and organizations which create their own data) become the true owners of their own data, while platforms remain merely tools for better & creative UX and convenient data aggregation.
We will have true data sovereignty:

- We actually keep our data in a “place” we own and control (POD) and we decide where it is hosted (just like the web site). The system guarantees (with help of security audit platforms) that no one else keeps unauthorized copy of our data, except for specifically allowed temporary caches at certain post-platforms.
- We (and not the platforms) decide who can access it and on what conditions. Please note that it does not matter which particular post-platform is used by authorized users.
- If we decide to sell our data, we control price and conditions, which all post-platforms have to respect
- No platform can “ban” us from data we need (e.g. facebook can lock you out for a month), since we can use many services to access data we need.
- We control not only our data, but all “networking data” we create: likes, comments, follow up connections etc
- We claim and retain cryptographically enabled ownership on our data, which can be easily checked up, together with the whole chain of provenance.
- We never lose track of important data due to Persistent IDs and Long-term preservation
- We also keep our identity separately from any post-platform, meaning that no Single-Sign On system like *facebook passport* controls us any more

Eliminating Monopoly of platforms

We are all so accustomed to the monopoly of platforms that most people just smile when they learn about Web 3.0 Data Space. However, the platform monopoly is not forever. It’s just that society mistakenly gave their data to platforms without considering it important. We have now realized this error and are going to fix it. At the same time, we really need platforms, because they provide us with data aggregation and processing! They just have to do it without taking our data.
Within Web 3.0 Data Space platforms become post-platforms:

- all of them will provide us access to exactly the same data at the millions of PODs.
- they will compete to provide better service, with help of AI and other technologies.
- as users and companies we may expect better services for lower prices.

By the way, it is a mistake to think that platforms will resist the implementation of Web 3.0 Data Space. Rather, on the contrary, most platforms readily accept these new rules of the game, and we discovered this when preparing the ECCCH grant in the summer of 2023, as described in the roll out section below.

Advanced Security

Web 3.0 Data Space is going to be a very, very large global system. With regard to security, there is a simple rule of thumb: the larger the system, the more advanced security is required. Hence Web 3.0 Data Space will require a military grade security. And we will provide it.
There are several principles for this type of security:

- it should be based on Strong ID/auth management (described in the next section)
- we will need PET to combine transparency and privacy
- it should be based on open technologies and standards
- we will rely on (historic) transparency of activities instead of “security walls” (“the eye of god”)
- the ongoing audit of the elements of the eco system should rely on crowdsourcing as much as on professionals

See details in the Security section in Level 3 below.

Strong identity management (e-Passports & e-Keys)

Instead of hundreds of logins/passwords or relatively insecure Single Sign-On systems, the Web 3.0 Data Space users will have one key and one e-Passport for all services. This e-key, based on physical device of some sort (crypto-chip on a phone, Mobile ID SIM card, USB fob), will offer state-of-the-art security and cryptographic authentication, and provide access not only to any digital service, public or private, via any platform, but also to physical spaces/devices, such as hotels, offices, cars or ATMs.

This type of e-Passport is called Verifiable Credential and it means that the identity of the user could be verified by any service “on the spot” without any need to get in contact with any Single-Sign-On operator, making the user uncontrollable for platforms and independent.

Unlike e-IDs currently existing in some European countries, this new e-Passport and e-key system will be international. It does not need to be dependable on governments, as the only purpose for the e-Passport is to authenticate the user. Nationality will be a changeable parameter, as the user moves from country to country, but the user’s ID will stay the same for the lifetime, although the keys will be changed either during regular maintenance or if compromised.

The “one e-Passport for all systems” is not only convenient for users, this is the only way to implement the advanced security, required to run the Web 3.0 Data Space. A powerful key management represent pillars which are needed to build any type of secure services on top of it, e.g. IPR control system.

Please note, that only people and things will have e-Passports, but organizations will not. We know it contradicts the architecture of Gaia-X and some other projects. Please see section Who may have keys? in Level 3.

The convenience of global ID/auth system with one-key-for-all comes at a price: we will have to develop and deploy a global Public Key Infrastructure (PKI) system to sign users’ public keys. This is not a technical task, but one of those “organizational innovations” required by the Web 3.0 Data Space. We plan to develop win-win roll-out biz plans to deploy the PKI via partners with established off-line offices (as users have to present themselves to the CA, the Certification Authority to get their public key signed) all around the globe, like mobile operators or banks.

The PKI system is not something new: corporations use it for internal purposes for 40+ years already. Yet the global system was never developed (we do not count SSL certificates as it is very limited and not secure enough due to weak ID verification). We believe that the cost of global PKI could be justified only by a really large system like Web 3.0 Data Space.

The reliability of the PKI is a big issue itself and we will explore it further. It depends both on its architecture (we need to avoid single point of failure of a root-CA)and on the reliability of the local CAs which will issue e-Passports (certificates) to users. E.g. we may consider issuing several types of e-Passports with different security levels, e.g.:

- low level (for transactions below €50 per day), issued via online apps
- mid level (<€1000), issued by mobile operators or banks
- high level (<€100’000), issued by certified notaries

Standards like W3C/SSI, W3C/DID or CEN/eIDAS will be used.

Long-term preservation of all our data

The requirement for data preservation for 500 years or more is at least 10 times higher than the life expectations of any platform. Web 3.0 Data Space solves this problem by storing data separately from post-platforms, which will be merely aggregating browsers to millions of PODs. Post-platforms can be easily replaced, and their disappearance in 20-50 years will not affect long-term preservation.
The only question that remains is how to store data on PODs for 500 years. After all, no PODs provider (for example, AWS) can guarantee that it will be available in 50 years. This problem can probably be solved by synchronizing 3 or more PODs provided by competing cloud services (POD providers). We call this the “revolving structure.” And then, in the event of a shutdown of the primary PODs provider, one of the two other synchronous PODs will become the primary one.
This scheme ensures the requirement for long-term preservation for 500 years.
We are accustomed to perceiving the Internet as a medium for very reliable data transmission. But Web 3.0 Data Space proposes to begin to perceive the Internet as an environment for very reliable data storage. And it really will be secure storage if you put this data through certified Web 3.0 post-platforms. The usefulness of this solution can hardly be overestimated: from now on, humanity will receive real long-term memory, which can exist as long as Egyptian texts carved into stone.
Please see details in the Level 3 and in the Long-term preservation whitepaper.

Persistent IDs (no broken links)

As we discussed above, Web 3.0 Data Space is a system that is designed to store data apart from platforms. This raises the question of identifying both PODs and the data stored on them independently from post-platforms which created the data. After all, usually the identification of data always depends on the platform that controls and stores it, and this range of IDs is global only within this platform. For example, in the Google document with the URL https://docs.google.com/document/d/1CUPnQdNIUg5Q2f33qWnoqgXT-E09CiLf the ID **1CUPnQdNIUg5Q2f33qWnoqgXT-E09CiLf** is global only within the Google’s universe, and does not make sense if the Google Docs system disappears.
Thus, decoupling data from platforms automatically leads to the requirement to create and maintain a Persistent ID system that is truly global. Unfortunately, we will not be able to use a system like DOI, since it is too narrow in its application and is not capable of handling trillions of objects. Plus, it's… yet another platform.
Of course, we will develop our Persistent IDs in full compliance with leading standards such as DID.
From a conceptual point of view, this raises several important questions:

- Will this system be centralized or not? (better not)
- What the Governance of this system will look like? (it will probably become the successor to DNS, and will be managed by ICANN, and we discuss it in the Governance section below)
- How IDs will be protected? For example, how can I make sure that no one can use my personal ID? (we will probably have to use cryptographic mechanisms similar to the IPR control described below)

We'll start answering these questions in Level 3, in the Register chapter. Indeed, we believe that the ideal mechanism for distributing and controlling Persistent ID is the Register, which is a successor to the DNS system, and will likely be managed by the same ICANN.
Here, at Level 2, we want to note that the introduction of Persistent ID is necessary not only because we have separated data from platforms, but also because we have the Long-term preservation task discussed above. The fact is that the data that humanity creates makes sense not only on its own, but also in the totality of all the links between them. And, of course, there is no point in solving the Long-term preservation problem separately without solving the Persistent ID problem,

because then all our URL links will fall apart.

IoT

Web 3.0 Data Space will significantly change the IoT market by making it completely open.
We can foresee the following cases:

Universal Digital Twins

It seems quite obvious to introduce PODs into the technological equipment of enterprises, so that any Digital Twin platform can control any devices. It will provide an enterprise to use one or few platforms of its choice to control all equipment in a holistic way. It also will raise competition between digital twin platforms, which will lead to more advanced functionality.

Transparency of equipment to partners

Access to the equipment will be given not only to the company that owns it, but also to insurance companies, banks, service companies and partners. E.g. if a bulldozer breaks down, the service company will know about it before the driver himself. Suppliers of building materials will change the delivery schedule, and the insurance company will pay all necessary compensation. The advanced Web 3.0 Data Space security will make sure that only authorized personnel of those partners will have the legitimate access.

Trillions of PODs

As eventually PODs will become a natural part of any device, from an excavator to a fridge, the number of PODs will reach hundreds of trillions.

Trust & e-Reputation

What is reputation? It is an accumulated pool of people’s opinions about a subject.
Indeed, we are already seeing how almost every platform shapes the reputation of the objects it works with, from hotels on booking.com to people on Facebook. And we understand that the value of booking.com is not only in the hotels presented there, but also in the volume of reputational information from millions of travelers.
If we expect to take back our data from the platforms, then it is natural to take back all the reputational information about us, our products and documents. This way, our PODs will begin to accumulate likes and comments from millions of users. For example, a notary's POD will begin to accumulate comments from all clients whom she has helped (or not helped). Let's take this notary as an example, and discuss how we can work with this information, and what the architecture of this solution should look like:

Calculation of e-Reputation vector

The notary's potential clients would like to compare her to other notaries. To do this, they need a simple indicator. Or perhaps several indicators (a vector): “value for money”, “reliability”, “professionalism”, “proactiveness”, etc. Thus, we can expect the emergence of ***e-Reputation platforms*** that will be able to calculate such a cumulative e-Reputation for this notary based on thousands of reviews from her clients.

All feedback must be signed

Of course, in such an important matter as assessing a notary, we cannot allow anonymous ill-wishers to ruin her reputation with several hundred negative reviews. This can be easily avoided if all users of the system are strictly authenticated and cryptographically sign their comments. Web 3.0 Data Space has such mechanisms. Therefore, anonymous likes and comments will be ignored when calculating e-Reputation

Weighted feedback

If you wrote an article about black holes, then the opinion of an astronomy professor should have a greater impact on the e-Reputation of your article than the opinion of a taxi driver. In another case,

when evaluating a car, the opinion of the taxi driver should be more important than the opinion of the astronomy professor. This suggests that in calculating the e-Reputation of any entity, the opinions of different participants must be weighed according to their own e-Reputation.

Protecting evaluator IDs

Perhaps not all of the notary's clients would like their real names to appear opposite her e-Reputation. Or, suppose that in your office the director offered to evaluate your direct superior. In both cases, you would want (a) your identity to be protected and (b) your own reputation to be taken into account.

Modern PET technology should help us in this matter. We will be able to hide participant IDs thanks to modern cryptography

Manipulation of e-Reputation should be punishable

If e-Reputation becomes an important foundation of society, we may expect certain people wanting to manipulate it. Consider possible acts of collective bullying or cancel culture.

The fight against manipulation will presumably be based on competition between rating platforms. Indeed, the quality of their work will influence their own e-Reputation, and, accordingly, the number of clients. And, of course, in the process of competition they will learn to identify acts of collective bullying and will be able to lower back the reputation of the participants in these actions.

In addition, anyone wishing to cheat the system will know that even if he or she cheats the system today, retribution may come in 5 years when the rating platforms learn to recognize this new manipulation technique. The fact is that all acts of participants are written to the PODs log (see details below in Level 3). Therefore, rating platforms will be able to evaluate participant behavior in a historical perspective. We believe that fear of delayed punishment will thwart attempts to manipulate the system. e-Reputation must be reliable.

What can be assessed?

We can evaluate anything: hotels, products, services, people, scientific articles and schools, platforms and services, politicians and their concepts, companies and cities, car brands and specific cars. We will make this world transparent and greatly limit the possibilities of deception.

How convenient will it be to give grades?

We already provide our ratings on all platforms. Of course, fierce competition between platforms will force them to collect user feedback more efficiently. They will learn to use voice assistants, AI, and will begin even to guess your opinion based on indirect signs. And if the platform does this poorly, it risks getting a “black ball” in its reputation.

To sum it up,

e-Reputation makes it possible to collect an unprecedented amount of auxiliary data on any person or legal entity. All the reviews, feedbacks, and assessments, after being carefully verified (as they are all signed) and weighted, can be transformed into a system of independent ratings we call e-Reputation. At last, it will be possible to quickly evaluate the trustworthiness of any internet user or any economic agent (from a plumber or a baker to a bank or an airline). e-Reputation will help build a true network of trust amongst people and companies and will completely transform the phenomenon of reputation in modern society, making it reliable and tangible asset.

IPR and Provenance

In order to provide IPR and Provenance control we need reliable mechanisms to prove (a) the authorship of digital assets, and then (b) control the assets changing hands (Provenance).

Web 3.0 Data Space solves both of these problems.

1. Solving the problem of authorship:

When creating a digital asset (such as a photograph), the Author will not only digitally sign it, but also have it timestamped by the notary (e.g. a standard CA from a PKI system). In the future, if a

third party claims authorship, then any IPR-platform will compare time stamps of two photographs from the competitors and identify the real author (who has the earliest timestamp). Please note that the losing challenger will receive a black ball in his/her e-Reputation, which will be taken into account in future cases.
As the problem of authorship is solved, we can move on to the problem of Provenance.

2. Tracking the Provenance:

When two parties want to transfer rights, they sign a contract using any IPR platform, put a time stamp, and save it on the two PODs of the parties. From this moment any IPR platform will derive the whole chain of such contracts, originating from the Author, and define who is the current owner of the asset.
As you can see, this is not a very complex technology, thanks to (a) the PKI system, (b) Persistent ID and (c) Data @ Source, i.e. at PODs.
We are confident that this solution will be of interest to projects such as C2PA (the Post-Platforms Foundation is a partner in this consortium).

Special case: already existing assets

We have discussed above how we can control IPR for new digital data. But in the real world there are quite a lot of objects that already existed before the creation of Web 3.0 Data Space. Consider an example of a painting, which is in the possession of a certain museum, with its ownership challenged by a number of people, claiming that it was stolen from them during WWII. We cannot guarantee an easy solution to this problem, but we can provide a number of steps that will speed up the identification of the real owner. Within Web 3.0 Data Space:

- Any experts involved in the provenance of this painting will be able to leave the signed results of their work (together with the e-Reputation of the experts) on the POD of this museum, linked to the painting forever. These examinations will accumulate with time, making the work of future specialists easier.
- Any claimant claiming that this painting was stolen from them will be able to post their claim on the museum's POD, and that claim will be visible to any experts working with the painting. The experts will see not only the claims, but also all the relevant documents, as well as the reputation of the claimants. If the experts find that these demands are unreasonable, this will affect the reputation of the claimants.

In this way, we create a transparent system that makes it easier for experts and applicants to work with objects with unclear IPR.

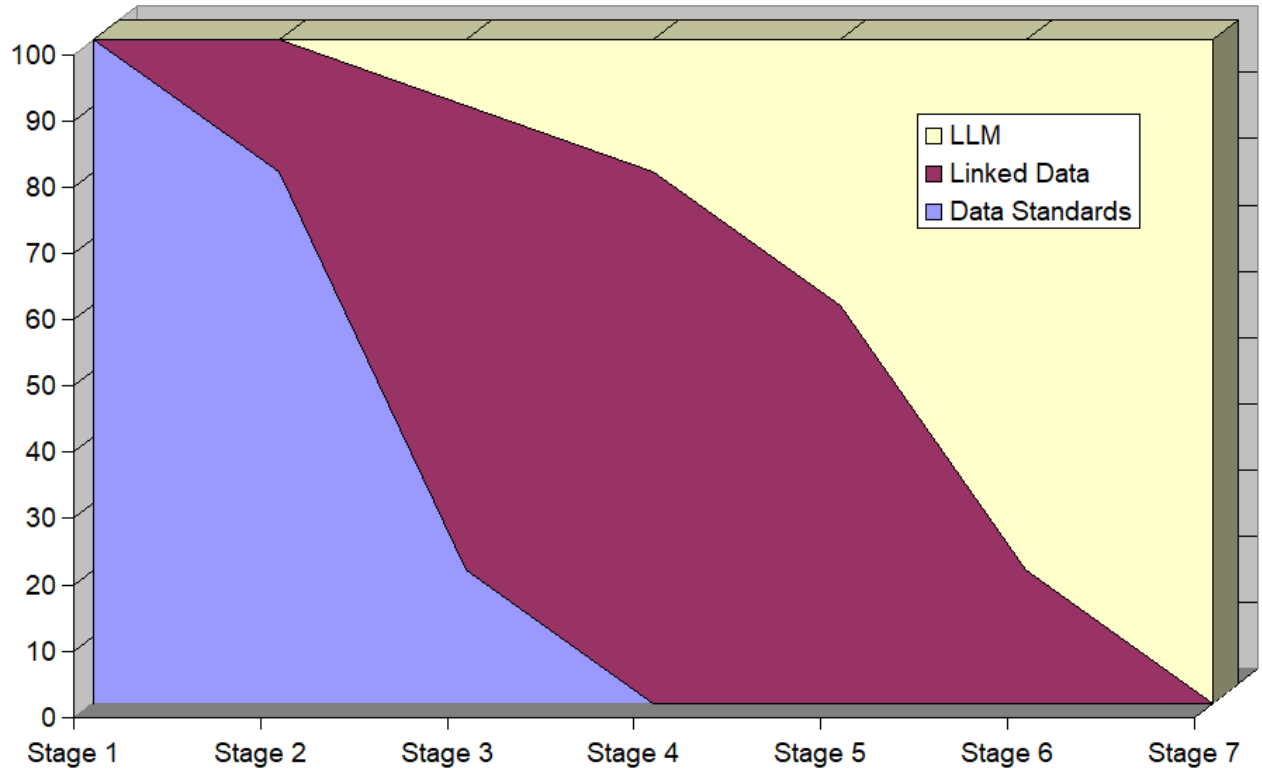
Data interoperability

Indeed, the scheme for separating data and platforms promises many benefits. But in nature nothing comes for free and the price for all these benefits is the need for different post-platforms to understand the data recorded by other post-platforms on the same POD.
At first glance it is hardly possible. But this is only impossible if you think that data can only be stored in strictly structured databases. Yes, at the dawn of the development of computer technology, working with tables and databases with clearly defined structures was the easiest way to work with big data. Rigid data structures were fully consistent with equally rigid algorithms like Fortran or Pascal.
But thanks to neural networks, we are moving away from rigid algorithms. Likewise, we are finding ways to move away from rigid database structures. The first step in this direction was Linked Data technology, proposed by Tim Berners-Lee. It allows us to start solving the interoperability problem: the post-platform that writes data to POD will wrap it into Linked Data structures (triads), well equipped with meta-information that allows the reading post-platform to understand the semantics of this data.
But Linked Data is just the first step in this process. If we compare the process of organizing

interoperability with understanding different languages, then Linked Data will resemble a dictionary that you can use to work with another language. However, a dictionary will not be enough for you to start speaking and understanding a foreign language. You need to feel it via practice. And this level became accessible to computers with the advent of LLM, based on the very same neuro-technologies. Chat GPT is the first and very effective example.
We expect LLM technologies to complement Linked Data and allow post-platforms to read and understand what other post-platforms have written on POD. Moreover, at a certain level of LLM development, as well as due to powerful competition between platforms, they will be able to “guess” the semantics and structure of the data so well that they will not need the writing post-platform to wrap the data into Linked Data at all (or partially).
Based on this, we can make the following important points about the organization of interoperability for Web 3.0 Data Space:

- Solving the interoperability problem for post-platforms is very similar to the process of people solving the problem of different languages.
- In this process, competition between platforms is the most important motivator for the effective use of technologies such as LLM.
- Responsibility for interoperability will increasingly be borne by those post-platforms that will read data, and not those that will write it down to PODs.

To sum it up, most probably we will see the following process of structured being displaced by the Linked Data approach, followed by the LLM approach.



PET (privacy enhancing technologies)

This is a new branch of cryptography that can be seen as an extension of the e-Voting task. PET allows to accurately answer statistically important questions like “*how many people in Germany order pizza at home after 18:00*” without revealing their names. This technology has a huge expected demand, because such statistics are needed by economists, politicians and society as a whole. On the other hand, we do need a strong system for protecting the privacy of citizens.
This topic requires deep discussion among specialists, and we are in contact with organizations that

deal with this, for example TNO.nl. As with other technologies based on the use of cryptography, it can be done only with use of the PKI and Persistent IDs, without which it is impossible even to approach this topic.
Of course, we will have to overcome citizens' disbelief in this technology. After all, in order for it to work, citizens will have to explicitly allow their data to be used, with the expectation that their names will not be revealed. It will take years for citizens to trust the reliability of this technology, but over time it will happen.

Economic Inclusion

Every person has many capacities. But the modern world offers him/her only one job, 8 hours a day. The reason is the dominance of companies that have resources, reputation, and markets, and they use people as elements of their businesses.
Although we see an increasing number of one man companies, one person is still not capable of being a full-fledged economic agent, and always loses to companies. First of all, due to the fact that the company has a reputation and a brand, while one man company does not.
Web 3.0 Data Space can change this situation.
Within Web 3.0 Data Space, each person will be able to declare all his/her abilities and wishes on a POD. And after that, all competing platforms will begin to sell this person's capacities. But their competition will lead to more than just selling that person to customers, as fiverr does. At the next stage the post-platforms themselves will become customers: they will begin to create virtual businesses that will begin to combine the abilities of different people, creating ***virtual companies***.
For example, a post-platform might bring together people who can cook and people with bicycles, and create a company that delivers food to offices. Each of these virtual workers can work in several of these virtual companies at once. Numerous post-platforms will coordinate micro-business activities 100% seamless and hassle free for millions of people, freeing them from need to work all their lives for one business.
As a result, people will be able to actively sell the entire range of their abilities simultaneously, adding new abilities in the process of life-long-learning.
In this process, of course, the e-Reputation of people will play a major role. E-Reputation will allow them to change countries, companies, industries, and each time they will leverage the trust created in the previous stages of his/her career.
As a result, the Web 3.0 Data Space provides maximum economic inclusion at personal level, helping people to evolve from consumers to ***prosumers***. Starting with the control of personal data by its owners, the Web 3.0 Data Space enables further self-determination and helps people fully realize their creative and economic potential.
For SMEs, the empowerment effects are quite similar: on one hand, the Web 3.0 Data Space lowers or even completely removes entry barriers in some niches currently monopolized by platforms and corporations, and on the other, it grants startups virtually free access to the widest user-base, with few or no marketing activities required. This global data crowdsourcing phenomenon will also give birth to numerous next-generation services and will make the entrepreneurial space incomparably more diverse and inclusive.

Eliminating fakes

The solution to the problem of fakes is very similar to the solution to the trust problem described above. The most reliable way to get rid of fakes is to establish total transparency, which will not allow bad guys to deceive opponents.
Let's try to look at several examples and the solution architecture for each of them, based on the biz-cases presented in the Challenges & biz-cases.

Fake news (Biz-case 1)
In this case BBC receives a news (a photo of a plane crashing) and wants to assess whether it might be true before publishing it.
The very first thing to do in ordinary (non-digital) life is to find out the reputation of the author of the news. And, if this reputation is high enough, then BBC can begin to discuss publication.
In the Web 3.0 Data Space ecosystem, we will do exactly the same as in real life: BBC will be able to check the e-Reputation of the author with help of any relevant post-platform. If the photo was received from a baker from a small village, known for the quality of his products and a good reputation from his fellow villagers, then you can trust him. If this is a student known for his practical jokes and knowledge of Photoshop, then BBC should be more careful with his photograph. It should be noted that the PET system will allow news authors to be “anonymous”, yet at the same time use their e-Reputation.
If the author passes the e-Reputation barrier, the Web 3.0 Data Space system will provide many opportunities for double-checking the news content itself due to the high transparency of the system. For example, you can easily check correlations between similar news items.
In this way, we can completely get rid of fake news, published, for example, by special teams from Russia and other authoritarian countries that spread fake news about Ukraine or interfere in the US elections just to damage certain communities. Their authors will never be able to pass the e-Reputation barrier.
Fake parts(Biz-case 2)
In this case we see a plane serviced somewhere in Hong Kong. It’s General Electric engine gets a fake turbine blade. It is clear that with a blade price of ~€50k, there is a very strong temptation to install a fake part. But when making a fake blade, you need to engrave ID on it. If this ID was never produced by GE, then this part cannot be supplied, because the fraud will be detected immediately. The only way to do this is to engrave one of the numbers that GE has actually produced in the past. Let's assume this is our case, and the part received a duplicate number. In the Web 3.0 Data Space system, any fake parts control platform will be able to interrogate all PODs at GE engines on the planet and compare their blade numbers. This will allow to quickly find blades with duplicated numbers and ask questions to the service centers that supplied them. Thus, the Persistent ID system and total transparency of the ecosystem make it impossible to produce and use fake parts in any industry.
Fake data at contracts negotiations (Biz-case 3)
With every prospect business partner, you always want to find out who it is, to find out what projects it did before you. Web 3.0 Data Space allows you to do both:

- The partner’s reputation is available to you through the e-Reputation mechanism, which we discussed above.
- Using any reputation checking post-platform, you will be able to view all previous contracts and clients. Even if these clients do not want to disclose their IDs, you can always look at their reviews on the relevant contracts.

Thus, unscrupulous partners will no longer be able to perform projects poorly and hide this when concluding new contracts.

e-Money

The Post-Platforms Foundation offers a better alternative to both current (central)bank-centric fiat currency system and to blockchain-based cryptocurrencies.
In the Web 3.0 Data Space, we place the ledgers to every POD of an individual or of an organization, thus creating a truly distributed network of ledgers. Every monetary transaction between people/organizations will be recorded on two respective ledgers (on PODs) of the two parties involved, and it will be signed/timestamped by trusted authorities (e.g. CA from PKI). Unlike

the bank-based system, e-Money require no “bank account”, as the money is transferred directly between parties, just like we transfer cash. This scheme will allow fully P2P direct payments between individuals and companies, with total security, transparency, and traceability, yet with no commissions or fees and with no banks involved.
The e-Money is totally based on the Advanced security of Web 3.0 Data Space (secure unattended PODs, e-Passports/PKI).
Please note that this system:

- much simpler than bank-based: (a) no need for bank accounts any more, (b) people can use the very same e-Passport
- works with any types of money
- free
- reliable
- controllable for all relevant authorities, e.g. tax authorities.
    - at the same time, people can hide the specific transactions from authorities, who only need to know that it was a legitimate transaction
    - actually, PODs will keep not only transactions, but all relevant invoices, contracts, negotiations, which provides economists and authorities with very deep linked data for analysis, yet, still protecting privacy via PET

Reducing Bureaucracy: No more government registers

We discussed this biz-case with the Cadastre of a European country. Their main problem is that the Cadastre database is never 100% up to date. It is always late for reality and there are always errors when transferring data from notaries or Cadastre engineers to the Cadastre Register.
Together with them we have discussed the solution: if we keep all the records on the PODs of houses and land parcels, then both problems are solved automatically:

- There is no data delay because the data is not transferred anywhere, but kept at origin.
- There are no errors in copying because there is no data copying.

As a result we get a 100% correct Cadastre data structure that lies remotely on millions of PODs.
This solution leads to an unexpected effect: the Cadastre will not need a database (the Register) at all. All data is securely kept at PODs and it could be reliably reached. E.g. when a Cadastre officer will need to know amount of buildings with metal roofs, any suitable platform will scan all PODs and return the number. The Cadastre office will shrink significantly to a team which will issue rules and determine policy.
As a result, in this Cadastre biz-case we will have better quality of service at a lower price. Actually, no government organization will need databases or registers any more. This will significantly reduce the role of the state and size of bureaucracy. For example, in order to register a marriage, you will not have to go to the city hall; it will be enough to sign a marriage contract between two people.

Transparency and Ideal Capitalism

As every economic actor is represented by their POD, we will have a world where customers find products, services and digital assets almost instantly. This will be facilitated by competition between platforms. Thus, when any new product appears on the market (at the moment it is published on a company’s POD), it will become known to all sellers who will constantly scan the Internet using search engines. Therefore, a new pencil factory in Bangladesh will not need a marketing campaign: its pencils will appear in all online stores next moment after the description of these pencils appears on the company's POD. And the very next day trucks will start stopping by to pick up goods, as truck owners have their capacities published on their PODs and the buyers can easily hire them.
It will introduce ideal capitalism with perfect competition:

- all players know all the information
- the system is completely flat
- everyone earns fair revenues, without monopoly/asymmetric information yield.

Many people complain nowadays that capitalism is broken. We argue that capitalism is fine. It was the platforms that temporarily hacked it and started earn unfair profits. But once we return the source of their wealth, the data, to people and companies, everything will fall into place and capitalism will be even better than it was, thanks to the amazing transparency that the Web 3.0 Data Space brings.

As all the information is available, it makes no sense to spend resources on advertising and marketing. Instead it will make sense to invest in quality goods and services, because the only reason why people will buy goods will not be the advertising, but other people's reviews about the quality of these goods (e-Reputation).

e-Voting

Electronic voting can guarantee that:

- The one who counts the votes does not know who voted for what, and knows only percentage of legitimate voters participated.
- The one who voted knows that his/her vote was counted correctly.

The electronic voting protocol is quite complex, but can be implemented using PET. The main challenge to secure voting system is not the technology of a particular protocol, but our ability to ensure control of the users' identities. And this is the organizational innovation which we discussed above, in the section Strong identity management.

The implementation of the e-Voting system may allow us to start experimenting with advanced democracy methods in some countries/municipalities, like:

- The transition from representative democracy to direct democracy.
- The ability to implement elements of meritocracy, for example, taking into account the e-Reputation of citizens.

Improved Democracy

Web 3.0 Data Space will help to improve democracy in several types of countries, with different levels of democratic development:

- in developed democracies (e.g. USA), Web 3.0 Data Space will allow:
  - organizing fair elections with reliable results
  - politicians to launch large projects for periods longer than their time in office, leveraging e-Reputation of experts, thus overcoming the short-term nature of democratic decision making;
- in weak democracies (e.g. Hungary), Web 3.0 Data Space will allow:
  - counter the lies of crooked politicians;
  - more accurately reflect the real reputation of politicians, especially populists;
  - try advanced methods as meritocracy to fight populism;
- in autocratic systems (e.g. Russia), a high level of security Web 3.0 Data Space will allow
  - citizens to organize resistance to autocracy and unite against it without risk to be imprisoned;
  - to easily organize alternative to official voting to demonstrate the real level of support to the dictator.

Overall, the transparency, security, trust and reputation mechanisms will act as the social glue between people and communities that strengthens a democratic society.

We are confident that we do not yet fully understand all the effects of Web 3.0 Data Space on the

development of democracy, and here we need the help of sociologists and specialists in political science. We want to start this discussion because the Web 3.0 Data Space gives us, for the first time, serious mechanisms for new ways of organizing social systems.

Environmental (Green) impact

Web 3.0 Data Space will reduce Carbon dioxide emissions in several ways:

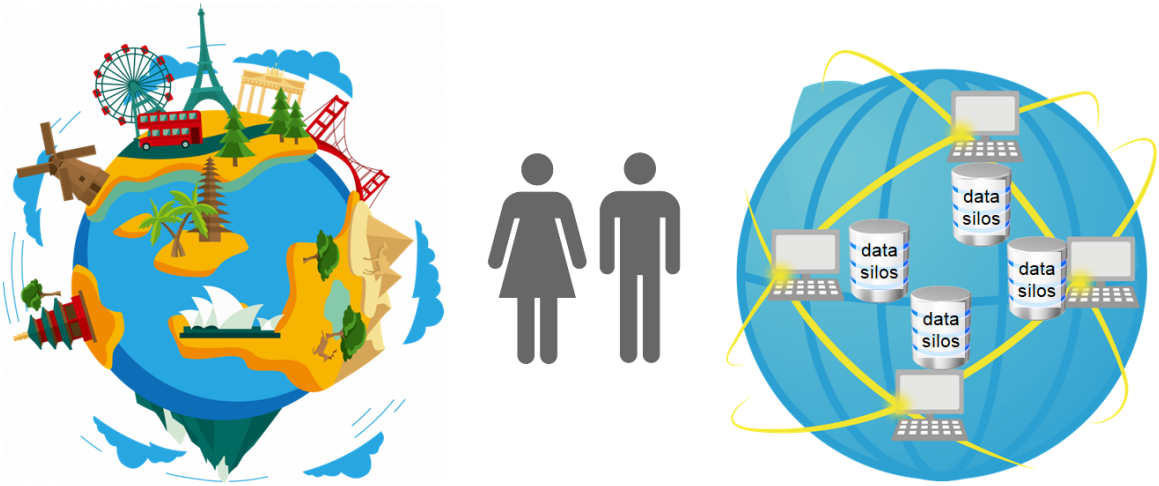
- First of all, the Web 3.0 Data Space is blockchain-free. At the same time, it will totally replace all typical blockchains, both in e-Money and other applications. Bitcoin alone is estimated to consume 127 terawatt-hours (TWh) a year — more than many countries, including Norway. Elimination of blockchain alone is a great support to Green agenda.
- Secondly, we get rid of hundreds and thousands of copies of the same or similar databases (so called data silos). Whatever will be the total number of PODs, they will use less data clouds capacity than multiple copies of the very same data in different combinations plus all relevant archive and backup systems. As we have dozens of copies of the similar data in private and professional life, we definitely will reach the 2x economy effect in storage/electricity use.
- Thirdly, the Web 3.0 Data Space optimize various aspects of both business interactions and everyday life in general, promoting better logistics, smarter homes and vehicles, and tighter links with local communities.

How it all affects the Internet

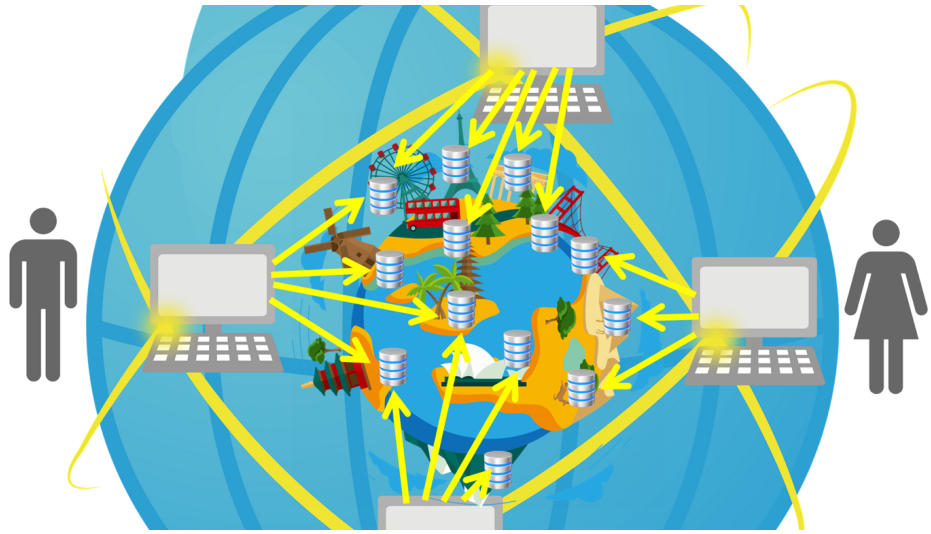
In previous chapters we looked at the technical and organizational aspects of the Web 3.0 data space.
In this chapter, we would like to look at the perception aspect of the Web 3.0 data space, that is, to understand how should we perceive this system as a new stage in the Internet development?

New Essence of the Internet

The Internet was originally built as a system for reliable communication over long distances.
With the advent of Web 1.0, for the first time we realized the ability to “look” at company websites from afar; we perceived the Internet not as a medium for transmitting data, but as an opportunity to “look at something remotely”.
The advent of Web 2.0 introduced us to the powerful effects of aggregating data from many businesses and people at once (to zoom out and deal with complexity), but it created many problems with data ownership.
Finally, Web 3.0 combines the power of Web 1.0 remote access and Web 2.0 aggregation. What does this give us?
Let's try to depict this. The following picture shows the current Web 2.0 world, which has created a copy of the real world, or rather, many copies (we call them data silos) that stand apart from the real world.



Web 3.0 Data Space brings these two worlds together and merges them, allowing each entity (person, company, thing) to have its own POD, which stores the single and ***original*** copy of that entity's data. And then all information systems deal precisely with these original data at PODs. Thus, we are turning the Internet from a separate standalone entity into an extension of the real world. The Internet seems to dissolve into the real world, in full accordance with the concept of the 4th Industrial Revolution.



Given the ability of the Web 3.0 Data Space to store data indefinitely, we get a world in which the Internet turns from a separate data transmission system into a digital avatar of our world, preserving the memory of it for centuries.

Reflecting on Web 3.0 Data Space: an “Internet Frontier”

A very interesting picture you get if you look at the emergence of Web 3.0 Data Space from an anthropological point of view. This is best demonstrated by comparing the development of the Internet with the American Frontier of the 18th to 20th centuries.

American Frontier

In the context of this discussion, American Frontier has gone through 3 important stages:

Stage 1. 18th century. Pioneers.

Nobody knows anyone and communities are very small. Colt solves all problems. This only worked in a primitive economy and society. Once the railroads and the big cattle and other companies came along, it couldn't work anymore.

Stage 2. 19th century. The power of corporations.

At this stage, the police and administrative control of the communities were concentrated in the hands of corporations, cattle breeding and railways. They even gave out their passports. They had their own prisons. But at some point, people realized that the railroad police is essentially… bandits. And it was time to change this.

Stage 3. 20th century. Public power.

The final echo of this transition was the fragmentation of the Standard Oil company. From that moment on, corporations stopped ruling America.

Internet Frontier

Let's now look at the similar stages of Internet development:

Stage 1. 1990-2000. Pioneers.

Nobody cares about anything. Complete anonymity and freedom. This worked until big business came to the Internet. With its arrival it became impossible to live like this.

Stage 2. 2000-2025. The power of corporations.

At this stage, all power was concentrated in the hands of corporations producing platforms. They even introduced their passports (Google, facebook and MS). Facebook even had a prison where they disabled undesirable bloggers for several months without trial! But at some point people realized that data in the hands of corporations turns them into digital slaves. And now it's time to change that.

Stage 3. After 2025. Power of the people.

Web 3.0 Data Space creates a world where passports are no longer issued by corporations, and all data belongs to those who created it. We are giving power back to the people.

Web 3.0 Data Space and AI

Web 3.0 Data Space will be the most crucial component for future AI systems, as any AI needs data for its training and operation. At the time of writing (Dec 2023), Chat GPT, the most advanced AI system was not capable of answering questions that required modern context. This is partly due to the fact that it was trained on outdated data, literally silos of data. In the same way, cows are fed silage in winter time.

Web 3.0 Data Space will be able to give AI systems fresh feed, the most modern and relevant, from billions of PODs.

In addition, the Web 3.0 Data Space can provide legal fodder for AI. We know that ChatGPT uses books, web pages and other open data. But where does it get the dialogues and discussions? Could it be that Facebook sells it? We don't know. But we know that with that kind of money the risk is high. Web 3.0 Data Space can enable each person to decide whether she is ready to give (or sell) her materials for AI training, anonymized or not.

Another unique feature of Web 3.0 Data Space is that it will provide AI with well-connected semantic data rather than just raw data. That is, the quality of this material will be much higher than just some texts from books, as it is the links and semantics which make sense out of any data.

To summarize, the Web 3.0 Data Space will enable AI:

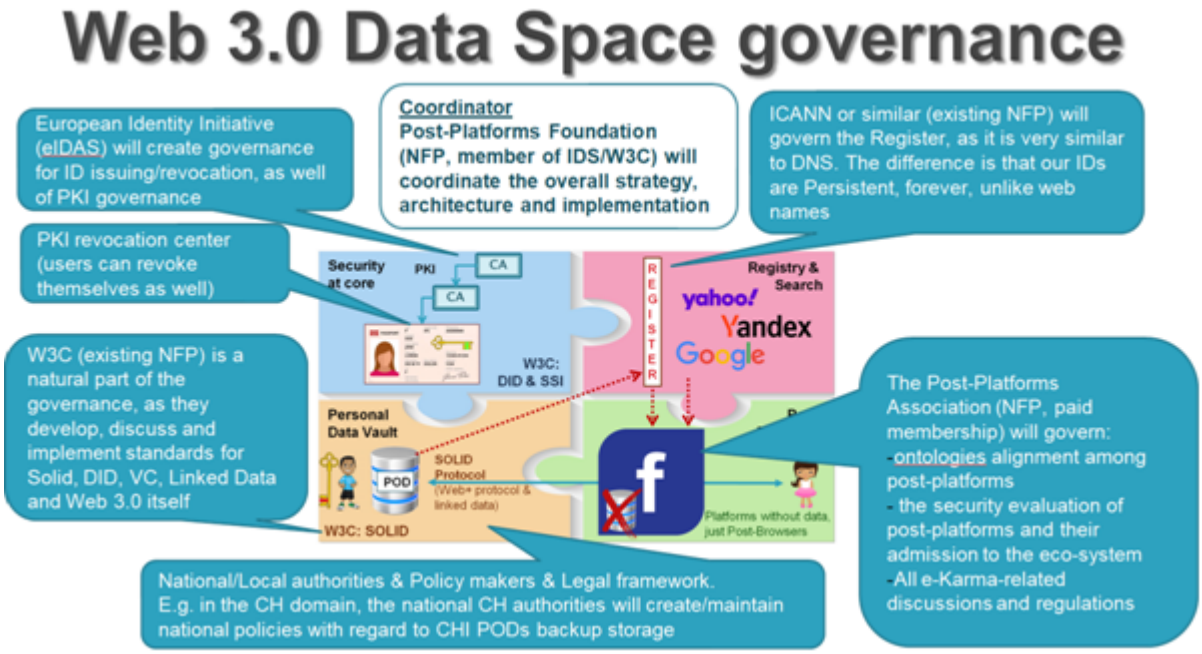
- with much more material for training, providing literally the whole world;
- fresh & up-to-dated';
- completely legal, with explicit consensus of the authors
- semantically rich and (thanks to Persistent ID) well interlinked.

Web 3.0 Governance

The Governance of the Web 3.0 Data Space is one of the most important questions. We would like to see it:

- independent from any few corporations, governments and other powers
- as much as possible based on the proven governance in Web 1.0 and on proven governance systems in other domains, e.g. Industrial Associations.
- sustainable.

Below we present the Governance which answer these requirements.
When we discuss the Governance, we need to start from the analysis of the architecture of the system which we are about to organize. The architecture of Web 3.0 Data Space (as presented below in Level 3) consists of 4 major elements: PODs, post-platforms, the Register and the Security. Therefore it makes sense to start from it, asking ourselves: “How all these elements are governed?”



At the moment we see the following elements of the Governance:

- Standards (we suggest to copy it from Web 1.0 and use W3C)
- To address the governance of the Register just like we did with DNS, via ICANN
- To control the post-platforms we suggest to use the proven mechanism of Industrial Association, just like associations in agriculture or in automotive.
- We need a governance over PKI, and we suggest to base it on numerous commercial players, similar to the current system of issuing SSL certificates (just make it more secure)
- We definitely need to land it on the national legal frameworks, and we will need support from EU parliament
- We may need a temporary body to orchestrate it all.

Below you will we will explore it to some extent.

Standards

We will need several standards in this ecosystem, for example:

- Web 3.0 Protocol(s) (related with Solid/IDSA)
- E-Passport (related with VC, eIDAS)
- Persistent ID (related with DID)

To develop standards, we will have to choose one of the following paths:

- ISO
- IETF
- CEN (European standards)
- W3C

Of all these organizations, W3C seems to be the most suitable structure for the following reasons:

- Web 3.0 Data Space is the successor to Web 1.0, which is managed through the W3C
- W3C has existing committees that work on the Solid protocol as well as on identification (DID) and authentication (VC)

Still, the choice of the path is subject for further discussion. E.g. we see that IDSA chose ISO, and we will discuss this choice with them.

Control over centralized structures (Register): ICANN

As we will discuss in Level 3 section, the Register is very similar to the DNS. And just like DNS, it is a centralized structure that requires centralized management. Accordingly, we either need ICANN itself, or we will have to create a structure similar to ICANN. We're very pleased that ICANN has demonstrated a strong track record over 30 years, and that experience will be very useful to us here. We understand that a centralized Register carries risks. Perhaps during the architecture development process we will be able to somehow mitigate this risk.

Regulating post-platforms: The Post-Platforms Association

The Web 3.0 Data Space project will create millions of post-platforms that will have to meet certain security requirements, harmonize certain behavior patterns and standards. It will be a very vibrant world of many commercial and non-commercial players.

As in any industry, the behavior of players must be regulated by the relevant association. And in this sense, the post-platforms industry is no different from agriculture or the automotive industry. After all, in both of these industries there are corresponding associations that regulate the lives of their participants.

Thus, all our historical experience suggests that the creation of the Post-Platforms Association is a completely natural and most reliable step for streamlining the activities of post-platforms.

We expect that post-platforms themselves will create such an association as the first post-platforms appear.

PKI: Numerous Commercial players

Typically, passports are issued to people by their states. And then every passport says which country you belong to. Having a passport without a country is considered something wrong.

We expect that in the world of Web 3.0 Data Space we will begin to issue e-Passports that will not be tied to any country. In similar way, e-Passports from Facebook or Google are also not tied to the country, and we somehow live with it.

We expect that initially our e-Passports will not be perceived as real passports, and thus we will be able to avoid government interference in the deployment of the entire PKI ecosystem.

Who will then issue e-Passports if not the governments?

It seems to us that the most convenient partners are banks and mobile operators, for one reason: they already have local offices where people can come to request an e-Passport (in cases where we cannot issue e-Passports online). For e-Passports with a highest degree of security (if different levels of security will be used), existing notaries are quite suitable. In any case, it is important that the number of commercial players be large enough to keep the cost of obtaining a passport low enough via competitions.

We expect the cost to be ~€5 for the cheapest e-Passports, which is much lower than the current prices for SSL certificates (about €100). Our confidence in a lower price is based on the economy of scale, since the number of e-Passports will exceed the need for SSL certificates by several orders of magnitude. E.g. our partner, Digidentity, the Dutch provider of certificates and inventor of Dutch DigiD government ID system, has a price ~€6 per certificate, and we are still far away from the

economy of scale..

Landing on the legal framework

Our entire system with IPR control and security sub-system is meaningless if the users cannot come to the courts with evidence of their position. Therefore we need the legal infrastructures of all states to accept for trial the evidence that users will present, for example, LOG files.
We do not think that this process requires any special legislation. Most likely, the courts will begin to accept our evidence quite naturally, just as they accept other technical evidences.
However, support from the European Digital ID program is likely to be helpful here, as well as support of European Parliament, EC and local governments. We definitely will discuss it with them.

Roll out strategies

This document primarily addresses the technical feasibility of Web 3.0 Data Space and its architecture. System deployment is beyond its main scope. However, we will touch on this topic a little to outline the general contours of the process of deploying Web 3.0 Data Space.
Please note that roll-out strategies address the issue of “how to move a system from a Web 2.0 state to a Web 3.0 Data Space state”. It is important to understand that it makes sense to discuss it only if we are sure that Web 3.0 Data Space system will be stable, which is achievable only if it meets the needs of all stakeholders. We dealt with this issue above when we examined numerous Biz-cases, which reflected the needs of those stakeholders.

Roll-out Approach: ready-to-use biz plans for certain industries

There is a number of types of commercial corporations which suffer from Web 2.0. The Post-Platforms Foundation team have commercially viable business plans, discussed with the relevant market players. These plans leverage specific situations in every industry. They are developed for the following industries:

- **Accommodation market**, where hotels are paying ~20% to the booking platforms, while in the adjacent airline ticket industry (where the Web 3.0-like architecture exists for 40 years, thanks to Amadeus) the platforms’ margin is around ~1%
- **Mobile operators market**, where the power of mobile operators (and their desire to monetize their clients via upsales of PODs, MobileID and e-Passports) allows to launch a mass deployment of PODs among citizens
- **Platform-related Education market**, where the new services will provide giant leap and billions of dollars to the pioneers.

As we will discuss the Biz-cases with many other domains we expect, together with the IDSA community, to develop biz plans for those domains.
These plans are openly available.

Roll-out Approach: generic Web 3.0 Data Space introduction in the enterprise sector

Deployment in corporations could be done in different ways. We will consider only one scenario. Before we do it, we would like to clearly articulate a couple of misleading interpretations of the role of corporations in Web 2.0 troubles and in the transition into Data Space.

Typical mistakes we do when we think about corporations

We see two typical mistakes we do when we think about corporations and their transition to Data Space.

Mistake #1. Corporations are not guilty of our problems with data. They are also victims of Web 2.0 platforms monopoly.

There is a common mistake that we do not distinguish industrial corporations (e.g. BMW, Accor or KLM) from corporations which provide the platforms services (like Booking.com, SAP or Oracle). We would like to note that the industrial corporations are suffering from Web 2.0 even more than citizens:

- They suffer from vendor lock-in, as it is impossible to change SAP into something else
- They suffer from data silos, as they use several hundred platforms (usual number is ~800)
- They suffer from difficulties in educating their stuff
- They suffer from Chinese walls between them and suppliers, clients and partners, and they still send invoices as PDF attachments to emails.
- They suffer from losing their data when some of platforms leave the market, eventually.

That's why we're a little surprised when we hear that “corporations are taking our data.” Corporations don't take anything. It is the platforms that take our data and the data of corporations as well. It can be that this confusion is originated from the fact that in many cases industrial corporations develop such platforms themselves. First of all, this is not so any more, they mostly buy platforms as SaaS or similar services. And, secondly, even if they develop some platforms, in such cases they suffer even more, as such “internal platforms” have only one client (the corporation) and experience zero competition. As a result, it takes years (!) to implement any new feature, as the development team is rather relaxed and “cares for the quality”, therefore they are very slow in any development. It creates enormous tension

Mistake #2. Industrial Corporation should implement Data Space projects themselves

So, how can Web 3.0 Data Space be implemented in corporations? What should a corporation actually do to achieve this?

Technically, nothing.

A corporation does not need to write software, implement protocols, redesign databases or work on ontologies.

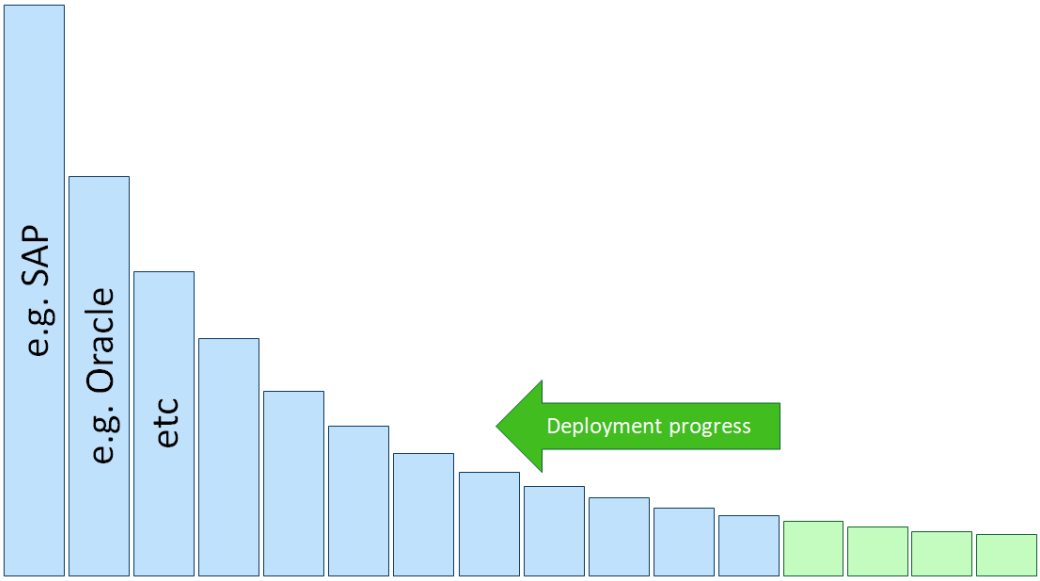
The only party which should dive into technological re-design are those 800 platforms whose services the corporation uses.

The corporation's task is to motivate these platforms to make the transition to post-platforms. Therefore, next we will try to figure out how this can be done.

Yet, the only exception is those platforms which were developed by the corporation itself for internal purposes. Then their project leaders have to redesign their platforms into post-platforms (we discuss in Level 3 chapter how to do it). When done, the project leaders will discover that their own internal platforms are not in a luxury position of “single customer and no competition” any more: their own corporation will have a choice among competing post-platforms, and such internal post-platforms will have to compete to survive!

The roll out plan: Step-by-step conversion from platforms into post-platforms

Those ~800 platforms used by a typical corporation, they have different value (or associated costs). If we distribute them by this value, we will get something like this picture.



Platforms used by a corporation, rated by their value

A possible deployment scenario would involve us taking a dozen platforms on the right end of this spectrum and incentivizing them to become post-platforms (green segments). This shouldn't be very difficult to do, because these platforms are either dependent on the corporation, or even developed within the corporation. This conversion assumes that:

- Their users and/or relevant departments will receive PODs
- The platforms themselves will most likely use the Web 3.0 Connector to connect to the system fast
- We will deploy a PKI system (if we are the first to implement Web 3.0 Data Space) for users of these platforms

Once this step is completed, we will be able to evaluate the complexity of this transition and its economic effect.

If (hopefully) this transition is successful, we will be able to connect the 11th platform, then the 12th and so on. As the number of participating platforms expands, the economic, social and other effects will only increase due to synergy effect as all of them will use the same data, users, search engines and other Web 3.0 Data Space services (see the section Web 3.0 services for post-platforms in Level 3 below) .

It is very important to note that in reality the large platforms on the left side of this spectrum will not wait until they lose their market. We expect them to join the project in the early phases as well, and the actual deployment will not only be from right to left on this "platforms spectrum". Proof of this is the fact that when the Post-Platforms Foundation brought together 32 partners to participate in the largest European ECCCH grant (€110M in total) in the field of cultural heritage in the summer of 2023, the two major participating platforms in cultural heritage decided to join our consortium, namely Axiell and Ex Libris. Both platforms said they understood the need to move to the Web 3.0 Data Space and would like to lead the change rather than being left behind in this major transition.

The roll out plan: balancing off Copies vs Data @ Origin

Usually, when we talk about PODs, we assume that they are the custodians of the Original Data, not copies. After all, we declared our main principle – Data @ Source – at the very beginning of the document. Without this, the entire Web 3.0 Data Space system ceases to make any sense.

But in most cases, when discussing the first scenarios for deploying a system, you may really want to use POD for... copies of data.

Several projects already faced this need:

- the government project Athumi.be, whose task is to provide PODs to citizens of Flanders.

- the startup Linckr.nl, which operates in Real Estate.
- the startup Digita.be in their case with BMW.

Indeed, if we are discussing a system for Real Estate, it would be good for the client's POD to store data from the Cadastre, from the Bank and from municipal authorities. In this case, her POD will contain enough information to attract major platforms to use this POD. We reasonably assume that from the very beginning of the project, not a single serious platform used by banks or Cadastre will want to keep the original data at our PODs.
Therefore, we will want to get copies of data from all these organizations in order to somehow fill our POD with initial data.
Isn't this dangerous? Does it compromise the Data@Origin idea?
Yes and no. As long as we have a good understanding of what is original information on our POD and what is (possibly an outdated) copy, we can work with it.
What will happen next?
Then we expect the participating large platforms of banks, insurances, notaries and Cadastre to go through the following phases with certain biz-cases:

- Phase 1 biz-case.
  As a platform, I keep all my data in the internal DB, but I do not mind this data to be copied from my DB to the citizens PODs. The project initiator (e.g. Athumi) is responsible to periodic update of PODs, using my API.
- Phase 2 biz-case.
  As a platform, I will start posting updates on PODs myself via Web 3.0 Protocol, because many stakeholders already use PODs and I want my data to be as updated as possible, to maintain my reputation.
- Phase 3 biz-case.
  As a platform, I would like to be notified when other platforms update data on PODs so that I have most up-to-dated information in my internal DB.
- Phase 4 biz-case.
  As a platform, I discovered that at this stage it is easier to become a full-scale post-platform (as I have made it half way already) and start using all other services of Web 3.0 Data Space, like users e-Passports, e-Reputation, search engines, Persistent IDs, IPR control etc.

Thus, if any platform begins to use PODs partially in the beginning, will gradually turn itself into a full-fledged post-platform simply because it is more reliable and convenient to work with information at PODs together with other post-platforms.
Thus, using PODs as a copy of the data is an acceptable first step in deploying the Web 3.0 Data Space ecosystem.
The key here is that the project managers and participating platforms have a good understanding of the kind of the game their are about to play.

Roll-out Approach: Government projects

There are domains where government can be a more effective partner than commercial corporations in deploying the Web 3.0 Data Space. For example, in these domains:

- **Cultural Heritage**
  In this area, the state is unrivaled. An example of the approach is the application of the Post-Platforms Foundation and 32 partners for an ECCCH grant of €25M (full amount €110M), which requires the creation of total access of any systems to all cultural institutions of Europe. See the details of our approach in this video.
- **Smart Cities**
  A city is managed by public office, yet it is essentially a large enterprise, and the logic we described in the previous section (Roll-out Approach: generic Web 3.0 Data Space introduction

in the enterprise sector) applies to it. Such a project can be initiated only by governments. A good example is the Athumi.be project in Flanders.

Rolling out Web 3.0 Data Space Infrastructure itself

In previous discussions, we have focused most on turning platforms into post-platforms because this is the most challenging step of deploying Web 3.0 Data Space. Indeed, few platforms will want to be pioneers, and our main problem will be their motivation.
However, once we have brought existing platforms into the world of Web 3.0 Data Space, we must provide the complete set of functions of this “operating system”.
In this section we will review the roll out of the elements of the Web 3.0 Data Space ecosystem:

- PODs
- Register
- Ontologies
- PKI
- Web 3.0 Connector
- Search Engines

If you want to to know more about these elements, we present them in details in the Level 3 section below.

Roll-out of PODs

In our current understanding, the deployment of PODs among people and organizations appears to be a consequence of the deployment of corresponding platforms. For example, in the ECCCH project (described in the previous section), when the first 5 platforms in the field of cultural heritage decide to become post-platforms, then all their museum clients will receive a proposal “*would you like to switch from storing data on our platform to storing data on your POD, because this gives you a number of benefits?*” In this case, museums will gradually learn the difference and eventually switch to PODs, and this process will go smoothly and comfortably for the entire ecosystem.

Roll-out of the Register

Presumably, the deployment of the Register will fall on the shoulders of the first project in the field of Web 3.0 Data Space. We believe it is possible to make the first Register simple and cheap, and improve its technology further. The only thing that is important to do from the very beginning is to make serious architectural decisions about the management of the ***Persistent IDs space*** and make sure that its governance is done correctly and is not in the hands of commercial players due to its “centralized nature”.

Roll-out of Ontologies

Perhaps in the first stages we can try using existing ontologies like schema.org and then see if it works. This element is quite important (after all, the failure of ontologies will block the system from working), and will require special attention from the governance point of view, but gradually we will work out a solution. In addition, the emergence of LLM systems will reduce the level of dependence of post-platforms on Ontologies.

Roll-out of the PKI

The first project will also have to solve this problem. We believe it can also be done quickly & simply, since all the necessary technologies already exist, and we only need to determine the standards that we will use. With regard to the PKI deployment we can probably count on players such as mobile operators, banks and notaries, for whom it will be “yet another product to sell”,

taking advantage of their reputation (!) and the mass presence of physical offices. Additionally, the lowest level of trust certificates can be issued online with the help of existing players in the PKI market. For example, in the Netherlands, our partner Digidentity (authors of the national DigID system) is technologically ready for this role.

Roll-out of the Web 3.0 Connector

Most probably, the first Web 3.0 Connectors will be developed within the framework of the first project, and we do not see any fundamental difficulties here. As always, the first solutions will be quite primitive. Competition in the commercial Web 3.0 Connectors market will then solve the quality problem.

Roll-out of the Search engines

This is hopefully the least problematic part of the ecosystem because the industry is already well established and because it is a highly competitive market. It will quickly adapt to the needs of post-platforms.

Conclusion on Rolling out of the complete Infrastructure

We have all reasons to believe that the most critical is only the first step: motivating the first few platforms to convert to post-platforms. It is this problem that the first projects in the field of Web 3.0 Data Space should pay attention to.

What kind of team is required for rolling out the Web 3.0?

Our western culture likes specialization. We used to the projects which require either AI specialists, or Linked Data specialists etc.
Yet, Web 3.0 Data Space is one of those new types when the implementation will require not only narrow specialists, but also generalists with ability to creatively “combine it all together”.
The team will require a combination of skills in security, Linked Data, LLM, data, platforms, communication, standardization, as well as skills in business strategies, ethics, political sciences and social impacts.
This is a rather challenging task, but the prize is really high: to change the whole world.

LEVEL 3. Web 3.0 Data Space for Engineers

At this level, we will look at Web 3.0 Data Space technology at the architectural and specific technology level, answering the HOW questions. We will rely on the analysis performed at Level 2, which answered the WHY questions.

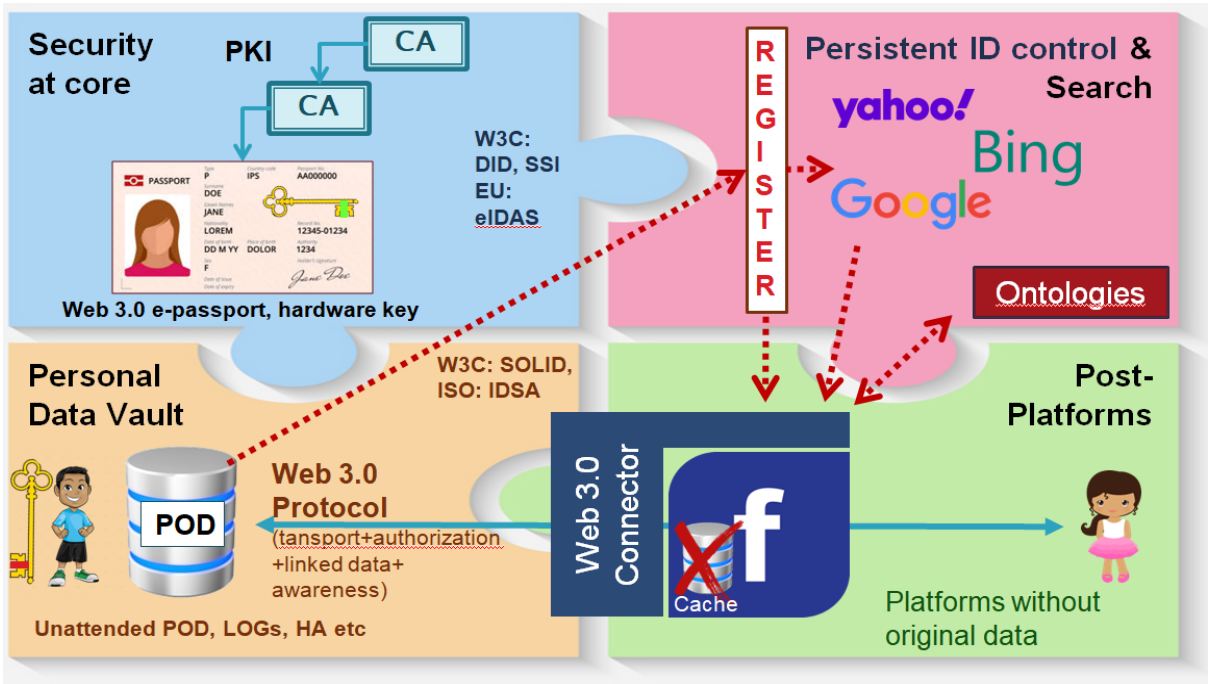
Overview

This section presents the architecture of the Web 3.0 Data Space.
However innovative and cutting-edge our vision is, most of the technologies we use have been developed long before us (https, Solid, Linked Data, ACL, LLM, DNS, PKI, etc.) and we just put them in the unusual order. Of course, the whole Data Space community will need to put a lot of efforts in order to bring all these protocols and technologies to the level of a complete and holistic Web 3.0 Data Space ecosystem. Although we are still at the very beginning of this journey, the current document already provides a pretty holistic and complete overview and architecture of the Web 3.0 Data Space ecosystem, as well as detailed discussions on its components.

Architecture

The architecture of the Web 3.0 Data Space – as we see it now – has four major components, each of them crucial for the existence of the entire system:

- **PODs**: secure individual cloud servers storing all the data concerning people, companies, and objects in Linked Data format. PODs are accessible via Linked Data-enabled Web 3.0 protocol (Solid or IDS).
- **Post-platforms**: new generation platforms & applications using a fully distributed PODs for storage of users' data.
- **Register**: a list of all PODs ensuring their discoverability and their proper indexation by semantic search engines. It also controls the lifecycle of Persistent IDs.
- **Security**: The complete and rather advanced security subsystem which protects all other elements, with Public Key Infrastructure (PKI) at its foundation to provide all users with keys/certificates, authentication SDK, etc.



The next sections of this document will review each one of these components in details.

PODs (Personal Online Datastores)

We took the concept of PODs directly from the Solid project, as it invented by Tim Berners-Lee. These are the cloud data storage vaults where post-platforms will keep all our data.

PODs are to keep data (not algorithms)

The core idea of the Web 3.0 Data Space is that:

- data is kept at the PODs
- algorithms are kept at post-platforms
- we connect data and algorithms via the Web 3.0 protocol

Yet, the reality will be more complicated. We can expect that in some cases, when data is too heavy (e.g. an original scan of the old movie, frame by frame, 12K resolution), it will be easier for a video editing post-platform to “move” the algorithm closer to the data, and in such a case a “container” with the code may be delivered very close to the POD. E.g. it could be a special service of the cloud provider where the POD is located.
In similar way, post-platforms will keep cache of data inside platforms to provide quality of service to their clients, but these are merely exceptions from the main rule: we split data from algorithms.

PODs are the advanced Web servers

PODs are based on the same principles as a traditional Web server, with the following difference:

- Web server was designed to be accessed and read by a human, while
- POD is designed to be accessed by a platform, therefore it requires machine-readable content (Linked Data-based) and machine-readable access protocols (Web 3.0 Protocol like Solid instead of http)

Who might have PODs?

- people
- organizations/departments of organizations
- things, and it means that the amount of PODs may reach hundreds of trillions, as Web 3.0 Data Space covers the IoT (Internet of Things)

Please note that every POD has its Master which “owns” it.
The personal POD is owned by a person, and such a person will have to have keys and e-Passport. The Organizational or Thing’s POD (e.g. a POD of a car) will be owned by a personal POD. Subsequently, a POD of the engine of a car will be “owned” by the POD of a car, probably, owned by a POD of the transport department and so on. In the end of this value chain there is always a personal POD, owned by a person with a key.

POD data ownership and access control

Data ownership and Access control are actually complex issues that are worth considering together so they can be better understood.

Data ownership

Typically, when most people think of a POD, they think that everything on it belongs to its owner. This is far from the reality, as is clear from our Data Space concept explained above. Your personal POD may contain information from the municipality (your registration), from your mobile operator (your phone number), the police (your parking fines), the university (your diploma), or from the tax authorities (accepted tax returns). Their data forms the actual global Data Space and allows all these institutions NOT to have their own databases.

Thus, the owner of a POD owns only part of the information on his/her own POD, where by ownership we mean the ability to “create,” “modify,” or “delete” data. It is the university which may change or even delete your diploma on your POD, not you.
In addition, the POD will contain a large amount of relational information about the owner and his objects: likes, comments from other people, which the owner also will not be able to change, as they will be signed by those who left those comments.
To sum it up: the owner of the POD will not be able to change information created by all those external parties.
Why people should keep the government registers on their PODs? We discussed the rationality of doing it above, in the Data Space section. Yet, we may consider it as a kind of responsibility the citizens have to bear in order to get rid of governmental datasets (registers) and associated bureaucracy. Indeed it is nice to have a Cadastre where only 5 people work and where data is 100% updated, but there is a price to pay:

- PODs have to be very reliable in time for centuries (we will discuss ***long-term preservation*** architecture further in the section Long-Term preservation), far beyond the lifetime of the owner
- PODs cannot be switched off or be occasionally offline (***high availability*** will be required, at the level of 99.99999% ("seven nines") and sometimes above)
- It will be mandatory to have PODs for people, organizations and certain things (e.g. car)

We may expect that governments will require people to have PODs will even pay us to buy it from certified POD providers. We believe that the POD price will be around ~€1 per month for a basic POD which can keep basic documents (and it will be higher if larger capacity is required).
This discussion also explains why we cannot have PODs in our smartphones, watches or on personal Synology server in the basement. Only professional POD providers will suit this set of requirements, and they will keep PODs in the clouds. The security requirements will also lead to the need to use cloud-based POD providers.
While the Ownership can be partial, as discussed here, the Access Control, discussed below, will require that the POD owner has 100% access control over his/her POD

Access control

Indeed, it seems that the owner of the POD will have 100% access control over ALL data on the POD. E.g. why do you have a diploma from this university or a prescription from this doctor at your POD? Because you hired them and provided access to your POD. You also give access to a specific municipality (by law). Thus you have 100% control over access to your POD.
It is very important to note that you are giving access to your data to specific people or groups of people, not to the platforms they will use. If you give access to your blood tests to “all pharmaceutical companies” on the terms of “1 euro cent per access, without providing my ID,” then these companies can use absolutely any platforms of their choice, as long as these platforms are certified (see section Platforms Web 3.0 certification below).
All these instructions will be kelp in a form of Access Control Lists (ACL) at your POD.
ACL are managed by the owner via any certified platform (used as a CMS in such a case). As the amount of the permission details in ACL might be rather high, we expect professional companies to sell “basic ACL services” to POD owners, eventually. Citizens will choose such services on their e-Reputation.
====
To sum it all up:

- A user has partial Ownership over the data on the POD, as it will keep user-related Public Data on the user’s POD
- A user has 100% Access control over all data on the POD, regardless who owns this data.

Hosting of PODs: POD Providers

As PODs are – in a way – advanced Web sites, the hosting of PODs will not be different from hosting of Web sites. As discussed above, requirements on high availability excludes hosting in a phone or at personal or corporate servers.
In order for the end user to receive a fully functioning POD, the participation of at least three market participants is necessary:

- **POD developer**. This is the company that develops the POD software, provides its support and development.
- **Cloud service provider**. These companies already exist and provide equipment for any service. Examples: AWS, MS Azure, etc.
- **POD providers**. These companies will buy the license of POD software, rent computing power from in the Cloud service providers, and provide POD-as-a-service (including the Revolver POD mechanism) to users and organizations. A good candidate is Snowflake, or the Cloud providers like AWS can do it as well.

It is POD providers that will become important players in the market, and they will provide PODs for people, organizations and IoT in the same way that modern cloud services provide Web servers.
It will be a responsibility of POD Providers to provide within the same contract PODs from at least 2 other POD providers (who use physically different cloud services), in order to provide the “Revolver POD” service, described in the very next chapter. A client will not be bothered with such details, as long as POD Provider will be properly certified by the Post-Platforms Association.
As Web 3.0 Data Space can provide a lot of services for post-platforms (see Web 3.0 services for post-platforms), the POD providers may as well provide the complete services also for post-platforms software developers, which includes the post-platforms deployment and Web 3.0 Connector services, described in the section Web 3.0 services for post-platforms below.

Providing Long-term Preservation (Revolver PODs)

The ***long-term preservation*** is one of the major challenges we have to meet.
We explicitly define the long-term as “500 years”, in order to make sure that:

- we go far beyond the typical life expectations of any platform and service (~50 years);
- we are within the life expectations of certain client organizations like museums and archives;
- we are almost at par with the knowledge preservation technologies purposely used by ancient Egyptians and Sumers (~5000 years).

This requirement is met within the Web 3.0 Data Space at 3 levels:

- **Independence from monopoly of platforms with their limited life expectations**
  We have to make sure that the owner of a POD does not depend on the platform she uses, as it may fail at any moment. This is done in a natural way within Web 3.0 Data Space, as platforms are interchangeable.
- **Independence from POD providers (“Revolver POD” scheme)**
  If a particular POD provider leaves the market 50 years from now, the data should not disappear. At the moment we believe that it is enough to combine 3 independent POD providers in a synchronized revolver-like POD triangle to resolve this issue: if major POD provider fails, then the “Revolver POD” rotates and second one will automatically pick up the contract and find the 3rd POD provider to replace the fallen one. If 3 POD scheme is not enough, we are sure that professionals and the market will provide a better solution in the future.
- **Independence from data structures and outdated formats**
  - Independence from data structures is also a natural feature of Web 3.0 Data Space and discussed in Data Types & Structures below

- Outdated formats present a strategic issue and could be addresses via organizational innovation. E.g. there will be commercial post-platforms which audit our PODs and indicate the data which might need to be converted from the aging format to a new one. Also, we can envisage commercial and non-commercial post-platforms which keep libraries of converters from ancient formats for those who forgot to do it in time.

When implemented, the citizens and organizations, as well as the whole society will know that "*If you uploaded your data via any Web 3.0 compatible post-platform, your data is stored for at least 500 years, as well as all links to/from your data, and you do not need any special backup arrangements whatsoever*". From this moment the Internet is not a media only to transfer data, it is a media to store your data for centuries.

Transferability of PODs

If the owner decides, the POD should be easily moved to another POD provider and we expect that certain post-platforms will provide such a service.

Merging & Splitting PODs

We may expect that PODs will need to be merged or spitted. For example:

- **Merge use case**: two land parcels are merged and become one object from Cadastre's point of view. Then the owner of the two PODs may decide to merge them (or still keep them separate, with all required links between them).
- **Split use case**: A painting from a museum needs to be transferred to another one. The museum decides to extract the painting from the general museum POD into a single-Painting POD, and such a POD will change the owner at the transaction

Offline use of data and services

The whole architecture of Web 3.0 Data Space heavily relies of online services. Yet sometimes we need offline use. Who is responsible for it and how should it work?
We see the following answers:

- In most cases post-platforms and their apps will take care of the offline operations (via cache data, discussed in Cache DB section below), and their abilities in offline mode will define their competitiveness.
- In certain cases (mostly in IoT) the producer of e.g. a ship may decide to keep one POD on board of the ship, assuming that this local POD on the ship will be just the 4th POD in addition to the triple-POD Revolver structure in the clouds. Such a POD will be synchronized with other three as frequent as possible, with conflicts resolved with help of professional post-platforms.

Providing Interoperability of Data Types & Structures

Any modern enterprise uses hundreds of usually incompatible information systems (typically 300-800), and each of them uses its own formats and data structures. This enterprise interact with many others, and the number of different systems increases substantially over the world. This is the context where we talk about ***data interoperability***.
This problem is one of the main challenges presented at the beginning of the document.
In the subsections we will address this issue from different angles.

The conflict of data types & structures IS natural

There are millions of platforms in this world with millions proprietary data structures. If we want to make them work together, it is inevitable to get into the data conflicts.
As we discussed in the section Fuzzy structures instead of strict structures, there is NO way we can make all platforms use some kind of universal data structures. Therefore the only way to go is to

learn to live with millions of different structures. We have an idea how to make platforms understand each other (Linked Data and LLM), yet before we dive into it, we have to reduce complexity of interconnections between millions of platforms.

Reducing complexity of interconnections

If we need to teach hundreds and thousands of platforms to understand each other, there are two ways to do it:

- Teach each of them to talk directly to others in 1:1 interactions (i.e. we are talking about ~N(N-1)/2 interactions)
- Invite them all to put all their data in the common Data Space and interact only through data, (~N interactions).

We deliberately chose the second path because the first one (usually associated with the original IDS approach) involves too many 1:1 interactions and is only suitable for a small number of platforms per enterprise, usually ~10. Otherwise the amount of connections (~$N^2/2$) make it impossible.

The problem is not the connection per se and its API, the problem is in semantic interoperability: we have to teach both platforms in 1:1 interaction to understand each other, and it takes enormous resources. Usually it is done with Linked Data technology, and we know that during the last 5 years Linked Data consulting companies growing 2x/year (and probably this growth is limited only with their ability to hire :-), as the demand to “connect this platform with that platform” just grows. It is good for the Linked Data companies, but it is certainly not scalable.

In case of Web 3.0 Data Space, “putting all the data in Data Space” means that the platforms put their data on the PODs of enterprises, people and machines and learn to understand “*what the other platforms wrote here.*” In this case we have ~N interactions instead of N^2.

To sum it up: in both cases we will have to resolve the Interoperability task, but it is easier to resolve it N times instead of N^2 times.

> In much the same way, the asymmetric cryptography reduces the amount of keys in the system to N keys instead of N(N-1)/2 keys in symmetric cryptography, and this is a major reason why we use asymmetric keys, even if we have to pay a price of setting up the PKI.

Therefore, in the context of the very large global Internet and millions of platforms, Web 3.0 Data Space approach (separating data and platforms) helps to reduce complexity from N^2 interoperability interactions to ~N.

There is one more advantage here: creation of a single Data Space of trillions of openly accessible PODs creates a possibility for mutual learning and cooperation, unlike N^2 connections between N platforms.

User experience with Interoperability: better and way cheaper

So what will this “data interaction” look like for an average user?

For example, an accountant at BMW decided to work with Oracle, even though her colleagues use SAP. Actually, she won't notice any difference. Oracle will continue to operate as usual.

Conclusion: nothing will be changed for a user in their interaction with platforms, except for a freedom to change them and work with the best (now they have to work with the system, adopted by BWM).

The BMW as a company also does not have to change anything. Actually, they do not have to officially choose a platform for this accounting department and it definitely will pay less due to competition among platforms. It also has much less costs on correcting all communication issues between BWM departments and with partners outside of the company. We may expect significant

cost reduction.

Who actually implements interoperability? The platforms

We would like to stress here again, that it is not industrial companies like BWM who have to do the job, but the platforms BMW uses.

And what does this interaction look like for SAP and Oracle? They will have to solve this problem from two sides:

- When SAP writes data to the POD of the BMW Financial Department, it must write it in such a way that another system can understand it, for example, by adding metadata "*this number is the bank account number,*" and "*this number is the invoice serial number.*" Linked Data technology is best suited for this.
- When Oracle reads this data from the POD, it will be able to understand most of the data thanks to Linked Data use. But there will certainly be data that Oracle cannot interpret correctly. Therefore it will have to "guess", and we believe that the LLM technology will probably help here.

Thus, by explaining data well when writing it to the POD, and guessing its meaning when reading, post-platforms will learn to understand each other.

Here we would like to declare an important principle:

"*The ultimate responsibility for interpreting the data and presenting it to the user in the App rests with the post-platform that reads it. At the same time, it is likely that post-platforms that are more supportive in writing and explaining their data well will also be appreciated by society in the process of their competition.*"

We would like to point out that the success of this approach depends entirely on whether we are able to launch healthy competition in the market, as it will make post-platforms to develop their communication capabilities, and only those who succeed in this will survive. See Competition instead of Monopoly at the top.

This is very similar to how people speak different languages. Linked Data is like a dictionary of foreign words, and LLM is like a complete immersion in a foreign family for a year.

Post-platforms will solve the problem of different languages in the same way as people do, with dictionaries and deep knowledge of languages.

To sum it up, we don't need to invent Esperanto as a single language. Languages are dynamic and living structures. We will let them live on, and let's not drive them into a Procrustean bed of the One format and data structure, because this structure must be flexible and living.

Therefore, we say NO to the idea of creating a Unified Data Format/Structure for Hotels, for Transport, etc. Let each post-platform speak the language it sees fit. And let competition select those who get along best in society and communicate with it.

Technology (initial): Linked Data

As discussed above, our first solution to this problem will be Linked Data technology, which essentially offers an ontological "dictionary" that will help Platform A understand the data written by Platform B. This means that Platform B, when writing data at the POD, must wrap the data into Linked Data structures that will explain to platform A that "this figure is the invoice number".

This leads us to the first conclusion: data on PODs is written not in the form of relational well-structured databases, but in the form of non-structural "triads" in Linked Data format.

Of course, this type of records will significantly slow down the work of post-platforms with PODs, and the only way to allow post-platforms to serve their clients fast is data caching within the platforms, which we will look at later in Chapter Cache DB.

The second conclusion is: all participating post-platforms will have to agree on the "ontological

dictionaries". We may start with something as simple as schema.org, and later on develop something more specific. What is important that it is the post-platforms themselves (not their clients like BMW or museums) who have to decide on "whats" and "hows" about such ontologies. The best organization to help them will be the Post-Platforms Association, discussed in the Governance section. Here we just note that such ontologies create the "centralization" problem, which we try to avoid as much as possible, as discussed in the section Decentralization vs. Centralization above.
The third conclusion: like any language the data structures will change over time, therefore we expect dynamic ontologies, controlled by post-platforms. We have a separate whitepaper on the topic of the so-called ***dynamic ontologies*** here.
The fourth conclusion: As different platforms will write down data in different ways, after several years the POD will be a mess. We will discuss it in the next section about DNA metaphor. Yet we have to interpret this mess somehow. And the larger the range of PODs our post-platform reads, the less chances it can understand 100% of data at these PODs. E.g. if we look at all PODs of all companies in the world, we doubt that their balance sheets could be all interpreted 100% correctly only with the help of the Linked Data, simply because there will be PODs somewhere in South America with very strange data, not properly explained by the platforms which put it there. We will need more advanced technology: LLM (Large Language Model).

Technology (advanced): LLM

LLM (Large Language Models) comes to the rescue when you need:

- process really big data, e.g., financial information of millions of enterprises.
- you are happy with accuracy that is less than 100%.

In general it will "guess" about the data which is not properly described with the Linked Data ontologies. It will use all possible context information to do the guess work.
We have several comments here:

- In general, LLM will complement the Linked Data technology in this quest of interpreting data at PODs
- Although Linked Data explanations will be very helpful, in the future we can predict that LLM-enabled post-platforms will be able to guess so good that they will not need Linked Data-explained data at PODs at all. Therefore we may consider Linked Data as important yet temporary technology, needed only for the next 50 years or so.
- We see a very unusual problem here: the mentality of professional communities. We expect that in most cases, clients will say: "*We can't afford to work with fuzzy data! We want the data to be 100% reliable, otherwise we don't want to deal with it.*"

  This is mistake. Web 3.0 Data Space allows us for the first time to access truly Big Data, millions of times more than we can obtain now. The fact that this data will not be very accurate will be more than compensated by the fact that on large data, even inaccurate raw data leads to very accurate final results. Very often people reject inaccurate data because they have no experience working with inaccurate Big Data. And it will take time for professionals to get used to the fact that a lot of inaccurate data is better than a little bit of accurate data. We also discussed it above in the Fuzzy structures instead of strict structures section.

DNA metaphor

Gradually, as we discuss data structures, we begin to understand that the POD will be the custodian of non-structural big data created by different platforms. As the ecosystem lives on for decades and centuries to come, PODs will begin to accumulate data generated by platforms that have long since ceased to exist.
And this is where the DNA metaphor really comes to our aid:
The human body uses about 10% of all information stored in DNA. The other ~90% represent no

more than biological baggage that has built up over years of evolution, left by some fish which was there before us. In similar way, we expect that PODs will accumulate unrequested digital baggage from previous generations of post-platforms.
To sum it up, the POD will be a vague storage of unstructured Big Data, and only Linked Data and then LLM will help post-platforms to make sense out of it. The times of structured rigid data will be gone.

Resume on Data Types & Structures

So, the move to storing data on PODs is leading to fundamental changes in how we think about data structures in the future. We will not try to create universal data formats, as some projects are trying to do. Instead, we propose a transition to unstructured data, where each platform can write it as it sees fit. The responsibility for reading data lies with the platform that reads it, not the platform that writes it. The platform that writes data can (if it wants) help other platforms understand it, but that is its decision. Obviously, users will prefer to use those platforms that are quite “polite” towards competitors. Thus, the “invisible hand of the market” will leave on the market only those platforms that best both record data in the Linked Data format and understand other people’s data.

What shall we do with a natural duplication of data, e.g. with messages?

As it was discussed in the Principles section above, keeping the Data @ Source is the foundation of the Web 3.0 Data Space. As we do it, we are moving from a world where all data has always been copied to many places (so-called Data Silos), to a world where all data is stored in a single and original copy at the POD of the data owner (which means no Data Silos). If someone needs to have a copy of the data, it is easier to make a link to this data than to store it. After all, when the data changes, you will have a link to the updated data, which is convenient.
However, sometimes we will have a situation where data may be stored in two copies. For example, when a message is sent, both the sender and the recipient may have it. Or a contract is signed, it can be kept by both parties. Or, when a financial transaction is made, an entry will be made in both the sender's ledger and the recipient's ledger.
There are several viable approaches here, and we have yet to decide which one is best. Let's have a look at them:

Use case 1. Alice sends a message to Bob.

Option 1: We keep two copies, but both copies point to a peer message with a "the same" explanatory link, using Linked Data technology.
Option 2: The message is stored only by the sender, and the recipient receives only a link to it, together with the right to “use it forever”. In such a case the recipient will see if the original is changed (just like Skype or Telegram allows). It is important that in case of the change the original is available as well, as usual.

Use case 2: A contract for the purchase of a house.

Option 1: Only one copy of the contract is on the POD of a house. Both the seller and the buyer have access to it “forever”.

Use case 3: Alice transfers money to Bob

Option 1: Transactions are duplicated in both ledgers of Bob and Alice, but have mutual links with the link description as “the same”. This allows any auditing platform to verify that both ledgers contain the same records, thus ensuring the integrity of the transaction.

How users change/control data at PODs? (CMS for POD)

When thinking about PODs, it may seem that POD owners can literally change data on their PODs directly. In fact, this is not true. The only way to change something on the POD is to use some kind of platform. Thus, platforms are needed not only to access data, but they are also used as CMS

(content management systems) for data management at PODs, which is completely natural.
In order to better understand this case, it is better to forget about “changing data at POD” and start thinking about dealing with data at platforms. E.g. we update our photo on LinkedIn, we create invoice in a SAP, we update our hotel info at Booking.com. In fact we do not update data on any of these platforms! We actually change data at our PODs VIA these platforms: at the personal POD with LinkedIn, and at the hotel’s POD with the booking.com and SAP.

Security of PODs

Although we have a separate section on the Security @ Web 3.0 Data Space below, we would like to discuss the POD-related security here

Historical data/Snapshot replication

One of the benefits of the ***data at origin*** approach is that if your data is changed via any post-platform, all stakeholders are always working with the updated data, rather than with just one of those out-of-date copies at different platforms like it works now with Web 2.0. But if the data on the POD is constantly changing, how will we be able to access previous versions? The answer is the standard snapshots technology, which enables the so-called “time machine”, when you can roll back data to any time ago. How this will be arranged on the POD is probably still worth discussing. This may be part of the business logic of the POD, or part of the Btrfs file system, or done in some other way. This is a technicality and could be left to competition.
But here we would like to note another aspect of the “time machine”. The point is that thanks to the use of Persistent ID and Linked Data technology, we will see more and more data that is linked to each other, even if it is located on other PODs. Therefore, if we want to roll back for 70 years, we will be interested in the old data not only on a specific POD, but in the old data on the entire set of PODs related to our request. That is, a specific platform that will provide us with a “time machine” effect (for example, Facebook) will have to “roll back” thousands of PODs by 70 years, and this should be possible to do. At the same time, the entire chain of links between old objects should not be destroyed, thanks to Persistent ID. Of course, we will experience some difficulties as it is impossible to synchronize snapshots for all PODs around the world on one exact point in time 70 years ago, but over time, the developers of Web 3.0 standards will come up with something to improve this situation.

LOGs

LOGs are at the foundation of the Web 3.0 Data Space security, as we will discuss in the section Castle vs. Eye of God below.
The owner needs to know who, when and via which post-platform accessed her data, therefore the LOG will record it all, and the visitors will sign their transactions.
No one (even the owner) should be able to access such log files for modification, hence the following requirement arises: Unattended PODs, which we discuss below.

Unattended PODs

We are accustomed to the fact that any system has a system administrator who has full power over it. For example, if the system administrator of the cloud service where your POD is located is able to change the log file of your POD, then the entire security system will be compromised. Thus, the POD must be a (virtual) computer that runs in ***unattended mode*** and can only be controlled by its owner, or by those assigned by the owner. Yet, even the owner cannot change the log files or comments of other people on her photo or the Police fines on her POD.
This is a very strict requirement, but, hopefully, it is not impossible. This is one of the reasons why we call the security system Web 3.0 Data Space military grade security.

Web 3.0 Protocol to access POD

The post-platforms (we discuss them in the next section) will access PODs via the Web 3.0 protocol.
At the moment we have several candidates for such protocol:

- Solid Protocol. It is more advanced in dealing with Linked Data
- IDSA Protocol. It is more advanced in authorization. Yet it is brand new.

It does not matter which one will win (or, probably it will be a merge of them) as Web 3.0 Protocol.
At this moment we would like to indicate certain requirements to this Protocol:

- **Transport**
  In a way, http is a good example of transport. It our case we may require significant scalability, as post-platform may need to access billions of PODs
- **Authorization**
  The post-platform will need to know which data on the POD a user may access. As the ACL (access control lists) are stored at the POD, the post-platform will use the Protocol to get/control such information.
- **Linked Data support**
  Most probably the Protocol will need to process the Linked Data, as PODs may use Linked Data to store data.
- **Awareness flow support**
  When Alice receives a message from Bob, she expects to receive it in her current messenger, which is Viber. Therefore Viber expects the Alice's POD to inform it when the POD receives a message from anyone.

Role of competition in development of PODs

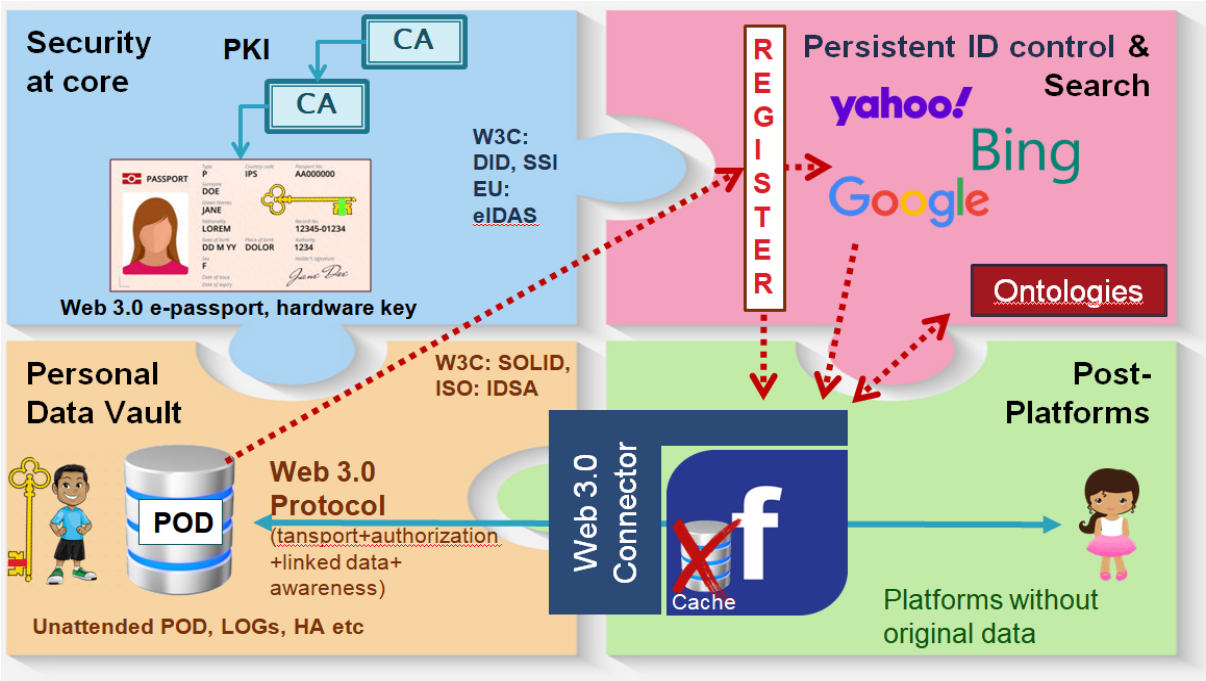
As discussed in Level 2, it is very important that everything around PODs will be guided by competition:

- POD sw development will be done by competing projects
- POD providers will be numerous and will compete to provide the best services.

It is important that we make capitalism work again, now in a totally flat and transparent world.

Post-platforms

While PODs are essentially "data keepers", platforms are "data aggregators and service providers". From the user perspective, Post-Platforms are just "good old platforms". The only difference is that they keep all "their" data at PODs, sometimes even at billions of PODs. Post-platforms will access PODs via the Web 3.0 Protocol.



Cache DB

Usually, when we present the Web 3.0 Data Space concept for the first time, we present post-platforms as “platforms without DB”. This is correct concept-wise, but incorrect technically. Indeed, in reality post-platforms ***will*** keep their DB, otherwise they will fail to serve their clients fast and effectively.

Does it endanger the system? Don’t we return data to platforms?

No, everything is just fine and the principle Data @ Source is not violated here. Actually, the question is not about whether the platforms will have a database. It is in how we ***interpret*** this database. In the world of Web 2.0 (conventional platforms) the platform’s database represented the repository of the ***original data***. In the world of Web 3.0 Data Space, this very same database is merely a ***temporary data cache***, while the original data is stored on PODs.

Indeed, if, using another platform, the data on some POD is changed, then the same data in the post-platform database will become outdated at the very same moment, and the post-platform urgently needs to re-read data from this POD in order to update the cache.

The post-platform can learn to do this itself, or can use the Web 3.0 Connector service described below.

Web 3.0 services for post-platforms

In the Web 2.0 world (which is where we live now) any platform is self-sustained: it has its own users (with logins/passwords), its own data, etc. The users enter this “universe of one platform” and get fully (at least this is the dream of the platform owner) served inside it. The problem starts when users have to use dozens if not hundreds of platforms simultaneously to fulfill the task.

In the world of Web 3.0 Data Space, any platform, becoming a post-platform, finds itself in a new world where most of its services will live not inside it, but outside, provided by the Web 3.0 Data Space ecosystem. Its data lives on PODs. Its users have their own credentials. These PODs can be found through an external Register, using external search engines. In general it reminds a giant OS. Let's have a look at these services. And remember, the list below is by no means complete because we haven't built this world yet.

All Users are available with their own profiles

Post-platforms will no longer need to force their users with creating accounts for every platform,

spending millions of dollars on attracting them to do it. Any Internet user can log-in into any program and realize that she does not need to waste time creating an account and profile. She will be able to immediately start using the service, because it will know everything it needs about her by using her POD (to the extent she allows).
Actually it means that any platform will receive ALL users in the world when it joins the Web 3.0 Data Space. This is a major change. Nowadays any investor expects to spend 90% of funds for every new platform only on attracting users. The Web 3.0 Data Space simplifies it dramatically.

All the data in the world is available to post-platforms

If previously a platform had to collect data itself, now Web 3.0 Data Space promises that all the data on the planet is available to any post-platform, of course, assuming that the particular user of this post-platform has rights (ACL-controlled) to access this particular data.

The Register service

We will describe the Register in more detail in a separate chapter below, but it is important to mention here that thanks to the Register, post-platforms will be able to find the necessary PODs and objects on PODs. However, given the huge number of PODs (up to a trillion), finding the right POD for a platform may not be a very easy task. And here the Search Engines described below will help.

Search Engines

The Data Space concept assumes that we give millions of platforms access to vast amounts of knowledge, globally. It will be very easy to get lost in this big data. Therefore, the role of search engines will be rather important. They will help post-platforms to find right PODs and even information inside PODs.
Their first task will be to find right PODs through the Register. As the Register has very lean information about PODs (only their ID/IP), in order to find out (for example) all citizens of Germany with a degree in geography or all hotels with parking lots a search engine needs to question many PODs. With IoT using PODs we expect trillions of them.
The second task for search engines will be to find information inside PODs for post-platforms.
Thanks to competition we expect that the market will be filled with tons of search engines to help post-platforms.

Persistent ID provision and support

Whenever a post-platform creates new data, such as a text file (if it is a word processor) or a photo (if it is an app inside a CANON camera), Web 3.0 Data Space will provide it a unique Persistent ID for that file via the Register, discussed below. This ID will allow 3rd parties to keep links (which are actually the IDs) to this file for centuries. NO more broken links.

Reliable and long-term data storage

Post-platforms no longer have to worry about how to save the data, as it will be stored securely on their owners' PODs for centuries, as part of the Web 3.0 Data Space service. See section Long-term preservation of all our data in Level 2.

Reliable IPR control

Any post-platforms can count on Web 3.0 Data Space to provide control over data ownership, so that any post-platform can always check who owns what. See section IPR and Provenance in Level 2.

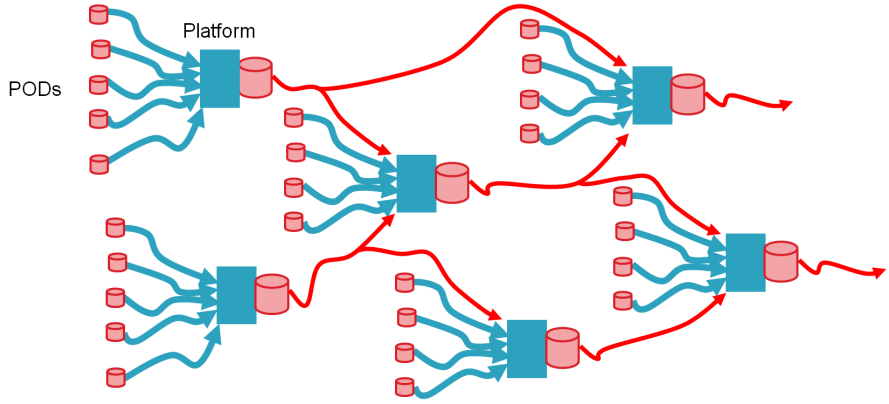
E-Reputation

Any post-platforms will have its own POD and this will allow users to rate it. This will attract new

users to the post-platform. Thus, instead of spending money on advertising, the post-platform will spend all its resources only on the quality of program, because only this will determine its e-Reputation. See section Trust & e-Reputation in Level 2.

How to sell stuff? Put it on your post-platform's POD.

If the post-platform derives information which it would like to sell, its POD will do the job. E.g. social network may derive the IQ level in certain territory and can sell the ***IQ map*** to the real estate businesses via its POD. It will form a network of interconnected platforms, which, in a way, reminds a neuron structure in the brain.



The ability to expand the scope of service

If previously each platform specialized in one market because its development cost billions of dollars, now entering new markets will be simple and cheap. This means that post-platforms will compete in their ability to serve users in different markets at once. This is the entrance to the Metaverse, but not only for one facebook.

Web 3.0 Connector

We already discussed above that post-platforms will continue to use their databases as cache, but they will need to synchronize these databases with the original information on the PODS in both ways:

- If our post-platform changes something in its database, this must be recorded on the corresponding PODs.
- If another post-platform changes something on some PODs, it needs to be updated in our post-platform's caching database, when relevant, using the "awareness protocol".

Presumably, this work could be handled by the so-called Web 3.0 Connector, which will simplify the interaction of the post-platform and Web 3.0 Data Space. This Connector will take on many functions:

- 2-way synchronization of the internal caching database with relevant PODs.
- checking the authorization for users (for example: "*can Alice edit a file ID093759207432857290357 2093759207 43? at the POD ID285729035720937592074 3?*").
- interaction with the Register and search engines.
- wrapping up data from the internal DB into Linked Data before uploading it to PODs
- interaction with ontologies
- dealing with LLM providers when "guessing" on data while reading it from PODs
- interaction with event flow in the Web 3.0 Data Space (e.g. when Alice gets a message, her Whatsapp platform would like to be alerted, as Alice chose it for her messages)
- and so on.

We expect the emergence of a full fledged market for Web 3.0 Connectors.

Speaking about the synchronization of the internal database of the platform and PODs, it is

necessary to remember that this is where the “packaging” of data from the internal DB into Linked Data will take place before sending it to the PODs, and this is where the interpretation of data from remote PODs will take place before putting them into the platform internal DB structure. Setting up such a Connector for every post-platform (which will be mostly about aligning ontologies) will require certain time and effort, as it addresses the main problem of Web 3.0 Data Space: resolving conflicts between different formats and data types. The development of Connectors will become the cutting edge of IT technologies, as LLM will start to replace Linked Data eventually, simplifying adjustment of Web 3.0 connectors.

Authentication

Post-platforms will no longer create accounts for users with logins and passwords. Users will have their own one key and one e-Passport for this key (see details in the Security section), and each post-platform will have to learn how to work with this.
There will be a number of SDKs on the market to verify user authentication, to work with revoked e-Passports, etc.
This will greatly simplify the work of post-platforms with user authentication: they just need to ask a user to show an e-Passport, confirm it with the private key, and after that the post-platform may trust that this user is authenticated (i.e. she is really who she said she is).
When authenticated, the question arises of her authorized access to resources at certain PODs, and here the post-platform will again receive support from the Web 3.0 Data Space, in the form of an authorization mechanism.

Authorization

Let’s take a use case: Alice (already authenticated) wants to change her profile photo through the particular post platform, e.g. SAP or facebook. Does she have a right to do this?
The post-platform does not and cannot know the answer to this question a priori. This answer lies on the POD, which knows who can change this photo. Thus, the SAP post platform will send a request to the POD and the POD will respond that “*yes, Alice can change this photo*”.
This functionality should be a part of the Web 3.0 Protocol and any Web 3.0 Connector will do the job for the post-platform.
It should be noted here that different platforms have different and sometimes quite complex mechanisms/data structures for authorization. Therefore, when Alice writes access rights to her objects to her POD, the specific platform of her choice will write authorization ACLs (Access control list) to the POD in its own format, and other platforms will have to interpret those ACLs.
NB! Although PODs are usually data agnostic when we talk about data formats, they may no longer be ***access control agnostic***, as the POD will have to explicitly answer the post-platform’s direct question “*can Alice change this photo?*”
We will still have to explore this topic (including the authorization in Web 3.0 Protocol) better in the future.

Event flow

The task of constant synchronization of post-platforms internal databases and PODs, as well as numerous messages and communications between users and agents in the Web 3.0 Data Space will require a developed ***event flow*** mechanism. For example:

- Alice sends a message to Bob.
- Bob currently uses Viber as his main messenger.
- Accordingly, Viber wants to know when Bob's POD will receive the message.

We still have to develop this topic further, as the Event flow will become a part of the Web 3.0 Protocol.

Summary on Web 3.0 services

As we see, all post-platforms will get an impressive range of new services in the new world of Web 3.0 Data Space. Most important, post-platforms will get users and data effortless, which is unthinkable in Web 2.0. These services will be provided by commercial and non-commercial projects as well as by the ecosystem itself.
Indeed, from this point of view, one can consider Web 3.0 Data Space as a super-OS for platforms that provides everything they need, including user data and users themselves!
We expect that cloud providers will play a major role in providing such services in a competitive way, and Snowflake is a good example: not yet aware of the existence of the Web 3.0 Data Space, Snowflake is trying to build their ecosystem on very similar principles, with one exception: they are building a closed system, while Web 3.0 Data Space can only be an open system.
Of course, on top of Web 3.0 services cloud providers (or POD providers) may provide extra services to post-platforms developers, e.g. a post-platform deployment.

Role of competition in development of post-platforms

Since we are discussing post-platforms in this section, we would like to point out that the most important thing we achieve by separating data from platforms is to release the enormous competitive energy of multiple platforms. Now each of them can access all the data and all the users, and for the first time, competition will be based not on the question "*how many users (and data) does your platform have?*", but on the question "*what functionality does your platform provide?*"
This will have implications that are important for the development of the Web 3.0 Data Space itself. For example, thanks to competition between platforms:

- The ability of platforms to understand each other will develop.
- New monetization models will develop.
- AI will develop, because for the first time we give it access to the huge data needed for its training.
- Dynamic ontologies will be developed, tracking temporal changes in terminologies in certain industries (see a separate whitepaper on this subject here).
- Security systems will develop around Web 3.0 Data Space
- etc

In this way, we will destroy the myth that "*our capitalism is not working any more*". It was not broken, it's just that the platforms have temporarily "hacked" it. Once we restore competition among platforms, good old capitalism will start working again, and it will work very well, because we will make the market very flat and very transparent.

Platforms Web 3.0 certification

We provide advanced military grade security for PODs, and we provide great authentication for users. Post-platforms are the middle-man between PODs and users, therefore we need to make sure they do things right. We foresee two ways to do it, and both will complement to each other:

Formal certification

To guarantee that post-platforms support our level of security, we will need to certify any post-platform that enters the Web 3.0 ecosystem that they do everything they are supposed to do correctly. For example, they should not keep user data longer than certain timeout and they authenticate users only with the certified Authentication SDKs.
This will be similar to the certification of applications in the Google Play market. Only this time it will not be done by a single private company. As in other industries, certification must be carried out by

the relevant Association, created and maintained by the post-platforms themselves. After all, the Association of Cadastral engineers or the Agricultural Association that controls the use of the “BIO” label on food products works in exactly the same way.
We will create such a Post-platforms Association as the market develops, and it will develop according to the same rules as other industrial associations. See the section Post-platforms Association above in the Governance chapter for details.
The Post-Platforms certification will be an important initial security mechanism. No Post-Platform will access Web 3.0 Data Space without the certification, unless the POD user specifically allows it (e.g. for testing purposes).
Yet, the e-Reputation will complement and add more security, as discussed in the next section.

Extra security via the e-Reputation of post-platforms

Every Post-Platform will have a POD, which will be used at least for two reasons:

- the platform will put its own services to the POD for sale
- clients will have an opportunity to complain (or praise) on services of the platform.

Eventually this feedback from clients will form the Post-Platform’s own e-Reputation, which will be a major reason to prefer one certified platform over another. This will supplement the value of formal certification with people’s opinion, eventually, and probably, in the future e-Reputation will become a major factor

Expected new Post-Platforms services

The appearance of post-platforms on the market will not lead to a fundamental change in the world of existing platforms like SAP, Facebook or booking.com. However, we will observe certain changes, for example, these:

Back links statistics

Persistent IDs will give us the opportunity to create links to objects and be sure that they will never become broken links. If you take a good photo, it will be referenced in articles, blogs, films and even books. And at some point you will want to know who, where and how referred to your photo.
We expect that there will be platforms that provide you with such a service, showing a map of references to your materials with full statistics of usage.

New types of AI assistants

AI assistants are not a new product. But the volume and quality (thanks to Linked Data and semantic richness) of data will take it to the next level.See Web 3.0 Data Space and AI below.

Metaverse

We have already written above that it will become easier for platforms to capture new markets. Each of them can turn into a universal platform giving you access to all services in the world. This will be the Metaverse that Facebook dreamed of, with the difference that Facebook wanted to bring the whole world into its own Metaverse, and we will bring all the platforms of the world (including Facebook) into our common and open Metaverse, called Web 3.0 Data Space.

Expected new Post-Platforms services based on security

Surprisingly, most of new services in Web 3.0 Data Space will be enabled by the advanced security of Web 3.0 Data Space. Indeed, usually we consider security as an unavailable burden. Here, it will become enabler of really great services. Below are some examples:

- **E-Reputation**
  There will be Post-Platforms which calculate e-Reputation for people, organizations, things, digital assets and platforms.

- **Authorship rights and Provenance (IPR control)**
  There will be post-platforms which will help to claim the ownership (by using the time-stamp service), selling assets, and checking the ownership and provenance. Their audit will be accepted by courts.
- **LOG and security investigation platforms**
  There will be security audit platforms, which will replace current “antivirus” platforms. They will help citizens and organizations to be assured that “everything is alright”
- **ACL list providers**
  As access control will become an important part of our life, we expect new post-platforms which will help to set up a tailored set of access control rules for your POD and will maintain it in the future in a convenient way.
- **E-money transfer services**
  Most probably the current personal management services (for citizens) and professional ERP systems (for companies) will adopt this new service. See e-Money description here.
- **E-Voting**
  There will be new platforms to allow citizens to run all kinds of voting or petitions (like change.org) at local, national or global levels. See details here.
- **PET** - Privacy Enhancement Technology
  We may consider this service as an extension of e-Voting, which allows to answer semantic-enhanced statistical requests like “*How many van Gogh owners live in France, who have formal education in art?*” without exposing names of these people. We do not expect new post-platforms here, yet we expect existing platforms to learn PET and improve privacy of their clients.

Register

The Register in Web 3.0 Data Space plays roughly the same role as DNS plays in Web 1.0: it allows to find the IP of a POD by its Persistent ID. Presumably, like DNS, the Register consists of two columns: ID & IP. Accordingly, each POD at startup sends information to the Register about its location or subsequent changes. This will probably require a heart beat protocol for the Register to exclude PODs that are off line.
Platforms can use the Register directly to find the right POD (for example, booking.com will use the Register to find hotels), but we doubt that this will be feasible once the number of PODs reaches trillions (thanks to IoT). It will probably be easier for platforms to use the Search Engines service, which will immediately provide a list of needed PODs, e.g. hotels for booking.com.
We have reasons to believe that the Register will be a very lean database, without any meta-information about PODs. The commercial and non-commercial search engines will collect and provide meta information about PODs to post-platforms.
The Register will be managed by either ICANN or a similar NFP. (See the Governance above)

Persistent ID management

Persistent IDs play an important role in Web 3.0 Data Space, and we need it first for PODs and then for all data assets at PODs. In both cases it will be one range for Persistent IDs

ID for PODs

For Web 3.0 Data Space to work effectively, we need Persistent IDs for PODs. It is very important that these IDs:

- will not change for centuries.
- will be global.
- will not be duplicated and will be protected from attacks in the form of the use of duplicate IDs (for example, when a child in Somalia is assigned the ID of a child from Germany to

impersonate it).
- will not depend on any platform or system or government or group of people.

We will have to follow the DID standard as a whole, but we will have to make more specific decisions about how we will do this, since DID is a fairly general standard. For example, we have to decide whether we will distribute such IDs centrally or use a UID approach (random number generator on a very big range).
At the moment we are leaning towards centralized distribution of IDs through Register. Presumably, this will protect ID holders from impersonation attacks, as then the Register will be able to sign the ranges it distributes. This is one of the most crucial subjects which the community has to discuss.

Universal ID for all assets

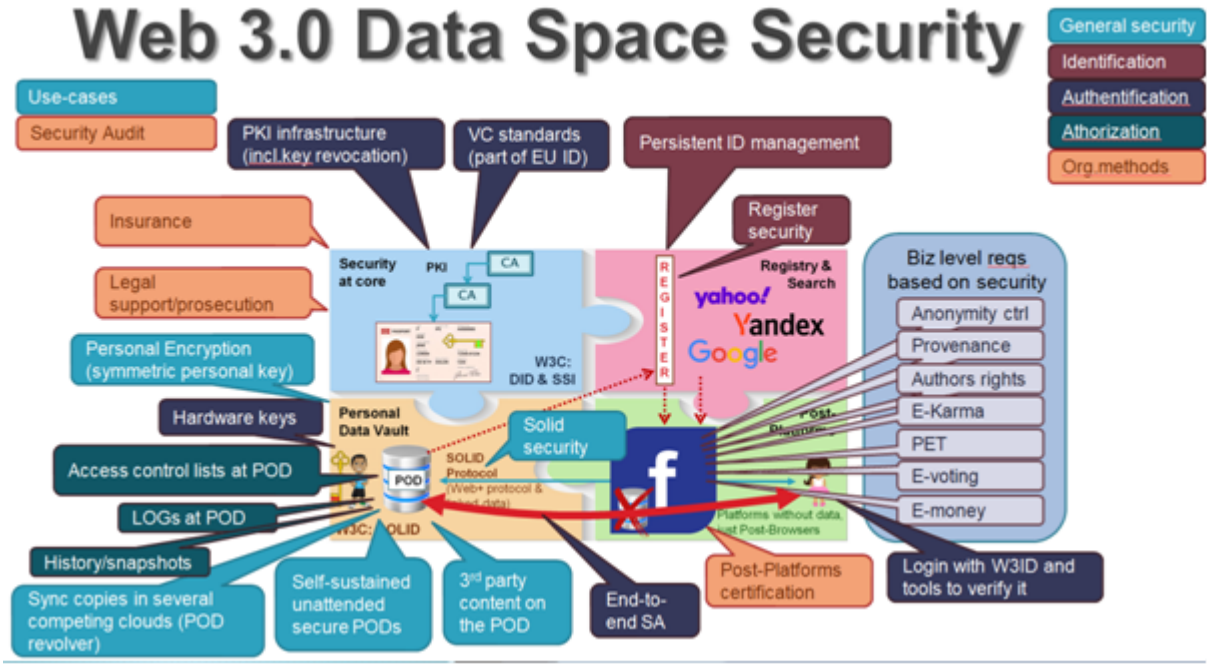
We will need Persistent ID not only for PODs, but also for all assets that will be located on PODs: documents, “likes”, messages, etc.
These IDs will be in the same ID space as the IDs for the PODs. Thus, by looking at a Persistent ID, it will be impossible to tell whose Persistent ID it is – a POD, a person, a company, a car, or a stapler.
This assumes that all objects on this planet will use the Persistent ID defined in Web 3.0 Data Space. And this is a very serious change.
Having a Persistent ID is a key requirement for a number of future services in Web 3.0 Data Space, for example, IPR control, long-term preservation or fake parts control.
And, of course, after implementing Persistent ID, we will never again encounter the phenomenon of broken links. Digital data will become as reliable and durable as real objects.
Persistent ID will change the digital world, making it sustainable.

Security of the Register

The issuing of Persistent IDs will be an obvious target for criminals who want to somehow seize control of the distribution (and signing, if any) of IDs or making the service unavailable as part of warfare.
These issues will need to be discussed as part of the Register development.

Security

It is probably not totally correct to call security one of the components of Web 3.0 Data Space. It is woven into each of the components, as we saw in the previous sections.



On the one hand, it strengthens them all, providing protection for both PODs, post-platforms, and the Register; on the other hand, it is an enabler for a number of new services, as we saw in the chapter Expected new Post-Platforms services based on security.
In this chapter we will skip many of the security elements that we have already discussed above and focus only on those elements that provide fundamental security of the entire system.

Why security is so important in Web 3.0 Data Space?

Security is a crucial element of the Web 3.0 Data Space for several reasons:

- Individual PODs concentrate virtually all the data about a person or a company, and they become the only authoritative source of original data, a single point of failure.
- We allow numerous actors to access data on the POD via numerous apps, platforms and services. Their authentication and authorization becomes a concern.
- We will need an Eye of the God concept to keep an eye on the whole system, to track activities, be able to roll them back, etc.
- The concept assumes that private PODs will keep elements of public and corporate data (we call it ***Data Space***), which required even stricter risk-management policies and procedures
- Related services, like e-Reputation, e-Money, e-Voting, etc., will require the highest level of security and strong authentication.

With all these and similar requirements in mind, we clearly need a system that is global and which at the same time attains what we call a “total security” level.

Basic principles

We see the following basic principles:

- Large systems require higher security levels
- Secure-by-design
- Key management is at the foundation of security
- Staged evolution of security
- Decentralized (crowdsourced) security
- “Castle” vs. “Eye of God” concepts
- Open Architecture

We discuss them below.

Large systems require higher security levels

This is a very simple rule-of-thumb, known to all security specialists. But we would like to explicitly present it here, because in the context of the Web 3.0 Data Space this simple principle becomes the most important one. It allows us to immediately answer negatively questions like “*Is it possible to use Web ID in the Solid project?*”, or “*Can an organization have a private key?*”
Web 3.0 Data Space will be a huge system, with trillions of PODs and millions of platforms and applications. This means that from the very beginning we must prepare to create the most advanced (military grade, if you like) security, secure-by-design.

Secure-by-design

All major digital systems built in the past decades – Internet (TCP/IP, ftp, email, web, DNS – were designed without “secure-by-design” approach, as it was believed that “*security will be added later on*”, which actually has never been done. And it made our life rather insecure and difficult. E.g. each one of us has to use hundreds of logins/passwords, and it is difficult to call it “good and convenient security”.
As we are building the real Web 3.0, we would like the Secure-by-design architecture is a must and

a major component of the entire system. It will be both reliable (and we are talking about military grade security) and convenient.

Key management is at the foundation of security

Modern protocols and crypto algorithms are very reliable. The only way for intruder to get into really secure system is to attack/compromise the keys. Therefore any real security starts from key management. We expect that with one key a person will be able to enter any platform or service, sign, encrypt, vote, transfer e-Money, get cash from ATM, open any hotel or other doors, a rental car etc. It will be convenient and reliable world without logins and passwords. Just one key “to open-them-all”. And if you lose your key, you get a new one, just like a bank card.

Who may have keys?

We know that PODs may belong to people, organizations and things.

But can people, organizations and things have keys and e-Passports? At the moment we see it this way:

- **People can have keys**
  People have will, and their keys allows them to express their will with the signature
- **Companies cannot have keys**
  In reality it is not the company which signs a contract, but a certain employee. If so, we expect that employee (let’s call her Alice) to sign the contract on behalf of the company with her own key (as she has a key already as a person). The other party (Bob) will trust this particular signature, because his post-platform (which he uses for managing the agreement) will check:
  - the signature of Alice
  - then it will request from her company’s POD the organizational chart and check whether Alice is authorized on this day to sign such a contract
  - then it will check the signature of the director of the company who signed the org.chart
  - then it will check the director’s contract
  - then it will check the charter of the company and find who are the shareholders and whether their signatures are on the director’s contract
  - and only then the post-platform will report to Bob “Yes, Alice can sign and her signature is valid”
  - Alice will do the same with the Bob’s signature if needed.

  As you see there is no reason for a company to have keys.
  There is another reason for a company not to have a key: if the company had a key, where exactly this key would be stored and how would it be controlled? E.g. in the table of the director? If so, how can we guarantee that this key is not compromised? We see no way to keep such keys safely. And, finally, even if the keys are stored securely, how sure are we that they were used by the authorized employee? It will be totally non-transparent system, and therefore not secure at all.
  NB! We know that some specialists will not agree with the idea of a company without a key, and we need to discuss it further. We do understand that in the world of Web 2.0 it is ok for a company to own SSL keys/certificates for its web site, yet we consider this totally insecure in a significantly larger system of Web 3.0 Data Space.
- **Things can have keys**
  As for the things, probably they may have keys. Indeed, things (e.g. a car) may generate a lot of data, and we need to know exactly which thing did it. In such a case – most probably – the maker will sign (and regularly re-sign) the e-Passport for this thing, certifying its public key. We may need to discuss it further.

Staged evolution of security

The “total security” we describe is a rather ambitious project. We can deploy it only in stages,

starting from much lighter versions for certain industrial applications. For example, it makes sense to start implementing Web 3.0 Data Space from Cultural Heritage domain, as the costs of mistake is low and most data is in public domain be default. Still, it will be a “secure by design” approach with appropriate key management at the core.

Decentralized (crowdsourced) security

Typically, security is based on centralized control and audits performed by special auditors.
Without questioning this approach, Web 3.0 Data Space will complement it with security audits from millions of non-professional users. Indeed, if a thousand people complain about the same problem, it is worth paying attention to. This is exactly what our e-reputation does. Thus, we believe that e-reputation will become a critical decentralized addition to the classic centralized security architecture, and its role will only grow.
For example, any platform must undergo certification in order to be admitted to the ecosystem. But over time, its e-reputation will play a much larger role in the choice of users than formal certification.

“Castle” vs. “Eye of God” concepts

There are two main approaches to security systems: closed and open.

- **Closed approach**: surround our city with a wall, and don't let anyone in without permission.
- **Open approach**: anyone can come into our city and do what they want. But they will know the rules of behavior in our city and that everything they do will be recorded and we will always be able to find out whether they followed our rules.

The second approach is more reliable, and we intend to implement it in our security system. This means that we need reliable log systems that not only record all events, but also record ***who*** participated in those events. Indeed, if all users of the system have keys and e-Passports, it will not be difficult to relate their actions to their IDs.
NB! There will be situations where we do not want to capture the names of participants, and the POD owner can determine this.

Open Architecture

Here we would like just to remind that the real security could be based only on the open architecture, as only open architecture could be scrutinized by professionals who find all issues and errors.
The only “closed” part of the real security is the private key of the user.

The Security Triad: Identification, Authentication, Authorization

Identification

We will use global persistent IDs for Identification. It is based on the DID/W3C and similar standards.

Authentication

We will base authentication on VC - verifiable credentials and PKI - public key infrastructure. Again, this work is linked with VC/W3C and eIDAS/CEN.

Public Key management Infrastructure (PKI)

The weakest point of modern security is not the algorithms and protocols, but the keys. One of the best things to manage them is the Public Key Infrastructure, a hierarchical network of notaries who certify users’ open keys.
Currently, full-scale PKIs are used mostly in corporate and bank environment, but nobody dared to deploy a global one. The only known global PKI system is the one that supports the https protocol of secure connections between browsers and web servers. But still, this is a one-way security, as it

protects (with a key/certificate) only the web server, and web servers, in their turn, cannot fully trust their users' identities. This issue is addressed in a very inconvenient way by using logins/passwords, phone numbers, or emails to authenticate users.
We suggest a very simple solution: a global PKI, which provides keys/certificates both to servers and to users. No more need for logins/passwords.
Let's emphasize that the strong authentication system can still provide a desired level of anonymity (so-called zero-knowledge proof) when needed.

Centralization issue

The PKI presents an issue of "centralization" which we have to address. We may go in the direction of "multiple-roots" or "cross-certification", and this is an important subject for further discussions.

PKI: levels of trust

We need different levels of trust in different levels of translations, e.g. the trust in using public tram is different from the trust needed to buy a house. Therefore we need different approaches here.
Modern banks demonstrate a possibility to run remote user passport verification with apps which can read NFC chips at the passport, challenge the user with "seeds" to verify his/her actual presence etc. We may consider such an App (actually, many competing apps) for the Web3.0 Data Space, and then it will allow us to establish just one root CA for automatic certificate issuing.
Yet, for certain mission-critical cases we might need personal visits to CAs, and for this purpose we will need distributed CA offices. Our biz plans suggest the use of mobile operators or banks offices.
Therefore we may introduce different levels of certificates (e-passports) here:

- low level certificates (for transactions below €500), provided in a remote way. We will implement it within Web3.0 Data Space
- middle level certificates (for transactions below €10k), provided in the office by partners like mobile operators and banks, acting as CAs.
- high level certificates (for transactions below €1M), provided in the office by partners like notaries, which will put efforts to make sure the person is authenticated and is able to express his/her free will independently.

Passport based vs DNA based authentication systems

In the first stages of the Web 3.0 Data Space evolution we will use paper passports as the foundation of our authentication, meaning that CAs will require users to produce national passports/birth certificates etc to identify themselves.
Strategically it means that we rely on the government system of documents to identify/authenticate a person.
Yet we would like to investigate (in line with eIDAS) future methods which will allow to skip the use of government-issued passports in the future. E.g. parents with a help of a notary (CA) could issue the first certificate in the hospital when the person is born, and the identification (NB! ***not*** the authentication!) could be based on the DNA of a newborn citizen.

Private key control

As we are building military grade security, the user's control over the private key should be enforced, and based on:

- use of hardware crypto-engines, e.g. USB-fobs, in-phone crypto-engines or Mobile IDs, which cannot leak the private key out.
- multi-factor authentication to access the private key (do not mix it with the VC Authentication discussed here!), e.g. fingerprint, pin code etc.

Keys Revocation

As for the revocation db, most probably we can avoid centralization (see the section Decentralization vs. Centralization above) by keeping revoked certificates at the relevant users' PODs, as PODs allow 3rd parties to keep their data (e.g. the data of the revoking authority, whatever it is).

A user may revoke her certificate herself, or it could be done by the PKI Revocation Center (TBD).

Authorization

It's based on the following assumptions:

- Any digital asset is in one (and original) copy only
- This digital asset is stored on the POD of the owner
- The owner defines access rules (e.g. who can access what, or even the price of access) and authorizes certain (groups of) users to access her assets
- The owner does not authorizes platforms, but she defines the "certification level" for platforms to be used
- All these instructions are kept at the POD as ACL (access control lists)

Please note that:

- The POD owner will Instruct POD with the creation of Access-Control-Lists (ACL) via any platform of his/her choice. We expect that the complexity of the task will be significant, therefore we look forward to ACL-platforms that provide ready-to-use ACLs as a service.
- We will have to set up a process of the Post-Platforms Certification discussed below in the Platforms Web 3.0 certification section.
- If a POD belongs to organization, the organizational chart will be used in the ACL mechanics. It means that firing a staff member will automatically exclude his/her access to any systems on behalf of this institution.

General security elements

In this section we will review general security elements. Please note that stuff like POD revolver, self-sustained PODs and 3rd party content on POD was reviewed in the Security of PODs section above.

Use cases and general threats description

Like in any security project we will develop docs like general threats description. Yet, we will complement it with the certain amount of use cases.
You have noticed already that the biz-cases play an important role in defining the Data Space since the beginning of this document. At certain level they will break down into more detailed use-cases, including security use-cases. Such use cases will be important to make sure we develop reliable security for Web 3.0 Data Space. Use-cases will also have to overcome issue like "unusualness" and complexity of the project. We have never seen such a massive use of modern cryptography and security, and just like quantum mechanics, it may require certain experience to get used to it, even for security specialists. Therefore use-cases will play an important role here.

Personal encryption

VC-controlled access to the POD is convenient and rather reliable, but it has certain flaws. E.g. It will allow a hacker access to a POD if the hacker corrupts a notary (CA) and issue a certificate for the name/ID of the POD's user. Of course the attack will be discovered, and the CA & hacker will be found and punished, but the hacker might get the sensitive information leaked at this moment. Therefore the user should be able to encrypt sensitive (personal) data.
We will need methods to do it. Such methods may even use symmetrical keys, i.e. not based on PKI and asymmetric cryptography.

Mobile phones as crypto-engines

We find that mobile phones are reasonable for storing key material and engaging in cryptographic

activities: signing, encrypting, running challenges, traversing chains of trust.
* It is more and more common for phones to have secure enclaves and cryptographic processors (see https://source.android.com/docs/security/features/keystore)
* Software is normally distributed to phones via app stores -- the binaries are signed and cannot be tampered with. Suspicious or compromised in any way applications are removed from the app store. Moreover, it is possible to notify its users of the danger or push automatic software updates with a security patch.
* Phones already provide additional layer of security by requiring to authorize each application separately for using sensitive hardware -- camera, microphone, location. Similarly, an application will not be able to use hardware crypto-processor without requesting permissions from users (one time, or permanent, but easily revocable).
* Phones have built-in authentication mechanisms: face scanners, fingerprint scanners, lock-screens.
* Phones can use various communication channels: NFC, bluetooth, http(s)
* And we always carry them with us.

Organizational methods

Organizational methods will complement all the security technologies we discussed above and will “land” the Web3.0 Data Space on the real world.
We see the following methods here:

- PKI deployment
- Security Audit
- Insurance
- Legal support/prosecution
- Acceptance of e-Reputation

PKI deployment

PKI deployment presents an organizational task of a global scale. We have biz plans with mobile operators and banks which cover this subject.

Security Audit

We will need it at different levels, e.g.:

- during the first launch of the Web 3.0 Data Space we will hire independent security audit
- later on we expect new security audit post-platforms entering the market.

Insurance

We will work with insurance companies to deal with risks in Web3.0 Data Space.

Legal support/prosecution

With development of Web 3.0 Data Space ideas and first launches we will start discussions with authorities. Possible directions are:

- e-Passports. Can we issue them without governments at the birth?
- Support from the legal system (courts, prosecution) in resolving conflicts in Web 3.0 Data Space
- Possibility to launch independent arbitration, independent from state courts.
- etc

Acceptance of e-Reputation

The whole Web3.0 Data Space project is based on the development of trust. We will develop cryptography-based technologies to establish the PKI-based “technological trust”, and we will also work with policy makers and authorities to legalize it within the eIDAS framework.
But one of the most powerful trust comes not from technologies or authorities, but from people themselves. We are going to rely on their opinions in a form of e-Reputation. It is the most reliable, powerful and legitimate mechanism, which will help in evaluating organizations, post-platforms, products and citizens.
Eventually e-Reputation will become the major pillar of the trust in our society. Yet it takes time to adopt it.