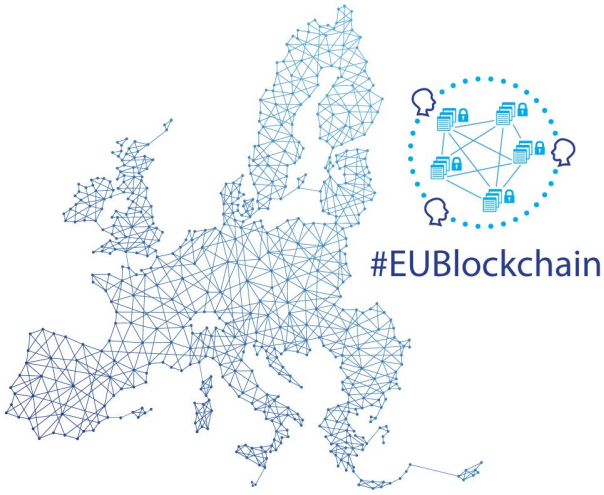
EU Blockchain Observatory and Forum

An initiative of the European Commission

EU BLOCKCHAIN OBSERVATORY AND FORUM

Workshop Report
Government Services and Digital Identity
Brussels, July 5, 2018



By the European Commission, Directorate-General of Communications Networks, Content & Technology.

Author: Tom Lyons
Published on July 23, 2018

Comments and inquiries may be addressed to the following email: info@eublockchainforum.eu

Table of Contents:

Context

From finance to pharmaceuticals, education to entertainment, there is hardly a sector or area of society that cannot potentially be transformed by blockchain technology. That is one reason why the European Commission has been focusing so strongly on it through, among others, efforts like the EU Blockchain Observatory and Forum.

Considering all this potential, it seems only fitting that Europe's governing bodies also look closely at what blockchain can do to improve government works too. That was what brought 36 thought leaders and practitioners to Brussels on July 5 for the Observatory and Forum's workshop on government services and digital identity.

Below are some of the highlights from the day.

Introduction to the day – Pēteris Zigalvis

Pēteris Zigalvis, Head of Unit, Digital Innovation and Blockchain, Digital Single Market, DG CONNECT, and Co-Chair, FinTech Task Force, European Commission, opened the proceedings.

- Welcomed both the members of the European Blockchain Observatory and Forum and the members of the European Blockchain Partnership who had also joined the workshop
- Announced that the three remaining EU States who had not yet signed up to the Partnership had now indicated they would do so. All 28 EU members states will then be official signatories.
- Purpose of the European Blockchain Partnership is to identify use cases for cross-border public services on blockchain, so it was very fitting that members of the Partnership are also at this workshop.
- The Partnership intends to identify these use cases by end of September.
- The Partnership intends to have functional specifications by end of December in order to start the launch of some public services next year.
- These will most likely be in the context of the Connecting Europe Facility.
- Substantial funding for relevant blockchain use cases is also foreseen in the next European budget.

Mapping public services use cases and required foundations – Ken Timsit – EU Blockchain Observatory and Forum

Ken Timsit is a member of the EU Blockchain Observatory and Forum Secretariat and Head of the ConsenSys Paris Office.

- There are a lot of actors, both public and private, experimenting with public and government services use cases across Europe.
- These use cases are usually in the context of making government more efficient, but can also be for reasons of transparency, auditability, and creating more fair and transparent single markets.
- Implementation of blockchain-based government services generally relies on three dimensions: a) use cases, b) infrastructure foundations, c) policies and regulations.
- **Use cases** are citizen's journeys. Among the most important / frequently addressed use cases are:
    - Title registrations: including land or business registry.
    - Healthcare: including data for research or patient ownership of data.
    - Government funding: for example increased transparency in government expenditure.
    - Supply chain traceability: ensuring food safety or traceability of goods.
    - Taxation and excise: Improving VAT systems and fighting VAT fraud.
    - Voting: for instance e-voting or the introduction of liquid democracy.
    - Payments and settlements: including tokenised fiat currencies or asset settlement.
- Accelerating use cases requires solid **infrastructure foundations** that all can leverage, including at least:
    - E-Identity layer / Personal data / KYC standards and infrastructure.
    - Blockchain Platform as a Service, generally a regulated or government sanctioned network of cloud servers which have instances of various blockchain technologies made available to users.
    - Tokenized fiat currencies, meaning tokens backed by financial institutions or central banks that would among other things allow the use of smart contracts to trigger payments in real time.
- On the **policy and regulatory** side, the most important impact that government agencies can have is by driving adoption of the technology, by launching projects themselves or sponsoring public/private projects (examples: Dubai, Singapore). Of course, regulatory measures are needed as well, over time, either by clarifying and adapting current frameworks and/or implementing new rules when needed.

Use Case 1 : Swedish Land Registry – David Suomalainen

David Suomalainen is a lawyer and Jurist at the Lantmäteriet in Sweden.

- The Lantmäteriet is the Swedish mapping, cadastral and land registration authority.
- It is collaborating with banks, the tax authorities, blockchain developers and some other stakeholders to map the real estate transfer process on the blockchain (not the transfer of title).
- Just finished the third phase, which is a successful proof of concept (successful test real estate transfer). Currently no plan to implement the system in a live setting mainly for legal reasons: a contract to sell property in Sweden needs by law to be on paper.
- While the real estate transfer process already worked well in Sweden, the goal of the project was to see if it could be improved, in particular by making it faster, more transparent and less costly.
- Users use e-signatures (such as Telia ID) to sign documents online in the contract engine.
- The contracts are then validated by the nodes on the network, and stored offline in a separate database.
- When all necessary steps are taken and validated, the bill of sale goes to the land registry (which is not on the blockchain).
- The contracts are stored off-chain among other things for GDPR reasons. Certain personal data, which is required to be made public in a real estate transaction in Sweden, is made public in the early stages.
- The solution is a private blockchain developed especially for the project. The goal is to provide technical verification of the data and the transactions. The nodes do not vote on the transactions but merely see to it that the protocol is followed.
- The incentive to create blocks lies in the parties' business models and legal demands that drive the process of selling real estate through to the point where the transaction is registered in the land registry.
- Challenges include cooperation between stakeholders, divergent regulations, policies and strategies among stakeholders, and aligning the decentralized process with stakeholder and legal requirements.
- Advantages include speed, efficiency, and increased trust, as well as making it easier to have both privacy and transparency, as needed (only the parties to the contracts can see the full data; ability to publicize legally required information, but only that).

Use Case 2: VAT systems – Sascha Jafari

Sascha Jafari is a co-founder of summitto, a blockchain company based in the Netherlands. He presented the company's blockchain-based VAT solution.

- EUR 50 billion is lost annually to VAT fraud, most of which goes to organised crime.
- VAT laws are supposed to be unified throughout Europe, but member states deviate, making it difficult among other things for businesses to operate cross-border.
- Trust is the main problem: Tax administrations have to trust companies to correctly report VAT. They can cross-check against tax returns after the fact, but this is expensive and slow. It is easy for dishonest actors to commit invoice fraud.
- Summitto is building the "the world's first blockchain-based, real-time, decentralised, and most importantly confidential triple entry accounting system."
- The summito solution relies on confidential time stamping of every invoice and the provision of aggregate invoice data to the tax authorities.
- By doing so, and assuming the majority of the companies in a country honestly report their invoices, at the end of the month the tax administration can easily identify the likely dishonest actors.
- There are many reasons why blockchain is appropriate for this solution, among them: cryptography (zero-knowledge proof), time stamping of data/invoices (easily done on blockchain), decentralised network architecture (improved data privacy and security compared to centralised solutions, resilient network architecture), transparency for the taxpayer (open source solution that anyone can examine and so understand what tax authorities do with the data), and affordable privacy-by-design.
- GDPR not a problem as only hashes of the invoices are stored on the blockchain and legislation allows for derogation for tax purposes.
- The solution uses proof-of-authority, so no mining as in Bitcoin.
- In terms of governance, member states are always involved and in control of the process.
- Summitto's proof of concept reached 700 transactions per second, which the company reckons covers the needs of a country like the Netherlands.
- Summito is next building a pilot, which will start in Q4.

Infrastructure foundations 1 – Securing public services with blockchain – Henry Rõigas

Henry Rõigas is Senior Policy Officer at Guardtime and the Estonian Representative in the European Blockchain Partnership.

- Estonia was the first nation-state to deploy blockchain technology in a production setting with its Succession Registry (wills) in 2012.
- Estonia uses Guardtime's KSI blockchain, a permissioned blockchain technology.
- The basic data flow is that a user has a digital asset, the public registry computes a hash of it to give it a unique digital fingerprint, the hash is sent to the blockchain, which then returns a proof of registration (KSI signature) to the user, which the user in turn can use to identify the asset's integrity, the signing time and the signing entity.
- KSI blockchain uses proof-of-authority, it aggregates hashes, and the public hash available to users is created once per second (calendar blockchain). This functions as the trust anchor.
- No data goes to the blockchain. The users, whether public or private organisations, develop their own KSI integration, hash the data, and the data hash is then sent to the blockchain.
- This means there are no privacy issues. The system aggregates the hashes and publishes a root hash, which is made public, as well as published monthly in publically witnessed media (the global edition of the Financial Times).
- The blockchain is used for immutability: a piece of information published on the blockchain can be trusted not to have been modified at any point.
- It is also used for trust: Citizens can at any time log in to the system and see who has handled their data (for instance see if the police have run their license plate or a doctor handled their medical data). Users can be sure everything has been securely logged and not tampered with by malicious insiders.
- Such a system can be used in other contexts outside of e-government in Estonia: ensuring the integrity of firmware, log files, backups, etc.
- Estonia also has an e-health registry backed by blockchain which can be used for paperless prescriptions. Blockchain helps handle sensitive medical data by a) securing a piece of data's entry into the database, b) providing solid proof of every entry's state at a given time, and c) maintaining tamper-proof access logs of who added, viewed or modified the data. This makes it easy to detect technical malfunctions, attacks or malicious insiders. It also provides a means for independent verification that data has been handled in a correct way.
- Estonia also uses blockchain for managing digitized paper records (for example wills). The document is scanned, meta data is added to the document (provides attribution), the resulting file is hashed, and the records are chained together and registered on the blockchain. This makes it impossible among other things to delete a record without detection.
- All legislation that is published in the Estonian State Gazette is also registered on the blockchain, providing indisputable proof of each law's state in time.
- These are only a few examples of what Estonia is doing with blockchain. Other projects being looked at include: government cloud, quantum immune ID scheme, connected

vehicle incident handling program (relevant to self-driving cars), and research on distributed registries.
- In general, all Estonian blockchain projects are about:
    - Integrity
    - Auditability
    - Trust

Infrastructure foundations 2 – Blockchain Platform as a Service: Benefits for governments and architecture – Bashar Lazaar

Bashar Lazaar is Director of Operations, Middle East & North Africa, at ConsenSys.

- The most common roadblocks in the journey to blockchain adoption in the public sector include: cost, issues around data sharing, interoperability, explaining the technology and knowledge transfer.
- Having observed some of these challenges, the Dubai government saw the need for the development of a Blockchain Platform as a Service (BPaas) in order to meet its goal of being the first government in the world to execute all applicable transactions on the blockchain by 2020. This approach can serve as an example for other governments contemplating blockchain for public services.
- Key pain points in terms of blockchain adoption include:
    - Speed: the process of use case identification and proof-of-concept building is slow. Issuing RFPs and selecting vendors are other examples of the kinds of things that slow down the process.
    - Cost: it is easy to get caught in a pricy loop of trial and error for things like vendor selection and development.
    - Absence of long-term value creation: agencies creating their own siloed solutions limits network effects.
    - Knowledge transfer: agencies creating their own siloed solutions leads to siloed information and hence limited exchange of experience and best practice. Vendor lock-in can also slow an agency's ability to build internal capabilities with regards to technical development, while BPaaS makes it easier for their respective teams to start prototyping.
- Important pillars of a BPaaS model include:
    - Lowest possible total cost of ownership: TCO should be reduced by providing a platform that enables government agencies to build and prototype around use

cases and proofs-of-concepts relatively easily. Agencies ideally can sign up, choose a protocol, choose the number of nodes, the consensus algorithm, establish governance, and then quickly deploy the network and start experimenting with it. This is easier and faster than using dedicated IT departments or individual vendors chosen via RFPs.
    - Accelerated adoption: Adoption should be sped up by reducing the time lost to trial and error. The platform allows for quick and flexible exploration of blockchain solutions so that agencies can among other things quickly learn what works but also quickly see if blockchain is not appropriate for the solution.
    - Interoperability: While interoperability on the blockchain protocol layer has yet to be developed (with multiple teams globally working on it), application layer interoperability can be explored as an intermediary alternative.
    - Security and Privacy: Certain security standards will be introduced, enabling agencies to build secure proofs-of-concept (important since security is often overlooked in early-stage development).
    - Product-driven: A product-driven solution will be delivered enabling agencies to deploy networks quickly at low cost, as well as lead to a marketplace for dApps that could be shared among agencies.
- Key benefits of the approach include:
    - Fast use case development & validation.
    - Provision of full-stack blockchain infrastructure, developer tools and an integrated development and technical operations environment.
    - Decreased cost of ownership, among other things through a ready-made sandbox environment in which to try new ideas.
    - Quick turnaround for proofs-of-concept.
    - In general, lower cost associated with error, enabling government agencies (relying on a public budget) to have more freedom in experimenting and validating value-add use cases, and building internal capabilities.

Panel: Focus on e-identity

The workshop featured a panel on e-identity. Panelists were:

- Elizabeth Renieris (Evernym)
- Catherine Mulligan (Imperial College)
- Rouven Heck (uPort)
- Kai Wagner (Jolocom)
- Hitesh Tewari (University of Dublin, Trinity College)
- Carlos Pastor (Alastria)
- William Skannerup (VeridenKey)
- Susan Poole (Moderator)

Highlights from the discussion included:

- Blockchain-enabled digital identity can move us to a new “self-sovereign” phase of digital identity in which we can decouple identity providers from their dual role as certificate authorities and registries. It allows individuals (as well as organisations and machines) to register their identities themselves, and load trust onto these identities by different means.

- Standards will play an important role in developing blockchain-based, self-sovereign digital identities. The World Wide Web Consortium and the Digital Identity Foundation are two important standards bodies in this space.
- There will likely be a need for new protocols at the Internet layer to provide identity, privacy and security (i.e., below the blockchain layer). These should also address basic ethical and moral questions associated with identity.
- Blockchain-based digital identity systems will have to take into account how identity attributes change over time during a person’s natural life cycle, and will need to offer different levels of transparency depending on the context (e.g., verifying that someone is over 18 without providing a birth date).
- Inclusivity is an important consideration. We need among others to take into account vulnerable populations, children, migrants, and those without access to devices or the Internet. This makes offline governance also very important (questions of guardianship, key management, etc.).

- Another important question in digital identity is where identity data gets stored.
- The most relevant options today for digital identity storage are the mobile phone, dedicated hardware (like smart cards), or the cloud.
    - Mobile phones are widespread (most people have one), versatile (easy to use and update), and personal (in control of the user, hence decentralized). But they are not ubiquitous (not everyone has one or knows how to use one) nor do all phones contain sophisticated enough hardware (cryptographic chips). Phones can also be lost or stolen (loss of phone means loss of identity?), may not always be connected to the Internet, and could be prone to tampering/hacking.
    - Dedicated hardware like smart cards can have information hardcoded into them, making them tamper-resistant, and are cheap to produce so that they could be provided to all individuals in a population at little or no cost to them. But they are inflexible (hard to update), generally must be used with another device (do not contain a screen or any connectivity), are not controlled by the individual (requiring the user to trust the provider), and are not decentralized.
    - Cloud-based identity is flexible, easy to access, provides security against loss of identity (data is backed up in the cloud), and can be accessed by a large number of devices. But cloud identity also requires users to trust the provider, can be expensive to setup and maintain, and is not decentralized.

- The question of who pays for the development and maintenance of blockchain-based identity platforms is key too. Today the paradigm on public blockchains involves incentives for people to participate in running the network, but it is unclear if such incentives will be sufficient to maintain such a network over a whole lifetime, which is a risk. This brings up the question of whether identity platforms should be seen as a public good that governments should be (solely?) responsible for.

- A similarly important question is the source of identity attestations.
- Today generally institutions like governments, banks or utilities provide identity attestations, and will continue to do so. Increasingly social media (Facebook) or other tech companies (Google) have become sources of identity too.
- Different locations/cultures seem to place trust in different types of providers. In some areas people seem to trust companies more, in others governments, in others individuals (the local doctor).
- Identity can also be seen as the sum of all your transactions, something you accrue over time and can save for future use.
- In the end there will likely not be one source of identity but many different sources, applicable to different contexts (official identity, work identity, social identity).
- Self-sovereign identity can level the playing field between online identity providers and the individual when it comes to using identity information cross-contextually. Today in the offline world a person can use a driver's license to prove his or her age in a bar. A self-sovereign identity, which an individual controls and can produce as needed, allows for similar interactions online.
- With self-sovereign identity entities (governments, financial institutions, businesses) will authenticate themselves to us as much as we authenticate ourselves to them.

Discussion: Action & Roadmap, approach at EU level

The day ended with an open discussion among all the participants at the Workshop. Among the points raised were:

- It is very important to get digital identity right because there are risks involved; getting it wrong can negatively impact people's lives. This risk is however mitigated by the fact that digital identity is likely not to be one single thing but more a set of statements from different sources.
- In the EC's FinTech Action Plan there is an action to coordinate and consolidate the general criteria and guidelines for regulatory sandboxes, including with regards to reporting on results. While this is geared mainly toward financial services, such sandboxes are also relevant to the digital identity/personal data discussion.

- As Europe moves public services onto blockchain as part of the European Blockchain Partnership, it will be a vehicle for cooperation amongst Member States to exchange experience and expertise in technical and regulatory fields and prepare for the launch of EU-wide blockchain applications across the Digital Single Market for the benefit of the public and private sectors.
- While there is a lot of information about projects and initiatives around blockchain in government services or digital identity, it can be hard to get concrete information about how they work; more transparency about the technology behind solutions could be helpful to the community.
- While standards are clearly going to be important, blockchain is still a very young technology. It can be counterproductive to introduce standards too early and run the risk of curtailing innovation.
- Education was seen as very important on a number of levels. The general public needs to be educated on blockchain or new use cases to mitigate against natural resistance to change. Self-sovereign identity for instance implies new capabilities but also new responsibilities for individuals, which they will have to understand. Similarly technologists and entrepreneurs will have to understand the paradigm shift that blockchain represents so they can develop use cases that truly make use of blockchain's capabilities and are not, for instance, simply a database in another guise.
- Usability and user experience will be key factors in the adoption of blockchain-based dApps by the general public, whether or not the public is aware that there is a blockchain under the hood.

Priority use cases at EU level

Over the course of the workshop, the following priority use cases for Europe were identified and discussed:

- Identity, both for citizens and for moral persons (companies/organizations)
    - Examples: Zug residents' IDs, Estonian e-identity
- Shared visibility over workflows and processes by multiple administrations
    - Examples: Sharing data between public administrations, Italy
- Blockchain-based notarisation of official titles and certificates, particularly public ones
    - Examples: Swedish Land Registry, Illinois Birth Registry, Dubai Business Registry
- Blockchain-based notarisation of the use of public utilities and public services by multiple parties, to facilitate usage-based invoicing and reconciliation
    - Examples: Blockchain supported Grid, UK
- Matching of Purchase Orders and Invoices for VAT tracking purposes
    - Examples: Tax collection and electronic invoice issuance, China

- Blockchain as a supporting tool to monitor and analyze compliance with regulations (eg. GDPR, AML, Loi Hamon in France)
    - Blockchain based access control

Appendix

Official agenda

Time	Duration	Activity
9:30	20min	**Introduction to the day - Peteris Zigalvis**
9:50	30 min	**Presentation - Mapping public services use cases and required foundations -** EU Blockchain Observatory and Forum
10:20	50min	**Use Case 1 : Land Registry - David Suomalainen** (presentation + discussion)
11:10	50min	**Use Case 2: VAT systems - Sascha Jafari** (presentation + discussion)
12:00-13:00 Lunch break		
13:00	50min	**Infrastructure foundations (**2 short presentations: Example of Estonia - Henry Roigas; BPaaS: Benefits for govs and architecture - Bashar Lazaar) +discussion
13:50	1h10	**Focus on e-identity** (panel + discussion) Elizabeth Renieris (Evernym), Catherine Mulligan (Imperial College), Rouven Heck (uPort), Kai Wagner (Jolocom), Hitesh Tewari (University of Dublin, Trinity College), Carlos Pastor (Alastria), William Skannerup (VeridenKey)
15:00	50min	**Collective structured discussion: action & roadmap, approach at EU level** Discussion among all participants
15:50	End of the Observatory and Forum workshop	

List of registered participants

Alessandro Piazza Anja Bedford, Blockchain Lead - Deutsche	Ivona Skultetyova, Lecturer/Researcher - Tilburg University

Bank Catherine Mulligan, Visiting Researcher - Imperial College London Paloma Gonzalez Marieke (Maria) van Putten, Program manager - Ministerie van Economische Zaken en Klimaat Guy De Ridder Jeroen Demuynck, Innovation & Technology Consultant - City of Antwerp Vittorio Allegri, Policy Advisor - EMF-ECBC Koen Vingerhoets, Project Coordinator - Belfius Rouven Heck, Project Lead - uPort Stefan Beyer, Head of R&D - S2 Grupo Carlos Pastor Matut, Digital Identity Leader - Alastria Erik Isak Bengtzboe David Suomalainen, Legal Adviser - Lantmäteriet Claire-Marie Healy, Senior Project Manager - GSMA Francisco Santos Kai Christian Wagner, Sustainable Business Development - Jolocom Jelle Hoedemaekers, Expert - Standardisation bij - Agoria	Daniel Du Seuil, Program mamanager - Informatie Vlaanderen Rasa Uzdavinyte, Consultant Louis Margot-Duclot, CEO - 97 ALAIN ROSET, Prospective - La Poste Hitesh Tewari, Assistant Professor - Trinity College Dublin Aleksandar Arsov Wim Stalmans, Founder - The Blockchain Academy Jean-Luc Verhelst, Author of Bitcoin, the Blockchain and Beyond Leonardo Vidal, Managing Director - Torlabix Javier Sebastián, Head of Blockchain - BBVA Elizabeth Renieris, Global Policy Counsel - Evernym Carlo Wolny, Founder - d.work Michel Avital, Professor - Copenhagen Business School Peter Stas Henry Rõigas, Senior Policy Officer - Guardtime Monica Vidal Tamás Chlepkó, Senior project manager of strategic projects - Tax and Customs of Hungary

Presentation slides

Presentation slides can be downloaded here

Video recordings

Video recordings of the sessions will be available here

Related links

- Lantmäteriet website (Swedish): https://www.lantmateriet.se/
- Lantmäteriet Wikipedia entry (English): https://en.wikipedia.org/wiki/Lantm%C3%A4teriet
- Summitto website (English): http://summitto.com
- e-Estonia website (English): https://e-estonia.com/
- European Blockchain Partnership official annoucenment (English): https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership