13

Advancing Digital Transformation in the Public Sector with Blockchain: A View from the European Union

Emanuele Baldacci and Joao Rodrigues Frade

Introduction

Digital transformation is an essential policy priority for the public sector. The Covid-19 experience set the motion for further acceleration of technological transfer making digitalization a dominant priority for the EU. One of the main findings of the pandemic was that public or private entities with an efficient digital layer were able to absorb better the shocks of the supply chain or the collapse in the demand, compared to entities with purely analogue operational models. The other major finding was that true operational resilience does not come from *digitization* per se (having in place digital capacity), but

[1]Weill, P. and S. L. Woerner, What's You Digital Business Model? (Harvard Business Review Press: Cambridge, MA).

Personal views hereby presented are the authors' only, and should not in any way be construed as to represent an official position of the European Commission.

E. Baldacci (✉) · J. R. Frade
European Commission's Directorate-General for Informatics, Brussels, Belgium
e-mail: emanuele.baldacci@ec.europa.eu

J. R. Frade
e-mail: joao.rodrigues-frade@ec.europa.eu

E. Kaili and D. Psarrakis (eds.), *Disintermediation Economics*,
https://doi.org/10.1007/978-3-030-65781-9_13

rather from *digitalization* (when digital capacity is coupled with organizational adaptations and procedures that blend digital technologies with human routines).[1]

The European Union public authorities, responding to the major need in creating a European digital capacity in addressing major issues affecting the resilience of the EU economy, adopted a strategy of digital transformation and sustainability. This strategy was reflected in the adoption of a comprehensive Just Transition Mechanism and a set of digital policy initiatives like the Paper of the Digital Future of Europe, the EU Data Strategy and the White Paper on Artificial Intelligence. Blockchain is an integral part of this policy.

The European Institutions responded immediately to the windows of opportunity that blockchain technology opened for better public services. The Directorate-General for Informatics, DG DIGT, of the European Commission is a pioneer in the digitalization of public sector creating a space of innovation and experimentation through a wide range of use cases that, when tested, can be then efficiently trickled down to the public sectors of the Member States. To make blockchain a success story of the EU, this diffusion effort is being carried out in close collaboration with the Directorate-General for Communications Networks, Content and Technology, DG CNECT, and the Member States.

The Blockchain and the Public Sector: Principles and Experience from the European Commission

The hype of bitcoin and the publicity of the Initial Coin Offerings was accompanied by a libertarian political narrative. According to technology enthusiasts, Blockchain has come to replace the existing Institutional setting with a "new one", where an automated decision-making architecture, based on pre-determined rules, will ensure that the agency risks and costs the world experienced in the last global financial meltdown, will not be repeated. In early 2020, we see that the experience accumulated by the blockchain projects around the world of the last four years, lead us to assume that the current technological capabilities of blockchain technology are more modest than the initial expectations of the enthusiasts. It also lead us to assume that disintermediation does not require decentralization, and that the public sector is a very useful field for experimentation for services to the citizens and to public authorities.

Bibliography proposes a wide range of distributed ledger taxonomies and definitions. For simplicity, we can define a complete blockchain solution as the one that includes a set of five digital properties: disintermediation, immutability, encryption, tokenization and decentralization. Though the development of current DLT applications we see in private and public initiatives include many, or even all of these digital properties, the vast majority of successful applications so far rely on the first three.[2] Solutions of this type, can be defined rather as *blockchain inspired* rather than *blockchain complete*. In practical terms, blockchain inspired solutions, also associated with centralized permissioned blockchain architectures, reflect the current limits of the technology and the need to hedge significant scalability risks (like the ones we encountered in the ethereum and bitcoin blockchains) as well as operational risks, including the risks of *forking* and the risk of a *single point of failure*.

Understanding the limits of the technology at a certain point in time is a major challenge for a public sector leader or change agent. This requires leaders in the public sector to spot what a certain architecture can deliver early enough and make bold decisions that reflect the principle "efficiency first" rather than "technology first". In the case of blockchain and the public sector this is sine qua non for two reasons.

First, a public institution that aspires to make a blockchain transformation should be able to select among different governance architectures. Technical experts, in most of the time, propose these governance architectures and the public official should trust his experts. If the proposal comes from a technology enthusiast, an expert who acts on the principle "technology first", the blockchain project could end up with thousands of lines of codes of smart contract, inefficient to deliver and inefficient to scale. For example, in a blockchain solution that aims to verify the educational credentials of a citizen, relying solely on symmetrical smart contract architectures could be, with the current status of the technology, an architectural mistake. An alternative solution, would be to use a standard "digital post" solution, a solution that collects and transmits information between different systems, thereby providing the means for blockchain-based systems to interact with common databases and real-world people.[3] In the degree verification case, if a citizen claims having a graduate degree from a certain university, the access point of the digital post could be used to connect to the database of the university to:

[2] Furlonger and Uzureau (2020), The Real Business of Blockchain: How Leaders Can Create Value in a New Digital Age (Harvard Business Review Press, Cambridge, MA).

[3] Primavera de Filippi and Aaron Write (2018), Blockchain and the Law: The Rule of Code (Harvard university press, Cambridge, MA).

- "ask" if the provided metadata is consistent with the metadata of the university, and
- the resulting "yes, it is" or "no, it isn't" would then be recorded in an immutable ledger.

The second reason is that the public sector, when tries to fulfil technological transformation initiatives, takes into its balance sheet every related risk: technological risk, operational risk, financial risk, procurement risk, etc. If a project fails, as it is possible to happen when somebody experiments with a new and still evolving technology, then either new funds should be directed to the project (a situation that is not always convenient from a budgetary point of view), or has to be abandoned (a situation that economically is not desirable if the potential is high).

The European Commission made careful decisions around prudently selected blockchain use-cases taking into account technological, operational, financial and scalability risks with the intention to address the "trust challenge" around the technology and not just to solve a "data synchronicity challenge", as for example in some of the most known cases in the banking sector or in the shipping industry.

When it comes to the public sector, governmental entities are important intermediaries of many transactions happening in our society as the documents they issue or certify are a common way to verify information about people (in the form of identity cards, work permits, driving licences, etc.) and goods (such as their origin, compliance to safety rules, etc.). Official documents and other sensitive information inherit the trust deposited in the governmental authenticities that issue them and therefore become key trust facilitators among the many players transacting in the single market, both within and across borders. In the era of misinformation, it is essential to address the challenge of digital fraud, in particular when digital documents are quite easy to duplicate and to modify. Governments, and society, need technology to verify the authenticity of information it handles. Blockchain is a trustworthy technological option that can increase the transparency of information in the public records, ensure access to the citizens and provide verifiable certified and authenticated data, not only within the national limits, but also cross-border. In that sense, blockchain is a strategic tool for higher quality public services that the citizens can enjoy with limited transaction costs.

Given the importance of the authenticity of information for well-functioning administrative processes, especially when applied across borders, this paper looks at the notarization and reconciliation of information as key

functionalities offered by blockchain to public administrations engaged in reducing bureaucracy while increasing efficiency and transparency.

A Short Introduction to Blockchain Technology

> "Truly innovative deployments of blockchain require a match between blockchain's specific benefits and use cases that enable realization of these benefits, followed by dedicated hard work to get it right and embed in organizations and industries".[4]

In Europe and elsewhere, blockchain technology is gradually becoming a sound complement to classical trust enabling technologies[5] such as:

- eSignatures, the expression in an electronic format of a person's agreement to the content of a document or set of data;
- eSeals, the electronic equivalent of a stamp that is applied on a document to guarantee its origin and integrity and
- eTimestamps, an electronic stamp issued to prove that a document existed at a point-in-time.

As explained in the picture below, blockchain builds on these technologies to create a highly distributed, tamper-resistant ledger. In short, unlike the above-mentioned classical technologies, blockchain has its information stored across a series of nodes in a network, rather than in a single location. In **short, blockchain does recordkeeping in a verifiable and permanent way** (Fig. 13.1).

A good example of blockchain's disruptive potential is its application for tracking the history and accurate "state" of consumer products in highly fragmented supply chains. It should be noted that there are around 4 trillion consumer products produced and launched onto global markets every year. Each one of these products is composed of several materials, sub-components and ingredients. Each product is subject to many transactions as it becomes sourced, produced, shipped, stored and retailed before being used and eventually disposed of, perhaps remanufactured or recycled. Given the distributed

[4] World Economic Forum's White Paper "Blockchain Beyond the Hype—A Practical Framework for Business Leaders".

[5] These definitions are aligned to the eIDAS regulatory framework: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

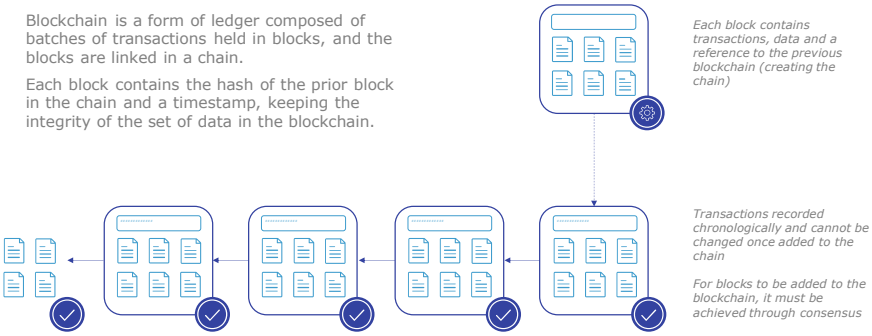


Fig. 13.1 How blockchain ledgers work (*Source* DIGIT, European Commission)

nature of modern supply chains and the many steps that they encapsulate, blockchain technology can be the right answer for keeping trusted records. Trusted recordkeeping and the authenticity of information are of the essence to private sector entities when carrying out their activities and to public sector entities when supervising the events associated to these activities and the lifecycle of consumer products.

Blockchain Applied to the Public Sector

It is important to point out that blockchain is not only interesting to the private sector. Blockchain's unique features are also important for the digital transformation of public administrations. Given the importance of the authenticity of information for well-functioning administrative processes, especially when applied across borders, this chapter explains how blockchain-led disintermediation may be a game changer for the public sector. Blockchain is a very promising technology for partial or full disintermediation of recurrent labour-intensive processes of public administrations. This is particularly important when it comes to:

- **Reconciliation of information;**
- **Notarisation of information.**

The use of blockchain in such processes is likely to advance the digital transformation of the public sector, making it on one hand more efficient (i.e. by saving time and money) and, on the other, more effective (i.e. by increasing

trust and transparency). The next sections will look into how blockchain-based reconciliation and notarization of information can be done in practice and the challenges associated to their adoption.

Reconciliation of Information

What Is the Problem to Be Solved?

Reconciliation of information is a quite prevalent activity in a public administration from accounting to human resources processes (internal focus). One good example of such reconciliation processes is the validation of the legal entities[6] with whom a public administration transacts. A legal entity is typically a private company or a natural person that has some sort of contractual relationship with the public administration. These validation processes often involve several standard checks about the legal entity, such as their solvency, and the status of their bank account. A typical validation workflow can be split into two distinct septs:

Step 1. Checks focusing on the entity itself:

- Does the person or company exist?
- Is it a reputable person or company?

Step 2. Checks focusing on the bank account of the entity:

- Does the bank account exist?
- Is it from a reputable bank?

The typical solution to address the reconciliation problem would be to centralize the verification processes in a single central clearing entity. The level of automation and complexity of the clearing entity can be high or low depending on the number of manual checks and the stakeholders involved in providing this information. However, often times, the dependency on a single central entity is not desirable given that it becomes a "single point of failure".

[6] Legal Entity File of the European Commission: http://ec.europa.eu/budget/library/contracts_grants/info_contracts/legal_entities/legEnt_privComp_en.pdf.

How to Disintermediate?

Blockchain makes it possible to disintermediate such centralized processes. This can be achieved by using a combination of classical electronic signatures (to verify the origin and integrity of the information) and a blockchain (to ensure traceability and auditability). This means that the reconciliation of information no longer needs to be done centrally by a single entity. Blockchain-based processes can accomplish the same results using a common distributed ledger. Once in place, an increasing number of trusted verifiers can check information in real time without needing to enquire the central entity. At the same time, and as a next step, a number of manual/labour-intensive checks may be suppressed via the use of smart contracts technology. Some of the benefits of such approach are listed hereunder:

- The time cycle to sign contracts is shortened and the overall process accelerated;
- Payment delays, accompanied with their expensive interests are reduced;
- Keeping the register of legal entities in a much more expedient way as re-running the verification process would be done at a fraction of its current cost;
- Virtually costless audit processes as the blockchain maintains information about the transactions associated to the verification process, from its creation to subsequent controls.

What Are the Challenges to Make This a Reality?

As explained by Cathy Barrera[7] in her post "Hidden Costs of Verification", the information about legal entities and bank accounts is not blockchain-native and, in most cases, it cannot be accessed by a smart contract through an application's interface (a.k.a. API). These barriers would need to be overcome for blockchain to fully deliver its potential benefits. Once these barriers are fully suppressed, the use of blockchain would set in motion the disintermediation of centralizing clearing and the associated auditing processes.

[7] Hidden Costs of Verification: https://goo.gl/kP5Lsw.

Notarization of Information

What Is the Problem to Be Solved?

Notarization of information is crucial to guarantee the authenticity and integrity of documents, and information in general, when completing administrative processes with a public sector organization such as:

- Requesting proof of registration of birth;
- Submitting a tax declaration;
- Registering a change of address;
- (…)

In some cases, citizens and businesses are still required to provide paper documents that are certified as authentic via a physical authenticity stamp (the so-called apostille). The verification processes of these documents are manual, time-consuming and costly for public administrations providing public services (external focus). When moving to digital processes, the importance of ensuring the authenticity and integrity of documents increases as, in general, a document in digital format is much easier to manipulate and falsify. Hence, in the world of digitized processes, there is a clear need to reduce the cost of verification and auditability of information.

How to Disintermediate?

Blockchain greatly facilitates the auditability of documents by recording their registration time together with key metadata about the document itself and the entity providing it. This not only ensures their authenticity and integrity but also future auditability. All this makes the automation of compliance checks in time-sensitive processes possible. Furthermore, it cuts red tape and guarantees seamless information verification. For public sector administrations to receive effortlessly notarized documents from persons and legal entities, a solution would be to establish a common blockchain-based "registry". This registry would offer notarization services to citizens, businesses and public administrations alike as well as the associated functionality to verify their authenticity/integrity in real time. This would in turn increase the efficiency and transparency of public services at a lower cost.

What Are the Challenges to Make This a Reality?

To make such a solution feasible, data quality is an important element in order to ensure the quality of information. Data quality ensures the accuracy, completeness and consistency of the information that is registered by the person or legal entity.

Another main challenge, not specific to blockchain but common to any online technology, is accurate identity provision and verification. Nonetheless, given its distributed nature, blockchain tries to move towards decentralized Identity/Self-Sovereign Identity (SSI[8]) concepts, involving not one but several identity providers.

The European Blockchain Services Infrastructure (EBSI)

Europe is working on a cutting-edge blockchain infrastructure for public administrations that will offer both notarization and reconciliation capabilities. In simple words, the European Commission and the Member States are currently working together to put blockchain technology at the service of public administrations for the purpose of verification of information, making it trustworthy. The result of this work will be the first EU-wide blockchain infrastructure, driven by the public sector, that respects European values with high level of data security, data protection and privacy. This section will provide detailed information about this EU-wide initiative known as the European Blockchain Services Infrastructure (EBSI).[9]

History

In 2018, the European Commission launched the European Blockchain Partnership (EBP), 26 Member States and Norway, as a preliminary step for the establishment of an EU-wide European Blockchain Services Infrastructure (EBSI). The EBSI will be materialized as a network of distributed nodes across Europe (the blockchain). On 14 February 2019, the European

[8] Self-Sovereign Identity is an emerging trend associated with the way identity is managed in the digital world. According it, users should be able to create and control their own identity, without relying on any sort of centralized authority. This may be achieved using Verifiable Claims, meaning that Users can control the pieces of information they want to share with third parties to identify themselves.

[9] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI.

Commission published the 2019 Telecommunications Work Programme of the Connecting Europe Facility (CEF)[10] creating the funding conditions for the launch of the EBSI. When fully in operation around 2021, the EBSI will enable the redesign of public services, better security and accountability in line with the approach advocated by current digital policy of the European Union, to which the Member States have committed themselves in the Tallinn Declaration on eGovernment.[11] Furthermore, the EBSI will also contribute and interact with the digital ecosystem of interoperability-enabling technologies that the European Commission is actively promoting through the "Connecting Europe".[12]

Guiding Principles

It is clear that a blockchain focusing on public administrations must be built around strong guiding principles such as:

- **Public Permissioned:** The identity of all participating nodes must be governed;
- **Decentralized:** Each member should run its own node or set of nodes;
- **Scalable:** Support of high-throughput and high number of nodes;
- **Open Specifications:** EU Public License and free from IPR;
- **Sustainable:** Energy-efficient consensus mechanism;
- **Interoperable:** should foster interoperability via alignment with the work of standardization bodies such as ISO, CEN or ETSI.

The table below shows how EBSI compares to other types of blockchain (Table 13.1).

The above means that EBSI Stack Nodes will exist across Europe in the EU Member States. The EBSI stack will provide:

- **Increased resilience** from a network of systems and data that can take over from failed nodes and distributes proofs of actions geographically;
- **Enhanced cyber security** from the enforcement of encryption practices;

[10] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL.

[11] All the European Union Member States and EFTA countries signed the 'eGovernement Declaration' in Tallin on 6 October 2017. The text of the Declaration is available at http://ec.europa.eu/newsroom/document.cfm?doc_id=47559.

[12] These include eID, eSignature among others, for more information: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Building+Blocks and https://ec.europa.eu/isa2/solutions_enprogram.

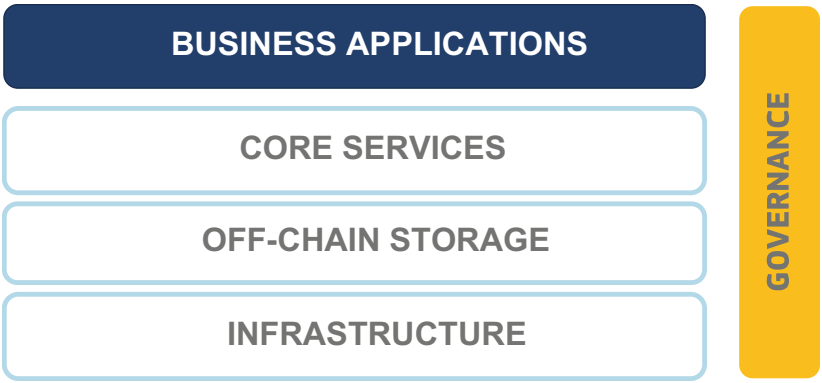
Table 13.1 EBSI compared to other types of blockchain—DIGIT, European Commission

	Allow anyone to join the network, to write to the network and to read the transactions from those networks	Whitelisted access is required, all transactions are publicly viewable	Only people with permission can read or write to such systems
Write access	Permissionless	Permissioned	Permissioned
Read access	Public	Public	Private
Topology	Distributed nodes	Distributed nodes	Distributed nodes
Typical consensus model	Proof of Work/Proof of Stake	Proof of Authority	Practical Byzantine Fault Tolerance, Raft
Example	Bitcoin/Ethereum/ECS/Tezos	European Blockchain Services Infrastructure (EBSI)	Hyperledger Fabric/Corda

- **Enhanced performance** for connected systems through the use of local copies of data;
- **Enhanced trust** with the use of blockchain smart contracts and ledgers.

The diagram below shows EBSI's layered architecture, the next section will explain it in more detail (Table 13.2).

Table 13.2 EBSI's layered architecture



Source DIGIT, European Commission

Architecture

The **infrastructure layer** is EBSI's network of interconnected nodes hosted by the European Commission and the Member States. Each node operates independently of each other and each host organization is responsible for its daily operation. It is worth highlighting that organizations hosting an EBSI node will be subject to the terms and conditions to be reflected in EBSI's governance arrangements.

The **storage layer** is where the data that is not kept on-chain is stored. Similar to the node, the off-chain storage is also under the responsibility of the host organization and will be subject to the terms and conditions defined by EBSI's governance.

The **core services layer** is the interfaces exposed by the EBSI nodes enabling them to support the integration of business applications with EBSI. These interfaces are associated to EBSI's Use Cases. Below are a few examples:

- **Notarization Use Case:** Upon signing information (to ensure its integrity and authorship), public administrations will be able to register it in the EBSI ledger. Technically, this will be done by using the hash of the document in a GDPR compliant way;
- **Diploma Use Case:** Universities will be able to turn diplomas into a set of tamper-evident claims and metadata that cryptographically prove who issued it and who was issued to;
- **European Self-Sovereign Identity Framework (ESSIF) Use Case:** Users of EBSI will be identified through a new type of identifier for "self-sovereign" digital identity known as Decentralized Identifiers (DIDs). Furthermore, the ESSIF being developed alongside, and within, will rely on EBSI's blockchain as its trusted registry.

The vast ecosystem of public and private sector entities will develop EBSI's business applications layer according to the guiding principles shown above.

Next Steps

The EBSI and its services are currently under testing. These tests involve a multiplicity of entities including the European Commission and public administrations of several Member States. Once this phase is concluded, the EBSI will go live. Full operations are expected in 2021.

Bibliography

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

Karl Wüst and Arthur Gervais. Do you need a Blockchain? 2017.

European Commission. Legal Entities. https://ec.europa.eu/info/publications/legal-entities_en.

Cathy Barrera. Hidden Costs of Verification. 2018.

Directive 2012/17/EU of the European Parliament and of the Council of 13 June 2012 amending Council Directive 89/666/EEC and Directives 2005/56/EC and 2009/101/EC of the European Parliament and of the Council as regards the interconnection of central, commercial and companies registers Text with EEA relevance. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012L0017.

European Commission. https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership. 2018.

European Commission. https://ec.europa.eu/digital-single-market/en/blockchain-technologies.

European Commission. https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership. 2018.

Ministerial Declaration on eGovernment—The Tallinn Declaration. https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovernment-tallinn-declaration. 2017.

Regulation (EU) No 1316/2013 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility, amending Regulation (EU) No 913/2010 and repealing Regulations (EC) No 680/2007 and (EC) No 67/2010 Text with EEA relevance. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R1316.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

World Economic Forum's White paper "Blockchain Beyond the Hype—A Practical Framework for Business Leaders".

European Commission. Blockchain for digital government, an assessment of pioneering implementations in public services: https://joinup.ec.europa.eu/sites/default/files/document/2019-04/JRC115049%20blockchain%20for%20digital%20government.pdf.