Distributed Ledger Technologies and Blockchain:

Perspectives for eu-LISA and the Large-scale IT Systems

Research and Technology Monitoring Report

2019

Legal notice

This report is public. Reproduction is authorised, except for commercial purposes, provided that the source is acknowledged.

This report has been produced to provide input for discussion on the large-scale IT systems operated by eu-LISA and associated infrastructures at the Agency and the Agency's stakeholders. Any views expressed in the report are entirely those of the authors and are not necessarily the views of the Agency itself.

Where direct or indirect references are made to products made available by specific vendors, this should not be taken as any endorsement of them by the Agency, as references are provided purely for the purposes of illustrating the arguments made in the report. All the web-address links provided were operational on 25 November 2019.

Contact

To contact the authors for further information, please email: research@eulisa.europa.eu
For enquiries regarding further use of the report or the information contained herein, please contact:
communication@eulisa.europa.eu

ISBN 978-92-95217-55-3
DOI:10.2857/111687
Catalogue number: EL-03-19-727-EN-N

Contents

Executive summary

Few topics have gained as much attention in the world of information technology as blockchain and distributed ledger technologies (DLTs), making it almost inevitable that entities involved in the development and management of information technology (IT) systems unwrap the technology for themselves and give some consideration to its relevance in their context. The research and technology monitoring function of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) decided therefore to analyse whether blockchain, its functionalities and the use cases in other domains might have strategic and/or technical relevance for the Agency's future work.

Blockchain has integrated several attractive functionalities – logging and timestamping of transactions, linked recording and digital signing, cryptography, access and permission, digital identity, consensus algorithms – under a single umbrella, making the technologies making the technologies more appealing. At the same time, it is often overlooked that many of those functionalities have been successfully introduced and applied in distributed computing and in e-governance frameworks prior to the surge in the development of blockchain. With a wider promotion, blockchain or distributed ledger infrastructures are nevertheless being intensively developed, supported and introduced to markets that until now have not been able to reach those functionalities for reasons of preference, accessibility or hesitancy. Admittedly, these technologies have great potential for disrupting data-sharing principles across industries and governments, though the current platforms and standards available are still far from being ready for widespread adoption in the public sector.

The research undertaken aims to give a dedicated insight into the functionalities of the technologies and the relevant legislative environment, in order to provide discussion space for discovering the use cases in which the data exchange ecosystem built around cross-EU large-scale IT systems could benefit from a blockchain or distributed ledger approach. The presentation of possible use cases serves as encouragement to the industry and academia to include the large-scale IT systems domain in their further work on technology development. The discussion following those insights reflects on the technology's potential, and aims to support expectation management and industry aspirations.

An overview of the EU-level legislative and policy environment suggests that application of blockchain or DLTs in the public sector within the EU, or for large-scale IT systems in the Justice and Home Affairs area, requires taking into account the existing and foreseen e-governance and interoperability structures. For systems managed by eu-LISA, the scope of dedicated regulations, implementing acts and accepted technical standards provides context for assessing the potential of new technologies.

Despite the expectations that blockchain and DLTs will revolutionise the provision of public services, the current technological advancements are still a few important steps away from actual implementation both in government services and in large-scale IT systems. First, in order to be integrated into eu-LISA's technology portfolio, blockchain and DLTs, plus their functional components, need to demonstrate reliability, trustworthiness and long-term sustainability. Second, for technologies – whether blockchain, DLTs or any other – to be successfully integrated into an existing government IT service infrastructure, they must be interoperable with different ledgers as well as existing ecosystem structures, ensuring that data can be exchanged with partners outside one's immediate ecosystem. eu-LISA envisages several use cases in which the functionalities of the technologies discussed would be beneficial for the end user or the systems, if the above-mentioned requirements were met.

The conclusion of the study is that, despite some applications of blockchain and DLTs emerging in some domains, these technologies are yet to prove that they may be applied reliably, especially for cross-EU

large-scale IT systems. Nevertheless, some elements or principles of blockchain (e.g. transaction timestamping and decentralisation of data storage) are definitely relevant and are already being applied.

eu-LISA anticipates further business use case analysis driven by the industry. However, it is important to underline that any implementation of those technologies into data exchange frameworks (ecosystems) that involve public administrations, or large-scale IT systems, should be requirements-driven rather than technology-led.

Further work on the individual functionalities of the technologies, proof-of-concept solutions to elaborate the applicability and coordination of development of standards, is what is most needed to prove the actual potential worth and capacities of the technologies and their various elements. Furthermore, both industry and academia should continue working on the systematic categorisation of the terminology, and on approaches and applications according to their functionalities, to ensure that the key stakeholders can assess the value the technology brings to their businesses.

Looking ahead, eu-LISA remains rather conservative about the relevance of blockchain within large-scale IT systems, but is open to the possible integration of data streams from approved blockchain ecosystems. The Agency will therefore be ready to engage in technical discussions with industry and decision makers in order to support the alignment of standards necessary for current potential to become future reality.

Introduction

Following the successes of cryptocurrencies and the widespread general promotion of blockchain and distributed ledger technologies (DLTs), stakeholders in various business fields and in public sector are actively mapping whether and how their data exchange, trust creation and activity logging, timestamping or identity management tools could benefit from those technological evolutions. Today, eu-LISA is responsible for three operational and three new large-scale IT systems, and working on interoperability between those systems. In view of the ongoing transformation, we believe it is the right time to review whether those new technologies may also have an influence on the core business of eu-LISA in the future.

Review of the available literature suggests that there are different views on what blockchain and DLTs are and what they can do. Transaction timestamping, secure logging, hashing or digital signing of records, linking archive data are often described as unique capacities of blockchain, yet those are in fact functionalities that are already attainable with conventional IT tools. Those functionalities have nevertheless become better known and more fully explored with the wider publicity of blockchain-based use cases, and have a great potential of providing a technology shift to trusted data exchange across domains.

Together with the Member States, the European Commission has been working intensively on the European Interoperability (EIF) and Electronic Identification and Trust Services for Electronic Transactions (eIDAS) Frameworks aimed at structuring tools for creating trust ecosystems to achieve interoperable cross-border data exchange. It has also recently started working on a number of initiatives related to blockchain[1]: the signing of the Declaration on the European Partnership on Blockchain, the establishment of the dedicated Blockchain Observatory and Forum and empowerment of the International Association for Trusted Blockchain Applications (INATBA) are the few first steps towards consolidating the future vision for the adoption of blockchain technologies in the EU and beyond. Both of these lines of initiatives coordinate the development of specifications and standards of services, the consolidation of reusable software components, prepare relevant legislation, contribute to the public and private sector collaboration as well as support the adoption of networked trust services across the EU.

In that context, the aim of the report is to contribute to the discussion on the potential applicability of blockchain and DLTs to the EU's large-scale and governmental IT systems, taking into account the functionalities rather than the existing capacities of platforms or solutions available, introduced in product promotion, covered in hypothetical scenarios, proof of concept and piloting or actually implemented. When predictions are made about the long-term 'fit' of the technologies in meeting the current and future business needs of the Agency and its stakeholders through use cases, the inapplicability of many capabilities in the short term is prominently kept in mind.

The report is structured as follows: Section 1 describes the scope, aim and method of the report; in Section 2, the technology review is presented; Section 3 provides an overview of the legislative and policy framework affecting the implementation of blockchain in the public sector context; in Section 4, the possible eu-LISA use cases are discussed; Section 5 provides a technology outlook and reflection from a technology-readiness perspective; and Section 6 includes conclusions and avenues for exploring further the best options for blockchain and DLTs for eu-LISA. Glossary explains the abbreviations and Annex I elaborates on a highlighted topic of self-sovereign identity.

[1] See more in Section 3 of the current report and on the European Commission's dedicated websites: https://ec.europa.eu/isa2/eif_en and https://ec.europa.eu/digital-single-market/en/blockchain-technologies

1. Scope, aim and method of the report

Based on stakeholder demands, the Agency provides analysis of the new concepts, technologies and solutions that might be relevant for the operation of eu-LISA and other stakeholders in the JHA community. eu-LISA's mandate to engage in research and technology monitoring was strengthened in the Agency's revised Establishing Regulation[2], encouraging active approach towards analysing available and emerging technologies and solutions with potential relevance to the IT systems for which the Agency is responsible. The research and technology monitoring function strives to gather and analyse materials and projects in the field to provide input for discussions and strategies beyond the immediate development needs of the core systems and their possibilities.

1.1. Motivation behind the current study

The currently prevailing view of blockchain and DLTs, to a large extent shared by the industry, international organisations and the academia, is that these technologies are capable of solving all networked data exchange and trust issues, while giving little consideration to the limitations. Often, some of the functionalities attributed to blockchain are achievable through normal digitalisation, identity and access management, action logging, timestamping, standardisation, backup arrangement, encryption, certification, security and data protection tools.

The motivation behind this report is twofold. First, it is to discuss the applicability of blockchain and DLTs, but also to remind the community that most of the elements or capacities that have been combined to be presented as blockchain, had been elaborated and developed in separate streams earlier, also applied in most EU Member States e-government ecosystems, but might have not been used in this combination or in large-scale IT systems before. Moreover, until recently, most of those functionalities have only been available to networks with major resources, such as governments and eu-LISA, and have therefore not as widely promoted as in recent years.

Second, the Agency must follow the developments in the Member States in regards to the application of new technologies, such as blockchain, as these developments may have direct implications for the core business of the Agency.

1.2. Scope and aim of the study

The scope of this report is to review the main elements of blockchain/DLTs and their functionalities, as well as the possible use case scenarios for application of these technologies relevant in context of operational management of large-scale IT systems.

The aim of this report is to reflect on the state-of-the-art development trends in the domain of DLTs (including blockchain) and to assess any potential relevance those technologies or their elements may have to the future business needs of public sector and large-scale IT systems throughout the EU. The growing number of research papers discussing blockchain and DLTs, of proof-of-concept projects testing the implementation of the technology, and of service providers offering solutions for implementation in various business fields, including possible use in government information systems, suggests that the potential relevance of the technology should be even further explored by eu-LISA.

[2] Regulation (EU) 2018/1726, OJ L 295, 21.11.2018.

1.3. Target audience of the report

The report is addressed to both internal (eu-LISA) and external readers. It will be used as a point for discussion within eu-LISA and with eu-LISA's stakeholders, as a contribution towards fostering an innovation mind-set.

This report can serve as a reference point for those contributing or aiming to contribute to the development of large-scale IT systems or their components. Stakeholders who plan, manage and/or develop public IT systems at EU or Member State level, as well as corporate users or developers of large-scale IT systems that interact with public sector information systems, should find the material of interest thanks to the general approach taken in identifying the new demands along with the new technologies, or can seek encouragement from it for their technology development plans.

The industry can use the current report as a reference to remind itself of the necessity of aligning systems with the already established or developing frameworks to which eu-LISA and governments are already bound to, whilst exploring how to provide connectivity and interoperability with other relevant solutions.

1.4. Method and sources

This report is based on a review of publicly available information, including reports and publications provided by the industry, think tanks, specialist media and public authorities, and also academic literature on the subject. In addition, relevant legal acts were consulted where necessary. To perform the technology analysis, numerous reviews of blockchain or distributed ledger technologies are available, provided in the form of product presentations (by either the platform provider or customers), online community forums, educative explanations, consultancy analysis documents, studies, governmental reviews, statements from EU institutions, proof-of-concept project descriptions and, last but not least, scholarly articles. On the other hand, with regard to applicability in eu-LISA's business field, EU legislation, policies, frameworks and initiatives on e-governance, blockchain and eu-LISA systems were reviewed for compliance.

The most reliable sources include consultancy reports and scholarly articles, which explain the elements one by one with full acknowledgement that those elements are mostly compatible with any system development, not only ledger technologies. The most critical sources, in terms of assessing applicability and performing capability analysis, are perhaps the online technology community reviews and product descriptions. Yet there is very little blockchain-related literature on large-scale IT systems. With this report we aim to fill this gap at least to some degree.

2. Technology review

To understand the phenomenon of the many industries wanting to transfer to blockchain solutions, in preference to traditional solutions, one must understand the arguments or expectation management behind the technology hype. Though the approach of blockchain seems novel, much of what is expected of blockchain or DLTs can be done within current solutions, as these technologies are more or less a combination of various cryptography and distributed computing tools. What makes blockchain and DLTs special, is the fact that the attractive functionalities are merged, applied at the same time and aimed at doing so with least effort, legacy systems and without central validation authorities.

The establishment of trust in the database and in the records' integrity has been the key argument for seeking new solutions to make the status of the updates or access to the information available to network participants. Tracing back to the users and logs, history and validation for auditability of the actions, events and transactions of a data record are not core principles that every connected database uses, but are nothing new. Adding timestamps and possibility to look into the history of the events is not new either, yet not that often used. Keeping an identical ledger over the transactions and saving an eternal immutable trace of those changes at a central database or at all the nodes is not too often applied as it adds complexity, yet trustworthiness.

The concept of each node having all records duplicated with full history available is the approach of the 'classical' blockchain, which distinguishes it from the regular centralised database management where records are kept in a single central database and changes to those records (events) are sometimes not logged, archived or even backed up. The tools for hashing records, linking them to their history, keeping a ledger of changes available at every user's node also to check the validity and change in that sequence through relevant software hub, is the new element that is brought to the spotlight with DLTs making it most attractive to many markets and businesses.

2.1. Terminology

Untangling the terms of blockchain or DLTs is complex, as approaches to what those technologies are, what they consist of or what they can do, vary across sources and communities. Despite the seemingly large amount of information available, the terminology has not been consistently used. Although in academic discourse the concepts of blockchain and DLTs have been used more or less consistently, in the non-specialist media these concepts have been applied rather inconsistently.

Blockchain and DLTs are a set of technologies, including the supporting network infrastructure, which allows computers distributed across the network to record transactions or events proposed and validated by the members by applying certain consensus algorithms. Information about these transactions is then stored in a continuous immutable ledger, with an identical copy of the ledger present at each of the network's nodes at all times. Updates to these records are linked sequentially upon agreement by the participants, and links to data can be supported with permission management for users to access data only dedicated to them.

One might refer to 'blockchain' when describing either blockchain itself or elements of DLTs in general or both of those together. Many developers claim applying 'blockchain' when in fact only some elements of blockchain functionality are introduced without any distributed ledger framework or blockchain being implemented at all. In many cases, the term 'blockchain' is used to make the solution stand out among other solutions, whilst in some cases, especially among new technology online communities, it is used as if it meant the digitalisation of records.

Blockchain is a technology that allows parties involved in a specific interconnected network or ecosystem to keep identical records and history of transactions. Each record ('block') is linked to a previous block through cryptographic means ('hashes') and immutably recorded across the network. The hashes may belong to a service provider's wider framework, and the hashing code (the 'Merkle tree') and keys are used for validation of the timestamp and therefore providing transparency to the history of the record and the changes made.

Distributed ledgers predate blockchain and can be defined as databases distributed across several computing devices, where each node replicates and stores an identical copy of the entire database. Each participant in the network updates itself independently on the basis of a certain consensus algorithm. This allows to eliminate the need for a central authority.

For this report, 'blockchain' is used as a general umbrella term referring to the both of the technologies, to reflect the common broader use of the term across various sources. The definitions of DLTs and blockchain align with the approaches commonly used by the academic community and international institutions: the European Commission, the European Commission's Joint Research Centre (JRC)[3], the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT)[4] and the Organisation for Economic Co-operation and Development (OECD)[5].

2.2. Evolution of the technologies

The work on components that are the backbone of contemporary blockchain technologies, and DLTs more generally, predate the technologies themselves by several decades. The major works on public-key management or asymmetric cryptography date back to 1970s, and the Merkle Tree to 1980[6], whereas the initial idea for timestamping digital documents was published in 1991[7]. A comprehensive overview of the development of the elements and their individual inclusion in various solutions is provided in a few, yet informative sources[8]. Since then, both public key cryptography and timestamping have been widely applied in several conventional secure networks or machine-to-machine data exchange solutions, starting from the first decade of the 21st century.

Only with the widespread emergence of solutions following the introduction of the blockchain concept in 2008, in the white paper published by Nakamoto[9], has blockchain gained wide traction, reaching far beyond cryptocurrencies, into domains ranging from healthcare and supply chain management to agriculture and forestry. It has been lauded as the next internet, as a technology with a potential to disrupt all industries.

Blockchain functionality therefore evolved to allow a mechanism to establish a trustworthy, autonomous structure of data exchange, recording of changes in records and allow the records to be shared between several counterparts across a distributed network, may those records be bitcoin, other tokens or listings of possessions. When ownership of the possession changes, the action and the transfer of the ownership is

[3] European Commission, Joint Research Centre (2019), *Blockchain Now and Tomorrow*, https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-now-and-tomorrow

[4] UN/CEFACT (2018), White Paper on technical application of blockchain to United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) deliverables — Annex: An introduction of blockchain, http://www.unece.org/fileadmin/DAM/cefact/cf_plenary/2018_plenary/ECE_TRADE_C_CEFACT_2018_9E.pdf

[5] OECD (n.d.), *OECD Blockchain Primer*, http://www.oecd.org/finance/OECD-Blockchain-Primer.pdf

[6] Merkle, R. (1980). *Protocols for Public Key Cryptosystems', IEEE Symposium on Security and Privacy*, http://www.merkle.com/papers/Protocols.pdf

[7] Haber, S., and Stornetta, W. S. (1991), How to Time-stamp a Digital Document, *Cryptology*, Vol. 3, No 2, pp. 99-111. https://doi.org/10.1007/BF00196791

[8] For example, Narayanan, A., and Clark, J. (2017), 'Blockchain's Academic Pedigree', *Security*, Vol. 15, No 4, https://queue.acm.org/detail.cfm?id=3136559

[9] Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, Satoshi Nakamoto Institute, https://nakamotoinstitute.org/bitcoin/

renewed and all participants' records are updated with the new information. That is to guarantee that different people cannot claim ownership by presenting an outdated record. Updating the data is managed by obtaining machine-managed consensus between the participant nodes.

At current stage of development, all of the formations of DLTs or blockchain technologies do, in full or in part, address the basic capacities and elements of the network's functioning elements and components that support the creation of trust in partnership, namely the consensus mechanisms on renewal, editing and access to records, the management of users, agreed identities of members, access rights and procedures, central management of rules by either one or several nodes, set-up of the structure and contract agreements on the functioning of the ecosystem, type of consensus algorithms used, timestamping, logged records with reversible view, non-deletion of archives, and reference codes (hashes) and keys, symmetrically or asymmetrically distributed records. None of those elements, nevertheless, is unique to blockchain or DLTs; a set of capacities, when applied in a certain combination, has become known as blockchain.

2.3. Key capacities of the technologies

One of the key elements of blockchain and DLTs is support for the establishment and management of trust between the participants in the network. This allows persons (natural and legal), as well as machines, to engage in transactions without having a prior trust-based relationship or a mediating entity providing trust services. Although it is claimed to be done without a need for a centralised authority, it would still need the issuing of the certificates and rules of conduct of the ecosystem to be coordinated, if working with government data[10].

The distributed nature of data storage in blockchain ecosystems aims to eliminate the potential risk of a single point of failure (i.e. there is no centralised intermediary or node, which is critical to the operation of the network and can be subject to a cyberattack), yet endpoint, backup and system security have to be addressed as much as in standard systems with several locations.

The shared nature of distributed ledgers, where information is either distributed between or duplicated at all parties in the network and is available for review, makes transactions more transparent and traceable. New data entities can be recorded only by appending the record or dataset's registry, thus helping to ensure data integrity. As those registries are stored on an immutable ledger, there is less need for centralised entities for validation of transactions.

According to the technology's core principle, transactions and record updates are, validated automatically by participating nodes in a peer-to-peer network based on consensus algorithms and rules to validate both the origin of the change and the validity of the data. Such mechanisms for updating simultaneously edited records are currently also the weakest elements in both in blockchain and DLTs (but also distributed computing) and therefore need most developments to provide optimal and highest-quality decisions.

The reduced power of intermediaries, potentially reducing transaction costs, is seen as a great advantage in many use cases. It is also likely that the cost of algorithmic trust will continue to decrease as DLTs develop and computing power increases, thus leading to a potential decrease in the transaction costs and in the necessity of additional record or information validation.

The type of blockchain and consensus protocol used affects the capacity of the network to process

[10] European Union Blockchain Observatory and Forum (2018), *Blockchain for Government and Public Services*, https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory_blockchain_in_government_services_v1_2018-12-07.pdf

transactions and the speed of processing. In cases of public blockchains relying on the proof-of-work consensus mechanism (e.g. bitcoin blockchain), recording new transactions can be very inefficient, being potentially very time-consuming as well as expensive. Therefore, whenever a service involves large numbers of transactions, private blockchains relying on proof-of-authority consensus algorithms should be considered. To save resources on updates being validated across the network, which needs high computing power or active participation from each node, an alternative is suggested for gaining consensus, using protocols managed at one or several central master-nodes (such as proof-of-authority and proof-of-stake protocols).

2.4. Relevant key functionalities of the technologies

Whereas the logic of linked timestamping, verifiable logs and single network participation identities (permissioned or permissionless) could be appealing to several data exchange services, not all the structures of platforms available on the market have all the elements, nor are these complete solutions applicable for all business use cases, government or large-scale IT systems. In addition, not all the capacities are always needed in a solution or component. That said, in some use cases where only a few elements are applied, the vendors or customers prefer to call the solution blockchain, thereby reassuring users that the solution applies these technologies despite the fact that it only uses the standard tools.

Below an overview of blockchain and DLTs' key functionalities and capacities for public sector services and their data exchange solutions is provided.

PLATFORM TYPE AND GOVERNANCE OF THE PLATFORMS

1) **Public and private platforms.** Blockchain platforms can be categorised as public (open) and private (closed). The records stored on public blockchains are open and available for review to anyone. For private blockchains, only authorised entities have access to the records.
2) **Permissioned and permissionless.** Blockchains can also be categorised as permissioned and permissionless. In permissionless blockchains, anyone can become a node in the network and execute or validate transactions. In order to execute or validate transactions on permissioned blockchains, the entity must be authorised by an authority that controls the blockchain.

MEMBERSHIP-RELATED FUNCTIONALITIES

3) **Membership of the trust ecosystem.** Platforms both with and without links to government databases or registries ensure that the users and data holders are adequately identified. All nodes, whether they represent an entity or individual, hold certified identities and authentication methods that can be traced back to the source.
4) **Membership management.** Membership and trust management can be run on various principles, and either through a one-to-one relationship between the member and the network or moderated by a trusted third party that takes responsibility for the identification of the members.
5) **Interoperability of various ecosystems.** It is expected that, to connect several data exchange frameworks, the identity certificates have to be interoperable (in a similar way to how eIDAS supports electronic identification) and can be forwarded to other networks if necessary.
6) **Fitting general e-government interoperability frameworks.** The dataset exchange principles, security level of both the infrastructure and communication, and user identification principles, must meet the criteria laid down in eu-LISA systems regulations and technical specifications and set out in relevant national standards, and must match the established European Interoperability Framework for cross-border digital public services.
7) **Identity mesh compatibility.** With the emergence of several identification and authentication tools and methods, there might be a temptation for the newly emerging platforms and solutions not to

bind themselves to any existing solutions, but instead to create a unique one, thus adding more layers to identity management. Rather like the ease of logging on to different regular services with the same accounts, both individual and business machine-to-machine membership of platforms should be more standardised.

CONSENSUS

8) **Consensus algorithms for ledger updates.** The method of updating records across nodes is run by various types of algorithms, addressed across distributed computing sub-disciplines, not only in the blockchain and DLT domain. Although the latter has developed the method further and made it more widely known, there are still major gaps in providing a functional, cost- and resource-effective mechanism for networks ranging across multiple locations.

9) **Formulation and selection of consensus partners.** It is agreed within the ecosystem how many accepting nodes are needed to reach consensus, make a decision and update records. The consensus algorithms vary and the functioning of those is a key in successful distribution and updates.

RECORD-, LOG- AND LEDGER-RELATED FUNCTIONALITIES

10) **Logging and timestamping principles.** Rules for logging and timestamping must be compliant with any agreed rule and have a governance model behind them. The platform or service providers decide upon reliable tools and third-party solutions to run the tools.

11) **Record, ledger and log exchange mechanism.** Any connected databases and information from them would benefit from compatibility with mechanisms to provide a distinguishable and verifiable proof of origin. In the ecosystem, the membership certificates and the public keys must be accessible to be checked.

12) **Linked hashes and linked timestamping.** Linked hashes and linked timestamping address the recording of the exact time (and location) of the record update (or other) event, sequentially verifying the status of the records at the time, but not necessarily provide, yet should provide also other tools to support the validation: for example who initiated the update or change.

13) **Generating and distributing the hashes.** Although hashes are generated, exchanged and possibly validated in a distributed manner, the control structures are mostly kept in one location or a few locations. When only keys are exchanged, at least one of the original locations must always be accessible to authenticate the validity of the key or hash. At the same time, locally generated hashes do not necessarily have to be constantly distributed, as long as they can be accessed for verification in cases of queries or misuse.

14) **Public and private keys and digital signatures.** To unlock a message or record, encrypted with any cryptographic tools or digital signatures, the keys are issued to each user. Whereas the private keys are known to and held by only the members themselves, the public key supports the initial third-party validation of the record or origin of the data.

15) **Public keys/hashes.** In some blockchain solutions, another layer is added, where an additional public hash is provided to support the validation of any record kept within the framework supported by a specific vendor.

16) **Hash pointing.** Hash pointing is an additional mechanism allowing hashes not only to seal specific parts of databases or records with a timestamp and hash/signature but also to include a link to the data or record within the database. Such actions allow multiple datasets to be altered, exchanged and logged in a ledger.

STANDARDS

17) **Varied formats.** The basis of the information-storing and operational software will in many cases still be varied, and the file formats for data exchange will still be dependent on the sector, although the standardisation process helps to keep the number of available solutions low. For government or EU

services, it is highly unlikely that one single standard or access type will replace the diversity across sectors, although some preferences have emerging.

18) **Standards.** Secondly, there might be a future in which several big players launch their own blockchain standards. However, it remains highly unlikely that all worldwide users and information systems will be using only one service platform and standard blockchain. The established public sector services, in which many of blockchain's capacities are already implemented using other tools, might not transfer to the new type of data exchange. International independent private data exchange platforms might yet be able to develop and use new and unique technological solutions, all using only principles that fit the term 'ledger technologies'.

IMMUTABILITY OF RECORDS, FAULT TOLERANCE AND ARCHIVES

19) **Immutability of records.** Immutability of data is not necessarily the most important aspect of what is needed in all solutions, as some of the data can be changed, but a log is expected to be kept and partners expected to be notified. In some cases, the data can be uploaded to selected nodes; in some cases, only tokens are exchanged and updated. Altering or deleting old blocks is conceptually not possible within the classical blockchain, although if the records become excessive in size or if legislative compliance reasons exist such deletions might need to be done. While permissionless blockchain is limited in its functionalities, permissioned (federated) blockchains or DLTs can be used in a more flexible way.

20) **Rules on archiving.** The advanced rules for archiving would need to be adopted to support the necessity of tracking back across previous changes to find who has the latest version, whereas the older versions can be reached in an archive.

21) **Fault tolerance.** Although distributedness is given a lot of credit for being by default a support for avoiding cyberattacks and preventing data getting lost, as it is stored at multiple locations, it might not be easy to implement for any data exchange framework. As DLTs provide ledgers recording changes, and do not necessarily keep the data at each location, several preventive tools have to be put in place.

22) **User interfaces.** If users are not knowledgeable enough, they may not be able to trace fraud unless they have operating instructions for the service or dedicated tools. Any solutions developed should make it simple to track the records and produce a log report.

SECURITY, CYBERSECURITY AND DATA SECURITY

23) **Improved security for both data exchange and storage.** Improved security and traceability of users and logs will enhance trust among the partners in the extended large-scale IT ecosystem. At the same time, all nodes must comply with the highest-quality cyberattack prevention tools, even though the technologies are promoted as if implementing the blockchain technology provided security by default.

24) **Trustworthiness of the developer.** When considering blockchain or DLTs as an option, one must remember that they are just technologies; the quality, security, trustworthiness and continuity of a certain platform or solution are, as emphasised earlier, still dependent on the developer, not on the type of the technology. Ledger technologies do not provide immutable and secure storage of data per se; they do so through the rules the developer has to follow while building, holding and running the service. Although blockchain solutions might diminish the immediate opportunity for a corrupt record keeper to alter the information, the application of a weak blockchain solution does not prevent the potential corruption from being shifted towards deals with the developer or platform supplier.

SELF-MANAGED IDENTITY AND USER WALLETS

25) **User wallets.** User wallets are an emerging concept. In addition to allowing the user to access various services with one or a few certified digital identities and operate based on those, a wallet is also a

node or device that offers an overview of service-related information and data, constantly updated and enabling the status of records or resources to be verified.

26) **Self-sovereign identity.** Self-sovereign identity (SSI) provides an additional layer to the wallet principle, allowing the users, most often private individuals, to operate with their identity data without being dependent on one single authority to prove their identity. It also helps keep track of and manage all records that are kept about the individual in any of the connected services and registries[11].

SMART CONTRACTS

27) **Smart contracts.** Smart contracts can in principle be managed in every environment, allowing activities or processes to be triggered by a pre-planned mechanism, whereby a pre-defined set of data or information has been submitted, events registered and authorisations granted. Smart contracts can be understood and applied in terms of digitalisation and automation of other, standard, contracts between partners, as well as actions launched by computers or information systems when certain conditions are met.

ASYMMETRIC APPROACH AND GOVERNANCE

28) **Asymmetric data use and support to interoperability.** For distributed computing solutions, some of the DTL applications have a comprehensive structure of storage, computation and messaging that operates with the ability to read multiple servers and the updates simultaneously. That might be to enable the update of all or selected data at all the locations based on updates by the partners, but doing so by tracking each record's history and applying various rules about the immutability of some data fields.

29) **Central versus distributed in rules and access management.** Distributed data and automatically made consensus decisions are promoted as making the data flow more transparent. They sound promising, yet it might still not be possible to do without a central system because, even if records are laid out in a distributed manner, the rules and access rights must still be centrally managed or programmed. There is nevertheless a central structure (including in most strictly equal-node blockchains) with a central management functionality disproportionate to the information-sharing platform needed. The rules are to be generated and handled by service providers and applied automatically. But the functionality must be there.

As can be deducted from the above, any of these elements can be elaborated upon separately and, when improving the implementation, can be applied as a separate element or module to the existing IT structure, or incorporated in a new combined technology solution.

[11] The idea of self-sovereign identity is further elaborated in Annex I.

2.5. Early use cases and proofs of concept in various domains

Some industries have already reported on developing or using such solutions, even if with relatively limited scopes; some consider the technology only an enabler for true distributed data exchange, but have not taken any steps yet. Some have doubts about its applicability overall; some express the view that the same results can be achieved with conventional methods, and confirm that they use the principles already without any blockchain implementation. To go along with the hype, many claim to use blockchain already, although a closer look reveals that the applications are not exclusively developed on a blockchain platform but just use certain elements in a new setting.

As blockchain or DLTs could be well suited to recording events, managing records, keeping registries, processing transactions, helping trace the origin of goods or components, or managing identities, some initiatives have been applied to private or public record keeping in finance, supply network, transport and mobility use cases.

Examples early use cases of blockchain and distributed ledgers include solutions addressing records and registries of ownership of digital or physical assets that have long-term or unlimited validity, be they property, shareholdings or tokens not related to physical goods. Relevant public sector examples include use cases of the application of those technologies to land registries (Georgia), health records, some local services to citizens or businesses, education or training results.

For running financial records or secure banking, blockchain has been under discussion and implemented to keep registries available to both the user and the bank, or both the bank and the central bank, in the most traceable way. For short-term records, such as insurance record keeping, blockchain solutions serve for validity and dissemination purposes, and also for the registration of single-use tamper-proof entries over a short timeframe, e.g. for voting or opinion polling, survey result collection and analysis, or performance records.

To certify the origin of components or products in manufacturing and in agriculture production management, blockchain has already been applied within closed business-to-business environments as test cases (e.g. by De Beers, Unilever, Pfizer, Walmart, Nestlé and Renault). Cross-border proof of concept projects have followed, showing that it can enhance supply network performance and log the actions taken with the goods, but the application still has to overcome the need for physical processing support in the initial digitalisation of records as well as technical support for automation through both the Internet of Things (IoT) as well as gaps in standards for data exchange. Last but not least, the applicability of such actions derives from the cohesion of a supply network, in which well-functioning partnerships with established data exchange can adopt new technologies more easily but, having already established trust, might not need to make additional investments. To expand the system to handle data exchange with governments, either in issuing certificates or in accepting documents in international trade, the lack of standards and interoperability has to be overcome.

For another supply-chain-visibility reason, logistics companies (e.g. in maritime shipping by Maersk in cooperation with IBM) and infrastructure service providers (such as the Port of Hamburg) have set up transport management and traceability of goods and containers to support the data exchange. For transport, solutions to track automatic vehicle routes and timings have also been addressed through blockchain (e.g. MAN in cooperation with Hamburg city and port area), whereas, for example, vehicle records and tachometers have already applied other tools to save tamper-proof records across the nodes.

Solutions for grid analysis have been emerging, such as energy grid or transport grid analysis for smart city or autonomous driving purposes (e.g. Toyota), roughly corresponding to small-scale route planning for individual vehicles, covered earlier. The tracking and dissemination of international aid or resources and the collection of contributions have been addressed at some non-EU locations where central or single-copy databases are expected not to be secure enough and where record keeping needs an additional layer of trust services. To keep records of customer actions or service histories, some samples of blockchain have been provided by advertising and customer management companies.

Examples of applying cybersecurity through implementing blockchain functionalities are as important to the domain as cybersecurity is to the blockchain solutions themselves, and that segment is expected to grow rapidly in the coming years. As a side-product or an additional functionality of blockchain, smart contracts have been explored by legal firms and consultancies. Whilst digital signatures and digital records meeting certain criteria serve as proof in legal transactions as well as in courts, legal offices are mapping the possible use of fully eligible self-executing smart contracts, which might also be implemented using blockchain.

Identity management and self-sovereign identity (SSI) management with the support of blockchain are a use case that have been explored and have a high potential as a separate service. Single or combined identities are verified by other bodies participating in the network, users have control over their unique identity and the validation of a user's single identity across several networks is improved. Examples of such shared identities operated in support of blockchain have been applied by the United Nations High Commissioner for Refugees (UNHCR)[12] and piloted in the context of the administration of asylum procedures in Germany[13].

Some proofs of concept and evaluations have been conducted by the industry and the academic community, which shed the best light on the possibilities or limitations. When people promote the introduction of these solutions, they often admit that the implementation of such developments is hindered by the lack of commonly accepted standards to allow growth across the sector, the lack of a coherent ecosystem that would involve governments in traceability or cross-border certification, or the low capacities of technology integration or reliable technologies, software or IoT solutions to connect the record keeping with physical actions.

The solutions, though, lack standards and agreed architecture for further interoperability between them and existing structures, be they the current established industrial software or government/public sector IT systems.

[12] UNHCR, https://www.unhcr.org/blogs/unhcr-accepting-proposals-digital-identity/

[13] See Annex I for a more detailed review on SSI and the Germany use case.

3. Legislative and policy aspects

Some of the earliest IT solutions for data sharing between Member States in the EU, backed by legislation and trust creation mechanisms, have been the Schengen area large-scale IT systems in the Justice and Home Affairs (JHA) domain that are now maintained by eu-LISA. As e-government data exchange rules (incl. newly introduced eIDAS) as well as blockchain and DLTs both address setting rules on creation of data sharing ecosystems and have much the same functionalities for creating that trust in a network, the opportunities and future interoperability between those frameworks are to be addressed by both the public sector and industry.

The search for common ground on standards and approaches to security and trust issues for interoperable e-governance or other data sharing frameworks has resulted in outlook of allowing multiple approaches tied together. The interest in integrating new tools and approaches further (such as blockchain and DLTs) is also increasing, but so is the pressure to do so. The exploration has brought new policy and legislative initiatives to the table, and with that possible future integration opportunities for new technologies.

The already established frameworks supporting the commonly recognised electronic identification and authentication services, permission management, advanced electronic signatures and record sealing, data exchange and logging, recognised timestamping principles and data integrity across participating nodes is expected be developed in a complementary and interoperable manner, and blockchain is encouraged a complementary, not necessarily an alternative to e-governance or business-to-government information sharing. So, whilst choosing and implementing IT strategies and addressing the long-term interoperability of digital services, the search for alternative technologies to support trusted and mutually recognised data exchange is already taking place.

3.1. The European Union legislative and policy framework

Work on interoperability and cross-border information exchange has been initiated in a number of policy domains, including the work that is being carried out by eu-LISA, the establishment of the Maritime Single Window[14], the Single Digital Gateway[15], EU customs cooperation and other interconnected registries. The EU, together with the Member States, has also been actively working on the development of frameworks and standards supporting the interoperability of IT systems across the EU[16], gradually touching upon the applicability of blockchain and DLTs.

The EU eGovernment Action plan for 2016-2020[17] and the Tallinn Declaration on eGovernment (2017)[18] are good references to understand the attitudes and ambitions of EU Member States with regard to trusted data sharing and e-government services, while they increasingly address the exploration of new technologies, including blockchain and DLTs. The European Interoperability Framework[19] provides support and guidance for the development of interoperable digital public services and government-to-government data exchange within Member States, as well as across borders.

The European Commission established the legal framework on electronic identification and trust services

[14] Regulation (EU) 2019/1239, OJ L 198, 25.7.2019.

[15] Regulation (EU) 2018/1724, OJ L 295, 21.11.2018.

[16] See for example the ISA² initiative, https://ec.europa.eu/isa2/home_en

[17] Communication from the Commission, EU eGovernment Action Plan 2016-2020: Accelerating the digital transformation of government, COM/2016/0179 final.

[18] Council of the EU (2017), Tallinn Declaration on e-Government.

[19] European Commission (2017), European Interoperability Framework: Implementation strategy.

for electronic transactions with the adoption of the eIDAS Regulation[20]. The eIDAS framework provides key trust and interoperability enablers, including timestamping, digital authentication, digital signatures, electronic seals and electronic delivery services, providing the initial digital trust ecosystems across Member States and policy areas in the EU. The eIDAS framework supports keeping up secure and tamper-proof registries or providing services that reach out to individual citizens and businesses in a highly secure way, if the framework is applied fully. Blockchain is an alternative solution for establishing trust in digital environments, which can be complementary to the solutions in place, for instance by providing timestamping or record-hashing functionalities.

3.2. EU-level initiatives focusing on blockchain and DLTs

Alongside the ongoing work on interoperability and digitalisation of public services or industries, the EU has recently launched a number of dedicated projects focusing on blockchain and DLTs. In February 2018, the European Commission initiated the EU Blockchain Observatory and Forum[21], with the objectives of mapping the existing initiatives, monitoring the developments and inspiring joint action aimed at the development of blockchain and DLTs in the EU.

To support the creation of an environment enabling the development of services using blockchain, in April 2018, 21 EU Member States and Norway signed the Declaration on European Partnership on Blockchain[22]. The ambition of the partnership is to work towards a trusted infrastructure accessible to support digital services deployed by public and eventually in the future also private actors. The document also suggests that blockchain and DLTs 'are seen as particularly promising in ensuring more security, integrity and transparency when delivering services, enforcing regulations and ensuring efficiency in legal compliance' and, most importantly, avoiding a 'fragmented approach'. The declaration also aims to develop a trusted, secure and resilient European Blockchain Services Infrastructure (EBSI)[23], which would support the newly emerging solutions in meeting the highest standards in terms of privacy, cybersecurity, interoperability and energy efficiency, as well as being fully compliant with EU law. Its second aim is, in the long term, to provide reusable software, specifications and services for further implementation by European public administrations and EU institutions.

The most recent initiative to scale up blockchain and DLTs across industries, also backed by the Commission, is the establishment of the International Association of Trusted Blockchain Applications (INATBA)[24] in April 2019. INATBA brings together representatives of different industries that develop applications of blockchain and DLTs, international organisations, regulatory and standardisation bodies, and civil society, with the aim of developing a framework for blockchain and DLTs that supports collaboration between the public and private sector and regulatory convergence, as well as ensuring the established system's transparency and integrity[25].

A dedicated administrative unit for Digital Innovation and Blockchain[26] has been set up within the Directorate-General for Communications Networks, Content and Technology (DG CONNECT) to coordinate those actions and provide moderate innovation funding. Among other tasks, the unit's role is

[20] Regulation (EU) No 910/2014, OJ L 257, 28.8.2014.

[21] EU Blockchain Observatory and Forum, https://www.eublockchainforum.eu

[22] European Council (2018), Declaration Cooperation on a European Blockchain Partnership, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50954

[23] European Blockchain Services Infrastructure, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi

[24] International Association of Trusted Blockchain Applications (INATBA), http://www.inatba.org

[25] European Commission, https://ec.europa.eu/digital-single-market/en/news/launch-international-association-trusted-blockchain-applications-inatba

[26] European Commission, Directorate-General for Communications Networks, Content and Technology, https://ec.europa.eu/digital-single-market/en/content/digital-innovation-and-blockchain-unit-f3

to develop and implement the Startup Europe Initiative, coordinate DG CONNECT's standardisation, devise policies, promote benchmarking and facilitate the sharing of best practices. In the blockchain domain, that is a major step not only in becoming recognised, but also in providing more structured and better targeted solutions solving specific use cases.

3.3. Initiatives at Member State level

Currently, the Member States have individual roadmaps and apply national interoperability frameworks[27] and eIDAS components or interoperability at their own pace[28], while at the same time seeking alternatives in additional tools that support either the transparency of record-keeping or data security. Nearly all the Member States search for improvement and transfer of best practices to establish a secure way to make their own systems and registries trustworthy and interoperable. The pace of adoption of novel technologies, such as blockchain and DLTs, varies between the Member States. To assess the opportunities for blockchain at the national level, Member States have convened national expert groups or strengthened the national associations working on the topic (in Germany[29], Italy[30], Poland and others) and have analysed, tested or implemented some limited solutions featuring blockchain functionalities (the Netherlands, Estonia). Malta has been referenced as one of the most proactive in regard to establishing a regulatory framework for DLTs and cryptocurrencies[31].

National public institutions are compiling dedicated analysis and think tanks have been commissioned to review either sectoral or general analysis documents (for financial services in the United Kingdom[32], and for transport sector in several Member States), where the blockchain-related discussion runs in parallel with addressing issues of digitalisation gaps in specific fields at the national or the regional level.

Regionally, in December 2018, ministers of Cyprus, France, Greece, Spain, Italy, Malta and Portugal signed the 'Southern European Countries Ministerial Declaration on Distributed Ledger Technologies'[33], providing an additional endorsement of the technologies through a deeper regional ambition to apply DLTs and smart contracts in search of support for the functioning of e-government services. In the Mediterranean countries, the new technologies are seen as supporting privacy for end users, empowering citizens to be in control of their own personal data and enhancing trust between partners on record-keeping and -accessing practices.

Member States are looking forward to better-regulated frameworks, both in Member States where less coherent e-government IT solutions are available and in those where e-government and interoperability are at their highest level and where trust ecosystems and several key functionalities attributed to blockchain and DLTs (digital authentication, timestamping and logging of records) are already in place and interoperable through eIDAS or eIDAS compliant frameworks. In the current state, all developments, like other cross-border or cross-sector developments, could benefit from a common EU approach to the standards and requirements of those platforms and services.

[27] National Interoperability Framework Observatory (NIFO), https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory

[28] European Commission (2018), ISA^2, eGovernment Factsheets and Infographics 2018, https://ec.europa.eu/isa2/egovernment-factsheets-and-infographics-2018_en

[29] Blockchain Bundesverband, https://bundesblock.de/about-us/

[30] Blockchain Italia, https://blockchainitalia.io

[31] PricewaterhouseCoopers, https://www.pwc.com/mt/en/publications/technology/pwc-malta-blockchain-alert.html

[32] Financial Conduct Authority (2017), *Discussion Paper on Distributed Ledger Technology*, https://www.fca.org.uk/publication/discussion/dp17-03.pdf

[33] Southern European Countries Ministerial Declaration on Distributed Ledger Technologies, https://www.sviluppoeconomico.gov.it/images/stories/documenti/Dichiarazione%20MED7%20versione%20in%20inglese.pdf

3.4. Initiatives of international organisations

In addition to the EU, other international organisations such as the United Nations[34], the International Monetary Fund[35], the OECD[36] and the World Economic Forum[37] are assessing the limitations and regulatory gaps, but also addressing possibilities of implementing blockchain and DLTs in different domains.

Work on harmonising and standardising procedures, documents and cross-border data exchange has been ongoing in the cross-border trade and customs domain for a long time. This domain was also one of the pioneers in embracing blockchain. The World Customs Organization (WCO) and other international organisations have been looking at blockchain as a possible solution for trusted cross-border transactions, tracking of goods and paperless reporting. Whereas trust in paper-based or digital files/records comes from accepting mutually and internationally recognised bodies (certification organisations, governments, other members of the network), the key for international data flows is enabled by trusted mechanisms of participants gaining membership of or partnership to an ecosystem, which would allow them to verify and authenticate the person or documents/records behind the actions, records and documents. Whilst eIDAS provides the framework for the EU, the rules beyond the EU are to be addressed by international organisations, associations, platforms and forums in the near future.

A variety of global certification bodies will be providing digital identities for accesses to regular and blockchain data ecosystems, driving the evolution of platforms supporting identity mesh, digital wallets and self-sovereign identities (SSI). While one person or business entity might belong to several of ecosystems, SSI provides users control over their access rights and also extends the interoperability of accesses and data exchange across multiple types of platforms or mobility of personal data (for example for use case introduced by UNHCR[38]). To manage access to EU digital services for non-EU customers and travellers from third countries, the interoperability between third party, possibly non-EU identity providers and EU Member States e-governance framework is also a topic soon to be under discussion.

Both of the international developments – standardisation and identity management – are nevertheless welcomed by eu-LISA as an agency working with data originating from public sources within the EU as well as from locations outside the EU, as well as from international travel documents or individuals themselves.

3.5. Legal framework of eu-LISA

Since this report focuses specifically on the potential application of blockchain in the JHA domain, it is necessary to outline the legislative environment in which eu-LISA operates. The legal framework supporting eu-LISA consists of the Agency's revised Establishing Regulation and the legal bases of the specific systems, in particular the legal bases of the Schengen Information System (SIS[39]), the Visa Information System (VIS[40]) and the European Asylum Dactyloscopy Database (Eurodac[41]). In addition, it includes the legal basis for the systems and components under development, such as the Entry-Exit

[34] United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT)., http://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain.pdf

[35] International Monetary Fund, https://www.imf.org/~/media/Files/News/Seminars/2018/LFS2018/usman-sheikh-blockchain-presentation-sept-26-2018.ashx

[36] Organisation for Economic Co-operation and Development (OECD), http://www.oecd.org/daf/blockchain/

[37] World Economic Forum, https://www.weforum.org/platforms/shaping-the-future-of-technology-governance-blockchain-and-distributed-ledger-technologies

[38] UNHCR, https://www.unhcr.org/blogs/unhcr-accepting-proposals-digital-identity/

[39] Regulation (EU) 2018/1860, Regulation (EU) 2018/1861, Regulation (EU) 2018/1682, OJ 312, vol. 61, 7.12.2018

[40] Council Decision 2008/633/JHA, OJ L218, 13.08.2008; Regulation 767/2008, OJ L218, 13.08.2008; Council Decision 2004/512/EC, OJ L213, 15.06.2004

[41] Regulation (EU) 603/213, OJ L180, 29.06.2013

System (EES[42]), the European Travel Information and Authorisation System (ETIAS[43]), the European Criminal Records Information System for Third Country Nationals (ECRIS-TCN[44]) and the interoperability components based on dedicated legislation[45].

Any technology proposed as a solution to operational or technical problems, or intended to complement the existing functionalities, amend procedures or support processes in the JHA large-scale IT systems managed by eu-LISA, must be fully aligned with the legal, functional and technical requirements as per the strict legal framework mentioned above.

3.6. GDPR impact

The General Data Protection Regulation (GDPR)[46] applies to all public and private IT developments in the European Union. In this respect, blockchain solutions should comply with GDPR in regard to the right of individuals to request information that is held on them, to request the modification or deletion of records, or to allow the deletion of outdated records. It is also expected that solutions including blockchain or DLTs must eventually be compliant with the demands placed on regular systems dealing with similar information. The regulatory framework affecting the implementation of blockchain and DLTs may need to be updated taking into account the lessons learned from the successful proof-of-concept implementations. The tensions between some of the properties of blockchain (e.g. immutability of records) and the requirements inscribed in the GDPR are to some extent balanced by some of the blockchain implementations, such as the self-sovereign identity (SSI). SSI addresses some of the intentions of the regulation directly, namely allowing the owner of the data to have control over the use of the data by third parties (i.e. ensure purpose limitation, data minimisation, etc.)[47].

[42] Regulation (EU) 2017/2226, OJ L327, vol. 60, 9.12.2017

[43] Regulation (EU) 2018/1240, OJ L236, vol. 61, 19.09.2018

[44] Regulation (EU) 2019/816, OJ L 135, 22.5.2019, p. 1-26

[45] Regulation (EU) 2019/817, OJ L 135, 22.5.2019, p. 27-84 and Regulation (EU) 2019/818, OJ L 135, 22.5.2019, p. 85-135.

[46] Regulation (EU) 2016/679, OJ L 119, 4.5.2016, p. 1-88

[47] Finck, M. (2019), *Blockchain and the General Data Protection Regulation*, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

4. Possible use cases at eu-LISA

To reflect on the technology and its components, eu-LISA provides an overview of the possible application of elements of blockchain technologies depending on the new functionalities becoming available. When reviewing the possible options, eu-LISA is aware that state-of-the-art blockchain technologies are not ready for direct application in its core business. Nevertheless, some of the elements or functionalities may be beneficial, and therefore need to be considered.

4.1. Domains of possible application of blockchain and DLTs at eu-LISA

The motivation of eu-LISA in adopting new technologies or approaches is:

- high availability and consistent datasets in systems;
- decentralised collaboration;
- application of interoperability between components;
- smooth and effective process handling for the end users;
- delivering its services to users at highest level of quality, speed and security;
- third-party communication to support pre-authorisation on external borders (service providers).

The areas of interest could be:

- interaction between central units and national systems, synchronising, storing and updating records in all connected premises and servers (i.e. the central database and national copies for SIS or the central database and national interfaces for VIS);
- applicability in the interaction between components within the eu-LISA internal information exchange architecture;
- data exchange with Member States and other public sector third parties, such as national governments outside the systems' framework and other Agencies;
- data exchange between eu-LISA and external non-governmental partners or interoperability with third-party solutions (such as carriers for EES/ETIAS), if such solutions come to be in the field;
- identity management for the individuals who have records in the systems, and possibly the ability for the individuals themselves to hold a valid ledger and participate in the network (VIS, Eurodac, ETIAS) for GDPR-related requests or compliance.

4.2. Possible use cases at eu-LISA

The possible use cases listed below do not consider the application of blockchain platforms or wider distributed ledger frameworks, but are those in which eu-LISA would be willing to discuss on-boarding new approaches that might benefit the functionalities or performance.

ACCESS SYSTEMS OR COMPONENTS AT MEMBER STATE LEVEL

1) **Interaction between the central systems and National Uniform Interfaces (NUI-s) and individual national systems.**
2) **Interaction of central system extensions or components with external governmental or administrative partners.** Some additional sections for queries could be built upon distributed ledger functionalities to allow partners or associated partners to use services, for example performing queries or using statistics.
3) **Providing extended and advanced support to the use of VIS between the system users and system hubs in cases of possible security concerns.** Support for communication channels and synchronisation of information between the central system and national services could be moderated with the help of blockchain. That would help service desks at embassies, visa-issuing partnership service providers and additional service hubs at border crossings or checkpoints to query the system.
4) **Access to statistics.** As more parties are interested in and assigned to the report data than have access to systems, whereas the statistics are mostly public, the use of the dedicated databases could be moderated using tools developed based on capacities of DLTs.
5) **Access and management of reports on data quality.** Use and handling of the reports, as well as compilation, response and tracking of milestones of action plans, could be built as a special module instead of or to support file repositories.

DATA WAREHOUSING

6) **Benchmarking from developing consensus algorithms.** This can also be useful for large-scale IT systems in keeping several identical or distributed databases up to date, running an active-active approach or distributing data between different applications or modules.

INTEROPERABILITY FACILITATION

7) **Interaction between the interoperability components.** The tools and methods, capacities and algorithms in data exchange within a distributed ledger solution might be a learning or benchmarking case for assessing best practices now and in the future.

TIMESTAMPING OR HASHING RECORDS AND REPORTS

8) **SIS record updates.** Records entered in SIS with a patch could be accompanied by a hash, allowing for timestamping and logging of record updates.
9) **Central Repository for Reporting and Statistics (CRRS) records or reports.** The data collected for the reports as well as reports generated and issued might be timestamped and hashed. Values, statuses or results, submissions or retractions of datasets could be logged and time-stamped in the future, although thus far the community has not indicated a need for such functionalities.

LOGGING OR HASHING ACCESSES

10) **The support mechanism for timestamping and hashing accesses and use of the systems by the end users.** This would support increased security and avoid unacceptable data queries or data breaches while also supporting the Member States with the functionality of traceable and unified logging.

VIS

11) **Visa holder's wallet.** As with other documents (e.g. identity), visa issuance can also be handled electronically. In such cases, a visa can be stored in a digital wallet and presented along with the

electronic boarding card on a mobile device when boarding. In addition, blockchain and DLTs can be used to fight visa fraud. The tool should allow a combination of EES, ETIAS and VIS information, but not allow access to the system by unauthorised persons.

ETIAS

12) **ETIAS pre-authorisation process.** The devices required for the functioning of ETIAS are to be developed by the industry to best meet the needs of the practical use of the systems (such as new scanners, software or other solutions). Some of the mechanisms for storing information and transferring it between those devices and IT systems might be proposed for development using blockchain functionalities.
13) **Extended travel authorisation services.** Third-party-managed pre-authorisations to ETIAS as well as authorisations possibly made at various kiosks/booths or via mobile devices could benefit from blockchain functionalities.
14) **Carriers' data exchange interface and application to check pre-authorisation smoothly.**
15) **Travel authorisation stamp/token structure.** This may be sufficient as long as the records are constantly verified and not usable unless online.

EES

16) **Pre-enrolment facilitation.** Pre-enrolment and authorisation back-end processes made at booths, and possibly also via mobile devices, would have the potential to use blockchain functionalities.

EURODAC

17) **Private entity's end-user function for tracking handling of claims and requests to access or delete of one's own information from the system (in accordance with legislation).**

BRIDGING TO THIRD-PARTY SOLUTIONS

18) **Connectivity and data exchange with international ecosystems.** For example, they could support data exchange with international partners, either governmental or trusted international organisations. The possible functionality of interconnection with, for example, the UNHCR Population Registration and Identity Management Ecosystem[48] utilising blockchain, or with other similar registries, could be considered by eu-LISA in case data need to be exchanged. This would most probably not involve connecting the named solutions to the eu-LISA systems but only creating a data exchange mechanism or dedicated structure for running a separate data exchange node.
19) **Connection to private ecosystems.** Several communities are discussing using DLTs. If data need to be retrieved from those ecosystems, eu-LISA could facilitate a dedicated data exchange mechanism or a dedicated node.

ACCESS TO SYSTEMS BEYOND THE EU (government, administration level)

20) **Use of SIS information outside the EU without providing connectivity to the database.** It is anticipated that, in the coming years, further international cooperation and integrated data exchange measures might allow cross-querying to SIS and similar systems. Given the differences in digital ID and trust network services principles within the EU and around the world, the systems will probably not be managed in the same way. A special query service, with repository and ledger technology functionalities supporting this function, might become an option.

IDENTITY AND ACCESS RIGHTS MANAGEMENT BEYOND EU BORDERS

21) **User identification and authentication.** All system users must have compliant user identification. For example, visa applications at foreign embassies around the world or external access or queries to

[48] UNHCR (2019). https://www.unhcr.org/primes.html

databases must be traceable back to the individual, both within the EU and outside.

SELF-SOVEREIGN IDENTITY MANAGEMENT

22) **Self-sovereign identity and identity management in general.** With the development of advanced applications, biometric identity management can shift from regular databases (owned by public bodies) to public-private combinations co-owned and co-managed by the government and the private body together. Furthermore, blockchain-based identity management solutions promise to put control of personal identity data back into the hands of end users, with the help of digital wallets stored in digital devices (e.g. smartphones). This can create both opportunities and challenges for eu-LISA in terms of the need to adapt the existing systems[49].

KEEPING ATTENDANCE AND TRAINING RECORDS AND CERTIFICATES

23) **Registry and updates of training records and manuals.** There would be benefits from using DLTs for training information, especially the instruction manuals for some activities or some reporting procedures. Some changes in manuals could be triggered centrally, and instruction and training information updated automatically, synchronised across all users' databases without human intervention or manual changes in files.
24) **Compatibility with market-driven training certificates.** Training certificates, when introduced in other frameworks, should be upgraded to be compatible.

SMART CONTRACTS WITH PARTNERS

25) **Procurement and finance.** eu-LISA could enter into smart or self-executing contracts in procurement and in cooperation with service providers if the partners use such solutions, when the output format for eu-LISA is comprehensive enough.

MANAGEMENT AND INTERACTION OF MULTIPLE LEDGER ECOSYSTEMS

26) **Partnering in external ledger ecosystems to facilitate data exchange.** eu-LISA might facilitate all interactions with any of the decided services built on ledgers by participating in the ecosystem. That would need either a data exchange through functional application programming interfaces (API-s) which is the current approach or a distributed ledger welcome server service. Neither of these services would allow direct access to and updates of records in eu-LISA databases, but they would provide a buffer service with trust partners and machine-to-machine multiple node exchange to the partners and their return data.

[49] Please consult Annex I below for further details on self-sovereign identity.

5. Discussion of the technology outlook

Although the potential of blockchain and DLTs is high, especially as the functionalities provide remedies for some issues that are difficult to tackle with standard tools, there are concerns in relation to the applicability of specific elements or solutions currently available on the market for government IT systems. At the same time, it is critical to remember that DLTs should be seen as a combination of various elements that are readily applicable separately without a specific service or platform. Second, those technologies are also not in themselves a replacement for databases, although they might challenge the application of centralised computing and replace it with a decentralised or distributed approach, especially in data exchange frameworks where participants would like to keep their own data under their own control, make some records partly or fully available to partners and keep track of all the changes in all the connected datasets.

5.1. Technology hype status and ripeness

Blockchain should be considered to be in its first stage of development and quite far from being ready for widespread implementation. Following the hype cycle approach proposed by Gartner[50], the technology is still in the 'peak of inflated expectations' phase in connection with its applicability in the public sector. The second stage, in which the larger investments and technology transformation really happen, seems to have begun. When taking a closer look, however, there is limited information about available fully operational solutions that would go beyond the application of certain functionalities (like timestamping or hashing). The third phase is expected to follow only after that, involving the widespread use of the technology[51].

Reviewing the limitations of the initial blockchain platforms leads to the conclusion that many of them are only pathfinders, demonstrating the possible impact of the new technology. Nevertheless, to analyse the possible uses as well as the limitations of the current functions, the technology developers are increasingly collecting input from various industries, in particular recently from governments.

As the blockchain solutions and DLTs seek to arrange the logic of database-to-database information-updating principles and the rules of such updates, and to provide data exchange without the need for building a central database, the true solutions for such functions are in a very early phase. The advanced application of consensus algorithms or synchronous updates to active records are of high interest to many use cases, especially in international business and government data exchange frameworks, including eu-LISA.

One of crucial, but not that much covered areas, is the trustworthiness of developers and security of the technologies and the systems[52][53], though addressing those topics is a key to wider applicability of those technologies in large scale.

The legislative support to define and accept blockchain registries, proofs of records or smart contracts as valid evidence for legal transactions, court cases or proof of ownership will take a while to solidify across the wider international community. Technology lawyers and academics still expect that, as in many trust

[50] Gartner (2018a), *Gartner Hype Cycle*, https://www.gartner.com/en/research/methodologies/gartner-hype-cycle
[51] Gartner (2018b), *Blockchain-Based Transformation: A Gartner Trend Insight Report*. https://www.gartner.com
[52] Accenture (2019), *Blockchain's potential starts with security.* https://www.accenture.com/_acnmedia/pdf-96/accenture-blockchain-technology-security-pov-digital.pdf
[53] European Union Agency for Network and Information Security (ENISA) (2016). *Distributed Ledger Technology and Cybersecurity.* https://www.enisa.europa.eu/publications/blockchain-security/at_download/fullReport

environments, digitally signed documents will be treated equally with paper-based documents (in both the public and private sectors, as well as in court proceedings). The expectation therefore is that the legislation will evolve following the successful development of new technological solutions based on blockchain and DLTs.

5.2. Technology outlook for EU-level use

While in the networked computing, public sector data exchange and multi-stakeholder database domain there are plenty of functional solutions available and operational to establish identity, logging and trust for digital ecosystems (especially in the EU and its Member States), it must be emphasised that not all areas and regions are equally covered or established in trusted frameworks.

In a number of countries around the world, including some European countries, e-governance tools are either not sufficiently developed or are not perceived as trustworthy by some user communities. In countries where government-backed trust frameworks might not be sufficient for users to feel confident in the security of their records in many fields, or where, for lack of digital identities and e-seals or digital stamping, the governments cannot validate the source of data submitted by businesses or citizens, community-regulated blockchain and DLTs can provide a supportive solution.

Governments seeking alternatives to the available options, and applying blockchain as a novel or suitable solution should take into account that new technologies have to meet certain security standards and requirements. In practice, transfer to blockchain or applying a related functionality, might be a suitable option to increase trust, provide a necessary secondary identification and record validation layer for a separately-functioning service ecosystem.

While looking into interoperability or data exchange with third party data holders or users, it is essential to identify the ecosystem extension and data exchange integration potential without integrating the two ecosystems through common memberships. For managing that, the EU might offer support to develop a kick-starter identity mesh and self-sovereign identity (SSI) frameworks in which several ecosystem membership mechanisms (either sectoral or global) are made interoperable by means of coordinated categorisation and mutual acceptance, building trust frameworks that are quite similar to eIDAS and at the same data from those ecosystems being interoperable.

5.3. Further steps to be taken to address eu-LISA's needs

eu-LISA, as the body in charge of the operational management of large-scale IT systems in the JHA area, has solid experience: the systems operated by eu-LISA, their components and interoperability, already combine numerous approaches to distributed data exchange, storage, security and logging tools. It is of the utmost interest to eu-LISA, therefore, to weigh up and assess the most recent, advanced and high-quality applications and solutions.

In the European context, the developments have to take into account the systems and government IT system functionalities and operational principles already in place or under development. Since the systems that eu-LISA manages and develops interact with all Member States over dedicated secure networks, and also authorities and regions beyond EU borders, such as Associate Countries, embassies, carriers and possibly booths in other countries' territories, the view of trends and alignment for compatibility should be wider than the EU.

Although some EU Member States and eu-LISA data exchange partners might seek alternatives or additions to conventional e-government tools, in the eu-LISA and e-government domain the interaction must still correlate with the established solutions. It may be possible to on-board some blockchain or DLT interactions only when the legal framework sets rules for their application.

Although the necessary and applicable new solutions (including blockchain and DLTs) may not be available for implementation, the emergence of the new approach to data sharing is taking place already and the discussions could be taken on-board to review the current functioning logics of the tools. Any technology advance can be made only after a thorough review of the use cases, proposed solutions and their elements. To suggest use cases for eu-LISA, keeping track of best practices and the development of capacities and functionalities in various domains is considered a necessity. Such review enables eu-LISA also to support and advise other entities seeking to establish cross-sectoral or cross-border data exchange ecosystems and weigh various technology options.

Taking into account that some of eu-LISA's future developments might also involve data exchange with external non-governmental third-party IT systems, which might choose to operate on a blockchain or DLT platform, eu-LISA itself unavoidably has to consider possible industry developments and align itself with them. For that reason, it needs to be ready for integration or data exchange with other databases (including government ones) on other platforms than those in use today, if that happens.

To maximise the security and traceability of such external data exchanges, eu-LISA might decide to prefer and accept a selected structured DLT and participate in such platforms via dedicated separate nodes. Nevertheless, such a limited ecosystem should not have any influence on the management and operations of the systems themselves. If any data exchange or connectivity interaction with new technical approaches becomes necessary, the legislative framework and technical requirements will be reviewed and updated accordingly prior to any development activity.

Even though the blockchain and DLTs' promoters are overwhelmingly expecting those technologies to replace all existing data exchange structures, it is likely that those technologies will only be complementary to the existing technologies. It is also logical that any blockchain or DLT ecosystems will sooner or later need to be interoperable with other systems, including other DLTs, and e-government frameworks.

Several aspects need to be taken into account before considering the deployment of new technologies in large-scale government IT systems. First, in order to be integrated into eu-LISA's technology portfolio, blockchain and DLTs, or their functional components, the prospective solutions need to demonstrate reliability, trustworthiness and long-term sustainability. Second, for technologies – whether blockchain, DLTs or any other – to be successfully integrated into an existing government IT service infrastructure, they must be interoperable with different ledgers as well as existing ecosystem structures, ensuring that data can be exchanged with partners outside one's immediate ecosystem. eu-LISA envisages several use cases in which the functionalities of the technologies discussed would be beneficial for the end user or the systems, if the above-mentioned requirements were met.

6. Conclusion and further actions

Following their initial success in cryptocurrencies and crypto-assets more generally, blockchain and DLTs have emerged as general purpose technologies with the potential to transform other domains. Although blockchain might have certain limitations, its parent technology – distributed ledger – may bring a new approach to networked data exchange and record-updating ecosystems.

The paths of possible development are bipolar: some of the less advanced or more hesitant data exchange communities welcome blockchain or DLT as a novel approach, and the more advanced communities, in which system interoperability and cross-domain data exchange already exist, recognise blockchain elements as something already in place and functioning.

Although the technologies discussed in this report are still at the early development stage, their rapid diffusion across domains suggests that they may have a transformative effect on the existing systems in the medium to long term. The technologies in their current state already affect processes in business-to-business or business-to-government data sharing, and in e-governance more generally. For that reason, blockchain and DLTs would play a role in encouraging distributed data storage and exchange.

It is also predicted that blockchain platforms that are kept operational based on anonymous networks and constant mining will not be applied in data exchanges that include public sector services. Rigid ecosystems are likely to be replaced by federated, functional, resource-effective and relatively flexible interoperable frameworks, to which best practices of blockchain or DLTs will provide an inspiration.

Also, many blockchain solutions currently being tested will probably remain as proofs of concept and will not be scaled up to production systems. Thus, issues and limitations outlined as obstacles to immediate technology application are expected to be rendered irrelevant or ruled out by technology developers and communities working on the same elements (cryptography, access point security or record update consensus algorithms) independently.

New service providers and functionality developers will emerge, providing alternatives, integration and competition to current conventional IT developers, while disrupting the current centrally-coordinated approach. It is possible that the functionalities, capacities and elements of DLTs will be successfully integrated with other software functions in the next 5-10 years.

6.1. Further actions to be taken by eu-LISA, the industry and stakeholders

Stakeholders are encouraged to work on the following topics in relation to further development of the blockchain and DLTs functionalities or platforms:

- Data exchange logic and principles should favour interoperability to various ecosystems, and those seeking output to eu-LISA or government ecosystems, should rule for interoperability with eIDAS framework member state trusted digital IDs and interoperability standards;
- Data security and cybersecurity aspirations as well as data protection regulations and implementation are expected to be met at the highest level in accordance to the levels set for government or EU information systems;
- The blockchain and DLT industry communities themselves are encouraged to define, categorise and standardise the solutions, functionalities and capacities, and develop guidance on service levels for applications and platforms, technical descriptions and rules that the service must meet in order to be verifiable.
- Identity and timestamping meshes as well as rules for certification bodies should be initiated and coordinated beyond EU, possibly globally through relevant international organisations. Joint work is

required on commonly accepted criteria for the identification, signature and timestamping frameworks for supporting the setup of solutions, where the conditions for high-level identification of users can meet a standard and secure traceable interoperability can be guaranteed.

- Developers or customers are reminded that any solution should seek interoperability between different other ledgers or various identity management platforms, so that it has a pathway to exchange data with partners outside its own ecosystem and allow its users to enjoy the consumer rights in choosing a data exchange platform.
- The Agency might consider participating in dedicated proof-of-concept or pilot projects for the technologies. That would be possible within, for example, the dedicated EU framework programmes, such as Horizon 2020, the Connecting Europe Facility (CEF) or the upcoming Digital Transformation Programme 2021-2027[54].

With this in mind, eu-LISA believes that the developments of DLTs new technologies might be of relevance to the core business of eu-LISA. It will continue monitoring the developments in blockchain and DLTs, expecting the community to go forward with the development of the functionalities.

eu-LISA encourages the industry to consider the business needs of large-scale public information systems, while advancing the technologies, or elements of them, and to move from fragmented to distributed and interconnected records and data, ensuring interoperability between various ecosystems to the benefit of system operators and end users.

[54] European Commission (2018), Connecting Europe Facility, Digital Europe and space programmes — legal texts and factsheets, https://ec.europa.eu/commission/publications/connecting-europe-facility-digital-europe-and-space-programmes_en

Annex I. Self-sovereign identity

Concept of self-sovereign identity (SSI)

Since the rapid expansion of crypto-currencies, blockchain has gained traction across a wide range of industries, from finance and insurance to healthcare and logistics. One of the developments in blockchain applications most relevant to the work of the Agency is in identity management – more specifically, decentralised digital identity management. Proof of identity is one of the most frequently used services in both the private and the public sector; identity often also has substantial legal implications for both the holder of the identity and the service provider (be it public or private). Therefore, securing proof of identity has major implications for issues such as identity fraud and identity theft.

Nowadays, in most cases, the national government is responsible for guaranteeing the authenticity of identity of its citizens or residents. State authorities register birth or right of residence in population registers and issue birth certificates, passports and other kinds of identity documents, which are, in turn, used as proof of one's identity in interactions with the government and the private sector. Hence, in most countries with well-functioning state institutions, these serve as the guarantors of trust that the claimed identity is true. This can also be referred to as the centralised identity management system.

With the proliferation of online services requiring users to create electronic identity records with the service provider (in the form of a user name and password), new forms of identity managers appeared, often replacing the traditional state-based sources of trust in the online environment. These new identity providers are the most common social media networks (e.g. Facebook, Twitter or LinkedIn) or other major online service providers (e.g. Google). Identities provided by such services are called federated identities. Although the tools provided by these private identity providers for user identification and authentication in online environments are often more convenient than the state-based ones, they have certain disadvantages. First, the issuer can track such identities whenever they are used anywhere on the internet[55]. Second, users of such identities have no control over what information is being shared every time the identity is used online. Finally, these identities can always be revoked by the issuer.

Over the last 20 years, governments around the globe have invested significant effort into developing digital identities for use in online environments, effectively replacing the physical documents in most cases. Today, digital identities have moved beyond simple credentials (e.g. user name and password) to more sophisticated tools, including e-signatures, digital certificates, public/private key cryptography and other means of protecting and certifying the unique identity and ownership of them. However, verification of identity still relies on a single central authority as an intermediary.

Despite the major advances in developing digital identities and the underlying building blocks, the main issue related to identity management online, namely the fragmentation of means of identification, remains unresolved. State-issued digital identities are still largely confined to the nation state[56] and often cover only public services, while identities issued by internet service providers also cover only some internet services and often violate user privacy[57]. Last but not least, the connection between the state-

[55] Mirani, L. (2014), 'How Facebook and Google are taking over your online identity', Quartz, https://qz.com/271286/how-facebook-and-google-are-taking-over-your-online-identity/

[56] The EU has made an important step towards regionalising digital identity with the introduction of eIDAS. However, it is not certain at this time at which pace the eIDAS-based means of identification will be mainstreamed across the EU (covering both public and private services).

[57] European Union Blockchain Observatory and Forum (2019), *Blockchain and Digital Identity*, https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

issued physical identity and the digital identity used online is often weak (except for the state-issued digital identity), which creates ample space for ill-intentioned individuals to abuse false identities.

Self-sovereign identity (SSI) is one of the key blockchain-based innovations today, addressing most of the challenges discussed above and in particular focusing on strengthening privacy and user control. It may be of relevance for the Agency should SSI develop into a commonly accepted means of personal identification, in particular because SSI has the potential to address the need to provide identification for refugees[58], who often do not possess a government-issued identity either because the government of their nation state is dysfunctional or because it is actively hostile.

SSI effectively transfers the responsibility for identity management to the holder and user of the identity, who creates a unique digital identifier and personally maintains a data repository (e.g. in a digital wallet in the user's smartphone), where different identity attributes are stored (e.g. state-issued identity, driving licence, bank's client ID, healthcare ID, etc.). These identity attributes can be created by identity holders themselves or provided by the authorities in question, and the authorities can revoke them whenever necessary. The validity of the issued attributes can be verified using digital signatures connected to the corresponding attributes. SSI allows users to maintain control over the data stored in the repository and the data issued to service providers who request identity. Thus, the user can provide only as much information as is essential for the provision of the service, not exposing other identity elements (as one does, for example, when presenting a physical ID). Furthermore, the validity of the state-issued attributes can be determined by verifying the electronic signature, for example, thus eliminating the need for the service provider to request attestation of the attribute each time the attribute is used. SSI can therefore improve data quality (data will be stored in one repository and updated when necessary) and data privacy, help reduce processing costs, make service provision faster, and allow easier cross-border use of identification, which could eventually lead to a unified global identity standard[59].

Proof of concept of blockchain and SSI included in asylum procedures

Blockchain has numerous potential applications; however, very few of the potential use cases have been tested in a public sector context, especially as pilots or proof-of-concept projects[60]. Therefore, the discussion of the possible transformative potential of blockchain for the public sector is still largely based on hypothetical and theoretical scenarios. There are, however, a few public sector domains where blockchain has been applied with some success. One of those is migration, in which the German Federal Office for Migration and Refugees has recently successfully completed a proof-of-concept project, which trialled the application of blockchain technology for managing asylum procedures in a federal state.

The main reason to test blockchain implementation is because of the possibilities that blockchain-based infrastructure provides for coordination between the numerous different entities involved at different stages of asylum procedures in a federal state. Blockchain makes it possible to develop a federated system for tracking asylum procedures, while retaining all sensitive data in source databases and sharing only the necessary metadata on the status of the procedure on blockchain.

The project in question relied on the private permissioned type of blockchain (based on Ethereum platform), with the use of a proof-of-authority consensus algorithm. In this way, protection of personal data was ensured. Blockchain was used to track changes in the existing IT systems used during the asylum

[58] See for example ID2020, a multi-stakeholder initiative supported by the UN aiming to promote the development of digital identities: https://id2020.org/digital-identity

[59] Blockchain Bundesverband (2018), *Self-sovereign Identity: A position paper on blockchain enabled identity and the road ahead*, https://www.bundesblock.de/wp-content/uploads/2019/01/ssi-paper.pdf

[60] For an overview see JRC (2019), *Blockchain for Digital Government*, https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-digital-government

procedure. Existing systems (or simulated source systems used in the proof-of-concept project) were linked through an adapter, which tracked the changes (events) in the systems and communicated those to blockchain. The blockchain technology records them as transactions and groups them into blocks. Smart contracts were also used and could trigger a change in the existing system on the basis of a procedure inscribed in the smart contract, thus essentially eliminating the time lag between the different steps in an asylum procedure.

The key conclusions of the proof-of-concept project were:

- Blockchain can effectively support cross-organisational (and cross-national) coordination, especially in those cases where during a certain procedure a number of organisations make decisions in a cascade.
- The use of blockchain becomes increasingly beneficial as the number of steps and parties involved in a procedure grows.
- Incorporating SSI in this process would also make it possible to reap benefits from the automation of procedures, would speed up the procedure, and make it more secure.

However, for more complex procedures with a number of sectoral actors involved, the authors of the study suggested implementing a federated blockchain architecture with several blockchain processes running in parallel and a central blockchain ledger that would only record the results of procedures carried out within the individual sectoral blockchains. This would make it possible to improve performance and increase the capacity of the system. On a higher level, the study concluded that blockchain-based architecture would be a technological enabler for federalism in asylum policy at the EU level, in particular facilitating the Dublin procedure by providing a transparent system for storage of the person's initial place of registration, for instance[61].

[61] For more information on the project please see Fridgen, G., Guggenmos, F., Lockl, J., Rieger, A. and Urbach, N. (2019), *Supporting communication and cooperation in the asylum procedure with blockchain technology: A proof of concept by the Federal Office for Migration and Refugees*, https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/944/wi-944.pdf

Glossary

CEF	Connecting Europe Facility
CONNECT	Directorate-General for Communications Networks, Content and Technology
CRRS	Central Repository for Reporting and Statistics
DLT(s)	Distributed Ledger Technology(-ies)
DG CNECT	Directorate-General for Communications, Networks, Content and Technology
EBSI	European Blockchain Services Infrastructure
EES	Entry/Exit System
eID	Electronic Identification
eIDAS	Electronic Identification and Trust Services for Electronic Transactions
EIF	European Interoperability Framework
ENISA	European Union Agency for Network and Information Security
ETIAS	European Travel Information and Authorisation System
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
Eurodac	European Asylum Dactyloscopy Database
GDPR	General Data Protection Regulation
INATBA	International Association for Trusted Blockchain Applications
IoT	Internet of Things
IT	Information Technology
JHA	Justice and Home Affairs
NUI	National Uniform Interface
OECD	Organisation for Economic Co-operation and Development
SIS	Schengen Information System
SSI	Self-Sovereign Identity
UNHCR	United Nations High Commissioner for Refugees
VIS	Visa Information System

EL-03-19-727-EN-N

ISBN 978-92-95217-55-3

DOI:10.2857/111687

Catalogue number: EL-03-19-727-EN-N