Please, cite as:

L. R. de Lope *et al*., "Boosting IoT data valorization through the adoption of DLT," *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, Montreal, QC, Canada, 2021, pp. 1-5, doi: 10.1109/ICCWorkshops50388.2021.9473741.

Boosting IoT data valorization through the adoption of DLT

Laura Rodríguez de Lope, JohnnyChoque, Luis Muñoz, *Communications Engineering Department, Universdad de Cantabria,* Santander, Spain.

Sofia Terzi, Kostantinos Votis, *Centre for Research & Technology Hellas/ITI,* Thessaloniki, Greece.

Andrés Sánchez Sandaza, Jorge Fernández Valdes, *FundingBox Accelerator,* Warsaw, Poland.

Har Preet Singh, *FIWARE Foundation* Berlin, Germany.

The authors gratefully acknowledge financial support from the European Union's Horizon 2020 research and innovation programme under grant agreement No 870603 project TOKEN

ABSTRACT

During the last decade Internet of Things has become one of the key technologies in supporting digital transformation of several ecosystems such urban or industry ones. The huge amount of data generated in such contexts as well as the imperative requirements in terms of trustworthiness, authenticity and integrity make compulsory the adoption of the proper solutions fitting those requirements. This paper presents the design, implementation and validation of a distributed ledger technology architecture emphasizing services linked to data valorization.

KEYWORDS

Blockchain, data valorization, distributed ledger technology, Internet of Things.

I. INTRODUCTION

Present digital ecosystems are characterized by the generation of a vast amount of data. Some very illustrative examples are smart cities, industry 4.0 or the agrifood sector. They are characterized by the use of heterogeneous monitoring and command infrastructures which provide contextual information linked to the processes they are supporting. One example is the generation of environmental data providing information about CO2, noise or humidity. Further to this, data citizens can expose their own data aiming at making a reality the paradigm of innovation and collaborative ecosystems. The use of that information by third parties is more and more common but in addition to that, it is necessary to valuing these data, which implies having the ability to extract from them the answers to the commercial interests of the companies. For example, the knowledge of traffic conditions in different areas of the city might provide critical information to the last mile delivery vehicle fleet enabling to optimize the performance and fulfilling the service agreements committed with the correspondent customers.

In this framework it is obvious that data interchange and processing has to be carried out with very specific requirements whilst guaranteeing their integrity. In addition, the owner of the data has the right to trace the use of them. All in all, issues such immutability and quality of the information play a key role in the scenarios as the ones aforementioned.

It is the objective of this paper to present a Distributed Ledger Technology (DLT) that has been adopted in TOKEN initiative [1] and applied to support the requirements linked to data valorization services. Thus, after this introduction, some background work will be presented. Afterwards the main hints in terms of architecture components and interfaces will be described. Finally, the use of such architecture for supporting data valorization services will be elaborated.

II. BACKGROUND AND RELATED WORK

FundingBox [2] started to explore decentralized technologies in the Horizon 2020 EU funded project LEDGER [3], where a blockchain using hyperledger fabric was built and integrated to its current platform for the purpose of adding trust, security and transparency to the process of distributing public funding.

Blockchain, a distributed ledger, refers to a data structure that is made up of data records or blocks of data that are linked to each other as a linked list using cryptography. It was successfully used in Bitcoin [5] to solve the double-spending problem [6]. Each of the data blocks is made up of a header containing relevant metadata about the block, followed by a long list of transactions. The block header mainly includes a reference to a cryptographic hash of the previous block, a set of fields relates to the mining competition (difficulty, timestamp and nonce) and the Merkle Tree root, a hash that summarize all the transactions of the block. The data chain is designed to resist modification, that is, before another block can add to the chain, it has to be first verified by at least one node in the system. Once the block is verified and added to the chain, the data block cannot be tampered with or altered. Blockchain can be used to record transactions involving different parties effectively in a permanent and verifiable way since the system provides accurate histories of uncorrupted data [7].

On the other hand, the increasing convergence between IoT technology and blockchain allows to overcome the significant challenges that hinder the full realization of IoT platforms. IoT devices have become part of our everyday lives with wearable devices, mobile phones, smart vehicles and smart home devices, but they are prone to cyber-attacks. Especially for IoT devices operating in public spaces, tampering of data through cyber-attacks threatens the integrity of the data transmitted due to unsecure environments as well as untrusted communications and centralized message exchanging models [8]. With these threats in mind, it becomes crucial to use a decentralized infrastructure for storing the information in order to prevent having a single point

of failure and to get advantage of the chained digitally signed blocks of information on the ledger to avoid tampering of data. The aforementioned blockchain characteristics will ensure a comprehensive layer of truth, transparency, traceability and visibility for all the records [9].

Another relevant technology that drives the deployment of IoT is FIWARE [10], whose mission is to build an open sustainable ecosystem and platform standards that will facilitate the development of new Smart Applications in multiple sectors. To fulfill this purpose, FIWARE platform provides common APIs that ease the design and development of smart applications. The specifications of these APIs are public and royalty-free. Besides, an open-source implementation of each of the FIWARE components (named Generic Enablers, GEs) is a set of general-purpose platforms available to application developers through APIs.

A Context Broker GE is the core and necessary component of any “Powered by FIWARE” platform or solution. It facilitates the management of context information in a highly decentralized and large-scale manner.

The Orion Context Broker Generic Enabler provides the FIWARE NGSI API which is a simplistic yet robust Restful API enabling to perform updates, queries or subscribe to changes on context information.

On the other hand, interaction with the Internet of Things (IoT), Robots, and third-party systems, to store updates on context information and translating required actuation and FIWARE avails various Generic Enablers are available making it easier to interface with the Internet of Things, Robots and Third-party systems to gather valuable context information or trigger actuation in response to context updates:

Due to the advantages offered by blockchain, IoT and FIWARE, applications are being created that combine these technologies.

One of the studies presented an architecture based on blockchain that introduces the edge computing layer and a new algorithm to improve data quality and false data detection [7]. Another application presents an approach for blockchain-based distributed IoT data transactions. In this [19], users can take advantage by trading their data, and the service providers acquire user's data to obtain access. Moreover, all activities of IoT data transactions are stored in the blockchain to increase the security of the transactions. However, these applications have several deficiencies because they are too customary.

III. TOKEN ARCHITECTURE AND SERVICES

The TOKEN platform can be defined as a decentralized architecture that leverages in state-of-the-art cryptographic techniques such as Distributed Ledger and Attribute Based Credentials to build a system that provides participants with the capability to securely store the data, give control and transparency over for what purpose data are shared and transacted with other participants or organizations. TOKEN platform is made of free and open source services and software components according to licenses approved by the Free Software Foundation Europe [12] and emerging open standards. It follows six architectural principles that enable the TOKEN ecosystem to develop technology that puts people in control of their personal data, giving them the ability to decide how it is shared: free and open source; modularity and interoperability; reuse don't re-invent; decentralization and federation; privacy by design; user friendliness.

The TOKEN platform infrastructure comprises:

- An organized collection of standards, specifications and data formats/vocabularies providing capabilities such as identity, authentication, authorization, verification, messaging, etc.
- A set of open source software components, APIs and SDKs (Software Development Kits) related to Decentralized Identity and Storage.

- Specifications and design notes describing an API to extend existing standards and achieve the interoperability with existing DLT solutions, to guide developers building servers or applications.
- A Testnet (distributed network) implementing the Token specification.
- A decentralized infrastructure that runs as Blockchain as a Service (BaaS) [10] to provide out-of-the-box ready to integrate services.
- A test suite for testing and validating TOKEN implementations.
- An ecosystem of applications, identity and storage providers, and helper libraries that run on the TOKEN platform.
- A community providing documentation, discussion, tutorials, and presentations.

This architecture is the basis for the services or components that will be provided by the TOKEN platform that can be summarized in the following four blocks with the correspondent subservices.

A. Blockchain based Notarization Services

The Blockchain based notarization services are intended to provide immutability and transparency to the services created using them. It is a service to assess that a transaction has taken place allowing to be time stamped or even to include certain non-binary data in the record. This block includes the following component or enablers:

- TOKEN TTS (Trusted Time Stamping): A REST-API to provide anonymous, tamper proof time stamps for any digital content as proof of existence of a given document, data or transaction in a given time.
- TOKEN Registry: A REST-API to provide tamper-resistant, immutable on-chain storage.
- TOKEN Sign: A decentralized application providing document signing and verification using DIDs (Decentralized Identifiers) and blockchain to store the signatures/transactions.
- FIWARE Canis Major: A blockchain adaptor enabling the integration of DLTs in powered by FIWARE solutions.
- TOKEN SSI (Self-Sovereign Identity): A blockchain based self-sovereign identity solution that enables secure and cryptographically verified authentication and authorization for the TOKEN platform users.

B. Decentralized and Self Sovereign Identity

This block is composed of two main components: TOKEN Connect and Identity as a Service (IaaS) [13]:

TOKEN Connect: is an identity wallet implementing the DID AuthN profile for OpenID Connect [14]. It allows the user to login in a service with their decentralized identifier, enabling relaying parties to use the Self Issued OpenId protocol [15] to authenticate the user.

Instead of an enterprise providing an identity on behalf of a user, the user becomes the identity claim provider. This means, the user will not share their personal information with any external party. Hence, the user could decide what information will be shared with whom and when.

This component will be facilitated through a REST API. The first release is compatible with did:ethr: method [14] and any other method based on the same specification like did:jolo did:uport [14] and any other method that allows the user the control of their own privateKey.

At this stage, it is intended only for authentication purposes. Therefore, it does not provide the mechanisms to interact with verified credentials. Future releases may include support for verified credentials, sign documents and receive notifications.

The IaaS solution is hosted on a fully decentralized BCPaaS (Blockchain Platform as a Service) network running Hyperledger Indy [16] DLT and supports the creation of an account for any participant of the TOKEN platform. After the user registers for an account a wallet is created for them to keep their private data that is accessible only to them. The original solution created by CERTH [17] supports full decentralization by storing the wallet locally and providing full control over it to the holder by engaging an agent, as well as supporting the usage of Zero Knowledge Proof (ZKP) for preventing disclosing any sensitive or not necessary information. For serving simplicity for the TOKEN project the solution has been modified and uses an online wallet to save the users from having to download special software to their computer or mobile.

By maintaining the SSI implementation fully online, the e-government bodies do not have to maintain their own servers, storage or even custom software as all these functionalities are provided out of the box and they can benefit from the Single-Sign-On solution [18] at zero costs. Thus, by integrating the SSI as a service of TOKEN platform to their custom applications, the public bodies achieve the decentralization, security and authentication levels needed for their e-government applications. Following you can view the architecture of the system and the interactions.

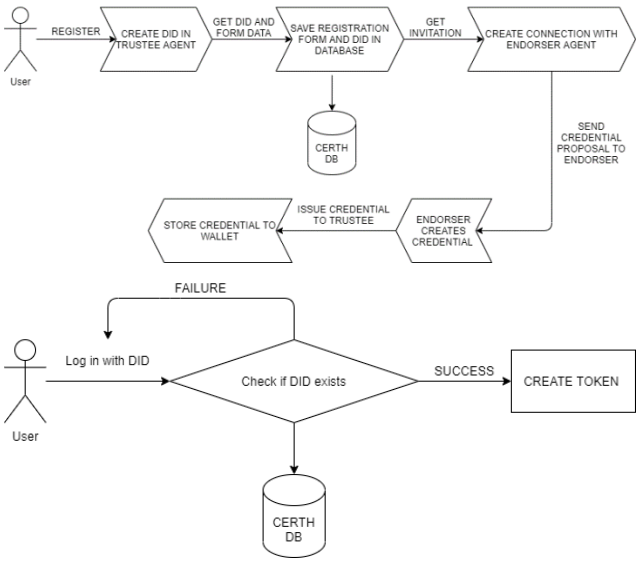

Fig.1. SSI as a Service TOKEN platform solution

C. Decentralized and Distributed Storage

1) TOKEN Storage Network

Unlike traditional cloud services, the service is built on open and decentralized protocols including the IPFS (InterPlanetary File System) and Libp2p [20]. It can serve websites, data, and even apps using the storage network. The TOKEN Storage Network (TSN) and APIs provides features such: i) create public/private (encrypted) datastores where apps can store data; ii) create personal datastores where app users can store data; iii) use public datastores to distribute content and

apps to the web, iv) collaboratively manage datastores as an app/organization or create automations with other TOKEN Services (files notarization, sending notifications with attachments, attach files to batch processing pipelines, etc.)

2) TOKEN Public IPFS Services

a) IPFS Web Gateway: TOKEN's read-only IPFS web gateway acts as a bridge between traditional web browsers and IPFS.

Through the gateway, Internet users can browse files and websites stored by third parties on the IPFS public network quickly and easily, without downloading any special software, as if they were stored in a traditional web server.

b) IPFS Storage & Pinning service: simplifies decentralized storage offering redundant and persistent data storage on the IPFS public network.

Through the TOKEN's IPFS storage API, users can upload, store and fetch files from the IPFS public network in an easy to use and agile way, while its built in pinning orchestration service ensures all uploaded information is replicated across multiple nodes and retained and accessible as long as needed.

We expect that our IPFS services will serve as the platform for highly-reliable and security-enhanced web applications.

D. Messaging and Events Streaming

The objective of TOKEN Stream is to communicates securely and reliably with end-to-end encrypted messaging from App2App-App2User-User2User

The WebSocket Streams API provides mechanisms for sending and receiving messages between users using DIDs or PKI (Public Key Infrastructure) where users hold private keys linked to their identity. With just their private and public key, a user can send and receive encrypted messages to other users in an app.

Combined with the Notarization services it will also provide evidence relating to the handling of the transmitted data, including proof of sending and receiving the data. It can also be used in other use cases such as, data pipelining, orchestration, chat or batch job scheduling.

The main components of TOKEN Streams are:

- Kafka [21] cluster
- TOKEN service connectors (Notarization, DID resolver/cache)
- Preconfigured - TOKEN Stream processors (Electronic Registered Delivery Service, ERDS)
- WebSockets API to produce/consume messages/streams
- API Gateway for pre-processing + Authentication/Authorization

IV. IoT and Data Valorization

Current digital ecosystems are characterized by the vast amount of data generated by IoT deployments. This section presents a use case focusing on better exploitation of IoT data through a better knowledge of its usage.

The implementation of this use case, linking IoT and data valorization, opens a new dimension enabling to set up synergies between technology and digital economy. In this sense, we will

leverage on the incipient IoT Data Marketplace [22] running in the city of Santander (Spain) for assessing the role and interaction of the involved stakeholders in the rising of a new paradigm of the binomial technology and economy.

The SmartSantander framework [23] has been consolidated as the catalyzer of the digital transformation of the city. Thanks to this transformation, Santander is able to improve their citizens' lives whilst increasing the efficiency of urban services. Furthermore, aiming at conceiving an inclusive city overcoming the digital gap, city managers offer different platforms and tools which encourage citizen participation. This brings a new dimension to the city and technology symbiosis offering the citizens a plethora of possibilities in terms of thinking, designing, implementing and assessing new services raised by urban collectives and activists. Exploring new economic models based on data valorization is a natural next step.

Through the adoption of TOKEN services, this use case wants to take advantage of the opportunities offered by DLT and smart contracts to trace the use of data made by third parties so that the supplier can have a better picture of the real number of consumers of a data source as well as how they exploit this data.

The use case envisions a state where a supplier of data receives an overview of how the exposed data is being used by third parties. This knowledge and valorization of data brings new business opportunities that will attract new stakeholders to the supplier side. In this sense, companies, associations, or even citizens will be encouraged to publish their urban data enriching the marketplace offer with the possibility of being reimbursed.

Looking at the demand side of the platform, these actors would be able to increase their current services by exploiting existing context data without making the investment on new IoT deployments. Next to this, they will be able to monitor the QoS (Quality of Service) ensured by the SLA (Service Level Agreements).

As depicted in Fig. 2, Santander IoT Data Marketplace core architecture is realized by a set of FIWARE components [24], which consists of a Context Broker, API Proxy, Identity Management and Policy Management linked to the Business App Ecosystem which manages the data sets offers, acquisition and policy terms.

Through the TOKEN API gateway, the different FIWARE components interact with the TOKEN BCPaaS.

Among others, TOKEN BCPaaS will allow to achieve the trustworthiness in the data ownership through the interaction of the Self Sovereign Identity service with the Identity Management. Notarization services facilitate the traceability of data usage, registering in the ledger the datasets acquisitions in the marketplace and the data requests to the context broker. In addition, the registration of requests solved with a “Denial of Service”, together with Canis Major module, which facilitates the registration of “out of range” data values, facilitate the monitoring of the QoS agreed on the SLA.

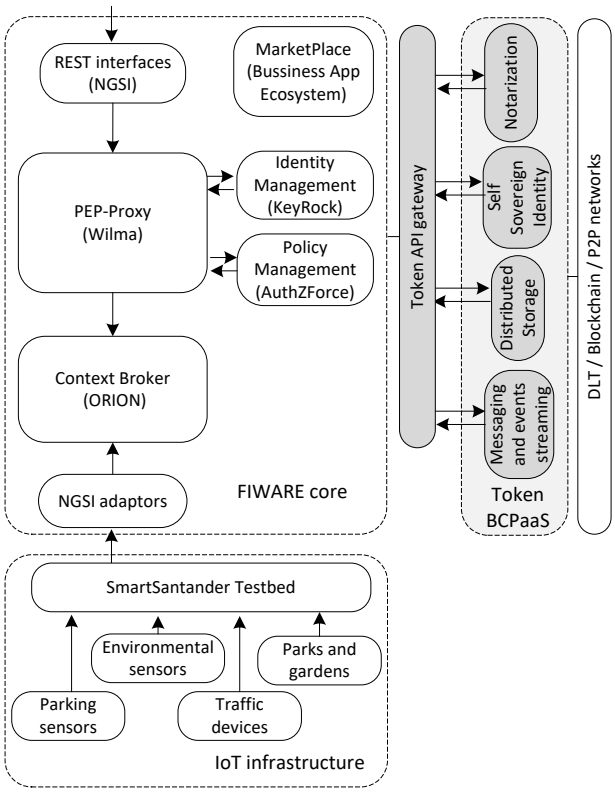

Fig. 2. SmartSantander reference architecture

V. CONCLUSIONS

DLT can help to secure the IoT implementations, especially in terms of data integrity, transparency and traceability. The immutable nature of the blockchain ledger that prevents data tampering along with the cryptography and digital signatures that accompany every record can add value to the solutions that utilize such technologies by increasing the verifiability and visibility for both the public authorities and citizens. With the addition of user centric designs as IaaS with SSIs for accessing the decentralized data, the required levels of authentication and authorization are met and by having the networks and services running as a service the costs for developing, maintaining and updating them for the public bodies are minimized or even eliminated.

Despite the aforementioned advantages, there are still challenges to tackle in the application of DLT to IoT ecosystems. On one hand, the technological challenges, like the lack of standards or clear example of best practices may lead to locking into a single vendor or technology. TOKEN BaaS tackles this issue by offering DLT agnostic solutions. On the other hand, there are legal challenges. For a technology whose main purpose is collaborative data sharing and immutability of data gathered, issues on data protection are among the most challenging. In a context where citizens and companies are fostered to publish data, the data offered in the marketplace should avoid personal information, encouraging data anonymization.

Last but not least, it has been shown a novel use of DLT in service valorization. This example should be one of the enablers in the fostering digital ecosystems, opening a new dimension enabling to set up synergies between technology and digital economy.

ACKNOWLEDGEMENT

This work is supported by the TOKEN Project: “Transformative Impact Of BlocKchain tEchnologies iN Public Services”, Grant Agreement 870603, belonging to the H2020 Framework Program. The authors want to acknowledge the valuable work carried out by the colleagues participating in this initiative.

REFERENCES

[1] “Transformative impact of distributed technologies in public services”. [Online]. https://token-project.eu/ , accessed 10-02-2021

[2] “Funding Box”, [Online], https://fundingbox.com/, accessed 10-02-2021

[3] “LEDGER project”. [Online]. https://ledgerproject.eu/, accessed 10-02-2021

[4] N. V. Kuchin, K. O. Polyakov and N. G. Butakova, "Transaction Protection in Corporate Networks Based on Distributed Ledger Technology," 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg and Moscow, Russia, 2020, pp. 2072-2076, doi: 10.1109/EIConRus49466.2020.9039210.

[5] Nakamoto S., (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[6] “Double-Spending—Bitcoin WiKi”, accessed on Mar. 15, 2016. [Online]. Available: https://en.bitcoin.it/wiki/Double-spending

[7] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, 2017, pp. 618-623, doi: 10.1109/PERCOMW.2017.7917634.

[8] X. Liang, J. Zhao, S. Shetty and D. Li, "Towards data assurance and resilience in IoT using blockchain," MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, 2017, pp. 261-266, doi: 10.1109/MILCOM.2017.8170858.

[9] Geetanjali Rathee, Ashutosh Sharma, Rajiv Kumar, Razi Iqbal, A Secure Communicating Things Network Framework for Industrial IoT using Blockchain Technology, Ad Hoc Networks, Volume 94, 2019, 101933, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2019.101933.

[10] J. Singh and J. D. Michels, "Blockchain as a Service (BaaS): Providers and Trust," 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, 2018, pp. 67-74, doi: 10.1109/EuroSPW.2018.00015.

[11] “FIWARE Foundation”. [Online]. https://www.fiware.org/ , accessed 10-02-2021.

[12] Free Software Foundation Europe. [Online]. https://fsfe.org/, accessed 10-02-2021.

[13] Vo, T.H.; Fuhrmann, W.; Fischer-Hellmann, K.-P.; Furnell, S. Identity-as-a-Service: An Adaptive Security Infrastructure and Privacy-Preserving User Identity for the Cloud Environment. Future Internet 2019, 11, 116. https://doi.org/10.3390/fi11050116

[14] W3C. “DID Specification Registries. The interoperability registry for Decentralized Identifiers”. [Online], accesed 10-02-2021

[15] DIF working group.”Self-Issued OpenID Connect Provider DID Profile v0.1” [Online] https://identity.foundation/did-siop/#did-siop, accesed 10-02-2021

[16] “Hyperledger Indy, Distributed Ledger Software”, https://www.hyperledger.org/use/hyperledger-indy, accessed 10-02-2021

[17] S. Terzi, C. Savvaidis, K. Votis, D. Tzovaras and I. Stamelos, "Securing Emission Data of Smart Vehicles with Blockchain and Self-Sovereign Identities," 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes Island, Greece, 2020, pp. 462-469, doi: 10.1109/Blockchain50366.2020.00067.

[18] H. Arslan, H. D. Karkı, A. G. Yüksek and O. Kaynar, "Examining of single sign on protocols and a model of business application," 2017 25th Signal Processing and Communications Applications Conference (SIU), Antalya, 2017, pp. 1-4, doi: 10.1109/SIU.2017.7960221.

[19] H. T. T. Truong, M. Almeida, G. Karame and C. Soriente, "Towards Secure and Decentralized Sharing of IoT Data," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 176-183, doi: 10.1109/Blockchain.2019.00031.

[20] “Libp2p, a modular network stack”, [Online] https://libp2p.io/ , accessed 10-02-2021

[21] “Kafka, a distributed streaming platform- documentation”. [Online]. https://kafka.apache.org/documentation/ , accessed 10-02-2021

[22] A. Gaglione, D. Puschmann, A.Gluhak , M. Maggio., “ Advanced data marketplace enablers” SynchroniCity, Rep. D2.5, Jan. 2020.

[23] L. Sanchez et al., "SmartSantander: IoT experimentation over a smart city testbed", Computer Networks, vol. 61, pp. 217-238, 2014, ISSN 1389-1286, doi: 10.1016/j.bjp.2013.12.020.

“FIWARE catalogue”, [Online], https://www.fiware.org/developers/catalogue/, accessed 10-02-2021