

A Blockchain-based Data Notarization System for Smart Mobility Services

Raimondo Cossu¹, Maria Iliana Lunesu³, Marco Uras^{1,2}, and Alessandro Floris^{1,2}

¹ Department of Electrical and Electronic Engineering, University of Cagliari, 09123 Cagliari, Italy

² CNIT, University of Cagliari, 09123 Cagliari, Italy

³ Department of Mathematics and Computer Science, University of Cagliari, 09123 Cagliari, Italy
{raimondo.cossu, maria.i.lunesu, marco.uras, alessandro.floris84}@unica.it

Abstract—Nowadays, Internet of Things (IoT) applications are widespread in different scenarios, such as industry, mobility, healthcare, and agriculture. A relevant share of the credit is due to the Blockchain technology, which provides important features to IoT services, such as decentralized validation of transactions as well as immutability and traceability of the transactions. In this paper, we propose a Blockchain-based data notarization system for mobility services. First, we present an IoT-based crowd monitoring system aimed at counting the number of people in a specific area and providing information regarding people mobility (i.e., how people move within the city) and dwell time (i.e., the time people stayed at specific places). Then, we discuss our proposed data notarization system focused on ensuring data integrity and immutability of the mobility data collected by the crowd monitoring system, regardless of the used Blockchain. Finally, we provide experimental results regarding people mobility data collected during a literary event as well as an implementation of the proposed data notarization system using the EthernZero blockchain.

Index Terms—Blockchain, Data Notarization, Smart Mobility, Internet of Things, Crowd Monitoring.

I. INTRODUCTION

The Internet of Things (IoT) paradigm has assumed an important role in connecting real world devices with their virtual counterparts in the cyberspace of computing systems forming the so-called cyber-physical system (CPS) [1]. Thanks to these characteristics, IoT applications have been developed for a wide diversity of scenarios in the last years, such as industry, mobility, healthcare, logistics, and agriculture.

Besides the relevant advantages introduced by the adoption of IoT, such as service decentralization, data and device heterogeneity, and network complexity, the IoT also includes important challenges, such as limited resources, poor interoperability, and privacy and security vulnerabilities. In this regard, the birth of the Blockchain technology has provided important features to IoT services, such as decentralized validation of transactions as well as immutability and traceability of the transactions [2] [3].

This work has been partially funded by the Italian Ministry for the Economic Development (MISE), under the framework “Asse II del programma di supporto tecnologie emergenti (FSC 2014-2020)”, project Monifive.

©2022 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
DOI: 10.1109/SANER53432.2022.00146

A blockchain can be defined as a distributed ledger spreading over the whole distributed system. Blockchains implement the decentralized consensus to enable a transaction to occur and be validated in a mutually distributed system without the intervention of the trusted third party. Moreover, each transaction saved in blockchains is essentially immutable since each node in the network keeps all the committed transactions in the blockchain. Moreover, cryptographic mechanisms can be used to guarantee the integrity of data blocks in the blockchains and to ensure nonrepudiation of transactions. Furthermore, each transaction in blockchains is traceable to every user with the attached historic timestamp [2] and data could be further analyzed using ad hoc tools [4].

The key role of the blockchain in the wide dissemination of the IoT [5] is mostly due to its nature of immutable public ledger of transactions structured as a chain of blocks that contains transactions and whose validation is entrusted to a consensus mechanism. In the case of permissionless or public blockchains, the consensus is distributed on all network nodes whereas in the case of permissioned or private blockchains all the nodes that are authorized to participate in the transaction validation process to be included in the register contribute to the consensus.

In this paper, we aim to support an IoT-based crowd monitoring system with the blockchain technology to leverage the immutability and traceability features of the blockchain transactions for validating crowd mobility data. The crowd monitoring system utilizes IoT devices to collect people mobility data from the real world. Such data is then stored and processed in a cloud platform to derive information regarding the mobility of people in the monitored area. The objective is to obtain important information that can be used to plan and manage private and public mobility services with regard to city events involving crowds.

The role of the blockchain in this regard is to provide a data notarization solution that certifies the mobility data processed by the crowd monitoring system. Mobility data concerns relevant information, such as number of people in a specific monitored area, number of people joining and leaving an event in specific slot times, and dwell times. The blockchain-based data notarization system is aimed to ensure data integrity and immutability of the mobility data collected by the crowd monitoring system, regardless of the used blockchain.

Finally, we provide experimental results regarding people mobility data collected during a literary event as well as an implementation of the proposed data notarization system using the EthernZero¹ blockchain.

The contribution of our work is summarized as follows. Section II presents the related work about the notarization in general and with particular focus on data coming from IoT sensors. Section III describes the proposed system that includes an IoT-based crowd monitoring system and a data notarization system. Section IV discuss experimental results achieved with the considered case study focused on mobility. Finally, Section V concludes the paper.

II. RELATED WORK

In this section, we summarize the notarization applications and services already existing in the literature. We start from the general notarization services and then we describe in depth those related to the IoT measurements.

The Blockchain phenomenon is constantly growing and expanding towards all fields such as media, healthcare, education and projects are growing in number and becoming more concrete and sophisticated all over the world. There are various ways in which companies today are approaching Blockchain technology. One of the clearest examples of this way of using Blockchain and Distributed Ledger is notarization. There several notarization services already existing. Their first uses were related to the notarization of personal documents, such as birth certificates and marriage, using Bitnation, which initially used Ethereum but is open to the use of other Blockchains.

In [6], the authors present a blockchain-based notarization service in the context of medical environment with the goal to ensure the retrieved data immutability. They proposed the use of blockchain technology to create smart digital contracts to seal the query and the respective results each time a third-party requests knowledge from a biomedical database. The feasibility of the proposed notarization approach is demonstrated using a real blockchain infrastructure and tested it on two different biomedical databases. Medical and academic data represent an example of critical and sensitive private information which is usually hosted across many data custodian systems that allow to store, manage and deploy their key personal data in a highly secure and structured way and a personal information control point for their data. Blockchain provides a shared, immutable and transparent history of transactions enabling the building of applications that incorporate trust, accountability and transparency. Authors propose a data sharing framework that will guarantee the authenticity of the shared data in real-time and provide transactional privacy in a blockchain network. The essence of the presented work is to provide sharing documents authenticity through the use of a permissioned Blockchain, in order to limit the access and the hashes document generation to a restricted set of valid data custodian. The proposed paper shows the architecture of blockchain

where is provided the notarization service and the mechanism to ensure the transactional privacy. In [7], the protocol named NFB (Notarizing Files over the Blockchain), which ensures the communication between a permissive Blockchain and a secured centralized archiving document management system, has been described. The proposed method is used to allow users to archive, control, analyze and validate their transactions in a system that offers confidentiality, security and distribution features.

In the IoT ecosystem, the huge amount of data that is generated from users' devices is constantly increasing. As a consequence, the value of the data is also increasing because big data analysis processes allow to extract precious information that can be used to drive IoT applications. However, the provisions of the European General Data Protection Regulation (GDPR) require data subjects to be able to control their personal data, be informed, and consent to its processing in an intelligible manner. In [8], the authors presented a framework, named ADVOCATE, that in IoT environments helps personal data GDPR-compliant processing. The aim of this paper is to assist stakeholders, i.e. Data Controllers and Processors, to satisfy GDPR requirements, such as informing data subjects in a transparent and unambiguous manner about the data they will manage, the processing purposes, and periods. At the same time a notary service that uses blockchain infrastructures for ensuring consents' security was described.

The blockchain technology can be used to build IoT system as well as to control and configure IoT device. In [2], a system to manage IoT devices using Ethereum blockchain computing platform is proposed. The smart contracts were used to save data coming from smart meters and smartphone devices. These devices sent electricity data and commands for air conditioner and light bulb, respectively. A survey of blockchain for IoT is presented in [5]. The authors highlight the fact that blockchain technology can complement IoT systems with the enhanced interoperability and the improved privacy and security. Also, blockchain can improve the reliability and scalability of IoT systems. Motivated by the potential opportunities that can be provided by the blockchain technology to IoT applications [9], in this paper we focus on a novel blockchain-based data notarization system for IoT-based crowd monitoring systems aimed at supporting the planning of smart mobility services.

III. PROPOSED SYSTEM

In this section, we present the proposed system, which is composed of the Crowd monitoring system (Section III-A) and the Data notarization system (Section III-B).

A. Crowd monitoring system

The proposed Crowd monitoring system is based on the People mobility Analytics (PMA) solution [10, 11], which fully implements the IoT technological chain shown in Fig. 1. Indeed, the PMA system is composed of sensing devices that acquire data from the real world (people mobility data) and send this data to the cloud computing platform, where the data is stored and then processed with machine learning

¹It is a Blockchain currently managed by the Department of Mathematics and Computer Science of Cagliari University (DMI) and by NetService as part of joint research projects.

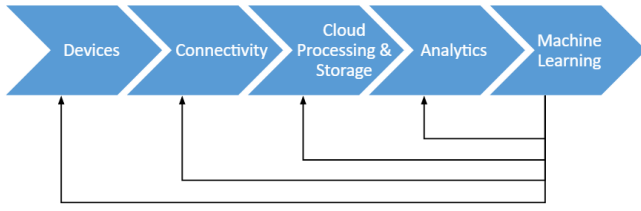


Fig. 1. IoT technological chain.

based algorithms to extract crowd information for mobility services. The main objective of PMA, in fact, is to support mobility services, i.e., those services aimed at organizing and implementing sustainable transport systems for the smart city. To reach this objective, it is important to monitor and understand how people move within the city.

The hardware sensing device is called *DataNode*, which is an electronic board equipped with Wi-Fi antennas aimed at collecting data from Wi-Fi signals generated automatically by the smartphone devices of people. Indeed, the Wi-Fi interfaces of the smartphones scan automatically and continuously the context in which they are located looking for an Access Point to connect to, by sending specific packets. The *DataNode* collects these Wi-Fi scan packets with the aim to identify the number of smartphone devices in its proximity. In particular, the information of interest is the MAC address of the smartphone device, which is transmitted within the Wi-Fi scan packets. More details regarding the Wi-Fi probes sniffing are provided in [12].

Although the role of the MAC address is to uniquely identify the network interface to which transmit and receive the data, many mobility solutions can be found in the literature that are based on tracking the movement of personal electronic devices (e.g., smartphone) by tracking the identification of the device's MAC address in different places. Therefore, tracking the MAC address corresponded to tracking the owner of that device and collect information such as movements, visits to websites, registration to services, etc. It is evident that such a technique constitutes a relevant privacy issue for people moving in the city with their Wi-Fi interface active. For this reason, the General Data Protection and Regulation (GDPR), Regulation (EU) 2016/679, included the MAC address as a personal data and must be treated as such.

However, in the last years, the manufacturers of the network interfaces (e.g., Wi-Fi and Bluetooth) intended for human-centered devices (e.g., smartphone, tablet, smartwatch) have implemented particular techniques to generate a random MAC address for these interfaces in order to protect the privacy of their customers. Due to these techniques, these devices are no longer utilizing a unique MAC address in data communication services, but a random MAC address is generated and used every few minutes or seconds. Thus, it is not longer possible to utilize a MAC address to identify and track people.

Motivated by the challenges introduced by the random

generation techniques implemented by recent human-centered devices, with the proposed PMA system we focused on the research and development of a de-randomization algorithm, explained in [11, 12], which allows to derive the exact number of devices sensed in the proximity of the *DataNode* and to temporarily trace these devices. The complete architecture of the PMA system is shown in Fig. 2. It is composed of several different microservices that can be grouped in 3 main parts:

- **Data Extraction:** includes the data entry service that collects the raw data received from the *DataNodes* and performs preliminary data extraction processes to facilitate the data storage and the subsequent data analysis processes.
- **Data Transformation:** includes the following services: Derandomization service, Path Generation, Dwell Time Calculator, Real Time Estimator, Job scheduler and Daily Report Generator services. The Derandomization service is called through the Job scheduler, which is the heart of the Data Transformation part that allows to provide the mobility statistics. At specific set time intervals, the Job Scheduler provides the processed data to the Real Time Estimator service, which computes the crowding level in real time. Subsequently, in a daily window, it provides the necessary data for the remaining services, allowing to extrapolate, via the Daily Report Generator, the statistics of the entire monitored day. These services are implemented with machine learning algorithms (in particular, unsupervised clustering and statistical analysis) that perform complex data analytics tasks to extract mobility information from the raw data collected by the *DataNodes*. More details are provided in [10–12]. All the statistics produced by this block are stored in a MongoDB storage system.
- **Data Visualization:** this block includes the front-end, sensor manager and user manager services. The sensor manager and user manager services allow to configure and manage the access to the *DataNodes* and to the cloud platform, respectively. The front-end consists in a cloud web-service that permits the administrators as well as the end-users to visualize the data statistics generated by the Data Transformation block. In Fig. 3, we show an example of management dashboard that provides graphs and statistics resulting from the analyzed data. The end-user (e.g., a public administration) can view in real-time the level of crowding with a heatmap and the trend of the number of people selecting the preferred time window. Additional statistics can be also produced and provided in the form of a PDF report.

The crowding information resulting from the monitoring and data analysis processes are computed every 15 minutes and are stored as a time series data type in a BSON document of the MongoDB storage system. An example of a single record is shown in the Listing 1. Each document contains the following information: *id* of the BSON, *ownerid* to identify the proprietary company, *stationid* and *stationname* to identify the

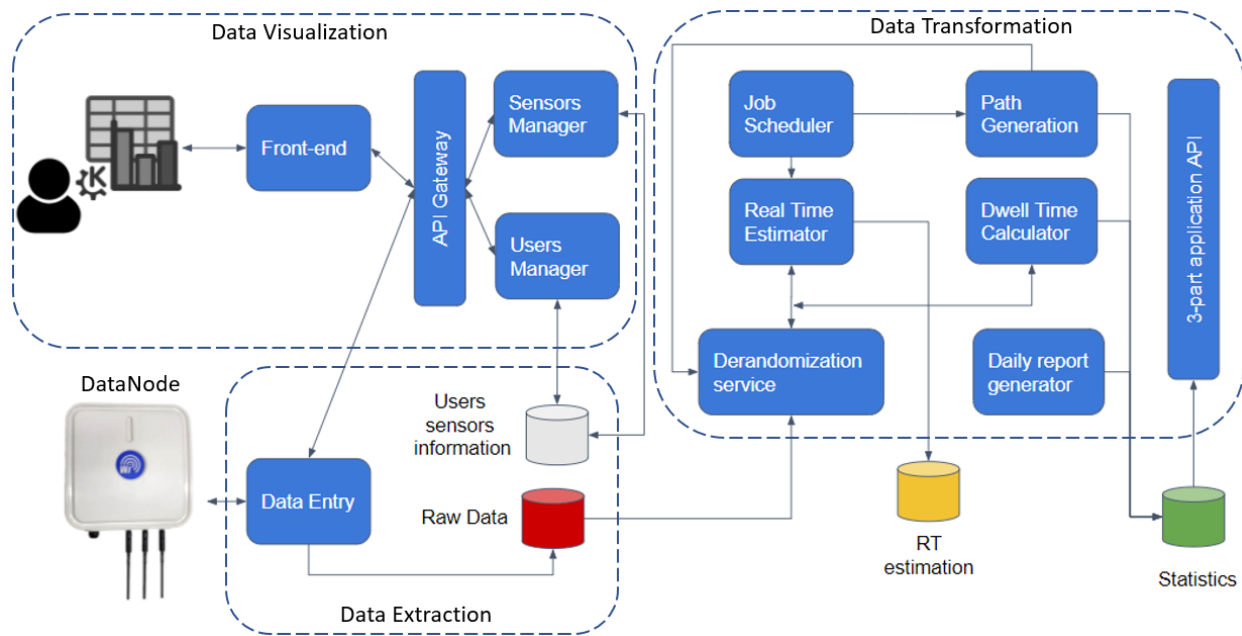


Fig. 2. PMA Architecture.

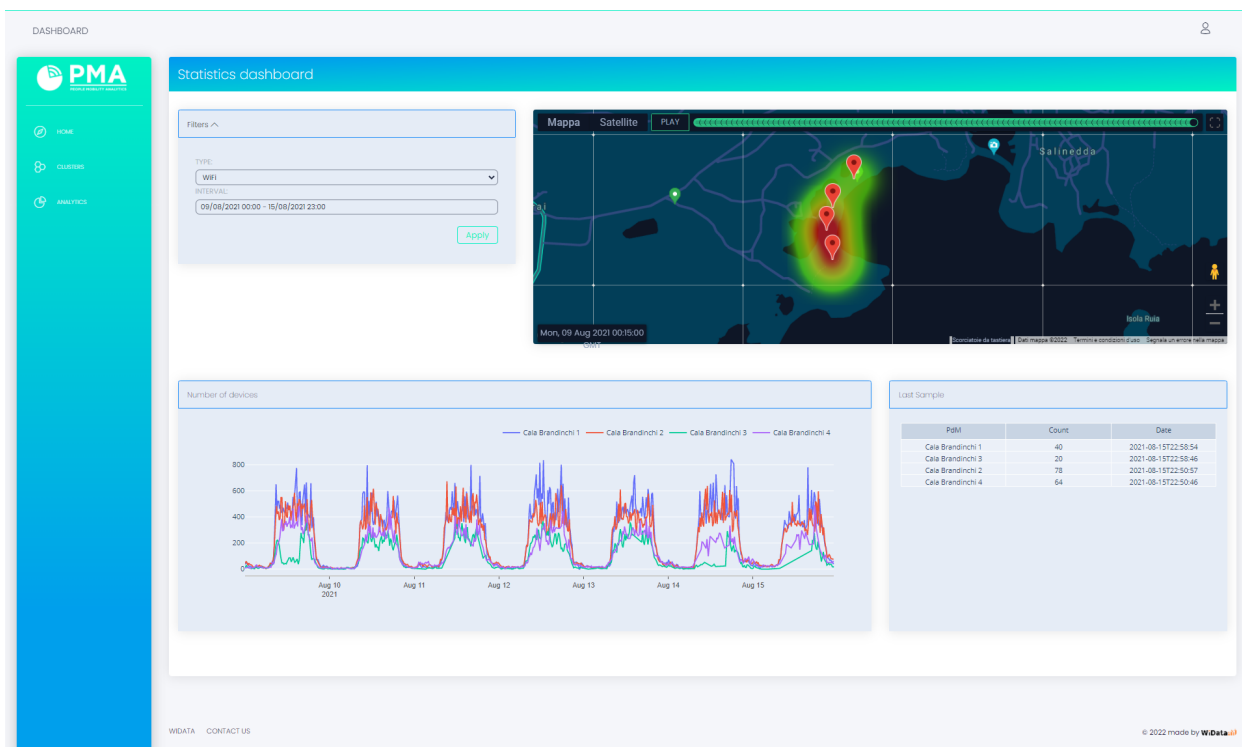


Fig. 3. Example of PMA Dashboard.

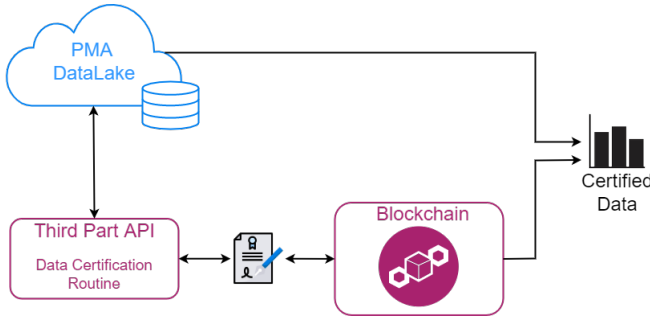


Fig. 4. Data certification framework.

DataNode collecting the data, *timestamp* to collect temporal information, *countvalue* containing the number of devices (people) counted in the proximity of the DataNode, and *crowdnesspercentage* that estimates the level of crowdness in the monitored area based on the number of monitored people compared with the expected number of people in that area.

```

1 {
2   "_id": {
3     "$oid": "60b8ab9f421de3fa3d339479"
4   },
5   "owner_id": "my-owner-id",
6   "station_id": "datanode-id",
7   "station_name": "datanode-name",
8   "timestamp": 1620915543.831004,
9   "count_value": 4,
10  "crowdness_percentage": 0.5,
11 }
  
```

Listing 1. Crowd information

B. Data notarization system

In this section, we describe the proposed Data notarization system aimed at certifying the data produced by the PMA system using Blockchain-based services.

In Fig. 4, we show the data certification framework that describes the process implemented to certify the collected data using the Blockchain. The API layer of the PMA system allows third party services to easily interface with our system via APIs. In particular, a Data Certification Routine (DCR) has been implemented to run specific APIs that prepare the data for certification. When the DCR is called, the PMA server is requested to process and collect the crowding data to be certified. The crowding information is that described in the Listing 1 whereas the monitoring period can be specified through the DCR options and can refer to single monitoring (information collected during the previous 15 minutes), daily monitoring (overall information collected during the previous day) or monthly monitoring (summary of crowding information observed during the previous month). These data is provided as a BSON document.

The details of the notarization application are shown in Fig. 5. The notarization application must be able to periodically

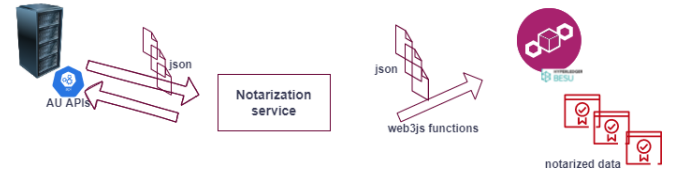


Fig. 5. Notarization application.

access the crowding data via the provided PMA API. The API call returns a JSON collection. The hashes of the obtained JSON are stored on blockchain and are closely related to a specific batch/real time measurements. If the number of measurements or files to be notarized is too high to perform an individual hash recording, through the use of an offchain part it will be possible to record the list of all certified files in an index file, and their respective hashes. The hash of this index file will then be calculated, in turn then recorded in the Blockchain through a transaction. Then, the notarization application sends the corresponding transactions to the related smart contract. Within the smart contract it is possible to decide whether to collect data based on the wallet/device/application that sends the transaction. A friendly front-end (GUI) that allows to browse the history of the transactions carried out is also provided. Regarding the system implementation, it will be used in Solidity, a Turing complete language, in order to properly develop the smart contracts in charge for data/file notarization. Node.js and Web3.js are respectively used for the execution of scripts related to Smart contracts and because it provides the APIs to communicate with EthernZero blockchain, which is the blockchain we decided to implement for the notarization service.

The proposed notarization service architecture is shown in Fig. 6. It is independent of the used Blockchain and is able to send both real-time and batch data, collected by the IoT application, to the Blockchain to ensure data integrity and immutability. Also, it includes an explorer for the navigation of the data notarized on the blockchain. The methodology used for the blockchain system design is the ABCDE methodology (Agile Block-Chain DApp Engineering), which was developed at the Department of Mathematics and Computer Science of the University of Cagliari [13]. The ABCDE methodology is an 8 steps software development process that provides the instructions from the requirements elicitation to the release, passing through the design and integration of different parts.

The proposed PMA system potentially requires massive use of the Blockchain for notarization and management of IoT devices data. For this reason, a permissioned Blockchain is certainly the most suitable choice. The periodic anchoring of the hash to the last validated block in the permissioned Blockchain within a public Blockchain also guarantees an inalterability of the data equal to that of a public Blockchain. The used Blockchain is a platform which makes the use of Blockchain technology simple and transparent for any application and process integration, thanks to its interfacing

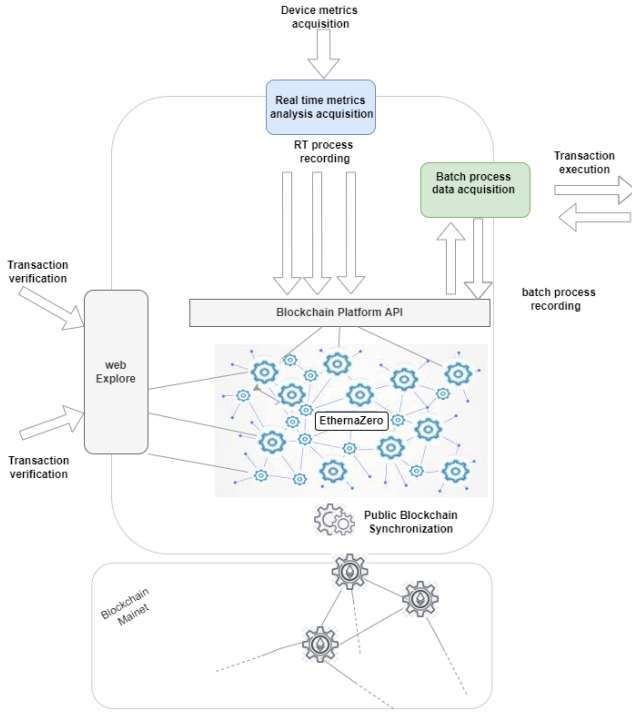


Fig. 6. Notarization service Architecture.

with its SideChain and the public Blockchains of Bitcoin, Ethereum and Litecoin.

The reasons that guided toward Ethernazero are manifold: it has no usage costs (gas consuming), i.e., the transactions do not consume gas and therefore lends itself to be well used for smart contract testing and the system under development testing. Ethernazero is a Hyperledger Besu Blockchain, consisting of 5 validating nodes. Hyperledger Besu is a platform for the development and distribution of blockchain projects based on Ethereum (Solidity language) compliant with the development languages of the Hyperledger universe (e.g., JavaScript, Java, etc.). It must be considered that BESU uses a type of proof of authority (IBTF2) consent with mining every 2 seconds and a capacity of about 500 transactions per second. It is an open Blockchain, and this means that transactions made by any type of compatible Ethereum wallet are accepted. It is important to highlight that it is possible to carry out transactions via API (using JSON RPC technology) and via batch of transactions at a defined frequency (hourly, daily, etc.) by reading the data periodically from pre-established databases or with data arriving in real time from the devices and therefore a realistic transaction can be carried out at the exact moment of the actual measurement: at the moment with Ethernazero it would be possible because it is a blockchain that does not provide for the consumption of gas to carry out the transaction otherwise it could be taken into consideration only in the case in where there was actually an appropriate amount of cryptocurrency in the wallet.

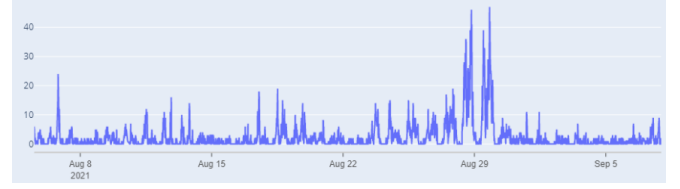


Fig. 7. Monitored number of people during the month of August.



Fig. 8. Monitored number of people during the event period from the 27th to the 29th of August.

IV. THE CASE STUDY

In this section, we describe the case study considered to test the proposed system. The objective was to monitor the number of people participating to a literary event and their dwell time to the event. To this end, we installed a DataNode within the open public place where the event took place, which was the courtyard of a historical building. The DataNode was connected to the CPE (Customer Premises Equipment) of a local MNO (Mobile Network Operator) so as to be able to transmit the collected data to the Cloud platform. The event was held between the 27th and 29th of August, but we decided to collect the data for a full month, from the 6th of August to the 6th of September, so as to compare the difference between the data analyzed during normal days with that analyzed during the event days.

Fig. 7 shows the observed number of people during the full month of monitoring. The weeks before the event the time slots 10 – 13 and 17 – 20 were those with the largest influx of people. However, it is evident the increment of the number of people (about 400%) measured by the PMA system during the event period. Fig. 8 shows in detail the number of people monitored during the event period from the 27th to the 29th of August. The 27th was the less frequented of the event days. Moreover, as it can be seen in Figs. 9-10, the peak of the number of people was registered the 28th and 29th of August counting 46 and 47 people, respectively. From these figures it can also be noticed how the trend is similar for these two days, increasing from 9 in the morning and decreasing after 13, then increasing after 15 and decreasing at the end of the event around 21.

The histograms in Figs. 11-13 show the number of people joining (blue bars) and leaving (red bars) the monitored area during the period event. Thanks to this information it is possible to understand how people join and leave the event, which is of utmost importance to organize similar events in the future. Finally, the histograms in Figs. 14-16 show the dwell time (in minutes) for the number of people monitored during



Fig. 9. Number of people monitored on the 28th of August.



Fig. 10. Number of people monitored on the 29th of August.

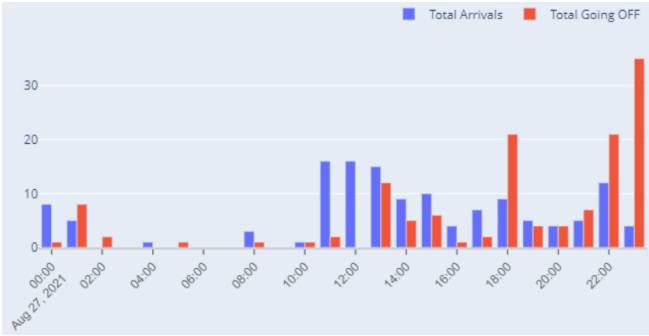


Fig. 11. Number of arrivals and outputs monitored on the 27th of August.

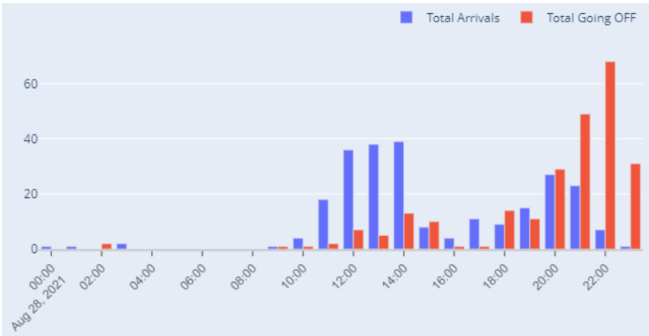


Fig. 12. Number of arrivals and outputs monitored on the 28th of August.

the period event. The dwell time measures the time people stayed at specific places, and in this case at the literary event. The first day of the event, the 37% of people remained around 100 minutes whereas the 19% remained around 200 minutes. The rest of dwell times (from 300 to 700 minutes) are around 10%. The situation is different for the next 2 days, where about the 20% of people remained for 50 minutes while a little more than 10% of people remained for a dwell time of 100-150 minutes. Percentages lower than 10% were obtained for dwell times longer than 150 minutes. Again, this information is very useful to analyze the behaviour of the people and to

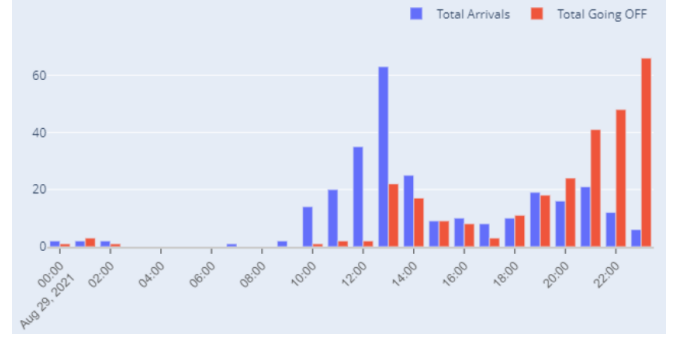


Fig. 13. Number of arrivals and outputs monitored on the 29th of August.

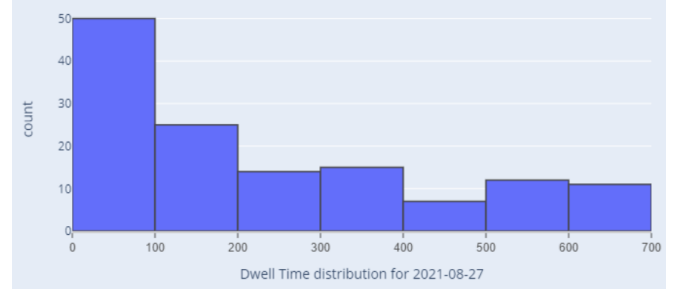


Fig. 14. Dwell time (in minutes) for the number of people monitored the 27th of August.

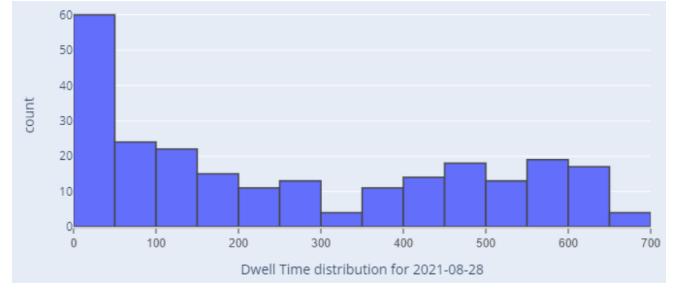


Fig. 15. Dwell time (in minutes) for the number of people monitored on the 28th of August.

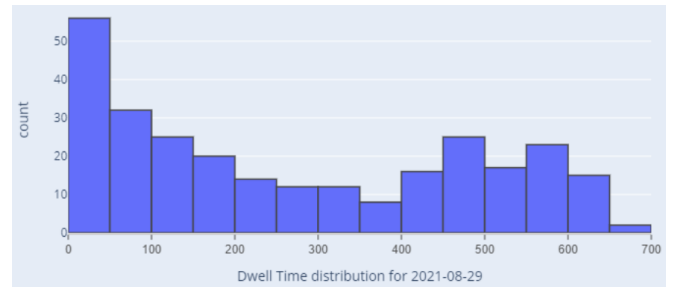


Fig. 16. Dwell time (in minutes) for the number of people monitored on the 29th of August.

better understand how to properly organize similar events in the future.

We used the proposed data notarization system described in Section III-B to deploy the smart contracts on the EthernZero

blockchain. We set up the notarization application to update the crowding information collected by the PMA system on a daily basis. Specifically, each daily BSON contained summary information for each event day, regarding number of people, number of arrivals and outputs, and dwell time, registered every hour of the monitored days. The data registered on the EthernZero blockchain was navigable from the implemented explorer service.

V. CONCLUSION

The adoption of Blockchain technology with IoT applications provides important features, such as decentralized validation of transactions as well as immutability and traceability of the transactions. In this paper, we proposed a Blockchain-based data notarization system for mobility services. First, we presented an IoT-based crowd monitoring system aimed at counting the number of people in a specific area and providing information regarding people mobility and dwell time. Then, we discuss our proposed data notarization system focused on ensuring data integrity and immutability of the mobility data collected by the crowd monitoring system, regardless of the used Blockchain.

To test the proposed system, we monitored the crowd information regarding people participation during a literary event. The implemented IoT-based systems provided important information concerning people mobility that could be used to properly plan similar future events. Compared with alternative methods (e.g., face recognition with cameras), our method preserves the privacy of people since it is based on Wi-Fi probes sniffing (anonymous MAC addresses) and also applies hashing algorithms to further guarantee the privacy. Moreover, the proposed data notarization systems, implemented using the EthernZero blockchain, validates and makes immutable the data collected by the IoT system so as to enable the presentation of this data even to public administrations and government authorities. In future works, we aim to test our proposed system with further case studies and then analyse the quality code with metrics as argued in [14].

REFERENCES

- [1] L. Atzori, A. Iera, and G. Morabito. "The Internet of Things: A survey". In: *Computer Networks* 54.15 (2010), pp. 2787–2805.
- [2] H.-N. Dai, Z. Zheng, and Y. Zhang. "Blockchain for Internet of Things: A Survey". In: *IEEE Internet of Things Journal* 6.5 (2019), pp. 8076–8094.
- [3] R. Tonelli et al. "Ethereum smart contracts as blockchain-oriented microservices". In: *Proceedings of the 19th International Conference on Agile Software Development: Companion*. 2018, pp. 1–2.
- [4] R. Galici et al. "Applying the etl process to blockchain data. prospect and findings". In: *Information* 11.4 (2020), p. 204.
- [5] S. Huh, S. Cho, and S. Kim. "Managing IoT devices using blockchain platform". In: *2017 19th international conference on advanced communication technology (ICACT)*. IEEE. 2017, pp. 464–467.
- [6] A.-S. Kleinaki et al. "A blockchain-based notarization service for biomedical knowledge retrieval". In: *Computational and structural biotechnology journal* 16 (2018), pp. 288–297.
- [7] H. Magrahi et al. "NFB: a protocol for notarizing files over the blockchain". In: *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE. 2018, pp. 1–4.
- [8] K. Rantos et al. "ADvoCATE: a consent management platform for personal data processing in the IoT using blockchain technology". In: *International Conference on Security for Information Technology and Communications*. Springer. 2018, pp. 300–313.
- [9] M. Marchesi et al. "Crypto-Trading. Rechargeable Token-Based Smart Energy Market Enabled by Blockchain and IoT Technology". In: *European Conference on Parallel Processing*. Springer. 2019, pp. 166–178.
- [10] M. Uras, R. Cossu, and L. Atzori. "PmA: a solution for people mobility monitoring and analysis based on WiFi probes". In: *2019 4th International Conference on Smart and Sustainable Technologies (SpliTech)*. 2019, pp. 1–6.
- [11] M. Uras et al. "PmA: A real-world system for people mobility monitoring and analysis based on Wi-Fi probes". In: *Journal of Cleaner Production* 270 (2020), p. 122084.
- [12] M. Uras et al. "WiFi Probes sniffing: an Artificial Intelligence based approach for MAC addresses de-randomization". In: *2020 IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. 2020, pp. 1–6.
- [13] L. Marchesi, M. Marchesi, and R. Tonelli. "ABCDE—agile block chain DApp engineering". In: *Blockchain: Research and Applications* 1.1 (2020), p. 100002.
- [14] M. Ortu, M. Orrú, and G. Destefanis. "On comparing software quality metrics of traditional vs blockchain-oriented software: An empirical study". In: *2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*. IEEE. 2019, pp. 32–37.