DIVAIRCITY

The power of Diversity & Inclusion for Climate Neutral Cities

Specifications of MSCCP and SCCCPs - Version 1

Deliverable 5.2 - Public

Lead beneficiary: CFH

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101003799

History of Changes

Version	Date	Authors	Sign off by
v1.0	20/06/2022	CFH, Blockchain Intelligence, AUTH, DTI	
V1.1	28/06/2022	AUTH	
V2.0	29/06/2022	AUTH	

List of Acronyms

Acronym	Meaning
API	Application Programming Interface
AQ	Air Quality
BaaS	Blockchain as a Service
BC	Blockchain
BFT	Byzantine Fault Tolerance
D	Deliverable
dApp	Decentralized Application
DI/DW	Digital Identity/Digital Wallet
DLT	Distributed Ledger Technology
EU	European Union
EUID	European Union Digital Wallet
GDPR	General Data Protection Regulation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identity
IDE	Integrated Development Environment
IdP	Identity Provider
IoT	Internet of Things
IPFS	Inter Planetary File System
LoRaWAN	Long Range Wide Area Network
LPWAN	Low power Wide Area Network
M	Month
NBS	Nature-based Solution
pBFT	Practical-Byzantine Fault Tolerance
PII	Personally Identifiable Information
PoA	Proof of Authority
PoS	Proof of Stake

PoW	Proof of Work
SP	Service Provider
SQL	Structured Query Language
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol / Internet Protocol
UI	User Interface
W3C	World Wide Web Consortium
WP	Work Package

Glossary

Acronym	Meaning
Application	The User Interface of the MSCCP.
Attestation	Evidence or proof, in this case in electronic form and delivered through the European Digital Identity Wallet (EDIW).
Attestation provider	Public or private sector body providing evidence of attributes and eligibility. These could include transport departments, health boards, insurance companies, employers and universities.
Attributes	Personal details, which a Relying Party may need to verify in order to provide their service; for example age, address, nationality, permits and licences.
Authentication	A “one-to-one” verification of a specific person’s identity. It compares specific attributes (PIN code, biometric information etc.) with reference data already stored in a system
Blockchain Platform	The BC to be used, e.g., Ethereum, Quorum, Hyperledger, EBSI.
Developer	Technical staff that works on the development and maintenance of the application.
Digital ID (DID)	Digital Identity is the twin of the identity of a person but in the electronic world.
Digital Wallet	Digital Wallet is the twin of the physical but in the electronic world.
EDIW	European Digital Identity Wallet is a service that allows the user to store identity data, credentials and attributes, to use them for authentication on and offline, and to create qualified electronic signatures and seals.
eIDAS	The EU Regulation on Electronic Identification and Trust Services. The original eIDAS regulation (eIDAS1) was implemented in 2014, while a new, significantly strengthened version (eIDAS2) is due for implementation in September 2023.

Identification	**The action or process of collecting and verifying information to represent unambiguously a natural or legal person**
Issuer	**The Authority that issues the credentials of the users.**
Level of Assurance	**Under the eIDAS regulation the term "level of assurance" refers to the degree of confidence in the claimed identity of a person**
Public and Private Relying Parties	**Public sector bodies and businesses whose services are required to use strong user authentication, and who will be required to accept the EDIW as proof of identity and attributes.**
MSCCP	**Main Smart Cities Contract Platform. Here, it stands for the overall system.**
SCCCP	**Smart City Climate Contract Platform. It is part of the MSCCP.**
Smart Contract	**Software programs which are executed when specified conditions are met.**
SSI	**Self-Sovereign Identity. A form of distributed digital identity.**
Tokenomics	**The ecosystem of the system rewarding mechanism including all potential transactions with the DivAirCity tokens**
User	**The user of the application, citizen and member of the diversity groups.**

Table of Contents

1 Introduction

1.1 Context of 5.2 within WP5

The Deliverable 5.2 within WP5 builds on Deliverable 5.1 and prepares the groundwork for the later deliverables in WP5 (the development of the DivAirCity Blockchain application). Deliverable 5.1 established the high-level requirements for the blockchain-based application(s) which are to be developed in 5.3, 5.4. and 5.5.

The Deliverable 5.2 aims to further specify the functionalities and technical requirements, which are then implemented in the development of the DivAirCity Blockchain application by M40 of the project. Next Deliverables in this WP are D5.3 which is a milestone representing the Smart City Contract(s), D5.4 the dApps Marketplace and D5.5 the federated data system, to be finalised in M44.

It should be noted that version 1 of D5.2 (this document) will be updated in M40, to reflect the project progress and to integrate the outcomes of the co-creation activities in the cities. Therefore, the content of this document should be understood as reflecting the current state of the project activities in the whole consortium, especially with regards to the needs of the citizens, the needs of the cities and the data framework established in the other WP.

1.2 SCCPs and MSCCP

This Deliverable 5.2 will define the specifications of the five Smart City Climate Contract Platforms (SCCCPs) for the 5 cities. The 5 systems are expected to have several sub-systems in common, while all of them are constituting the Main Smart City Contract Platform (MSCCP).

For example, all the SCCCPs will support any Air Quality (AQ) sensors placed in houses, cars, bicycles, backpacks as a result of the DivAirCity project. Through the SCCCPs and the developed decentralized applications (dApps) the citizens will be rewarded for providing their input. Moreover, the SCCCPs will support citizens' properly designed input, like route tracing, behaviour changes etc so as to get the relevant rewards. SCCCPs will also include custom functionalities, addressing each city's needs, as they have been identified in the city DNAs.

The SCCCPs will include the selection and further development of the blockchain (BC) basic infrastructure and the development of the Smart Contracts and Tokenization Model.

1.3 Data

The data to be handled in 5.2 according to the application can be defined, but not exclusively as follows:

- **Citizens' locations and routes so as to allow the implementation of effective nature-based solutions (NBS) by the cities**
- **Citizens' use of green means of transport,**
- **Citizens' provided input of AQ sensors, steady or mobile in their possession, to allow the cities to implement and sustain efficient NBS,**
- **Citizens' visions, ideas, suggestions, etc to create a novel participatory communication approach.**

However, in the discussion of the data framework in WP2, it became clear that the data needed by the cities are more complex than the four categories imply. Therefore, as part of 5.2, we suggest conceptualising the following data layers:

Data	Storage
Personal Data such as Name, Address, Location Routes, Citizens' use of green means of transport	Locally and securely stored by the user
Encrypted personal data to interact with the BC	Locally stored in the digital identity wallet
AQ Data and other non-personal data, survey results from interactions with citizens	Centrally and securely stored as anonymized data in databases out of the BC
Data related to the tokens received and spent, smart contracts and the corresponding transactions	Decentrally stored in the blockchain

2 Background and State of the Art

2.1 Blockchain Technology and Smart Contracts

Distributed Ledger Technology (DLT), like BC, is the technology which allows the decentralized file storage of transactions, data and other information. This technology is rapidly evolving around the world, creating inexhaustible opportunities in many different areas, as well as security models for recorded information. The term DLT is a general term used to describe a technology that distributes files or information, either privately or publicly, thus creating a digital copy of the same data across multiple sites. By nature, this technology can result in significant reduction in the amount of money and time spent for the transactions, as it removes intermediaries and promotes efficiency through decentralization.

BC is a type of database where data is stored in blocks which are connected building a chain. Each block can contain any kind of data type cryptographically transformed into a hash. The block is introduced into the chain of blocks and it incorporates also the hash corresponding to the previous block. This procedure ensures that the data corresponding to each block will not be altered, as this would need the modification of all the corresponding hashes. By this way and based on the distributed nature of the BC, data can only be appended to the BC and not be removed or altered.

BC technology can be used for multiple applications, incorporating the so-called smart contracts. A smart contract comprises computational code which can be uploaded into a BC network. It can be used for executing different operations, providing the ability to two or more interested parties to agree on decisions or exchange information and data autonomously, without needing for intermediaries. Every smart contract execution leads to a transaction and information regarding this transaction can be then stored into the distributed ledger, in an immutable manner. By this way, the development of dApps can be supported and the variety of BC applications has been widely broaden. A dApp has its backend run distributed and not in a specific server. A programming language out of a great variety can be used for writing a dApp frontend and the corresponding user interface. Even though the maintenance of such an application is more challenging, it is better from a privacy, runtime and trustless computation perspective.

2.2 Consensus Mechanisms

The consensus algorithm constitutes the agreement procedure that the nodes follow in order to validate a transaction and add it to the BC. In this way, the trusted third party of traditional centralized systems is eliminated, making consensus the most important part of the BC execution. Proof of Work (PoW), Proof of Stake (PoS) and Proof of Authority (PoA) are the most known and used consensus mechanisms.

PoW is the first proposed consensus mechanism and it is the backbone of Bitcoin BC. The protocol relies its integrity on solving a cryptographic puzzle in order to validate a new transaction. The robustness of the network is achieved as long as the majority of the computational power is distributed among honest nodes regardless their number. It is ensured that the users are not malicious, and the data stored in the BC is consistent. Regardless it is considered secure, it is also expensive in terms of power consumption, since the network nodes who compete with each other to solve the cryptographic puzzle, must use massive computing power for this task. This is called 'mining' and the first node to solve the cryptographic puzzle gets the mining reward. PoW is based on the idea that the user who has solved a computationally intensive problem first, adds a new block on the chain. Once the puzzle is resolved and the new valid block is created, approval from the 51% of the nodes is required in order for the block to be added to the chain. Otherwise, the block is rejected, and the miner is not remunerated. In this way, malicious attacks, i.e., effort to insert a false transaction, are not approved. Users competing for the insertion of new blocks are called 'miners'. Anyone can be a network node and can run the consensus algorithm and compete for new blocks insertion, given the existence of computational strength. It is obvious that the probability of validating a block depends on the available computational power. Although this scheme is extremely good in the protection of the BC security from any cyberattack, it is a time- and energy- consuming process. Therefore, the speed of the BC, defined as transactions per second, is low in the systems which use this consensus scheme

PoS is a mechanism, alternative to PoW, which use validators instead of miners to update the blocks. It is based on the idea that the creator of the new block is chosen depending on its wealth, i.e., digital currency, namely stake. This leads to a more centralized BC where wealth is concentrated to specific nodes, comparing to PoW. It can be deduced that the probability of malicious attacks reduces when the stake is large, supposing that the nodes with big stakes will not cheat, for not risking losing their stakes. The stake increases from transaction fees and not from the rewarding of adding a new block. Additionally, the stake increases, and consequently the probability of becoming block creator, when the node is exposed to cryptocurrency. To add new blocks to the BC, the validator is chosen among participants with significant stake on a pseudorandom basis, analyzing several factors. One of the weaknesses of PoS is security. While the PoS uses significantly less computational resources than PoW, it may have an issue that the nodes who have large proportion of stakes are more likely to become the validators of the blocks and this may manipulate the consensus mechanism.

In PoA the consensus is reached by a group of known and reputable nodes, authorized to validate transactions and add new blocks to the BC. It is deduced that not anyone can be a validator and being a validator presupposes that the identity is known. As the validators' identity is known, assuring trustfulness, their work does not have to be controlled and verified by the other nodes. Thus, consensus algorithm

does not ensure trust. As a consequence, the execution time and cost are reduced leading in simpler and faster algorithms. Nevertheless, the initial principle of the non-existence of a central authority is not totally followed. The most known algorithm is the practical-Byzantine Fault Tolerance (pBFT). PBFT is characterized by low complexity and high practicality in distributed systems. The consensus of 2/3 of the network is needed for the block to be validated.

Overall, the selection or the design of a proper consensus scheme is an open challenge in BC research. The selection of the consensus mechanism should be based on the specific operational characteristics of the application and must be the best compromise between efficiency, both in terms of energy consumption and BC performance speed, and robustness against potential malicious attacks.

2.3 Blockchain Platforms

The BC technology has already been adopted for several different applications, both in the academia and in the public and private sector. Here, the most popular and suitable ones for the application to be developed in the framework of DivAirCity project are briefly presented. In the technologies analyzed, the transactions are carried out for free, smart contracts and dApps can be created, while the tokenization procedure can be built according to the needs of the specific application.

2.3.1 Hyperledger Fabric

Hyperledger Fabric (https://www.hyperledger.org/use/fabric) is a platform backed by the Linux Foundation and IBM among others, suitable for developing private permissioned BC applications. It supports pluggable consensus mechanisms to adapt to the specific application requirements. When compared to other BC protocols, its architecture is based on a novel execute (endorse) – order – validate paradigm. Specifically, a transaction is executed and checked for its correctness, i.e., it is endorsed, a meaning corresponding to the transaction validation procedure in other BC platforms. Afterwards, the ordering through a consensus protocol follows, which is irrespective of the transaction semantics, and the transaction validation per application-specific trust assumptions. The permissioned nature of the platform is maintained through the cryptographic identities, which are associated with peers by a modular service provider. A stand-alone certificate authority is provided, called Fabric-CA. However, alternatives are supported, such as the one relying on anonymous credentials, i.e., without linking to an identity. Hyperledger Fabric allows the execution of dApps written in standard programming languages, which can be executed consistently among many nodes. Moreover, smart contracts are supported, called chaincode, written within a Docker container environment for isolation and in standard programming languages like Go and Javascript; however, they have not

direct access to the ledger state. Hyperledger Fabric provides Turing-Complete smart contracts and halting is avoided using an upper bound on the execution times, after which the execution is halted. For the correct execution of the smart contracts, there are endorsement policy specifications, to allow the parallel execution and increase the overall performance and scaling of the system. On the top of that, Hyperledger Fabric enables privacy through its channel architecture. Only the interested peers shall gain access to the data of a specified transaction. For testing the right way of executions, there is no need to use the nodes of the network, in order to avoid deliberately change in their state. Finally, Hyperledger Fabric incorporates the ERC20 token standard; thus, providing backwards compatibility with platforms like Ethereum.

2.3.2 Hyperledger Besu

Under the umbrella of Hyperledger leans also the Hyperledger Besu infrastructure (https://www.hyperledger.org/use/besu), an Ethereum client written in Java and suitable both for public and for private use cases. As an Ethereum client it is composed of (i) execution environment for processing transactions in the Ethereum BC, (ii) storage for data related to transactions, (iii) tools for peer-to-peer networking among other Ethereum nodes, and (iv) possible interaction with the Ethereum BC via Application Programming Interfaces (APIs). To become suitable for both public and private applications, it can work with several consensus algorithms, including PoW and PoA. In the core of Hyperledger Besu lie the transaction processor and the block validator, to help the Ethereum Virtual Machine run more efficiently, the transaction pool responsible for storing information related to transactions, and the synchronizer to facilitate the synchronization between the nodes and the network. Hyperledger Besu enables modularity via plugins, existing or built by the users via Plugin API. There are two types of nodes, i.e., full nodes and archive nodes, where archive nodes require much more disk space than full nodes. As in Hyperledger Fabric, the private transactions between involved participants can also be supported. Hypeledger Besu does not support key management inside the client. Instead EthSigner or third-party tools, such as MetaMask and Web3j, can be used. The dApps development is also supported using Truffle or client libraries.

2.3.3 Quorum

ConsenSys Quorum (https://consensys.net/quorum/) is an Ethereum-based permissioned platform, with no public option. It leverages Ethereum for high-value applications. It supports plug-and-play consensus algorithm in order to adapt to the specific application requirements. Each main Quorum node consists of two main services, i.e., the Quorum client, responsible for executing the Ethereum peer-to-peer protocol by accepting connections only from participants to the permissioned

network and the consensus algorithm, and the privacy manager, a software module enabling private transactions and smart contract operations. Every node in Quorum is responsible for validating transactions, either the ones being known to everyone in the network, or the ones that they are allowed to, by executing the contract code associated with the transactions. This means that similarly to Hyperledger Fabric and Hyperledger Besu, Quorum can also support private transactions between certain network participants. As in PoA consensus mechanisms that are also among the supported ones for the Quorum platform, the blocks are validated by an a priori selected group of authorities, which means that any misbehavior can be detected, while malicious nodes can be voted out of the consensus procedures. Finally, the smart contracts in Quorum are written in Solidity, as in the Ethereum BC.

2.3.4 EBSI

EBSI (https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home) stands for European Blockchain Services Infrastructure, born in 2018. Currently, it has 25 live nodes, 11 in setup phase. It comprises a peer-to-peer network of interconnected nodes operated by Member States' authorities at a national level, coordinated by the European Blockchain Partnership (EBP). EBSI is designed based on standards and a transparent governance model, following five key principles, i.e., (i) public good, (ii) governance, (iii) harmonization, (iv) open-source infrastructures, and (v) EU regulations compliance. Its architecture is composed of three layers, namely the infrastructure one, which provides generic capabilities and connectivity to BC networks, the chain and storage one, both for on- and off- chain storage, and the core services and set of standardized interfaces (APIs), which are useful for application development, while ensuring compliance with principles set by the EBP. EBSI can be employed by public administrations, businesses and citizens, for fraud avoidance, effortless interaction with minimum administrative and compliance costs, and for secure data management. It is also suitable for cross-border services, related for example to identity management and educational credentials. This protocol is suitable for permissioned applications, while the PoA is the used consensus mechanism, where the validation is executed by approved accounts/nodes. Finally, smart contracts are supported.

The European Blockchain Service Infrastructure should be specifically considered as one of the DLT infrastructures to be used to build the DivAirCity application. Built under the auspices of the EU institutions, EBSI´s aim is to provide use cases with a solid decentralised, energy and cost-efficient DLT under EU legislation. EBSI nodes are owned by public administrations, and it is currently supporting public-private cross-border cases. DivAirCity is following its development under the possibility of applying for the early adopters programme.

2.4 Desk research on existing applications

Based on the references of D5.1 a review on the technical approach has been performed. The BC technology adopted, the Internet of Things (IoT) interaction and the rewarding approach have been identified.

Ethereum is the BC platform used in [1] and [2]. [1] builds a peer-to-peer transactive energy system for community microgrid with demand response management. The verification of the data transmission and the safety of the ledger are ensured by the BC network. The users interact directly with the BC network through a communication channel. The architecture consists of three layers, i.e., physical layer, smart meter layer, and BC layer. The smart meter establishes connectivity between the physical layer and the BC layer. The BC layer contains a smart contract that receives bids from buyers and offers from sellers. The smart contract calculates the market-clearing price and the quantities of the respective market time interval using double auction and publishes it. The transaction is carried out at the end of each market time interval.

Hyperledger has been also widely used in the development of BC applications [3] – [7]. In the first case, a solution to meet the need for monitoring the health in the working environment in real-time is proposed. Once a monitoring device is installed, it begins to collect data, detecting any high levels of harmful gases, suspended particles, odors, and noise, which may be harmful to the employees. Any anomaly or alert is stored in the device along with the time and date, ensuring that this data has not been altered. In addition, this process checks and certifies that the data conforms to the most demanding regulations. Hyperledger Besu has been employed via the Alastria (https://alastria.io/en/) network for the certification and the protection of the data collected. Calibration and Data Quality Certificates for IoT devices are kept in the BC. A smart contract is generated and stored in the device, certifying that the device has been verified and calibrated by a suitable laboratory.

Hyperledger Indy (https://www.hyperledger.org/use/hyperledger-indy) has been deployed for the creation of a Digital Identity/Digital Wallet (DI/DW) system to be used by immigrants [4]. Since a lot of immigrants have no personal papers, their assigned identities, together with any official qualification are stored in digital wallets and can be used where needed. To verify or authenticate a user, Tykn API automatically check the BC to confirm the authenticity of the user's credentials. Therefore, verifiable Credentials are available anywhere, at any time, without the need to communicate with the issuer, as they are only stored in the users' digital Wallets. Only the public cryptographic signature of the organisation who issued a credential is stored on the BC and not any personal identifiable information. This signature is instantly checked to verify that the source of the credential and its authenticity are trustful, and the credential has not been revoked.

Hyperledger Fabric is used in a wide range of applications [5] – [7]. In [5] there are two different actors, i.e., the actor and the medical center. The medical center submits information about the threats affecting their infrastructure in JSON format and as it is, it is stored in the BC. In an external database additional information is stored. The hash of this information also passes through the BC to ensure its integrity. Two certified nodes are considered per medical center. The actors act as BC users communicating with a BaaS (Blockchain as a Service) through an API node. Hyperledger Fabric is the BC technology, BaaS is employed, while the Go programming language is used for the Smart Contracts. Docker has been used for deploying the different components of the BC network and different bash scripts have been developed to create, start, stop, restart and clean the network. The connection between the client application and the BC nodes are made using a secure API REST communication. Specifically, this is an Secure Sockets Layer (SSL) over Hypertext Transfer Protocol (HTTP) (Hypertext Transfer Protocol Secure - HTTPS). JSON format and MongoDB are also used in [6]. Crowdsourcing tools, tokens and wallets, a rewarding system, and a virtual marketplace, are implemented in order to twist plastic reuse practices by boosting citizens' awareness, circular economy practices, and sustainable innovation in line with the new plastics economy vision. Twitter's Streaming API has been used to collect all tweets containing any of the keywords defined. After making a call to Twitter Streaming API each response is in JSON format; each response is actually a single tweet, packed together with multiple type of information. Once a keyword is matched, the tweet is collected. The second part of filtering process has to do with the language of the tweet. For each of the languages, there is a different Mongo DB Database with five different collections, each one referring to a different group of keywords.

Algorand green BC is employed for providing a tool to allow the sensor owner to split rewards with a third party [8]. It is used for both storing data immutably and for tracking and rewarding all data streams. The aim is to collect, analyze and share air quality data, to monitor key parameters and to reward data providers.

The development of air quality, air pollution and environmental monitoring systems based on the combination of IoT and BC has been widely investigated also by researchers around the world. Air quality sensors are typically battery-operated devices, which need IoT infrastructure to execute computational tasks [9]. This means that in order to transmit the data obtained through them to the external world, for the identification of the devices and the validation of the data, they should be accompanied by IoT. The proposed solutions differentiate from each other with regards to, among others, the BC infrastructure employed, how the BC is used and to the adopted data flow scheme.

In [10], data sensors are used to monitor the air quality in smart cities. The sensors send their measurements to a data broker in the cloud, where specified users can have access to them, for several purposes, such as risk evaluation and risk alerting. To revoke data access to interested stakeholders, smart contracts in the BC are used,

which also implement rewarding schemes based on tokens. People providing measurements from their devices and those who want to access them, interact with each other via a cloud-based data streams exchange hub. This hub is managed by the overall smart monitoring project coordinator. The measurements can either be sent directly to the BC to be checked or stored, or the sensors used can store them temporarily for some time, as proposed in [11]. Afterwards, the data signed and encrypted can be sent to the blockchain nodes to be validated.

To decentralize the procedures of data retrieval from IoT sensors comprising a decentralized pollution monitoring system, a BC-based solution is proposed in [12], employing the Ethereum BC. Specifically, the Ethereum Light Client is used instead of the Ethereum full nodes, as it is a faster and a less memory consuming option. The communication between the sensor nodes and the network is established through the Long-Range Wide Area Network (LoRaWAN) communication protocol, in order to tackle the issue of long-range communications and high energy consumption. Data obtained from the IoT sensors is transferred to the BC either directly or through the LoRa network. Then, the data is stored to a local database to ensure the fast offline processing and quality checks. One of the data flows tested is the combination of LoRa gateways and BC, employing the NodeJS and Web3 API. A smart contract is used to ensure that the measurements initially obtained from the IoT sensors and stored into the BC have no violations.

The Ethereum BC is also used in [13] in order to store data received from air quality sensors. The data collected is stored, employing the InterPlanetary File System (IPFS), in order to avoid the huge cost of storing data directly to the BC. In this way, the data is stored in a distributed manner and only the hashes are incorporated into the BC. However, such a scheme to be effective, multiple IPFS nodes should be used to store the same data; thus, IPFS servers may be useful. For identification, uPort is used, while Infura allows dApps to interact with the Ethereum BC. The combination of Ethereum BC for the main infrastructure, IPFS protocol for the data storage and Infura for the dApps creation is adopted also in [14] to manage air quality data. A No – Structured Query Language (NoSQL) database is used, named Firebase. For the BC development, Ganache is employed, an open-source software. At first, the data is stored in the database centrally; then transferred to the IPFS nodes and a string/hash is created and sent to be stored in the BC in an immutable manner, i.e., the hashes corresponding to air quality sensors measurements are stored into the BC and not the whole data packages, in order to both assure the security and tamper proofness of the data, and to minimize the cost and memory usage which would be increased if on-chain data storage was chosen.

Except for the Ethereum BC, also the Hyperledger Fabric has gained great attention among the scientific community for air quality and pollution monitoring systems [9], [15], [16]. An extended version of docker-based Hyperledger Fabric images (version 1.4.1) supported by Golang v.1.11.5 and Docker v18.09.6 has been employed in [9]. Specifically, in order to reduce the time needed to execute the transactions, the BC

nodes used must be tuned based on the docker images. The BC nodes belong to various organizations, each one of which should have a copy of the ledger. The data obtained from the sensors, among which are both air quality data and metadata related to it, is validated regarding its authenticity and an ordering service then works in order to reach the final step of committing blocks to the ledger. The Hyperledger Fabric is also employed in [15], with each involved organization comprising a node, in order to build its own rules according to the needs and special characteristics. As far as the application is concerned, the data can also be saved locally in the devices. Through internet infrastructure and IoT services, the data obtained via environmental monitoring are sent to the BC clouds and when a batch is formed, the hashes that correspond to the data are sent for storage into the BC ledger. The data is retrieved and validated autonomously and then stored into InfluxDB, i.e., an open-source database accompanied by ready for the user HTTP endpoints and multiple tools, after being encrypted.

In [16], as only authorized consortium members are supposed to be allowed to operate validating nodes, the Hyperledger Fabric as a permissioned BC is also employed. In this work, only consortium members are full nodes, meaning that they store locally the ledger, to minimize the storage consumption. Data is supposed to be retrieved only from authorized users/ sensor nodes, i.e., from sensors that belong to people belonging to the consortium. The authorized sensors can be positioned in different areas for a certain time interval, and measurements are gathered for that time interval. After that, the obtained data is digitally signed, using a private key stored in encrypted storage, and broadcasted over a wireless network, Low Power Wide Area Network (LPWAN) technology, to surrounding gateways in order to reach the nodes of the distributed ledger, via Transmission Control Protocol/Internet Protocol (TCP/IP). The validity of the data signature is assessed via smart contracts running in the node of the distributed ledger. If the signature is valid, the transaction occurs, and the data is stored.

The above studied test cases, in which the BC technology is employed, will be thoroughly considered while designing the architecture of the MSCCP to be developed in the framework of the DivAirCity project. Special attention will be provided to those applications related to air quality assessment in cities, while others where the citizen partnership is included will be further exploited.

3 Scenarios of User Interaction and Tokenization

3.1 Overview

The following chapter outlines the interaction of the DivAirCity project citizens with the applications, the databases and the distributed BC-based ledger. It is important to mention that the actual tokenomics/rewarding system will be developed in the co-creation as part of WP3.

The term 'tokenomics' practically refers to the way an established rewarding system in the framework of the BC application works. The 'tokens' are the rewarding units and tokenomics is the process of earning tokens, keeping tokens, exchanging or trading tokens and eventually spending tokens.

Since, generally in the BC technology the term 'token' refers to some asset with a certain, stable or variable value, some further definitions are necessary to define how the DivAirCity tokenomics will function

- **The first definition is that there will be no fixed amount of tokens. The number of tokens for each city will be practically unlimited, under the control of the city authorities, avoiding therefore any possibility of manipulation of the DivAirCity tokenomics.**
- **The DivAirCity token will have no monetary value, e.g., they cannot be exchanged with money or any other asset of value. Therefore, they can be used only inside the DivAirCity marketplace and in the specific city limits.**
- **The DivAirCity tokens can be exchanged with certain 'benefits'. These benefits may, but not exclusively, include free access to municipality services, free use of the municipality assets (e.g., bicycles) etc.**
- **DivAirCity is open to private actors who can participate as sponsors in the DivAirCity rewarding system. However, the whole sponsoring process is proposed to be done at the municipality level and then municipalities can transform any offered benefits to be included in the DivAirCity tokenomics.**
- **Restrictions on the use of the DivAirCity tokens for several reasons can be imposed by the cities**

In the following part a rewarding case will be presented together with some indicative tokenization scenarios to illustrate how the DivAirCity tokenization and the corresponding data flow might work. The indicative scenarios are following:

Scenario 1:

- **A citizen hosts a mobile air quality sensor in the backpack. He/She receives tokens for providing the designated data.**

Scenario 2:

- **A second citizen changes her/his means of travel/route, in order to improve air quality. She/He receives tokens for her/his efforts.**

Scenario 3:

- **The two citizens combine their tokens to finance a project in their city.**

In each of the scenarios, the tokens can be redeemed for non-monetary benefits provided by the cities, like city services or any other benefit in the ownership of the city such as sponsor rewards etc.

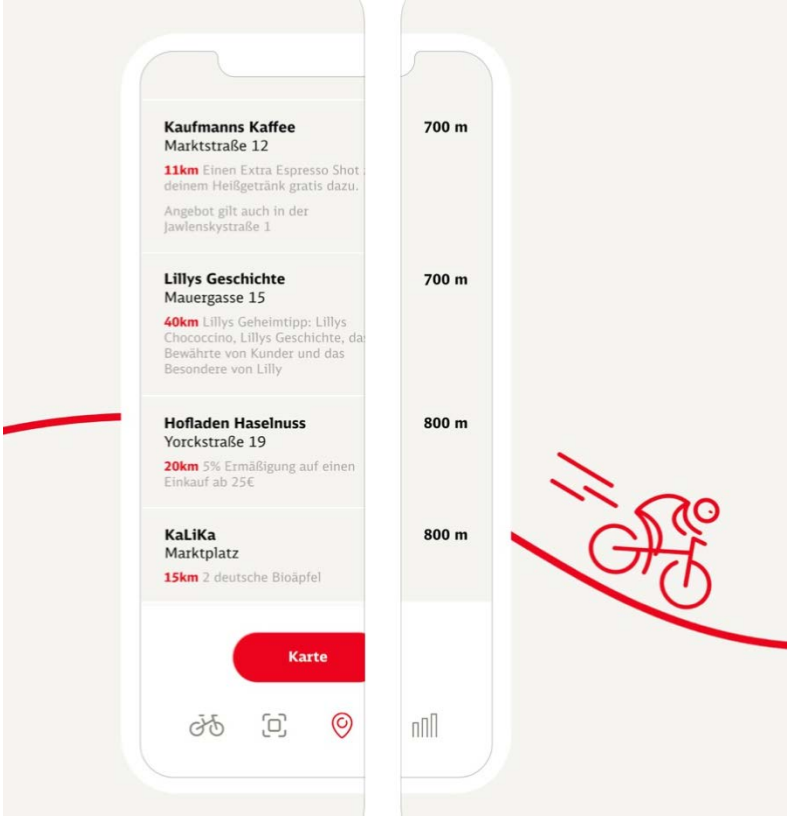
The DivAirCity tokens are linked to the public key of the users' digital wallet. The link between wallet and token is unique. As discussed in Chapter 1, the token is on the BC, therefore the ownership of the token can change through a BC transaction, without having to move the physical or virtual item.

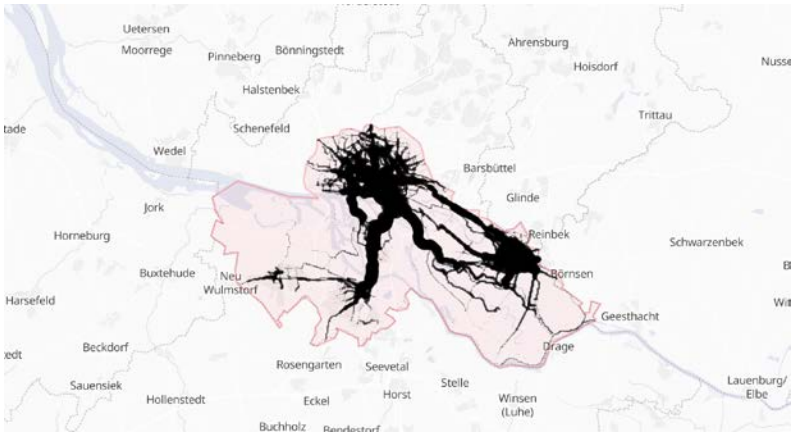
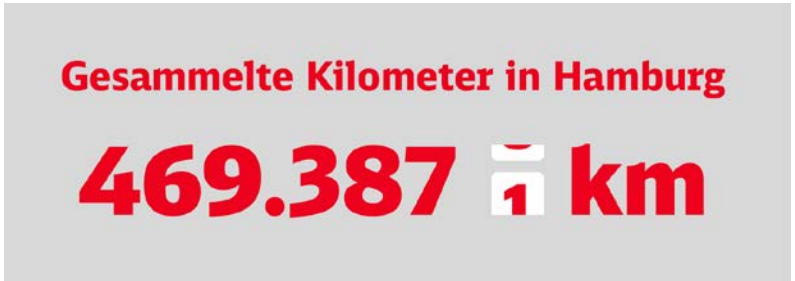
In these scenarios, we assume that a city (called "Belleville" for the purpose of this task description) has certain needs, but at the same time can offer certain benefits to its citizens. The tokenization thus serves two purposes: a) it provides incentives to citizens to adapt certain behaviour b) it allows the citizens to choose the reward for their actions.

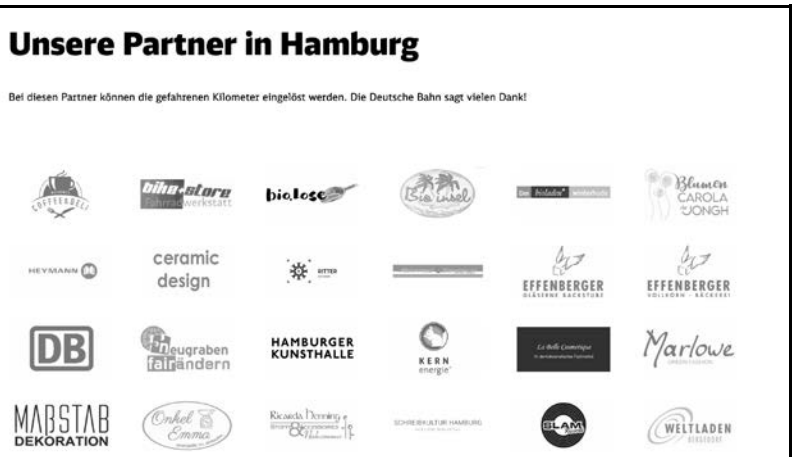
This "voucher 2.0" system allows for more flexibility in the whole system, because the tokens can be collected, pooled, transferred, and interchanged, so that the incentivization fulfils both the needs of the citizens and the cities. In contrast, a simple voucher system where an action X is linked to a reward Y could prove to be too rigid in order to be fitting to the situation in each city.

3.2 A Rewarding example

The example below, is a real implementation of the German railways and illustrates how the rewarding operates. Although the specific application does not use BC to store the tokens, the rewarding vouchers are flexible enough to fulfil the needs of citizens.

Example: The DB Rad+ App (https://radplus.bahnhof.de/)	
The German Railway Corporation, Deutsche Bahn has developed an application which incentivizes citizens to cycle. The application is hosted and maintained by Deutsche Bahn and rewards are provided in collaboration with cities and private partners.	
The citizens download the app. For each km cycled, they receive a "km"-token within their map. On the application, they can find local shops to redeem the "km"-token for local services. **The application shows local services, the distances to local services and the "km"-tokens to receive a discount.** **For the participating shops, the application serves as a tool for marketing, customer acquisition and customer loyalty.** **For the users, the application provides an efficient way of redeeming "km"-tokens.**	

At the shop, the citizens decide how many of their "km"-tokens they want to spend. **The shop scans the voucher, the voucher is validated, and the used "km"-tokens are subtracted from the balance of the citizen.** **The citizens know how many "km"-tokens are in their wallet.**	
The city can map the routes of the citizens and use the data to make decisions about future development of bike routes. **The citizens can also see the data and become part of a community of cyclists.**	
The total amount of "km"-tokens is published as well. **At certain milestones of total "km"-tokens, new rewards are introduced by the city, which benefit all citizens.**	

Partners in the city can be local stores (cafés, bike stores, supermarkets), public cultural institutions (museums, galleries, music halls), or public transport companies.	

The advantage of such a flexible arrangement is that users can choose which rewards they would like to have. The DivAirCity application will be even more flexible than the DB Rad+ App, as it will also allow the transfer of tokens between citizens, which is not possible on the DB Rad+ App.

3.3 Scenario 1: Rewards for using mobile air quality sensors

The city of Belleville does not have enough air quality data from lower-income areas. Belleville would therefore provide an incentive for people to utilise mobile air quality sensors, which it provides to citizens living in the lower-income areas. The mobile air quality sensors can be carried around in a backpack. The citizens having a mobile air quality sensor can upload the recordings of their sensors, using the BC application and get a reward. The submitted air quality data is not stored in the BC, but will be stored, anonymized, in terms that no trace back to the source is possible, in a secure database operated by the city of Belleville.

The city decided to provide free entrance to the public swimming pool for every person who regularly upload the readings of their mobile AQ sensors for a given time period. The citizen Daniela would like to go to the public swimming pool and would also like to participate and provide data on air quality. The data which she provides will not be linked to the identity of Daniela, or to any other personal details, like habits, routes etc. Instead, the BC will be used to store her contributions to the air quality database, as transactions, and will assign the corresponding tokens to Daniela.

Daniela contacts the city manager of Belleville, indicating she wants to have an AQ mobile sensor. The city verifies that Daniela lives in the area where the city needs air quality data and provides her with an AQ sensor together with the corresponding digital credentials to allow the use of the city BC application.

From this point on, all Daniela's transaction will be done using a digital id and a digital wallet. Therefore, Daniela's personal data are fully protected and all her transactions over the BC application are done using her digital id and wallet. Her digital wallet

stores also all her tokens received and allows her to handle them in the BC marketplace.

The smart contract works as follows: every time Daniela uploads the AQ sensor readings, she receives the corresponding DivAirCity tokens.

After a period of time, Daniela has collected a number of tokens. Inside the BC application, she chooses to receive a voucher for free entrance to the public swimming pool, which has a price tag of X tokens.

The BC application executes another smart contract, which reduces her balance by X tokens and sends the voucher to her digital wallet. This voucher then can be used to create a ticket with some e.g., barcode on it to allow her the foreseen free entrance to the public swimming pool.

Using the provided AQ data, the city can analyse AQ patterns and take measures to improve AQ. The AQ data and all related information is not linked to the personal identity of Daniela, due to the use of BC technology.

3.4 Scenario 2: Incentivising citizens for improving AQ

In this scenario, we assume that Scenario 1 has already taken place or is running in the city of Belleville. Based on AQ data from lower-income areas, the city of Belleville wants to reduce air pollution in certain designated areas of the city.

In this scenario, we assume that based on the overall air quality monitoring, weather forecasting etc, the city of Belleville is expecting increased air pollution on the next day for certain parts of the city. The city has created a list of voluntarily actions for the citizens, to improve AQ, for instance switching from using the private car to using public transportation.

The city of Belleville has assigned a number of tokens if a citizen switches to public transport on a day with expected low AQ. The city sends a notification to all users of the application, proposing the use of alternative ways of travel instead of the car. This notification invokes a smart contract, stored on the BC, which provides incentives to citizens from the relevant areas to use alternative ways of travel.

The citizen Elisa lives in an area include in this poor AQ situation. Elisa wants to help in improving the AQ where she lives but does not want to stop driving her car. However, she would be willing to not use her car on days when AQ is low, thus contributing to AQ improvement measures.

After receiving the AQ notification, Elisa registers her intention to use public transport on the application. Next, she uses public transport to go to her work and back. The design of the dApp needs to ensure a way for Elisa to transfer the data without being traced or identified. The smart contract is executed, and the wallet of Elisa receives the tokens assigned to the specific action. It is impossible to trace back

the tokens to the personal identity and travel data of Elisa. After Elisa has earned enough tokens, she can redeem them by exchanging them for a voucher for free access to the public theatre.

3.5 Scenario 3: Letting citizens pool their tokens to invest in AQ infrastructure

The third scenario assumes that the first and second scenario have happened before, it is thus not an alternative scenario, but a subsequent scenario. We assume that the City of Belleville would like to plant trees and would like to involve citizens to improve AQ. In the DivAirCity application, all citizens can see the prices of vouchers which the tokens can be redeemed for. The city declares that 200 tokens are sufficient to plant a tree.

Daniela and Elisa have collected enough tokens which represent the value of a tree. Elisa and Daniela pledge their tokens to buy the tree. However, the tokens are only pledged - the pledged usage is saved on the blockchain through a smart contract. The pledge can be understood as a pre-sale contract where the terms of the (smart) contract are public, but that only becomes valid when both parties agree that the contract is executed. The pledge signals that one party agrees, then the other party (the city) has to agree as well.

Only after both have pledged their tokens in the application, the tokens are transferred to the digital wallet of the city. The city spends the 'benefits' represented by the tokens on a tree. The tokens are removed from the wallets of the citizens.

The personal details of the participating citizens need to be fully protected.

3.6 Target audience

As with the overall DivAirCity project, the target audience of 5.2 is the same as the target audience for the whole DivAirCity project: citizens belonging to the 6+1 diversity groups. The eligibility of a citizen to participate in the DivAirCity BC application can be controlled using digital credentials provided by the cities.

Nevertheless, the above condition is not a restriction but rather a preference to engage the DivAirCity citizen groups. It should be mentioned that all the functions described in this Deliverable can be readily extended to include also other citizens; categories, not included in this project. This depends on proper decisions of the cities which are implementing the DivAirCity digital solutions.

3.7 Cross-border utilisation of tokens

The BC ecosystem that will be developed in the framework of WP5 of the DivAirCity project will be addressed to each one of the participating cities individually. This

means that each city may have own SCCCPs, perhaps partially different. Therefore, the BC application can be seen as a local implementation in each one of the DivAirCity cities. This includes also the restriction that tokens can be used and spent only inside the city.

An additional feature of the DivAirCity BC ecosystem could be its globalization, so that citizens of different cities can interact, using tokens in cities different from the one where they are earned. Although for the moment this may be not of interest, due to the very small number of participating cities, it could become more realistic in future.

Therefore, this can be regarded as a potential capability of the BC application to be developed, despite the fact that the cross-border utilisation of tokens may raise legal or financial issues. This option is under development however at the EU level and DivAirCity will follow closely all related outcomes.

4 Digital Identity Model

Privacy and full respect of personal data are at the core of EU regulation and is a guiding principle of the DivAirCity project. Each city needs to ensure full compliance with EU and local legislation. An important tool for protection of private data is Self-Sovereign Identity (SSI), which links to the conclusions brawn by Deliverable D2.3 *Ethics, privacy and security data management requirements*.

4.1 Self-Sovereign-Identity for data protection

The design of the DivAirCity rewarding model to citizens for their contribution to AQ related data and improvement of AQ levels, requires the valid identification of citizens as well as use of further related personal data. This might partly be related to sensitive information (such as health, race, social status, address, behaviour, minority group, etc). It is of the outmost importance to ensure the highest protection to citizens with regard to the use of their personal data.

The DivAirCity rewarding system is designed as a technological tool that should be inclusive, user friendly, trusted and cost-efficient. Over the past few decades, as life and business have become increasingly reliant on digital transactions, the need for trust online has become critical. From booking a flight to signing a major business deal, our transactions depend on a robust, efficient way to prove who we say we are, electronically. New technology means have been deployed, aiming to empowering citizens to have full control over their own personal data.

One such means is the SSI, also translated as self-managed-identity. It is a digital identity scheme in which the user acquires the power to manage how and in what context own personal data is used without the intervention of intermediaries. This scheme allows people to interact in the digital world with the same freedom and trust capacity as in the offline world. It includes the ability of identity holders to have multiple "decentralised identifiers", issued for different activities and to separate out the attributes associated with an identifier in "verifiable credentials" [17]. This gives the holder greater control over how its identity is represented to third parties and in particular greater control over the personal information that is revealed to other parties.

In a nutshell, the purpose of SSI is to provide identity holders with greater control over their identity by adding features which provide a degree of distribution of identity related information.

In 2016, Christopher Allen [18] identified ten principles of self-managed identity that today are a benchmark in this field:

1. **Access: Users must have access to their own personal data.**

2. **Consent: Users must agree to the use of their identity.**
3. **Control: Users must control their identities.**
4. **Existence: Users must have an independent existence.**
5. **Interoperability: Identities must be as widely usable as possible.**
6. **Minimization: Disclosure of credentials should be minimised.**
7. **Persistence: Identities must be durable over time.**
8. **Protection: User rights must be protected.**
9. **Portability: Information and services about identity must be portable.**
10. **Transparency: Systems and algorithms must be transparent.**

A SSI model allows personal data to reside with the individual and not with a third party that grants or tracks access to it. Users are in control of their data at all times. They can choose with whom they share their data and for what purpose.

Considering that in the framework of the DivAirCity project, data to be accessed is personal and to a certain extent sensitive, the introduction of a SSI model will provide a proper trust environment, to motivate citizens collaboration, while protecting their privacy and empowering individuals to share their data in a sustainable way.

In this context of SSI models, two concepts are essential. The *Decentralised Identifier "DID",* which is the identifier of each actor in the blockchain network, allows each actor to be uniquely identified and to be able to interact with the rest of the parties. The *"Verifiable Credential"*, which is a digital file that contains one or more certifications or statements about an entity to be identified, called User.

Digital Identity Wallets allow users to store identity data, credentials and other attributes linked to their person, in order to use it for authentication purposes, whether online or offline and also to create qualified electronic signatures and seals. This practically means the creation of a corresponding digital version of our physical wallet where we carry a set of documents that provide information linked to our identity (ID, driver's license, bank cards, health cards, etc).

4.2 Self-Sovereign Identity in the EU and its impact on DivAirCity

4.2.1 EU Regulatory Framework for Digital Identity

The EU is immersed in a deep change of the regulatory framework for Digital Identity, as well as the creation of the digital identity wallet and toolbox. DivAirCity is closely following the evolution of regulations, standards and of the technical toolbox for the creation of the EU Digital Wallet (EUID). In order to facilitate a trusted way to use ID electronically the EU approved the "eIDAS Regulation" [19], creating the first regulatory framework for electronic trust services.

With the clear objective to improve the digital trust and cross border use of digital identity, the EU Commission published the proposed Regulation eiDAS2 on June 3, 2021, as a Framework for a European Digital Identity, to guarantee the proper

functioning of the internal market and provide an adequate level of security for electronic identification means and trust services. The scope of EIDAS2 is focused on:

a) **the electronic identification systems notified by the Member States,**
b) **the trust service providers established in the Union, and**
c) **the European digital identity wallets. This last element is an essential point of attention and practical impact for businesses and citizens and is the key tool in the DivAirCity BC implementation.**

4.2.2 EU Digital Identity Wallets and Toolbox

The new eiDAS2 regulation envisages improving the cross-border recognition of national digital identity schemes. eiDAS2 proposes the deployment of a network, composed of nodes, eIDAS-Nodes, for each of the EU Member States. Which may be used both as Services Provider (SP) or Identity Provider (IdP) in the authentication processes for all types of public or private services. When a SP detects the access request of a user from another Member State, it will issue an authentication request that will be routed by the eiDAS protocol to the node of the country that will act as the IdP.

The use of the eiDAS2 protocol offers secure and cross-border communication between the nodes that make up the network, allowing the Member States to be free in choosing the internal authentication protocols used at the national level, thus not implying any change in the current national infrastructure.

Common guidelines and standards are under development including cybersecurity requirements. However, each of the Member States will issue its own solutions.

A relevant aspect is that the issuers of the digital wallets may not collect any information about their use with the sole exception of the data which is necessary to provide the identification service.

4.2.3 Benefits for EU citizens

The digital wallet will be accessible free of charge to every EU citizen, resident and legal entities. It creates a standardised way to verify digital identity for both public and private sectors. The use of the European digital identity wallet will allow its users to have greater control over their data. They will be given the possibility to choose which aspects of their identity, data and certificates they wish to share with third parties and keep control of all interactions.

This provides new means to protect privacy, very much in line with General Data Protection Regulation (GDPR) objectives and vision. It also enhances cybersecurity, auditability and therefore limits the possibility of fraud, which is always a specific concern for public administration authorities.

4.2.4 How does EIDAS2 and EUID Wallets impact DivAirCity

Each city at DivAirCity will co-create its own rewarding scheme for their citizens´ contribution to AQ improvement. DivAirCity´s SCCCPs create relationships between the cities, their citizens and eventually also some private sector providers. In this sense, eIDAS2 and the EUID bring significant options to use private (partly sensitive) data, connect different data to create incentives, link public and private services and use BC for smart contracting and tokenization while keeping privacy at the highest protection levels.

In principle, in the DivAirCity it is not planned to create a cross-border platform or services, but the BC related services will deployed by the cities for their citizens. Each city could indeed use its own Digital Identity Wallet or digital identification system. However, using a common EU standard would present benefits for the SCCCPs. First, we need to ensure that citizens may use identity information which has been issued in a different EU country, such as the national ID of a resident from another Member State. Besides, the development should provide flexibility for future upgrades, not excluding the possibility that evolving the project there may be necessary to extend the implementation level, in a multi city environment by connecting their different SCCCPs and the selection of a global EU standard will definitely help.

We are currently in the middle of an enormous evolution of the EU digital identity scheme. The text of eIDAS2 Regulation is still in progress in the EU legislative process. Vivid discussions are being held regarding the nature and features of the new EU digital identity wallets. Meanwhile, we need to deploy a market ready solution which includes the use of digital identity. This is why, while following closely the evolution of the Digital Identity Framework and Wallets, we need to focus on current solutions that offer EU (specifically GDPR) compliant digital identity solutions and are market ready.

4.3 SSI Standards and EU approach

Following European Blockchain Approach will be considered in the development of the DivAirCity BC application:

- **Guidelines of the "e-Identity Workshop Report" of the "EU Blockchain Observatory and Forum" [20].**
- **Compliance with the eIDAS regulation, according to "Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93 / EC" and take advantage, in due course, of the opportunities that the ongoing revision of the regulation, namely eIDAS2, may offer.**
- **Expand the framework of use of eIDAS with BC following "SSI eIDAS Legal Report" [21].**

- **Make digital identity on BC and GDPR two complementary tools, following the recommendations described in "Blockchain and the GDPR" of "The European Union blockchain observatory and forum" [22].**

Besides EU regulation, it is essential to follow the evolution of specific SSI standards that are currently being developed by a diverse number of standardisation organisations. The model or solution used for DivAirCity could select an infrastructure and SSI framework that is compliant with the current legal framework, but also follows the most relevant standards in order to ensure market adoption and reduce risks. In this sense, the model chosen should be aligned with currently published standards such as "UNE 71307-1: 2020" [23] and the work of CEN-CENELEC, ETSI ISG PDL, ITU and the World Wide Web Consortium (W3C) [24] to complete the standardisation processes and methodologies.

The Spanish Standards Association published the first world-wide standard on management of decentralised digital identities based on BC and distributed ledger technologies (UNE 71307-1). It defines a generic reference framework for issuance, administration and decentralised use of those attributes that facilitate identification of individuals or organisations, allowing them to create and control their own digital identity in a self-managed way without the need for centralised authorities.

On the other hand, W3C defines what a Verifiable Credential is and what parameters this credential requires. Likewise, the W3C defines how to create, resolve, update or deactivate a DID, actions that are defined in the DID method specification.

DivAirCity is closely following the evolution of the EBSI, a joint initiative from the European Commission and the European Blockchain Partnership. The vision is to leverage BC to accelerate the creation of cross-border services for public administrations and their ecosystems to verify information and to make services more trustworthy. Since 2020, EBSI has been deploying a network of distributed nodes across Europe, supporting applications focused on selected use cases [25]. Furthermore, DivAirCity will seek solutions that are compatible with the EBSI technical specifications for ID wallets and verifiable credentials [26]. EBSI has set up a process to examine whether ID Wallets are EBSI conformant [27]. These specifications should be considered in the selection of a DivAirCity ID Wallet.

Without precluding the selection of any current Digital ID solution within DivAirCity, we believe it is useful to understand the technical features and the related data flows and use cases of a specific available solution to understand the procedures linked to the protection of personal data in digital multi stakeholder´s processes.

In this sense, we analyse the Alastria ID model because: a) it is currently available and functional, b) it has been developed to be compliant with EU legislation, c) it has included w3 and UNE standards, c) it has been developed by a non-for-profit decentralised organisation, d) the members and observers include public

administration and e) it already offers market solutions that include public and private stakeholder.

4.3.1 Alastria ID

Alastria ID is a digital identity model developed by Alastria [28] Non-for-Profit- EU Association to be used in digital services. Alastria fosters the digital economy through the development of decentralised distributed ledger technologies. It has become one of the pioneers in the creation of new models of digital identity. It promotes an innovation methodology that anticipates the needs of our society in relation to the use of products and services based on decentralised technologies.

The Alastria ID is based on the concept of SSI in which citizens themselves are the owners of their data by managing, governing and recovering it. That is, the user is the owner and maintains control over its own personal data autonomously, without unnecessarily depending on third parties. This identity protocol has become a benchmark in Spain and Europe and is currently being used for several use cases such as Dalion and Digitalis. It is compliant with EU law as well as with the current Digital ID standards.

There are three stakeholders that interact with each other:

- **First, the "User" who manages its own data. The user manages its credentials, certified by the issuers. On the other hand, the user can share its credentials with service provider companies that need the user's information in order to provide a service.**
- **The "Issuer" is an entity that meets the minimum requirements to be able to issue credentials to users. That is, it must have internal processes that allow it to validate user data with a certain level of trust.**
- **The "Service Providers" are entities that provide services to users. They need trusted data in order to provide the service.**

It should be noted that entities (companies, organisations, associations, etc.) can have the role of Issuer, Service Provider or both.

In order for the stakeholders described above to interact satisfactorily, a series of technical elements that provide security in communication between them have been defined, together with the flows of the different operations that can be done with the identity model on which they work. More details of the Alastria ID model can be found in the documentation published by the Alastria Identity Commission. Functional roles of the parties involved in the use of a Digital Identity Model are described below.

ID creation/ User DID record:

The creation of the Digital ID is the first milestone that makes it possible for the users to have a self-managed identity and to be able to perform any other detailed action in the rest of the user stories. For this, the user must be identified by one of the entities that are part of the project.

The first step in the creation of the DID is to download the proper application (Wallet) and the assignment of a password (and / or fingerprint) by the User. Next, the User generates the public-private key pair in the Wallet. The private key with which this DID is controlled is generated and remains in the identity wallet in possession and under the exclusive control of the User.

The DID is then registered with the associated public key. Therefore, this ledger links the DID with its public key and indirectly with the private control key of the DID. Binding can only be done by controlling the private key. The control key can be later revoked or replaced by the User itself (key rotation).

- **What is recorded on the BC:**

In the first DID record, Alastria ID creation, the public key corresponding to the creation private key is recorded.

For subsequent updates, to revoke the current public key or register the new public key (key rotations) it is necessary to have the current control private key of the DID with which the registration transaction will be signed.

Registering the public key allows credentials to be verifiable. Rotation allows the user to change the control key at any time (periodic rotation, suspected compromise, etc.). Its revocation allows it to indicate that said password should not be used from that moment by any third party.

- **What is saved in the User Wallet:**

The private key, the public key and the user's DID are stored in the secure location of the mobile. The Private key can never be removed from the secure location, and it is used to sign the Presentations from there and update or publicly revoke the key.

Credential delivery:

Once the User has already downloaded the identity wallet and has its DID, the next step is to complete it with the data that the User considers. Each entity will offer the User to include its related data in its wallet. This operation is called delivery of credentials to the User.

The entity, through its website or app, offers the credentials to the User, it selects the ones it considers appropriate and starts the delivery process. The Issuer builds the credentials associating a certain level of trust with them and sends them to the user's wallet. If the user accepts the credentials, these will be stored.

Only the user has access to the credentials that are stored in the secure location of the mobile and only the user makes use of them, for example, to share them whenever they want with a service provider.

- **Content of Credentials:**

A Credential contains technical information and data relating to the user, which is signed, that is why it is usually called a Verifiable Credential in the W3C standard, and it is sent directly from the issuer to the User through a secure channel.

- **What is recorded on the BC:**

Digital evidence of the issuance by the issuer and the reception by the user is recorded.

The content of the credential is never written. Hashes are used on the signed credential, so that the hashed information is considered unpredictable and therefore these hashes are considered irreversible.

To process any of the records, it is necessary to know the content of the signed credential. That is, at this time only the issuer and the user can significantly use the registration of said Credential.

- **What is stored in the Wallet:**

The signed credentials are kept in the secure enclave of the wallet. Only the user has access to them.

The User Revokes the use of a Credential:

Likewise, the user also has the power to decide that no more use is made of a credential issued by an entity, for example, the User changes house and revokes the credential of the address of his old address from his identity wallet.

This action generates an event in the BC that both the issuing entity of the credential, as well as the entities that are using the credential as service providers, will listen, with the aim of marking that credential as revoked and cease its use as long as possible.

- **What is recorded on the BC:**

The status of the revoked Credential is updated using the SubjectCredential Hash and signing the transaction with the User's private control key from the secure enclave of the wallet.

- **What is stored in the Wallet:**

When the Credential detail is shown to the user, the status of the Credential will be shown with the updated value.

Issuer revokes credential:

Some of the Users' credentials may change from time to time or even revoked by the Issuer, for example credentials which may have an expiration.

Besides expired Credentials, when the issuing entity cannot continue to maintain the validity of a credential, for example, if the User ceases to be a customer, the entity

that issued them must update the status of the Credential on the BC. This action is called a credential revocation by the issuer.

When any of these circumstances occurs, the issuing entity of the credential marks the relevant credentials as revoked on the BC. In this way, the entities with the role of service provider that are making use of them and the User itself will be notified through an event in the BC that those credentials are not valid, and that therefore they have to stop using them.

- **What is recorded on the BC:**

The BC status of the Credential is updated, using the Issuer Credential Hash. The transaction is signed with the issuer's DID control key.

The user and those service providers with whom the user has shared the Credential, will be able to interpret the event produced and the information recorded in the BC.

- **What is stored in the wallet:**

The details of the Credential are shown to the user with the current value. A warning to the User about the status of the Credential may be produced.

Authentication with identity wallet (DID):

Thanks to the self-managed identity and the identity wallet, the user will be able to authenticate easily and safely in the applications and websites of the entities that are part of the project using the user wallet.

This functionality allows the User a safe alternative to the use of usernames and passwords as a digital authentication method against entities.

The above-described procedure has been implemented in several applications. However, recently Dalion project, formed by financial, commercial and research entities, aims to develop a decentralised self-managed identity solution based on blockchain technology. The project main objective is the implementation and real production of the Alastria ID self-sovereign identity model in a massive rollout.

5 Architecture Overview and Technical Specifications

In the MSCCP to be developed in the framework of the DivAirCity project, the AQ and decarbonization in five European cities, i.e., Aarhus, Bucharest, Castellon, Orvieto and Potsdam, will be evaluated based on real measurements. For that purpose, sensors will be used, both stationary installed in areas under analysis, and mobile ones used by people who will express their interest in collaborating with the project and belonging to the 6+1 DivAirCity target categories. Sensors, i.e., the end devices, will be connected to the network to communicate and share data. Security measures will be implemented such as cryptographic elements, to avoid malicious attacks. The communication infrastructure will be based on either wired or wireless network, i.e., LoRa network, zigbee, WiFi or Bluetooth. Gateway functions will be performed to protect the network and connect to IoT devices. The data obtained from the sensors will be finally stored to dedicated database/s, either SQL or non-SQL, outside of the BC. The use of separate database/s for data storage, instead of storing the measurements into the BC is due to the high amount of data. If data would be stored in the nodes of the BC network, this would need much more time for execution. Instead, the BC platform will be used for the identification of the participants, both those comprising network nodes, and those who will grant access to the use of the application, and for ensuring that the transactions that should be accompanied by rewarding, will be evaluated based on the participants authentication and their validity. This means that through the BC and specifically the SCCCs, the transactions occurred will be stored into the distributed ledger, will be reported and counted for each one of the users involved, leading to the appropriate tokenization procedure.

The overall system architecture is presented in fig. 1 and the associated components along with their specifications are analyzed below.

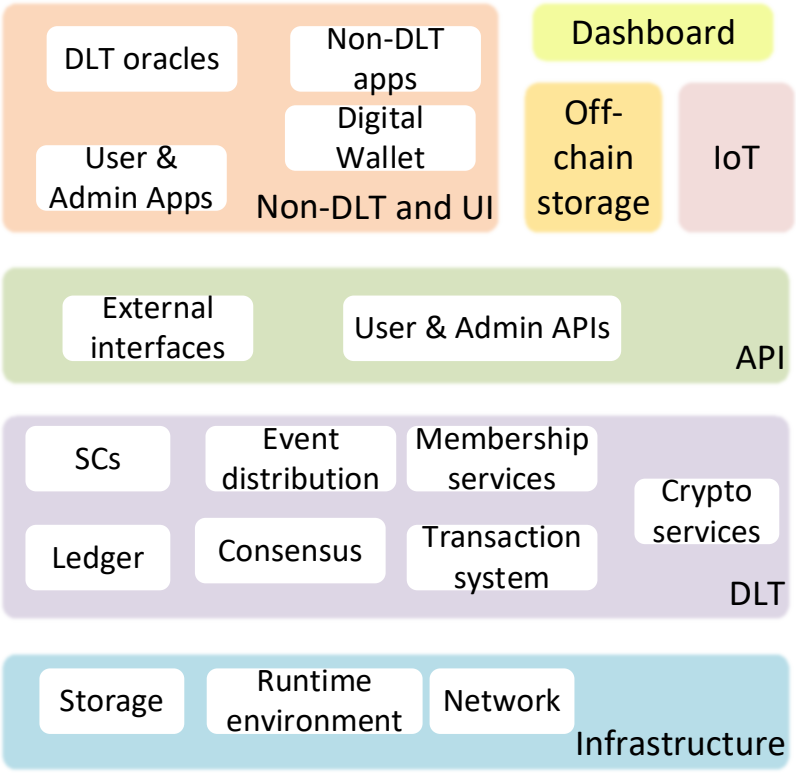


Figure 1. DivAirCity BC system Architecture

5.1 Infrastructure layer

The Infrastructure layer provides the operating environment, including networking, computing and storage components required for the normal operation of a blockchain system. It refers to the nodes of the BC network that will be used in the framework of DivAirCity project application.

5.1.1 Data Storage

Data Storage function should:

- **be deployed and used by each node in the peer-to-peer network**
- **be deployed distributed or local**
- **support appropriate data sovereignty, given that network nodes are in general run and managed by different legal entities**
- **provide data recording and query services efficiently, safely and stably**
- **provide enough storage space for the growing requirements of the ledger as transactions accumulate with time, thus the infrastructure of the DivAirCity nodes will be chosen properly to have specific memory capabilities.**

5.1.2 Runtime Environment

Runtime environment should be provided to each node in the DivAirCity BC network.

5.1.3 Communication Networks

Communication networks are required for

- **the peer-to-peer networking of the DLT system nodes and**
- **the communication between the DLT system and the entities in the user layer, the non-DLT systems, the IoT, the off-chain storage and the dashboard.**

5.2 DLT Platform layer

The DLT Platform layer contains the core functions of the DLT system that can run in DLT DivAirCity nodes and which also involves communication between nodes. Key capabilities include:

- **Non energy intensive consensus mechanism.**
- **Communications between DLT nodes and perhaps systems, via events and secure protocols. This will be decided in the first implementation phase.**

5.2.1 Smart Contracts

A Smart contract, i.e., SCCC, is a distributed application running on and distributed with the distributed ledger.

- **SCCCs should be executed in a Secure Runtime within the DLT platform of any node in the DLT system, when a user sends a transaction of a particular type to the DLT system. The type of the transaction will trigger different smart contracts. The SCCCs will implement the logic running inside the DLT system and update the ledger data.**
- **During runtime, a transaction may invoke smart contract functions requiring a secure environment. Thus, a secure runtime environment for hosting SCCCs is required to implement a so-called Trusted Execution Environment and to protect from rogue Smart Contracts or even malicious ones.**

5.2.2 Ledger

A ledger is an information store which keeps a final and definitive record of transactions, as outputs of the executions of the SCCCs. The information stored in the ledger will be used in the DivAirCity tokenization/rewarding system. For DivAirCity:

- **A ledger includes data storage capabilities.**
- **Data Storage function supports writing and query of various types of data, generated during the operation of the DLT system, such as the ledger, transaction information, etc.**

5.2.3 Transaction System

The transaction system will manage the addition of transactions to the ledger.

5.2.4 Membership Services

Membership Services are services that manage the identity, privacy, confidentiality and auditability within the DLT system. In DivAirCity they will include:

- **The identity of the nodes that will operate within the BC network should be managed and for the transactions to be executed only a set of permissioned ones will be selected. The selected nodes should be chosen with compliance to the policies of the DivAirCity consortium.**
- **It is required a node permissioning mechanism which cannot be modified arbitrarily by participating entities.**

5.2.5 Consensus Mechanism

Based on the desk research presented in Chapters 2–4, a proper consensus mechanism will be selected respecting low energy consumption and meeting the DivAirCity MSCCP requirements. In DivAirCity the consensus mechanism will be such that:

- **The minimum number for having necessary Byzantine Fault Tolerance (BFT) protection is 4, and this maximizes performance, but provides the minimum level of safety and decentralization.**
- **The efficiency and transaction throughput should be high and low energy consuming.**
- **The transaction cost should be zero. The examined BC platforms comply with this requirement.**
- **The whole network has to trust that the selected nodes perform their duties as expected.**
- **The nodes should be selected respecting decentralization and avoiding concentration of power in any single entity or on a reduced group of entities.**

5.2.6 Event Distribution

The event distribution component should handle the distribution of events generated within the DLT platform.

5.2.7 Crypto Services

The Cryptographic Services component should provide the DLT system with access to the necessary cryptographic algorithms, employing hash functions and digital

signatures, either directly or by providing an interface to hardware or software that implements the algorithms.

5.3 API layer

The API layer contains functions that provide reliable and efficient access to the DLT system for applications, users, non-DLT systems and off-chain storage by calling functional components in the DLT Platform layer and provides unified access and node management.

- **The API layer of DivAirCity will enable increased performance by facilitating efficient cache, reliable storage, load balancing, and provide users with reliable and efficient access capabilities.**
- **Non-DLT and off-chain storage access services (external interfaces) provide secure means to access capabilities outside the DLT system such as trusted data sources or functions.**
- **Application programming interface (User API) should provide access to domain specific function meant to accomplish some application related purpose.**
- **Application programming interface (Admin API) should provide access to DivAirCity MSCCP administrator and operator functions.**

5.4 User layer

User layer contains functions to enable DLT users to interact with DLT functions.

- **The DivAirCity end Applications (i.e. SCCCPs built around the MSCCP) should run separately from the DLT systems that acts as a client to the DLT system, used by users, usually to perform domain specific or applications specific functions.**
- **Administration Applications should run separately from the DLT systems that acts as a client to the DLT system, used by administrators supporting capabilities to maintain and/or update applications and systems.**
- **The Application will be provided free of charge and will be compatible with multiple operating systems. It should provide visualization of the individual, own activities, and transactions of the users, and allow tracking past activity and current activity.**
- **The User Interface (UI) will be user friendly, easy to use by the different user categories, translated in the 5 DivAirCity local languages, customizable according to users' needs, accompanied by instructions on how to be used. The UI should allow data entry.**

5.5 Non-DLT Systems Layer

The non-DLT systems layer contains systems outside the DLT system that the DivAirCity DLT system communicates with in order to accomplish its operations. In particular, the DivAirCity DLT systems layer will support the following:

- **DLT oracles should be included, as a trusted service, in order to supply external data to a DLT system.**
- **Non-DLT applications should be included, i.e., any applications outside the DLT system with which the DLT system communicates, either to send or receive data.**
- **Digital wallet should be used to ensure anonymization, security, identity tracking.**

5.6 Off-chain storage

Off-Ledger data should be included, i.e., any data store outside the DLT system that can hold data related to the DLT system in some way. It will be a Database where the data from sensors and their meta-data will be stored. It will be of either SQL or non-SQL technology.

5.7 IoT

Data obtained from both stationary and mobile sensors will be acquired in the framework of the DivAirCity system to be developed. In order for the sensors measurements to be eventually stored into the database, the sensors will be accompanied by IoT infrastructure.

- **The communication infrastructure between the sensors and the final destination of the collected data will be chosen accordingly, to be compatible to the selected devices requirements.**
- **The obtained data will be checked for their validity, for possible outliers, quality etc before being stored into the database.**

5.8 Dashboards

On the Dashboards, the aggregated DivAirCity results and targets reached will be presented along with the relevant statistics.

- **Historical data will be demonstrated in the form of figures, on demand of the user. The figures should be appropriately visible and easy to understand from all users.**
- **The data will be retrieved from the off-chain storage.**

5.9 Cross-layer functions

The cross-layer functions will support the components across all the functional layers. High Levels of security will be applied for the user layer, API layer and DLT Platform layer, therefore security will be a cross-layer functional component. Cross layer functions will support other cross layer functions as well. The functions that will be implemented can be grouped into Development, Operations & Management, Security, and Governance & Compliance categories as following:

- **Development functional components support the activities of DLT system developer, including application and system implementation development, build management and test management. Integrated Development Environment (IDE) functional components provide tools for the development of smart contracts, DLT and related applications, including development of support modules.**
- **Update and version management functions, include management of code bases and implementation artifacts for the nodes and DLT systems.**
- **Provide security attributes such as authentication, authorization, confidentiality, integrity and accessibility for all the functional layers of the DLT and the protocols between nodes.**
  - **The authentication and identity management functions should provide user's identity verification process to determine whether the user has access and usage rights to a resource, thereby enabling the DLT system access control policy to be performed reliably and efficiently.**
  - **The security policy management functions should provide permission for users to access to or use a resource and develop a set of rules that must be followed by all security-related activities in a secure area.**
  - **The access management component is used to provide control over access to specific capabilities of the DLT system.**
  - **The Personally Identifiable Information (PII) protection component should provide capabilities to assist the provision of appropriate protection to any PII handled by the DLT system.**

6 Requirements – Specifications mapping

In the table below we map the requirements identified in D5.1 to the specification of the DivAircity BC MSCCP and SCCCPs.

	REQUIREMENTS		SPECIFICATIONS
R1	**The Developer must be able to log in to the platform.**	**S1**	**The Developer will be able to log in to the platform via an Administration App or a Cross – layer App.**
R2	**The Developer must be able to create a Smart Contract.**	**S2**	**The Developer will be able to create a Smart Contract via the specified IDE, which will provide tools for the development of smart contracts.**
R3	**The Developer must be able to deploy a Smart Contract.**	**S3**	**A Smart Contract, that will implement the logic running inside the DLT system and will be able to update the ledger data, will be developed as part of the DLT Platform layer.**
R4	**The Issuer must be able to grant permissions to one or more users to enter the MSCCP.**	**S4**	**The Issuer will be able to grant permissions to one or more users to enter the MSCCP via the Membership Services, provided by the DLT Platform layer.**
R5	**The Blockchain Platform must support Smart Contracts.**	**S5**	**Both DLT Oracles (which is a non DLT System) and the DLT Platform layer will be deployed and support advanced Smart Contract.**
R6	**The Blockchain Platform must support dApps (i.e. decentralized Apps).**	**S6**	**The Blockchain Platform is a priori designed to support a decentralized concept. The DivAirCity BC platform will be able to support any other dApp built on top of the implemented BC technology.**
R7	**The Blockchain Platform must support tokenisation.**	**S7**	**A BC network supporting tokenization will be used.**
R8	**The Blockchain Platform must support DIDs and Digital Wallets.**	**S8**	**A BC network that supports Digital Ids and Digital Wallets will be used or a BC network that supports pluggable Digital Ids and Digital Wallets.**
R9	**CEN/CLC/TC 13 *Cybersecurity and data protection* standard must be considered while developing the MSCCP/SCCCP.**	**S9**	**The security layer that will be designed (i.e., Cross - layer) will provide several security attributes including authentication, authorization, confidentiality, integrity and accessibility for all the functional layers of the DLT and the protocols between nodes.**
R10	**The data format obtained from heterogeneous sources, i.e., external devices, should be checked and adapted (if necessary) to comply with the MSCCP/SCCCP input profiles.**	**S10**	**Suitable data pre-processing methodology will be used before storing the measurement data to the database.**

R11	**The data provided by sensors and the IoT must be checked syntactically and semantically before being stored and used.**	**S11**	**Monitoring functions will include monitoring, analytics, and automation tools that will be used to respond to several necessary changes to the data to be stored.**
R12	**The SCCCP must be compatible with the software of the devices of the IoT (such as sensors).**	**S12**	**The SCCCP's technical capabilities will be implemented and checked so as to be fully compatible with the selected IoT devices.**
R13	**The MSCCP/SCCCP must be scalable, allowing extensions and generalisations without a need for extreme adaptation.**	**S13**	**The BC platform, the DI/DW, the database and all the non-DLT components used will be chosen and deployed in such a way in order to be scalable.**
R14	**The Blockchain platform consensus costs must be low to make the MSCCP viable.**	**S14**	**The transaction cost should be zero. The examined BC platforms should comply with this requirement.**
R15	**The Blockchain Platform must consume the lowest energy possible, i.e., green blockchain.**	**S15**	**The use of consensus algorithms which are more efficient, provide higher throughput and still providing an adequate level of safety will be considered. The efficiency and transaction throughput will be high and the consensus mechanism will be low energy consuming.**
R16	**The Users must be protected from profiling/tracking to avoid retrieving background information from external parties.**	**S16**	**Only encrypted data will be stored in the BC. The rest could be kept in a separate from the DLT system, secure database in an anonymized form, avoiding any trace back to the users.**
R17	**Confidentiality must be considered to protect personal and nonpersonal information from unauthorised external usage.**	**S17**	**The BC will allow and facilitate regulatory compliance by the members, in this case GDPR.**
R18	**The MSCCP must be compliant with all legislation applicable in the involved jurisdiction. The cities must provide legal and technical structures that assume responsibility for ensuring compliance with the MSCCP.**	**S18**	**The selected BC infrastructure will allow and facilitate regulatory compliance by the members, for example about rules and recommendations of the EU on Cybersecurity.**
R19	**Ethical principles, as defined in DivAirCity Ethical Charter, relevant EU legislation, national and international law, including the Charter and the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Supplementary Protocols, must be respected.**	**S19**	**The selected BC will allow and facilitate regulatory compliance by the members, for example about laws on Services of the Information Society and Electronic Commerce.**
R20	**The MSCCP/SCCCP should respect the principle of proportionality, the right to the physical and mental integrity of a person, the right to non-discrimination and the need to protect**	**S20**	**The smart contracts and the UI will be inclusive and respect the environment, human health and diversity.**

	the environment and human health protection.		
R21	The MSCCP must comply with the Ethical Framework and ethical Chart designed in the framework of the DivAirCity project.	S21	The smart contracts and the UI will respect the Ethical Framework and ethical Chart designed in the framework of the DivAirCity project.
R22	The MSCCP and every action related to it and its impact should comply with the equality principle of the UN Human Rights Convention on the grounds of sex, racial or ethnic origin, age, disability, sexual orientation, religion, or belief.	S22	The smart contracts and the UI will be developed respecting the UN Human Rights Convention.
R23	The MSCCP/SCCCP should ensure equitable and universal access to opportunities and treatments.	S23	The selected BC will allow and facilitate regulatory compliance by its members.
R24	MSCCP governance must be transparent for all involved users.	S24	The selected BC will allow and facilitate regulatory compliance by its members.
R25	The MSCCP must provide users with a user-friendly interface.	S25	The functions that will be developed and contained in the User layer will enable DLT customers to interact with DLT functions, DLT operators and administrative functions.
R26	Users' private data must be protected from unintended public exposure and exploitation.	S26	The PII protection component will provide capabilities to assist the provision of appropriate protection to any PII handled by the DLT system.
R27	Data collection must be handled with privacy, e.g., sensitive data anonymisation, when necessary, separate data on or off-chain to avoid using sensitive personal data in the chain when required, etc. Privacy in data separation must be considered by design.	S27	The data collected will be handled with privacy, i.e., sensitive data anonymisation, when necessary, separate data on or off-chain to avoid using sensitive personal data in the chain when required, etc.
R28	Data must be stored with privacy implementing encryption and de-associating data from physical identities.	S28	The PII protection component will include functions concerning identification and classification of the PII.
R29	Data must be shared and processed with privacy, e.g., deploying data privacy policies, etc.	S29	The MSCCP will allow and facilitate regulatory compliance by its members, in this case GDPR.
R30	No back traceability of any data or correlation of data to its source should be allowed.	S30	The MSCCP will allow and facilitate regulatory compliance by its members.
R31	Both the proposed eIDAS 2 Regulation and the proposed EU identity wallet should be considered.	S31	The proposed eIDAS 2 Regulation and the proposed EU identity wallet will be considered while developing the MSCCP.
R32	For the Issuer to provide credentials, the identity must be proofed, while the identity information must be verified.	S32	The authentication and identity management functional components will support the establishment of identity management

			strategy, determine whether certification will be based on user-known information, user-owned information or user's unique physical characteristics.
R33	The credential management process must be clearly identified.	S33	The authentication and identity management functional components will support the use of specific identity authentication methods to support identity management policies.
R34	The users' level of anonymisation should always be transparent to all engaged stakeholders.	S34	All the engaged stakeholders will be aware of the level of anonymization to which they agree.
R35	The SSI approach should be considered for the Users to maintain control of their digital identities.	S35	Security policy management functional components will include function to set specific authorization and security rules.
R36	Verifiable credentials should be created for data transfer in an understandable and usable way.	S36	The authentication and identity management functional components will support the establishment of user identity management mechanisms based on identity authentication.
R37	The SSI should be considered as a fully portable digital identity for providing access to all the MSCCP services.	S37	The implemented security policy management functional components will include function to authorize users to access and use resource.
R38	The DID must provide a single user account.	S38	The authentication and identity management functional components will support user certification based on user-known information, user-owned information or user's unique physical characteristics.
R39	The DID must provide a safe user account.	S39	The implemented security policy management functional components will include functions allowing that authorization and security rules will be controlled by security authority.
R40	The Digital Wallet must allow users to interact with the MSCCP, perform transactions, and participate in the rewarding system.	S40	The User API will provide access to domain specific function, in order to accomplish the needs of the cities/end users. In this case, the purpose will be to allow citizens to interact with the MSCCP, perform transactions, and participate in the rewarding system.
R41	The Digital Wallet must store users' balance, transactions and other necessary data for the transactions and implement the Smart Contracts.	S41	The user API will provide access to domain specific function, to accomplish specific purposes for the user. In this case, the main aim will be to keep functional user's digital wallet.
R42	The Digital Wallet must be created upon account creation	S42	The Digital Wallet designed will be part of User's Application, thus associated only to one user's account.
R43	The system must be provided free of charge, with users able to create free accounts.	S43	The users of the SCCCPs will be able to operate the applications in order to obtain benefits on a longer-term basis, creating free accounts.

R44	**The Application and the included information must be accessible and usable by the users.**	**S44**	**The access management component will be used to provide control over access to specific capabilities of the DLT system. This will include access controls applied to the various interfaces in the API layer.**
R45	**The Application should be simple and easy to be used by different user categories by customising the interface according to their needs.**	**S45**	**The access management component will be used to access controls applied to the various interfaces in the API layer, hence, allowing customization based on users' needs.**
R46	**The Application may be personalised according to the needs and preferences of the users.**	**S46**	**The access management component will be used to access controls applied to the various interfaces in the API layer, hence, allowing personalization according to the needs and preferences of the users.**
R47	**The Application should allow the users to perform changes, e.g., turn on/off data acquisition, give/deny their consent, when appropriate.**	**S47**	**The access management component will be used to allow access controls applied to the various interfaces in the API layer, hence, allowing users to perform any wished and allowed changes, when appropriate.**
R48	**All users, especially those with low digital literacy, should use the Application and access any available content.**	**S48**	**The access management component will support access control applied to the various interfaces in the API layer. Hence, it will make the app more easily accessible.**
R49	**Appropriate instructions should be incorporated for guidance in using the Application.**	**S49**	**The access management component will provide instructions for guidance to the users.**
R50	**The Application and the incorporated instructions should be translated into the local language of the users in the pilot sites.**	**S50**	**The access management component will support access controls applied to the various interfaces in the API layer. Hence, it will be deployed to provide the UI and the incorporated instructions translated into the local language of the users in the pilot sites.**
R51	**The Application should provide visualisation of the individual, own activities, and transactions of the users.**	**S51**	**Via appropriate dashboards, the User will be able to have an overview of their own activities and history of transactions.**
R52	**The users should be able to see their past activity and track their current activity.**	**S52**	**Via appropriate dashboards, the User will be able to have an overview of their own activities and history of transactions.**
R53	**The Application should be compatible with multiple operating systems.**	**S53**	**DLT System Management function will provide management of DLT systems including and focusing on performance and availability.**
R54	**Registration and any other input required by the system to be inserted manually by the user should be implemented via the Application. The user interface should be the only way of interaction between the Users and the application's backend.**	**S54**	**The access management component will support access controls applied to the various interfaces in the API layer. Hence, it will make UI the only way of interaction between the Users and the application backend.**

R55	**The users must be able to log in to the Application whenever they need, using their DID.**	**S55**	**The authentication and identity management functional components and the access management component designed will be always available upon users' requests.**
R56	**The Blockchain Platform must support tokens to enable users' rewarding for their achievements and the provision of data by introducing a rewarding system.**	**S56**	**A longer-term incentivization - tokenization mechanism will be introduced and used.**
R57	**The users must be able to exchange tokens of the same kind with other members of the MSSCP keeping track of the transactions, but trading is not allowed.**	**S57**	**This will be one of the longer-term incentivization of the designed tokenization mechanism.**
R58	**The tokens must be able to be stored in the individuals' Digital Wallet.**	**S58**	**This will be one of the longer-term incentivization of the designed tokenization mechanism.**
R59	**The Application must provide the capability to exchange tokens for benefits.**	**S59**	**This will be one of the longer-term incentivization of the designed tokenization mechanism.**
R60	**The Application may allow the users to set interest locations, e.g., home, work, etc.**	**S60**	**The dApp will allow users to set interest locations, will offer recommendations for behavioural changing, with the ability to save them, and will send alerts about air pollution levels.**
R61	**The Application may offer recommendations for routes with less CO_2 production and better air quality harmonised with projects goals.**	**S61**	**The dApp will allow users to set interest locations, will offer recommendations for behavioural changing, with the ability to save them, and will send alerts about air pollution levels.**
R62	**The users should be able to save recommendations for later.**	**S62**	**The dApp will allow users to set interest locations, will offer recommendations for behavioural changing, with the ability to save them, and will send alerts about air pollution levels.**
R63	**Users may be able to set notifications for air pollution increases.**	**S63**	**The dApp will allow users to set interest locations, will offer recommendations for behavioural changing, with the ability to save them, and will send alerts about air pollution levels.**
R64	**The MSCCP may be able to use the location data of the users in the framework of the rewarding scheme only with a full privacy guarantee. For this, SSI mechanisms will be explored.**	**S64**	**Users' locations and routes will be tracked, either automatically, or introduced manually by the users, and will be employed in the rewarding scheme respecting privacy.**
R65	**The MSCCP should keep aggregated records of the routes, CO_2 and air quality based on users' actions and visualise them, without any correlation or traceback to the source.**	**S65**	**The anonymization mechanism will not allow any traceback to the source of the information.**

R66	**Diversity must be considered in defining the rewarding mechanisms at the cities level.**	**S66**	**The functions of the SCCCs related to the rewarding mechanism will be created in an inclusive manner respecting diversity, based also on the feedback and input received by the first trials**
R67	**The MSCCP must provide interactive dashboards for visualisation customisable to the diverse user categories without any correlation or traceback to the source.**	**S67**	**The access management component will support access controls applied to the various interfaces in the API layer, without any correlation or traceback to the source. Historical data will be demonstrated in the form of figures, on demand of the user. The figures should be appropriately visible and easy to understand from all users.**

7 Bibliography

[1] H. R. Bokkisam, S. Singh, R. M. Acharya et al., "Blockchain-based peer-to-peer transactive energy system for community microgrid with demand response management," CSEE Journal of Power and Energy Systems, January 2022, vol. 8, no. 1, pp. 198-211.

[2] Decentralized Energy Exchange Platform - https://www.d33p.org/

[3] hopu - https://hopu.eu/blockchainenindustria40/

[4] https://tykn.tech/

[5] SPHINX Horizon 2020 - https://sphinx-project.eu/

[6] PTwist Horizon 2020 project - https://ptwist.eu/

[7] PRIViLEDGE Horizon 2020 project - https://priviledge-project.eu/

[8] PlanetWatch - https://www.planetwatch.io/

[9] S. Benedict, P. Rumaise and J. Kaur, "IoT Blockchain Solution for Air Quality Monitoring in SmartCities," 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2019, pp. 1-6.

[10] M. Zanasso, E. Pasquali, D. Bettini, et al., "Smart Monitoring for a Smart City. Environmental Monitoring using Internet of Things (IoT) and Blockchain: Key Solutions for an Efficient Work Execution and an Improved Environmental Communication," wood ecosteer, Title of the Session: Citizen science involvement and resident-driven impact assessment.

[11] J. Yan, F. Zhang, J. Ma, et al., "Environmental Monitoring System Based on Blockchain," Proceeding of the 4th International Conference on Crowd Science and Engineering (ICCSE), October 2019, pp. 40-43.

[12] S. R. Niya, S. S. Jha, T. Bocek and B. Stiller, "Design and implementation of an automated and decentralized pollution monitoring system with blockchains, smart contracts, and LoRaWAN," NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, 2018, pp. 1-4.

[13] C. T. de Tazoult, R. Chiky, V. Foltescu, "A Distributed Pollution Monitoring System: The Application of Blockchain to Air Quality Monitoring," International Conference on Computational Collective Intelligence (ICCCI), 2019, pp. 688-697.

[14] D. Sofia, N. Lotrecchiano, P. Trucillo, et al., "Novel Air Pollution Measurement System Based on Ethereum Blockchain," Journal of Sensor and Actuator Networks 9, 2020, no. 4: 49.

[15] V. Tran, M. Pham, H. Ho, L. Nguyen, "Advanced Environmental Monitoring Solution Using the Internet of Things (IoT) and Blockchain," The 4th International Conference on Future Networks and Distributed Systems (ICFDS), November 2020, Article No.: 48, pp. 1-5.

[16] M. Lücking, N. Kannengießer, M. Kilgus, *et al.*, "The Merits of a Decentralized Pollution-Monitoring System Based on Distributed Ledger Technology," in *IEEE Access*, vol. 8, pp. 189365-189381, 2020.

[17] ENISA Report - Digital Identity - Leveraging the SSI Concept to Build Trust, January 2022 https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust
[18] The Path to Self-Sovereign Identity, Christopher Allen, April 25 2016 http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
[19] Regulation (EU) 910/2014, of July 23, 2014, on electronic identification and trust services for electronic transactions in the internal market, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=ES
[20] https://www.eublockchainforum.eu/sites/default/files/reports/workshop_5_report_-_e-identity.pdf
[21] https://joinup.ec.europa.eu/sites/default/files/document/2020 04/SSI_eIDAS_legal_report_final_0.pdf
[22] https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf
[23] https://www.beuth.de/en/standard/une-71307-1/334272079
[24] https://www.w3.org/TR/vc-data-model/
[25] https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi
[26] https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Verifiable+Credentials+Lifecycle
[27] https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Become+conformant
[28] https://alastria.io/wp-content/uploads/2019/04/Alastria_Id_2019_03_21_EN.pdf