A Decentralized Marketplace for M2M Economy for Smart Cities

A decentralized marketplace for M2M economy for Smart Cities

Guido Perboli
ICT for City Logistics and Enterprises Lab
ICELab@Polito - Politecnico di Torino
Turin, Italy
guido.perboli@polito.it

Alessandro Manfredi
Deloitte S.p.A. Milan, Italy
amanfredi@deloitte.it

Stefano Musso
Center for Automotive Research and Sustainable mobility
CARS@Polito - Politecnico di Torino
Turin, Italy
stefano.musso@polito.it

Mariangela Rosano
ICT for City Logistics and Enterprises Lab
ICELab@Polito - Politecnico di Torino
Turin, Italy
mariangela.rosano@polito.it

***Abstract*—By 2020 the number of smart cities will reach 600 worldwide, and 5 years later almost 60 percent of the worlds GDP will be produced in them. In particular, Data Marketplace will be the engine of economic progress. In order to foster the new Business Models of the Data and the Machine-to-Machine Economy, there are two needs: managing the plethora of sources of data and link them by a trusted, decentralized and scalable infrastructure. The two disruptive technologies able to foster this innovation are the Internet of Things (IoT) on the data-sources side and the Blockchain on the data marketplace side. In this paper we present a distributed data marketplace framework allowing different actors to purchase and monitor data streams coming from the smart city thanks to the use of IOTA technology, a Blockchain specifically developed for IoT networks. The framework is publicly available and can be the starting point of other IOTA-based solutions.**

***Index Terms*—M2M data marketplace; Blockchain; IOTA**

I. Introduction

Internet of Things is the concept of inter-networking of physical devices, embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. A "thing" in the internet of things can be a person with a heart monitor implant, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an IP address and is able to transfer data over a network. The current number of internet connected things already exceeded our population back in 2008. By 2020 this number is expected to reach 50 billion. A distributed trust technology, ensuring scalability, privacy, and reliability, is a key factor for the growth of such IoT environments [9]. In recent years, the Blockchain (BC) technology emerged as a promising solution in achieving the goals mentioned above thanks to its intrinsic security and decentralized design.

While working on this paper, Prof. Guido Perboli was the leader of the Urban Mobility and Logistics Systems initia-tive of the CARS@POLITO Interdepartmental Center. The authors want to thank the IOTA Foundation for the possibility to be part of its Data Marketplace project.

The Blockchain is a disruptive innovation, due to its capability of ensuring data immutability and public accessibility of data streams. Moreover, its decentralized and distributed infrastructure prevents the problems of the present centralized approaches, including trust issues, such as fraud, corruption, tampering and falsify information, and their limited resiliency. Centralized systems are vulnerable to collapse since a single point of breakdown might lead the whole system to be crashed [12]. The main feature distinguishing a Blockchain from a normal database is that there are specific rules about how to put data into the database. That is, it cannot conflict with some other data that is already in the database (consistent), its append-only (immutable), and the data itself is locked to an owner (ownable), it is replicable and available. Finally, everyone agrees on what the state of the things in the database is (canonical) without a central party (decentralized). These two combined technologies (DLT/Blockchain and IoT) could bring big advantages in the Smart City since the Blockchain creates a digital record containing data produced by the IoT (and not only) that is incredibly secure and is easily accessible to the public [11]. A Smart City combines information, communication technology, and the network of physical devices referred to the Internet of things to make city operations, commuting, quality of life, and sustainability as optimal as can be.

In this context, it emerges the need of developing software framework able to interconnect different sensors in a larger network and create sustainable business models over data exchange. A decentralized application on a Blockchain would reduce costs associated with using the platform while giving users more control of their data and information [13]. Moreover, in Smart City applications the presence of a decentralized marketplace is seen as the key success factor for the creation of a Machine-to-Machine economy and factual services over areas larger than the single city [4].

Among the different Blockchain frameworks, IOTA is emerging as the best choice when large IoT sensors networks must be considered. IOTA is a cryptocurrency specified for micro-payments and for IoT applications [6]. IOTA is not based on the traditional BC technology, but it exploits TANGLE, which is an acyclic graph, making IOTA a system highly scalable. Furthermore, IOTA is an asynchronous network without the need of mining, and thus it is a system with zero transaction fees.

The Blockchain literature mainly considers the business process modeling and the technology design process of the proposed solutions. In particular, in [14] a Blockchain solution is proposed to solve the problem of the lack of trust in collaborative processes. Recently, more attention has been devoted to Blockchain applications in the fresh food market. In this field the importance of Blockchain applications relies in the trust and immutability of the data in a system in which different actors are involved in the supply chain. [7] proposes a public Blockchain solution based on double chain architecture to enhance the efficiency of Blockchain in the agricultural supply chain, also guaranteeing the transparency and security of transaction information and privacy of enterprise information. All the analyzed cases have been just simulated, without a real industrial application. Therefore, the main drawbacks come from the size of the underlying networks, and the related performance issues. Moreover, the frameworks analyzed in literature lack in the development of a standard methodology to design, develop, test, and validate the proposed solutions at a strategic level. In particular, there is a limited evidence of the value for the different actors involved in the process, with their costs and benefits. As a consequence, few Blockchain projects have a high longevity. The only article that proposes a standard and repeatable methodology to address the design phase of a Blockchain project is [12]. Moreover, the paper presents the results of a real use case in the fresh food delivery, highlighting the critical aspects of the implementation of a Blockchain solution, showing the benefits in terms of reduction of the logistics costs and optimization of the operations.

From the IoT point of view, several papers deal with different aspects of the interconnection between IoT and BC, in particular in the Smart City context [1, 2, 3], but just recently a few of them consider the problem of the creation of a data marketplace and its integration with the IoT network [4, 8, 10, 13]. They consider single aspects of the integration and adapt BC framework not scalable for IoT solutions as Ethereum. This is a limit, in fact while the connection between a sensor and a classic BC as Ethereum is somehow simpler compared to the use of a more complex framework as IOTA, the limited speed and scalability of traditional BCs might prevent the practical introduction of their solutions. In this paper we aim to overcome this limit, by presenting PEGASUS, a decentralized Marketplace specifically designed to be interconnected with the IOTA BC and compliant with the IOTA Data Marketplace APIs [5].

Even if the adoption of BC will grow exponentially in future years, nowadays it presents some problems. Some of the major issues are related to its cost (both economic and environmental) and the scalability of the system.

II. IOTA

A possible solution to this problem of scalability is to revolutionize the basic structure of the DLT. For this reason the third generation blockchains are born, ie dlt with a basic structure that is based on the concept of a DAG (Direct Acyclic Graph) rather than being based on a chain of blocks like the current one. One possible technology that uses graphs is IOTA. First of all, let's see what the acronym of DAG means and how it is applied to the concept of distributed ledger. The DAG (Fig. 1) literally Direct Acyclical Graph, is a data structure that has no direct cycles, that is, by choosing any vertex of the graph it is not possible to go back to it by going through the edges of the graph. A sequence can only pass from the first to the next and not vice versa. The DAG is often applied to problems related to data processing, scheduling, searching for the best route for navigation and data compression.

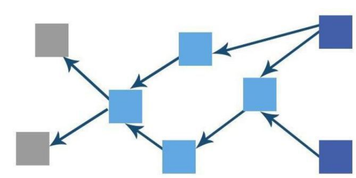

Fig. 1. General Structure of a DAG

In the blockchain, transactions are collected in blocks, which can only be created sequentially, thus forming a chain. In the DAGs, the "blocking concept as a set of transactions is not used", as all transactions are directly linked to each other. Therefore, a block will consist of a single transition within the DAG. In this way it is possible to execute transactions simultaneously, in parallel and in a faster way, increasing the network throughput.

IOTA is a next generation distributed ledger, which is based on a cryptocurrency called MIOTA (Millions of IOTA or Mega IOTA). The digital currency is specifically designed for the Internet of Things (IoT). IOTA aims to increase efficiency in the m2m economy which is based on the principle that the sensors or devices are able to send and receive funds without human presence. Sending and receiving IOTA tokens is guaranteed by the nodes present within the IOTA network. The name of these nodes is IRI. To send and receive transactions, iota nodes create bundles. To send and receive IOTA tokens, clients send packages of transactions called bundles to IRI nodes. The transactions in a bundle instruct the node to transfer IOTA tokens from one address to another. These addresses are generated by using a client's unique secret password called a seed. When the bundle is confirmed in the Tangle, the IOTA tokens are transferred. The basic architecture of IOTA is based on the concept of DAG and is called *Tangle*. The tangle is a DAG-valued stochastic process where new vertices get attached to the graph at Poissonian times, and the attachment's locations are chosen by means of random walks on that graph. These new vertices (also thought of as "transactions") are issued by many players (which are the nodes of the network), independently. It is proved the existence of Nash equilibria for the system where a part of players tries to optimize their attachment strategies. So, The Tangle is the data structure formed by the connections among transactions in the distributed ledger on all IRI nodes. One of the validation critera of a transaction is that each one must directly reference two previous transactions (*tip transactions*). After many studies, the IOTA Foundation decided to adopt the ternary system instead of the binary one. This choice was made because it was discovered that this type of system leads to big savings from an energy point of view and turns out to be more efficient in resolving operations. In binary, data can be represented as either 1 or 0. These values are called bits. Eight bits is equal to one byte, which can have

$$256(2^8)$$

possible values. In ternary, data can be represented as 1, 0, or -1. These values are called trits. Three trits is equal to one tryte, which can have

$$27(3^3)$$

possible values. IOTA represents data as tryte-encoded characters, according to the tryte alphabet where each of the 27 characters consists of one tryte.

A. MAM: Masked Authentication Message

IOTA is the first distributed ledger that has no transaction fees and is built for the Internet of Things ecosystem; enabling a future in which devices can securely communicate with and autonomously compensate each other. IOTA uses a gossip protocol to propagate transactions through the network. This mechanism means that any data with sufficient weight can be propagate to the opposite side of the cluster efficiently. MAM has a Channel in which owner publishes data and viewers receive them. Viewers subscribe channel in order to get available data. Thanks to MAM, the users can publish a message at any time. They only need to conduct a small amount of proof of work to allow the data to propagate through the network. If nodes are listening for the channel ID (= address) in real time, the message (gossipped through the network) will be received by a subscriber when it reaches the subscribers node. MAM uses a Merkle tree based signature scheme to sign the cipher digest of an encrypted message. The root of this Merkle tree is used as the ID of the channel. Since a single tree only lasts for a short period of time, each message contains the root of the next Merkle tree. Each message is encrypted with a one-time pad that consists of the channel ID and the index of the key used to sign the message; an additional nonce may be used as a revocable encryption key. The resulting cipher hash is signed using the private key belonging to one of the leaves. The encrypted payload, the signature and the leafs siblings are then published to the tangle where anyone knowing the symmetric key can find and decrypt it.

III. Decentralized Data Marketplace

The present work is based on the development of an extension for Google Chrome that implements a decentralized marketplace of data emitted by sensors connected to the IOTA network. The end user is able, thanks to the use of this extension, to send and receive transactions, monitor their balance, and most importantly, to buy streams of data emitted by the devices. Since these data streams need to be written on the IOTA tangle in order to be available to the final user, a program has also been developed to take data from the sensors and write them on the IOTA tangle thanks to the use of the MAM protocol described previously. Therefore, the development of this work is made up of two applications: the extension for Google Chrome installed on end users' PCs and a program able to collect data from the sensors and write them on the Tangle. Google Chrome extensions are made of different, but cohesive, components. Components can include background scripts, content scripts, an options page, UI elements and various logic files. Extension components are created with web development technologies: HTML, CSS, and JavaScript. An extension's components will depend on its functionality and may not require every option. Regarding the first, that is the application that allows you to interact with the marketplace, has been developed using the most used development couple in the cryptospace, React and NodeJs, while for the demo, it was enough only the use of NodeJS as this application does not have a graphical interface. The creation of Web applications, regardless of the framework chosen for development, necessarily involves the three fundamental languages of the platform: HTML for the structure, CSS for the stylization and JavaScript for the application logic. React is a Javascript library created by Facebook and Instagram that allows you to create a single-page application (Single Page Applications, SPA) through a structure that divides it into dynamic and reusable components.

A. Architecture

This system is called Pegasus (a Smart City can be seen a collection of objects connected to each other almost as if it were a constellation), and, as previously written, is composed of two applications. As for the first application, the one that allows you to interact with the sensors installed within the city, has different features. The first one implements a decentralized marketplace in which it is possible to buy data directly from the sensors installed in the city. Moreover it implements all the functionalities of a wallet, because these features are intrinsic to the fact that in order to buy data streams it is necessary to have funds, which are managed directly by the application itself. So, as described in the previous chapter, a cryptocurrency wallet must allow the user to send and receive tokens and monitor its balance. The most delicate functionality in implementing a wallet is key management. In the case of IOTA, the most delicate part is the management of the seed because in order to perform operations it is necessary to supply the seed. The second application, is the one that must be installed on sensors belonging to this marketplace, i.e. those sensors that allow sending data to users who have purchased this right. Each sensor connected to the IOTA network sends the data detected on the IOTA Tangle thanks to the use of the MAM protocol. The sensor, thanks to this protocol, creates a restricted channel which will provide the key to decrypt the content of the data, to the users who will make the payment to the sensor to have visibility of the data. Since this type of channel is based on symmetric cryptography, the data is encrypted with a symmetric key and the user must possess the key in order to receive correct data. So, to be able to send this key, is used the asymmetric encryption: when the user pays the sensor, in addition to sending the amount for which you can access the data, he also sends his public key so that the sensor, after receiving the amount necessary to allow him to receive the data, will send him the key of the MAM channel encrypted with the public key just received, so that only the user who actually paid will be able to decrypt the access key to the MAM channel with his private key.

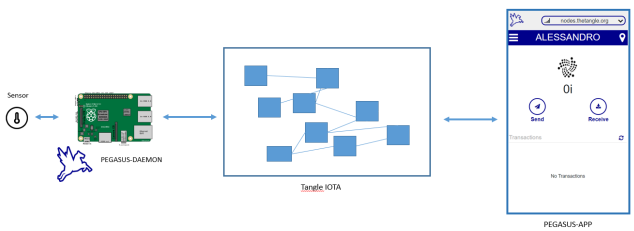

Fig. 2. PEGASUS Architecture

B. Marketplace

The most important part of this thesis work is the development of a protocol above the IOTA network able to create a decentralized marketplace where payments are made thanks to the use of the MIOTA token. A decentralized marketplace allows for truly peer-to-peer transactions without centralized authorities taking their fees. This is made possible through IOTA technology. We no longer need the trusted third party verifying sellers and ensuring payments. Since the marketplace is decentralized, it was necessary to develop a protocol for which each connected sensor is able to supply its own data (e.g.: latitude, longitude, address, name, etc.). If the marketplace was centralized, this operation would have been simple as it would be enough to communicate such data to a web service, which will save them on the database and provide them to other users. In this case, the thing is more complicated: each sensor connected must communicate to all users connected its data without going through a server. To simulate this behavior, an ad-hoc application was created in order to simulate this scenario. The application, during the initialization process, in addition to initializing all the parameters necessary for the creation of a restricted MAM channel on which to send data, generates two seeds. The first one is related to the sensor account, while the other is used to simulate a receiver so that it is possible to send a transaction containing the sensor data to the receivers's seed. This transaction is identified by a specific *tag*, so that every user connected to the marketplace is able to find on the Tangle all the transactions with this type of tag and then find all the sensors connected to the marketplace and their data. Once initialized, the sensor sends the detected data to the MAM channel every 20 seconds. Moreover, every time the sensor receives a payment from a user, it sends to this user the (symmetric) access key to the MAM channel and the root from which to start receiving data. Since the transactions sent on the IOTA Tangle are visible to everyone, it was necessary to implement a key exchange algorithm. For this purpose we chose to use the *RSA* algorithm. In cryptography, the acronym RSA indicates an asymmetric cryptographic algorithm, invented in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman, which can be used to encrypt or sign information.

Every time a user accesses the markeplace, the application performs the following procedure:

1) Through the *findTransactionObjects* function provided by the *iota.js* library, the application searches for all transactions with the word "pegasus" as *tag*. In this way, as mentioned previously, it is possible to find all the devices connected to the marketplace.
2) To retrieve the actual data of each sensor connected to the marketplace, for each transaction received, it is necessary to read the contents of the *signatureMessageFragment* field, and first through a conversion function from trytes to ascii, and then a conversion from ascii to JSON, it is possible to get the content of the data sent by the sensor, and then show the sensor-related marker on the map. The data sent by the sensor have the following structure:
   - *deviceName*: name of the sensor
   - *lat* : latitude of the sensor
   - *long* : longitude of the sensor
   - *address* : address of the sensor on which it is possible to make the payment to have access to the data stream
   - *price* : stream price
3) Once this data is correctly decoded, the application shows on the map the position relative to each sensor, thanks to the use of markers in order to facilitate the user.
4) As a user may have purchased streams of sensor-related data, it is necessary to find all the transactions that identify a payment to a certain type of user by a given sensor, since inside this transaction there are both the sidekey and the root to access the MAM channel. This type of transaction is identified by the "pegasus-payment" tag so that, thanks to the use of the *findTransactionObjects* function, it is able to find all the transactions issued by a sensor to a particular address. Again, once you have found all of them, you need to apply the decoding

described above to the *signatureMessageFragment* field. The data sent by the sensor have the following structure:

- *root*: address from which to start fetching on the MAM channel
- *sidekey*: sidekey encrypted with the user public key sent during the payment.
- *deviceName*: name of the device

5) Once the sidekey and root of each sensor have been received, the application executes a thread that every minute is able to receive the data sent by the sensors of which you have the root and key to access the MAM channel.

COMPUTATIONAL TESTS

In order to test the framework, we created a test by simulating the presence of a data provider and a buyer.

C. Receive transaction

To simulate the reception of a transaction, the *faucet* service was used which, once inserted the address of the wallet on which the tokens have to be received, it generates a transaction at the address selected above with an amount equal to 1000 IOTA tokens. It is possible to check the status of the transaction thanks to the use of the tangle explorer. The test for receiving a transaction consists of several parts:

1) Copy the address using the ”receive” screen in the application.
2) Paste the address in the appropriate form within the *IOTA faucet* platform and press enter .
3) Wait for the wallet to synchronize with the tangle in order to be able to show this transaction.
4) If the user wants to check the status of the transaction, just click on the row relating to the transaction whose status you want to know in the list of transactions on the home page and copy the address of the bundle or an internal transaction (Fig 3) to that bundle and paste it into the tangle explorer.

D. Send transaction

In order to access the functionality of sending tokens, as well as having available a minimum amount for which you can send them, you need to know the address of the recipient. The application also offers the possibility of sending transactions at value 0 or entering 0 in the appropriate form relative to the amount of tokens to be sent, or leaving it empty. It is also possible to send a message if the transaction is a value of 0 which is nothing but a text string that will be converted into trytes by the application at the time of sending.

E. Buy data stream from sensors

The main part of this work is the development of a decentralized marketplace that allows a user to buy data directly from a sensor. The process of purchasing a sensor consists of the following steps:

- Access the marketplace through the application.

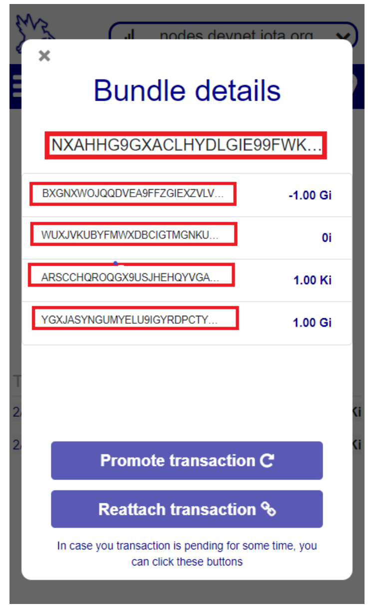

Fig. 3. Bundle details

- Select the marker on the map relative to the sensor for which you want to purchase the data stream and click the ”buy stream” button (Fig 4).

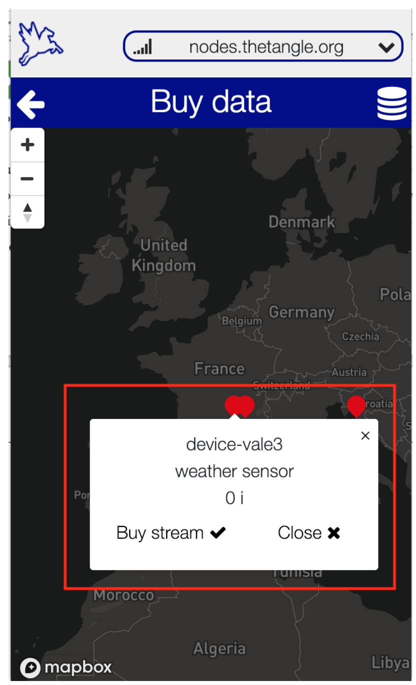

Fig. 4. Selected sensor for which you want to purchase the data stream

- Once clicked, it is necessary to wait for the operation to complete. In this process the application sends the payment and its public key to the sensor, so that it is able to send it the access key to the MAM channel on which it is sending data, encrypted with the public key just received (Fig 5).

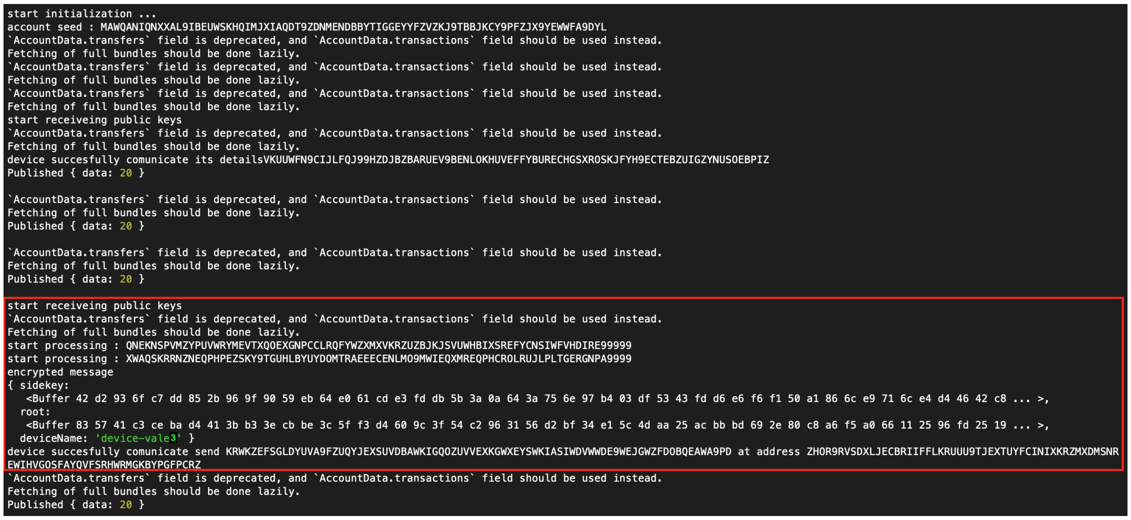

Fig. 5. Message containing the sidekey and the root both encrypted

- In case the payment is successful, once all the transactions have been confirmed by the Tangle, it is possible to monitor the data that the sensors constantly write on the Tangle through the MAM protocol.

The code of the project is publicly available at the following links:

- https://github.com/allemanfredi/PEGASUS
- https://github.com/allemanfredi/PEGASUS-DAEMON

References

[1] R. B. Chakraborty, M. Pandey, and S. S. Rautaray, "Managing computation load on a blockchain–based multi–layered internet–of–things network," *Procedia computer science*, vol. 132, pp. 469–476, 2018.

[2] A. Duda, O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, and F. Zanichelli, "Iotchain: A blockchain security architecture for the internet of things," in *IEEE WCNC*, 2018.

[3] M. English, S. Auer, and J. Domingue, "Block chain technologies & the semantic web: A framework for symbiotic development," in *Computer Science Conference for University of Bonn Students, J. Lehmann, H. Thakkar, L. Halilaj, and R. Asmat, Eds*, 2016, pp. 47–61.

[4] R. Giusti, C. Iorfida, Y. Li, D. Manerba, S. Musso, G. Perboli, R. Tadei, and S. Yuan, "Sustainable and de-stressed international supply-chains through the SYNCHRO-NET approach," *Sustainability*, vol. 11, no. 4, p. 1083, feb 2019.

[5] IOTA Foundation, "Iota data marketplace," 2017. [Online]. Available: https://data.iota.org

[6] ——, "IOTA: The Next Generation of Distributed Ledger Technology," 2018. [Online]. Available: https://www.iotatoken.com/

[7] K. Leng, Y. Bi, L. Jing, H.-C. Fu, and I. Van Nieuwenhuyse, "Research on agricultural supply chain system with double chain architecture based on blockchain technology," *Future Generation Computer Systems*, vol. 86, pp. 641–649, 2018.

[8] K. R. Ozyilmaz, M. Dogan, and A. Yurdakul, "IDMoB: IoT data marketplace on blockchain," in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE, jun 2018.

[9] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration. A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.

[10] G. Papadodimas, G. Palaiokrasas, A. Litke, and T. Varvarigou, "Implementation of smart contracts for blockchain based IoT applications," in *2018 9th International Conference on the Network of the Future (NOF)*. IEEE, nov 2018.

[11] G. Perboli, A. De Marco, F. Perfetti, and M. Marone, "A new taxonomy of smart city projects," in *Transportation Research Procedia*, vol. 3, 2014, pp. 470–478.

[12] G. Perboli, S. Musso, and M. Rosano, "Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases," *IEEE Access*, vol. 6, pp. 62 018–62 028, 2018.

[13] V. P. Ranganthan, R. Dantu, A. Paul, P. Mears, and K. Morozov, "A decentralized marketplace application on the ethereum blockchain," in *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, oct 2018.

[14] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, "Untrusted business process monitoring and execution using blockchain," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9850 LNCS, pp. 329–347, 2016.