# Corporate Digital Identity based on Blockchain

Guillermo Balastegui-García, Elvi Mihai Sabau Sabau,
Antonio Soriano Payá, Higinio Mora

Department of Computer Science Technology and Computation, University of Alicante, Spain
guillermo.balasterri@ua.es; emss5@alu.ua.es
soriano@ua.es; hmora@ua.es

**Abstract**. Digital Identity refers to the set of information that defines an entity, generally a person, which can be presented to other entities of digital world. This information represents different information such as skills, biological, activities and other data that may result useful. There are currently several projects developing digital identity systems for personal use and aiming to standardize its use among the population. Digital Identity finds in blockchain the support technology to enable this decentralized management in a secure and reliable way. Blockchain allows citizens identification to each application, contract or business, by providing only the information requested, and avoiding unnecessarily exposing of other private information about citizens. However, there are no digital identity systems for legal entities. Currently, the digital identity concept for business and corporations is limited to its appearance in the digital environment and their corporate image on internet. The objective of this work is the proposal and development of a digital identity for legal entities based on a blockchain network. The methodology is based on applying the same idea of personal digital identity. In addition, the proposal considers Ethereum blockchain since it is strongly accepted for the deployment of smart contracts. As a result, the proposed corporate digital identity provides companies the control of the information they share with government, people and other companies. In addition, the relationships between entities can be defined, and eventually automate, through smart contracts in the blockchain. The main limitation of this idea is the technology adoption by institutions and public administrations in order to normalizing digital relations between all agent involved: corporates, citizens and administrations.

**Keywords:** Blockchain, Digital Identity, Legal Entities, e-government.

## 1 Introduction

Currently, the creation and transfer of digital content which occurs in the world are overwhelming. Such a data flow generates opportunities for people who can acquire, process, and understand that information. The Internet has changed the way people interacts in their lives between them and with their environment.

In this context, the need to protect and authenticate information arises in order to provide control over data and trust in information communications between entities. Governments, firms and governments search for comprehensive solutions that enable citizens and identities to identify themselves.

While there is developing a digital identity concept for personal data [1], there is not an equivalent solution for companies yet. Currently, there is not a reliable system that allows a legal entity governs its own data, nor to share and exchange information through a digital environment in a safe, trustworthy, fast, and efficient manner with another entity or regulatory or certifying agency.

This is an important issue for modern societies where digital relations between participants are encouraged in order to increase productivity, reducing costs, and provide a better service to citizens and firms.

A recent example was the pandemic caused by Covid-19. In this situation, personal relations and paper-based document exchange were not recommendable practices [22]. The generalization of an interoperable digital identity among citizens, firms and public administration will allow ubiquitous relations where anyone could be able to make transactions anywhere at any time.

In this work it is proposed the idea about a corporative digital identity system that gives enterprises a tool for sharing information and storing procedures, taking a special focus on integrity and authenticity, making easier communication and operation processes with the agents with it relates (citizens, public administrations, regulatory entities and commissions, and other companies).

The methodology adopted starts from analysing the Digital Identity concept for personal purposes since this tool already has many of the desired features. From this starting point, this work proposes an implementation based on the same technology and includes transaction support for interaction operations.

The structure of this work is as follows. Section 1 gives the introduction and provides the purpose of the work. Section 2 describes the background and related work about digital identities and implementations under blockchain technology. Section 3 introduces the main elements of the proposed idea. Section 4 portrays an example of implementation using Ethereum and smart contracts blockchain and Section 5 illustrates the conclusions of the work.

## 2 Background

Self-sovereign digital identity gives back the user the control of this data, letting him know who and in which terms accesses its information.

### 2.1 Personal Digital Identity

Digital Identity, also known as Identity 2.0, is all information related to a person which is located in a digital storage, including all the publications in which the person appears, regardless of the publisher, its documentation, and its data in general [2]. On the digital world, this is equivalent to its real-life identity.

Digital identity is increasingly used is many processes related to information sharing in the digital world, such as employee recruitment [3], financial services [4], and also in healthcare [5].

Currently, digital identity implementations based on blockchain provide the desired features of security, data integrity and anonymity. In addition, there is no need of a third-party organization in the middle or in charge of the data communications [6].

Consequently, this technology enables that digital identity becomes the primary source of authentication for digital services and other trust systems in the near future.

Blockchain technology is based on cryptography and distributed ledger systems (DLT), which operate through decentralization and consensus. These pillars provide security to a system that is based on a Blockchain network, making it tamper-proof and fraud-proof. This system offers strong advantages such as privacy, identity self-management, safe communication, security and trust through smart contracts, and immutability of information [7]. Based on these features, blockchain technology provides solutions for data sharing by providing trust to participants without any intermediary organization [19, 20]. These blockchain solutions give people back control over their data, letting them decide who can see or use their information in a precise way [8, 9].

Public and private key pairs must be created and used through "identity wallets" to create a Blockchain-based digital identity system. Those wallets are responsible for calculating the hash of the public key and storing it in a blockchain, which is immutable. The user has control of their identifiers from that moment on, which are decentralized and independent of any higher body.

The identity wallet is also the interface that allows the user to interact with the Blockchain network and the other users, being a simple and usable method. The premise is that as long as you keep your cryptographic keys stored, you remain in control of your information [10]. Meanwhile, user data is stored in the network's cloud, which is distributed and replicated across the various devices in the network.

As shown in Fig.1, an entity, such as a university, creates a degree that certifies that a person has an education, gives the credential to the owner, and rises this to the Blockchain network, so that when another entity needs to check if the person owns this degree, it will only have to look for the credential, which will be backed by the Blockchain network [11].

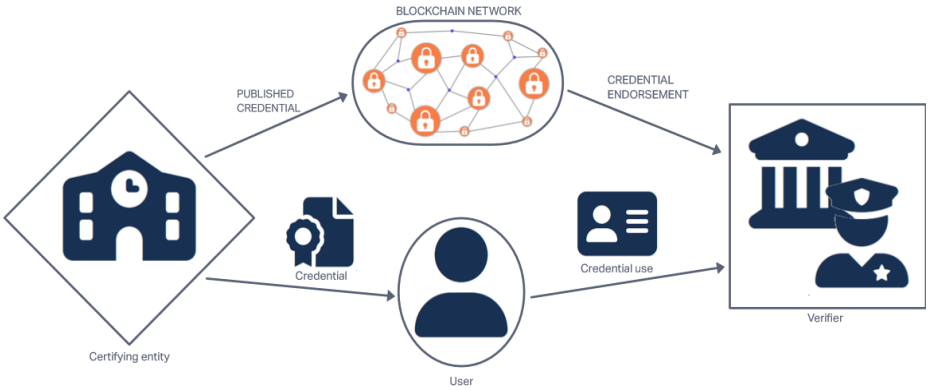


**Fig. 1.** Blockchain-based Digital Identity Flowchart

Big companies such as Microsoft and various governments including European Union are currently working on diverse projects of decentralized digital identity [12, 13, 14].

### 2.2 Corporative Digital Identity

The concept of Corporate Digital Identity (CDI) is currently understood as the image that a company has online through the content that generates, shares and controls on the various platforms on which it is located [15]. This concept of identity shapes a "digital reputation", the opinion that its followers and community have of the company. This identity and this reputation are shaped by the media manager or by marketing decisions [16].

Although those are concepts that go hand in hand, they are not the same, digital identity is more tangible, it can be seen in the image, the colours, the publications, the logo of the brand, and reputation has a more abstract nature, formed by the perception and opinion of people about the brand.

According to Spanish National Cybersecurity Institute (INCIBE), most companies have a digital identity that they actively maintain, which generates a reputation [17].

This reputation can be attacked in different ways, INCIBE itself offers prevention and reaction guidelines for corporations to protect themselves from attacks, although these are based on community relations solutions rather than on technical or technological means.

### 2.3 Findings of the related work

SSI – Self-Sovereign Identity and blockchain are currently gaining importance thanks to the advantages they offer to their systems users and various international organizations are already committed to their use.

The digital identity of a company is currently understood as the image the corporation shows to the public through its social networks, its website, its blog, and sometimes through the image offered by its customers when they rate its product and publish their opinions about the company. This concept of corporate digital identity is only related to its image, not as a tool that can be given a utility beyond representing.

The advancement of SSI systems and digital identity should also reach corporate-type profiles enabling companies to take advantage of the SSI benefits supported by blockchain networks.

## 3 Corporate Digital Identity Model

Companies have a large amount of documentation of different areas keeping all their legal and economic aspects up to date, and they must also be confident that all the information and products they obtain from other organizations are true, complete, and authentic. There is also relevant formal documentation for regulatory entities such as tax entities, employment entities or labour institutions among others, which may vary depending on the region where the company is located, the sector, and the type of services it offers.

Human resources dedicated to keeping the company formalized are costly and usually perform repetitive tasks that consist of receiving, formalizing, and forwarding contracts. All these tasks can be addressed by a blockchain-based Digital Identity system for legal entities that automates the document exchange and verification

processes. These legal entities can be firms, societies, institutions, and even governments at different level.

A Blockchain network that interconnects legal entities with each other, allows them to verify the authenticity and originality of their documentations, products and services and their ability to carry out transactions legally, among other operations, improves efficiency in government, industrial, commercial, and service processes.

A priori, digital identity services for organizations can be connected to digital identity services for individuals, thus improving processes in which information provided by a person must be verified or in which information generated by another company about that person must be accessed in a transparent, legal, and secure way. Fig 2 depicts the most overall scheme of this proposal.

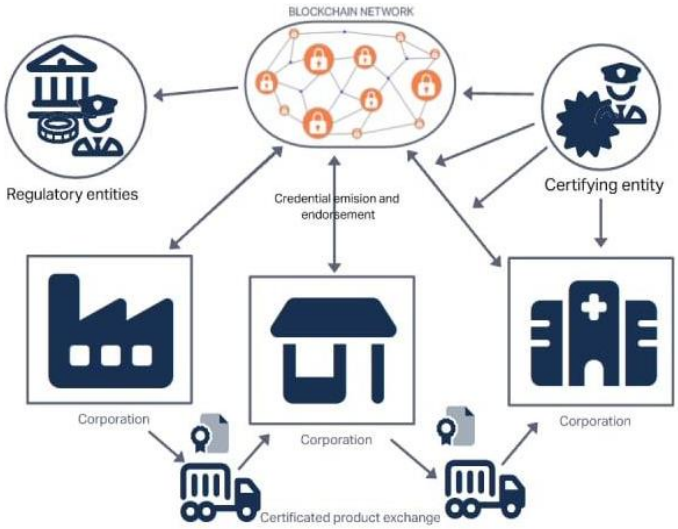


**Fig. 2.** Corporative Digital Identity Scheme

This scheme represents the digital relations of corporations with other entities and administrations. In fact, the CDI concept becomes in a tool for enhancing digital relations with any other agent of the society, including citizens, and other firms. The ability to include in this CDI not only information, but also functions and contracts enhances digital operations to interchange information and make transactions.

The advantages of a corporate digital identity system are of a different nature. Next, the most relevant aspects are listed:

- Agility in the exchange of information between corporations.
- Improved trust during exchanges of goods, services, or information between people.
- Improved security during communication between two or more undertakings.
- Reduction of bureaucratic costs.

- Reduction of regularisation times for companies.
- Transparency in information exchanges, both in the eyes of a company and in the eyes of its customers and partners.
- Traceability of exchanged products.
- Reduction and control of fraudulent sales of a product by persons or organizations external to the product developer.
- Increasing of automation and making digital transactions.

The proposed CDI model provides companies with a tool that allows them to store their information, which may vary depending on the sector and field in which the company is located, but in general terms, it may be composed of:

- *Assigned attributes* (for example): Fiscal and legal data of the company; Identity of the company (name, image, values, mission, etc.).
- *Cumulative attributes* (for example): Patents, products and services; Certificates; Employees; Subsidiaries or branches; Ubication; Current payment certificate.

These are some of the data that the proposed digital identity could contain. In addition, it facilitates an easier relationship with other companies, and not only with companies but also with employees, customers and users using its SSI system, providing confidence to them, as they will be able to see authentic information about the company, thus facilitating recruitment of new human resources.

## 4 Blockchain-based implementation

There are currently many different implementations of blockchain. Not all of these implementations follow the original model of the Bitcoin network as a public, pseudo-anonymous network.

As a proposed implementation, we use the *Ethereum protocol* (https://ethereum.org/en/) and Smart Contracts to develop a system that can manage said attributes for a legal entity based on the blockchain technology.

### 4.1 About the blockchain used.

Ethereum is a public blockchain which adds a trust factor over the users who use it, since any transaction, process, or modification of the stored data can be verified by anyone. In addition, Ethereum protocol is open source anyone can develop their own blockchain using this protocol, although it is recommendable to use an already existing and well-populated one, since the more nodes and users a blockchain has, the more solid and secure it becomes.

Smart Contracts (SC) are programs that run over the Ethereum protocol. SC is a software stored on a blockchain that are automatically executed when predetermined terms and conditions are met. This feature guarantees that the contract cannot be modified, and it will always behave in the same way. This immutability in execution allows to program automatic executions avoiding bureaucratic processes that are energy and time-consuming [21].

The programming language used can be an already existing one such as JS, C++, Rust, Python, or Solidity since there are many libraries for each language that brings the Ethereum ecosystem into the development environment.

Each function calls on a smart contract represents a transaction in the blockchain since the function will execute a logic or change the state of the data stored in the blockchain.

In the Ethereum ecosystem, to prevent infinite loops, speed up transaction time, and to incentivize users to validate the transactions issued by a smart contract, function calls have a fee in "gas". Gas is a unit used to measure the cryptocurrency needs to execute logic on the blockchain, and it varies from time to time depending on a few factors such as the computational load of the blockchain, the storage used, and the complexity of the operations to be computed [18].

### 4.2 Implementation details

Smart contracts provide the ability to develop a system that manages the desired attributes of the digital identity for each company, share them specifically with any entity or with anyone, and verify their integrity and validity.

A data model can be defined by using data structures that will define the assigned and cumulative attributes of the company as an entity in the blockchain. Fig. 3 shows an example of company data structure.

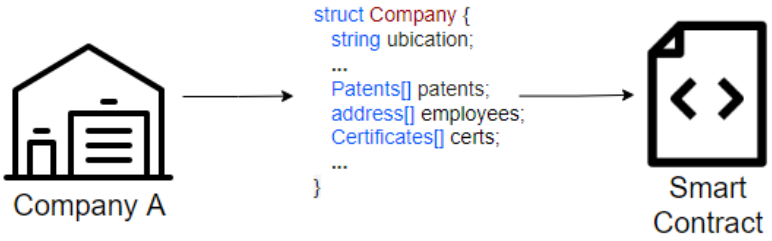


**Fig. 3** Example of company data structure.

Certain attributes such as certificates can be hard-bound to accounts, in a way that no one can alter the contents or change the ownership of the attribute. And others such as patents can be traded between companies as assets, for example by turning these attributes into "Non Fungible Tokens" (NFTs). NFTs can also be managed and transferred by approved entities. By this way, the resposability of managing certain assets could be delegated to external companies. Fig 4 illustrates some cases of NFTs management.

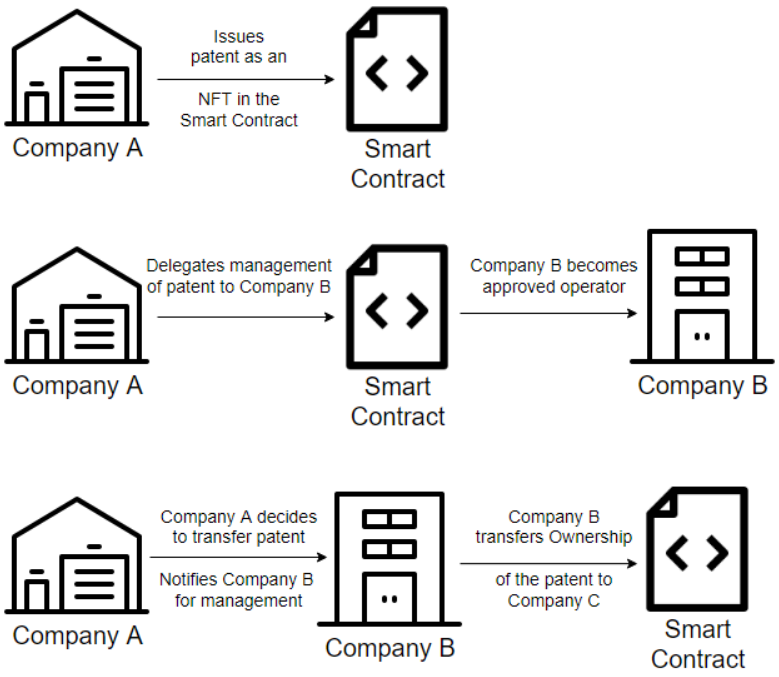


**Fig. 4.** NFT management examples.

And for private data transfers, the only way to share private data without letting other parties read its contents is by encrypting it.

The public and private keys bound to each account can be used to encrypt and decrypt private data shared between entities, by using public-key cryptography and hashing functions for data integrity validation. Fig 5. describes a simple encryption-decryption process. In this way, entities can share private data with other companies by encrypting the data with the receiver's company public key.

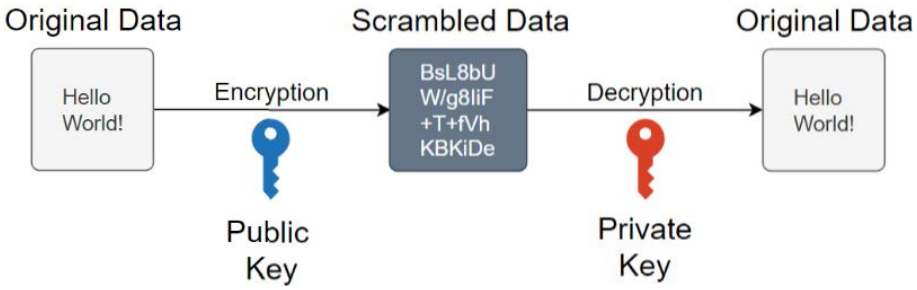


**Fig. 5** Encryption and decryption process.

## 5 Conclusions

Self-governed digital identity is emerging as a tool of the future that can change the way we understand information exchange and data management. There is a growing number of public and private projects that aim to implement this technology in people's lives and improve the digitalization of society.

In this work, a technological proposal based on Ethereum blockchain and Smart Contracts for building a Corporate Digital Identity has been proposed. This idea extends the personal digital identity concept to companies and allows integrate Smart Contracts in order to perform transactions with other agents of the society. This self-governed digital identity tool for legal entities, such as companies, corporations and even governments, should allow the business world take advantage of the many benefits brought by this technology, and enhance the development in the digital world. To this end, technologies such as blockchain and SSI play an important role in this transformation. This concept could have application at different areas, such as in healthcare, commerce, sport, and production.

However, digital Identity debate is open. Access to a universally recognized Digital Identity could unlock new and better experiences for users and enterprises as they interact online with businesses, service providers, public administrations and their community. The implications and the expectations are high. The high efficiency of the transactions and the ubiquity of the interactions will boost the development of new kind of social interactions and business.

Currently, technology is ready to support identity value-added services both for companies and citizens, and it is expected that, in the near future, regulatory entities could advance in normalization of SSI proposals for legal entities. Even so, there are also disadvantages. Society could not be sufficiently prepared for assimilate the disruptive changes witch new technologies provide. In addition, other drawbacks exist, such as new cyberattacks forms, technological dependence, etc.

As future work, we aim to explore regulation frameworks at national and European level, in order to propose applications to develop the capabilities and potential of CDI.

## Acknowledgements

This work was supported by the Conselleria of Participation, Transparency, Cooperation and Democratic Quality, of the Community of Valencia, Spain, under SDG oriented projects of the University of Alicante.

## References

1. Seifert R. (2020) Digital identities – self-sovereignty and blockchain are the keys to success, Network Security, Volume 2020, Issue 11, Pages 17-19. https://doi.org/10.1016/S1353-4858(20)30131-8
2. Feher K. (2019) Digital identity and the online self: Footprint strategies – An exploratory and comparative research study, Journal of Information Science, https://doi.org/10.1177/0165551519879702
3. Krishna S. Digital identity, datafication and social justice: understanding Aadhaar use among informal workers in south India, Information Technology for Development Volume

27, 2021 - Issue 1. https://doi.org/10.1080/02681102.2020.1818544
4. Jessel B., Lowmaster K., Hughes N. Digital identity: The foundation for trusted transactions in financial services," Journal of Financial Transformation, Capco Institute, vol. 47, pages 143-150. 2018.
5. Houtan B., Hafid A. S.; Makrakis D. A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare, IEEE Access, vol. 8, 2020. https://doi.org/10.1109/ACCESS.2020.2994090
6. Malyan R.S., Madan A.K. Blockchain Technology as a Tool to Manage Digital Identity: A Conceptual Study. In: Singari R.M., Mathiyazhagan K., Kumar H. (eds) Advances in Manufacturing and Industrial Engineering. Lecture Notes in Mechanical Engineering. Springer, Singapore. 2021. https://doi.org/10.1007/978-981-15-8542-5_55
7. Mora, H., Morales-Morales, M.R., Pujol-López, F.A. and Mollá-Sirvent, R., "Social cryptocurrencies as model for enhancing sustainable development", Kybernetes, Vol. 50 No. 10, pp. 2883-2916. 2021. https://doi.org/10.1108/K-05-2020-0259
8. Mora H., Mendoza-Tello JC., Varela-Guzmán EG., Szymanski J., Blockchain technologies to address smart city and society challenges, Computers in Human Behavior, 2021, 122, 106854. https://doi.org/10.1016/j.chb.2021.106854
9. Mora, H., Pérez-delHoyo, R., Sirvent, R.M., Gilart-Iglesias, V., Management City Model Based on Blockchain and Smart Contracts Technology. In: Visvizi, A., Lytras, M. (eds) Research & Innovation Forum 2019. RIIFORUM 2019. Springer Proceedings in Complexity. Springer, Cham. 2019. https://doi.org/10.1007/978-3-030-30809-4_28
10. Soltani R., Nguyen U.T., An A. Practical Key Recovery Model for Self-Sovereign Identity Based Digital Wallets, IEEE Intl Conf on Dependable, Autonomic and Secure Computing, https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00066
11. Mora, H., Pujol-López, F.A., Morales, M.R., Mollá-Sirvent, R. (2021). Disruptive Technologies for Enabling Smart Government. In: Visvizi, A., Lytras, M.D., Aljohani, N.R. (eds) Research and Innovation Forum 2020. RIIFORUM 2020. Springer Proceedings in Complexity. Springer, Cham. https://doi.org/10.1007/978-3-030-62066-0_6
12. Spanish Standard (2020) UNE 71307-1. Digital Enabling Technologies. Decentralised Identity Management Model based on Blockchain and other Distributed Ledgers Technologies. Part 1: Reference Framework.
13. European Parliament, (2021) EPRS, Updating the European digital identity framework, legislative briefing, October 2021
14. DIF - Decentralized Identity Foundation. https://identity.foundation/, accessed on 01/05/2022
15. Saran S.M, Shokouhyar S. Crossing the chasm between green corporate image and green corporate identity: a text mining, social media-based case study on automakers, Journal of Strategic Marketing. 2021. https://doi.org/10.1080/0965254X.2021.1874490
16. Mora, H., Sirvent, R.M. (2019). Analysis of Virtual Currencies as Driver of Business Marketing. In: Visvizi, A., Lytras, M. (eds) Research & Innovation Forum 2019. RIIFORUM 2019. Springer Proceedings in Complexity. Springer, Cham. https://doi.org/10.1007/978-3-030-30809-4_48
17. Digital identity: the online reputation of companies (in Spanish), Spanish National Institute of Security (INCIBE), Available online at: https://www.incibe.es/protege-tu-empresa/blog/infografia-id-empreas, accessed on 01/05/2022.
18. Werner, S.M., Pritz, P.J., Perez, D. (2020). Step on the Gas? A Better Approach for Recommending the Ethereum Gas Price. In: Pardalos, P., Kotsireas, I., Guo, Y., Knottenbelt, W. (eds) Mathematical Research for Blockchain Economy. Springer Proceedings in Business and Economics. Springer, Cham. https://doi.org/10.1007/978-3-030-53356-4_10
19. Sicilia, M. and Visvizi, A. (2019), "Blockchain and OECD data repositories: opportunities and policymaking implications", Library Hi Tech, Vol. 37 No. 1, pp. 30-42.

https://doi.org/10.1108/LHT-12-2017-0276
20. Çekani, V. (2021). The Role of Blockchain Technology During Covid-19 in the Healthcare Sector. In: Visvizi, A., Troisi, O., Saeedi, K. (eds) Research and Innovation Forum 2021. RIIFORUM 2021. Springer Proceedings in Complexity. Springer, Cham. https://doi.org/10.1007/978-3-030-84311-3_4
21. Sirianni, C.A., Sabbagh, P., Marra, F. (2021). An Ethereum-Based Chain for Diagnosis and Control of Covid-19. In: Visvizi, A., Troisi, O., Saeedi, K. (eds) Research and Innovation Forum 2021. RIIFORUM 2021. Springer Proceedings in Complexity. Springer, Cham. https://doi.org/10.1007/978-3-030-84311-3_6
22. De Falco, C.C., Romeo, E. (2021). ICT and Social Value Co-Creation During the Covid-19 Emergency: The Case of MascherinAmica. In: Visvizi, A., Troisi, O., Saeedi, K. (eds) Research and Innovation Forum 2021. RIIFORUM 2021. Springer Proceedings in Complexity. Springer, Cham. https://doi.org/10.1007/978-3-030-84311-3_1