# Blockchain and Self-Sovereign Identity for Public Administration

Michele Dell'Era[1,2]

[1]InnovaPuglia S.p.A., Valenzano (Bari), Italy
[2]Guglielmo Marconi University, Rome, Italy

**Abstract**
The e-Government is based on the use of ICT and represents a strategic goal in government agendas. Recently, a lot of attention has been directed towards blockchain technology. It has characteristics that could have a strong impact in several sectors, including the public one. The Self-Sovereign Identity, for its part, is a technology that could solve some critical issues highlighted with the use of current digital identity systems.

**Keywords**
e-Government, Blockchain, Digital Identity, Self-Sovereign Identity

## 1. Introduction

The emergence of new needs has often led to changes in social values, sometimes accompanied by technological advances that have marked history in a more or less important way, depending on the political, economic, social and cultural context. The development of information and communication technologies (ICT) has become a strategic goal in the agendas of governments. The use of ICT in administrative processes is called e-Government. It clearly is a dynamic entity, which evolves with the changing economic, social and cultural needs [1]. Recently, concepts such as digital identity have been introduced and a lot of attention has been directed towards technologies, such as blockchain, which could have a strong impact in various sectors: financial, logistics, Public Administration (PA), guaranteeing trust, responsibility, transparency and immutability.

## 2. e-Government

The e-Government can be identified as the introduction and use of ICT in administrative processes, with the aim of providing services that more efficiently meet the new needs, which over time change at the same pace as the evolution of society, in terms of organization and lifestyles. However, it should be noted that it not only coincides with the computerization and general digitization of the PA, but is also a useful tool to offer a valuable contribution to the improvement of the final services provided to users. The innovative processes introduced, related to the e-Government, have necessarily changed the type of interaction between the PA and citizens and businesses, based on methods that are profoundly different from traditional ones. Today the user and his needs are placed at the center of administrative proceedings. The PA has to manage the dematerialization processes, innovating the back office processes that prepare the online delivery of the final service [1]. Since, the PA also needs to manage efficiently own telecommunication infrastructure, the involvement of Edge Cloud Computing technologies is crucial [2]. This also gives the opportunity to provide a better distribution of media content [3]. All these actions are expected to be realized within the "Next Generation Network in 2030" [4], also characterized by intelligent use of FPGAs [5] digital filters [6] and neural networks [7, 8, 10].

### 2.1. Digital Agenda for Europe

The Digital Agenda for Europe is a tool that the European Union has adopted in order to promote innovation, progress and economic growth, exploiting the potential of ICT, with the main aim of developing the digital single market [12]. Since the 1990s, ICT has played a decisive role in increasing productivity and growth in the EU. The digital unique market has been launched over the past decade, with the aim of presenting the main legislative proposals, for example on the development of e-commerce, copyright, private life and electronic communications, harmonization of digital rights and cybersecurity [12]. Among other things, it involved the development of digital identities, investments in artificial intelligence, cybersecurity, 5G networks, quantum computing and blockchain [13].

### 2.2. Digital Agenda for Italy

The Digital Agenda for Europe has been implemented by each Member State, each of which has adopted its own

*ICYRIME 2022: International Conference of Yearly Reports on Informatics, Mathematics, and Engineering. Catania, August 26-29, 2022*

strategy. Italy has developed its Digital Agenda, that is a national digitization strategy, aimed at achieving the targets set out in the European Agenda, identifying priorities and methods of intervention suited to the needs of the Italian context [15]. The Digital Agenda for Italy is defined through the Italian Strategy for Digital Growth 2014-2020. The document sets out the guidelines for digital growth, both in infrastructural terms and through the provision of enabling platforms: the National Registry of the Resident Population (ANPR), which is a centralized database that takes over from the municipal registers and the Registry of Italians Resident Abroad (AIRE); a mandatory electronic invoicing system to the PA; PagoPA, that is a system that gives citizens and businesses the opportunity to make payments electronically, to the PAs and public utility service providers; Open Data, adopting national guidelines that define models, methodologies and timing common to the PAs; digitization in the sectors of health, education, justice, tourism, agriculture [16]. From an infrastructural point of view, it contemplates: the Public Connectivity System, which defines the ways in which the information systems of the PAs must cooperate with each other; Digital Security for the PA, with the aim of increasing the level of security of digital information and communications, protecting the privacy, integrity and continuity of PA services; a rationalization of ICT assets, with consolidation of data centers and cloud computing; SPID, which guarantees citizens and businesses safe and secure access to the digital services of the PA and of the private entities that join to them [16]. The Agency for Digital Italy (AgID) plays a fundamental role in this scenario: established in June 2012, it is responsible for achieving these objectives [16].

# 3. Digital Identity

Digital identity is the set of digital resources uniquely associated with a citizen who identifies him, representing his will, during his digital activities. Digital identity is usually presented to access a computer system or information system or to sign digital documents. The Public Administration uses digital identity to provide access to online services through a single credential, which is activated only once and is always valid [21]. Access to online public services is therefore only possible with the Public Digital Identity System (SPID) and the Electronic Identity Card (CIE). All PAs must have integrated SPID and CIE into their information systems, as the only digital identity systems for accessing digital services, leaving the old credentials. Thanks to SPID and CIE, access to public services becomes uniform throughout the national territory, with the advantage of having greater security of personal data, no longer having to manage different credentials depending on the service they want to use and also being able to access the services offered by Member States of the European Union [21].

## 3.1. SPID

The SPID identity is issued by private entities accredited by AgID, called Identity Providers, which in compliance with the rules issued by AgID, provide digital identities and manage users authentication. The choice of the identity provider, by citizens and businesses, is free. After verifying the data, it issues the digital identity, releasing the credentials [22]. There are three SPID security levels: the first level allows access to online services through a username and password chosen by the user; the second level allows access through a username and password chosen by the user, adding the generation of a one time password, sent to the user via text message or through the use of an app given by the provider; the third level requires a particular hardware that manages the cryptographic keys, such as a smart card or a remote digital signature device, in addition to the username and password [23].

# 4. Regulations for electronic identification

## 4.1. eIDAS

EU Regulation No. 910/2014 - electronic IDentification Authentication and Signature (eIDAS) - was defined to provide Member States with a common regulatory basis for the management of trust services and electronic identification means, increasing security and effectiveness of electronic services and transactions of e-business and electronic commerce in the European Union. It has been in force since 2016 [24]. Among other things, it establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic certified delivery services and services relating to website authentication certificates; it defines the conditions under which Member States recognize electronic identification system of citizens and businesses, who fall under a notified electronic identification system of another Member State [25]. Unlike electronic identification systems, according to eIDAS, each Member State can notify the electronic identification systems provided to citizens and businesses to enable mutual recognition [24]. In Italy, the national eIDAS Node allows Italian citizens to access the online services of other EU countries - such as public, university, banking services - using SPID or CIE. Moreover, citizens of other European countries in possession of digital identities are recognized in the eIDAS framework, to access the services of the Italian PA [26].

## 4.2. Self-Sovereign Identity

The Self-Sovereign Identity (SSI) is a digital identity directly controlled by the user, who has the possibility to choose which data to allow sharing, among those available, when accessing a particular service [27]. In the first historical period of Internet activity, the main problem was to create a network of networks. The TCP/IP protocol fulfills this purpose, but is limited to identifying the address of the computer connected to the network, without providing information relating to the citizen or business who is using it. To solve this problem, a model based on the concept of an account has been introduced. The accounts are registered by the entity who provides the online services. However, this causes several problems, linked to the multiplication of identities and the existence of that account only on the servers of that particular entity, the total absence of control over the data by the person who owns the account, and greater exposure to possible thefts of identity. The next model, developed to address these issues, is that of federated identity. In this case, the existence of a third party, the Identity Provider (IdP), is expected between the service provider and the person who would use it. The latter therefore has an identity registered by the IdP and can access services provided by third parties, without having to re-register at their sites, but by accessing through that identity. SPID is an example of this model. SSI represents a third model, decentralized and made possible thanks to distributed ledger technologies, such as the blockchain. The feature that distinguishes this model from the others is that it operates in the same ways as a real identity. In fact, it is based on a direct relationship between the owner of the SSI and the entity who needs to verify an attribute [27]. The SSI ecosystem has three main roles. The issuer is the person responsible for creating and issuing the credentials for the holder. The holder is the owner: he receives the credentials from the issuer, owns them and, when requested, shares them with a verifier. He has full control over the use of his SSI and decides which data to share from time to time, among those contained in his identity. Furthermore, he must be in a position to carry out all operations relating to his identity, or to assign control of certain functions to third parties on his behalf. Finally, the verifier is a person responsible for verifying the credentials presented by a holder [28].

### 4.2.1. SSI in Europe and Italy

The current federated model used in the EU took shape as a result of the eIDAS Regulation [27]. For several years now, the EU has considered the issue of creating a digital identity management system to be central, for the creation of a digital single market and for the concrete possibility of guaranteeing all citizens of the Member States those rights of free movement and freedom of establishment which can only be achieved by guaranteeing an efficient dialogue with all the PAs of the Member States. In April 2020 the European Commission published the SSI eIDAS Legal Report, with which it mainly suggests the creation of an eIDAS Bridge, exploiting the European Blockchain Systems Infrastucture (EBSI) which already, autonomously, includes among its goals that of creating in Europe an SSI model) and to proceed gradually according to a schedule that includes a series of steps. In the short term, the use of eIDAS digital identities (such as SPID) is planned for the purpose of issuing VCs. In the medium term, the issuance of qualified certificates, the issuing of technical specifications for VCs, the adoption of new specifications based on the European Self-Sovereign Identity Framework (ESSIF), on the EBSI platform, for identification are planned. In the long term, the need is identified to regulate Identity hubs as trust services, to regulate the services that offer wallets for the management of cryptographic keys as independent trust services, to regulate some specific nodes of the registers distributed as trust services. The goal, in the long term, is therefore the complete integration of the services related to the SSIs within the framework of the trust services currently governed by eIDAS [27]. The Italian strategy, prepared by the Ministry of Economic Development, in the field of blockchain, highlights the advantages of the SSI model also, with a series of proposals that have, among others, the goal to providing Italy with a regulatory framework that is competitive with those of other countries; increase public and private investments in Blockchain technologies and promote information and awareness among citizens; improve efficiency and effectiveness in interacting with the PA through the adoption of the Once-Only principle and decentralization; promote European and international cooperation, with the adoption of the common European infrastructure by EBSI [31].

### 4.2.2. European SSI Framework

The European Self-Sovereign Identity Framework (ESSIF) is an initiative designed to make interoperable the various SBS initiatives developed at national level in each EU Member State [31]. The eSSIF-Lab project, funded by the EU, aims to strengthen the reliability of the Internet with digital identities, through the development and adoption of SSI technologies. The ultimate goal is to promote the widespread adoption of SSI as a next generation, open and reliable digital identity solution for faster and more secure electronic transactions via the Internet and in real life [32][33].

# 5. Blockchain

The blockchain is a shared and immutable ledger, the entries of which are grouped into concatenated blocks in chronological order. It facilitates the transactions registration process and the traceability of data on a network, ensuring its integrity thanks to the use of cryptography. Only authorized network members can access the ledger. A blockchain network can, among other things, track orders, payments, accounts, production and much more. Since the data is seen uniquely by the various members, they can access all the details of an end-to-end transaction, thus generating greater reliability, security and efficiency [34].

## 5.1. Components of a blockchain

A blockchain network is made up of nodes, transactions, blocks, ledger and Hash. Nodes are the members of the blockchain and are physically represent each participant's servers. Transactions consist of data that represent the values being exchanged and that need to be verified, approved and then archived. Blocks represent a set of transactions, grouped to be verified, approved and then stored by the participants in the blockchain. The ledger is the register in which all the transactions carried out are recorded in an immutable way, with maximum transparency and in chronological order. It consists of the set of blocks that are linked together by means of a cryptographic function and thanks to the use of hashes. The Hash is a non-invertible operation, which allows you to transform a text string into another of arbitrary length (regardless of the length of the original string). The Hash uniquely and securely identifies each block, without allowing to trace the text from which it was generated [35].

## 5.2. Functioning of a blockchain

The blockchain works like this: the cryptographic keys of the sender and those of the receiver are created in preparation of the transaction. The transaction is created, containing information about the sender, the receiver and the cryptographic key. In addition to these, the information you want and even conditions can be reported. The transaction starts with the digital signature and public key of each participant. The transaction becomes part of a block, which can also include other transactions. Each block has a Hash, which records all information relating to the block itself. A Hash with the information of the previous block will allow to create the chain and link one block to the previous, forming a chain. The blocks certify the time - via timestamps - and the sequence of transactions and connect to each other in a secure way, in order to avoid that one of them is altered or inserted between two existing blocks. So each additional block reinforces the verification of the previous block. This eliminates the possibility of tampering and creates a transaction log that all members of the network can trust. The block is verified and approved by the blockchain network. Finally, the block is added to the chain. From this moment the transaction is complete and is present and accessible in the archives of each participant, therefore on all the nodes of the blockchain. The blockchain is structured in such a way as to automatically update itself on each of the clients participating in the network. All the operations carried out must be automatically confirmed by all the individual nodes, using cryptographic software, which verifies a packet of data defined as a private key, used to sign the transactions. In this way, the digital identity of those who authorized them is guaranteed [34][35].

## 5.3. Blockchain at the service of SSI

There are some implementations of SSI based on blockchain, in which the data is not stored, but only the keys of the cryptographic algorithms that allow the exchange of data in a secure and unassailable way. This logic not only makes the system fully compliant with regulations, but also avoids exposing oneself to the risk that such information, despite being encrypted with the most sophisticated algorithms, can be decrypted and therefore stolen. More sophisticated implementations of SSI, therefore, negate this risk as well [36].

# 6. SSI and Blockchain to access services of a Public Administration

The Public Administration is a very complex machine and it is plagued by excessive bureaucracy. It is often a fragmented reality, whose organizational structures are disconnected and do not share data with each other. These characteristics collide with the needs for efficiency and effectiveness required by a society in constant evolution and in which technology has accelerated the pace. Due to its characteristics, the blockchain technology can be one of the best solutions to be able to overcome the inefficiencies in current systems and increase the effectiveness of the service to citizens. In fact, in addition to guaranteeing high data protection, it introduces elements to increase the levels of transparency and traceability of transactions, such as to determine a substantial decrease in fraud and corruption. Consequently, citizens would have an incentive to place more trust in institutions. With the blockchain both parties - citizens and businesses and PA - derive benefits: on the one hand, citizens and businesses have a certified identity to be able to relate to the

PA; on the other hand, the PA must no longer possess citizens' data in centralized structures, more vulnerable to cyber attacks. The added value of this transformation is realized by constituting a new model for the management of one's data: in traditional systems, personal data are managed centrally by a plurality of institutional subjects, which often do not integrate with each other. Citizens do not interact with a single government counter, but are forced to provide their data to each PA they contact. Sometimes the set of SPID data to be shared is designed for access to a variety of services. This means that in some cases the user must share data that are actually superfluous, in relation to the single service he would like to access. The SSI, seen as an evolution of SPID, solves this problem, as it allows the user to share only the data that is necessarily needed for access to a particular service, and to select any other data that it deems appropriate to share. In this context, the blockchain guarantees the security of the tracing of requests, by the various PA platforms, for access to user identity data.

## 7. Case study

For this work, a system that allows access to a PA platform, via Self-Sovereign Identity (simulated) was implemented. A blockchain is used to store the accesses. The platform asks the citizen which data to share, by their identity. Then it makes a request to the identity manager, which verifies that the requesting platform is actually a blockchain node, provides the requested data and stores the transaction in the blockchain itself. The identity manager uses several databases to manage various data. A blockchain ledger is used to store blocks of transactions.

### 7.1. Implementation

For the implementation, the Python language was chosen, object-oriented, based on high-level data structures, and suitable for developing distributed applications, among other things.

Each block can contain from one to N transactions. Each transaction represents the access of a platform to the data of an identity.

A series of information is recorded for each block, including the Hash of the previous block and that of the block itself (necessary to ensure the consistency of the entire chain), the timestamp, the Merkle Root (which is a recursive concatenation of the Hashes of the transactions), the number of transactions contained in the block and the list of transaction identifiers.

All the other data related to transactions are stored in a dedicated database. In it, the fiscal code of the identity is not stored in clear text, but a Hash is applied to the combination of it with other data.

```
class Transazione(object):

    def __init__(self, idNodo, cfUtente,
                 informazioni=None):
        self.idNodo = idNodo
        self.informazioni = informazioni
        self.timestamp = int(datetime.timestamp(
            datetime.now().replace(microsecond=0)))
        self.datetime = datetime.fromtimestamp(
            self.timestamp)
        if cfUtente:
            self.cfUtente = cfUtente
            self.idTransazione = hashlib.sha256(
                (self.idNodo + self.cfUtente +
                 str(self.timestamp)).encode('utf-8'))
                       .hexdigest()
            self.hashNodoUtente = hashlib.sha256(
                (self.idNodo + self.cfUtente)
                    .encode('utf-8')).hexdigest()
```

**Figure 1:** creation of a transaction

```
class Blocco(object):

    def __init__(self, ultimoBlocco = None):
        if ultimoBlocco:
            self.indice = ultimoBlocco.indice + 1
            self.hashPrecedente = ultimoBlocco.hashBlocco
        else:
            self.indice = 1
            self.hashPrecedente = ''
        self.versione = versione
        self.merkleRoot = None
        self.timestamp = None
        self.numeroTransazioni = 0
        self.transazioni = []
        self.hashBlocco = None
```

**Figure 2:** initialization of a block

The block is completed with the Hash generated on the concatenation of the other information contained therein, before being added to the chain. It is also possible to consult the history of accesses made to the manager by a platform, to the various platforms by a citizen and in detail by a citizen to a specific platform. These functions are necessary to fulfill the typical needs of the PA, related to any requests for access to documents, as well as to the Audit, the aim of which is to objectively verify that the management of the service complies with the provisions of the law.

## 8. Conclusions

An overview of the relevant European and Italian regulations was made. The regulatory and technical aspects of SSI and Blockchain have been described. And through a case study, it was illustrated how their combination, applied to the context of the PA, allows for optimal privacy management. In fact, on the one hand, the blockchain guarantees the transparency and immutability of the data. On the other hand, the user can choose which data to share with the platform to which he accesses. The system could evolve by allowing access to private platforms as well. A smart-contract, that is a program stored on the blockchain, and executed under certain conditions, in

```
39    def merkleTree(self):
40        step = 1
41        numero = self.numeroTransazioni
42
43        temp = list()
44        final = list()
45
46        for transazione in self.transazioni:
47            final.append(transazione.getHash())
48
49        while numero > 1:
50            step += 1
51
52            temp.clear()
53
54            for i in range(0,numero-1,2):
55                temp.append(hashlib.sha256((
56                    final[i] + final[i+1])
57                    .encode('utf-8')).hexdigest())
58
59            if numero > 1:
60                if numero % 2 == 0:
61                    numero = numero//2
62                else:
63                    temp.append(hashlib.sha256((
64                        final[numero-1] + final[numero-1])
65                        .encode('utf-8')).hexdigest())
66                    numero = numero//2 + 1
67
68            final = temp.copy()
69
70        return final[0]
```

**Figure 3:** Merkle Tree Algorithm

```
34    def completaBlocco(self):
35        self.merkleRoot = self.merkleTree()
36        stringa = str(self.indice) + self.versione +
37            self.hashPrecedente + self.merkleRoot +
38            str(self.timestamp) + str(self.numeroTransazioni)
39        self.hashBlocco = hashlib.sha256(
40            stringa.encode('utf-8')).hexdigest()
```

**Figure 4:** completion of a block

order to automate the execution of a workflow, would regulate access, guaranteeing preferential channels for the PA platforms, compared to private managers.

## References


[1] QualitaPA (2014) *E-government*, URL: http://qualitapa.gov.it/sitoarcheologico/relazioni-con-i-cittadini/open-government/e-government/index.html

[2] Ciccarella, G., Giuliano, R., Mazzenga, F., Vatalaro, F., Vizzarri, A. (2019). Edge cloud computing in telecommunications: Case studies on performance improvement and TCO saving. 4th International Conference on Fog and Mobile Edge Computing, FMEC 2019, 2019, pp. 113–120.

[3] Ciccarella, G., Vatalaro, F., Vizzarri, A. (2019). Content delivery on IP network: Service providers and TV broadcasters business repositioning. 3rd International Conference on Recent Advances in Signal Processing, Telecommunications and Computing, SigTelCom 2019, 2019, pp. 149–154.

[4] R. Giuliano, "The Next Generation Network in 2030: Applications, Services, and Enabling Technologies, 2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), 2021, pp. 294-298.

[5] Cardarilli, G. C., L. Di Nunzio, R. Fazzolari, D. Giardino, M. Re, A. Ricci, and S. Spanò. 2022. An FPGA-Based Multi-Agent Reinforcement Learning Timing Synchronizer. Computers and Electrical Engineering 99.

[6] Cardarilli, G. C., L. D. Nunzio, R. Fazzolari, A. Nannarelli, M. Petricca, and M. Re. 2022. Design Space Exploration Based Methodology for Residue Number System Digital Filters Implementation. IEEE Transactions on Emerging Topics in Computing 10 (1): 186-198. doi:10.1109/TETC.2020.2997067.

[7] Bonanno, F., Capizzi, G., Lo Sciuto, G. , Napoli, C. (2015). Wavelet recurrent neural network with semi-parametric input data preprocessing for micro-wind power forecasting in integrated generation Systems. In 2015 International Conference on Clean Electrical Power (ICCEP) (pp. 602-609). IEEE.

[8] Capizzi, G., Lo Sciuto, G., Woźniak, M., Damaševicius, R. (2016). A clustering based system for automated oil spill detection by satellite remote sensing. In Artificial Intelligence and Soft Computing: 15th International Conference, ICAISC 2016, Zakopane, Poland, June 12-16, 2016, Proceedings, Part II 15 (pp. 613-623). Springer International Publishing.

[9] Magistris, G.D. , Rametta, C. , Capizzi, G. , Napoli, C. (2021) FPGA Implementation of a Parallel DDS for Wide-Band Applications. CEUR Workshop Proceedings, 3092, 12-16.

[10] Capizzi, G., Lo Sciuto, G., Napoli, C., Woźniak, M., Susi, G. (2020). A spiking neural network-based long-term prediction system for biogas production. Neural Networks, 129, 271-279.

[11] Avanzato, R. , Beritelli, F. , Russo, M. , Russo, S. , Vaccaro, M. (2020). YOLOv3-based mask and face recognition algorithm for individual protection applications. CEUR Workshop Proceedings, 2768, 41-45.

[12] European Parliament (2022) *Digital Agenda for Europe*, URL: https://www.europarl.europa.eu/factsheets/en/sheet/64/un-agenda-digitale-europea

[13] European Union (2020) *Europe's moment: Repair and Prepare for the Next Generation*, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A456%3AFIN

[14] Brandizzi202166, author=Brandizzi, N. , Bianco, V. , Castro, G. , Russo, S. , Wajda, A. (2021), Automatic RGB Inference Based on Facial Emotion Recognition. CEUR Workshop Proceedings, 3092, 66-74.

[15] Ministro per la Pubblica Amministrazione *Agenda digitale*, URL: http://www.funzionepubblica.gov.it/digitalizzazione/agenda-digitale

[16] Presidenza del Consiglio dei Ministri (2015) *Strate-*

*gia per la crescita digitale 2014-2020*, URL: https://presidenza.governo.it/GovernoInforma/ documenti/piano_crescita_digitale.pdf

[17] Dat, N.N. , Ponzi, V. , Russo, S. , Vincelli, F. (2021). Supporting Impaired People with a Following Robotic Assistant by means of End-to-End Visual Target Navigation and Reinforcement Learning Approaches. CEUR Workshop Proceedings, 3118, 51-63.

[18] Ciancarelli, C. , De Magistris, G. , Cognetta, S. , Appetito, D. , Napoli, C. , Nardi, D. (2023). A GAN Approach for Anomaly Detection in Spacecraft Telemetries. Lecture Notes in Networks and Systems, 531 LNNS, 393-402, doi: 10.1007/978-3-031-18050-7_38.

[19] Napoli, C. , De Magistris, G. , Ciancarelli, C. , Corallo, F. , Russo, F. , Nardi, D.(2022). Exploiting Wavelet Recurrent Neural Networks for satellite telemetry data modeling, prediction and control. Expert Systems with Applications, 206, 117831, doi: 10.1016/j.eswa.2022.117831.

[20] Aureli, R. , Brandizzi, N. , Magistris, G.D. , Brociek, R.(2021) A Customized Approach to Anomalies Detection by using Autoencoders. CEUR Workshop Proceedings, 3092, 53-59.

[21] Ministero per l'innovazione tecnologica e la transizione digitale (2022) *Identità digitale*, URL: https://innovazione.gov.it/progetti/identita-digitale-spid-cie/

[22] Agenzia per l'Italia digitale (2022) *SPID - Sistema Pubblico di Identità Digitale*, URL: https://www.agid.gov.it/it/piattaforme/spid

[23] SPID Helpdesk *Quali sono le differenze tra i tre livelli di sicurezza?*, URL: https://helpdesk.spid.gov.it/ knowledgebase.php?article=14

[24] Agenzia per l'Italia digitale *Il Regolamento UE n° 910/2014 - eIDAS*, URL: https://www.agid.gov.it/it/piattaforme/eidas

[25] Official Journal of the European Union (2014) *Regulation UE No 910/2014 of the European Parliament and of the Council*, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32014R0910

[26] Agenzia per l'Italia digitale *Nodo eIDAS italiano*, URL: https://www.agid.gov.it/it/piattaforme/nodo-eidas-italiano

[27] Agenda Digitale Europea (2021) *Self Sovereign Identity, perché il futuro dell'identità digitale passa dalla blockchain*, URL: https://www.agendadigitale.eu/ cittadinanza-digitale/data-management/self-sovereign-identity-perche-il-futuro-dellidentita-digitale-passa-dalla-blockchain/

[28] Nitin Naik, Paul Jenkins *uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain*, URL: https://pure.port.ac.uk/ws/portalfiles/portal/25003650 /uPort_SSI_DrNitinNaik.pdf

[29] Ministero dello sviluppo economico *Blockchain - Consultazione pubblica*, URL: https://www.mise.gov.it/index.php/it/consultazione-blockchain

[30] Marcotrigiano, V. , Stingi, G.D. , Fregnan, S. , Magarelli, P. , Pasquale, P. , Russo, S. , Orsi, G.B. , Montagna, M.T. , Napoli, C. , Napoli, C. (2021). An integrated control plan in primary schools: Results of a field investigation on nutritional and hygienic features in the apulia region (southern italy). Nutrients, 13, 9, 3006, doi: 10.3390/nu13093006.

[31] Annalisa Casali (2021) *Self Sovereign Identity: norme, applicazioni, benefici e sviluppi futuri*, URL: https://www.blockchain4innovation.it/tecnologie/self-sovereign-identity-norme-applicazioni-benefici-e-sviluppi-futuri/

[32] European Commission *European Self Sovereign Identity Framework Laboratory*, URL: https://cordis.europa.eu/project/id/871932

[33] eSSIF-Lab *European Self-Sovereign Identity Framework Lab*, URL: https://essif-lab.eu

[34] IBM *Il successo nell'utilizzo della blockchain inizia da qui*, URL: https://www.ibm.com/it-it/topics/what-is-blockchain

[35] Mauro Bellini (2022) *Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*, URL: https://www.blockchain4innovation.it/esperti/ blockchain-perche-e-cosi-importante/

[36] LinkedData Center *La blockchain a servizio dell'Identità digitale*, URL: https://it.linkeddata.center/b/self-sovereign-identity/