TIZIANA CROCE*

*From Bitcoin to the Internet of Things: the role of the Blockchain***

Summary: Introduction. 1. Digital currency categorization – 1.1 Technology – 2. Looking for a definition – 2.1 *Quid Juris?* – 3. Outlook – 4. The Internet of Things – 5. The Blockchain – 6. Blockchain and personal data protection

Introduction

The last few decades have been marked by a groundbreaking digitalization process, that is, the information conversion from its original form into that expressed in binary numbers. Computer-processed information is subsequently converted into analog format, so that it can be used. Recently, information is created directly in digital format. Nowadays, everything concerning information generation and transmission deals with the use of computers.

Currency, which is an information carrier *par excellence,* has followed this trend more slowly and even today it is still in the early stage of the digitalization process. Every day a huge amount of analog currency is handled by IT platforms and the use of so-called digital currency is increasingly widespread, but the next step, which is the direct generation of digital currency, has not been accomplished yet.

In 2009, digital currency took shape for the first time and in the same year a protocol governing the generation and transfer of Bitcoin[1] was implemented by an unknown programmer or group of programmers.

* *Professore Aggregato di Informatica giuridica presso l'Università degli Studi di Camerino.*

** *Contributo sottoposto positivamente al referaggio secondo le regole del double blind peer-review.*

[1] I. W. SCHIAROLI, *Dark Web & Bitcoin*, Laterza 2012, p. 16 and subsequent "In 1998 the concept of cryptocurrency was first debated in the mailing list of cypherpunks, who are an influential group of cryptographers

Bitcoin is based on the Blockchain digital structure, which essentially includes a distributed database, a kind of ledger using peer-to-peer technology, namely a list of events where all the operations performed are recorded and controlled by users in order to prevent changes to the contents of the shared register without the consent of Blockchain users.

The Blockchain can definitely be applied in the field of personal data protection, since there are many people and companies that must preserve and ensure information integrity. From this point of view, using a storage system with Blockchain technology would even be more effective than a traditional management model.

The Internet of Things is one of the new frontiers in the use of the Internet: things, objects and tools now acquire intelligence, namely the ability to collect and communicate information. More specifically, the terms "thing" and "object" refer to categories such as devices, equipment, systems, materials and tangible items, works and goods, machinery and tools.

The sudden development of the Internet of Things' technology and the resulting speed and amount of data collected by sensors installed in various smart objects enable information to be turned into data or, more specifically, into big data through datafication and big data analytics, threatening security and privacy. Why not use the Blockchain technology even in this field?

---

inside the digital world, known for waging battles that gave us the possibility to use technologies often considered unpopular by power systems, such as Skype. Among these are the inventor of Bit Torrent, Bram Cohen, the inventor of the peer-to-peer, Julian Assange of WikiLeaks and Sathoshi Nakamoto, the future creator of Bitcoin and an expert of cryptocurrency and e-money. However, the first who talked about cryptocurrency was not Nakamoto but Wei Lai, who proposed a sort of digital currency called *b-money*, aimed at encouraging e-commerce. Some features of this currency, such as non-traceability and autonomy from central oversight, are deemed to be essential elements in conceiving the idea of Bitcoin, which is actually one of the first forms of crypto-currency. Satoshi Nakamoto started debating about the project in 2007 and two years later he finally accomplished the mission, officially becoming the founding father of a new digital currency, Bitcoin, together with the software project of the same name developed for its use. We do not know much about him; it is common belief that Satoshi Nakamoto could be a pseudonym, an identity specifically created to hide the real Bitcoin creator or group of creators. Nevertheless, in 2009 Bitcoin appeared for the first time. Building upon the notion that money is any object, or any sort of data accepted as payment for goods and services in a given country or socio-economic context, Bitcoin was designed around the idea of using cryptography to control the creation and transfer of money, rather than relying on central authorities. As a result, in no way can central authorities manipulate Bitcoin value; on the contrary, since it is created through a peer-to-peer system, a distributed architecture, Bitcoin can exist and be used without central oversight […]"

Consequently, it should be pointed out that current technological progress obsoletes what was still widely unknown yesterday. It may happen that some cutting-edge technologies based on other ones go largely unnoticed at first and then constitute a necessary prerequisite for the development of other services at a later time.

1. *Digital currency categorization*

There are distinct digital currency schemes categorized by the way they interact with real currencies and the economy: the so-called closed virtual currency scheme, mostly used within gaming platforms; the unidirectional virtual currency scheme, in which the real currency is converted into the virtual one, which can be used to purchase both virtual and real goods and services, but cannot be exchanged back into real money; lastly, the bi-directional virtual currency, which is comparable to any other real currency, for it can be bought with and sold back for legal tender. Bitcoin belongs to the last category.

1.1 *Technology*

The issuance and circulation of Bitcoin use a peer-to-peer technology similar to that of digital file sharing, through double-entry systems with digital keys both in anonymous and public form, so that any Bitcoin contains the entire set of transactions made. Transactions are verified by the so-called mining process, namely an extremely complex mathematical verification of the set of transactions, voluntarily performed by persons who receive a specific number of new Bitcoin units as a reward for every solution found. Within the Bitcoin system, this computing and verification activity is the only one authorized to generate new amounts of currency.

The Bitcoin growth rate is evaluated through algorithms able to determine the Bitcoin maximum number, currently equal to 21 million units, which may be created should their growth progress according to the geometric rate resulting from said complex computing operations. The maximum limit of Bitcoins in circulation is expected to be reached in 2040[2].

[2] Satoshi NAKAMOTO, *Bitcoin*: *A Peer-to-Peer Electronic Cash System,* in *https://bitcoin.org/bitcoin.pdf.*

Bitcoin circulation also involves other calculations made by network nodes which, by using the cryptographic protocol, verify and validate payments, thus ensuring the reality of the transactions made. From this perspective, the Bitcoin-based value represents the service offered, not the good exchanged. The generation of six confirmation blocks validates the transaction, which is verified by peers through the application of a *hash* function in order to receive an alphanumeric string called *digest*, which changes according to the variability of the file elements. Every operation is validated with a timestamp to verify whether the activities have been performed according to the established time sequence and to prevent the transferor from carrying out a new transaction using a unit he/she has already transferred[3].

The Bitcoin system uses distributed database nodes and cryptography to face the so-called double-spending, generally considered as the most critical issue concerning digital currency. A central body commonly verifies whether the currency has already been spent. In this case, distributed systems are used to prevent double-spending. Bitcoins can be saved in a digital wallet in the user's PC or in specific storage servers. This system is highly reliable because the nodes cryptographically verify the transactions, making them irreversible.

2. *Looking for a definition*

Once the Bitcoin phenomenon has been described, the focus must be shifted onto a few legal issues with the purpose of explaining and evaluating, even with an interpretative effort, its economic and social impact.

Can Bitcoin be considered as a new legal tender? With regard to the concept of currency, reference to both statist and economic theory is needed.

The statist theory establishes that the State has power over currency, for it is the creator and guarantor and, as such, currency is able to discharge pecuniary obligations and cannot be declined as a payment method. Since Bitcoin has never been declared as a legal

[3] I. W. SCHIAROLI, *Dark Web & Bitcoin*, op. cit, p. 20 and subsequent "The entire Bitcoin monetary system is run by a database located among nodes, which is able to record all transactions made within the network without being governed by an external or central authority. Network nodes track and control any transaction-related information and provide for safety verification, thus ensuring the bitcoin is spent by its current owner".

tender by the State, it has no discharging effect, unless the creditor accepts this payment method.

According to the economic theory, currency has three main functions: it is a store of value, serves as a control unit and represents a medium of exchange.

Bitcoin cannot constitute a store of value because of its significant volatility, namely the highly variable purchasing power it has over time and the unpredictable nature of its convertibility into scriptural money. Bitcoin can undoubtedly promote circulation of wealth and trading, but its acceptance as a medium of exchange depends only on the parties' will. Since it has no legal status, Bitcoin cannot acquire the status of legal tender by default. The possibility that Bitcoin can represent an evaluation method is negligible, for its users calculate the equivalent value of goods and services relying on the official currencies as a result of the considerable exchange rate turbulence.

2.1 *Quid Juris*?

Can Bitcoin be considered as electronic money? Directive 2009/110/EC[4] gives a definition by stating that "[…] electronic money means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC[5], and which is accepted by a natural or legal person other than the electronic money issuer […]". Bitcoin is certainly a "dematerialized" unit of account, electronically stored and accepted within e-commerce, but unlike electronic money, as defined in the aforementioned Directive, its equivalent value cannot be calculated on the basis of a monetary amount expressed in a previously assigned official currency. The unit of account is merely virtual, has no extrinsic value and is based on the fact that others accept it in exchange for goods and services. It is also to be noted that there is no authority responsible for the creation of a Bitcoin fund. Actually, as mentioned before, there is a

[4] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009, on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, L. 267/7, 10/10/2009.
[5] Directive 2007/64/EC of the European Parliament and of The Council of 13 November 2007, on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC , L. 319/1, 5/12/2007.

method to automatically generate new bitcoins: through the mining process, an activity strictly connected to the sources that so-called miners are able to deploy to solve specific mathematical issues. This results in the lack of a constant redeemability as per article 11 of the above Directive[6]. It is also worth noting that, as long as Bitcoin is not broadly used but represents a solution for a limited range of goods and services, it will never be considered as electronic money, since it does not comply with the requirements of said Directive. Anyway, Bitcoin can be considered as a payment method, although taking place within a voluntary and consensual environment and constantly adapting to social and economic changes[7]. The crypto-currency system cannot apparently fall under existing legal categories, for it can be conceived as a unit of value, a medium of exchange and a commodity at the same time[8].

3. *Outlook*

The most significant improvements in the current Bitcoin usage scenarios and the future outlook are probably meant to be marked by the promising technology supporting the complex Bitcoin frame. Actually, most analysts agree in considering the distributed ledger technology, namely the Blockchain, as the key innovation enabling the payment system to

[6] Art. 11 Dir. 2009/110/EC "Member States shall ensure that, upon request by the electronic money holder, electronic money issuers redeem, at any moment and at par value, the monetary value of the electronic money held".

[7] Directive 2007/64/EC "…any personalized device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used by the payment service user in order to initiate a payment order".

[8] According to literature, some think that bitcoins belong to the category of atypical financial products. Even if they do not fall within the scope of jurisdiction of the Finance Consolidation Act for atypical financial products, they have the same features such as capital expenditure, financial performance expectancy and the risk-taking related to such expenditure. These characteristics would allow for the application of the public offer rules set forth by articles 94 and subsequent of the Finance Consolidation Act, submitting issuers to the inspectoral, restrictive and disciplinary powers of CONSOB and the Market Competition Authority, which has recently taken restrictive and disciplinary measures against a bitcoin issuer by classifying such activity as bad commercial practice according to the Consumer Code. In 2012 Virtual Currencies Schemes paper, the European Central Bank pointed out some potential risks for virtual currencies, such as price, financial and payment systems' stability, lack of regulation and reputational risk for central banks. In 2014, the ECB issued another paper on virtual currencies in order to promote a regulatory convergence on a European scale, providing a thorough explanation of the risks resulting from the use and detention of virtual currencies and proposing the long-term creation of an harmonized regulatory framework to assign virtual currency operations to authorized subjects and define capital requirements, market participants' governance and customer account segregation. As for the short term, it called for the urgent need to mitigate the risks resulting from the interaction between virtual currency schemes and regulated financial services, and invited national supervising authorities to discourage intermediaries from buying, holding or selling virtual currencies.

run completely decentralized and with no need of an intermediary[9]. The underlying concept of such distributed multi-agent system undoubtedly represents a smart solution made possible by an integrated approach able to take advantage of the contact points of modern cryptography and peer-to-peer computing. However, this new technology, which is mostly appreciated for its effectiveness against double-spending that affects all payment methods lacking support from financial institutions or centralized services, may lead to far-reaching changes in a wide range of fields by giving more valuable and lasting contributions within web-based solution applications.

The paradigms underlying the construction of the Bitcoin system[10], properly overhauled and adjusted for the particular situation, may not only allow the issuance of unchangeable certifications even in relation to public events (digital truth), but also enhance the speed, efficiency and security of transferring any on-line digital asset: transferable securities, sport bets and confidential information requiring authenticity certification[11]. In the light of a not-too-distant future, improved design and development of flexible, scalable, open-source[12] and fully auditable platforms for big data[13] commodity storage should be promoted, as well as the implementation of encrypted messaging networks, less vulnerable than the current email services[14].

Significant development shall be triggered in different fields such as smart contracts[15] and smart property[16], as well as decentralized autonomous organizations[17] and machine-to-

[9] SWAN, *Blockchain, Blueprint for a New Economy,* p. 10 and subsequent, Sebastopoli, CA, 2015.
[10] It is the frequently mentioned distributed timestamp system, known as Blockchain, namely computing according to a proof-of-work scheme and public key cryptography.
[11] Worth mentioning are: the issuance of passports, driving licenses and diplomas, the constant updating of the criminal record, vehicle and land registers, as well as the procedures relating to the management of systems of identity and digital evaluation in a context of delegative democracy.
[12] Open-source is software whose source code is disclosed by its right holders in order to promote a free analysis and enable independent programmers to make changes and extensions.
[13] The term "big data" is used to describe a data set so large, fast or complex that it requires advanced analytical methods to extract value.
[14] E.g. the communication protocol called *Bitmessage.* Wikipedia: "Bitmessage is a decentralized, encrypted, peer-to-peer, trustless communication protocol that can be used by one person to send encrypted messages to another person or multiple subscribers. Bitmessage encrypts each user's message inbox using public-key cryptography and replicates it inside its P2P network, mixing it with inboxes of other users in order to conceal user identity, prevent eavesdropping and allow the network to operate in a decentralized manner. The Bitmessage communication protocol avoids sender-spoofing through authentication and hides metadata from wiretapping systems".
[15] G. SARTOR, *Gli agenti software e la disciplina giuridica degli strumenti cognitivi*, in *Diritto dell'informatica e dell'informazione*, 2003, p. 55 and following: "[..] they are math-based negotiable schemes involving a high-level

machine communication systems, since these are important components of a wider but increasingly less futuristic scenario featuring cutting-edge ICT interconnected platforms and cyber-physical systems[18], whose contact point can be found in their common reference to the Internet of Things[19].

The overall consideration of such interesting evolution probably leads to the conclusion that Bitcoin is meant to be the cornerstone of new complex peer-to-peer distribution systems basically oriented to offer a wide range of services such as asset management, industrial automation, smart power grids, smart cities and immotics.

Without necessarily assuming that the Bitcoin purpose to replace the official currencies is no more reliable and doomed to fail, the most likely scenario seems essentially related to the rise of one or more killer applications based on the decentralized ledger ecosystem, by means of which these remarkable innovation shall penetrate the market and overcome the existing technologies, paving the way to a new batch of secondary applications.

Looking at it as a solution seeking for a problem, that is the initial stage of a broader process of social, communicative, financial and technological experimentation where the current economic system is not replaced but reformed, Bitcoin would lose its destabilizing, liberal and iconoclastic aura – drawing its original inspiration from crypto-anarchism[20] –

---

of automation in the improvement, monitoring and enforcement process. To provide a definition system-wise could be difficult as well. According to literature, smart contracts can probably fall under the digital contract's category, more specifically under the cybernetic contract's one, where specific software agents are widely used".

16 The term "smart property" means all the goods whose usage, access or transfer of title is governed by a "smart contract". Primitive forms of smart property are represented by cars equipped with immobilizers and smartphones with an encoded PIN: objects which can be used without being necessarily bought, but just booked using cryptography (e.g. car sharing services).

17 They are true virtual organizations with no legal status able to replicate corporate functions.

18 They are artificial calculation and communication mechanisms constantly, directly and dynamically interacting with the physical systems in which they are integrated.

19 The Internet of Things refers to infrastructures in which many sensors are designed to record, process and store local data, or to interact with each other by using both medium frequency radio technologies and electronic communication networks.

20 There is an almost hidden world which thrives on legal or illegal exchanges between individuals. This world is located within the World Wide Web and is defined as crypto-anarchism. To be a member of this world there is no need to be a geek, a professional hacker, and a hacktivist with political ideals, like Anonymous. The term crypto-anarchism was coined by the sci-fi writer known as Vernor Vinge to define that kind of anarchy existing and thriving on the Internet, which widely uses cryptography in relation to privacy matters or to prevent activists from being intercepted by governments. TOR is one of the most used encrypted networks ensuring complete online anonymity and the impossibility of tracking users. It is widely used in all those countries where a comprehensive monitoring of the network is established, like China, Iran and other

but it could nonetheless lead to solutions able to deeply change our societies and improve our lives.

4. *Internet of Things*

The constant development of technology increasingly affects the human activity, causing relevant effects in terms of autonomy and privacy. More specifically, the sudden rise of the Internet of Things[21] (a neologism referring to the expansion of the Internet over the world of objects) brought with itself the need to worry about data protection within a new and constantly evolving scenario[22].

The internet of things is aimed at making the digital world able to trace a map of the real one, thus giving a digital identity to things and places belonging to the physical environment. Therefore, it represents a possible evolution of the network use. Objects can be recognized and acquire intelligence thanks to their ability to communicate data concerning themselves and to access aggregate information relating to other persons: there are alarm clocks ringing in advance in case of traffic congestion, running trainers transmitting time, speed and distance in order to compete in real time with people on the other side of the globe, pill bottles alerting family members if they forget to take their medicine. All the objects, by means of the network connection, acquire an active role in leading to significant changes, especially by improving efficiency in everyday life. However, the complex nature of the IoT (Internet of Things) ecosystem not only depends on the enormous amount of

---

Middle East countries, since it enables many dissident groups to communicate with the outside world and to share files which may possibly threaten the relevant regimes. All these services are not only used by "wannabe terrorists" or kids who want to buy low-cost magic mushrooms. These services also meet the fundamental need for privacy the Internet can no longer guarantee since any message, byte and call are constantly monitored seeking for potential risks for governments; for example, businessmen, industrial secrets or political oppositions persecuted in some countries.

21 In 1999 the neologism "Internet of Things" was introduced by Kevin Ashton, a British researcher at the Massachusetts Institute of Technology, who was the pioneer of the theory of a world of sensors distributed everywhere and directly connected to the Internet. Among his many projects, worth mentioning is the Central Nervous System of the Earth, subsequently improved at Hewlett Packard labs in 2009 with the purpose of using smart sensors able to detect any environmental change, from pressure to temperature, through marine and atmospheric currents.

22 Antonello SORO, President of the Data Protection Authority, in presenting the 2015 annual report, declared that: *"From the most advanced forms of communication available on the Internet, we moved to the collaborative consumption of the so-called sharing economy, to the Internet of Things, to connected spaces where even objects can autonomously communicate with each other. The matter of data protection is intertwined with new realities which, like home automation or wearable technology, have widely increased the ability of collecting, storing and using information."*

data collected from different automatically communicating devices, but also on the possibility that said data can be shared by different persons such as device manufacturers, software developers, cloud providers, analysts and any individual other than the parties concerned. This is most likely to result in the users' lack of awareness in relation to their personal data processing, the person(s) in charge of the treatment and the purposes thereof[23]. Consequently, the IoT's impact on consumers' privacy against the backdrop of a social-oriented environment is not to be underestimated[24].

A further evolution of the Internet of Things is the Internet of Everything, which implies connecting devices not only to other devices but also to people, data and processes by means of an intelligent net which is able to listen, learn and give information[25]. Thus, the IoE can be seen as an implementation of the Internet of Things whenever the network is used for communication and data exchange by electronic devices only. The IoE is about interconnecting devices: smartphones, tablets, smartwatches, fitness trackers and common wearable devices, smart TVs, household appliances and more, people, processes and data. At the heart of it all, we have an intelligent network which is able to listen, learn and give

[23] Being connected to the network and integrated in the objects, sensors allow data transfer supported by the object's main characteristics. The object receives inputs which, from the outside world, communicate the acquired data to a server which, after having performed their processing, generates commands to be sent to the smart object so that it can give an output. Data individually collected are almost negligible but, if analyzed in large volumes, they can give an outline of models and trends which, together with other information sources, produce knowledge.

[24] In this regard, this year's edition of the Privacy Sweep 2016 international survey was devoted to the protection of privacy in the Internet of Things, with special emphasis given to differences and peculiarities of the single national laws at both a domestic and an international level. The initiative, coordinated by the Global Privacy Enforcement Network (GPEN), the international network born to strengthen cooperation among privacy authorities of several countries, took into account a wide range of devices: from smart meters to web-adjustable thermostats, from smart cars to blood pressure and heart rate-measuring smartwatches, from remote-controlled elevators to refrigerators warning users about food expiry date. The Italian privacy authority took part in the survey together with the corresponding bodies of 28 other countries, focusing its actions on home automation in order to assess the transparency level in the use of customer-related personal information and to ensure the compliance with personal data protection provisions by the relevant companies, including corporations.

[25] http:\\www.theconomy.it Dave EVANS, Cisco Chief Futurist: *"Internet of Things is just one of the four dimensions – people, process, data and things – we talk about in the Internet of Everything"*. In other words, interconnected things are just one side of a multifaceted revolution where the four main players are not islands in the sea, but they grow and reach their full potential due to their very interconnection. Cameras and parking sensors, for example, should be able to count the number of cars and persons going into stores; these data, matched with sensors placed on shopping trolleys and retail store traffic pattern analysis, shall enable "the system to forecast downtimes or lower inflow hours in order to automatically adjust the staff number according to peak hours. This could bring several benefits: customers will be happy to avoid long queues and retail stores will maximize staff productivity by selecting the right number of cashiers".

an answer in order to make the most different fields safer, easier and more reliable by offering new services and features.

Likewise, home automation (or domotics) – an interdisciplinary science based on studying new technologies to improve the quality of life in domestic and, more generally, human environments – plays a lead role in making appliances, devices and systems (and the home itself) more intelligent by offering nearly unlimited possibilities of data acquisition: from centralized, remote control of household appliances and device-based home access monitoring system to internal and external video surveillance.

Thus, there are a lot of implications closely related to personal data processing, all the more because we are talking about everyday aspects of living in our own house: a refrigerator connected to a network managing its content and performance can tell something at least about the eating habits of its owner but, even without connecting the appliance directly to the network and simply relying on energy consumption management, we can obtain eating-related information. That is, a bundle of personal data which has been processed for the simple fact of having been collected.

5. *The Blockchain*

The Bitcoin-generating mining activity must be validated by a proof of work[26]. As an output, the operation generates a Bitcoin block which is assigned to the first computer that solved the problem and is added to the logic chain – called blockchain – together with all related transactions[27].

The blockchain is basically a database with special features: every record consists of a node containing information and the single nodes are linked with each other so as not to be modified, and consequently jeopardize the whole chain. When this chain is replicated on several systems we have a distributed database. Since the blockchain is linked to the record of the single transactions of each node within the scope of Bitcoin or crypto-currency, it

[26] In the system proposed by Satoshi Nakamoto, the timestamp server is not centralized but distributed on a peer-to-peer network. The implementation of a timestamp server on a p2p network implies a proof-of-work system – that is, a system which ensures that every block (containing a group of transactions and a timestamp) belonging to the chain has been created by performing a given work and therefore it would not be convenient to change it, because changing one element would mean taking on another task and changing any subsequent element accordingly.

[27] R. BOCCHINI, *Lo sviluppo della Moneta virtuale*, in *Diritto dell'informatica e dell'informazione*, 2017, p. 38.

can be also seen as a ledger: as a matter of fact, the blockchain represents the technical infrastructure of Bitcoin and crypto-currency.

Despite its concise description (see footnote for a thorough explanation of this technology), the applications already developed and the ones yet to be engineered allow us to qualify the blockchain[28] as a service due to its capability of supplying a very wide range of

[28] With its versatility and groundbreaking potential, the Blockchain is experiencing a quick and relentless development. It has been analyzed by a recent study promoted by the European Commission (*Blockchain applications & services. Case study 68, Business Innovation Observatory*, April 2016) and constantly monitored by the European Banking Authority in *EBA Consumer Trends. Report 2016*, 21 June 2016, https://www.eba.europa.eu/-documents/10180/1360107/Consumer+Trends+Report+2016.pdf. Not surprisingly, therefore, models and variants of this digital tool are being experimented with in order to tailor it to the wide range of purposes for which it has shown great suitability. In fact, Blockhain 2.0 is already being discussed: as eloquently pointed out, "not only is the Blockchain industry an area of prodigious activity as of the fall of 2014", but also "*Blockchain 2.0 space is in development*", adding that "there are many different categories, distinctions and understandings of it, and standard classifications and definitions are still emerging". However, we shall hereinafter refer to the most basic and, in a certain way, proven technology which is the root of the bitcoin; in this sense, the Blockchain could be initially compared to a generally open source, new generation peer-to-peer network gradually expanding by adding new users. It is also defined as a distributed ledger technology, that is, a publicly shared registry owned by its very users – who all have a similar role – which is able to safely record and file all the transactions taking place inside of it and to prevent them from being subsequently modified. It should be duly noted that all of this occurs in a self-sufficient and autonomous way, with no need for centralized authorities and/or third parties to monitor and control access to this tool and the proper execution of the transactions recorded on it. On the basis of these assumptions, the Blockchain functioning could be briefly described by analyzing the very technical solutions that it deploys to solve the core issues arising from its self-sufficient, decentralized and public framework (which are basically limited): the unique – even though generally anonymous – identification of the subjects performing transactions; the suppression of the risk that users may unduly perform multiple operations having the same digital object (transferring the same amount of BTC twice, for instance); finally, transaction safety in the absence of Third Trusted Parties supervising the process itself. As can be inferred from its literal meaning and not unlike P2P networks, the Blockchain is based on a peer-to-peer architecture shaped as a chain of blocks or nodes. Each user stores devices a digital copy of the whole ledger on his/her own hardware. The first chain block is called *Genesis Block*: each block could be compared to a sort of digital ledger where all the data capable of being translated into digital codes can be recorded, whether they are crypto currency transactions – as in the case of bitcoins – or contractual terms – as in the case of smart contracts. It can be therefore deduced that the Blockchain implies two different kinds of recordings: the first one is for single transactions containing the real digital data, while the second one is about creating a single block where transactions are gradually filed. With the first type of recording – also known as proof of stake – the technology concerned solves all the problems related to the unique (even though anonymous) identification of the users by providing each of them with a digital signature represented by an alphanumeric code to be used as a marking in every single operation. As long as bitcoins are concerned, in order to be the sole legitimate party to access his/her own portfolio, the user generates an asymmetric cryptography-based digital signature and, during money transfers, he/she creates a message containing the amount to be transferred by entering the public key of the recipient's digital signature. Moreover, the message is undersigned by the sender with his/her own private key, in order to assure the provenance of the message, the amount of money to be transferred and, ultimately, the recipient identity. But this is not enough yet. The final improvement provides that transactions are submitted to the second type of recording which, by adding a proper timestamp, occurs after the creation of new chain blocks. These new blocks are then duplicated in the database of every other network node and even on the personal computer of each Blockchain user, thus becoming irreversible and unchangeable. In this way there is no risk for users to perform a transaction with the same digital content more than once. More specifically, each new block is added

services.

This represents a central point, since the development of Blockchain-based applications for the supply of services is currently one of the most important fields of Industry 4.0 and therefore one of the most relevant business sectors. This is the dawn of a new business paradigm – the fourth industrial revolution called Industry 4.0 –, where every productive step is managed and influenced by the information collected, from design to after-sale, by diverse enabling digital technologies intertwining productive systems, product and consumers[29].

---

by means of a mathematical procedure converting an amount of data in a lean digital string: it is the so-called hash, which becomes the digital identification seal of each block. This is the reason why any block other than the first one is positioned in a strict, not only linear but also chronological order; although fully independent, each block is linked to the previous one and assimilates its digital mark, so as to consolidate the whole chain at every node. New blocks are generated at the end of a complex operation having as an object the solution of sophisticated algorithms – the so-called proofs of work – which implies considerable computing resources and subsequent costs in terms of both hardware and electric consumptions, and usually rewarded with an economic advantage (in the case of bitcoins, for instance, the generation of a new block is rewarded with the allocation of some BTC). Moreover, the proof-of-work difficulty – currently limited to an average time of approximately ten minutes – is automatically increased by the Blockchain according to the number of miners and the computing power of each of them, in order to prevent single users from attempting sabotages, tampering or rising to power. In order to be added to the chain in a linear and chronological order and simultaneously be accepted by the other nodes, each new block shall keep an endogenous track of successfully passing both a proof of stake and a proof of work. Consequently, should a block be transformed or, more reasonably, should someone try to change it, that very block would be deemed invalid together with all the blocks thereafter and thus this newborn chain of irregular nodes would be suppressed. This happens because the Blockchain integrity is constantly verified at every proof of work, so that it is very unlikely that a sabotaged or flawed chain branch could last on some node for more than it takes to generate the next block (that is, for more than an average time of ten minutes). Furthermore, a copy of the whole Blockchain is always kept within every network node besides being stored on the personal computer or other device of each Blockchain participant; in this way, should a great number of blocks be destroyed, the Blockchain would survive anyway. Therefore, even the last one of the listed criticalities has been solved and everyone can easily understand the characteristics that are usually associated with the Blockchain: inherent reliability, constant transparency, unchangeability and almost utter resilience. Clearly, this technology makes unnecessary the presence of bodies, parties or authorities keeping the ledger and monitoring the activity on the network and data, which are secured in a fully endogenous way.

[29] The term *Industry 4.0* shows a tendency of industrial automation at integrating new production technologies to improve working conditions and increase systems' productivity and quality. Industry 4.0 relies on the concept of smart factory, which lies in three basic assumptions: smart production, that is new production technologies able to interface all the elements of the production cycle such as operator, machines and instruments; smart services, that is all the IT and technical infrastructures allowing for system integration and the whole range of structures allowing for the proactive integration of companies (supplier – customer), mutually and with external structures (streets, hubs, waste disposal management, etc.); smart energy, that is keeping a closer eye on energetic consumptions by creating even more performing systems and by cutting down energy waste according to the dictates of sustainable energy. The keystones of Industry 4.0 are cyber-physical systems (CPS), namely physical systems strictly connected with IT systems able to interface and cooperate with other CPS systems. This is the basic assumption of system decentralization and cooperation, which is strictly related with the notion of Industry 4.0.

The development of Blockchain-based applications may involve the deployment of artificial intelligence with a new set of huge possibilities for companies and final users alike.

It is now possible to develop applications for smart contracts, which are not real contracts but operations performed automatically when certain conditions are met: within the scope of a contract for electric power and gas supply, for instance, as soon as consumptions are read, payment is made. Smart contracts are still currently linked to the idea of financial transactions, but undoubtedly other applications expanding their scope of use could be developed in the future. One crucial point is transaction security, which could prevent any tampering with the operations.

Even identity profiling can be tackled through the Blockchain. Identifying a person can often be a difficult task, especially when it comes to virtual identities[30]. As a matter of fact, the Blockchain allows developing applications in order to make the identification of a person easier and to access such information safely. These are technological solutions that allow legitimate and previously authorized parties to ascertain someone's identity: in more practical terms, some companies need to clearly identify the individual in order to provide credit or services. Blockchain-based applications have already been developed, such as immigrants' identity management. Besides representing a legal obligation governed by the law and being an added value to the information managed by public administrations, digital record keeping can undoubtedly be implemented by means of the Blockchain technology along with the digitalization of the whole public administration system. We can easily figure out the fields of use, such as in telematics: as of now, telematics is based on different platforms depending on the jurisdiction (civil, administrative or fiscal) in order to simplify some aspects and to give more safety guarantees as for the information collected.

Blockchain applications are not independent of each other: on the contrary, they can be interlaced together (to interface identity management with payment system management, for instance), and this assumption actually came true in some sectors[31]. The inter-

[30] In Italy there is a Public System of Digital Identity (*Sistema Pubblico di Identità Digitale*, SPID), governed by Legislative Decree 82/2005 – Digital Administration Code, OJ 16/5/2005.

[31] *The province of Sulcis Iglesiente* "We developed the idea of certifying energy meter reading with Blockchain technology since we want our relationship with the customer to be based on absolute certainty of consumption with punctual and fair bills". This is a statement from Abbanoa's General Manager Sandro Murtas, an-

twining of miscellaneous services is another central point of the Blockchain.

6. *Blockchain and personal data protection*

Blockchain is by all means a groundbreaker, but still there are critical issues when it comes to personal data processing. The privacy and protection of personal data are cornerstones envisaged by articles 7 and 8[32] of the EU Charter of Fundamental Rights. In order to implement such principles, establish a digital single market and perform a legislative harmonization amongst the acceding countries, the European Union set forth Regulation 2016/679 (General Data Protection Regulation[33]) which shall apply – despite being already effective – as of 25/05/2018 in each Member State.

Applicable regulatory provisions are set forth in the Personal Data Protection Code (Legislative Decree no. 296/2003) and the principles underlying these provisions refer to Directive 1995/46 EC; in those years, personal data processing was strictly related to database utilization and the automatic processing of personal information. In today's society, digital data processing is the backbone of every interpersonal relationship beyond the mere physical contact. Our society is not just based on a relentless exchange of data, but it keeps on producing more and more of them, to use them by means of new and constantly-evolving techniques, technologies and purposes[34].

This regulatory framework calls for some reflection when it comes to protecting the personal data of the individuals forming the Blockchain. Among the cornerstones of per-

---

nouncing the introduction of the FLOSS-Certification program, the first Blockchain-based certification system for reading energy meters.

[32] *Charter Of Fundamental Rights Of The European Union* (2012/C 326/02), GUCE 26/12/2012,C 329/391, Article 7: *Respect for private and family life Everyone has the right to respect for his or her private and family life, home and communications.* Article 8*: Protection of personal data. 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.*

[33] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), GUCE 4/5/2016, L 119/1. This regulation marks a new season for European citizens' rights toward public administration and companies, since it represents an attempt towards harmonizing privacy rules on a European scale and it is aimed at developing the European digital single market by creating and promoting new services, applications, platforms and software. Among its cornerstones, the regulation provides for the accountability principle for all the parties involved in personal data processing.

[34] F. PIZZETTI, *Privacy e il Diritto europeo alla protezione dei dati personali*, Turin 2016, p. 10 and subsequent.

sonal data processing we can find the information note to the interested party and his/her prior consent. In order for the processing to be lawful, the person concerned must be provided with all the information necessary for them to form an opinion about the purposes and methods of data processing.

The Blockchain as we know it is based on trust; we talk about web of trust in encryption modes, such as Gnu Privacy Guard. Actually, for a substantial implementation of the Blockchain on every level we cannot disregard the importance of data protection provisions and the ways to fulfill them.

Anyway, these topics have been tackled only security-wise by increasing more and more IT infrastructure's security measures, often by means of encryption algorithms. However, since the concept of security is different from personal data protection, approaching the issue in this way is not legally sound. Since we are dealing with a relatively new scenario, we cannot rely on ready-made solutions or recipes. We should always perform a case-by-case assessment in order to identify the proper modalities and find the right solutions for a suitable level of compliance with new regulations.

Implementing specific policies is of the essence, but they should envisage other solutions aimed at granting personal data protection. The person concerned should be given prior notification about the processing of his/her own personal data in order to freely express his/her own consent.

The development of Blockchain-based applications should take into account the principles set forth in article 25 of the GDPR[35] governing data protection by design and by default. Such principle calls for appropriate technical and organizational measures complying with the applicable legislative provisions by adopting internal policies which meet data

[35] Art. 25:1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, at the time of both determining the means for processing and processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

protection cornerstones by design and by default.

In order to be used accordingly to the GDPR, the Blockchain technology should overcome two inherent issues: the data recorded in the Blockchain ledger, including users' and event owners' identification data, are disclosed and publicly available. This implies providing for the concerned person's consent, as per regulation. Data should be kept indefinitely to ensure the ledger authenticity: this case is governed by the data minimization principle, which implies, among the other things, a definition of data storage times.

There is no doubt about privacy by design being an advanced technique in the processing of personal data; similarly, the Blockchain-based technology will surely be able to manage the documentation requirements needed by data processing owners and controllers, because it allows managing all the operations performed on a given database in a knowledgeable and unchangeable way. Moreover, it will lead the implementation of the accountability principle as proposed by the WP29 at the European Commission by introducing *ex-ante* accountability mechanisms for data processing owners (that is, the need to adopt and implement suitable and effective safety measures)[36].

Risk should be assessed and safety measures should be enhanced on a permanent basis according to the latest technological advances or in case of proven inadequacy. General regulation is clear in defining the most suitable technical and organizational safety measures when facing risks of possible Data Protection Impact Assessment (that is, an impact evaluation considering privacy risks and the effectiveness of the actions taken to face them). An important screening is performed during the audit, at the end of which a general framework emerges; then other possible solutions are taken into account according to the applicable law. Security is an essential aspect, although it cannot replace the fulfillments required

[36] WP29, Opinion 3/2010, 17/07/2010 "[…] Data protection must move from 'theory to practice'. Legal requirements must be translated into real data protection measures. To encourage data protection in practice, the EU data protection legal framework needs additional mechanisms. In the discussions on the future of the European and global data protection framework, accountability based mechanisms have been suggested as a way of encouraging data controllers to implement practical tools for effective data protection. […] In a nutshell, a statutory accountability principle would explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the Directive and demonstrate this on request. In practice this should translate into scalable programs aiming at implementing the existing data protection principles (sometimes referred to as 'compliance programs'). As a complement to the principle, specific additional requirements aiming at putting into effect data protection safeguards or at ensuring their effectiveness could be set up. One example would be a provision requiring the performance of a privacy impact assessment for higher risk data processing operations [...]".

by law when it comes to personal data protection.

Camerino, dicembre 2017.