Civil Procedure Review
AB OMNIBUS PRO OMNIBUS

2

Blockchain records: is the evidence admissible? A challenge for European Member States

Rebecca Berto[1]

Dr.jur. University of Padova. Pg. Dipl. International Dispute Resolution (Arbitration) Queen Mary University – London. Lawyer at the European Consumer Centre Italy.

Abstract: Agreements, transactions and their records play a fundamental role in the economic system of every country: records identify parties, govern their interaction and register events. When agreements are infringed, the aggrieved party would lodge a claim to a court, in order to ask for damages or specific performance. Consequently, the aggrieved party would submit proves in order to found its claim.

The digitalization process leads to the creation and storage of digital records. However, digital records are still subject to the same admissibility rules as paper-written documents. Consequently, when digital records are admitted as evidence in legal proceedings, they point out legal ambiguities. These ambiguities are going to be exacerbated by blockchain records because of its technical features. For this reason, the admissibility question of blockchain receipts in legal proceedings is one key point for the future employment of blockchain technology in a country economic system.

Keywords: blockchain records, admissibility, evidence

1. The view expressed herein are solely the author's and represent neither the one of the ECC-Italy nor of its host structures and any other of its public financiers. All opinions and errors are of the author.

1. INTRODUCTION

Generally speaking, means of evidence are documents, testimony, and real evidence which prove directly or indirectly facts on which the claim is based.

The weight, credibility, and sufficiency of the evidence produced by the parties, in order to support their legal position, are decisions of a Court. However, the admissibility of evidence means in a legal proceeding is a question of law: in this legal aspect lies the profitability of records and more generally of a commercial receipting system. Indeed, the failed admission of an evidence mean, may be a reason to lodge an appeal.

The digitalization process introduced changes on the modalities to create and keep stored records through the employment of informatics systems or other devices. Especially, blockchain technology promises to change how agreements and transactions are recorded and performed. Indeed, blockchain receipts are claimed to be algorithm-produced, cost-efficient and permanent since they eliminate middlemen or transaction verifiers. Blockchain technology combines the features of a hand-to-hand transaction in a transparent manner because the transaction is validated and recorded on a public ledger by employing a network of shared computers.

The key question of this new receipting system lies on the admissibility of its records in future litigation or arbitration procedures. Blockchain records are an advanced form of digital records.

Digital records, such as digital pictures, have already raised legal ambiguities when they are admitted in legal proceedings because they are subject to the same admissibility rules as paper-written records. It is true that interpretative mechanism may be employed to extend or analogically apply existing rules or law principles to new circumstances. However, digital records pose a different legal issue because the technical features are completely different from a paper-written document: the question of integrity or authenticity of a paper-written record, as going to be seen, is dissimilar from those concerning digital records. Blockchain records exacerbate this problem due to its technological features.

Leaving this legal problem only to Courts may cause several troubles because a Court is called to rule on a single specific case without clear legal parameters. A Judge is bound by the application of laws because it has to ensure the adversarial principle not only by conducting the legal proceeding but also during the stage when means of evidence are admitted. For example, according to art. 246 Italian civil procedure code, a Court should exclude those witnesses, who have a legal interest in the legal proceeding, which may justify their participation in it as part.

For this reason, the admissibility question of blockchain records is a contentious matter, because it touched the parties' fundamental right to present their case. Moreover, in absence of a specific provision, by employing an interpretative mechanism, it becomes evident how the border between an analogical interpretation of existing rules and the creation of new law is extreme thin, especially when a Court is called to apply criminal provision on a single case criminal provision.

Civil Procedure Review. v.10, n.3: set.-dez. 2019.
ISSN 2191-1339 – www.civilprocedurereview.com

Leaving this legal issue only to self-regulation by taking advantage of technological improvements, such as the employment of a special chameleon hash function, does not solve the core problem of the legal admissibility of blockchain receipts in legal proceedings. On the contrary, it adds management matters of trapdoor key and conflicts management.

This paper begins with recollecting the features a record should meet according to the archival science in order to be considered a trustworthy document. In this way, it becomes more transparent the legal challenges raised by digital records and lastly by blockchain receipts. In the third part it is given a look at the e-IDAS European Regulation: it emerges how the European legislator remain adherent to signature requirements. Also a digital record should be digitally signed, in order to be equated to a paper-written hand signed record. In the fifth part is analyzed how existing law of evidence may be applied to blockchain records and its consequences. In part six, a technological approach and its legal consequences are discussed. Finally, conclusions are draft: a new legislative approach towards digital records would relieve law inconsistencies and encourage, at the same time, the development of a digital a crypto-economy.

2. PAPER-WRITTEN RECORDS AND DIGITAL RECORDS: AUTHENTIC, ACCURATE AND RELIABLE

The judicial evidence is used to prove either fact in issue or facts from which facts in issue may be properly inferred.[2] Means of evidence are documents, testimony and real evidence: every legislator provides rules on these evidence means and their admissibility.

Generally speaking, testimony is the declaration, which must be admissible in a court of a person, who actually perceived the fact in issue or facts from which facts in issue may properly be inferred. Real evidence is described as "material objects other than documents produced for the inspection of the court,[3] so a Court can reach its own conclusion on the basis of its own perception.[4] Finally, documents are understood as every suitable mean able to keep note of a fact for future recalls, such as certified documents, letters, pictures, accounting books, etc.[5]

The essential essence of a written record is that it is something concerning a recorded information directed to someone else, kept by a support on which a record is registered and has the potential to make a factual account: for example, a picture is a proof when it is put in a qualified factual context, which assigns to the picture the

2. Colin Tapper "Cross and Copper evidence", 12th edn, Oxford University Press 2010, pag. 20.
3. Hodge Malek Phepson "On Evidence", 18th edn Sweet & Maxwell 2013, par. 1-14.
4. Stephen Mason and Daniel Seng "Electronic Evidence", 4th edn Stephen Mason and Daniel Seng, Institute of Advanced Legal Studies, University London, pag. 39.
5. Schlesinger e Torrente " Manuale di Diritto Privato" 16th edn, Giuffrè editore , Milano, pag.271.

quality of an evidence mean. However, no general definition of document is provided by the Italian legislator, but in single specific provisions: for example, in Italy art. 240 of the Italian criminal procedure deals with anonymous document. Or a specific definition for document is provided in art. 2 (1)(c) legislative decree number 36 of 2006 which implemented in Italy the Directive 2003/98/CE on the re-use of public sector information. According to this rule, a document is a representation of acts, fact or data whatever its medium and which is available to the public administration or bodies governed by public laws. However, this definition does not cover computer program. Moreover, it should be kept in mind that the scope of this rule is restricted to the relationship between public administration and citizens and to the information recorded and stored by the public administration.

In Cyprus the Evidence Law, art. 2 (1) defines as document "anything in which information of any description is recorded."[6] Though, this definition is broad, either the Italian and the Cyprus rules do not further address those distinctive features a document or a record should have in order to be trustworthy.

Being legislative provision so poor on this point, help may be get by the archival science. Indeed, the archival science detailed three requirements a trustworthy record should have, namely, accuracy, authenticity, and reliability. According to the Society of American Archivists' glossary, accuracy is defined as "the degree of precision to which something is correct, truthful and free of error or distortion, whether by commission or omission."[7] This definition aligns with the common understanding of the term. Reliability means "the degree to which a record can be considered reliable is dependent upon the level of procedural and technical control exercised during its creation and management in its active life".[8] To achieve reliability, a record should have three additional characteristics: completeness at the time of creation, consistency with the rules of creation and the so-called naturalness. In order to be complete, a record should respect those formal characteristic required for that kind of document, which makes it capable of generating legal consequences. For example, a sale agreement needs the mention of the parties, the object of the sale agreement, its price, the date of creation and the parties' signatures. Naturalness refers to the fact that the materials accumulate out of a routine process.[9]

Beyond reliability and accuracy, a record must also be judged to be authentic. In the archival science, authenticity is defined as "the trustworthiness of a record as a

6. This provision is identical to the one of Section 13 of the English Civil Evidence Act.
7. Society of American Archivists Glossary, Accuracy available at https://www2.archivists.org/glossary/terms/a/accuracy.
8. Gilliland-Swetland, Anne J., and Philip B. Eppard, "Preserving the Authenticity of Contingent Digital Objects: The InterPARES Project" D-Lib Magazine 6:7/8 (July/August 2000).
9. Society of American Archivists Glossary, Naturalness available at https://www2.archivists.org/glossary/terms/a/archival-nature.

Civil Procedure Review. v.10, n.3: set.-dez. 2019.
ISSN 2191-1339 – www.civilprocedurereview.com

record; i.e., the quality of records establish that it is what it purports to be and that it is free from tampering and corruption."[10] Further, a record must have been created by the individual represented as the creator. The presence of a signature, whether it be physical or digital, serves as a test for authenticity because the signature identifies the creator and establish a relationship between the creator and the record. Accordingly, there are two pre-conditions for authenticity: identity and integrity of the record. A record is made or received in the course of an activity as an instrument or a product of such activity and set aside for action or reference.[11] This relationship links each record, incrementally, to the previous and subsequent ones and to all those which participate in the same activity. This relationship, called the archival bond, has a double scope: not only it relates a record to a specific creation context, but also define the archival aggregate to which it belongs. Without reference to an archival bond, it is impossible to establish if a record is genuine or a forgery. In other words, it is necessary to analyze the relationships between the records and the organizations or individuals that created, employed and kept them in the conduct of their daily life or business activity.[12] These controls are done because integrity relates to the potential loss of physical or intellectual elements after a record has been created.

In the pre-digital era, integrity meant, for example, control of numbered entries in registries or numbering individual documents in file folders. Laws on evidence regulated and are still focused on paper-written documents and records. However, though the digitalization process, digital records as well as paper-written records must meet the same legal requirements in legal proceedings: evidence must be relevant and admissible.

2.1. Digital records – integrity and authenticity

The digitalization introduced technical alternatives to create and keep stored records: several information systems are capable of storing, manipulating or transmitting data. Digital records cannot be compared to traditional paper records because they have other technical properties and features. For example, digital records record and store a factual account in binary language or the same word document may be re-written several times or a digital picture may be manipulated with Photoshop. However, the features of reliability, accuracy, and authenticity should be met by a digital record. In concrete, this would mean to establish the identity of digital records, such as the name of the purported author, the date they were created, the place of origin and the subject matter. The record's integrity means it has not been corrupted over time or

10. R. Pearce-Moses, "Autheticity InterPares Trust Terminology Database" ed.2017, available at https://interparestrust.org/terminology/term/authenticity/en.
11. International council on Archives 2004 "International Standard Archival Authority Record for Corporate Bodies, Persons and Families", 2nd Edn (ICA 2004).
12. Victoria L. Lemieux "Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: an Archival Theoretic Evaluation Framework" in Future Technologies Conference , 2017, pag. 4.

in transit; in other words, the same set of sequences of bits that came into existence when the object was created are still present.[13] The integrity of a digital record implies the assurance of information systems' integrity, in which records are created, modified and stored. Assuring integrity in information systems means for example to adopt measures such as access controls, user authentication, regular maintenance of the information system, in order to grant the records' integrity and authenticity. A record representing a fact legally relevant should be kept by its creator respecting those rules granting the record affidability and its conservation over the years.

However, digital records raise two important legal issues on the law of evidence: on one hand, it is not possible to distinguish copies from an original record and on the other hand, the custody chain of digital records is lost. Actual rules look at paper written documents, rather than to digital systems in which data are created. Indeed, in paper written documents, authenticity is linked to the ascertainment of identity, while integrity is given by the perfection of the record. In absence of an original record, the identity and integrity of a digital record are interwoven becoming interdependent. Further, copies and originals of digital records are indistinguishable.[14] Consequently, this has a legal impact on the employment of those civil procedures which allows a party to argue the exclusion of a document or a record from a proceeding when its integrity is questioned. In Italy, for example, only original document may be the object of this kind of procedure.[15] This exclusion procedure was extended by the Italian legislator to those electronic documents signed with an advanced or qualified digital signature because these signatures grant the author's identity, the record's integrity, and inalterability.

The second problem is the burden to demonstrate the continuity of custody necessary to show that a digital record is authentic. There is little guidance on how to determine the authenticity, so other information is going to be considered. Therefore, the authentication of digital record can be done by verifying the means associated with the record, such as the organizational criteria demonstrating the provenance of the digital document, and the documentation concerning the custody chain. Timestamps, signatures, and seals may help to test the provenance of the digital record. However, a case dealt by the Court of Rome shows that timestamps and signature were not knock-out arguments against the action brought by a party, whose aim was to get a sentence, which deletes the legal effects of digital records. These digital records were signed with a qualified signature apparently by him, which was the cause of a replacement of a Chief Executive Office in a company and lead to the adoption of other deliberations by the board of directors. Those digital records were declared void because a malicious user with unauthorized access to private password digitally

13. Lynch, Clifford A., "Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust" Council on Library and Information Resources, 2000, pp 32-50.
14. John D Gregory "Authetication Rules and Electronic Records", 2002, 81 Can Bar Rev. 529, 533.
15. Sentence of Tribunale di Roma n.1127 of 2017.

Civil Procedure Review. v.10, n.3: set.-dez. 2019.
ISSN 2191-1339 – www.civilprocedurereview.com

signed those records. The Court reached this decision through the circumstances of the specific case: the claimant kept the receipt of the parking house, which confirmed the witness statement of his fiancée, who declared he had passed all the time with her. During that time span, the digital documents were signed. Moreover, other contradictions of witnesses' testimonies on time and place the digital records would had been digitally signed by the claimant, supported the over-mentioned decision of the Court in Rome.[16]

In conclusion, the issues concerning the digital records may be framed as follows "Can be data be trusted? Can records be from which data are derived be trusted? Are these records complete? Are they authentic? How are they generated, by whom and under what conditions? Is there sufficient contextual information to enable them to be understood?[17]

3. THE EUROPEAN APPROACH: THE E-IDAS REGULATION

Svetonio in "Vita Neronis[17]" wrote, "*Adversus falsarios tun primum repertum ne tabulae nisi pertusae ac ter linum per foranima traiecto obsignarentur*.". In other words, Nero in 61 a.C. introduced the "*Senatusconsultum Neronianum Adversos Falsarios*", according to which a parties' agreement was void if it did no respect three formal conditions: the agreement should had been recorded in polyptychs not perforated, with three times thread biding them, before being sealed with a sealing.[18]

The European legislator remains adherent to the fundamental idea that the signature of a document fulfills three purposes: identify the author, externally manifest the author's will to assume the legal effect of facts or acts and keep over the years the evidence of legally relevant facts or acts.

The repealed directive 93/99 was inspired by a technologically neutral approach, whose aim was to grant the choice on how to link an electronic record to an author: it could be employed an electronic signature or an user ID and password, in order to get access to the information system.

From the 1st July 2016, the Regulation (EU) 910/2014 repealed the directive 93/99: the new rules were published under the name „Regulation on electronic identification and trust services for electronic transactions in the internal market," commonly referred as the e-IDAS Regulation. The e-IDAS Regulation provided rules on trust services such as electronic signatures, electronic seals, electronic time stamping, electronic delivery

16. Ibid. supra note.
17. Duranti Luciana and Rogers Corine, Trust in Digital Records: An Increasingly Cloudy Legal Area, in Computer Law and Security Review, 28, 2012.
18. See also Pauli Sententiae 5.25.6 "Amplissimus ordo decrevit eas tabulas, quae publici vel privati contractus scripturam continent, adhibitis testibus ita signari ut in summa marginis ad mediam partem, perforatae triplici lino costringantur atquae impositae et supra linum cerae signa imprimatur, ut exteriori scripturae fidem interior servet. Aliter tabulae prolatae nihil momenti habent".

service, electronic documents admissibility, and website authentication. This legal framework is based on the Member States' reciprocal obligation to recognize such trust services when those services are based on a qualified certificate issued in one Member State. Therefore, the scope of the e-IDAS is to design a legal framework, in order to ensure a harmonized recognition of several electronic identification means, eIDs, employed by the Member States. However, Member States are obliged to recognize those eIDs contained in a list published by the European Commission based on the Member States' notifications.

Art. 3 e-IDAS Regulation introduced the electronic signature, the advanced electronic signature, the qualified electronic signature. According to art. 3, 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. The advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26, which are ":(a) it is uniquely linked to the signatory; (b)it is capable of identifying the signatory; (c)it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable." The qualified electronic signature means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures (art. 3 comma 1 number 12 e-IDAS Regulation). Art. 25 (2) Regulation (EU) 910/2014 equated the qualified electronic signature to the legal effect of a handwritten signature.

In other words, the e-IDAS Regulation distinguished between electronic signatures, which are data linked to other data, and advanced electronic signatures, which are data linked to a digital record or document. Electronic signature, such as user ID and password has the only function to allow the service provider to identify the individual user. An interesting provision was introduced by art. 25(1) e-IDAS Regulation. According to this rule, electronic signatures should be admitted in legal proceedings, even if they did not meet the requirement for a qualified electronic signature: their admissibility should not be denied solely on the ground that the signature was done in electronic form. As a consequence, electronic records with a simple electronic signature are admissible but are freely weight by the Court on quality, integrity, and features of digital records to keep stored the information. Put it in other terms, a Court is called to judge on the grade of affidability of the electronic system in relation to the integrity and identity of the digital record.

However, this law provision should get into the civil procedures of every single Member State: for example, according to art. 633 and 634 Italian civil code procedure an electronic record should satisfy the written evidence requirements, in order to get a payment order. This would mean that only an electronic record signed with an advance or qualified signature can fulfill the mentioned condition: an electronic signature would not be sufficient.

Civil Procedure Review. v.10, n.3: set.-dez. 2019.
ISSN 2191-1339 – www.civilprocedurereview.com

The European legislator with the e-IDAS Regulation focused its attention on the electronic signature in order to determine the authenticity of digital records. According to the Regulation, the generation and management electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider,[19] whose requirements are set out in art. 24. Between these conditions, a qualified trust service provider should employ appropriate technological measure, in order to keep the integrity of data and integrity of the data process, which includes the adopted protocols in order to preserve the data' validity and accuracy.

However, the integrity of the information system, through which a digital record may be created, modified or stored is not properly addressed. Further, the European legislator does not consider computer-generated records without human intervention and under what conditions they could be admitted in legal proceedings. This European legal vacuum would be fulfilled by national law and this would imply legal fragmentation because every Member State would look and apply its own civil procedure provisions. At least this has legal implications especially when records of distributed ledger technologies are considered.

4. BLOCKCHAIN: WHAT IT IS AND HOW IT WORKS

The blockchain technology is a global digital infrastructure, which can move assets, such as money, securities or commodities, through a network of shared computers.[20] Blockchain technologies are characterized by being open-source technologies, with no central server or central entity controlling the distributed public ledgers. Moreover, blockchain technology's key features are the presence of a peer-to-peer network, the use of cryptographic algorithms, the employment of a decentralized consensus mechanism[21] and a permanent record system, where transactions are recorded, without the intervention of trusted third parties.

In this technical environment, the consensus mechanism is a process of solving mathematical problems, in order to validate blocks: this activity is carried out by nodes, a network of computers, who offer their computing power in exchange for getting newly minted crypto coins. The consensus mechanism provides rules on how to resolve double spending, by determining which of two conflicting transactions is admissible. From another point of view, the consensus mechanism is also a new form of auditing

19. Regulation (EU) 910/2014, Annex II, Art. 3.
20. Trevor Kviat "Beyond Bitcoin: Issues in Regulating Blockchain Transactions", 2015, Vol.65 Duke Law Journal, pages 569-608; see also Don Tapscott and Alex Tapscott, "Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World",2016, Penguin Random House LLC.
21. Aaron Wright and Primavera De Filippi "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" ,2015, at pages 4-5, available at https://www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/SSRN-id2580664.pdf.

because only those transactions, which has been validated by the nodes, are added in the blockchain. Blockchain is a chronological database of transactions validated and recorded by nodes. This chronological database is encrypted and broken into blocks.

Miners collect the incoming transactions through an incoming packeting process. In order to create valid blocks, miners must solve a mathematical problem. Once this problem is solved, the other network's nodes verify that the solution corresponds to a previous transaction. Basically speaking, when nodes check that another node created a new block, whose hash in the header, has the same value as the hash value of the verifying node, the latter recognizes the new block to belong to the valid chain. This is the proof-of-work consensus model employed for Bitcoin transaction. In the Bitcoin protocol, the hash of the previous block is referenced by 256-bit hash in the hash prev block field in the block header. [22]

Once the transaction is validated the new block is added to the ledger and is propagated through the network until every node has an updated version of the blockchain. Rather, blockchain exists on the personal computers or other mobile devices of all those persons or entities, who take advantage of this technological tool.

The most famous application of blockchain technology is Bitcoin. As has been seen, though the backbone technology on which Bitcoin run, is quite complicated, moving Bitcoins is quite simple. A user can purchase Bitcoins online, from miners, exchanger platforms or from private sellers on online marketplaces, as well as, in person from local sellers or ATMs. To transfer Bitcoins, the seller and the buyer must own a wallet, which is made up of two mathematically related keys: a public key and a private key. Wallet owners are identified by the public key, which serves also as a pseudonym. In order to process a Bitcoins transaction, the seller takes advantage of a computer program or an app, through which he needs to enter only the recipient's Bitcoin address, the payment amount and click send: a significant feature of public keys is that they are not inherently tied to the user's real-world identity. Technically speaking, a Bitcoin owner employs his private key, in order to sign the hash of the transaction in which he got Bitcoins. In this way, the user proves that he owns Bitcoins. At the same time, the owner authorizes with the private key the transfer to the public address, representing the receiver's wallet.

5. THE ADMISSIBILITY OF BLOCKCHAIN RECORDS IN LEGAL PROCEEDINGS

Blockchain technology's main feature is the absence of a central authority: every update is automatically carried out on every computer of the blockchain network through a constantly-updating algorithm. Moreover, due to the absence of human intervention in generating the record, blockchain records may be considered as computer-generated. As has been seen, even if a user employs an app in order to

22. Andreas M. Antonopolous "Mastering Bitcoin", 2015, Sebastopol CA, O'Reilly, at XX.

Civil Procedure Review. v.10, n.3: set.-dez. 2019.
ISSN 2191-1339 – www.civilprocedurereview.com

transfer, for example, Bitcoins, and enter data such as the recipient's address and the payment amount, the receipt of this transaction is generated without human influence.

Legally speaking, even if is put relevance on the circumstance, for example, that a Bitcoin transaction is signed by the employment of the user's private key, the user's private key is a data linked to another data. Indeed, the validation process is done by a network of shared computers and blockchain is a shared technology, whose records are computer-generated. It is a plain consequence that the e-IDAS Regulation does not apply to blockchain technologies for two reasons: on one hand, there is no qualified trust service provider, which met the requirements set out by art. 24 e-IDAS Regulation, and on the other hand, the advanced and qualified signatures conditions are not fulfilled. However, it may be recalled art. 25 e-IDAS Regulation, according to which an electronic record should not be excluded for being an electronic record, even if it does not meet the requirements of the e-IDAS Regulation. A Judge is bound to apply rules found in legislation. Consequently, a Court cannot exclude blockchain receipts solely because it is an electronic record. But a blockchain record would be subject, or better subsumed under the civil procedure rules of every European Member State.

This would lead to a legal fragmentation in Europe because every Member State would recall its own rules on evidence law. For example, in Italy, all digital records which have no digital qualified or advanced signature should be regulated by art. 2712 civil code, as real evidence. This lead to further consequences: a record with a qualified digital signature may be subject to a voidness procedure when a party argues that its private digital key to sign digital documents has been abused by an unauthorized person.[23] In case of a positive outcome, the legal effects of the record are void.[24] Another procedure, whose aim is to object to the authenticity of a private signature of a paper-written record, is a sort of exclusion procedure. The outcome of an exclusion procedure may lead to the exclusion of the record from the legal proceeding and consequently, the receipt or record is not comprehended in the proofs, part of the weighing process, carried out by the Court.[25]

The voidness, as well as the exclusion procedure, may not be employed in case of real evidence. As a consequence, a Court can ascertain the integrity and authenticity of the digital record by employing other means of evidence. In this scenario a digital record is not formally excluded from the proofs produced in the legal proceeding and a Court may still decide over the fact represented, even if a party argues on its integrity or on its authenticity. In other words and changing example, if a digital picture is produced and a defendant raises objections on the integrity of the picture because the event represented was manipulated with Photoshop, a Court may still

23. Art. 221 and following of the Italian civil procedure code.
24. See for example sentence of Tribunale di Bari number 2741 of 2012.
25. Sentence of Corte di Cassazione number 23155 of 2014.

decide over the fact represented in the submitted picture.[26] By this simple example, it becomes clear that the failed adjustment of the law of evidence to new technological developments added legal risks because the admissibility of a digital record, whose integrity or authenticity has been questioned, is left to the sole judgment of a Judge, without legislative parameters.

As has been previously seen, matters like unauthorized employment of digital key to sign digital records requires the party to lodge a legal proceeding, in order to request the voidness of the legal effects of a digital record. Certainly, this party is called to sustain its position.[27] A similar scenario is possible also with blockchain technologies: the blockchain network is not able to distinguish between a transaction submitted by the actual user and a malicious user with unauthorized access to the private key. Further, the reliability and accuracy of digital records on the blockchain are still not addressed. If a piece of false or wrong information is registered, as long as the correct protocols are employed, this record will be accepted by the network and added to the blockchain. In these cases, the aggrieved party would have legal difficulties to request the voidness of the legal effects of a blockchain recorded transaction because in Italian law voidness and exclusions procedures are only foreseen for paper-written records and for those digital records signed with an advanced or qualified signature. Being blockchain receipts computer-generated without human intervention, there is a legal vacuum because the Italian law of evidence does not expressly cover the legal admissibility of this kind of digital records.

In order to stress the point of how blind is the choice to leave the legal point of the admissibility of blockchain records in legal proceedings solely to a Judge, it would be useful to change law sector and add an example from criminal law. It is technically possible to record on blockchain backups of link lists to child pornography. According to section 184c of the German criminal code,[28] a person may be charged for possession of illegal content when she knowingly possess an accessible holding of the said content.[29] Further, section 11 comma 3 of the German criminal code hardware disk,[30] as well as, sound and video recording are equated by the German legislator to written documents. The critical legal point is the following: a hard disk holding blockchain, where is recorded an illegal content which can be easily be resembled by a user, would

26. Nathan Wiebe "Regarding Digital Images: Determining courtroom Admissibility Standards", 2000, Manitoba Law Journal vol 28 no.1, p.61-77: in this paper the author specifically addressed the legal problems related to digital pictures.
27. Sentence of Tribunale di Roma number 1127 of 2017.
28. Section 184c German criminal code available at https://dejure.org/gesetze/StGB/184c.html.
29. Matzutt, Hiller, Henze, Ziegeldorf, Müllmann, Hochfeld, Wehrle "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin", 2018, on Conference: Financial Cryptography and Data Security 2018, At Curaçao, available at https://www.comsys.rwth-aachen.de/fileadmin/papers/2018/2018_matzutt_bitcoin-contents_preproceedings-version.pdf.
30. Section 11 German criminal code available at https://dejure.org/gesetze/StGB/11.html.

Civil Procedure Review. v.10, n.3: set.-dez. 2019.
ISSN 2191-1339 – www.civilprocedurereview.com

be considered as a document, so that the user may be charged for possession of illegal content? This legal point is not easy to be solved because law principles which guarantee the fundamental constitutional rights of a citizen, such as the principle of legality, the principle of no-retroactivity and the prohibition of analogy reasoning *in malam partem*[31] must be respected. Accordingly, the principle of legality implies that a criminal offense and its sanctions should be based only on a prior enactment of a prohibition that is expressed with adequate precision and clarity. As a consequence, the employment of the analogy reasoning *in malam partem* is not allowed, because this would mean to ascribe a new criminal offense which is not clearly proscribed by a legal provision.

From this last example, it is clear that a Judge is called to apply the rules found in legislation and to decide over a single specific case. It is not the role of a Judge to create new rules when there is a legal vacuum. In a constitutional democracy, a legislative gap should be covered by the Parliament. According to Constitution Law, one of the main function of the Parliament, as elected branch, is to assume the responsibility of law reforms, especially those law reforms which has an impact over several law sectors, such as civil or criminal laws. And a law reform would imply a re-examination of subsidiary rules, in order to implement law reforms.

6. TECHNOLOGICAL IMPROVEMENTS: DOES IT SOLVE LEGAL QUESTION?

Blockchain technologies are based on a double consensus: consensus of the natural or legal person, who employs this technology in order to transfer money or other assets and the consensus protocols, on which the functioning of blockchain technologies are based. As has been seen consensus protocols rules are a specific set of rules, which determine who, under what circumstances and when a transaction can be carried out. Further, protocols set also rules on double-spending that nodes on the network will implement during the validation process of the block and of the transactions within it.

Blockchain receipting system poses legal problems on its admissibility, as for example when a user would like to get the annulment a transaction validated by the blockchain networks because his private key was abused by an unauthorized person. Or when a user would like to correct information registered in a distributed ledger because it is not correct or false.

There are calls to leave these legal issues to self-regulation:[32] the technology itself and the market would find out an adequate technological solution. In particular, it has been advanced the idea to manipulate blocks through the employment of a special

31. Ferrando Mantovani „Diritto Penale, Parte Generale", 3rd edn, Cedam Padova 1992, p.974.
32. As in note 20.

chameleon hash.[33] A chameleon hash[34] is a cryptographic function which contains a trapdoor: everyone, except the holder of the trapdoor information, is prevented from computing collisions. Blockchain relies on a chain of hashes which connects the blocks, creating a sequence of blocks. The information contained in the blocks is permanently recorded because of the collision resistance of the hash function. However, if a lock is added to each link of the hash chain, it would be possible to find collisions and consequently to replace the content of a block in a chain.[35] Most importantly, only the holder of the trapdoor information allows him to efficiently generate collisions.

Taking advantage of a special chameleon hash, in concrete, this would mean to redact any block in the blockchain keeping the integrity of the original blockchain. As a consequence, there is no need to create a hard fork and to rebuild blocks. In order to identify the corrected blocks, the changes carried out on the block should leave a mark, which cannot be removed even by the holder of the trapdoor information.

Redacting the block appears to be simple: the chameleon hash is employed to unlock the link between the block that must be changed and its successor. The chameleon hash allows replacing the block with a new one without breaking the hash chain. Redaction is publicly examined by existing miners because they must approve the new blockchain and have access to old copies. Another advantage of this technological solution is that it is possible to maintain the virtue of immutability, which characterizes the blockchain technology.

This special chameleon function, on one hand, provide a technical solution, in order to correct or updates blocks, but on the other hand adds a new problems: the management of the trapdoor key with an eye of the specific application which is running on blockchain and the management conflict when miners do not agree with the redacted blocks and the new blockchain.

On the first issue, emerges the difference between a permissioned and a permissionless ledger. Indeed, it is easier to employ a chameleon hash function in permissioned ledgers. With a permissioned ledger, a developer may choose to make the ledger available for everyone to read, but may limit the parties who can transact on the blockchain and also set who can serve the network by writing new blocks on the chain. The trapdoor key would be managed by the developer or by a predetermined set of parties.

Though it appears to be more difficult to employ a chameleon hash function in a permissionless ledger, like the one, for example, on which Bitcoin is running, several

33. Ateniese, Magri, Venturi and Andrade "Redactable Blockchain or Rewriting Hostory in Bitcoin and Friends" 2nd IEEE European Symposium on Security and Privacy—EuroS&P 2017 available at https://eprint.iacr.org/2016/757.pdf.
34. Krawczyk, H., Rabin, T. "Chameleon hashing and signatures" Proc. Network and Distributed System Security Symposium (NDSS) 2000, Internet Society, pp. 143-154.
35. As in note 29.

Civil Procedure Review. v.10, n.3: set.-dez. 2019.
ISSN 2191-1339 – www.civilprocedurereview.com

key management solutions may be advanced. The easiest would be the distribution of the trapdoor key to public authorities, dealing with digital and crypto-economy or to an authority created ad hoc for this new emerging sector. More complicated appears to be the management of the trapdoor key when it is distributed to miners: in a permissionless blockchain environment, where potentially everyone can serve the network as miner in order to create blocks, it would be necessary to write requirements to identify who within the miners community should hold the trapdoor key, in order to correct blocks.

An alternative would be to distribute the trapdoor key to a predetermined number of miners: in reality, mining is no more a hobby performed by early adopters on ordinary personal computers: according to the data of blockchain.eu mining activity is professionally carried out. According to this data, mining pool like KnCMiner or GHash.io ceased their activity in 2016, while BTC.com was launched in the same year.[36] It appears there is a frequent entry of new mining pools and the exit of a successful one. If one mining pool, who owns a trapdoor key, ceased its activity, what procedures and rules will be applied, in order to transfer the trapdoor key to another mining pool operator? Therefore it should be ensured that the trapdoor key, would not be sold or distributed without control, in order to avoid abusive employment of the trapdoor key. Another scenario may be that a mining pool operator is part of a business, whose company get into administration: would the trapdoor key be considered as an asset? If so, would bankruptcy law apply? Or would the trapdoor key simply be considered lost?

But apart from the trapdoor key management, there is a second and more tricky question: what happens when miners do not agree with the redacted blocks and the updated blockchain? Mining pools operators hold considerable power in terms of which protocol rules they want to support by running client implementation. Miners ensure that only blocks as defined in the protocol are added to the blockchain. If a redacted block enforce rules not recognized by the majority of miners, they would reject the redacted blocks. The result may be a conflict within the network, in which there is one chain backed by a considerable computing power but not accepted by the holder of the trapdoor key and a chain considered valid by the holder of the trapdoor key but not backed by as much computing power. If nothing is established in a protocol on how to solve this conflict, it may be thought that the dispute would be brought to a Court. Again, we are pussyfooting around the same core question: would a blockchain record be admitted in a legal proceeding, in order to get a sentence on this issue?

When a new technology is dipped into economic reality, it is no more a question of conflict management or to correctly write protocols in order to establish who, under

36. Compare data mining available at https://www.blockchain.com/en/pools and Hileman and Rauchs "Global Cryptocurrency Benchmarking Study" Cambridge Center for Alternative Finance available at https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf, pag 92.

what circumstances and condition a block may be redacted. Or what would happen to the trapdoor key when the mining pool operator ceased to work or how would be a conflict between mining pool operators and the trapdoor key holder be solved in case of disagreement over a redacted block. It is a question to provide legal procedures, dynamic rules to a new technology which is going to be employed in the real world in more economic sectors, impacting on several laws.

Further, independently from the economic sector, where blockchain is employed, it is also a question to grant to a natural or legal person to be in the legal condition to bring a claim, in order to exercise a right, it assumed to be infringed. Technical improvements, as the special chameleon hash, provide a technical solution to the exigence to modify or change a block recorded in the blockchain. But the legal question on blockchain admissibility in a legal proceeding remains on the floor.

From the above examples, in a constitutional democracy, it is the duty of the Parliament, as an elected branch, to assume the responsibility to provide a regulation of blockchain technology and to grant the constitutional right to grant the access to justice. According to an Italian sentence of the Constitutional Court, sentence number 18 of 1992, the right of defense and access to the justice must not be deleted or diminished: this right may be diminished also when a party experiences obstacles in bringing a claim to a court. In absence of specific rules, it is the duty of the Parliament to remove these obstacles.

A Parliament is a right place, where a law reform on new technology should be discussed and enacted. A law reform may have an impact on several law sectors, not only commercial or criminal law, but also on bankruptcy, administrative, procedural and evidence law. A reform implies also the examine subsidiary rules and to change them, if necessary. Therefore, a Parliament is in the position to fully appreciate the economic and policy implications it is asked to make and to address the economic policy of a country.

7. CONCLUSIONS

Blockchain technologies raise challenges, which require a tough reply: a legislator could take this hint to dictate a completely new discipline on the digital records law of evidence.

As has been seen in section one, digital records raise several questions about integrity and authenticity. Actual rules on the evidence law are addressed to paper-written documents, whose provisions are not always fit to be interpretatively or analogically extended to digital records. The European legislator decided to introduce advance or qualified signatures in order to equate digital documents to written-paper documents. However, digital records and blockchain records cannot be thought in the same terms as paper-written documents: for example, paper-written records may exist in originals and copies, digital records not. Digital records are technologically different and pose different legal problems. However, the admissibility rules for paper-written

and digital records are still the same. Further, as has been seen in section three legislator failed to rule on records generated by computers without human intervention, which are also subject to the same admissibility rules.

In section four were explained how blockchain technology works, also by providing the example of how a Bitcoin transaction is technologically carried out behind the curtains of an app. Considering the features of blockchain technologies, in section five was discussed that blockchain records would be admitted in legal proceedings according to the civil procedures rules of every single European Member State. This lead to a legal fragmentation in Europe, because every Member States has its own procedural rules. For example, in Italy, if blockchain records are admitted as real evidence a Court is called to evaluate the integrity of an information system and the record produced. As has been pointed out, blockchain technologies do not address the reliability and the accuracy of a record, so if a protocol was respected a record with a wrong or false information would be added to the blockchain. The aggrieved party would not have a proper procedure to rely on, in order to request the voidness of the content of that receipt or its exclusion from the legal proceedings.

Moreover, in section six, was discussed whether technological improvements may make up the deficit of legislative intervention. Technological advancements are a response to needs, in order to keep blockchain competitive. However, between the several ideas on the economic sector where blockchain technology may be applied and its implementation, there is a legal span because the real economy experiences also conflicts and legal disputes. Disputes would mean the application of procedures to grant the right of both parties to present their case: as a consequence, the admissibility of blockchain records in legal proceedings is an unavoidable question for a legislator.

In conclusion, blockchain records and digital records raise several legal questions on the law of evidence: it would be a quite blind choice to pass to the Courts the duty to decide over legal problems put on the floor especially by blockchain technologies for three legal reasons.

Firstly, Courts are bound to apply the rules found in legislation. It is perfectly true, that there are interpretative means and mechanisms which allow a Court to extend or to analogically apply existing rules or principles to new circumstances. As has been seen, the law of evidence is still focused on paper-written documents, whose technological problems are completely different from digital records. For example, with digital records it is extremely difficult to distinguish between the original record and its copy: the actual provision provides rules which cannot be applied to an information system. This has an impact on civil procedural means, such as whether exclusion procedures may be applied or not in the single case.

Secondly, a legislator should keep in mind that a Court is called to decide over one single case. It is not the role of a Judge to provide a general rule because, in a constitutional democracy, the power to modify a provision or dictate a new one is reserved to a Parliament: only this one is in the position to fully appreciate the

economic and policy implications it is asked to make. This kind of major changes to the law requires, for example, to modify subsidiary rules.

And finally, it is a question of constitutional law. In an advance constitutional democracy, it is the duty of the Parliament, as an elected branch, to assume the responsibility of a law reform, whose policy and economic implications were fully analyzed and discussed by its members.

It would also be a blind choice to pass the duty to decide over legal problems solely to the technology and its improvements. As has been seen technological improvements may provide a solution to an exigence. However, blockchain technology is not kept in a closed environment but would dip into the real economy: the admissibility of blockchain records is key legal point, in several law sectors.

These are the legal risks for a failed adjustment that a legislator assumes and which would also have an impact on the economic growth of a country because legal certainty encourages investments.