doi:https://doi.org/10.15407/emodel.41.05.103

UDC 004.056.55, 347.441.142.52

O.I. Konashevych
Erasmus Mundus Joint International Doctoral Fellow in Law, Science and Technology
(Via Galliera, 3, 40121, Bologna, Italia;
e-mail: oleksii.konashevych2@unibo.it)

Data Insertion in Blockchain For Legal Purposes. How to Sign Contracts Using Blockchain

The use of blockchain technology, in particular, data insertion (anchoring, hashing) in the blockchain as a way of signing documents or imparting legal properties to facts is researched. A comparative analysis of the known methods of using electronic digital signature with the method of inserting data into the blockchain is carried out. The following issues were addressed. What is the data insertion in the blockchain and what properties do the data acquire? What is the difference between insertion, anchoring, and hashing on the blockchain? What is the difference between blockchain hashing and a digital signature on a document? Will the document be legally binding if it is anchored in the blockchain? What conditions must be met to give legal force for the document? How can anchoring be used to sign contracts, certify evidence that has legal value, denote time stamps, confirm authorship and copyrights, as well as transfer them, issue, and transfer power of attorney and delegate other rights, issue and transfer bearer instruments?

K e y w o r d s: Blockchain, OP_DROP, OR_RETURN, electronic signature, eIDAS, PKI, proof-of-existence.

Introduction. The blockchain has been designed to securely store transaction data [1]. However, starting from the first block, non-payment information was inserted into the database, also as «ledger» [2]. Since then, not only different methods of inserting data into Bitcoin have been invented, but a variety of blockchains appeared specifically designed for such and similar purposes. Although the technical side of the question of inserting data into the blockchain is already well studied, not much is said about the use of data insertion for legal purposes. In publications [2, 3], the accumulated experience of data insertion on Bitcoin is revealed.

Therefore, we decided to explore this area and answer the following questions. What is data insertion in the blockchain and what properties do the data acquire? What is the difference between insertion, anchoring, and hashing on the blockchain? What is the difference between blockchain hashing and a digital signature on a document? Will the document be legally binding if it is anchored in the blockchain? What conditions must be met in order to give legal force for document?

How can anchoring be used to sign contracts, certify evidence that has legal value, denote time stamps, confirm authorship and copyrights, as well as transfer them, issue, and transfer power of attorney and a general concept of delegation of rights, issue, and transfer bearer instruments and others? To understand blockchain technology and how a distributed ledger and infrastructure work, the reader must understand the basics of cryptography: asymmetric pair, cryptographic hash function. Therefore, it is recommended that you first expand your knowledge in this area.

Data insertion for legal purposes. 1. *What is data insertion in the blockchain?* There are a few methods of data insertion in the blockchain. The analysis of known methods in Bitcoin can be found in this paper [2]. However, this can be irrelevant in some aspects for other blockchain protocols. Accordingly, to summarize the existing experience of data insertion in the blockchain, we will emphasize the following. The arbitrary data is inserted into the blockchain as the result of a transaction. By the transaction, it is understood that the individual has spent some cryptocurrency. However, this is not a normal sending of «coins» to someone but a transaction when some cryptocurrency is permanently immobilized («burned») in the result of the application of some scripts (OP_RETURN, OP_DROP, etc.).

Such transaction as any other on the blockchain is signed by the sender using their asymmetric cryptographic private key. The user attaches arbitrary data which is signed within the body of the transaction.

The use of the blockchain provides a set of advantages, which are inherent to the blockchain itself:

I m m u t a b i l i t y. Once published on the blockchain the data cannot be altered or deleted; therefore, it is tamper-proof.

P u b l i c. User's data is stored on each node of the network; therefore, it is public.

U n c e n s o r e d. Using the blockchain is permissionless. The only condition of the transaction being accepted by the network is that it must be performed as per the blockchain protocol. Because each node is a carrier of the copy of the protocol, each block of transactions is verified by mining nodes. When the node propagates a new block to the network, other nodes using the same set of rules verify the validity of this block before to add it to their copies of the ledger.

P e r m a n e n t a c c e s s. The published data in the blockchain database can be retrieved from any remote node in the network, and the system will work while at least one node exists, including a local node as well.

T i m e s t a m p. The blocks of the transactions are sequentially «chained», and because of immutability, the chronology is preserved as well. Therefore, the time and date of any transaction are available with the accuracy of the average time of block creation (for example, in Bitcoin it is 10 minutes in average).

P s e u d o n y m o u s (anonymous[1]). Each transaction belongs to a specific blockchain address[2]. To spend the balance from the address, the user must have only the private key to this address. The address itself is retrieved from the public key. Therefore, users are authenticated only by their private keys.

There are some negative aspects of data insertion. One of the main concerns is about ledger overfilling. This is because the blockchain is a distributed database on which copies are kept by every node of the network. During ten years of operation Bitcoin database grew up to 197 Gb [7], and after four years Ethereum grew to 720 Gb [8].

Such redundancy is emphasized, for instance, in Bitcoin wiki in a discussion of one of the existing methods of insertion: «Many members of the Bitcoin community believe that use of OP_RETURN is irresponsible in part because Bitcoin was intended to provide a record for financial transactions, not a record for arbitrary data» [9].

2. *What does it mean to insert the data?* The user may wish to insert in the blockchain the data itself or anchor it by publishing a hash. The method of publishing itself is constrained by the maximum size of data, which can be inserted in one transaction. The maximum size depends on a chosen method and script and can be from 8 kB to ≈50 kB, which is not much from the perspective of usability[3]. For the reason of data redundancy but not as the main one, it proposed to store checksums (hashes) of data. Those hash functions are based on «strong cryptography»[4] [10] and provide for some advantages against keeping data itself [5]:

---

[1] In paper [1] of Satoshi Nakamoto offers to ensure privacy by keeping keys anonymous. However, some researchers [4, 5] claim that it does not guarantee complete privacy because other digital fingerprints (IP addresses, behavioral patterns and others) can disclose the user; instead of this, it is proposed to use the term «pseudonymity» instead.

[2] The blockchain address is retrieved from public key, see [6].

[3] It should be noted that, some blockchain similar technologies (distributed ledger technologies, DLT) are purposely developed to store unlimited amount of data. In other cases nodes do not store the data in the ledger as well or at least not all of the nodes, therefore, the information is not copied to every node of the network, instead some approaches to reduce data redundancy are applied (Maidsafe, Storj etc.).

[4] According to PCI DSS and PA-PSS (2016), as of the publication day of these standards, industry-tested and accepted standards and algorithms include AES (128 bits and higher), TDES/TDEA (triple-length keys), RSA (2048 bits and higher), ECC (224 bits and higher), and DSA/D-H (2048/224 bits and higher). See the current version of NIST Special Publication 800-57 Part 1 (http://csrc.nist.gov/publications/) for more guidance on cryptographic key strengths and algorithms.

[5] There can be different types of hashes. Here we are talking about cryptographic hashes. Other hash functions may not necessarily provide for mentioned advantages.

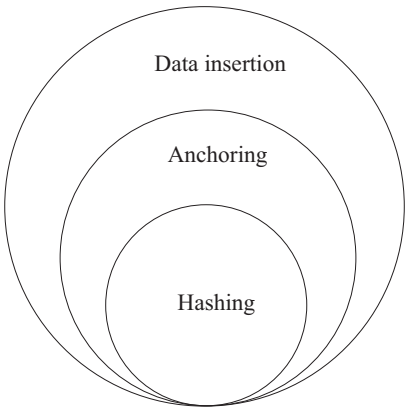

Fig 1. Relationship diagram: data insertion, data anchoring and data hashing in the blockchain

P r i v a c y. User's data does not become public. Hash is the result of a one-way function. It is not feasible to generate a message from its hash value (often also called a «digest» or a «checksum») except by trying all possible messages [11], which in practice is extremely difficult when strong cryptography is used.

A u t h e n t i c i t y v e r i f i c a t i o n. When the file is not inserted, the blockchain cannot protect an integrity of it itself, but it can provide for an auditability of integrity. When a hash function is applied, the same message results in the same hash with the negligible probability of a collision [12] if the strong cryptography is in use. Therefore, to verify the integrity of data, the user can compare the output hash with the hash which was earlier published in the blockchain.

The existing experience of data insertion in the blockchain is showed in the following relationship diagram (Fig. 1), from which the relationship diagram is: data insertion, data anchoring and data hashing in the blockchain. We can see that data insertion is a general concept attributed to any insertion which includes the subset of anchoring and hashing. When not the message itself but something which represents this data is inserted, it is referred to as a notion of «anchoring». Hashing is a subset of anchoring, referred to publishing hashes (usually understood as cryptographic hashes) in the blockchain. Anchoring in general might be referred to publishing of non-cryptographic hashes and some other data which may represent the original file (date, time, index number, author etc.).

The second column of Table 1 shows the properties that the original data source acquires when it is directly inserted into the blockchain and in the third column, the properties that acquire the data, if not the data itself is published in the blockchain, but only their hash sum.

3. *What is the difference between digital signing and blockchain hashing*? This question can be raised considering that a blockchain transaction is signed using an asymmetric cryptography. As it known, asymmetric cryptography is widely used beyond blockchain transactions. For example, to sign legal documents (transactions).

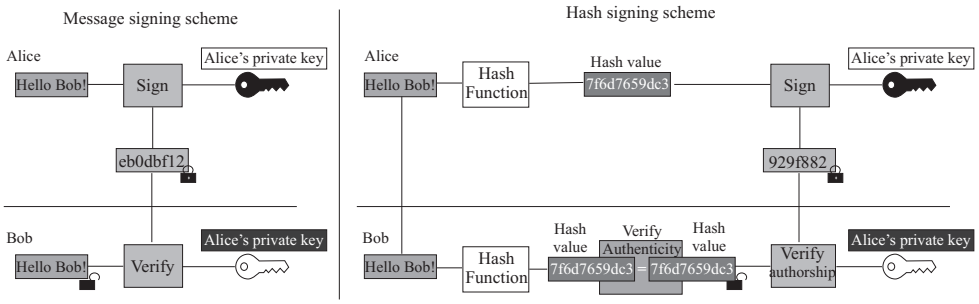

Fig. 2. Comparison of signing schemas: «message recovery» vs. «signature with appendix» (hash signing)

Table 1

Source	Data insertion	Hashing insertion
User's data become	Public	Private
	Limited (up to 50 kB)	Unlimited
	Tamper-proof	Verifiable

There are two basic approaches in terms of what to sign: the data (the message) or the hash (the message hash)[6] [13]. It means that the user may decide to apply a digital signature to the legal document itself or to sign the cryptographic hash of the document, which is presented on Fig. 2.

In the first scheme the message is encrypted by Alice's private key, and then Bob decrypts it using Alice's public key. In the process of decryption Bob recovers Alice's initial message. The difference in the second scheme is that Alice encrypts not a message, but a hash of the message, and Bob recovers this hash. The hash without the message is useless for Bob, that is until Alice also sends him the original message. Therefore, Bob calculates the hash from the message and compares the two hashes. If they are equal, then Bob understands that this is the original message which belongs to Alice. The hash signing scheme is widespread; however, some other schemas exist, but this is not crucial for the level of our discussion.

[6] To sign a digest message (hash value) is a scheme also known as "signature scheme with appendix" developed in Public Key Cryptography Standards # 1 (PKCS#1, based on RSA-PSS standard). The implementation can be found in RFC 8017 https://tools.ietf.org/html/rfc8017, and a similar approach is found in DSS-DSA standard (US Federal Information Processing Standard) and ENISA Standards (EU); this method is opposed to the initial concept of message signing, which however is also standardized. For example, ISO/IEC 9796-2:2010 — Information technology — Security techniques — Digital signature schemes giving message recovery.

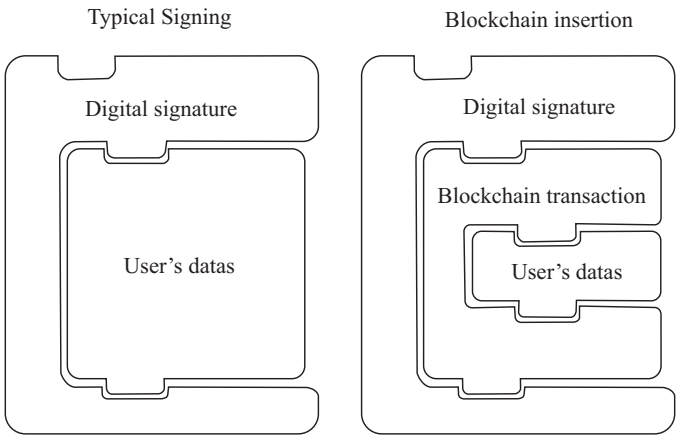

Fig. 3. Typical document e-signing vs. insertion in the blockchain

In typical digital signing, as an input is taken, only user's data (a document or a hash value) is to be signed, but in the blockchain, both the transaction data and user's data are signed (Fig. 3). In blockchain scheme it can be seen that the user's data can be a document itself or a hash of the document. Therefore, the practice of asymmetric cryptography is still in place in such case when the blockchain is applied: either document inserted itself, or a hash of it. In both situations this data is signed within the blockchain transaction with the user's private key. Some principal differences are found in comparison with the use of a Public Key Infrastructure.

4. *Public Key Infrastructure and Blockchain.* More substantial differences are apparent in a comparison of document e-signing with the use of Public Key Infrastructure (PKI). PKI is a set of technologies and procedures that enable the deployment of public-key cryptography-based security services [14].

In practice, to use digital cryptography for signing legal documents, many countries introduced regulations that mainly provide for:

trust services – which are performed by Certificate Authorities[7] (CA) or Trust Service Providers[8] (TSP) to identify signatories, so they can interact with each other remotely.

Timestamp – To guarantee that during signing, the trusted third party provides for a timestamp, known as a Time Stamping Authority [9] (TSA) or a Trusted Timestamp Authority[10].

---

[7] More common name in the USA.

[8] An official name as per eIDAS regulation in the EU.

[9] Typically in EU [15, 16].

[10] Terminology commonly used in the US [17].

Obviously, there are a lot of other aspects of PKI relationships. The regulations are supplemented with a set of technical standards and best practices.

A distinguishing feature in a blockchain is that it does not require TSA as a standalone service. As mentioned, the timestamping is an inherent feature of the technology that does not require any trust to a certain provider but depends on a distributed consensus scheme, in some academic literature this is called «decentralized trusted timestamping» [3].

As to identity, the blockchain is the technology that provides for pseudonymity. The blockchain address works as an authentication and authorization mechanism meaning that only the holder of the private key to this address can perform a transaction. Therefore, the blockchain itself can be called a decentralized pseudonymous PKI. At the same time, PKI-based identity services are standards that allow trusted parties (usually authorized/licensed by the government) to provide IDs. Similar services can also be applied as an overlay service of a blockchain infrastructure.

One of the most developed PKI schemes is in the EU and was introduced by eIDAS regulation [18]. Typically, the scheme is the following: TSP identifies a user in person and generates an asymmetric pair using one of the recognized standards. The public key is signed by such TSP and included in a certificate (using x.509 standard), which then is uploaded to a public repository. When the user computes a signature for a document using their private key, the software enquires a timestamp from the TSA server and includes it in the signing package. When the timestamp is retrieved and the signature of the document is computed, the system will form a data package in a container (see for details standards XAdES, CAdES, PAdES, and ASiC [19]). An addressee of the signed document will check the certificate (valid or not at the time of signing) and will verify the file and the digital signature. The successful verification means that an addressee holds a copy of the document, which is signed by the person who is specified in the certificate.

To ensure the sustainability of this system, there are some mechanisms to revoke certificates when the key is outdated, lost or compromised. To enable an Advanced electronic signature (AES), the TSP provides a scheme for multifactor authentication of the user and some other technical and organizational measures, which add more reliability that the transaction is signed exactly by the claimed person.

To enable a Qualified Electronic Signature (QES), the TSP provides for the highest standards of the security, including hardware devices for signing. The user will use only a certified device that computes the signature on a secure cryptoprocessor [20] (smart cards, USB devices, etc.). QES signature guarantees the authenticity from the point of view of the technology and the law.

The European Union Agency for Network Information Security (ENISA) issued a guidance brochure where they explained «non-repudiation of a signature» as a signature for which the signatory cannot deny that they are the originator of such a signature. For that reason, signature is archived with a set of technologies and standards described as follows: «Such electronic signatures thanks to the obligations set by the eIDAS Regulation on both the TSP managing them (in particular the CAs) and on the underlying technologies: warrant data integrity, identify the signatory with a high level of certainty, and ensure the non-repudiation of signing» [21].

This system is also typical in many other countries and based on the high attention of the government in this domain and thorough regulation and standardization. However, eIDAS also guarantees for technological neutrality and does not deprive any electronic signature of its legal force only based on the premise that it does go along with existing standards or accepted schemas [18]. Nevertheless, the use of other e-sign schemas may require proof of the evidentiary value in any concrete case. For that reason, there may be applied a methodology introduced by UNCITRAL.

5. *UNCITRAL and Legal Validity.* An electronic signature is considered to be reliable as per the requirements provided in [9]:

«(a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) any alteration to the electronic signature, made after the time of signing, is detectable;

(d) where the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable» [22].

An analysis of the blockchain insertion. Requirement (a) is ensured by the strong relationship between the signatory and the document by the use of asymmetric cryptography, where the blockchain address (public key) is an identifier. Requirement (b) is also ensured by the nature of asymmetric cryptography: the right to sign the transaction exclusively belongs to the holder of the private key, meaning that technically there is no any other way except by this key.

Of course, any fact of unauthorized seizure and use of the private key ends the legal validity of the e-signature. In [9] of the mentioned article discusses the level of reliability: «Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was

generated or communicated, in the light of all the circumstances, including any relevant agreement».

For that reason, to ensure requirement (b) of being «under the control of the signatory and of no other person», the use of the blockchain may require overlaid services of identification and authentication, which depend on a combination of certified hardware, standardized software, and participation of an authorized trust service provider (CA/TSP).

The compliance with the requirements (c) and (d) – the integrity of the signature and data itself is also based on asymmetric cryptography. The usage of asymmetric cryptography itself can provide for a certain level of reliability to the transaction notwithstanding the use of the blockchain.

The analysis is correct for the blockchain, which is based on a standard asymmetric signature among the existing; otherwise, it may require additional expertise of the applied cryptography itself. For example, Bitcoin is based on ECDSA cryptography, which is a standard in the USA, EU, and many other countries. The compliance of the used technology to any certain standard is ensured by the fact that blockchain is open source, and thus, verifiable.

6. *Applicability.* The usage of any blockchain requires an understanding of whether the network itself it reliable or not. As of the day of publication, there are no technical standards that allow for formally defining the security of the network, but it is clear that the network with 3 nodes is less reliable than the one having three thousand. Therefore, an empirical analysis of number of nodes, hash rate, consensus mechanism, and existing experience of the use will help to find a proper blockchain for concrete legal tasks.

As it was found, data insertion inherits both features of the asymmetric cryptography and the blockchain. In practice, blockchain provides for a reliable decentralized timestamping and a secure immutable public repository.

Being decentralized, timestamping becomes more effective: disappears so called «single point of failure», meaning that the risk of corruption, multiple sorts of denial-of-service attacks is much lower especially if we are talking about scaled blockchain networks. At the same time, the transactional costs as to the achieved level of data protection and timestamping are affordable if not say, low. For example, the cost per publication in Emercoin is around 0,1 cents of US dollars (at the time of this publication). The average cost per transaction in Bitcoin is 2 US dollars, and at the highest historical point of exchange rate, it was around 25 dollars, which still can be affordable, for example, if the alternative to timestamping of copyrights is a visit to a notary public in person, which can be costly and time-consuming.

Timestamping is important for contracts, protection of copyrights and authorship and other evidence where proof-of-existence is required. But before the

blockchain, timestamping itself was not an open issue, the blockchain just raises the reliability of timestamping when compared to previous technologies. The real advantage of the blockchain is that it can extend the use of electronic communication, make it more «smart».

When data insertion is applied with some sort of blockchain-based technologies as tokens (Ethereum, NXT, NEM and others), smart contracts[11] (Ethereum, EOS and others), name-value storage (NVS) (Emercoin, Namecoin and others), it can make legal relationships more «intelligent» and interactive. The electronic document, while it is a file, is still a paper analogy – «flat» and non-interactive. With blockchain, the user can issue bearer instruments, power of attorneys, transfer and manage rights online.

For example, an artist can create a copyright and use www.emernotar.io to protect it in the blockchain. The artist will publish via this web-service in Emercoin a hash sum of the file adding a hash of his/her identity with the help of PayPal payment. In the result, the artist will have a NVS record[12] in Emercoin blockchain [24], where «Name» field is a hash record of the created picture and the field «Value» which contains the hash of email of a PayPal account which was retrieved as a result payment (therefore, the payer is the owner of the record). The user may also wish to add to this record a license data or any other public message. Then such NVS record can be transferred (i.e. sold) to any other user, and copyrights are transferred as well.

Another example can be a power of attorney. The hash of the file that contains the text of a power of attorney can be inserted in a NVS record or a smart contract. This then carries this data and has an expiration date and can be terminated by the issuer. To check the authorization of the attorney, the counterparty will check the integrity of the file by comparing hashes, and the status of NVS record or smart contract will tell the user if delegated rights are still valid or not. In «flat» paper PoA or even in an electronic file digitally signed, that would not

[11] Usually the term «smart contracts» is attributed to [23], however, Ethereum introduces their smart contracts as a tool for creating applications, which by fact are not necessarily contracts.

[12] Name-Value Storage is similar to the concept of tokens but non-monetary. In this record, data is stored in the form of «key & value» pair. «Name» is a searchable indexed key, and is always exclusive in the database; therefore, no one can create the record with the same Name while it is valid. «Value» is the second field, where the user adds any arbitrary information related to this Name (for example, user's name and telephone number). The NVS record is valid during the period defined by the user. The NVS record can be transferred to any other user of the blockchain, terminated or updated. In all these cases the initial record is not changed (the data is immutable in the blockchain) but new records with the same Name are inserted in following blocks with the updated information. See more details in Namecoin https://namecoin.org / and Emercoin https:// emercoin.com/

be possible, the principal cannot remotely revoke PoA at any moment, or vice versa to issue a new document or extend the existing PoA in minutes.

Another important feature of that as any closed system it can provide for proof of non-existence. It should be noted that «evidence of absence» is a fundamental gnoseological issue [25]. To assert the absence, one needs to check all the existing places, after which it can be argued there is nothing found. Due to the fact that the blockchain is a closed database, it can serve as a solution for a reliable local proof of non-existence.

This is important for jurisprudence since the parties can agree that a certain fact should be reflected in the blockchain to trigger the legal consequences for them or some rights and obligations to appear. The absence of the expected data in the specified blockchain will be considered as reliable evidence for private relations.

To mention here that the original blockchain protocol does not have a native lookup tool for inserted data. But for practical use, especially for legal purposes, it is important to have a reliable data retrieval system. To provide for the exclusiveness of records, there must also be developed algorithms that deny repetitive insertion, if the same data has ever been published thereof. There is no known implementation in the blockchain as a part of protocol core by the moment of this publication, but it can be be developed as an overlaid technology using the Name-Value Storage technology and custom developed decentralized applications (DApps) using smart contracts.

The main idea of this solution is that algorithms trace the ledger and select the inserted data to the custom database, which is by the fact an interpreter (the filter). When the user tries to publish the same data (for example, in «key-value» pair where the field «key» must always be exclusive through the whole database), the algorithms will then deny the publication. By fact, such «watchdog» can be omitted by publishing directly to the ledger the same record because as we mentioned above, the blockchain has no native censorship mechanisms to filter data (except the double spending denial), which is already published. Anyway, double publishing does not make much sense, because there is still timestamping, and strict chronology is in place. So, the first record is always the first, and the evidence of absence thereof is achieved by the whole scan of the ledger. Therefore, the role of a data retrieval mechanism is very important here, as it must present the reliable result of the search in the ledger.

Also, the blockchain database can be used for public purposes. For example, the government can keep cadastral records of ownership of real estate. The difference is that the blockchain is a distributed database that does not require a high level of trust in the central holder of such a database. However, this is a topic for another research, as there are a lot of other legal issues as well.

Table 2

#	Issue	Comment
1	Is the blockchain reliable?	Consensus mechanism, number of nodes, hash rate, history of successful use helps assess the reliability of concrete technology.
2	Which asymmetric cryptography is in use?	Is it a standard cryptography? Which standard? Is there any expertise of the compliance with the standard? If the cryptography is not standardized, is there any expertise? Does it comply with Art.6 of UNICITRAL Model Law on Electronic Signatures?
3	Which method is chosen: data insertion, anchoring or hashing?	Anchoring is useful if other metadata must be published. Data insertion for public purposes, and to protect the data integrity itself. Data integrity and privacy are also provided if data is ciphered. Hashing is for privacy and for verification of data authenticity, but the user must securely keep the data itself beyond the blockchain.
4	What method of data insertion is chosen? How much data can be inserted per one transaction?	Different scripts and methods provide for different file capacity limits. There may be some constraints, and theoretical flaws that must be taken into account depending on the purpose and required reliability.
5	Is there a reliable data retrieving mechanism from the ledger?	The blockchain wallet may not necessarily have native lookup tools or they may not have a user [friendly] interface.
6	Are there tools for the search of proof-of-existence or proof-of-non-existence?	Typically, the blockchain will not have native censorship mechanism. Therefore, the applied filters must be reliable and correspond with the use case. If the task is proof-of-existence and exclusiveness, only the first record must be considered as valid. If local proof-of-non-existence, then the absence through the whole ledger must be ensured.
7	Is exclusiveness of entry necessary?	If so, then take into account that a blockchain is designed as free of censorship. Therefore, there needs to be some sort of «watchdog» solutions developed on top to ensure that the same data will not be inserted, otherwise, the lookup instrument need to know how to filter irrelevant data when finding the first ever entry. Such overlaid solutions are available in Name-Value Storage technology (Emercoin, Namecoin and others) or if designed through a smart contract/DApp (Ethereum, EOS, TRON and others).
8	Is there an applicable law or an agreement between the parties to use the blockchain for a contract signing?	Any specific jurisdiction may or may not provide a framework for electronic signing. And thus, do parties need to have a prior-agreement where they mutually recognize blockchain signing/insertion as legally binding for themselves (if the law does not provide this by default)?
9	Are identity and authenticity reliable?	Typically, trusted third parties (CA/TSP) may provide for identification and authentication services. As many standards and best practices are applied as better, as they all are imperfect. However, any use case may require a different level of identification/authentication.

Ending of Table 2

#	Issue	Comment
10	If data insertion is used for copyrights	The non-third-party scheme may include a prior "handshake" when signatories identify each other and exchange with each other their public keys (blockchain addresses) by meeting in person, for example. Signatories may publish their public keys through their public social accounts or perform a penny bank transition or use other services which are not purposed to provide ID services howbeit can be relevant evidence as well. A good practice is if an author will: insert in the blockchain the hash prior to sharing the file anywhere include license terms in the publication include the author's name (pseudonym) or hashes of their contact details (if privacy is preferred) publish blockchain transaction ID in their public social account or use third-party services to connect transaction ID and their identity (for example, using a banking payment).

The user may wish to sign the data or a hash it is depending on the purposes. Some facts that require publicity can be inserted in the blockchain in its initial state and vice versa hashed or cyphered data provides for privacy.

A buzz question that recently appeared in the blockchain-oriented community is whether the smart contract is a contract? It is important to admit here that there is no general answer. As it comes from this research any concrete blockchain and any concrete case must be considered in the context of law and practice. This is the same as if someone were to ask if a napkin constitutes a contract or not. If one wrote a contract on the napkin (meaning that it has all elements of a contract), then yes, this is a contract.

The result of this study is Table 2, which allows you to analyze the applicability of the data insert for legal purposes.

Conclusion

In the result of this research we saw that the blockchain is useful for legal relations. The blockchain transaction is signed using asymmetric cryptography. That is why it inherits all properties of the modern cryptography and can be applied to sign legal documents and certify facts. This is also confirmed by the analysis of UNCITRAL Model Law on Electronic Signatures.

The real use of the blockchain comes from the nature of this technology. Towards the legal counter-parties (signatories) the blockchain plays the role of a re-

liable channel of the communication and a timestamp machine ensuring that the message will be public, immutable, irrevocable and accessible at any time.

The comparison of the blockchain in regard to the public key infrastructure shows that trusted third parties are required to play the role of certificate authorities; otherwise blockchain addresses are pseudonymous.

Users may wish to establish their own private channels of communication by peer exchange of their public keys (actually, blockchain addresses). They can also use open channels of communication, such as social accounts, where they share their public keys (blockchain addresses) upon the so-called scheme of «web of trust» or they can use conventional public key infrastructures with Certificate Authorities/Trust Service Providers.

The blockchain itself does not have any layer of «trusted services» and, therefore, cannot compete with such highly developed systems as European eIDAS. But it does not mean that the blockchain cannot be endowed with relevant layers of ID services, multi factor authentication, hardware signing devices and other properties. For that reason, the blockchain and blockchain-related technologies must be standardized.

The practical advantage over PKI is that the blockchain has one inherent feature out-of-box, which is timestamping. It does not require any centralized third party such as TSA, as in the traditional PKI scheme.

The blockchain which uses standardized asymmetric cryptography can be applied to legal relationships without obstacles. Otherwise, non-standard cryptography may require painful expertise to prove its reliability. Many known blockchain projects (Bitcoin, Ethereum, EOS, Emercoin, Litecoin and others) are based on standard cryptography.

Data insertion in the blockchain is a method of use of the blockchain beyond cryptocurrency. To make it happen, the user must publish a transaction, applying special scripts to add arbitrary data and «burn» coins.

Blockchain anchoring and blockchain hashing are subsets of the concept of data insertion. Instead of the initial data, the user publishes some metadata and(or) a hash value of this data. Anchoring and hashing are useful when privacy is required. Also, it reduces the bloat of the ledger.

Why might one wish to use the blockchain for legal purposes?

Reliable timestamping is useful for protecting copyrights. The author can publish in the blockchain the data (hash) before to share it with anyone. Any claims in the future can be resolved easier because of the timestamp which provides evidence of having this data earlier than anyone else.

The blockchain can make electronic contracts more interactive. For example, the Power of Attorney can be revoked or extended remotely by the principal at any moment by publishing updated information of the status of the document. For example, using Name-Value Storage or a relevant smart contract app.

Such publishing of legal documents can be useful for any sort of bearer documents. To make them more interactive, beyond revoking, the parties may wish to transfer NVS records or tokens. The bearer will show the electronic file of the warehouse receipt to certify their rights. The hash sum of the file will be published in NVS record or a token data. Therefore, it can be transferred to a new owner or filed for receipt of goods at the warehouse.

To sign a contract remotely, the first signatory can hash their legal document in the blockchain and send it to the counterparty. The counterparty will answer by publishing it again. Therefore, signatories, having each other's blockchain addresses known, will understand that they remotely came to the agreement.

This paper is an outcome of the PhD research performed inside of the Joint International Doctoral (Ph.D.) Degree in Law, Science and Technology, coordinated by the University of Bologna, CIRSFID in cooperation with University of Turin, Universitat Autonoma de Barcelona, Tilburg University, Mykolas Romeris University, The University of Luxembourg. Thanks to supervisors of Oleksii Konashevych Professor Marta Poblet Balcell, RMIT University (Melbourne, Australia) and Professor Pompeu Casanovas Romeu, La Trobe University (Melbourne, Australia). Special thanks to Oleg Khovayko, who is a developer of Name Value Storage in Emercoin for the consultation during this research.

REFERENCES

1. Nakamoto, S. «Bitcoin: A Peer-to-Peer Electronic Cash System», available at: ttps://bitcoin.org/bitcoin.pdf (accessed August 28, 2019).
2. Sward, A., Vecna, I. and Stonedahl, F. (2018), «Data Insertion in Bitcoin's Blockchain. Ledger. 3», pp. 1-23.
3. Gipp, B., Meuschke, N. and Gernandt, A. (2015), «Decentralized Trusted Timestamping using the Crypto Currency Bitcoin», the Proceeding of iConference 2015, iSchools, 2015.
4. Ober, M., Katzenbeisser, S. and Hamacher, K. (2013), «Structure and Anonymity of the Bitcoin Transaction Graph», Futur. Internet, Vol. 5, pp. 237-250.
5. Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T. and Capkun, S. (2013), Evaluating user privacy in Bitcoin, In: Lecture Notes in Computer Science, p.596.
6. «Bitcoin address · Programming The Blockchain in C#», available at: https://programmingblockchain.gitbook.io/programmingblockchain/bitcoin_transfer/bitcoin_address (accessed August 28, 2019).
7. «Bitcoin blockchain size 2010-2019 | Statistic», available at: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/ (accessed August 28, 2019).
8. «Ethereum Chain Data Size Growth», available at: https://etherscan.io/chart2/chaindatasizefast (accessed August 28, 2019).
9. «OP_RETURN», available at: https://en.bitcoin.it/wiki/OP_RETURN (accessed August 28, 2019).

10. «Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS)», Glossary of Terms, Abbreviations, and Acronyms, available at: https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf?agreement=true&time=1548119951687 (accessed August 28, 2019).
11. Schneier, B. (1996), Applied cryptography: Protocols, algorithm, and source code in C. John, Wiley & Sons.
12. «Announcing the first SHA1 collision», available at: https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html (accessed August 28, 2019).
13. Menezes, A.J. (1997), Handbook of applied cryptography, CRC Press.
14. Trcek, D. (2006), Managing information systems security and privacy.
15. (2011), Electronic Signatures and Infrastructures (ESI), Time stamping profile (ETSI TS 101 861).
16. (2008), Electronic Signatures and Infrastructures (ESI), Policy requirements for time-stamping authorities ETSI TS 102 023 , ETSI-TS102.
17. Barker, E.B. (2006), Recommendation for Obtaining Assurances for Digital Signature Applications, NIST.
18. «Trust Services and eID» (eIDAS), available at: https://ec.europa.eu/digital-single- market/en/policies/trust-services-and-eidentification (accessed August 28, 2019).
19. «KSI Blockchain», available at: https://e-estonia.com/component/keyless-signature-infrastructure/ (accessed August 28, 2019).
20. Anderson, R., Bond, M., Clulow, J. and Skorobogatov, S. (2005), Cryptographic processors-a survey Cryptographic processors-a survey, Technical Report Number 641.
21. (2016), «ENISA: Security Guidelines on the Appropriate Use of Qualified Electronic Signatures. Guidance for Users», European Union Agency for Network Information Security.
22. (2001), UNCITRAL Model Law on Electronic Signatures with Guide to Enactment.
23. Szabo, N. (1997), «Formalizing and Securing Relationships on Public Networks», First Monday, Vol. 2.
24. «Emercoin NVS», available at: https://wiki.emercoin.com/en/Emercoin_NVS (accessed August 28, 2019).
25. Turvey, B.E. (2008), Criminal Profiling: an Introduction to Behavioral Evidence Analysis, Elsevier Science.

Received 07.08.19

А.И. Конашевич

ВСТАВКА ДАННЫХ В БЛОКЧЕЙН ДЛЯ ЮРИДИЧЕСКИХ ЦЕЛЕЙ.
КАК ПОДПИСАТЬ КОНТРАКТ С ПОМОЩЬЮ БЛОКЧЕЙНА

Исследована технология блокчейн, в частности, вставка данных (привязка, хеширование) в блокчейн как способ подписи документов и придания юридических свойств фактам. Проведен сравнительный анализ известных способов применения электронной цифровой подписи с методом вставки данных в блокчейн. Рассмотрены следующие вопросы. Что такое вставка данных в блокчейн и какие свойства они получают? В чем разница между вставкой, привязкой и хешированием в блокчейне? В чем разница между хешированием в блокчейне и цифровой подписью на документе? Будет ли документ юридически обязательным, если он будет закреплен в блокчейне? Какие условия надо выполнить, чтобы придать законную силу документу? Как можно использовать привязку для подписания контрактов, сертификации доказательств, имеющих юридическую ценность, обозначения временных отметок, подтверждения авторства и авторских прав, а также их

передачи, выдачи и передачи доверенностей и делегирования других прав, выдачи и передачи инструментов на предъявителя?

К л ю ч е в ы е с л о в а: блокчейн, OP_DROP, OR_RETURN, электронная подпись, eIDAS, PKI, доказательство существования.

О.І. Конашевич

ВСТАВКА ДАНИХ У БЛОКЧЕЙН ДЛЯ ЮРИДИЧНИХ ЦІЛЕЙ.
ЯК ПІДПИСАТИ КОНТРАКТ ЗА ДОПОМОГОЮ БЛОКЧЕЙНА

Досліджено технологію блокчейн, зокрема вставку даних (прив'язку, хешування) в блокчейн як спосіб підпису документів і надання юридичних властивостей фактам. Проведено порівняльний аналіз відомих способів застосування електронного цифрового підпису із методом вставки даних у блокчейн. Розглянуто такі питання. Що таке вставка даних в блокчейн і які властивості вони отримують? У чому різниця між вставкою, прив'язкою і хешем у блокчейні? У чому різниця між хешуванням у блокчейні і цифровим підписом на документі? Чи буде документ юридично обов'язковим, якщо він буде закріплений у блокчейні? Які умови треба виконати, щоб надати законну силу документу? Як можна використовувати прив'язку для підписання контрактів, сертифікації доказів, що мають юридичну цінність, позначення тимчасових відміток, підтвердження авторства та авторських прав, а також їх передачі, видачі та передачі доручень і делегування інших прав, видачі та передачі інструментів на пред'явника?

К л ю ч о в і с л о в а: блокчейн, OP_DROP, OR_RETURN, електронний підпис, eIDAS, PKI, доказ існування.

KONASHEVYCH Oleksii Ihorovych, Erasmus Mundus Joint International Doctoral Fellow in Law, Science and Technology, European Union. Graduated from National Aviation University in 2005. Field of research — use of blockchain for electronic governance and electronic democracy.