Emercoin Blockchain Anchoring as a Way of Singing Contracts

Oleksii KONASHEVYCH[a]
[a] *Erasmus Mundus Joint International Doctoral Fellow in Law, Science and Technology, EU*

Abstract. This paper explores benefits of a new method of cryptographic signing of legal transactions using the Name-Value Storage (NVS) technology of Emercoin. NVS not only permanently stores data, but also allows to change ownership by transferring data between blockchain addresses, establishing its validity and even changing data, while keeping a history of records with timestamps. A signatory creates an NVS record with the hash of a document and transfers it within the circle of signatories until everyone has signed it. The method also works for unilateral deeds, which can be transferable (for bearer instruments) or non-transferable, including a method where the signatory keeps the record under one's control. The third party can also be involved in the role of a notary, an arbitrator or an escrow, who can identify signatories, change the status of the deed and manage the NVS record. The article analyzes a probative value of the proposed methods for legal proceedings and compares these with the traditional PKI, such as eIDAS in EU. The conclusion is that the Carousel method can be considered as an alternative to existing methods, but mass adoption requires standardization and a normative background.

Keywords. Blockchain, Emercoin, eIDAS, digital signatures, smart contracts

1. Introduction

The use of the blockchain beyond cryptocurrencies is noticed in early days of running Bitcoin network, when the first arbitrary data (a newspaper title) was inserted in the generic block [1] in so called "ledger", the database in which the blockchain appears itself. Inherent features of being public and immutable and the strict chronology of records opened a variety of ideas of its use: permanent messages, hashing (anchoring) or ever creating decentralized applications and smart contracts [2].

There some methods mainly based on scripts how to insert data when the user performs a transaction and in the result the user's data is inserted in the ledger and the amount of coins they used are "burned" (terminated). The concept of hashing files on blockchain was described by Gipp, Meuschke, and Gernandt (2015) and proposed as a Decentralized Trusted Timestamping [3]. There is also a notable paper about methods of data insertion [1].

This paper explores the benefits of Name-Value Storage[4] technology (NVS) developed on the blockchain of Emercoin,[5] and it describes the original methods of a uni- and multilateral signing of users' data. These methods are presumably useful for signing contracts and deeds, and the reason they are discussed here.

The method of contract signing works as follows: signatories create an NVS record with a hash of the document and transfer it within the circle until every signatory has signed it. The method also works for unilateral deeds, which can be transferable (for bearer instruments) or non-transferable, including a method where the signatory keeps the record under their own control. In these scenarios, a third party can also be involved as a notary, an arbitrator or an escrow who can change the status of the deed and manage the NVS record.

This paper analyzes the probative value of the proposed methods for legal proceedings and compares them with Electronic Identification, Authentication, and Trust Services (eIDAS)[6] in the European Union which is considered a highly structured and developed system.

The second part describes the technology of Name-Value Storage in enough depth to explain the proposed methods and proposes methods for signing of legal transactions. The third part analyzes the legal aspects and probative value of electronic documents signed in this way.

2. Name-Value Storage Technology

Let us first describe the technology we consider using herein. Name-Value Storage (NVS) was developed by Emercoin [5] (since 2014). It provides for a service of storing pairs of data [name -> value] on the blockchain. The initial concept was inherited from the Namecoin [7]. However, Emercoin NVS allows not only arbitrarily cast information on the blockchain but to manage it using the wallet or API.

"Key" is an indexed, searchable and unique field (up to 512 Bytes). "Value" is a field where the user can store data exclusively related to the specified "Key" (up to 20 Kilobytes). Users can manage such NVS records:

- specify period of storage "Lease time", it is permanently stored in the ledger but during this specified time it is actively managed in a special Nameindex database of the wallet);
- transfer between blockchain addresses while the record is valid (during lease time);
- delete the record from the list of valid records at any time;
- update the Value data in the record (but the Key remains the same, users can track the history of all updates);
- atomic transactions, i.e. to transfer NVS record in exchange of Emercoin cryptocurrency;
- add a prefix and a suffix to the Name field to group records (for example, to create a ground of records of a same kind, therefore, it is easy to find them);
- NVS record is a payable, which means that any user can specify the name instead of the blockchain address and the wallet will automatically find the address to which this name is connected.

- user can send NVS record to anyone's address without the permission, when user creates a new NVS records, they may add explicitly any address (own or someone's else) or leave the field address blank, so the system by default will generate a new address which belongs to this user [4].

This feature technology enable the creation of a set of services: EmerDNS, EmerPDO, EmerSSH, EmerSSL, ENUMER, etc [8].

3. Carousel Transaction

Let us now discuss how this technology can be applied to real world situations. The "carousel" method for signing contracts is based on useful properties of a hash function and NVS technology. The user creates a file of a contract that contains EMC addresses of signatories that must sign this contract.

It is recommended that the contract contains a clause that describes the procedure of signing after which parties consider its text to be legally binding. For example: "The contract becomes valid when the Parties of this Agreement published its hash (SHA-512) in NVS record in Emercoin ledger from the addresses specified below: Address of the Party A [...], Address of the Party B [...]."

Then the first signatory calculates the hash of the file and adds it in the field "NAME" of the NVS transaction form. Following that, the signatory adds in the field "NEW ADDRESS" their own address, which was defined in the contract.

Then the first signatory creates an NVS record with the mentioned parameters, including LEASE TIME during which the NVS record stays under the control of the first signatory's EMC address.

When the transaction is published to the blockchain, it appears in the user's wallet among NVS records. What this means is that the user's data is cryptographically signed and inserted on the blockchain. From this moment they can send this record to the EMC address of the next signatory. It is important to note here that the first signatory should not leave the field "NEW ADDRESS" blank because the wallet will generate a new EMC address and automatically add it. If the user wants the transaction to be obtained on a specific address (as we mentioned earlier all signatories add their addresses in the text of the contract), they must explicitly indicate the address in the blockchain transaction.

It should be added here that the fact some addresses own a specific NVS record does not mean that they were signed by this address because the creator of the transaction can indicate any address they would like. Therefore, the second act after the signatory has created the record (or anyone created, as we mentioned, for example, the secretary sends the NVS record to the signatory) must sign it by transferring this record to the recipient.

When the next or the last signatory receives the NVS record, they make an update of this record and send it on to a specified EMC address.

The order is not important (unless it is important to the signatories themselves). Moreover, if the signatories send the transaction to the wrong address or to another person, for example to the lawyer, it is not a problem. The point of this scheme is that the party of the contract must sign it by transferring the NVS record from their own address.

The signatories must agree in the contract which address is the last. It is important that when the last signatory receives the NVS records, they must take an action as otherwise the signing is incomplete. The last address can be one of the following:

- the address of any signatory;
- an address of the third party such as a public notary, an escrow or an arbitrator, or any authorized person, whose role in the legal relations is mutually agreed upon by the parties, for example, to keep NVS record and change its status, to resolve claims, to terminate the contract, etc.;
- an unspendable address.

The described method is schematically shown in Fig. 2.

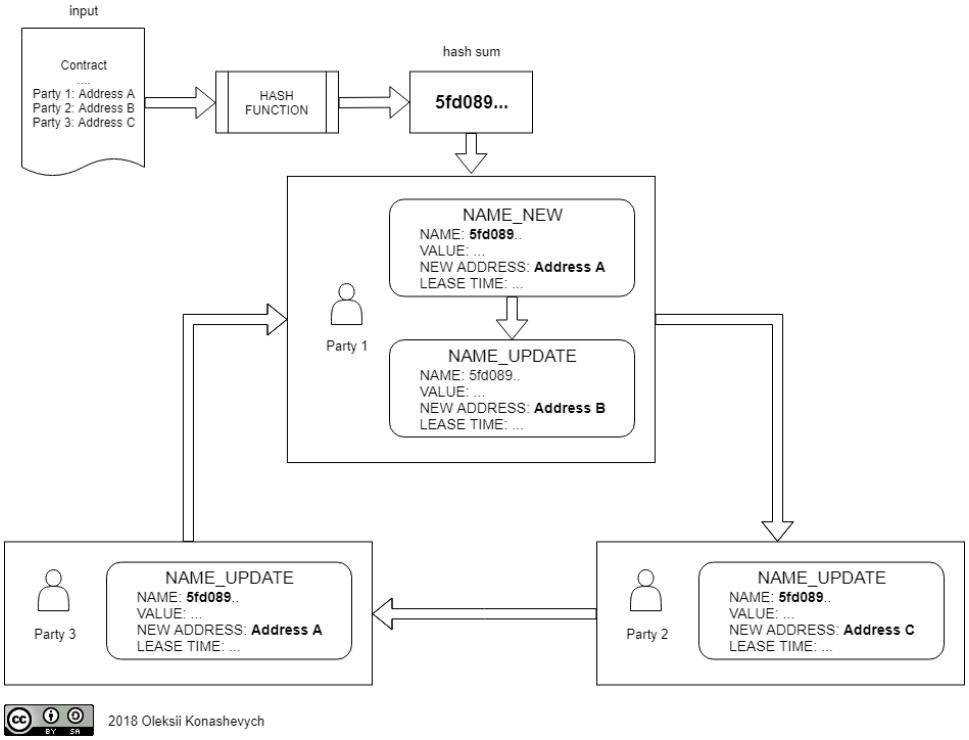

Figure 1. The scheme of Carousel method of contract signing using Emercoin Name-Value Storage.

3.1. What is an unspendable address?

An unspendable address is an address that has no private key. If the NVS record is sent to this address, no one can manage it during LEASE TIME. There is no key possible because the address was not created according to the algorithm (the blockchain address is the hash of the public key, and the result of Base58 encoding), but only as per formal requirements. The address itself can contain some humanly-readable information, so for this reason it is clear, that there is no private key possible. For example:

EMERCoinUnspendab1eAddressXXY2HB8a,
EMERCoinDeadDummyAddressXXXXZGgkUQ,
EMERNotarUnspendab1eAddressXTXM4L4 or
MERNotarDummyAddressXXXXXXXYSQRBh.

3.2. LEASE TIME and NAME_DELETE

The field LEASE TIME, which can be defined in days, months or years, must be no less than the period that is required for a full circle of signing among parties. It is preferable (but not critical) that the NVS record remain valid during the period that the contract is ongoing. Otherwise, anyone can "pick up" this record and create a mess in interpretation. The parties can relate the validity of NVS record to the legal validity of the document.

LEASE TIME can be terminated at any moment using NAME_DELETE command by the user who controls the address that retains ownership of the NVS record. Of course, the record is not deleted from the ledger, but only released from the control of the address, to say, becomes just an archived record on the blockchain.

3.3. VALUE

In this case, VALUE must contain any arbitrary data that will be publicly available on the blockchain in relation to the NAME record where parties keep the hash of the legal transaction. For example, one can keep a link where the document is stored, contacts, instructions for the next signatory or even the file itself.

3.4. Signing Irrevocable (non)-Transferable Unilateral Legal Transactions

Irrevocable unilateral deeds, like a gift or an irrevocable trust, can be performed by sending the NVS record from the signatory to the recipient. The signatory cannot revoke the NVS record after it has been sent to the recipient.

The nature of NVS technology is that NVS record can be sent to anyone's address without the permission of the recipient. That is why if the law requires the recipient's acceptance of the deed, the parties must follow the same steps as described in Subsection "What is an unspendable address?" i.e., the Carousel scheme; otherwise, if there is no need for the recipient's acceptance, they can perform this scheme.

There is also another aspect that must be considered regarding the fact that the keeper of NVS record can transfer it to any other address. Therefore, if the deed restricts the right of the recipient to convey their right or power to a third party, the signatory must specify the recipient's EMC address in the text of the deed, as described in Subsection "What is an unspendable address?", and add a notice in the deed that it will be invalid if transferred to any other address except the one mentioned.

The transferable nature of NVS records can be useful. If the deed is supposed to be transferable, the signatory should not write the address of the grantee in the text of the deed. So, any holder of the record will have the rights and power that follow from the deed. This is applicable to bearer instruments.

Therefore, the scheme looks as follows. The signatory creates the NVS record with the hash of the file and sends it to the recipient. The signatory can add the address of the recipient in the text of the deed; however, it is only a legal restriction, not a technological one, because the recipient still can transfer the NVS record to any other address or stop LEASE TIME. Therefore, it is recommended to define a legal consequence of these actions in the text of the deed.

3.5. Revocable non-Transferable Unilateral Legal Transactions

Revocable non-transferable unilateral deeds, like a power of attorney, can be performed by sending an NVS record from the signatory to their own address. Thus, the record is kept under the signatory's control and can be revoked by using the NAME_DELETE command. The signatory can also complete the signing by sending the record to the third party, who can serve the role of a notary, escrow, arbitrator, etc., see details in the next subsection. The recipient or anyone who wants to verify the record, receives the file with the deed, calculates the hash, and compares it with the hash published in the field NAME of NVS record.

3.6. Public Notary Scheme

Signatories will use a third party such as notary, arbitrator, or escrow (to simplify this let us call it just "notary") for two basics reasons.

Firstly, if the notary is a trusted party between counterparties that do not know each other, the notary can confirm each person's identity remotely.

Another use of the notary is that they can change the status of the deed in cases when the NVS record is out of the user's control.

There are two basics methods: to manage the validity string of the deed or to manage the NVS record of the deed.

The first scheme works as follows. The notary creates an NVS record with the "Identifier" of the deed as a NAME of NVS record and status (for example "Valid") as the field "Value." The signatory adds this Identifier in the text of the deed. Then the

signatory can ask the notary to change the NVS record to another status (invalid, expired, etc.).

This is useful because when the signatory transfers the NVS record to the recipient, they are not able to revoke the NVS record from the recipient's ownership. Thus, they can cancel the deed, asking the notary to change the status of the validity string.

The second is when the NVS record with the hash of the file is sent to the notary. The notary can change the status of the deed upon the request of a party.

These are also useful because the signatory can lose the private key, and they would, therefore, be unable to perform NAME_DELETE command.

Anyone who knows the Identifier can find it in NVS database since the NAME field is indexed and searchable.

3.7. EmerNick Instead of EMC Address

There is another useful feature of NVS records—an alias can be used as the payment and recipient's address. If one creates an NVS record, it can be used as an identifier of one's address, which is called in Emercoin infrastructure "EmerNick."[4] In the field NAME, the user adds their alias. In the field VALUE, the user can add their contacts, URLs, and other details.

Anyone can pay EMC to EmerNick or transfer an NVS record there, just by putting EmerNick as an address. The system will find the address to which EmerNick is attached and substitute it when the transaction is submitted. Parties can use their EmerNicks instead of addresses in their contract.

In terms of legal interpretation, "EmerNick" can be used if the deed allows cessation of rights without the authorization of the counterparty.

Parties must consider that EmerNick can be transferred to another address. Thus, if the legal transaction must be connected to the concrete person with a specified address, EmerNick cannot suit this purpose.

4. Legal Validity and eIDAS compliance

4.1. Methodology

Electronic Identification, Authentication and Trust Services (eIDAS) is a regulation on standards for electronic identification and trust services for electronic transactions, established in EU Regulation 910/2014 of 23 July 2014.[6] eIDAS established formal and actual requirements for digital signatures and identification of users. Neither Emercoin nor the proposed method herein has obtained any certificates or licenses at the time of writing this paper.

However, Article 25 of eIDAS makes this regulation technologically neutral since it does not exclude other technologies and methods: "An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures."

Thus, let us consider the probative value of the proposed methods. For this reason, we found relevant the methodology which is provided by Article 6 “Compliance with a requirement for a signature” of UNCITRAL Model Law on Electronic Signatures (2001):

“(1) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person.

(2) The signature creation data were, at the time of signing, under the control of the signatory and of no other person.

(3) Any alteration to the electronic signature, made after the time of signing, is detectable.

(4) Where a 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.” [9]

4.2. Analysis

As for the first requirement, there is a solid relationship between the signatories and the file of the contract provided by cryptographic primitives and the blockchain.

The blockchain addresses of all signatories are explicitly mentioned in the contract. The hash sum is calculated from the file of the contract and placed in the field NAME of NVS transaction. Then, the NVS record with the hash sum is sent to the next signatory as per the address mentioned in the contract. This transfer is performed by signing the blockchain transaction with the private key. Therefore, when the next user receives the NVS record from the address mentioned in the contract, they can be assured that it was cryptographically signed by their counterparty (whose EMC address is mentioned in the contract).

If the NVS record is sent to another address not mentioned in the contract or sent from the address out of the contract, then the mismatch is visible.

The sole control of the address is provided by the private key. The blockchain address is generated from this private key through a series of transformations using hash functions and Base58 encoding.[10] The private key is the only way to make an NVS transaction from the address to which it is related.

Emercoin blockchain is based on Bitcoin code, and it is open source;[11] therefore, the mechanism of blockchain addresses and private keys is verifiable.

The alteration of an electronic signature is impossible on the blockchain without its detection. It is guaranteed by ECDSA algorithms used for signing blockchain transactions.

To ensure verifiability, the wallet must work as a full node, i.e., to keep the complete history of transactions. The default Emercoin wallet works as a full node.

The integrity of the file is ensured by casting the hash sum (checksum) of it on the blockchain in the NVS record. Since the hash is a one-way function, any alteration of the file that contains the text of the contract is detectable because it will not match the original hash stored on the blockchain.

There is another way to ensure the integrity of the file. To publish the file in the field VALUE. However, it can only store 20 KB, and it is public by design. Therefore, hashing has another benefit, the file remains disclosed to the general public.

In addition, it is better to use hashing with a length of 512 bits for two reasons: 1) it provides better encryption and 2) the field NAME is limited to 512 bytes length). It is not recommended to use old hash algorithms, for example, SHA-1, since at least one

collision is already known (the collision means that one hash sum equals to more than one input).

As we see from the above analysis, this method offers a high probative level for the transaction and relation with the signatories. However, this level can be achieved using just asymmetric cryptography with a number of existing tools. What therefore distinguishes this method?

4.3. Timestamp

One of the most distinguishing features of the blockchain is timestamping. Each transaction has its own proof of existence at the exact time. Average tolerance accuracy is around 10 minutes per block.

Asymmetric cryptography and existing methods of signing legal transactions cannot guarantee a correct timestamp because the signatory performs it on the local machine and can change time and date settings. This can only be achieved with the help of Public Key Infrastructure and third parties.

A public key infrastructure (PKI) is a set of technologies and procedures that enables deployment of public-key cryptography-based security services.[14] In PKI, one of the providers is responsible for the provision of time and date information. At the moment when the transaction is performed, this third party "Time Stamping Authority" (TSA)1 logically adds timing data to the transaction through the internet connection.

The blockchain in this sense is a kind of third party, but a collective one and has a distributed non-centralized nature; thus, it significantly reduces the risk of corruption and centralization.

4.4. Identification

Public key cryptography requires public key infrastructure for a simple reason—to guarantee that a particular public key belongs to a claimed entity/person. This is done by a certification authority (CA), which issues a certificate (mainly x.509 standard is used) that ensures this is binding. Such a certificate can be verified by anyone knowing the CA's public key, because the certificate is digitally signed.[12]

The blockchain network can serve as a kind of Public Key Infrastructure, where the blockchain address is a public key. However, without certificates issued by a CA, the blockchain itself ensures anonymous identity (or better to say "pseudonym"), because only the person that has the private key to the particular address can sign the transaction.

Signing the blockchain transaction is actually the same as signing data when we are talking about PKI, but the difference is that the signatory signs the blockchain transaction that also contains the user's data, while the classical scheme of digital signing includes only the user's data.

[1] Trusted timestamping processes are specified in RFC 361 (Adams et al., 2001) and the ANSI ASC X9.95 standard (American National Standards Institute (ANSI), 2005), which augmented RFC 361 with data-level security requirements. Both specifications describe processes that require a central time stamping authority (TSA) to issue timestamps and ensure their validity.

There are two practical reasons for an identification: to allocate the holder of rights and to impose obligations.

For rights, the holder is interested in proving their identity. Even at the moment of signing, the acquirer of a right is anonymous, but they can prove their identity at any moment using the private key, to say, the person who holds the key is the right holder.

The obligation has a different interested party. Here the creditor is concerned about the identification of the debtor. The proposed method in its pure implementation cannot provide for a high level of identification.

Parties need a preliminary agreement and an arrangement to share with each other their addresses. Doing so ensures that legal transactions signed from such addresses lead to the exact person and this person agrees that this is legally binding.

The qualified electronic signature complaint with eIDAS compared to this scheme has an advantage because it does not require the signatories have prior relationships; they can even not know each other. However, the signatory must have a relationship with a trusted service provider (TSP), which is the third party that identifies the user and ensures non-repudiation of the signature. Let us consider this case.

4.5. eIDAS Compliance

The qualified electronic signature complaint with eIDAS (QES) can provide for the equivalent legal effect of a handwritten signature (Article 25 of eIDAS Regulation), which ensures non-repudiation.

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 it 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.”[13]

To add to this, QES also requires a special secure hardware device. The device stores the private key and signs transactions. The device must be certified. For this reason, the proposed method herein cannot be considered as an equivalent to QES without a sufficient upgrade to the concept.

There is another type that is called “advanced electronic signature” (AES), which does not require hardware devices.

Since both QES and AES require compliance with standards and formal certification of a TSP, the proposed method cannot be considered comparable in this field.

In fact, the proposed method, if applied with the “notary” scheme (as we called it here) for identification of parties, would be similar to AES. But if a hardware device was also added, it could be considered as QES as well.

The benefit of the use of blockchain technology when compared to the classical PKI is that it eliminates the necessity of TSA since timestamp is an inherent feature of all blockchain transactions.

5. Conclusion

The Carousel method and its multiple variations must consist of two steps: the user inserts a hash of the file as NAME in the NVS transaction and then they use this record.

The NVS technology allows a user to transfer a record to another user, which is the same as if we passed the document to the next signatory. However, the most interesting aspect of this method is that the signatories include their blockchain addresses (which are analogs to public keys) in the text of the electronic document. Then the hash of this document is inserted in the blockchain transaction, which is then signed from the mentioned addresses.

The method is suitable for unilateral legal transactions when the record is stored on the signatory's address. The signatory can also issue bearer instruments. They sign the record and send it to the recipient, and the recipient is free to grant it to anyone else. The immutability of the blockchain is an advantage and a restriction at the same time. If the user sends the transaction to someone, they cannot retrieve it back. The user can keep the record on their own address, but they still lose access to the record if the key is lost. Therefore, we designed the Carousel method with the concept of a "notary." A third party issues a record where they certify the validity of the deed. Then the signatory includes the link to this record in their own record. Then the signatory can ask the notary to change the status.

The proposed method has advantages over traditional PKIs:

- timestamping is decentralized, while it is performed by TSA in PKI;
- hashes are irrevocably and permanently public because the blockchain plays the role of a global repository, while in the traditional scheme the signature is local.

We see that the digital signing is similar in principle. The traditional cryptographic signing scheme has an INPUT (something to be signed) and an OUTPUT (a string of characters which are obtained in the result of a cryptographic operation). The blockchain signing is almost the same, but the only difference is the user includes in as INPUT the arbitrary data (for example, hash of the contract) and data of the blockchain transaction and scripts. However, the insertable volume in blockchain is restricted to dozens of kilobytes. That is why the user may be interested in signing not the file (photo, document, etc.) but a hash (checksum), which gives the same effect in terms of validation of data integrity.

The traditional PKI method has advantages when it is regulated and performed by trusted service providers (TSP). TSP is the third party that identifies the person when they issue an asymmetric key. The x509 standard certificate issued by TSP is connected with the public key and indicates a specific person; with a special hardware device that securely stores the digital signature, it ensures non-repudiation. The person who signed the legal transaction cannot deny this fact. The blockchain signing by inserting hashes does provide the same level of data integrity because it uses the same

cryptographic algorithms but does not ensure identification out of the box. Therefore, signatories must take care of that themselves.

The blockchain is in this sense just an infrastructure where trusted services can be built upon, including the use of hardware devices.

This paper has explored the benefits of a new method of cryptographic signing of legal transactions using the Name-Value Storage technology (NVS) of Emercoin blockchain. As we can see, it is not just a method of digital signing. Blockchain NVS technology brings a user a set of services because of its design. NVS permanently stores users' data in the ledger, allows ownership change by transferring data between blockchain addresses, establishing its validity and even changing data, while keeping a history of records with timestamps. With these methods users can connect blockchain technology to the content of the legal text: for example, one can manage the date of legal transaction use LEASE_TIME feature or create bearer instruments and evolve third parties as an escrow or a notary, make gifts by granting the NVS record to recipients blockchain address. This is different from just a signing a file, it is a new level of digitization of legal transactions. The main conclusion is that the Carousel method can be considered as an alternative to existing methods, but mass adoption requires standardization and a normative background.

Acknowledgement

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 Autònoma 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. Sward, A., Vecna, I., Stonedahl, F.: Data Insertion in Bitcoin's Blockchain. Ledger. 3, 1–23 (2018).
2. William Mougayar: Understanding the Blockchain, https://www.oreilly.com/ideas/understanding-the-blockchain.
3. Gipp, B., Meuschke, N., Gernandt, A.: Decentralized Trusted Timestamping using the Crypto Currency Bitcoin. In: iConference 2015 Proceedings. iSchools (2015).
4. Emercoin NVS - Emercoin Community Documentation, https://emercoin.com/en/documentation/blockchain-services/emernvs.
5. Emercoin, https://emercoin.com/.
6. Trust Services and eID, https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification.
7. Namecoin, https://namecoin.org/.

8. Introduction to Emercoin Services - Emercoin Community Documentation, https://docs.emercoin.com/en/Blockchain_Services/Introduction_to_Emercoin_Services.html.
9. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001. (2001).
10. Andreas M. Antonopoulos: Mastering Bitcoin, Chapter 4. Keys, Addresses. O'Reilly Media, Inc. (2017).
11. Emercoin Github, https://github.com/emercoin.
12. Trček, D.: Managing information systems security and privacy. (2006).
13. ENISA: Security Guidelines on the Appropriate Use of Qualified Electronic Signatures. Guidance for Users. European Union Agency for Network Information Security (2016).