June 2020

Using trace:original for digitizing documents according to MLETR

Commentary for the UN/CEFACT White Paper on MLETR-compliant records

ENIGIO TIME AB
Drottningholmsvägen 10
112 42 Stockholm Sweden
www.enigio.com

Content

Introduction

Enigio

Enigio Time AB is a Swedish tech company with a team of senior professionals in computer science and cryptography working closely with experienced individuals in banking and finance to digitize financial instruments and thereby lower transactional costs and operational risks involved with traditional paper documentation. Enigio has long been constructing a tenable solution for digitization of paper-based instruments where there is an expressed need or want to maintain a unique original. The presentation of an original to verify the legality and enforce a claim is still fundamental to the use of negotiable instruments and documents of title, which previously has only been thought possible by way of some sort of physical medium.[1]

Negotiable Instruments

Negotiable instruments have up till today not been digitized as no one has been able to fulfil all the requirements set out in the law. The required contents of negotiable instruments are laid out in national substantive law, but the law governing this area is greatly influenced by international trade and a globalized legal history. Our common historical use has allowed for a global acceptance of paper-based negotiable instruments which fulfil the mostly uniform requirements found in national legislations.

trace:original

The patented trace:original solution is a way of creating a digital document, which in all aspects mirrors the characteristics of a paper original, trace:original can be used to create any type of digital documents

Why trace:original?

trace:original originally aimed at mirroring the requirements laid out in the Swedish law on bills of exchange and promissory notes (Lag (1936:81) om Skuldebrev), which in turn reflect those laid out in the Geneva Convention providing a Uniform Law for Bills of Exchange and Promissory Notes of 1930. These requirements are to:

- be identifiable as an original (i.e. distinguishable from a copy);
- be an irrevocable, unconditional promise to pay;
- to a holder in due course;
- who can freely transfer it; and
- be evidenced in an original document controlled only by the holder.

The requirements set out for negotiable instruments and documents of title are formal, providing legal security by ensuring validity and enforceability so long as these requirements are fulfilled. Although national legislations seldom explicitly include electronic instruments, many countries have adopted a technologically neutral stance, providing for the existence of electronic alternatives if every formal requirement regarding content and form – including transferability and originality – is met.

[1] MLETR Explanatory Notes paras [81-82]

trace:original and MLETR

The United Nations Model Law on Electronic Transferable Records (MLETR) aims at further unifying international formal requirements for negotiable instruments, by encouraging technological neutrality and inclusivity. In Europe, the principle of technological neutrality and the general allowance of electronic documents and signatures is established in the eIDAS regulation No 910/2014, preventing documents from being denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form. The MLETR must be a globalized attempt at achieving the same effect, that electronic documents be given the same respect and legal recognition as paper documents – specifically regarding negotiable instruments and documents of title.

Our commentary on the MLETR and MLETR-compliant titles will focus on the use-case, trace:original, for a blockchain-based Distributed Ledger Technology (DLT), a Notary Service, working together with an electronic transferable document which complies with and exceeds the current goals of security and integrity in the normal course of international trade. The use-case must be made with regards to the construction of the model law, and so an analysis will be made regarding the relevant articles and general reliability standard to ensure that genuine blockchain supported documents will be MLETR-compliant, and warrant standardized acceptance across borders.

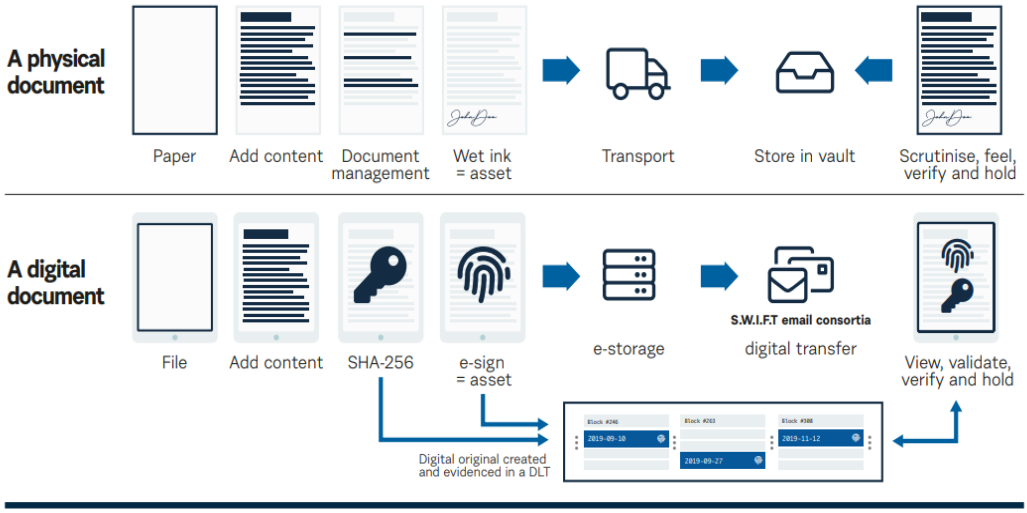
trace:original and Blockchain DLT

Cryptographic security, key-pair control, and singularity

Blockchain DLT works on a principle of cryptographic security, key-pair control, and singularity. Briefly put, a creator of a digital document using trace:original would fill in an ordinary file with the desired contents including eSignatures, it will then be "locked" by a public key to which only the recipients unique private key will correspond.[2] Only one individual, the holder of the private key which corresponds to a public key, will be able to control and amend the document in question. By limiting the control over the document to a single holder of a private key, we manage to replicate the legally defined requirement of possession as well as transfer of possession. The transfer is done by assigning the digital original to a new public key where the corresponding private key is held by the transferee.

Naturally the concepts of singularity and originality also follow this public key cryptography, the attachment of a digital signature – timestamped together with the digital contents on the document at that time – will prove that the document has not been tampered with since the signature was added, and verification of the cryptographic fingerprints (hash) will show the contents to be the original unless it has been changed or amended since the latest registration in the blockchain (i.e. latest version of the document). If an attempt at verifying the document to be an original should fail, it is immediately clear to the party concerned that another document is now the relevant original, it has since been invalidated, or it is an attempt at fraud.

[2] https://www.tradefinanceglobal.com/posts/the-key-to-digital-trade-finance-public-key-cryptography-explained/



1. *Figure 1: trace:original, how it compares to physical paper documents*

At a technical level, the validity is proven by using mathematical algorithms and "hashes", i.e. strings of generated characters and numbers. This cryptographic evidence is created by running a digital document of information through a hash algorithm and adding additional cryptographic fingerprints. This evidence will then be documented both in the document and the blockchain across distributed ledgers (acting as the cryptographic notary service) and given a public key. The actual document will be stored by the owner 'off chain', with only the corresponding cryptographic evidence and public key being published in the public ledger to act as evidence. This document may then be shown to contractual parties, opened up to add signatures and verified against the public ledger. Although a digital document will correspond to the cryptographic fingerprints in the ledger, it is practically impossible to reverse-engineer the original information from the hash or the private key from the public key to gain access or control.[3] These hashes will be reissued whenever a private key holder decides to make an amendment to the document, perhaps adding an eSignature, with an added timestamp. This has the consequence of invalidating previous versions, as the current digital original will have a new amendment, hash, timestamp and potentially also a new public key.

trace:original technology in summary

In summary, the technology is at the point where we can create an entirely digital singular document, which can be controlled by one individual and subsequently verified by whomever is presented with that document as evidence for a claim. There are additionally very few restrictions to the legality of electronic signatures as evidence globally.[4] And so, creating a digital document which may be legally signed and subsequently transferred between single owners as the only verifiable original is now a reality.

[3] https://www.eetimes.com/how-secure-is-aes-against-brute-force-attacks/#
[4] https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/document-cloud-global-guide-electronic-signature-law-ue.pdf

MLETR application and requirements

Application

The MLETR applies generally and internationally, providing for national legislators to incorporate the law for domestic application in a global environment. Electronic records are given legal recognition when functionally equivalent[5] and exculpated from any inter-jurisdictional discrimination.[6] The adaptation for global trade finance is important, as electronic records will do little to increase efficiency if subject to constant national scrutiny when crossing a border.

Legal validity

The explicit legal validity for electronic alternatives to paper-based documents[7] and wet-ink signatures[8] may not be strictly necessary, however it does certainly contribute to further harmonization. The eIDAS regulation in Europe and a multitude of other national and regional regulations accept the concept of electronic information as a substitute for writing on a physical instrument, as well as electronic signatures albeit with varying levels of security. Disregarding the more extensive formal requirements for negotiable instruments and documents of title, electronic documents and signatures have been successfully proliferated in many avenues of trade and finance. What these articles do provide for is the express allowance of digital amendments (e.g. endorsements) and signatures with regards to electronic transferable records as functional equivalents of paper instruments.

Electronic transferable record

The definition of an electronic transferable record is of course vital to the intended, perceived, and actual impact of the model law. A distinct characteristic of negotiable instruments is they must be unique to serve their purpose, and so it is vital for any court to be able to confirm the uniqueness of an electronic record to conclude that it functions as an actual original. The requirement of uniqueness is embodied in the MLETR[9], and is met by a block-chain supported digital document through the public-private key functionality. By ensuring that a single private key corresponds to a document which maintains its integrity, there is only one digital document in the world which has the same characteristics as the intended original. This is dubbed the 'singularity' approach within the MLETR, which aims to ensure that the holder may legally request performance while simultaneously avoiding the possibility of multiple claimants with electronic copies.[10]

The explanatory notes

The explanatory notes of the MLETR discusses the technological feasibility of guaranteed non-replicability, stating that the identification is not as obvious as with a physical medium.[11] This is incorrect, with the exception that the paper medium has a longer history within international trade contexts that grant it perceived certainty. The concept of a single paper document with a wet-ink signature is perfectly matched by a digital original evidenced in a DLT. Just as one would review a paper document and estimate whether

[5] MLETR Art. 7.
[6] Ibid Art. 19.
[7] Art. 8.
[8] Art. 9.
[9] Art. 10(b)(i).
[10] MLETR Explanatory Notes paras [83-84][94].
[11] Ibid. paras [81-82].

the contents are to be trusted, a digital original would be verified against a ledger as the currently valid version. Provided that the DLT used is secure, a digital original is easier, safer, and quicker to verify.

Functional equivalence

The rule of functional equivalence in Article 10 promotes the idea of a unique singular document in the digital sphere, and a blockchain-based freely transferable digital document is exactly that. Firstly, there is no limitation regarding contents, which may be written freely by contracting parties to meet requirements in national substantive law. Secondly, the holder of a private key will have complete control over the document, being able to make amendments and transfer it as necessary. Finally, the integrity of the document is secured through cryptographic keys. The private key must be kept safe in order to maintain continued integrity and prevent outstanding parties from interfering, but this is no different from the caution required when storing and handling traditional paper contracts. The Model Law further explains the notion of integrity and the required level, that level being absolute (either the document maintains integrity or not). What is required is the possibility to prove that *each set of authorized information,* (excluding purely technical data) *has remained unaltered from the time of its creation until it ceases to have any effect.* Blockchain entries supported by timestamping acts as evidence of this.

Possession

The MLETR also provides for express functional equivalence regarding possession and transfer of possession.[12] If a reliable method is used to establish exclusive control and to identify the person in control, an electronic transferable record will act the same as a paper document with regards to its transferability. Once again, the use of a private key, held by the person who would normally possess the paper document, acts as a perfect functional equal. There are no concurrent owners of a private key (unless they for some reason be issued), and the private key should act as a suitable identifier – although the possibility of endorsement through name in the contract would act as a further identifying mechanism. In addition, instances of new transfers and amendments are registered as new "blocks in the chain", providing for transparency and the possibility of identifying each transfer that occurs. The MLETR does not require the information itself to carry an identifying function, so the naming of a rightful possessor is not necessary; the identifying nature of public key cryptography should be sufficient.

Reliability standard

The final deciding factor to whether a method lives up to the MLETR-requirements is the general reliability standard.[13] In practice the included "safety clause"[14] will undoubtedly be useful for administrators and owners of DLT based documentation, allowing for evidentiary principles to decide whether or not a solution has achieved functional equivalency. Enigio is proud to offer a solution which can be proved to provide a secure digital original. Regarding security there is a list of factors to be considered should the reliability of a given solution be called into question, and they may illustrate the suitability of blockchain supported digital documents as electronic transferable records.

a. **Operational rules**: The use of blockchain DLT relies upon a distributed (public) ledger to verify a common truth. In the case of trace:original a public ledger will be responsible for verifying the hashes corresponding to digital documents, and thereby ensuring that a

[12] MLETR Art. 11.
[13] MLETR Art. 12.
[14] Art. 12(b).

person can safely verify a public key as the most recent iteration of that document. This is also enshrined in the terms of each digital document, ensuring that any individual who signs a trace:original contract is subject to the evidentiary rules connecting the document to a public ledger. The points of evidence that prove the integrity and validity are found in these operative rules.

b. **Assurance of data integrity**: General assurance that the information is tamper-proof and immutable. As mentioned previously, this is achieved with trace:original blockchain timestamping; each step of the document's lifetime is recorded and remains intact even after the owner has decided to finally invalidate the instrument. The holder of a private key is furthermore unable to erase information, so there is no risk of fraudulent behaviour on their part.
c. **Prevent unauthorized access to and use of the system**: The exclusive control encompassed by public-private key pairs prevents any unauthorized changes. Such changes would also be visible to a public ledger which may then discount that change as performed by an unauthorized participant.
d. **Security of hardware and software**: Encrypted public key cryptography is incredibly secure and works based on a one-way hash – practically ensuring that the only way to access and make amendments to the document are by using the private key. Analysing it from a functional equivalent standpoint, it is just as easy to put a private key in a safe as a normal paper document, although a key offers additional subtlety. As mentioned, this one-way mathematical hash is practically impossible to reverse-engineer.
e. **Regularity and extent of audit by an independent body**: trace:original has been subject to a technical audit from an independent organization, and while it may be helpful for a potential user to perform a technical due diligence it should not weigh heavily in a court. The court itself ought to be the body that determines whether a digital solution is viable if there is a conflict related to the reliability of an electronic transferable record.
f. **Declaration of a supervisory body, an accreditation body or a voluntary scheme regarding the reliability of the method**: If there is a related national authority available that can give guidance and declare a method to be valid it should naturally be accounted for.
g. **Any applicable industry standard**: International industry trade standards for blockchain based digital originals have yet to be fully developed, however it is clear that DLT systems which operate within a closed community will create its own standard – as the operative rules within that community will guide any conflicts that may arise under the guise of party autonomy. With regards to individual components we have – wherever possible – used the industry standard. For instance, our hashing algorithm was developed by the American National Security Agency.

In brief, blockchain DLT should pass the general reliability standard without issue, being able to prove integrity, safe transferability, and uniqueness with no possibility of multiple individuals gaining access to the singular original. The inherent nature of the technology is one of evidential ownership, and it has been adapted to also allow for safe transfers.

Key Issues

Interoperability

A key point of issue in the past when discussing blockchain-operated platforms has been interoperability. While DLTs generally operate on a membership basis, counting on members to sign up to a unified set of rules and being unable to initiate agreements with parties outside of this membership, trace:original has circumvented this requirement. A subscription may be required to create a document but receiving or verifying such documents is completely possible without prior membership status – all that is needed is a computer and internet access. This will ensure it to be fully effective as a transferable instrument. If the system is closed, there is an established risk for a 'plethora of ledgers' to spring up without any possibility of cross-platform interaction, creating digital islands which attempt to increase inefficiency but to an extent far below what could be achieved otherwise.[15] There is also an issue regarding substantive law when considering DLT solutions which operate with a common rulebook; As negotiable financial instruments are characterized by an *unconditional promise to pay*, having this promise subject to conditions found in DLT registries may hinder the diffusion of digital solutions.

Ease of use

The use of the internet within a commercial context requires a level of trust between the two parties, as there can be questions regarding the legal significance of data received. This is especially true when parties are invited to operate outside their national *Common Trust Infrastructure*.[16] What Enigio has done is created a digital document which operates seamlessly within commercial entities own recognized infrastructure. A company which operates with their own unique web portal, SWIFT or by standardized encrypted e-mail may be reluctant to trust an independent ledger which they are unfamiliar with. The assurance that comes with a digitized solution that fits into previously existing trust infrastructures may come to be invaluable for the widespread adoption of electronic transferable records.

Conclusion

The technological foundation is sound for the creation, administration and secure use of electronic records as negotiable instruments and documents of title. A white paper which clarifies that a blockchain DLT based solution is the leading example of a digital document which fulfils every requirement set out in the Model Law would go a long way towards the perceived security and legal validity of functionally equivalent documents. Our understanding of the MLETR and the attached explanatory notes is that trace:original documents we have developed are suitable for circulation as transferable records, and that blockchain DLT in general is a suitable technology for providing the necessary notary service for those electronic functional alternatives to original documents. These further supporting guidelines to the Model Law would be very welcome, as digitizing negotiable instruments and documents of title will increase efficiency, security, and opportunity in the world of trade and finance.

For any queries regarding the Enigio trace:original solution please feel free to visit us at https://www.enigio.com/ or get in contact directly.

[15] White Paper Technical Applications of Blockchain to UN/CEFACT deliverables p. 10.
[16] White Paper on Trusted Transboundary Environment Ensuring Legally Significant Trusted Trans-Boundary Electronic Interaction p. 3.