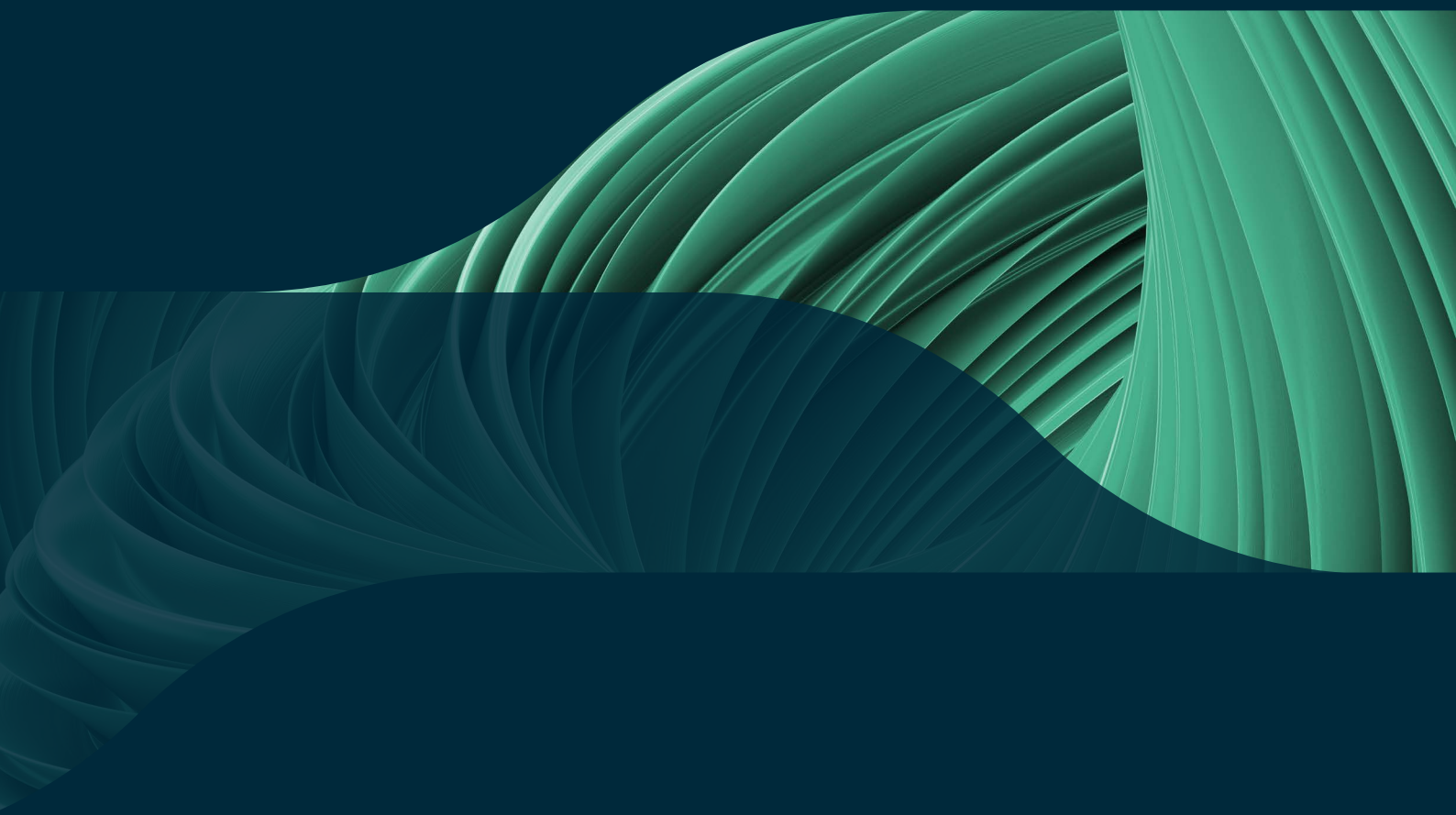
trace:original

A DIGITAL ORIGINAL DOCUMENT | How does it work?

JUNE 2021



enigio

Introduction

Fig.1| trace:original is like a freely transferable container for data

A large share of the communication in a trade finance transaction is already digitalised. Banks structure customer communication through portals, negotiate via safe e-mail and sign using e-signatures, not to forget SWIFT which has already enabled the digitalisation of many products and process steps between banks. A major obstacle for achieving a completely digital trade finance world has been the requirements to be able to manage and present documents in their original form.

Our focus has therefore been to create a digital document with the same properties as its paper equivalent. The trace:original document is designed to be able to hold all necessary data to execute a transaction and at the same time not being tied to any specific transaction infrastructure. More importantly it can also be managed manually by anyone with access to a computer and the internet.

If we want to see rapid digitalisation of trade and trade finance and corresponding processes and infrastructures, paper and digital documents must co-exist. We will have countries being early digital adopters and others lagging. An infrastructure agnostic digital trade finance document of any type can serve all the aspects of the global digital ambition extremely well.

Interoperability can be achieved on different levels and by using different tools. One of the most forceful ways of achieving interoperability is by standardisation of data definitions and data formats. A widely used standard is JavaScript Object Notation (Json Schemas). Using Json Schemas increases the usability significantly as it enables trade finance systems and other software to exchange data in a defined way regardless of which transaction platform or messaging system the transacting parties are using. A combined Json Schema library for trade finance documents coupled with data definitions standards would significantly boost digital interaction between transacting parties' through a step by step approach. This, without the need for any major re-engineering of the current IT infrastructures in banks and corporates. Json Schemas and the trace:original document is a perfect connector to achieve digital interoperability not only between blockchain based trade finance platforms but for all trade finance platforms.

How does trace:original work?

The trace:original solution is a method to achieve all properties needed to create, manage and invalidate a digital document such as a digital negotiable instruments or document of title or any other document that needs to be represented as an original.

Enigio provides technology that can create transferable, fraud safe and at any time verifiable digital original documents, where the holder can evidence possession and full control over the latest version of the document.

In a physical comparison, the digital trace:original file is represented by paper and the characters in the file are represented by the printed text and/or ink of a pen if the intention is to ensure originality. It has the same functionality as its paper equivalent but enables faster, safer and significantly more cost-effective management of these documents and does this in a digital environment.

Solution

The solution is unique and differs from other documents and has a different thinking compared to current blockchain and distributed ledger solutions as it introduces a new possessable digital asset and digital information class; the trace:original document. The document, the asset, is like a pdf document in that the document can be digitally stored in any way the holder finds suitable.

The trace original document is also a cryptographically secured file which means that the text (by technicians referred as the payload) of every version of the document is cryptographically locked by hashes evidenced both in the document and on a publicly distributed ledger. We will come back to the function of the distributed ledger below.

The trace:original solution consists of three components:

- the trace:original document, a data "container" with a defined beginning, end and content.
- a secured document key, with which the holder of the document can legitimise possession
- a public ledger, with the function of being a cryptographic notary service for all trace:original documents

The document

The document, the file, is written in plain text characters, supporting almost all languages in the world (the UTF standard). By using plain text, the document can be read in the simplest text editor but also read by a computer enabling Straight Through Processing of documents in front- and back office systems. The document is stored by the holder and no business content is published on the trace:original public distributed ledger.

To ensure that no text that has been previously written in the document has been altered or manipulated the text is secured using mathematical one-way algorithms, "Hash-functions". A Hash function is a publicly and open mathematical function that produces a sting of characters that is a unique identification of the data set, a "digital fingerprint" of the document (a file). Every time a file is processed by the Hash function it gives the same result as long as the data in the document stays exactly the same.

For a trace:original document, Hash functions are used to create cryptographic evidence proving the properties of the trace:original document. Enigio uses a Secure Hash Algorithm developed by the US National Security Agency based on 256 bits (SHA256). SHA256 produces a character string of 32 characters that can create 2256 unique character

strings, i.e. more combinations than the number of atoms on the planet earth. The hash becomes unique for the document and is also time stamped. By publishing the hash in a publicly available blockchain the evidence of the existence and the properties of the document are evidenced with mathematical certainty. Therefore, hash functions are ideal when:

- you want to ensure that digital data has not been manipulated and
- you do not want to publicize the content of the document.

Hash functions have been in common use since the 1950s and are used to ensure the integrity of passwords.

Anyone coming in contact with a trace:original document can verify its status and authenticity by using the public block chain. If the hash of the document produces the latest hash that has been published in the block chain for the document you know with certainty that your copy corresponds perfectly with the original, if it corresponds to a hash published earlier than the latest ledger entry for the document the copy is obsolete, and if the has does not correspond to any entry on the blockchain for the document, the document is either corrupted or a forgery.

The holder of the original document has complete and exclusive control of the asset. All business information is contained in the document and stored "off chain" by the document holder. That is, no business details are stored on the blockchain. When registering the document in the ledger, only the cryptographic hash-references – think of them as digital fingerprints — of the document identity, document properties, any evidence of amendments, and the holder's public key of the document are stored "on chain". Therefore, the blockchain is only a "publicly available digital notary service". A holder in possession of the correct document and the correct cryptographic key has full control of the document and is allowed to register amendments to the document in the ledger. Anyone with a copy of the document can verify if the received copy corresponds to the current version of the original against the ledger.

Cryptographic key pairs

To enable control and possession of the trace:original document the document is linked to an asymmetric key-pair. The key pair consists of a public and a private key. If the key pairs match you receive the value" true", in all other cases the value is "false". The public key is inserted in the document and published on the distributed ledger. In the trace:original solution a distributed ledger is used as an "incorruptible mathematical notary service" holding the evidence of the state of the document and to which public key (who is the current holder) the document is tied to.

To be able to prove ownership (possession) and add text to the document and successfully evidence this you need the correct private key and the latest version of the document to be identified as the holder of the original document. When the holder is identified and accepted the holder can publish the new cryptographic hashes that include the evidence of any added text to the document on the distributed and public ledger. However, you cannot alter anything previously written in the document, you can only add new text after the previous text entry. To be able to create new trace:original documents you must be a Full Node Member, a trace:original customer.
As a holder you can add text to the document or add a new public key to the document if you want to transfer it to a new holder.

The Distributed Ledger

The distributed ledger functions as a mathematical an incorruptible notary holding the history and the audit trail contained in the document without revealing anything about the contentions of the document. All is the "proof of the truth" hidden in plain sight as cryptographic hashes, ready to verify the documents stored "of chain" with the current holder.

Possession, Transfer and Endorsement of a trace original document

Proving Possession

If someone holding a copy of a trace:original document wants to verify that the holder really is in possession of the document the holder can create a "proof of ownership". The holder will use his private key and create a signature that is unique for the cryptographic key pair published in the document and in the public ledger.

Transfer

If the holder wants to transfer the document to a new holder the receiver needs to;

- create a new key pair,
- store the private key safely and
- send the public key to the current holder of the document.

The current holder needs to;

- insert the receivers public key into the document and
- publish the hashes of the document and the public key on the Distributed Ledger.

The holder has now lost control of the document, but the new holder cannot manage the document yet, because the document has changed and exists in a new version.

The now previous holder;

- now sends the new version of the document to the new holder who thereby has received the document and has the means (the private) needed to be identified a as the new holder of the document.

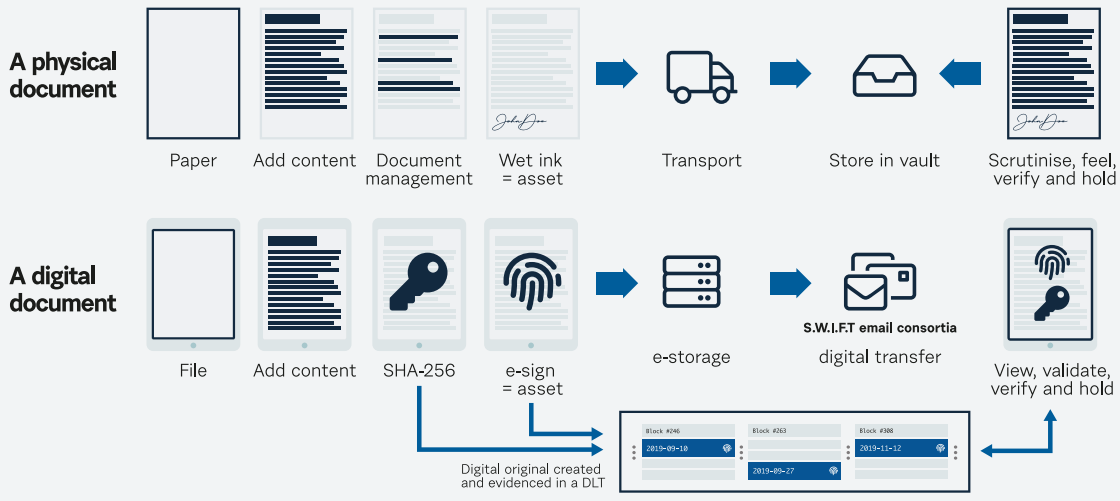
Enigio offers API's, software and free web services to do all the above.

As any valuable physical asset, you need to store your digital assets safely, i.e. the private key needs to be kept safe and not disclosed. If you lose the private key, you have lost the original just as in the physical world.

Endorsement

Endorsement is achieved by opening the document for an amendment (addition) and then adding the endorsement. This amendment can, if needed, be an e-signature. This can be performed in several different ways depending on the use case.

Fig.2 | trace:original, how to recreate what a paper document represents digitally



How to implement and use trace:original

To be able to create a trace:original document you have to be a subscriber. Banks or their software supplier can integrate trace original through the trace:original API framework.

Creating a trace:original document

Very simplified a new printer function is added to produce digital original documents. The user can choose if it wants to use its current KeyStore (HSM) and document archiving system. Enigio can if desired provide these utilities if needed.

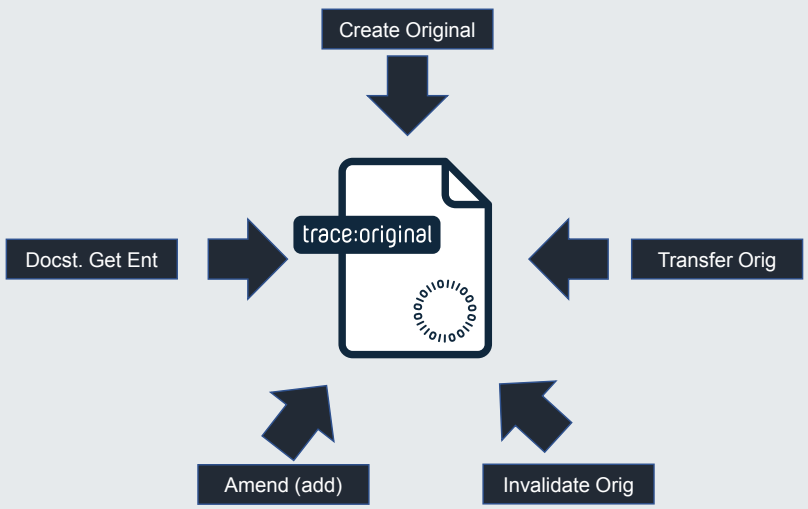
How to receive a trace:original document

A receiver of a trace:original document must inform the sender of the address to which the document should be assigned. In the physical world that would be the name and the address where to send the document. As possession of a trace:original document is defined by holding the private key associated to the original documents public key, the sender needs to assign the control of the document to the receiver's public key. The receiver needs to send chosen public key to the sender and hold the correct private key. If the private key is lost the new holder of the document cannot evidence possession of the document. Hence control of the private key is essential. Once the sender has inserted the receivers public key and registered this on the trace:original ledger and sent the new updated document to the receiver, the transfer of possession is complete.

Tools to manage trace:original documents

High volume users of trace:original would typically integrate their front and back office systems to the trace:original APIs. Subscribers to trace:original have a specific API enabling the creation of new trace:original documents. Subscribers will also maintain a synchronized and fully updated copy of the ledger, a Full Node. Other typical high-volume receivers of documents can once in possession

Fig.3 | trace:original APIs

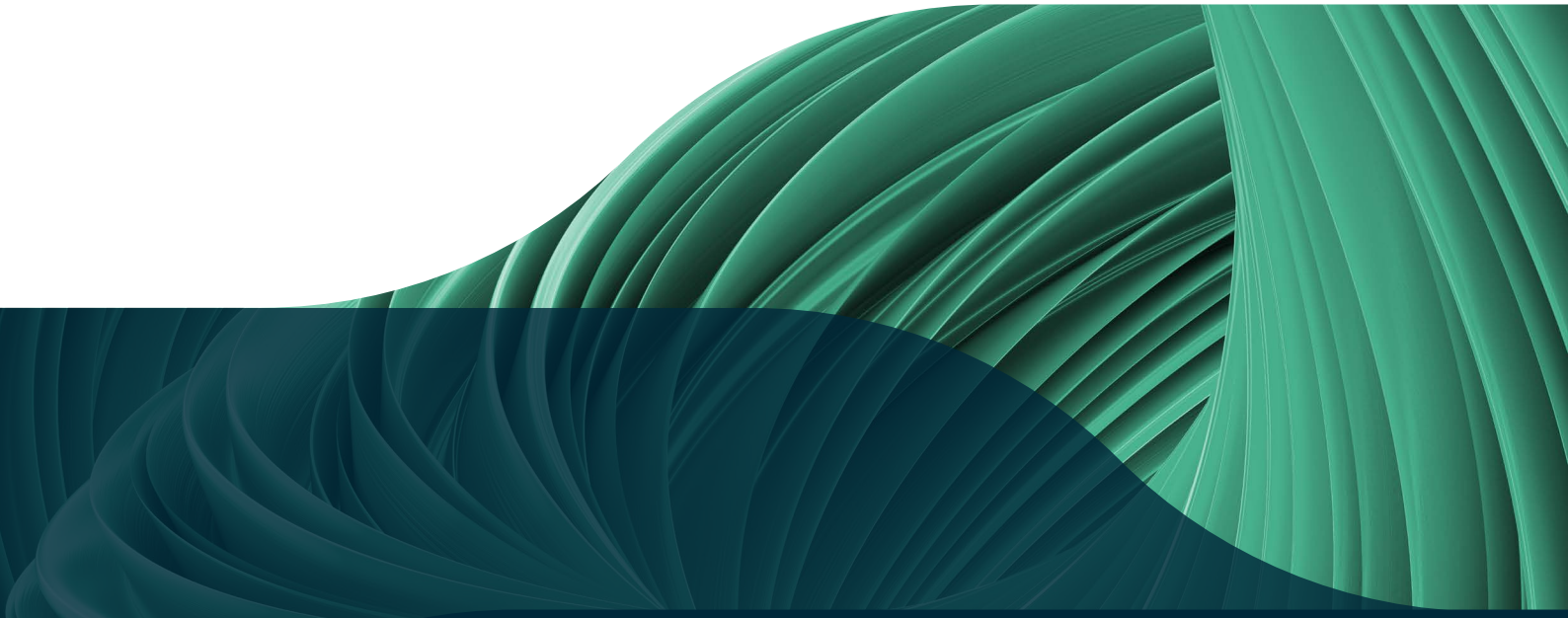


of a document make additions to, invalidate and transfer the document using APIs, and a Stakeholder node (e.g. a customs authority department handling customs guarantees). The node can be installed on premises, as a cloud service or as Software as a Service (SaaS).

User with lower volumes with limited need for automated processing can log on a web page (www.trace-original.com) where the user can receive and manage trace:original documents. Use of traceoriginal.com is free of charge and available to anyone, making it possible for any person or organisation to manage a trace:original document. However, on traceoriginal.com, you cannot create new digital originals, for this you need to become a customer of Enigio and have a full node installed. What is needed for anyone who needs to handle a trace:original document is access to a computer with a reasonably new web browser installed and access to the internet.

Json Schemas

The trace:original solution supports Json Schemas. Schemas are designed depending on the issuer of the documents and the purpose the document. The schema makes it easier to process the document content, for all parties concerned, as it defines objects in the document file. If a Json Schema is used in a document the document's schema is published on an internet URL by either the document issuer or an organisation responsible for a Json Schema standard. This schema can be downloaded by anyone coming in contact with the document. All trace:original documents are Ricardian contracts and are therefore readable by both man and machine, using a Json Schema does not in any way affect that ability for neither the machine nor the man.



enigio

ENIGIO TIME AB
Drottningholmsvägen 10
112 42 Stockholm, Sweden

Enigio offer solutions that ensure integrity and traceability of all your information to enable true and complete digital processes.

For more information, whitepapers and ways to contact us, please visit www.enigio.com.