siticom

INSIGHT: DISTRIBUTED LEDGER TECHNOLOGY.

A first step to tamper-proof documents based on DLT

© BY SITICOM GMBH
ALL RIGHTS RESERVED

WHY READ THIS INSIGHT?

Nowadays, sharing documents and information has never been easier. It is possible to share information by e-mail, to make it available **on websites for download or store it within various file systems distributed on hundreds of platforms worldwide**.

Some examples of common file sharing systems:

- DropBox
- OneDrive
- GoogleDrive
- IPFS
- Bittorrent

The mentioned solutions work great as long as **no one manipulates** the documents.

However, how can anyone make sure the content created and shared through the different systems has not been manipulated or changed. Knowing that a minor change in the content could sometimes have great consequences. For example, someone changes somewhere a “one” for a “no”, which may lead to a complete different interpretation of the intended content.

Taking the above into consideration, let's show **how to secure the content** you wanted to share, using the new Distributed Ledger Technologies (DLTs).

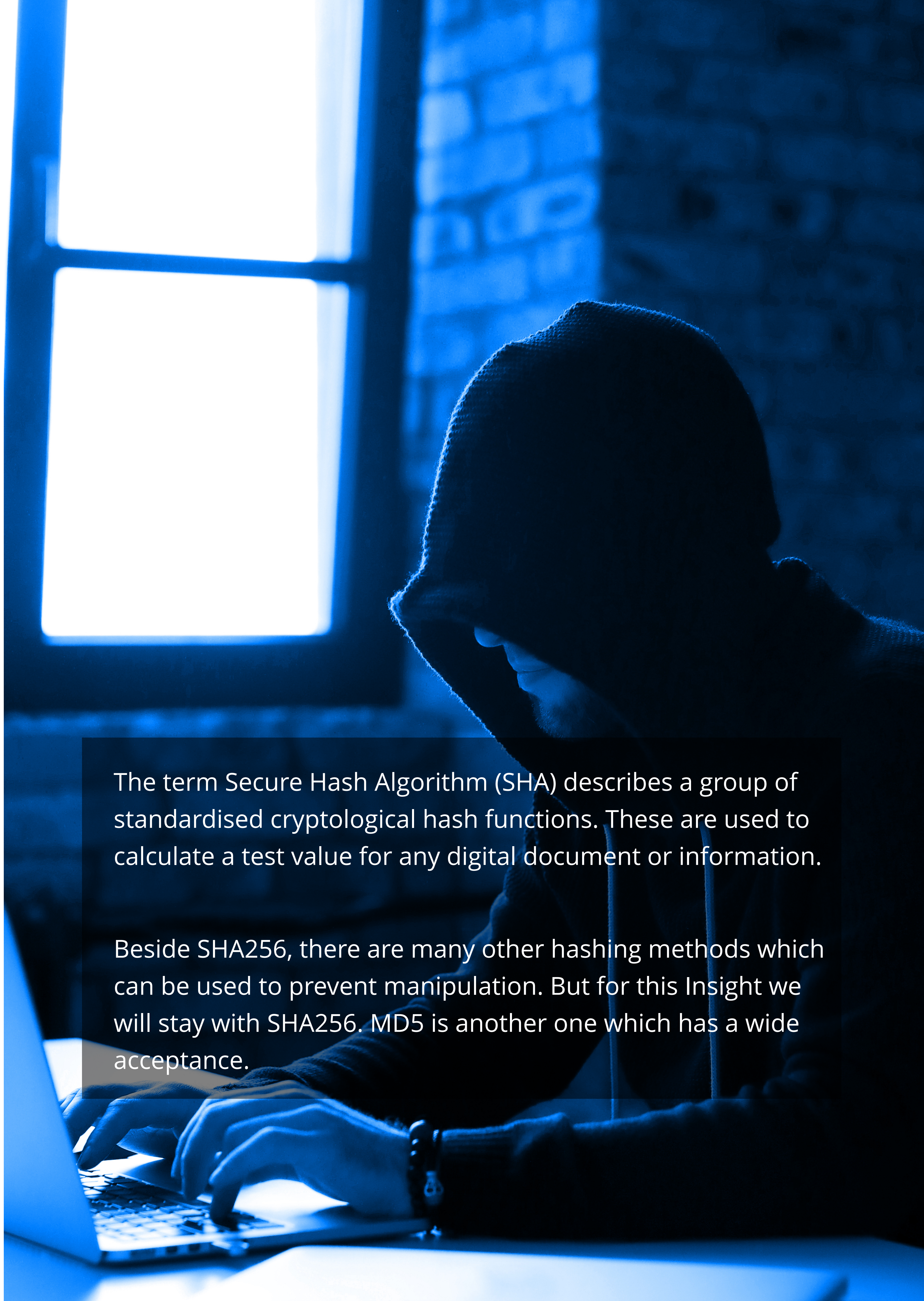
Let's talk about that.

SIGNETS AND HASHES - A SIGN OF TRUST

Before we dive into the digital methods, let's take a look at a more simple example such as letters and see how it was made sure, they weren't manipulated while being sent.

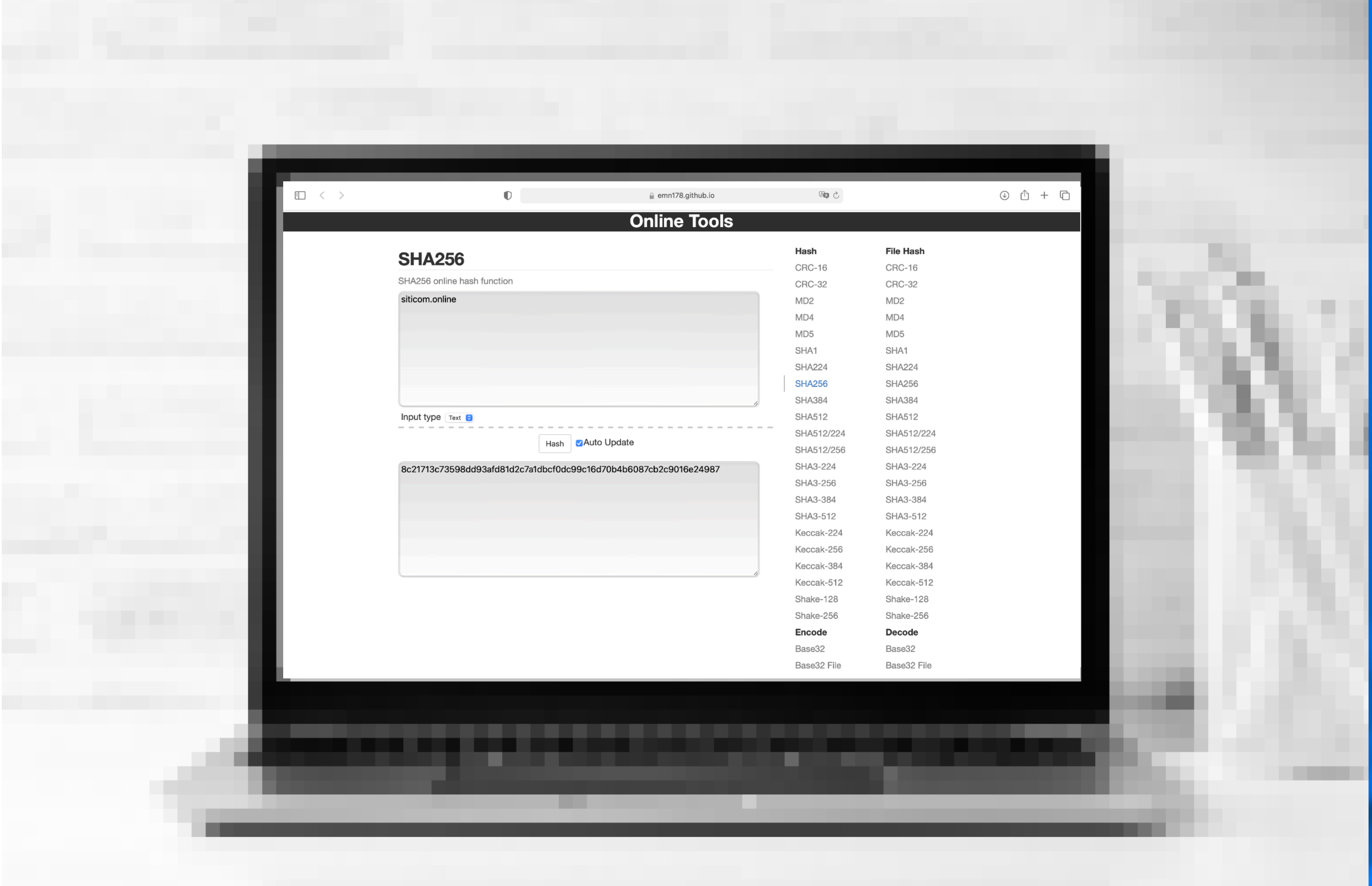
A common method to do so is to use a signet or a seal pressed into sealing wax or stamped on an envelope over the closing. If the seal or stamp is received broken or not fitting correctly, then the letter has been most probably manipulated.

Similarly, we can check today if the information within a document has been changed or not by using Hashing Algorithm such as SHA256.



The term Secure Hash Algorithm (SHA) describes a group of standardised cryptological hash functions. These are used to calculate a test value for any digital document or information.

Beside SHA256, there are many other hashing methods which can be used to prevent manipulation. But for this Insight we will stay with SHA256. MD5 is another one which has a wide acceptance.


emn178.github.io

Online Tools

SHA256

SHA256 online hash function

siticom.online

Input type Text

☑ Auto Update

8c21713c73598dd93afd81d2c7a1dbcf0dc99c16d70b4b6087cb2c9016e24987

If you want to verify, you can go to the webpage https://emn178.github.io/online-tools/sha256.html and try it yourself. Just type "siticom.online" into the text box.

Simply explained, SHA is a repeatable cryptographic algorithm which takes the information and calculates a unique checksum of letters and numbers with always the same length.

To make sure this is true, we prepared a small example where you can try it yourself.

If you take the string "siticom.online" and use SHA256 to generate it's checksum, you should receive the string

"**8c21713c73598dd93afd81d2c7a1dbcf0dc99c16d70b4b6087cb2c9016e24987**".

If you tried it yourself, then you can be sure, that this is true. You can do the same with documents and files, which also can have a SHA256 checksum.

POWERED BY IOTA

The IOTA Tangle is a new type of distributed ledger technology (DLT). It was created by the IOTA Foundation, a non-profit foundation incorporated and registered in Germany. The Tangle Network immutably records the exchange of data and value. It ensures that the information is trustworthy and cannot be tampered with nor destroyed.

COMBINE SHA AND DLT TO MAKE PUBLIC DOCUMENTS SAFE

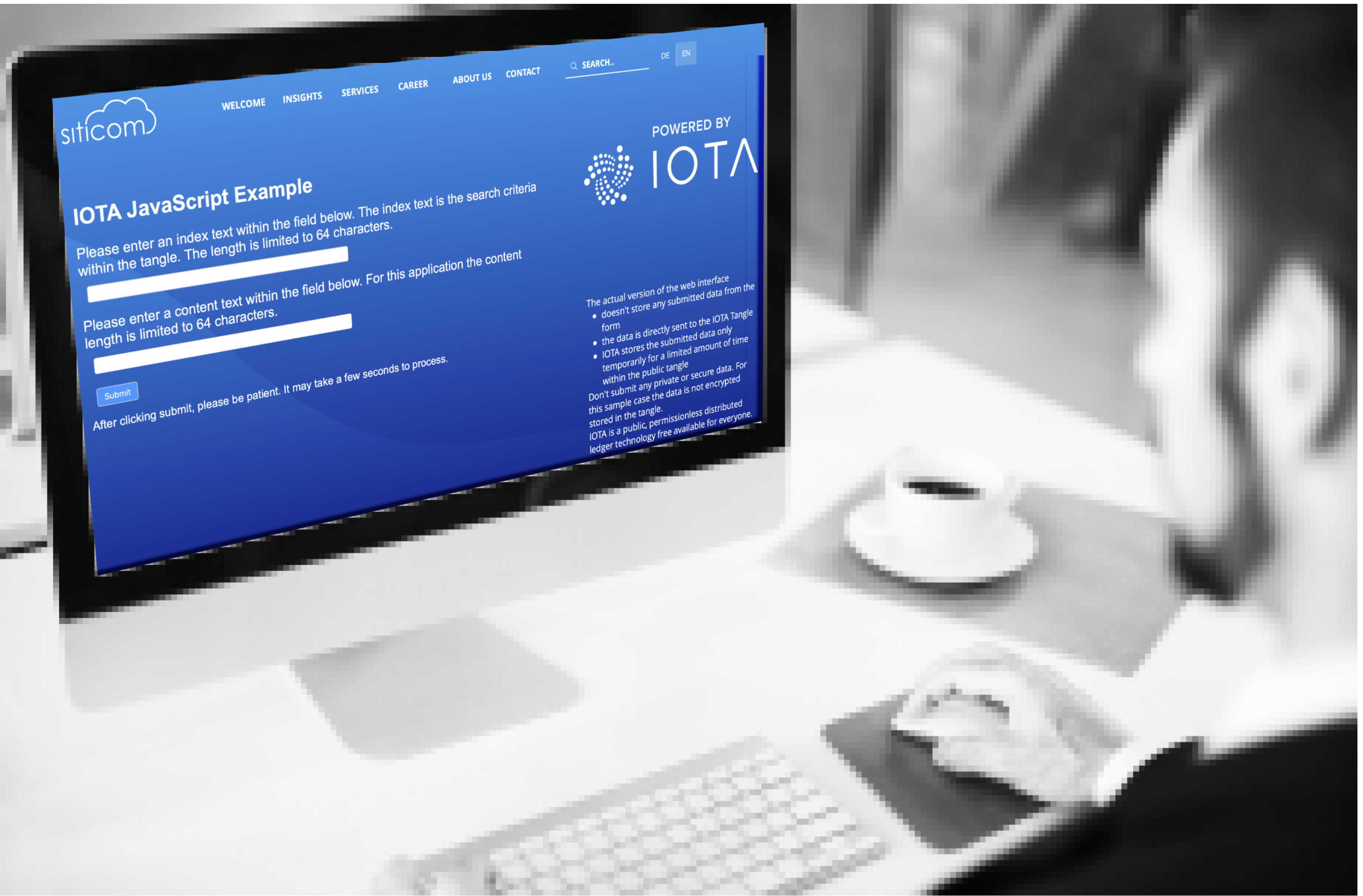
So far, so good. If we have a document and generated the checksum, we know the document wasn't changed at this moment. But how does this work if someone takes our document, changes it and sends it around with another checksum?

And here comes the DLT into play. Within a DLT we can store the checksum connected to a specific address which belongs to the author. This way it is possible to offer a check mechanism which allows to verify the information with a checksum tamper-proof stored in combination with a unique address.

For our small example we stored the checksum in the IOTA Tangle.

siticom implemented a web site which allows an easy way to add information to the Tangle.

https://www.siticom.online/add-data-to-iota-tangle



IOTA JavaScript Example

Please enter an index text within the field below. The index text is the search criteria within the tangle. The length is limited to 64 characters.

Please enter a content text within the field below. For this application the content length is limited to 64 characters.

After clicking submit, please be patient. It may take a few seconds to process.

The actual version of the web interface

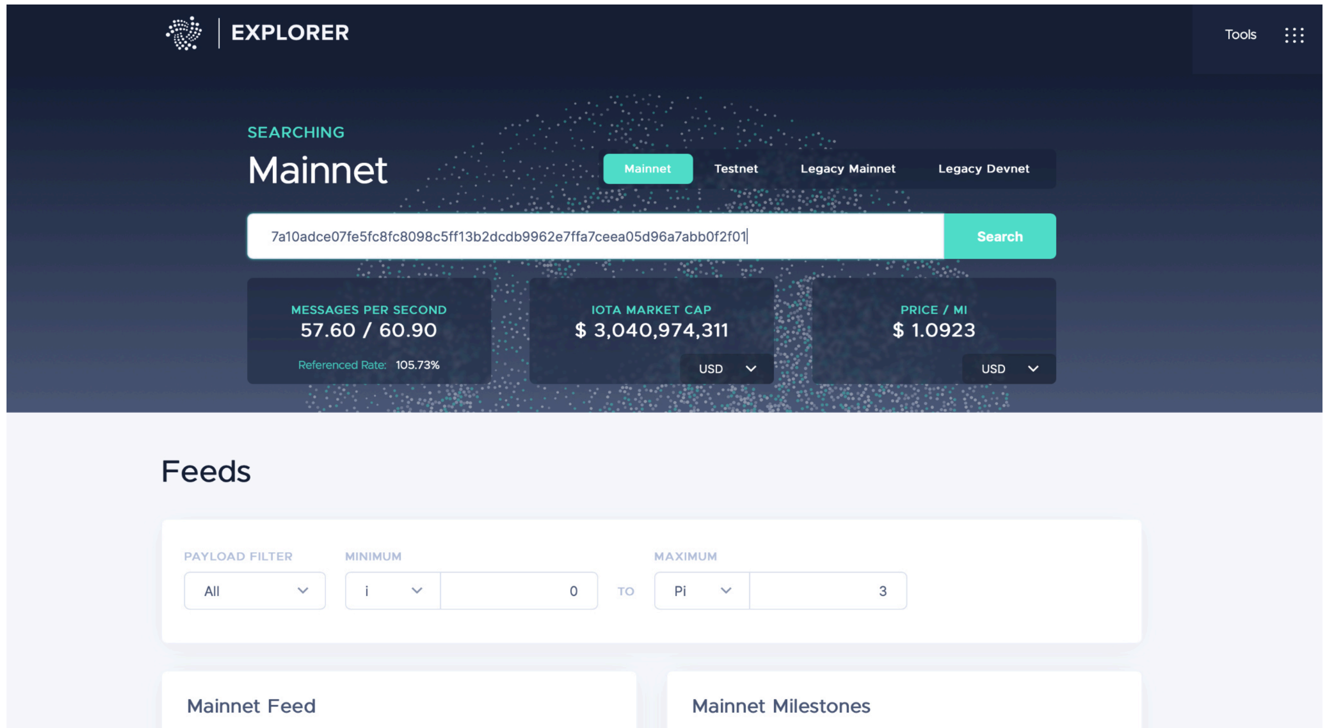
- doesn't store any submitted data from the form
- the data is directly sent to the IOTA Tangle
- IOTA stores the submitted data only temporarily for a limited amount of time within the public tangle

Don't submit any private or secure data. For this sample case the data is not encrypted stored in the tangle.
IOTA is a public, permissionless distributed ledger technology free available for everyone.

If you want to test it, go to the following DLT explorer - https://explorer.iota.org - and enter the following unique message ID

"7a10adce07fe5fc8fc8098c5ff13b2dcdb9962e7ffa7ceea05d96a7abb0f2f01"

within the search field. You should see the checksum, tamper-proof stored with the message ID.



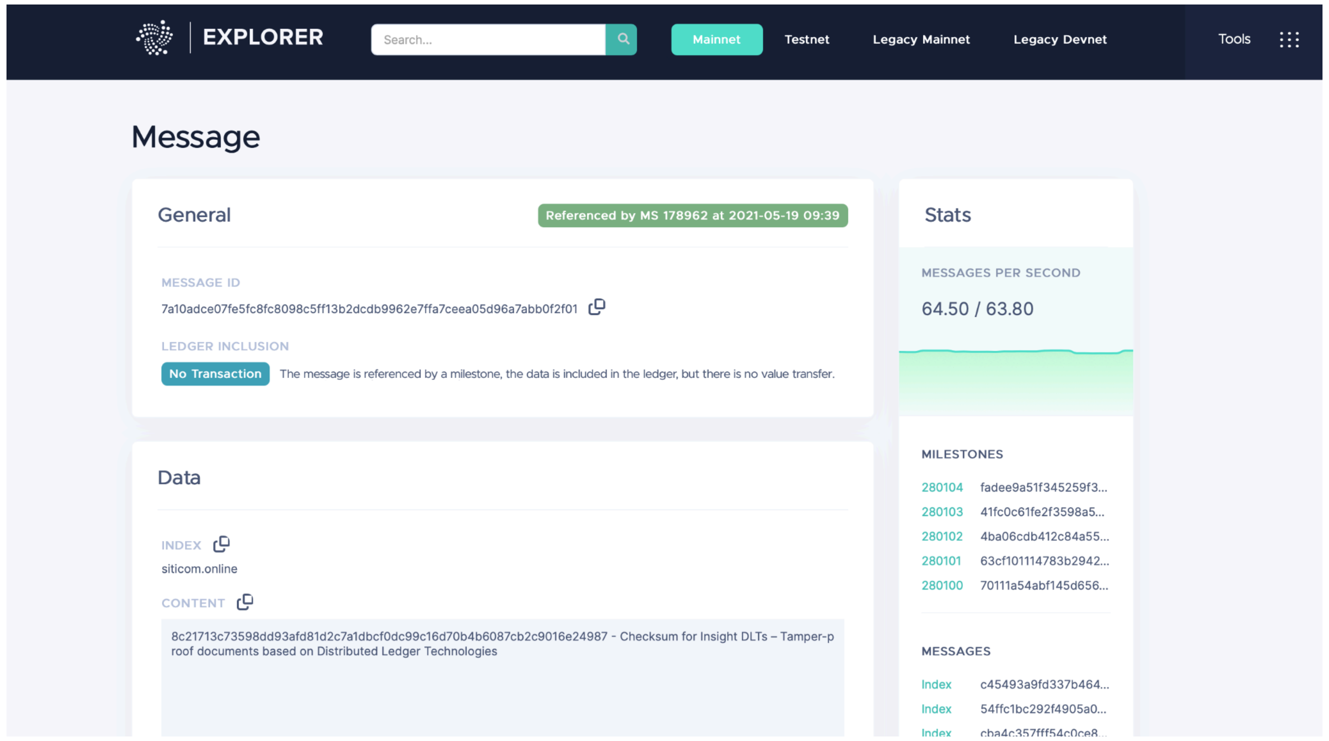
7a10adce07fe5fc8fc8098c5ff13b2dcdb9962e7ffa7ceea05d96a7abb0f2f01

MESSAGES PER SECOND 57.60 / 60.90
Referenced Rate: 105.73%

IOTA MARKET CAP $ 3,040,974,311

PRICE / MI $ 1.0923

PAYLOAD FILTER: All
MINIMUM: i 0 TO MAXIMUM: Pi 3



Referenced by MS 178962 at 2021-05-19 09:39

MESSAGE ID
7a10adce07fe5fc8fc8098c5ff13b2dcdb9962e7ffa7ceea05d96a7abb0f2f01

LEDGER INCLUSION
No Transaction The message is referenced by a milestone, the data is included in the ledger, but there is no value transfer.

INDEX
siticom.online

CONTENT
8c21713c73598dd93afd81d2c7a1dbcf0dc99c16d70b4b6087cb2c9016e24987 - Checksum for Insight DLTs – Tamper-proof documents based on Distributed Ledger Technologies

MESSAGES PER SECOND
64.50 / 63.80

MILESTONES

280104	fadee9a51f345259f3...
280103	41fc0c61fe2f3598a5...
280102	4ba06cdb412c84a55...
280101	63cf101114783b2942...
280100	70111a54abf145d656...

MESSAGES

Index	c45493a9fd337b464...
Index	54ffc1bc292f4905a0...
Index	cba4c357fff54c0ce8...

A DID could be used as an unique digital ID which can be signed and confirmed by public organisations and governments.

The DID itself is tamperproof stored within a DLT and represents a person or organisation within the digital world.

As soon there are decentralized identifiers (DIDs) available, you can even connect a document directly and the author can additionally be certified by an official source, and you can even proof if the source where you get the message ID from is trustable.

SOME MORE INFORMATIONS

If you want to know more about DIDs, SHA and tamper-proof documents, we added some links where you can find further details.

- https://www.w3.org/TR/did-core/
- https://www.iota.org/solutions/digital-identity
- https://blog.iota.org/enabling-document-authenticity-through-dlt-a-project-by-cgi-and-nordakademie/
- https://en.wikipedia.org/wiki/SHA-2

siticom

THE NETWORKS OF TOMORROW. TODAY.

CONTACT

FRANK REINEMER
EXPERT DIRECTOR

+49 175 2664139
frank.reinemer@siticom.de

ALEXANDER HEIGL
CHIEF CONSULTANT

+49 172 8849899
alexander.heigl@siticom.de

ABOUT SITICOM

siticom is a technology innovation company founded in 2010 with a focus on the digital transformation of infrastructure and networks of tomorrow. siticom's portfolio is geared towards the complex technological challenges of the future. The solutions and services range from technical and strategic advice to engineering services for planning and realizing network infrastructures in communication networks and corporate networks. Thanks to a highly innovative, flexible grid of system partners, siticom is able to implement high-quality solutions at short notice. The combination of consulting, design and architecture bundled with the assumption of system and implementation responsibility as well as test-automation distinguishes siticom as an independent system integrator.

For more information, please visit: **https://siticom.online**
Or Email us **info@siticom.de**