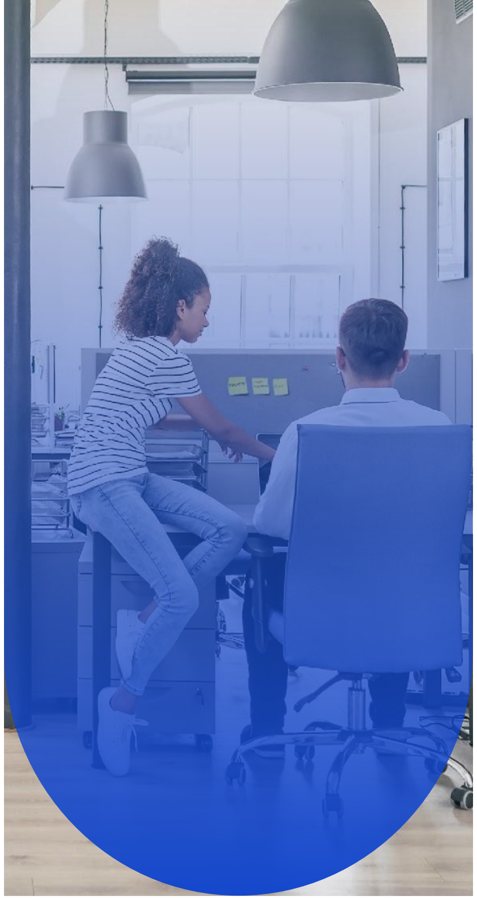
DocStudio

as Distributed Document Ledger

Using Blockchain ledger technology for providing documents immutability and notarization



Challenge: Document Existence and Integrity Verification

- Companies often face the challenge of securely establishing document existence.
- Traditional methods involving notaries or witnesses can be time-consuming.

However, now there is a better solution: Blockchain and Document Ledger Technology (DLT).

Key Benefits:

- ❖ Irrefutable proof of document existence at specific moments in the past.
- ❖ Assurance that the document's content remains unchanged since creation.

Understanding Blockchain

- ➔ Blockchain (with capital B): A distributed database established on a global network of over 100,000 enthusiast hosts.
- ➔ Used for recording data about transactions involving Bitcoin and various cryptocurrencies.

Key Features

- ➔ New blocks of data (known as "The Block") are posted every 10 minutes.
- ➔ Each block can contain approximately 2000 records of BTC or other cryptocurrency transactions.
- ➔ The first block, known as the "Genesis Block," was posted on January 3, 2009.
- ➔ Currently, there are approximately 792,900 blocks (as of June 21).

Short Text Messages on the Blockchain

- ➔ "OP_RETURN" allows the posting of very short text messages.
- ➔ Messages can have a maximum length of 80 bytes.

How can we use this?

Utilizing Blockchain: Document Fingerprinting with Hash Values

Limitations of OP_RETURN message size make it unsuitable for posting substantial documents.

The ideal alternative is to post a document's fingerprint, known as a hash value.

Hash Value

Hash value is a compact and fixed-size representation of a large amount of data.

Any changes to the original data will result in a different hash value.

Analogous to Notarization

Hash values can serve as a digital equivalent of notarization.

Publishing the hash value does not make the original document content public.

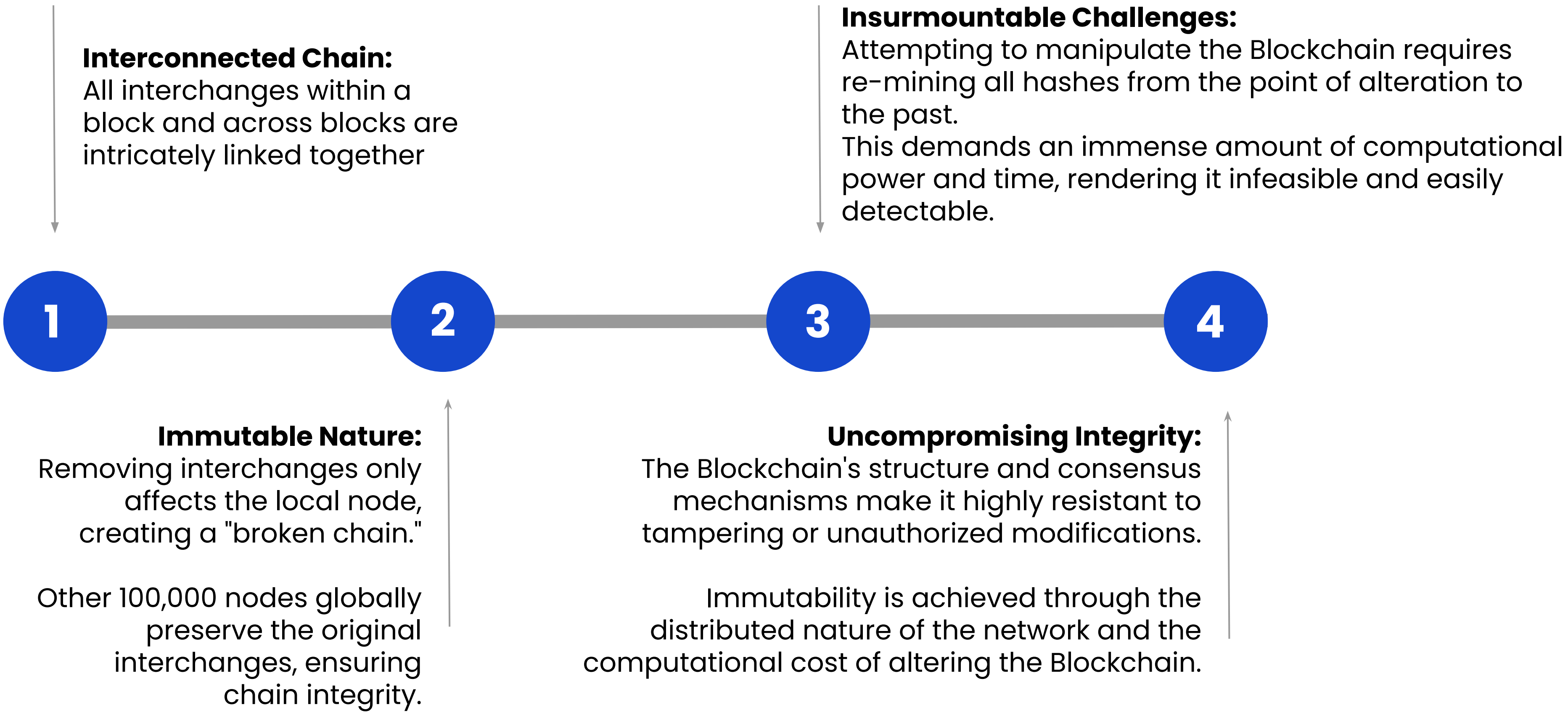
Confidentiality and Flexibility

Documents can be digitally notarized while keeping their content confidential.

The original document can remain unpublished until the need arises.

In summary, by utilizing hash values on the Blockchain, we can establish document authenticity and integrity without revealing the document's contents, providing a secure and flexible digital notarization solution.

Maintaining Immutability on the Blockchain



Interconnected Chain:
All interchanges within a block and across blocks are intricately linked together

Immutable Nature:
Removing interchanges only affects the local node, creating a "broken chain."

Other 100,000 nodes globally preserve the original interchanges, ensuring chain integrity.

Insurmountable Challenges:
Attempting to manipulate the Blockchain requires re-mining all hashes from the point of alteration to the past.
This demands an immense amount of computational power and time, rendering it infeasible and easily detectable.

Uncompromising Integrity:
The Blockchain's structure and consensus mechanisms make it highly resistant to tampering or unauthorized modifications.

Immutability is achieved through the distributed nature of the network and the computational cost of altering the Blockchain.

Few words about "Hash"

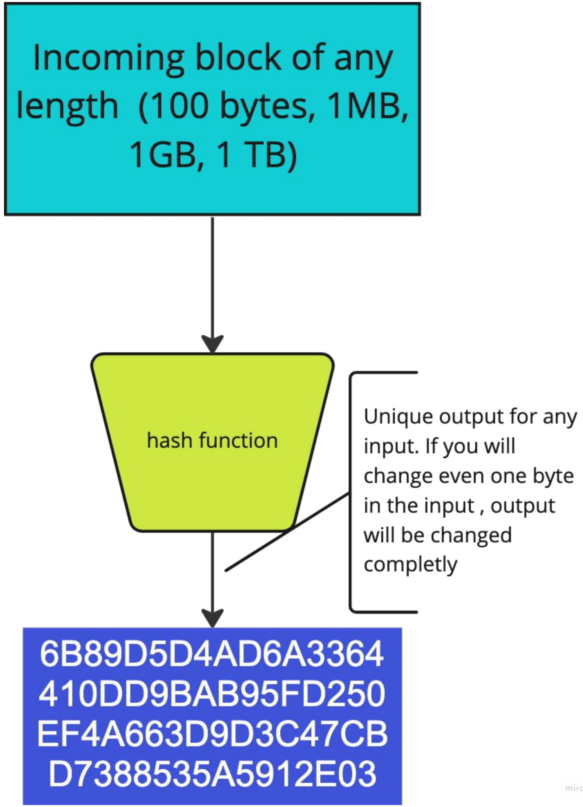
We like to call hash as fingerprint.

Like all people have their unique fingerprint

"Hash" is a cryptographic function that converts a string of characters of any length (100 bytes, 1MB, 1GB, 1TB) into a unique output, or hash, of a fixed length

The essentials are as follows:

- Hashing is a one-way method for cryptographically encoding data (the term "one-way" means that the original input cannot be reconstructed from the hash).
- It produces a fixed-length output for any input.
- The same input will always produce the same hash.
- The most popular algorithm used today is SHA-256.


Incoming block of any length (100 bytes, 1MB, 1GB, 1 TB)
hash function
Unique output for any input. If you will change even one byte in the input , output will be changed completly
6B89D5D4AD6A3364
410DD9BAB95FD250
EF4A663D9D3C47CB
D7388535A5912E03

Hash samples made by SHA256 function

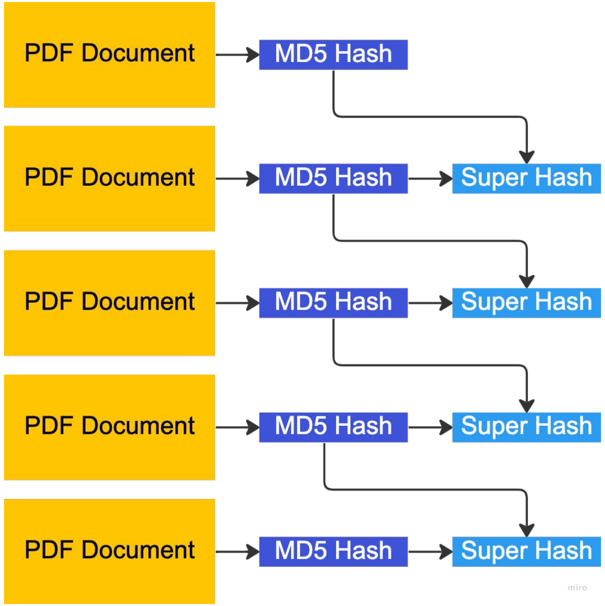
Input	Output
hello	2CF24DBA5FB0A30E26E83B2AC5B9E29E1B161E5C1FA7425E73043362938B9824
Hello	185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969
Hello!	334d016f755cd6dc58c53a86e183882f8ec14f52fb05345887c8a5edd42c87b7
It's a good day to HODL.	6B89D5D4AD6A3364410DD9BAB95FD250EF4A663D9D3C47CBD7388535A5912E03
The entire novel Bleak House by Charles Dickens	4F144CC612CA27E2DD6DFD6663F68BABC3B758D602B5102BF14E717E823EB741

You have to save hash for this document (and document itself) somewhere. Whenever later you may use the same hash function and if document wasn't changes, hash value will be the same.

There are many hash functions

Md2	a9046c73e00331af68917d3804f70655
Md4	866437cb7a794bce2b727acc0362ee27
Md5	5d41402abc4b2a76b9719d911017c592
Sha1	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d
Sha224	ea09ae9cc6768c50fcee903ed054556e5bfc8347907f12598aa24193
Sha256	2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
Sha384	59e1748777448c69de6b800d7a33bbfb9ff1b463e44354c3553bcdb9c666fa90125a3c79f90397bdf5f6a13de828684f
Sha512	9b71d224bd62f3785d96d46ad3ea3d73319bfbc2890caadae2dff72519673ca72323c3d99ba5c11d7c7acc6e14b8c5da0c4663475c2e5c3adef46f73bcdec043
Crc32	3d653119
Crc32b	86a61036

Basic concept. Small exercise



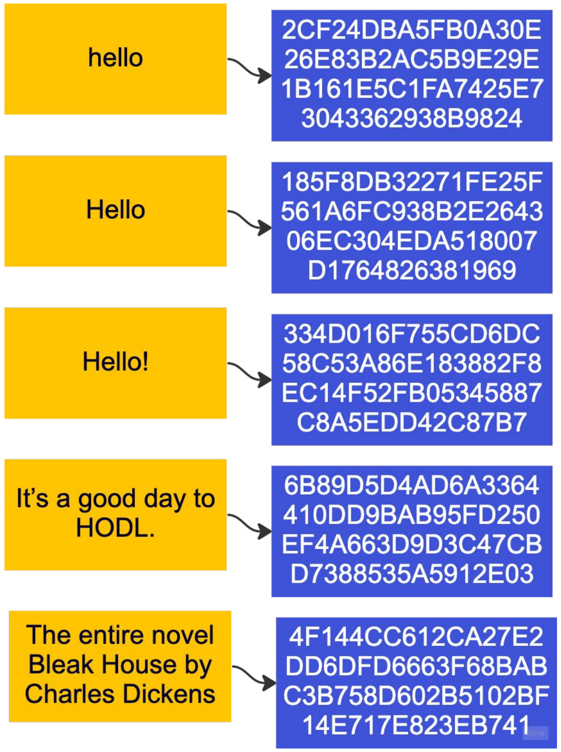
Link to the file	MD5 Hash	MD5(CurHash+Prev Hash)
https://s3.my.com/D1.pdf	6582b48e3f323b431ca8255ed610c262	6582b48e3f323b431ca8255ed610c262
https://s3.my.com/D2.pdf	83c9ca1abfd764eaf831c3c2bea15719	37468fcd8d1fa9985d99f709c750c800
https://s3.my.com/D3.pdf	f891a09eed789d9eadc62909cc5458f4	cee21a9e1151c55564b71fd3e5b676b1

Why does it matter?

Hash functions make it virtually impossible to generate the same output from two different inputs.

Verifying Document Integrity:

- Share the hash with a trusted person without revealing the actual document.
- After a specified period, such as 10 years, ask them to verify if the document remains unaltered.
- The trusted person recalculates the SHA-256 hash for the document and compares it with the original hash provided.
- This serves as proof of immutability but not as proof of existence. If the hashes are equal, it confirms that the document hasn't been altered by anyone, including yourself.



hello

2CF24DBA5FB0A30E
26E83B2AC5B9E29E
1B161E5C1FA7425E7
3043362938B9824

Hello

185F8DB32271FE25F
561A6FC938B2E2643
06EC304EDA518007
D1764826381969

Hello!

334D016F755CD6DC
58C53A86E183882F8
EC14F52FB05345887
C8A5EDD42C87B7

It’s a good day to HODL.

6B89D5D4AD6A3364
410DD9BAB95FD250
EF4A663D9D3C47CB
D7388535A5912E03

The entire novel Bleak House by Charles Dickens

4F144CC612CA27E2
DD6DFD6663F68BAB
C3B758D602B5102BF
14E717E823EB741

Proof of Immutability vs. Proof of Existence:

The hash verification serves as proof of immutability, confirming that the document hasn't been altered.

However, it does not provide proof of the document's existence, only its integrity.

Blockchain Mechanics

Network and Fees:

- Blockchain operates through a network of enthusiasts.
- Posting an OP_RETURN message requires a fee of approximately 0.0002 BTC ($5), leading to potential charges for companies with high document volumes.

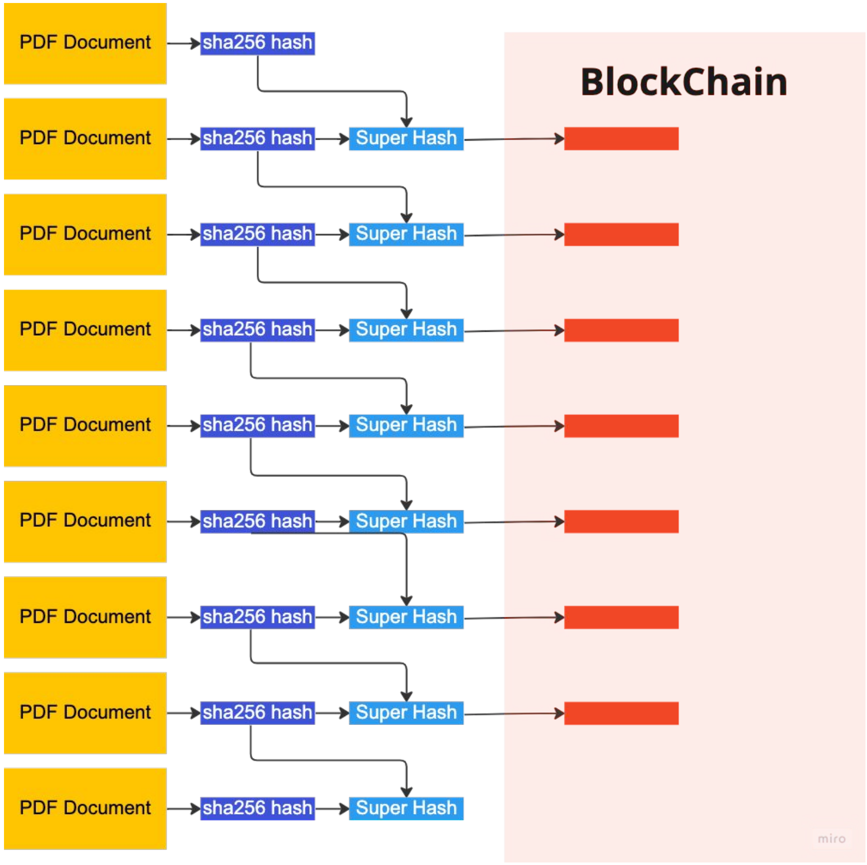
Interchange Process:

- OP_RETURN interchanges enter the MEMPOOL for inclusion in the next block, posted every 10 minutes.
- A reward must be provided to miners for processing the interchange, typically within 10 minutes.

Prooflink for Data:

- Once posted, a permanent prooflink is generated, providing a verifiable record.
- Example prooflink: https://www.blockchain.com/explorer/transactions/btc/b48e6f03f0dba6e9ad0d8a14b4c59269e69f6220764f7a4476d9df26220de95b

Blockchain and Alternatives



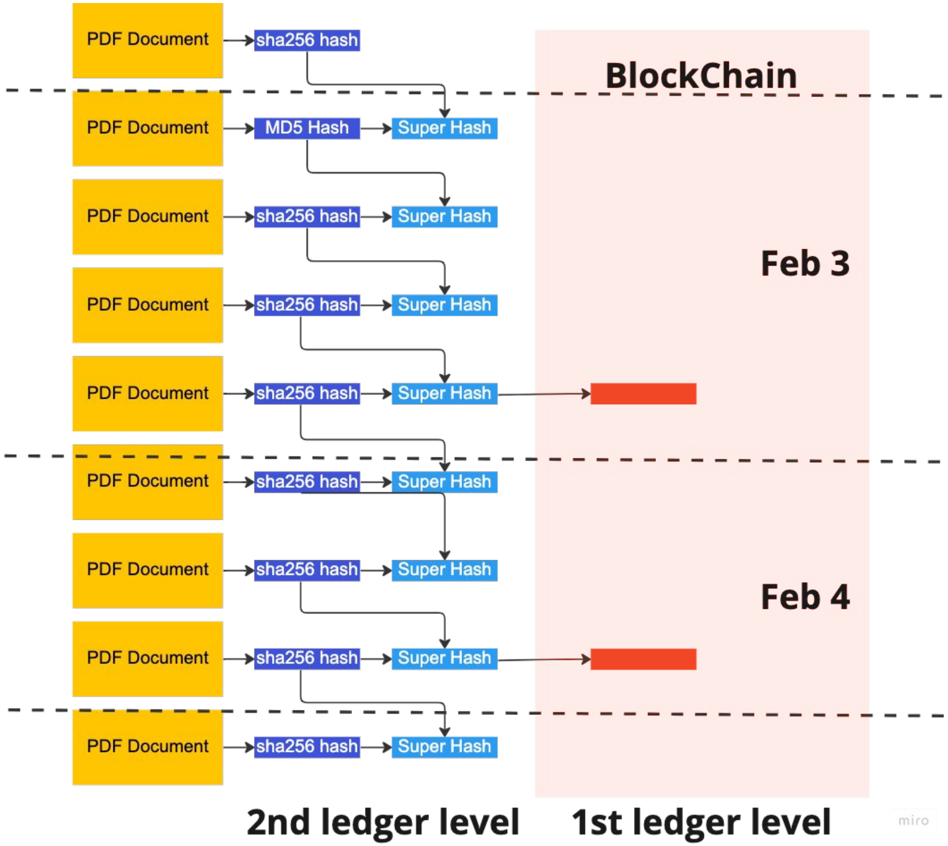
This is where the Blockchain network comes, serving as a distributed database or distributed ledger, but it has certain limitations:

1) Each record can only hold a maximum of 40 bytes.
2) Posting each record comes with a significant cost, ranging from $10 to $50.
3) The maximum speed of the global Blockchain network is limited to 10 interchanges per second.
4) There is a waiting period of approximately 10 minutes before a message (transaction) gets published and confirmed on the Blockchain.

Problems arise due to these limitations:

1) Storing all data on the Blockchain is not feasible; only hashes, evidence, or fingerprints can be posted.
2) Even posting only hashes incurs expenses and is a slow process.

Solution: Trust through a Secondary-Level Ledger

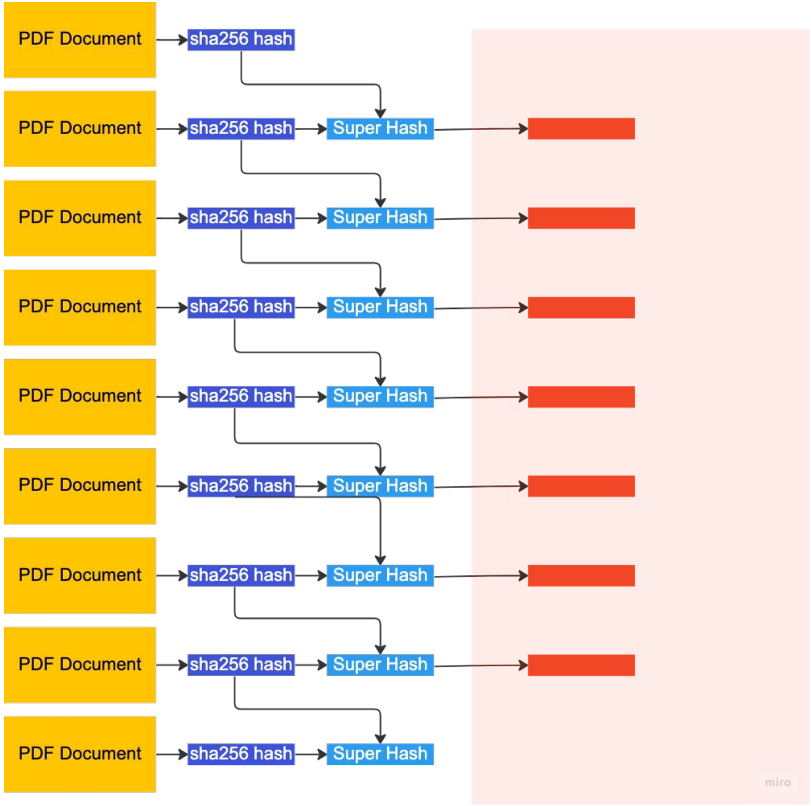


The Blockchain network is a powerful solution, serving as a distributed database or ledger.

Approach: Submit global Blockchain hash-records daily or at specified intervals.

Theoretically, data manipulation is only possible until the hash, which depends on the documents, is posted to the public Blockchain.

The Second Layer Ledger: Cost Optimization



Concept: Create an internal chain of blocks with hash values for a large document collection

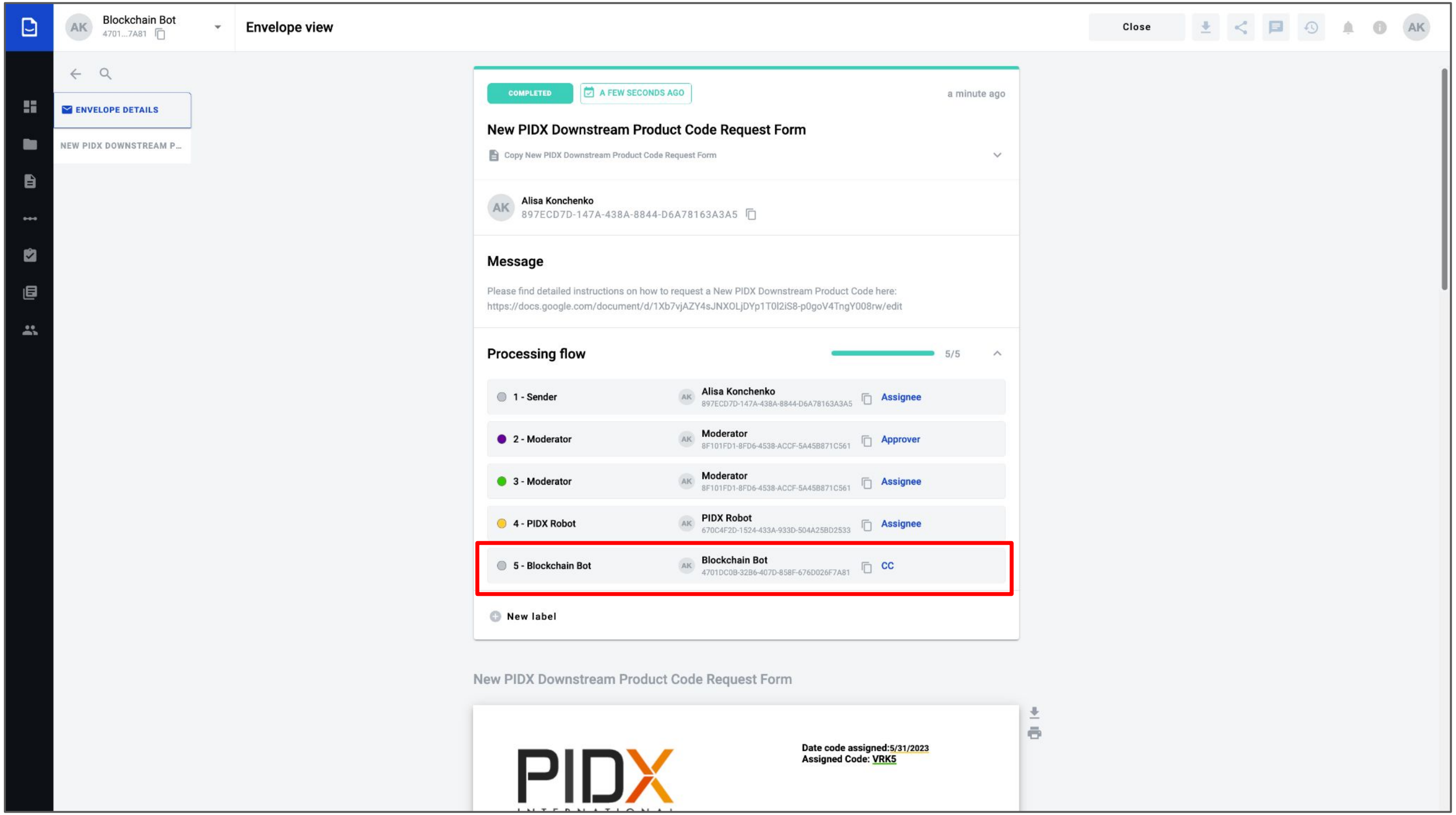
Key idea: Selectively post every N-th document to the blockchain within the chain

Challenge: Trusting the blockchain if we can modify it by adding new documents and recalculating hashes

Solution: Publish the super-hash in a public location beyond our control to prevent deletion or alteration

How can we achieve this in DocStudio?

You have the option to create a template for any desired document, and within the processing flow, you can include a user named "Blockchain Bot."



COMPLETED A FEW SECONDS AGO a minute ago

New PIDX Downstream Product Code Request Form

Copy New PIDX Downstream Product Code Request Form

Alisa Konchenko
897ECD7D-147A-438A-8844-D6A78163A3A5

Message

Please find detailed instructions on how to request a New PIDX Downstream Product Code here:
https://docs.google.com/document/d/1Xb7vjAZY4sJNXOLjDYp1T0l2iS8-p0goV4TngY008rw/edit

Processing flow 5/5

1 - Sender	AK	Alisa Konchenko 897ECD7D-147A-438A-8844-D6A78163A3A5	Assignee
2 - Moderator	AK	Moderator 8F101FD1-8FD6-4538-ACCF-5A45B871C561	Approver
3 - Moderator	AK	Moderator 8F101FD1-8FD6-4538-ACCF-5A45B871C561	Assignee
4 - PIDX Robot	AK	PIDX Robot 670C4F2D-1524-433A-933D-504A25BD2533	Assignee
5 - Blockchain Bot	AK	Blockchain Bot 4701DC0B-32B6-407D-858F-676D026F7A81	CC

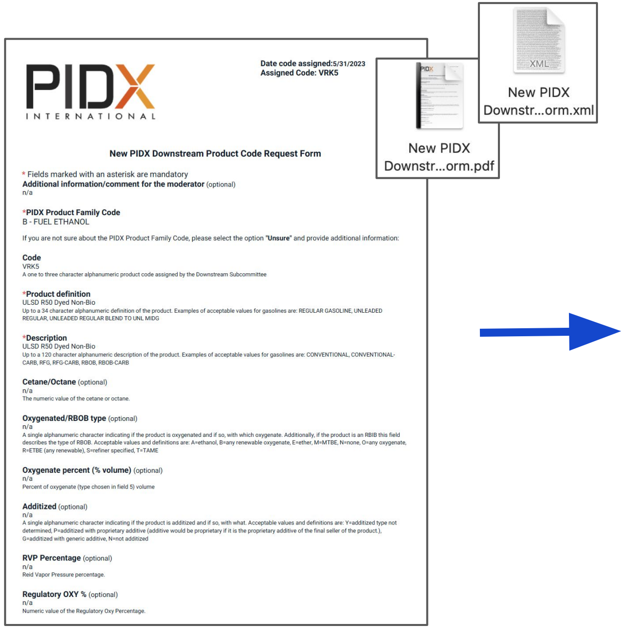
New label

New PIDX Downstream Product Code Request Form

Date code assigned:5/31/2023
Assigned Code: VRK5

How can we achieve this in DocStudio?

When the processing flow for an envelope, created from such a document, reaches the Blockchain Bot, the hash of the document (in XML/JSON or PDF format, or both) will be directly posted to the Blockchain or transmitted through a so-called Second Layer Ledger.



PIDX INTERNATIONAL

Date code assigned:5/31/2023
Assigned Code: VRK5

New PIDX Downstream Product Code Request Form

* Fields marked with an asterisk are mandatory

Additional information/comment for the moderator (optional)
n/a

***PIDX Product Family Code**
B - FUEL ETHANOL

If you are not sure about the PIDX Product Family Code, please select the option "**Unsure**" and provide additional information:

Code
VRK5
A one to three character alphanumeric product code assigned by the Downstream Subcommittee

***Product definition**
ULSD R50 Dyed Non-Bio
Up to a 34 character alphanumeric definition of the product. Examples of acceptable values for gasolines are: REGULAR GASOLINE, UNLEADED REGULAR, UNLEADED REGULAR BLEND TO UNL MIDG

***Description**
ULSD R50 Dyed Non-Bio
Up to a 120 character alphanumeric description of the product. Examples of acceptable values for gasolines are: CONVENTIONAL, CONVENTIONAL-CARB, RFG, RFG-CARB, RBOB, RBOB-CARB

Cetane/Octane (optional)
n/a
The numeric value of the cetane or octane.

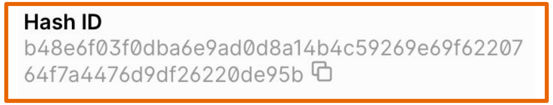
Oxygenated/RBOB type (optional)
n/a
A single alphanumeric character indicating if the product is oxygenated and if so, with which oxygenate. Additionally, if the product is an RBIB this field describes the type of RBOB. Acceptable values and definitions are: A=ethanol, B=any renewable oxygenate, E=ether, M=MTBE, N=none, O=any oxygenate, R=ETBE (any renewable), S=refiner specified, T=TAME

Oxygenate percent (% volume) (optional)
n/a
Percent of oxygenate (type chosen in field 5) volume

Additized (optional)
n/a
A single alphanumeric character indicating if the product is additized and if so, with what. Acceptable values and definitions are: Y=additized type not determined, P=additized with proprietary additive (additive would be proprietary if it is the proprietary additive of the final seller of the product.), G=additized with generic additive, N=not additized

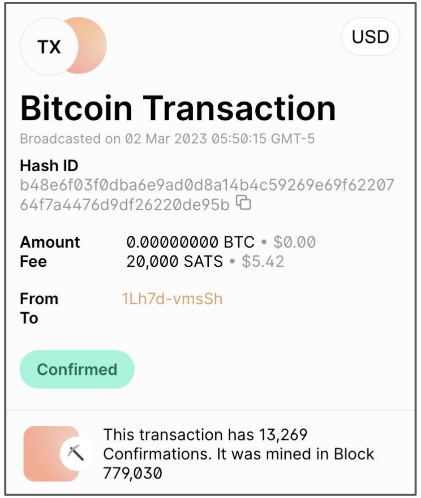
RVP Percentage (optional)
n/a
Reid Vapor Pressure percentage.

Regulatory OXY % (optional)
n/a
Numeric value of the Regulatory Oxy Percentage.



Hash ID
b48e6f03f0dba6e9ad0d8a14b4c59269e69f62207
64f7a4476d9df26220de95b

New Blockchain Record



Bitcoin Transaction

Broadcasted on 02 Mar 2023 05:50:15 GMT-5

Hash ID
b48e6f03f0dba6e9ad0d8a14b4c59269e69f62207
64f7a4476d9df26220de95b

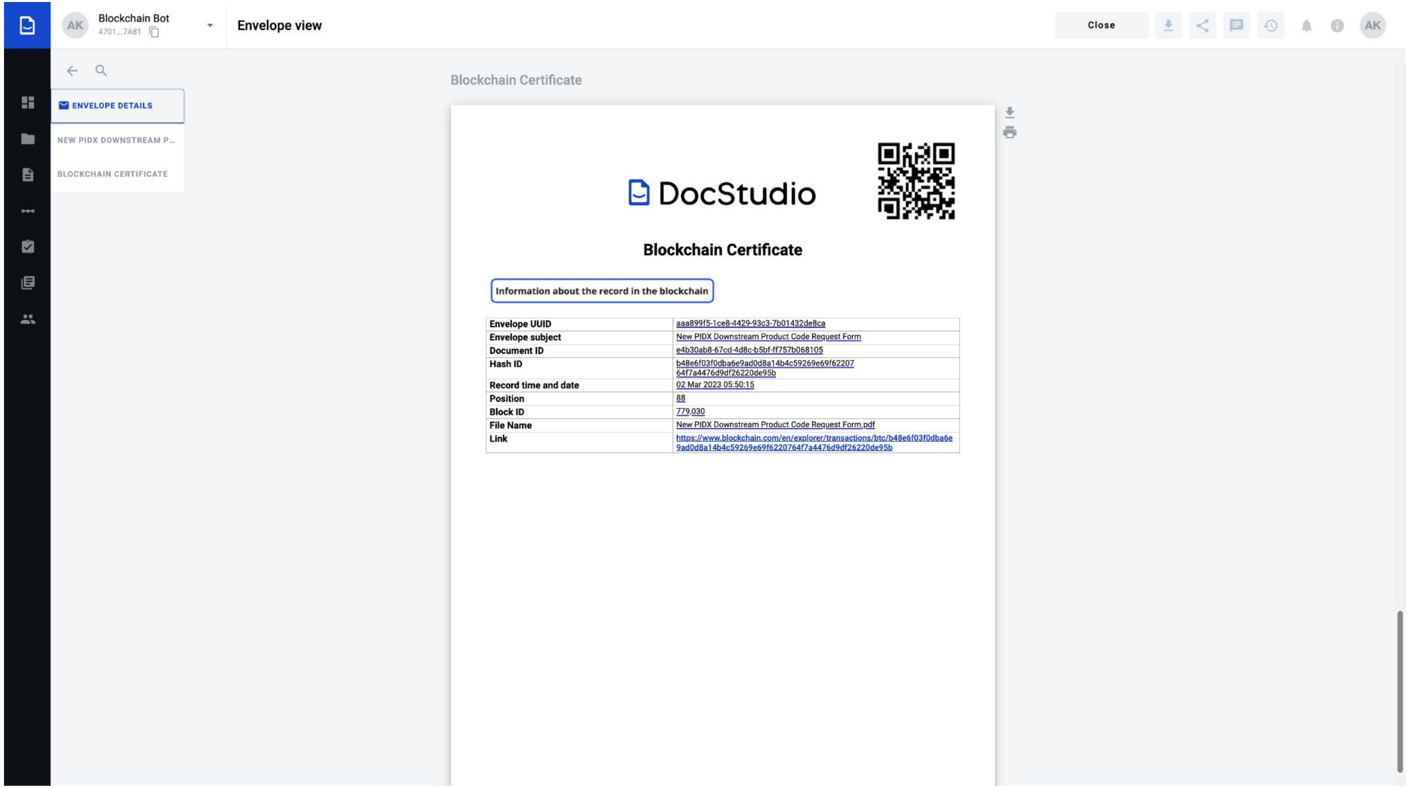
Amount	0.00000000 BTC • $0.00
Fee	20,000 SATS • $5.42
From	1Lh7d-vmsSh
To	

Confirmed

This transaction has 13,269 Confirmations. It was mined in Block 779,030

How can we achieve this in DocStudio?

Within approximately 10 minutes, a new document called "The DocStudio Blockchain Certificate" will be generated in the same envelope. This certificate will contain a permanent Blockchain link along with a few other relevant data points.



DocStudio

Blockchain Certificate

Information about the record in the blockchain

Envelope UUID	aaa899f5-1ce8-4429-93c3-7b01432de8ca
Envelope subject	New PIDX Downstream Product Code Request Form
Document ID	e4b30ab8-67cd-4d8c-b5bf-ff757b068105
Hash ID	b48e6f03f0dba6e9ad0d8a14b4c59269e69f6220764f7a4476d9df26220de95b
Record time and date	02 Mar 2023 05:50:15
Position	88
Block ID	779,030
File Name	New PIDX Downstream Product Code Request Form.pdf
Link	https://www.blockchain.com/en/explorer/transactions/btc/b48e6f03f0dba6e9ad0d8a14b4c59269e69f6220764f7a4476d9df26220de95b

Variety of Blockchain Platforms

The world of blockchain encompasses a diverse range of platforms, each utilizing different software but sharing similar approaches. These platforms are accessible to the public, but it's crucial to recognize that they all have their respective limitations.

BITCOIN
NEO
DASH
MONERO
CARDANO
LISK
QTUM
LITECOIN
ZCASH
ETHEREUM CLASSIC
RIPPLE
IOTA
ETHEREUM
WAVES
BYTECOIN
NEM
STRATIS
VERGE
BITCOIN CASH
BITSHARES

Thank You!

Zack Dikhtyar, CEO
dz@docstudio.com

Alisa Konchenko,
VP of Business Development
ae@docstudio.com

Eugene Soloviov, CTO
js@docstudio.com

DocStudio's source code registered under the codename WhiteDoc in US Copyright Office (case number 1-9052495699 07/23/2020)