DOCUMENT
CHAIN

# Documentchain - Blockchain for document revision

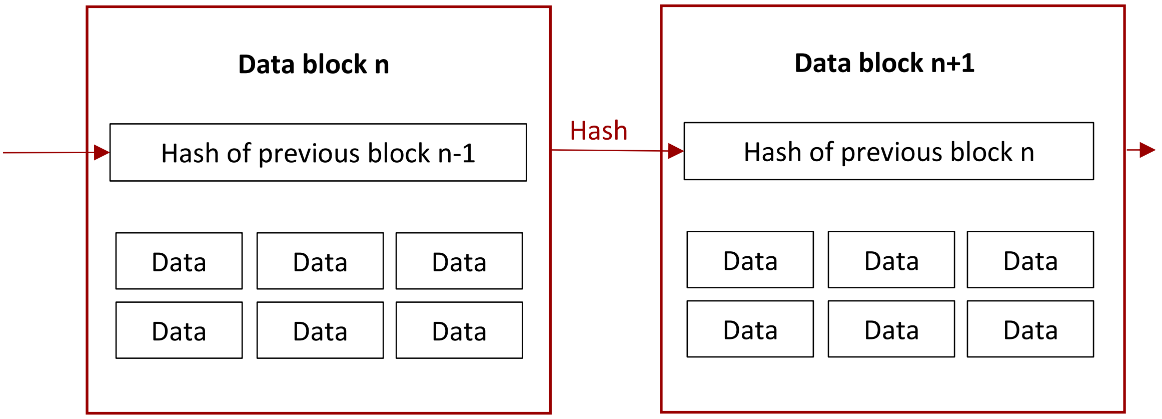
White-paper Version 1.4 dated November 3, 2019

The Documentchain is a document management solution, developed especially for the decentralized blockchain. Descriptions as well as hash values of the document files are distributed in the database and can be compared with the document itself later. This allows a tamper-proof confirmation that a document has not been changed since then.

## Basics

A blockchain is a decentralized database in which transaction records follow one another like a chain.

In the blockchain, information (= data) are stored as in a history. Information are grouped into blocks of data, and for each block a hash, a digital fingerprint, is calculated. Each new block also contains the hash of the previous block. These hashes connect the individual blocks into a chain.



The important thing is - and that makes the blockchain so valuable to us - that the information subsequently cannot be changed. Because if one information changes, its hash will change, too and the whole chain will break apart. As a consequence, the hashes of all subsequent blocks must be recalculated.

And that´s just not that easy. Because a blockchain is managed via a decentralized network, to which everyone can join. You too! Each member has a full copy of the blockchain on his computer. This checks whether the chain is still intact. A new block is only added if all the computers on the network have verified it. Exactly this principle makes the blockchain so safe: Everyone controls everyone.

## Everyone controls everyone and the „third party“ becomes superfluous

A blockchain holds data completely and unchangeable. Because everyone on the network can check one piece of information at any time and each piece of information is checked with each new one of hundreds of computers, trust is no longer a matter of human judgment.

This also makes a central instance, the “third party”, superfluous. The monitoring and thus the confidence are produced technically and decentral by the blockchain. The side effect: In this way, processes are also accelerated. Because if there is no central authority, it could not fail. In principle, the blockchain is organized similarly to the internet: decentralized.

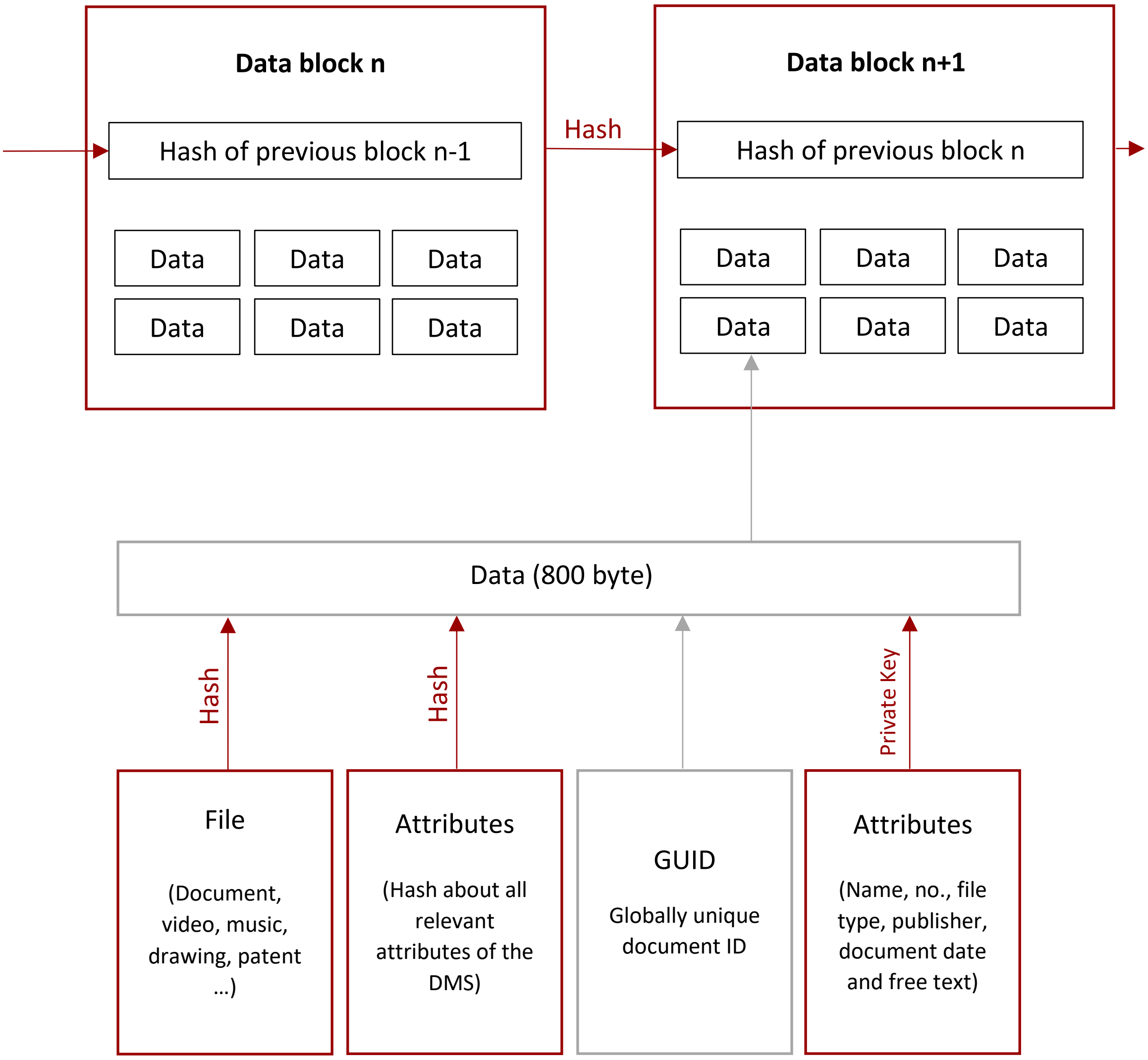
## From the Blockchain to the Documentchain

Companies must keep important documents in a legally secure manner. The integrity (i.e., completeness and immutability) and authenticity (i.e., confirmation of the authenticity of the data and their unequivocal assignment to the author) of these documents must be maintained beyond the statutory retention period.

A challenge that can be handled with the blockchain technology: A contract that is concluded today remains locally on your computer or your company server. However, the information and the fingerprint (= data) are stored in the document chain - in a well-encrypted data block. At any later date, it can be proved beyond doubt that this contract was in place at the time of its storage.

Likewise, a musician can prove that a document with the piece of music written by him or his audio recording already existed at a certain time: He can prove the copyright.

## Demonstrate integrity with the blockchain



Data block n

Hash of previous block n-1

Data | Data | Data
Data | Data | Data

Hash

Data block n+1

Hash of previous block n

Data | Data | Data
Data | Data | Data

Data (800 byte)

Hash

Hash

Private Key

File

(Document, video, music, drawing, patent …)

Attributes

(Hash about all relevant attributes of the DMS)

GUID

Globally unique document ID

Attributes

(Name, no., file type, publisher, document date and free text)

The complete storage of the documents in the blockchain would require an incalculably high storage space and could lead to data protection problems.

However, this is not necessary for a document revision. To check whether data is unchanged, it is sufficient to compare a hash value stored with the current hash.

To ensure the integrity of a document, an electronic fingerprint (hash) of the digital or digitized document is created and written to the blockchain. Thus, at any later time, the fingerprint of the locally archived file can be compared with that stored in the blockchain. If they match, the integrity is unequivocally proven.

## API – Application Programming Interface

The document revision can be carried out directly within the wallet “DMS Core” from version “Dave” or by means of RPC, for example, from a document management system:

1. Determine input for payment of the transaction fee of at least 0.1 DMS:

```
Post('{"jsonrpc":"1.0","id":"DMSExposed","method":"listunspent"}');
```

2. Calculate change and set receipt for this:

```
change = usedinput - fee;
Post('{"jsonrpc":"1.0","id":"DMSExposed","method":"getrawchangeaddress"}');
```

3. Create transaction with document information and change:

```
Post('{"jsonrpc":"1.0","id":"DMSExposed",'
   + '"method":"createrawtransaction",'
   + "params":[ [{"txid":"usedinput","vout": usedvout }],'
   + '{"changeaddr":change, "data":"thehexdata"} ] }');
```

4. Sign transaction:

```
Post('{"jsonrpc":"1.0","id":"DMSExposed","method":"signrawtransaction",'
   + '"params":["thetrans"]}');
```

5. Send transaction:

```
Post('{"jsonrpc":"1.0","id":"DMSExposed","method":"sendrawtransaction",'
   + '"params":["thetrans"]}');
```

For a complete example, see

https://github.com/Krekeler/documentchain/blob/master/src/qt/documentlist.cpp

## Cryptocurrency „DMS“

To prevent masses of unnecessary data overloading the blockchain, each transaction is costly. This transaction fee is collected in DMS Coins, the project-own cryptocurrency, and distributed to the supporters of the network.

| | |
|---|---|
| *Coin name* | Documentchain |
| *Symbol* | DMS |
| *Maximum amount* | 21 million |
| *Block time* | 6 minutes |
| *PoW algorithm* | YescryptR32 (CPU mining) |
| *Masternode* | 5000 DMS Collateral |
| *Premine* | 0 DMS |

## Wallet: The virtual wallet for storing information

To store information into a blockchain, a virtual wallet is needed. It also manages your balance of DMS Coins and allows you to send and receive payments. “DMS Core” is developed as open source software, the source code is available at https://github.com/Krekeler/documentchain/