DOCUMENT CHAIN

Documentchain - Blockchain für Dokumentenrevision

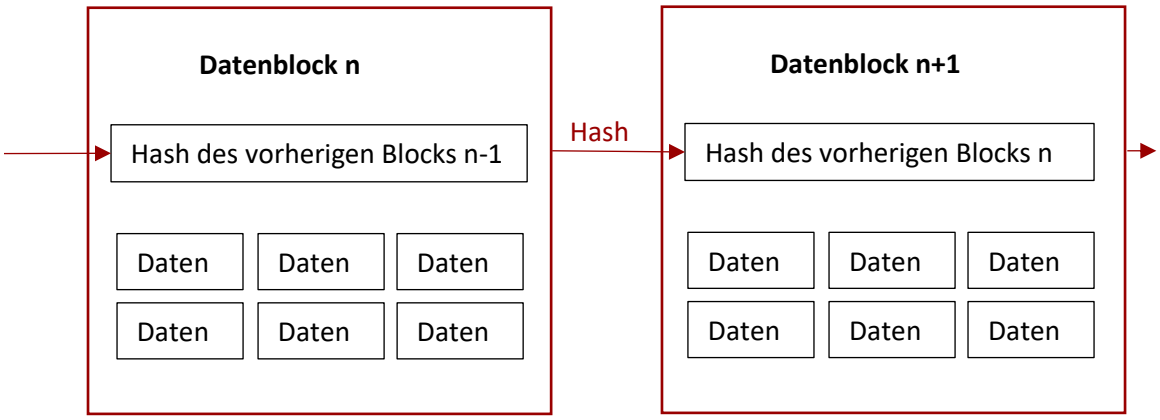
White-paper Version 1.4 vom 03.11.2019

Die Documentchain ist eine speziell für das Dokumentenmanagement entwickelte dezentrale Blockchain. Beschreibungen sowie Hashwerte der Dokumentdateien werden in der verteilten Datenbank gespeichert und können später mit dem Dokument verglichen werden. Dies erlaubt eine manipulationssichere Bestätigung, dass ein Dokument seitdem unverändert ist.

Grundlagen

Eine Blockchain ist eine dezentrale Datenbank, in der sich Transaktionsdatensätze aneinanderreihen wie bei einer Kette.

In der Blockchain werden Informationen (= Daten) wie in einem Verlauf gespeichert. Informationen werden zu Datenblöcken zusammengefasst und für jeden Block wird ein Hash, ein digitaler Fingerabdruck, berechnet. Jeder neue Block enthält außerdem den Hash des vorherigen Blocks. Über diese Hashes werden die einzelnen Blöcke zu einer Kette verbunden.



Das Wichtige dabei ist – und das macht die Blockchain so wertvoll, dass die Informationen nachträglich nicht verändert werden können. Denn ändert sich eine Information, ändert sich auch ihr Hash und die gesamte Kette bricht auseinander.

Und genau das ist nicht so einfach. Denn eine Blockchain wird über ein dezentrales Netzwerk verwaltet, dem jeder beitreten kann. Auch Sie. Jedes Mitglied hat eine vollständige Kopie der Blockchain auf seinem Computer. Dieser prüft, ob die Kette noch intakt ist. Ein neuer Block wird erst hinzugefügt, wenn ihn die Computer im Netzwerk verifiziert haben. Genau dieses Prinzip macht eine Blockchain so sicher: Jeder kontrolliert Jeden.

Jeder kontrolliert jeden und der „Dritte“ wird überflüssig

Eine Blockchain hält Daten also lückenlos und unveränderbar fest. Weil jeder im Netzwerk jederzeit eine Information überprüfen kann und jede Information mit jeder neuen wiederum von hunderten Computern überprüft wird, ist Vertrauen keine menschliche Abwägungssache mehr.

Damit wird auch eine zentrale Instanz, der „Dritte“, überflüssig. Die Kontrolle und somit das Vertrauen werden von der Blockchain technisch und dezentral hergestellt. Der Nebeneffekt: Auf diese Weise werden auch Prozesse beschleunigt. Denn wo es keine zentrale Stelle gibt, kann diese auch nicht ausfallen. Im Prinzip ist die Blockchain also ähnlich organisiert wie das Internet: dezentral.

DOCUMENT CHAIN

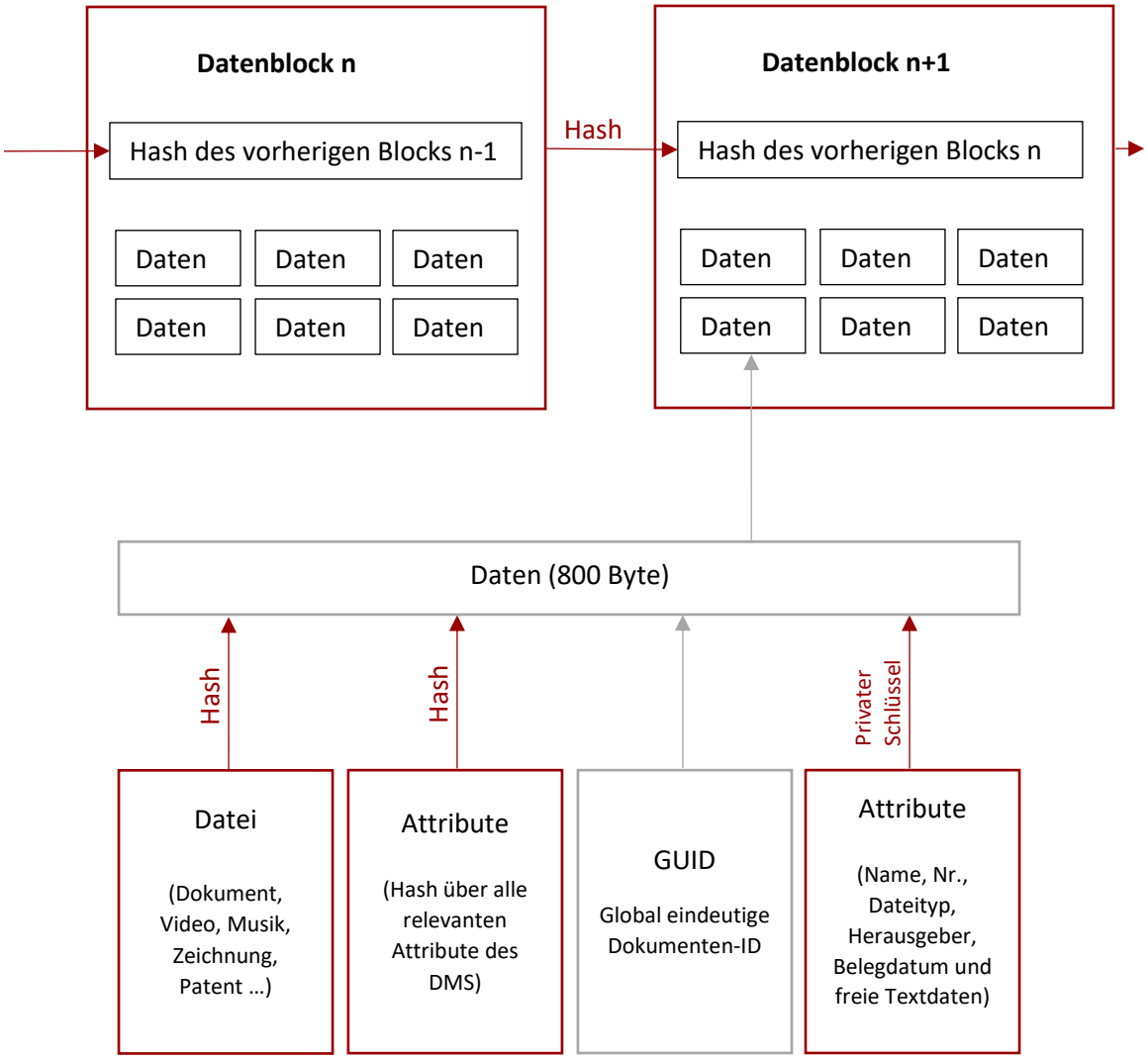
Von der Blockchain zur Documentchain

Unternehmen müssen wichtige Dokumente rechtssicher aufbewahren. Dabei muss die Integrität (d. h. Vollständigkeit und Unveränderbarkeit) sowie Authentizität (d. h. Bestätigung der Echtheit der Daten und ihre zweifelsfreie Zuordnung zum Verfasser) dieser Unterlagen über die gesetzlich vorgeschriebene Aufbewahrungsfrist hin gewahrt werden.

Eine Herausforderung, die mit der Blockchain-Technologie bewältigt werden kann: Ein Vertrag, der heute abgeschlossen wird, verbleibt zwar lokal auf Ihrem Rechner bzw. Ihrem Unternehmensserver. Die Informationen und der Fingerabdruck (= Daten) werden aber in der Documentchain hinterlegt – in einem gut verschlüsselten Datenblock. Zu jedem späteren Zeitpunkt kann zweifelsfrei nachgewiesen werden, dass dieser Vertrag im Moment des Speicherns in genau dieser Fassung vorhanden war.

Oder ein Musiker kann nachweisen, dass ein Dokument mit dem von ihm geschriebenen Musikstück oder dessen Tonaufnahme zu einem bestimmten Zeitpunkt bereits vorhanden war. Er kann die Urheberschafft beweisen.

Mit der Blockchain Integrität nachweisen



Die vollständige Speicherung der Dokumente in der Blockchain würde einen unkalkulierbar hohen Speicherplatz erfordern und könnte zu datenschutzrechtlichen Problemen führen. Für eine Dokumentenrevision ist dies aber auch nicht erforderlich. Für die Überprüfung, ob Daten unverändert vorliegen, reicht der Vergleich eines für die Revision gespeicherten Hashwertes mit dem aktuellen Hash.

Um nun die Integrität eines Dokuments sicherzustellen, wird ein elektronischer Fingerabdruck (Hash) des digitalen oder durch Scannen digitalisierten Dokuments erstellt und in die Blockchain geschrieben. So kann zu jedem späteren Zeitpunkt der Fingerabdruck der lokal archivierten Datei mit dem in der Blockchain gespeicherten verglichen werden. Bei Übereinstimmung ist die Integrität zweifelsfrei bewiesen.

API – Application Programming Interface

Die Dokumentenrevision kann direkt innerhalb der Wallet „DMS Core“ ab Version „Dave“ oder mittels RPC beispielsweise von einem Dokumenten-Management-System durchgeführt werden:

1. Input für die Bezahlung der Transaktionsgebühr von mindestens 0,1 DMS ermitteln:

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

2. Wechselgeld berechnen und Empfangskonto hierfür festlegen:

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

3. Transaktion mit Dokumentinformation und Wechselgeld erstellen:

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

4. Transaktion signieren:

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

5. Transaktion senden:

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

Ein vollständiges Beispiel finden Sie unter

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

Kryptowährung „DMS“

Um zu verhindern, dass Massen unnötiger Daten die Blockchain überlasten, ist jede Transaktion mit Kosten verbunden. Diese Transaktionsgebühr wird in DMS-Coins, der projekteigenen Kryptowährung, erhoben und an die Unterstützer des Netzwerks verteilt.

Coin-Name	Documentchain
Symbol	DMS
Maximale Anzahl	21 Mio
Blockzeit	6 Minuten
PoW-Algorithmus	YescryptR32 (CPU-Mining)
Masternode	5000 DMS Collateral
Premine	0 DMS

Wallet: Die virtuelle Geldbörse zur Speicherung von Informationen

Um eine Information in einer Blockchain zu speichern, wird eine virtuelle Geldbörse benötigt. Diese nennt man Wallet. Sie verwaltet auch Ihr Guthaben an DMS Coins und ermöglicht Zahlungen zu senden und zu empfangen. „DMS Core“ wird als Open Source Software entwickelt, die Quelltexte sind unter https://github.com/Krekeler/documentchain/ abrufbar.

Softwarebüro Krekeler
Inhaber Dipl.-Wi.-Ing. Harald Krekeler
Friedrich-Engels-Str. 45
15712 Königs Wusterhausen, Germany

Telefon +49 3375 203631, Fax +49 3375 203622, E-Mail mail@documentchain.org
Impressum https:// documentchain.org/impressum/

Verantwortlicher i. S. d. § 55 Abs: 2 RStV: Harald Krekeler (Anschrift s. o.)