

Industrie 4.0 Recht-Testbed: Juristische Testumgebung und offenes Repository

Bochum, 22. November 2022 – Transfermodul 3.1



**INSTITUT FÜR
RECHTSINFORMATIK**
UNIVERSITÄT DES SAARLANDES



Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Einleitung

Dieses Transfermodul stellt eine grobe Übersicht über die Gesamtarchitektur des Industrie 4.0 Recht-Testbed bereit. Das öffentliche Experimentierfeld des Recht-Testbed demonstriert, wie Unternehmen eine automatisierte, rechtssichere, und technisch abgesicherte Vertragsdurchführung zwischen mehreren Vertragsparteien im Industrie 4.0 Umfeld, nutzen können. Dabei kann jede Vertragsdurchführung in fünf verschiedene Phasen eingeteilt werden

- (1) Auswahl eines Vertragstemplates
- (2) Vertragsaushandlung
- (3) Vertragsschluss
- (4) Vertragsdurchführung
- (5) Vertragsabschluss

Jede Phase erfordert die Verwendung von unterschiedlichen technischen Komponenten zum Ausführen des Vertrages.



Die Basis des Vertrages

- Das Vertragstemplate bildet die Grundlage für eine automatisierte Vertragsdurchführung
- Ein Vertrag der speziell für einen Anwendungsfall konzipiert wurde
- Vertragsparameter lassen sich automatisiert in Phase 2 befüllen
- Besteht aus zwei Komponenten: menschenlesbar und maschinenlesbar
- Diese Kombination macht das Vertragstemplate zu einem Smart Legal Contract
- Direkt einsatzfähig: Vorgefertigte Vertragstemplates für Transport- und Produktionsverträge
- Die Vertragstemplates bauen auf dem Accord Project auf
 - Vorteil: Offenes Ökosystem
 - Flexibel: Nicht an bestimmte Technologien (Blockchain) gebunden
 - Ausführbare Logik für automatisierte Verträge
 - Anpassbar: Vertragstexte und Ausführungslogik können individuell gestaltet werden



Phase 1 Vertragstemplate

Ein **Smart Legal Contract** ist ein rechtsverbindlicher Vertrag, der digital ist und seine Bedingungen und die Erfüllung seiner Verpflichtungen mit externen Datenquellen und Softwaresystemen verbinden kann.

Das **Accord Project** ist ein offenes Ökosystem, das es jedem ermöglicht, intelligente Vereinbarungen und Dokumente auf einer technologieneutralen Plattform. Siehe: <https://accordproject.org/about>

Zu den Vertragstemplates: <https://gitlab.cc-asp.fraunhofer.de/legaltestbed>

Die Vertragsaushandlung

- Nachteile der klassischen Vertragsaushandlung
 - Benötigt Zeit und Ressourcen
 - Verschiedene Angebote müssen eingeholt und gesichtet werden
 - Manuelle Nachverhandlung
- Vorteile der automatisierten Vertragsaushandlung
 - Mitarbeiter legen nur noch Grenzen fest (bzw. Entgelt, Zeitpunkte)
 - Spart Zeit und Ressourcen, da die Verhandlung Softwareagenten übernehmen
 - Gleichzeitige Verhandlung mit vielen Anbietern möglich
- Das RTB Projekt setzt dabei das Verhandlungsframework GeniusWeb ein
- Die Verhandlung übernehmen Softwareagenten, die Grenzen setzen die Unternehmen selbst
- Automatisierte Vertragsgenerierung durch Befüllen der Vertragstemplates mit ausgehandelten Parameter
- Flexibel: Nicht an bestimmte Technologien (Blockchain) gebunden



Phase 2 Vertragsaushandlung

GeniusWeb ist eine offene Architektur für die Verhandlung über das Internet. Auftragnehmer können in vordefinierten Grenzen automatisiert, mit einer Vielzahl von Anbietern Vertragsdetails aushandeln.

Siehe:

<https://tracinsy.ewi.tudelft.nl/pubtrac/GeniusWeb>

Der Vertragsschluss

- Die Vertragsparameter wurden ausgehandelt und das Vertragstemplate damit befüllt!
- Kontrolle: Die Vertragspartner haben die Möglichkeit die Details zu überprüfen
- Papierlos: Der Vertrag wird digital geschlossen
 - Hierfür werden digitale Zertifikate und digitale Signaturen genutzt
 - Verwendung von international anerkannten Standards zur Signierung
 - Signierung der menschenlesbaren und maschinenlesbaren Vertragskomponenten
- Nachweisbar: Digitale Signaturen können unabhängig überprüft werden
- Speicherung: Signierter Vertrag wird dezentral auf einer Blockchain gespeichert
- Vorteile:
 - Dezentral: Jeder Vertragspartner hat die gleichen Informationen
 - Nachweisbar: Willenserklärungen sind beidseitig durch die Blockchain-Lösung verifizierbar
 - Manipulationssicher: Blockchains verketteten Hashwerte von Informationen und lassen sich nicht manipulieren



Phase 3 Vertragsschluss

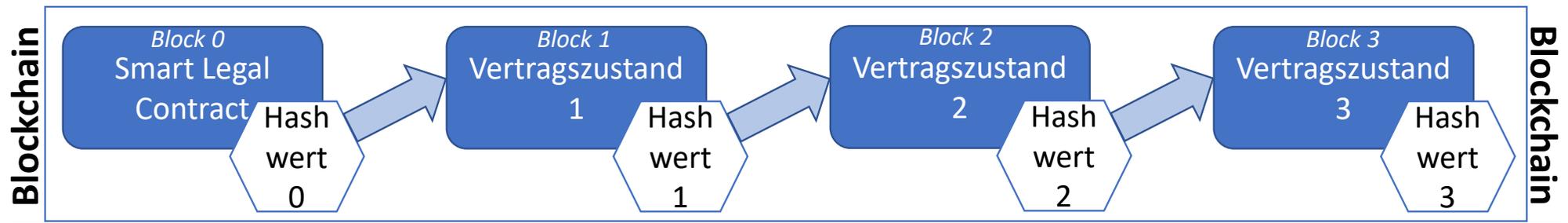
Digitale Zertifikate enthalten die geprüfte Identität einer Partei und einen kryptografischen Schlüssel. Durch die Kombination von **digitaler Signatur** und Zertifikat kann sichergestellt werden, wer das Dokument unterschrieben hat und das keinerlei Daten seit dem Zeitpunkt der Signatur geändert wurden.

Ein **Hashwert** ist ein numerischer Wert mit fester Länge, welcher kryptografisch berechnet wird und der den Ausgangsdaten eindeutig zuordbar ist. Jede Manipulation der Ausgangsdaten führt zwangsläufig zu einem anderen Hashwert. Somit lassen sich Manipulationen zweifelsfrei erkennen.

Die Blockchain

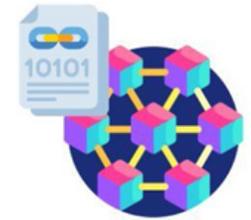
- Blockchains verketteten Hashwerte von Informationen, wie den aktuellen Vertragszustand
 - Vorherige Hashwerte fließen als Eingabewerte für den nächsten Block ein
 - Somit ist jeder Block über eine Hashkette verbunden
 - Manipulationen an einem Block führen zu anderen Hashwerten und lassen sich somit erkennen
- Dezentral: Jeder Vertragspartner hat eine Abbildung der gesamten Blockchain und jederzeit Zugriff auf alle Ereignisse des automatisierten Vertrages
- Sind die Vertragsdaten trotz dezentraler Blockchain vor unbefugten Zugriff geschützt?
 - **Ja!** Durch den Einsatz sogenannter Private Data Collections werden Klartextdaten nur bei den direkten Vertragspartner gespeichert
- Mehr Informationen zu Blockchains im *RTB Transfermodul 3.2*

Was ist eine Private Data Collection? [Erklärung](#)



Die Vertragsdurchführung

- Nachdem der Vertrag digital geschlossen wurde und nachweisbar auf der Blockchain gespeichert wurde, beginnt die vierte Phase: die Vertragsdurchführung
- Bei der Vertragsdurchführung von Transport- oder Produktionsverträgen entstehen viele Schritte die Einfluss auf den aktuellen Vertragszustand nehmen
 - Bspw: Abholung der Ware, Übergabe der Ware an den Empfänger etc.
- Jede eintretende Zustandsänderung wird als signierte Anfrage an die Blockchain gesendet
 - Vorteile: eindeutige Zuweisung einer Anfrage zu einer Person oder Sensor
 - Überprüfbar: durch die digitale Signatur kann die Gültigkeit einer Anfrage automatisiert überprüft werden
- Das in Phase 1 ausgewählte Vertragstemplate stellt unter anderem die Logik des speziellen Anwendungsfall bereit
 - Bevor Daten auf die Blockchain geschrieben werden, überprüft die Logik des Smart Legal Contracts die eingehenden Anfragen zu Zustandsänderung
 - Überprüfung auf Sinnhaftigkeit zum aktuellen Zeitpunkt
 - Überprüfung des Absenders: hat der Absender die für die Anfrage korrekte Rolle inne?
 - Bspw: Anfrage: "Übergabe der Ware an den Empfänger" darf nur vom Transporteur initiiert werden
- Nachweisbare Speicherung: valide Anfragen führen zu einem neuen Zustand des Vertrages. Dieses Ergebnis wird auf der Blockchain nachweisbar persistiert
- Kontrolle: Beide Vertragsparteien führen die gleiche Logik aus, einseitige Manipulationen am Smart Legal Contract oder einem Blockchain-Knoten führen somit nicht zu einer ungewollten Zustandsänderung



Phase 4 Vertragsdurchführung

Die **Geschäftslogik** ist der maschinenlesbare Teil des Smart Legal Contracts. Dabei wird die Logik, über die Variablen des Vertrages ausgedrückt und reagiert auf Anfragen, die während der gesamten Laufzeit des Vertrages auftreten.

Der Vertragsabschluss

- Ein Transport- oder Produktionsvertrag endet in der Bezahlung des Auftragnehmers
- Im Beispiel des Transportvertrages bildet die Zahlungsfälligkeit die Ablieferung der Ware und die gleichzeitige Bestätigung des Empfängers über die Annahme und korrekte Beschaffenheit der Ware ab
 - Die Logik des Smart Legal Contracts kann bei diesem bestätigten Vertragszustand die Zahlung vollautomatisiert initiieren
- Eine Zahlung wird über abgesicherte Schnittstellen, durch eine Zahlungsanweisung an die Bank des Schuldners, ausgelöst
 - Eine Zahlung wird nur bei Erreichen und Bestätigen des definierten Vertragszustandes vom Smart Contract ausgelöst
 - Absicherung der Transaktion durch digitale Signaturmechanismen



Phase 5
Vertragsabschluss

In Form einer verschlüsselten Nachricht verbindet die digitale Signatur einen Unterzeichner sicher mit einem Dokument in einer aufgezeichneten Transaktion. Digitale Signaturen verwenden ein standardisiertes, akzeptiertes Format, die so genannte Public Key Infrastructure (PKI), um ein Höchstmaß an Sicherheit und universeller Akzeptanz zu gewährleisten. Bei der PKI wird ein digitales Zertifikat zur Identitätsprüfung verwendet.