

# Smart Contracts in der Blockchain

Kluge Programme, selbständige Agenten und wirksame Verträge?

Begleitender Text: Most Wanted:Music



Steffen Holly  
Leite Geschäftsfeld Media Management & Delivery  
Fraunhofer IDMT  
[sholly@idmt.fraunhofer.de](mailto:sholly@idmt.fraunhofer.de)

Der Begriff „Smart contract“ hat keine klare und ständige Definition, wird aber ein zentraler Bestandteil der Blockchain-Plattformen der nächsten Generation sein und wird als Schlüsselfunktion für jede praktische Unternehmensanwendung gesehen.

Aktuelle Definitionen fallen meist in eine dieser zwei Kategorien:

- A. **smart contract code**: Technologie bzw. Code, der gespeichert, überprüft und auf einem Blockchain ausgeführt wird
- B. **smart legal contracts**: Anwendung dieser Technologie als Ergänzung oder Substitution von rechtlich bindenden Verträgen

Die Verwendung eines Begriffs, um sich auf unterschiedliche Konzepte zu beziehen, macht die Beantwortung sogar einfacher Fragen unmöglich, wie z.B.: Was sind die Fähigkeiten eines intelligenten Vertrag?

- A. abhängig von den Fähigkeiten der verwendeten Programmiersprache und den Funktionen der Blockchain
- B. bei der Verwendung der Technologie für einen verbindlichen Rechtsvertrag oder einen wirksamen Ersatz für einen rechtlich bindenden Vertrag ist die Antwort abhängig von der bestehenden Rechtslehre und davon, wie sich unsere juristischen, politischen und kommerziellen Institutionen für die Behandlung der Technologie entscheiden. Wenn die Manager dem nicht vertrauen, der Gesetzgeber es nicht anerkennt und die Gerichte es nicht interpretieren können, dann wird es kein praktisch nützlicher „Vertrag“ sein

### **Smart Contracts als Smart Contract Code**

Blockchains können neben Transaktionen auch komplexere Operationen auf Basis von vollwertigen Programmiersprachen durchführen. Da diese Programme in der Blockchain ausgeführt werden, haben sie spezielle Eigenschaften im Vergleich zu anderer Software.

- sie sind wie die Blockchain selber beständig und nicht manipulierbar durch den wirkenden Konsens
- sie können selbständig Blockchain Assets kontrollieren, z.B. die Speicherung und Übertragung von Bitcoins (einmal geschrieben -> selbständig ausgeführt)

Es hat sich bei Entwicklern neben dem ursprünglichen Begriff „smart code“ eben auch der Begriff „smart contracts“ etabliert, der in diesem Kontext auf diese komplexen Programm verweist, die in einer Blockchain gespeichert und ausgeführt werden können. Das Wort „contract“ verdeutlicht den Wert, den diese Art Code steuert, z.B. Identitäten, Kryptowährungen und Assets im Allgemeinen.

- Programmcode als finanzielle Transaktion = "sende 1 Bitcoin von Alice an Bob am 11.11. 2016"
- Programmcode als Steuerung einer Berechtigung = "wenn Alice JA gesagt hat, dann entferne Bobs Stimmrecht zur Anwendung X und benachrichtige die folgenden Konten ... "

In vielen Fällen wird „Smart Contract Code“ nicht isoliert, sondern als kleines Stück in einer größeren Anwendung verwendet. Diese Programme können Salden von Kryptowährung halten, oder andere intelligente Anwendungen steuern. Sie handeln autonom sobald sie einmal erstellt wurden, um eine bestimmte Aktion auszuführen. Deshalb bevorzugen viele den Begriff "Smart Agent", analog zu dem allgemeineren Konzept eines Software-Agent.

Die Fähigkeiten und der Zweck von „Smart Contract Code“ im Unterschied zu anderen Programmcode wird ohne die Verwendung einer Analogie wie „Vertrag“ klarer. Ähnlich zu JavaScript als Programmiersprache für Web-Anwendungen auf Basis von HTML als Markup Language, über deren Trennung heute auch keiner mehr nachdenkt.

## Smart Contracts als Smart Legal Contracts

In der Finanzwelt und im Rechtssystem bezieht sich der Begriff „Smart Contract“ auf einen spezifischen Anwendungsfall des oben erwähnten „Smart Contract Code“, eben auf die Möglichkeit mit Hilfe der Blockchain Technologie bestehende rechtliche Verträge zu ergänzen oder diese zu ersetzen. Man möchte durch die Verwendung von Programmcode etwas artikulieren, überprüfen und eine Vereinbarung zwischen den Parteien durchzusetzen, einen „Smart Legal Contract“ einsetzen.

Mögliche Beispiele für so eine Kombination aus intelligentem Vertrags-Code und mehr traditioneller Rechtssprache:

- ein Hersteller tritt in einen rechtlichen Vertrag mit einem Händler und die Zahlungsbedingungen könnten als Programmcode definiert und automatisch ausgeführt werden, wenn die Lieferung erfolgt ist
- der Händler würde in einem Vertrag auf einer Absicherungsklausel zur etwaigen Entschädigung bei einem Defekt bestehen
- hier macht es keinen Sinn geben, diese Klausel im Programmcode darzustellen, weil es sich nicht selbst ausführen kann sondern vor einem eventuell auch vor einem Gericht ausgelegt werden muss, bis zur Vollstreckung

Kommerzielle Verträge sind voll von solchen Klauseln, welche die Parteien in verschiedenen Fällen schützen. Die verschiedene Deutung und die vielen Randbedingungen formuliert durch die natürliche Sprache in verbindlichen Verträgen lässt eine Verschmelzung in Programmcode auf absehbare Zeit noch nicht zu.

Könnten intelligente Rechtsverträge jemals als rechtlich durchsetzbar erachtet werden? Wahrscheinlich, denn trotz vieler Bedenken sind die Bedingungen, unter denen aus einer Vereinbarung ein rechtskräftiger Vertrag wird, flexibel und auf die zugrunde liegende Beziehung zwischen den Parteien abgestimmt und nicht abhängig von der Form des Vertrages. Mündliche Vereinbarungen können genauso wie E - Mail - Konversation vor dem Gesetz Gültigkeit erlangen. Doch von den vielen verschiedene Arten von Verträgen sind nur einige offensichtlich als Kandidaten für den Einsatz als „Smart Legal Contracts“ geeignet. Die größte Aufmerksamkeit bekommen sie aktuell im Bereich der

intelligenten Finanzinstrumente wie bei Verträgen im Handel von Aktien, Anleihen oder Derivate. Durch die Artikulation dieser Kodex-Verträge könnten die Finanzmärkte automatisiert und viele prozessintensive Systeme im Zusammenhang mit dem Handel und der Aktualisierung von Finanzinstrumenten vereinfacht werden.

### **Alternativen zu traditionellen rechtlichen Vereinbarungen**

Anstatt die gesetzlichen Verträge, die wir heute nutzen, einfach zu imitieren oder zu ergänzen, könnte mit Hilfe der Blockchain Technologie ein intelligenter Vertragskodex entstehen, der bestimmte, neue Arten von kommerziellen Vereinbarungen erleichtert. Dafür würde die Definition „Smart Alternative Contracts“ stehen.

Dieser Ansatz bietet eine umfassendere Sicht auf reale Probleme, die durch Verträge gelöst werden. In der Geschäftswelt agieren Einzelpersonen, welche stabile, vorhersehbare Vereinbarungen mit einander treffen. Verträge, zusammen mit einem starken Rechtssystem, sind die primären Mechanismen, die wir verwenden, um gegenseitig genug Anreize mittels Vertrauen für Beziehungen und eventuell riskante Geschäfte zu schaffen. Oft sind rechtliche Vereinbarungen nicht die einzige Lösung für dieses allgemeine Problem. „Smart Contract Code“ bietet neue Werkzeuge, um Begriffe und Anreizsysteme zu artikulieren und durchzusetzen, die wiederum Geschäfte ermöglichen.

Die am meisten diskutierte Möglichkeit dieser Art ist der direkte Handel zwischen Maschinen. Das wachsende Ökosystem von intelligenten Geräten, insbesondere solchen, die in gewisser Weise eigenständig sind, benötigt Programmcode um geschäftliche Interaktionen miteinander zu tätigen, z.B. für ein Auto, welches für seinen Strom selber zahlt. Diese Transaktionen erfordern immer noch ein Mindestmaß an Vertrauen, um kommerziell lebensfähig zu sein, sind aber schlecht für juristische Verträge geeignet, die vergleichsweise teuer sind und die Beteiligung juristischer Personen oder eines Menschen erfordern. Intelligente alternative Verträge könnten eine völlig neue Art von Handel ermöglichen, die zwischen unseren Computern, Autos, Telefonen und Geräten durchgeführt wird. Intelligente alternative Verträge können das Netz des Vertrauens jenseits der Reichweite des Rechtssystems ausdehnen, wo sie neue Formen des Handels ermöglichen, die heute nicht möglich sind.

## Fazit

Bei der Beschäftigung mit der Blockchain Technologie müssen sich alle bewusst sein, wie der Begriff „Smart Contracts“ in verschiedenen Communities verwendet wird. Dazu müssen eine Reihe schwieriger aber notwendiger, klärender Fragen zur ihrer Natur und ihrem Potenzial gestellt werden.

Auf Grund des interdisziplinären Ansatzes der Blockchain-Technologie und insbesondere die „Smart Contracts“ betrachten die Akteure die Technologie nur aus ihrem Blickwinkel und eventuell auf Kosten der anderen Beteiligten.

Rechtsanwälte sehen häufig „Smart Contracts“ nur als marginal verbesserte gesetzliche Vereinbarungen, ohne das sie das volle Potential der Blockchain Technologie und deren mögliche Reichweite betrachten.

Entwickler hingegen betrachten bei „Smart Contracts“ vor allem die grenzenlosen Möglichkeiten von Software, ohne die Feinheiten und kommerziellen Realitäten, die in traditionellen rechtlichen Vereinbarungen widerspiegeln, zu hinterfragen.