Bitcoin, Blockchain, Smart Contract

Jens Lechtenbörger

Oktober 2018

1 Überblick

Erinnern Sie sich daran, dass der technische Begriff *Konsens* (engl. *consensus*) gemeinsame Entscheidungen verschiedener Prozesse bezeichnet und dass Konsens in verteilten Systemen je nach zugrunde liegenden Annahmen schwierig bis unmöglich zu erzielen ist. Bitcoin strebt Konsens mit einer Technik namens Proof-of-Work an, wobei im Hintergrund kryptographische Hashfunktionen und digitale Signaturen zum Einsatz kommen.

Bitcoin wurde am 31. Oktober 2008 mit diesem Beitrag auf der Cryptography Mailing List vorgestellt, der wiederum einen Verweis auf das berühmte Bitcoin-Whitepaper von Satoshi Nakamoto enhält. Lesen Sie den Artikel von Nakamoto (die Abschnitte 7, 8, 9 können Sie auslassen), und beantworten Sie folgende Fragen: Mit welchen Eigenschaften würden Sie Bitcoin charakterisieren? Welche Probleme löst Bitcoin mit welchen wesentlichen Mechanismen?

Zum Vorlesungstermin werde ich auf Auszüge aus diesem Vortrag über Blockchain zurückgreifen.

Zudem werden wir frühe (1994) Ideen (1997) von Nick Szabo zu Smart Contracts diskutieren. Heute wird unter *Smart Contract* ein Programm verstanden, das auf einer Blockchain gespeichert ist (offen sichtbar, geschützt vor Manipulationen), durch Ereignisse gestartet wird und je nach Programmablauf neue Einträge auf der Blockchain vornimmt. Beispielsweise könnte ein Smart Contract die Rolle eines Auktionators, eines Notars oder einer Crowdfunding-Plattform übernehmen. Man beachte, dass Smart Contracts *keine* Verträge sind. Ob sie „smart“ sind, ist wohl Ansichtssache.

2 Lizenzangaben