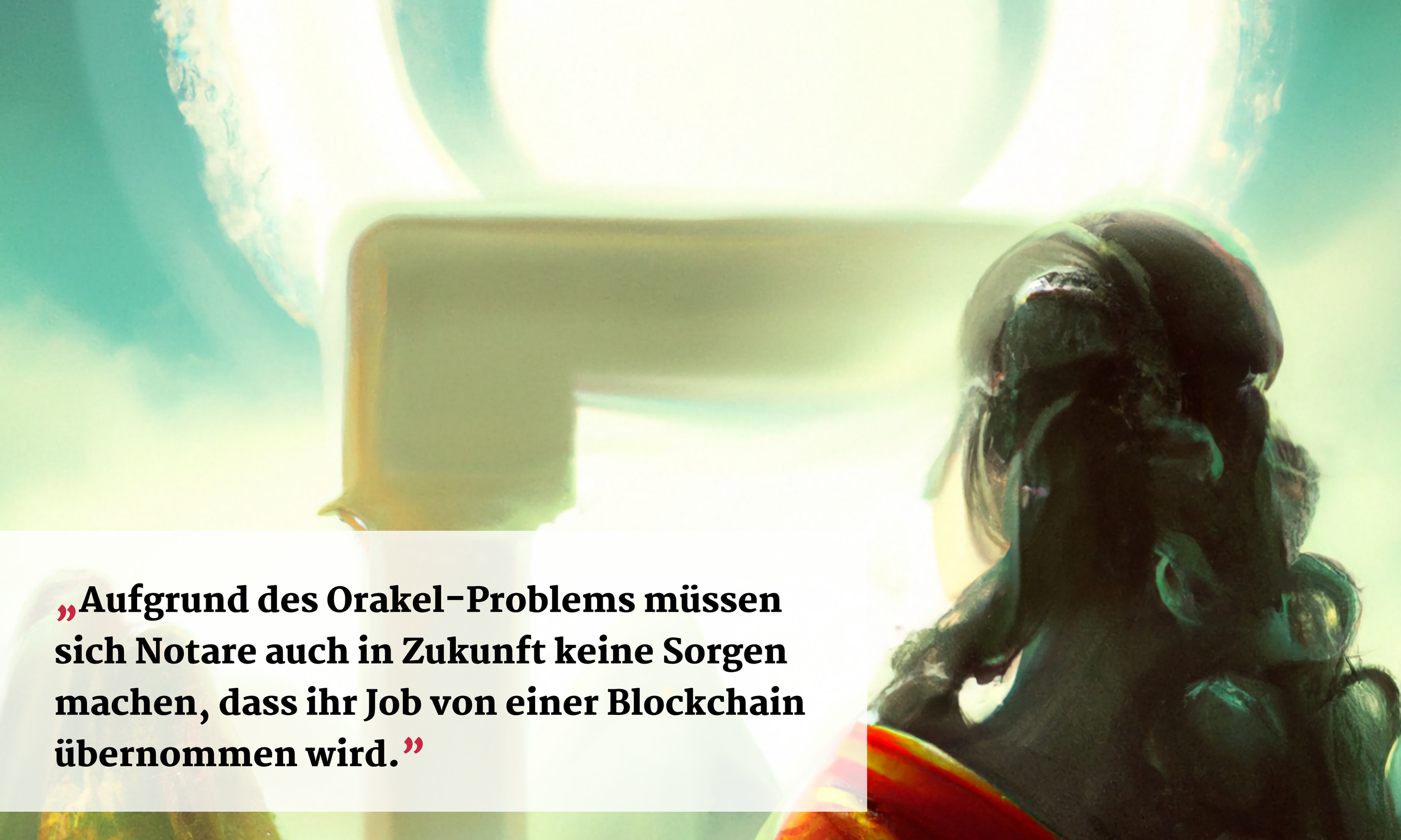


„Aufgrund des Orakel-Problems müssen sich Notare auch in Zukunft keine Sorgen machen, dass ihr Job von einer Blockchain übernommen wird."

Kolumne

Das Orakel-Problem oder: Warum Blockchains keine guten Notare sind

Roman Reher

Open Peer Review

Dieser Beitrag wurde lektoriert von:
Ferdinand Wegener & Jonas Neubert

Roman Reher (auch bekannt als ‚Blocktrainer') ist ein deutscher Informatiker, Bitcoin-Educator und Content-Creator. Sein YouTube-Kanal ‚Blocktrainer' ist mittlerweile einer der weltweit größten Kanäle mit Bitcoin-Fokus.

René Ackermann ist bei Blocktrainer.de für die Inhalte der Seite verantwortlich. Er verfasst News- und Wissensbeiträge, moderiert einen Podcast und berät Privatpersonen und Unternehmen zu allen Bereichen rund um Bitcoin.

„*Vergesst Bitcoins – die Zukunft heißt Blockchain.*"
„Man muss nicht an den Bitcoin glauben, um in die Blockchain zu investieren". „Bitcoin ist veraltet, es gibt ja schon neuere Blockchains". Solche und ähnliche Sprüche hat vermutlich jeder, der sich mit Distributed Ledger Technologies oder sogenannten Kryptowährungen beschäftigt, schon mehrfach gehört.

Bereits seit einigen Jahren und besonders in den beiden ‚Hype-Phasen' in den Jahren 2017/2018 und 2020/2021 konnte man zahlreichen Medien entnehmen, dass die Erfindung der Blockchain-Technologie unsere Welt verändern wird und dass diese gekommen ist, um zu bleiben. Egal ob Tech-Branche, Finanzindustrie oder sogar die Rechtswissenschaften, die Blockchain wird alle Bereiche unseres Alltags erfassen, so waren sich die Experten einig. Es brach eine regelrechte Blockchain-Manie aus.

Einige Unternehmer nutzten diesen Hype, ähnlich wie die ***Dotcom-Bubble*** in den 2000ern, direkt zu ihrem geschäftlichen Vorteil aus. So etwa der Eistee-Produzent ***Long Island Iced Tea Corp.*** aus New York. Die Führungsetage der Firma erkannte den Wahn, der von dem Buzzword ‚Blockchain' in vielen Menschen ausgelöst wird und benannte sich kurzerhand in ***Long Blockchain Corp***. um.[1] Der gewünschte Effekt ließ nicht lange auf sich warten. Der Aktienwert des Unternehmens stieg zwischenzeitlich um fast 500 %, obwohl sich an den Geschäftsprozessen oder Verkaufszahlen nichts geändert hatte.

A. Bitcoin statt Blockchain

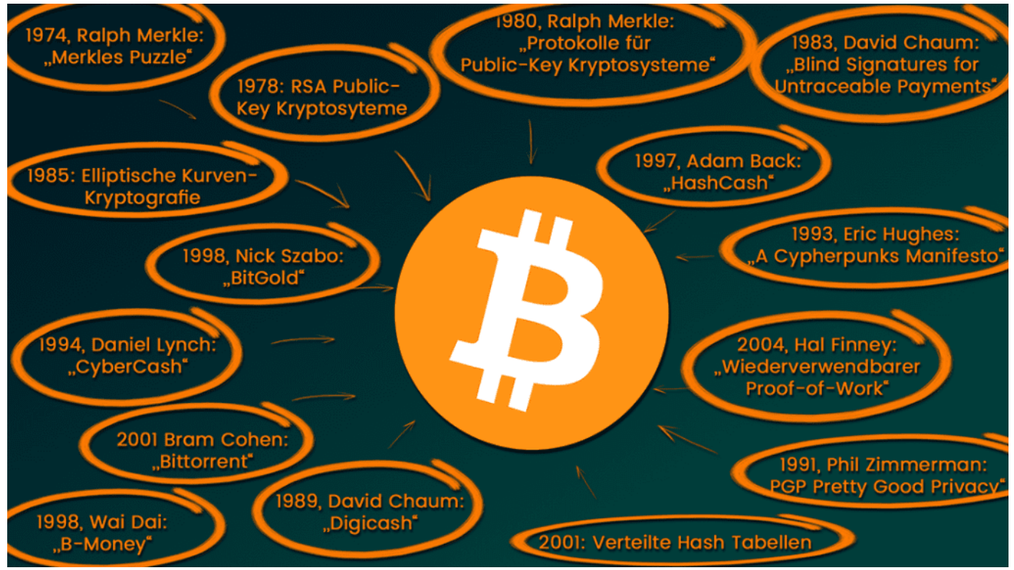
Während für viele Menschen der Begriff ‚Blockchain' eng mit ‚Bitcoin' verknüpft ist und teilweise sogar synonym verwendet wird, gibt es andere, die aus voller Überzeugung behaupten: „***Bitcoin ist eine veraltete Technologie, aber Blockchain wird die Welt verändern***". Interessanterweise wird das Wort ‚Blockchain' im berühmten Bitcoin-Whitepaper[2] kein einziges Mal erwähnt und nicht überall wo ‚Blockchain' draufsteht, ist auch wirklich ‚Blockchain' drin.

Weiter macht aber auch nicht in jedem Fall, in dem eine Blockchain für die Umsetzung einer Anwendung verwendet wird, dies tatsächlich Sinn. Blockchains sind hergebrochen im Grunde langsame Datenbanken, deren Technologie weder neu noch bahnbrechend ist. Tatsächlich gehen die ersten Überlegungen dazu bis in die 1970er Jahre zurück.

„Nicht in jedem Fall, in dem eine Blockchain für die Umsetzung einer Anwendung verwendet wird, macht dies tatsächlich Sinn."

Oft wird Bitcoin als die erste Blockchain, das erste digitale Geld oder auch die erste Kryptowährung betitelt. Genau genommen ist dies aber nicht korrekt, da bereits in den 1990er Jahren erste Kryptowährungen konzipiert wurden. Leider hatten diese aber mit verschiedenen Problemen zu kämpfen, die deren Sicherheit und Nutzbarkeit beeinflussten. ***Satoshi Nakamoto***, dem Erfinder von Bitcoin, gelang es im Jahr 2008 jedoch, diese Probleme zu beheben und Bitcoin zum ersten sicheren und limitierten digitalen Gut der Welt zu machen. Er verknüpfte geschickt bekannte Konzepte und ihm gelang es durch einen Energieaufwand in der physischen Welt eine digitale Knappheit zu erzeugen. Dies ist der eigentliche Durchbruch, der mit dem Start des Bitcoin-Netzwerks einherging.

1 *Gründerszene*, Eistee-Hersteller nennt sich in Blockchain um und lässt Aktie explodieren, hier abrufbar (Stand: 29.01.2023).
2 *Satoshi Nakamoto* (Pseudonym), Bitcoin: A Peer-to-Peer Electronic Cash System, hier abrufbar (Stand: 29.01.2023).



Bitcoin ist eine Komposition aus vielen älteren Konzepten. Quelle: blocktrainer.de

Die Erzeugung von digitaler Knappheit dient allerdings der Lösung von Problemen in einem sehr spezifischen Anwendungsfall, der Schaffung eines monetären Systems im virtuellen Raum. Diese Knappheit, und damit die technische Umsetzung über die Blockchain, wird in vielen anderen Fällen aber überhaupt nicht gebraucht und kann im Gegenteil zur Zweckerreichung sogar hinderlich sein.

Oft werden Zensurresistenz und Unveränderbarkeit ebenfalls als zentrale Eigenschaften von Blockchains genannt. Einmal davon abgesehen, dass man diese auch ohne eine Blockchain sicherstellen könnte, läuft man bei der Verknüpfung von der physischen und der digitalen Welt aber immer in das sogenannte ‘Orakel Problem’.

B. Was ist das Orakel-Problem?

Das Orakel-Problem bezieht sich auf die Herausforderung, wie man in eine Blockchain vertrauenswürdige Informationen von außerhalb, also aus der ‚realen Welt’, einspeisen kann. Grundsätzlich bezeichnet ein Orakel, lateinisch von ***oraculum*** für ‚Götterspruch’, eine Offenbarung oder Erkenntnis, die mittels der Befragung einer höheren Instanz – etwa einer Gottheit – gewonnen wurde.

Ein Orakel ist in diesem modernen Fall ein Mittelsmann, der entweder eine externe Datenquelle abfragt oder eine externe Schnittstelle aufruft, um aktuelle Informationen zu erhalten. Es muss jedoch sichergestellt werden, dass dieses Orakel, sei es eine staatliche oder private Quelle, vertrauenswürdig ist und dass die gelieferte Informationen wirklich unverfälscht und korrekt sind.

Das berühmteste Beispiel ist das antike Orakel von Delphi am Hang des Berg Parnass in Griechenland

Ein Anwendungsbeispiel könnte etwa ein Smart Contract sein, der auf Basis der Durchschnittstemperatur in einer Region die monatlichen Raten anpasst, die Kunden einer Versicherung für den Schutz vor Sturmschäden zahlen müssen. Selbst wenn dieser Smart Contract nun vollständig auf der Blockchain abgebildet wäre, so müsste er sich bei der Umsetzung externer Wetterdaten bedienen, die außerhalb der Blockchain stehen. Diese Wetterdaten müssten von Wetterstationen geliefert werden, auf die sich der Smart Contract und seine Nutzer wiederum verlassen müssten.

Einige Lösungen für das Orakel-Problem beinhalten die Verwendung von mehreren Orakeln, welche ihre Ergebnisse miteinander vergleichen und abstimmen, bevor sie bestätigt werden. Dies ist zwar für einige Anwendungsfälle eine zufriedenstellende, aber für wirklich wichtige Daten keine gute Lösung, denn auch hier ist Verfälschung möglich und Vertrauen in die Verlässlichkeit der Orakel notwendig. Bis dato ist es nicht möglich, Daten aus der Realwelt völlig vertrauensfrei in die digitale Welt und dementsprechend auch in Blockchains zu übertragen.

C. Die Blockchain als Notar?

Das Orakel-Problem ist auch der Grund dafür, warum sich beispielsweise Notare keine Sorgen machen müssen, dass ihr Job bald von einer (staatlichen) Blockchain übernommen wird. Unter dem Begriff ‚Tokenisierung' träumen einige Blockchain-Enthusiasten davon, dass bald Grundstücke und Immobilien, aber auch Vermögenswerte wie Kunst, Uhren oder Oldtimer in Form von sogenannten Nicht-Fungiblen-Token (NFTs) auf einer Blockchain dargestellt und repräsentiert werden können. Wer Halter des jeweiligen Tokens ist, soll dann auch automatisch Eigentümer des Vermögenswertes in der realen Welt sein. Wird ein Token über die Blockchain auf einen anderen Eigentümer übertragen, dann werden die Eigentumsverhältnisse überprüfbar verändert, so zumindest die Wunschvorstellung.

> „Notare müssen sich keine Sorgen machen, dass ihr Job bald von einer (staatlichen) Blockchain übernommen wird."

Einmal davon abgesehen, dass das deutsche Rechtssystem ohnehin noch nicht dafür ausgelegt ist und Notare, Grundbuchämter und Co. noch weitere Aufgaben (z.B. Beratungs- und Warnfunktion) erfüllen, stößt man bei der Tokenisierung von realen Objekten wieder auf das Orakel-Problem. Wer garantiert, dass die Daten zu einem Haus oder Grundstück auch tatsächlich korrekt sind, wenn sie in die Blockchain aufgenommen werden? Was passiert, wenn Token-‚Besitzer' ihre sogenannten ‚privaten Schlüssel',[3] also den Zugang zum jeweiligen Token verlieren? Muss das tokenisierte Haus dann abgerissen werden? Was ist, wenn mein Eigenheim-NFT durch einen Hack gestohlen wird? Muss ich dann ausziehen? Schlussendlich muss man sich bei all diesen Fragen wieder auf zentrale Instanzen verlassen. Den Blockchain-Hokuspokus hätte man sich demnach von Anfang an sparen können. Die erhoffte Disruption der Grundbuch- und Immobilienbranche wird wohl noch lange Zeit ein Traum bleiben und damit der Beruf des Notars auch in den kommenden Jahren sicher vor digitaler Konkurrenz sein.

3 *Blocktrainer*, Was sind Private & Public Keys?, hier abrufbar (Stand: 29.01.2023).

Roman fasst komplexe technische und ökonomische Sachverhalte in leicht verständliche Worte zusammen. Er war zudem mehrfach als Experte für diverse Medienformate tätig. Der ***Blocktrainer*** und sein Team stellen kontinuierlich aktuelle Bitcoin-Inhalte für ein deutschsprachiges Publikum bereit.

BLOCKTRAINER

YouTube

Reinhören lohnt sich:
Der Blocktrainer Bitcon Podcast

Zurück zum Inhaltsverzeichnis

CTRL

1/23

3. Jahrgang,1. Ausgabe
www.legaltechcologne.de/ctrl

Cologne Technology
Review & Law

Hier geht‘s zur ganzen Ausgabe!

Was das BGB mit Data Science und das StGB
mit Deepfakes zu tun hat und noch vieles mehr
in 12 spannenden Beiträgen!

LEGAL TECH LAB
COLOGNE

Cologne Technology
Review & Law