Blockchain (Teil 2)

Kryptographie II

VL 29

24.01.2019

Buch des Tages

Titel: Cryptography – Theory and Practice (4th Edition)

Autor(en): Doug Stinson

Verlag: CRC Press, 2018

Umfang: ca. 430 Seiten

Hinweise zum Inhalt:

Dies ist ein weiteres Standardwerk, das bereits mehrere Jahrzehnte existiert. Im vorliegenden Fall wurde jedoch regelmäßig aktualisiert und die derzeit 4. Ausgabe stammt aus dem Jahr 2018.

Das Buch zeichnet sich aus durch eine gut verständliche, wenngleich formal mathematische Darstellung der Grundlagen und wichtigsten Algorithmen. Schwerpunkt liegt auch bei diesem Buch auf Public Key Verfahren.

Blockchain Hype

- In jüngster Zeit entstand ein regelrechter Hype um das Thema Blockchain. Zahlreiche neue Anwendungen werden präsentiert, die sich zwei Merkmale der Blockchain zu eigen machen:
  a. Fälschungssicherheit bzw. Integrität eines Datenbestands
  b. Dezentralität bzw. Verzicht auf eine zentrale, regelnde Instanz
- In vielen (um nicht zu sagen den allermeisten) Fällen hätte man die benötigten Designmerkmale auch mit konventionellen Methoden wie Datenreplikation und/oder digitalen Signaturen erreichen können.
- Zudem wird zumeist nicht verstanden, dass die Mechanismen von Bitcoin (z.B. Motivation der User, eine Kopie der Blockchain zu speichern und zu verifizieren) nur selten auf andere Anwendungsbereiche übertragen werden können.

Blockchain vs Database

- Kann man eine Blockchain als besondere Art von Datenbank bezeichnen? Eigentlich schon, es gibt jedoch gravierende Unterschiede, die beim Einsatz einer Blockchain zum Problem werden können.
- Frage in die Runde: wer kann Aspekte bzw. Beispiele nennen?
- Datenschutz: alle Transaktionen, personenbezogene Daten (z.B. „aufgedeckte“ Pseudonyme) etc. sind in der Blockchain frei für alle lesbar; ist eine Identität erst zugeordnet, so lassen sich ALLE Transaktionen sehen
- Änderungen der Geschäftsanforderungen: die Datenstruktur der Blockchain ist unveränderbar. Müssen Anpassungen vorgenommen werden, führt dies ggf. zu Problemen („Hard Fork“). Bei einer gewöhnlichen Datenbank sind Änderungen dagegen einfach vorzunehmen.

Blockchain Nodes

- Voraussetzung für das Funktionieren einer Blockchain ist die Existenz von (möglichst vielen) unabhängigen Instanzen bzw. Usern, die eine eigene Kopie der Blockchain bei sich local speichern. Solche an der Blockchain-Anwendung aktiv beteiligte User bzw. deren IT-Systeme nennt man ***Nodes*** (Knotenpunkte).
- Man unterscheidet drei Arten von Nodes:
  1. ***Full Node***: speichert eine vollständige Kopie der Blockchain
  2. ***Publishing Node***: ein Full Node, der zudem auch neue Blocks publiziert
  3. ***Lightweight Node***: speichert nur für bestimmte Transaktionen relevante Teile der Blockchain und leitet Ergebnisse weiter an Full Nodes.

Pseudonyme Bitcoin-Adressen (1)

- Es hängt von der jeweiligen Blockchain-Anwendung ab, ob deren User in den gespeicherten Transaktionen namentlich genannt werden oder ob stattdessen Pseudonyme verwendet werden.
- Bei Bitcoin werden Sender und Empfänger in einer Transaktion mit ihrer sogenannten ***Adresse*** angegeben. Diese enthält keine Klarnamen sondern besteht aus einem eigens erzeugten String aus Ziffern, Groß- und Kleinbuchstaben (neuere Adressen unterscheiden nicht mehr zwischen Groß- und Kleinbuchstaben).
- Um Fehlinterpretationen beim Lesen zu vermeiden, werden hierbei folgende Zeichen vermieden: 0 Null, großes Oscar, großes India, kleines lima.
- Die Stringlänge beträgt hierbei 26-35 Zeichen, zumeist sind es 34 Zeichen.

Pseudonyme Bitcoin-Adressen (2)

- Mehrere Zeichen im Adress-String dienen als Prüfsumme, um Vertipper zu erkennen und die Adresse als ungültig zu identifizieren.
- Die Wahrscheinlichkeit, dass bei einem Vertipper eine falsche, jedoch gültige Bitcoin-Adresse entsteht, ist verschwindend gering. Schätzungen nennen eine Wahrscheinlichkeit von 1 zu 2^{32}.
- Dies schließt natürlich nicht aus, dass jemand bei auszuführenden Überweisungen beispielsweise in der Zeile verrutscht und einen anderen Empfänger einträgt. Auch ein absichtlicher Austausch (händisch oder durch Malware) ist leicht möglich.
- Bitcoin-Adressen warden manchmal auch als QR Code dargestellt.

Pseudonyme Bitcoin-Adressen (3)

- Jeder Bitcoin User besitzt ein kryptographisches Schlüsselpaar bestehend aus Secret Key und Public Key. Den Public Key kann man zur Identifizierung von Sender und Empfänger verwenden und hieraus eine Adresse ableiten. Vereinfacht dargestellt:
  - jeder User wird zunächst identifiziert mit seinem Public Key
  - der Public Key wird durch eine Hashfunktion geschickt
  - der resultierende Hashwert wird in einen Zeichenstring aus Ziffern und Buchstaben konvertiert und dient als Identifier bzw. Adresse in der Blockchain
- Da keine Klarnamen verwendet werden, lässt sich ein Bitcoin User nur anhand seiner Adresse identifizieren.

Pseudonyme Bitcoin-Adressen (4)

- Eine Zuordnung von Bitcoin-Adresse zu Klarnamen versuchen User zumindest dann zu verhindern, wenn sie in kriminelle Geschäfte verwickelt sind. Gelegentlich gelingt eine Zuordnung, falls eine Adresse nicht nur z.B. im Darknet, sondern auch im Alltag verwendet wird, beispielsweise beim Bezahlen legaler Produkte und Dienstleistungen.
- Beim Tausch von Bitcoin in herkömmliche Währungen ist oftmals eine Personenidentifizierung (ID Card) gesetzlich vorgeschrieben.
- Zur Verschleierung von Identitäten und Zahlungsströmen verwenden viele User für jede Transaktion eine andere, neu erzeugte Adresse.
- Ein eigener Zweig der digitalen Forensik beschäftigt sich mit Methoden, die realen Personen hinter Bitcoin-Adressen aufzudecken und/oder mehrere Adressen einer gemeinsamen Identität zuzuordnen.

Pseudonyme Bitcoin-Adressen (5)

- Die Blocks einer Blockchain enthalten nicht immer nur Transaktionen, die Personen zugeordnet werden können.
- Eine wichtige Anwendungsart sind sogenannte Smart Contracts. Diese haben Bekanntheit erlangt nicht im Zusammenhang mit Bitcoin, sondern mit einer anderen Währung: Ethereum.
- Die bei Ethereum in der Blockchain abgespeicherten Smart Contracts adressiert man über sogenannte Contract Accounts, dem Analogon zu Bitcoin Addresses. Die Contract Accounts werden abgeleitet von der Adresse ihrer jeweiligen Erzeuger.
- Natürlich gibt es auch Blockchain Anwendungen, in denen keine Namen benötigt werden, oder solche, in denen keine Anonymität gewünscht ist (z.B. elektronisches Grundbuch).

Private Key Storage

- der private Key eines Bitcoin Users ist dessen alleiniges Zugangsmedium zu seinem digitalen Geld
- geht der Key verloren, ist auch das Geld verloren: Bitcoins sind zwar weiterhin in der Blockchain abgespeichert, aber nicht mehr zugreifbar
- nahezu alle Angriffe auf Bitcoin fokussieren sich auf das Entwenden oder Erraten privater Schlüssel
- Erraten von Schlüsseln erfolgt hierbei über das Raten von Passwörtern, mit deren Hilfe z.B. eine Bitcoin Wallet gesichert wurde
- Wurde ein Private Key entwendet und die zugehörigen Bitcoin in der (öffentlich einsehbaren) Blockchain mithilfe einer Transaktion an einen neuen Besitzer übertragen, so lässt sich diese Transaktion nicht mehr rückgängig machen.
- Wallets dienen der sicheren Aufbewahrung privater Schlüssel. Ferner können sie Public Keys und Adressen speichern, ähnlich wieeine Liste mit Überweisungsempfängern in einem Homebanking-Programm.

Permissionless vs Permissioned Blockchains

- In der Praxis kann man zwei Typen von Blockchain-Anwendungen unterscheiden: permissionless und permissioned.
- Eine ***Permissionless Blockchain*** erlaubt aktive Beteiligung ohne vorherige Autorisierung. Prominentestes Beispiel ist Bitcoin.
- Permissionless Blockchains erzwingen besonders hohe Anforderungen an die Sicherheit, da hier keinerlei Schutzvorkehrungen getroffen werden können, die nicht per se in den Funktionsregeln der Blockchain-Implementierung eingebaut sind. Jeder Teilnehmer muss als potentieller Betrüger behandelt werden.
- ***Permissioned Blockchains*** werden i.a. von einer Institution betrieben, die eine Teilnahme an bestimmte Bedingungen knüpft, beispielsweise einen Status als Kunde, Mitarbeiter, etc.

Consensus Modelle

Wie wächst eine Blockchain

- Bereits bestehende Teile einer Blockchain müssen gegen Veränderungen geschützt sein. Doch wer ist berechtigt, neue Blöcke an die existierende Blockchain anzufügen?
- In vielen Blockchain-Anwendungen, insbesondere bei Cryptocurrencies wie Bitcoin, ergibt sich ein finanzieller Gewinn, wenn man einen neuen Block an die bestehende Blockchain anfügen kann und diese Ergänzung durch die User Community akzeptiert wird.
- Da es keine übergeordnete Instanz gibt, die solche Fragen entscheidet, muss innerhalb der Teilnehmergruppe ein Konsens erreicht werden.
- Grundsätzlich muss hierbei davon ausgegangen werden, dass jeder Teilnehmer den eigenen Vorteil sucht und dies auch – soweit möglich – auf unfaire Weise verswuchen kann.
- Fairness-Regeln und Betrugsprävention müssen daher quasi eingebaut sein.

Wettstreit und Dissens

- Betrachten wir Bitcoin als Beispiel für eine Anwendung, in der – zumindest theoretisch – alle Anwender gegeneinander spielen.
- Jeder Teilnehmer möchte neue Blocks erzeugen und als neuen Bestandteil der offiziellen Blockchain etablieren. Der monetäre Vorteil besteht wahlweise in der Schaffung neuer Bitcoin-Einheiten oder in der Gewinnung sogenannter Transaction Fees.
- Kein Teilnehmer hat automatisch einen Vorteil darin, neue Blöcke anderer Teilnehmer anzuerkennen.
- Mehrere Teilnehmer publizieren nahezu zeitgleich neue Blocks, es kann jedoch immer nur ein ausgewählter Block an die bestehende Blockchain angefügt werden und die anderen Kandidaten werden ggf. verworfen.
- Alle Beteiligten müssen sich effizient verständigen auf eine Lösung bzw. den nächsten offiziellen Block, damit das System im allseitigen Interesse weiter funktioniert.

Konsens Modelle (1)

- Consensus Models sind ein zentraler Bestandteil von Bitcoin sowie zahlreichen anderen Permissionless Blockchain Applications, insbesondere Cryptocurrencies.
- Das Konsens-Modell beschreibt die Regeln, nach denen eine untereinander konkurrierende, sich nicht wechselseitig vertrauende und nur den eigenen Vorteil verfolgende Gruppe von Benutzern vorgehen muss, um Einigung zu erzielen, wie neue Blöcke als gültig anerkannt und an die Blockchain angefügt werden.
- Die Herausforderung besteht hier darin, ohne eine Trusted Third Party auszukommen, die für viele andere kryptographischen Anwendungen unverzichtbar ist.
- Die Kriterien, nach denen ein Teilnehmer die „Berechtigung“ erhält, neue Blocks anzufügen, können völlig unterschiedlich definiert sein.

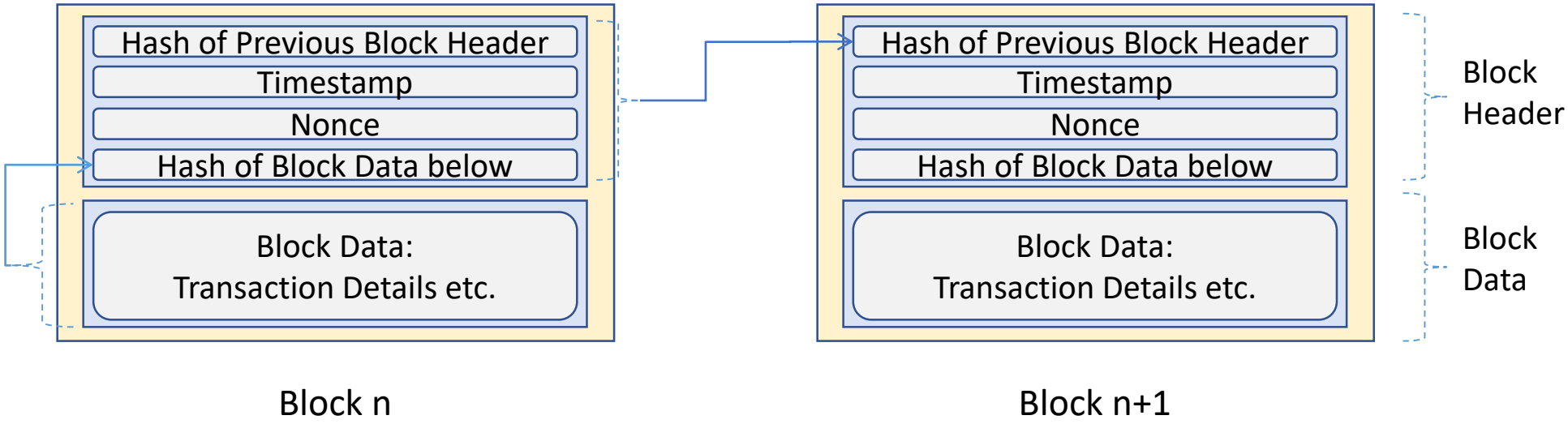
Konsens Modelle (2)

- Das Konsens-Modell muss unterschiedliche Arten betrügerischer Versuche abwehren können. Beispiele:
  - Manipulationen an der bestehenden Blockchain
  - Betrügerisches Erschleichen der Berechtigung zum Anfügen neuer Blocks
  - Erlangung unfairer Vorteile zwecks Erlangung der Berechtigung zum Anfügen neuer Blocks
  - Unterbindung legitimer Blockchain-Erweiterungen durch andere Teilnehmer
  - Denial of Service gegen die gesamte Blockchain-Anwendung
  - Herstellung von Patt-Situationen, die eine Entscheidungsfindung verhindern
  - feindliche Übernahme der Entscheidungshohheit betreffs Akzeptanz neuer Blocks
  - kryptoanalytische Angriffe aller Art
  - Manipulationen der System- oder Netzwerkinfrastruktur
  - Ausnutzen von Fehlern im Code oder Manipulationen am Code
  - ...vieles mehr...

Proof of Work

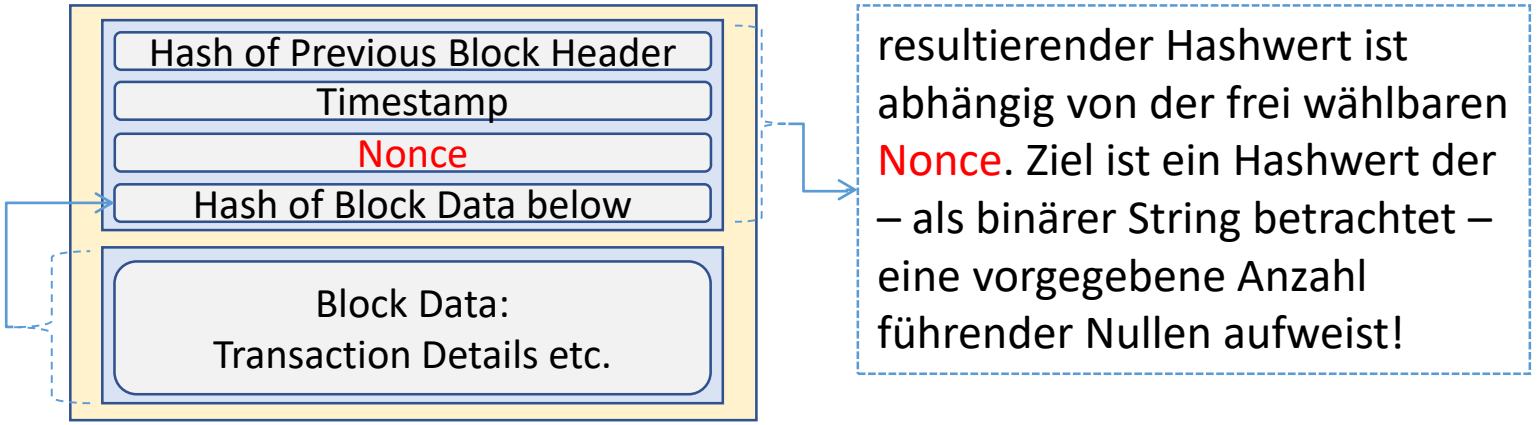
- Das bekannteste und in Bitcoin verwendete Consensus Model ist der sogenannte ***Proof of Work***. Hierbei erarbeitet sich ein User das Recht, den nächsten Block anzufügen.
- Die Arbeit besteht im Falle von Bitcoin in der Lösung eines Computationally Intensive Puzzles.
- Ein solche Puzzle muss relativ schwer zu lösen sein und die Verifizierung der richtigen Lösung durch die restlichen Teilnehmer muss wiederum einfach sein.
- Wir haben in der Asymmetrischen Kryptographie bereits Probleme kennengelernt, die dieses Kriterium erfüllen: beispielsweise das Faktorisieren großer Zahlen oder die Berechnung diskreter Logarithmen.
- Bitcoin und einige andere Kryptowährungen haben sich jedoch für eine andere Art Puzzle entschieden: zu dessen Lösung muss eine große Anzahl Hahwerte berechnet werden.

Aufbau eines Bitcoin Blocks



Die Bedeutung von Hash-Berechnungen bei Bitcoin (1)

- Der Proof of Work in Bitcoin erfolgt durch Berechnung des Hashwerts des Block Headers. Den Hashwert kann man beeinflussen durch Änderung der frei wählbaren Nonce.
- Das Puzzle ist gelöst, sobald der Hashwert eine vorgegebene Struktur aufweist.
- Die Nonce wird typischerweise bei einem Zufallswert begonnen und dann schrittweise um eins inkrementiert.



Die Bedeutung von Hash-Berechnungen bei Bitcoin (2)

- Für jeden neuen Puzzle-Lösungsversuch ist folgendes zu tun:
  - neue Nonce wählen (z.B.: Nonce_neu := Nonce_alt + 1)
  - Hashwert des modifizierten Block Headers neu berechnen
  - prüfen, ob der Hashwert die gewünschte Form aufweist
- Angenommen, das Puzzle gilt als gelöst, sobald der Hashwert insgesamt k führende Nullen aufweist.
- Nehmen wir an, dass Hashwerte wie Zufallswerte aussehen, so erfüllt einer von 2^k Hashwerten die Anforderung an eine gültige Puzzle-Lösung.
- Wenn man durch reines Ausprobieren eine Lösung finden möchte, so braucht man durchschnittlich 2^{k-1} Versuche.
- Das Präsentieren eines passenden Hashwerts (Puzzle-Lösung) gilt als Proof of Work.

Anpassung der Puzzle-Schwierigkeit

- Bei Bitcoin strebte man an, dass etwa alle zehn Minuten ein neuer Block publiziert wird. Es soll also ca. zehn Minuten dauern, bis innerhalb der gesamten Teilnehmergruppe ein Teilnehmer eine neue Puzzle-Lösung findet.
- Die Schwierigkeit des Puzzles wird im System regelmäßig an obige Bedingung angepasst, und zwar genau alle 2016 Blöcke.
- Die Anpassung erfolgt durch Herauf- oder Herabsetzen des Parameters k, also der geforderten Anzahl führender Nullen im Hashwert.
- Auf diese Weise reagiert das System flexibel auf eine steigende Nutzeranzahl sowie immer leistungsfähigere Hardware. Der Parameter k steigt folglich regelmäßig. Theoretisch könnte er im Bedarfsfall aber auch wieder gesenkt werden.

Bitcoin Mining

- Eine maßgebliche Rolle beim sogenannten Bitcoin Mining (also dem systematischen Versuch eine Puzzle-Lösung zu generieren) spielt die verwendete Hardware einerseits und die Stromkosten andererseits.
- In Ländern mit exorbitant hohen Strompreisen wie Deutschland kann Bitcoin Mining kaum wirtschaftlich betrieben werden. Professionelle Miner weichen aus in Länder mit sehr geringen Stromkosten. Lange Zeit war dies beispielsweise China, bis Mining dort verboten wurde. Heute finden sich Miner u.a. in Island, wo zu niedrigen Stromkosten zusätzlich noch die natürlich vorhandene Kühlung nutzbar ist.
- Auf einem Standard-PCeignet sich die Grafikkarte (GPU) weitaus besser zum Berechnen von Hashwerten als die CPU. Mehrere Jahre lang hat man spezielle Mining Racks gebaut mit zahlreichen GPUs.
- Mittlerweile sind GPUs nicht mehr konkurrenzfähig und professionelle Miner verwenden speziell für die Hashberechnung optimierte Spezialhardware.

Warum Hashing als Puzzle (1)

- Die zuvor formulierten Anforderungen an ein Puzzle zwecks Proof of Work können auf ganz unterschiedliche Weise realisiert werden. In der Tat gibt es in der Praxis nicht nur den bei Bitcoin verfolgten Ansatz, sondern eine ganze Theorie rund um Proof of Work Verfahren.
- Wichtiges zusätzliches Merkmal ist folgendes: angenommen, zahlreiche User sind “mitten drin”, ein Puzzle zu lösen.
- Dann publiziert ein anderer User seine Puzzle-Lösung.
- Das System funktioniert nur dann, wenn alle User bereit sind, die neu publizierte Puzzle-Lösung anzuerkennen, die Blockchain um einen Block zu erweitern und auf dem neuen Block wieder von vorne zu beginnen mit dem Versuch, das Puzzle zu lösen.

Warum Hashing als Puzzle (2)

- Angenommen, man käme der Lösung eines Puzzles schrittweise näher, wenn man bereits einige Arbeit hineingesteckt hat.
- Dann wäre niemand daran interessiert, die neue Lösung eines anderen Users anzuerkennen, da dann die eigene bereits geleistete Arbeit “vernichtet” würde.
- Der Bitcoin Proof of Work basiert jedoch auf willkürlichem Durchprobieren von Hashwerten. Es entsteht kein Vorteil oder Nachteil, wenn man die Arbeit auf dem n-ten Block einstellt und stattdessen auf dem n+1 ten Block weiterarbeitet.
- Aus diesem Grund eignet sich Hashing als Proof of Work weit besser als beispielsweise einige der in asymmetrischer Kryptographie kennengelernten Verfahren (Primfaktorisierung etc.), da man dort schrittweise einer Lösung näher kommen kann.