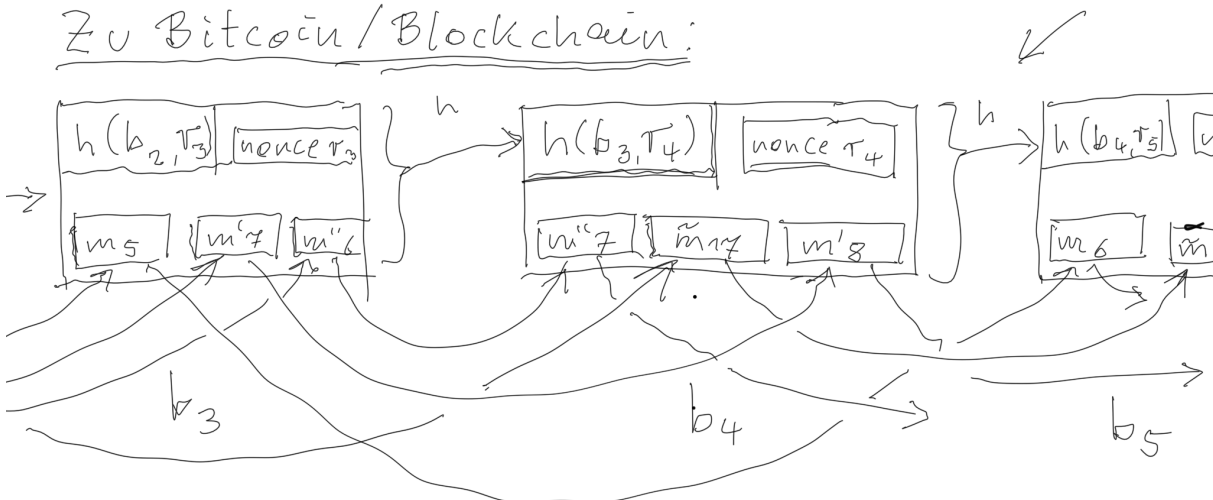


Vorlesung Kryptographie


Aufzeichnungen vom 21.6.

Zu Bitcoin/Blockchain:

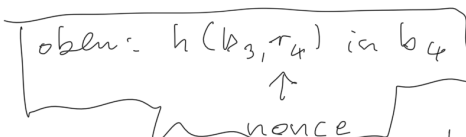
Viele Hashchains (= Einträge im Kassenzettel) in einer globalen Hashchain: Blockchain

- Blockchain verteilt & öffentlich auf etlichen Rechnern
- Jeder kann Transaktionen m_i einreichen zur Aufnahme in den nächsten Block b_j .

Im Prinzip kann jeder neue Blöcke veröffentlichen.
Dazu: 3 Bedingungen

1. b_{j+1} aus b_j berechnen ist aufwendig
2.  wird bezahlt (in btc)
3. Nur der längste Zweig gilt.

Zu 1.: Finale Zahl r_{j+1} , so dass $h(b_j, r_{j+1})$

 mit K Nullen beginnt
Kontrollschraube. Ziel: ein
neuer Block alle 10 min. (Wird alle 14 Tage
geprüft & evtl angepasst)

- Aktuell: 1.3.2014: $\approx 16 \cdot 10^{18}$ rs ausprobieren
- " 1.3.2014: $\approx 200 \cdot 10^{18}$ " "

~~mining~~ (mining)

7

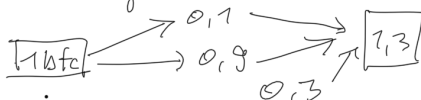
Zu 2. Im Moment: 12,5 btc/block. Halbiert
sich alle 210000 Blöcke (≈ 4 Jahre) (ab 2020:
6,25) Bis im Jahr 2140 21 Mio btc erzeugt
werden. = Maximum. Dann nur noch

- Transaktionskosten: Wer Transaktionen mit
einreicht, kann Gebühren anbieten.
(Neulich: 2013: 0,17 btc/block)

Anfang 2014: 1 btc = 800 US\$, 7.6.2014:

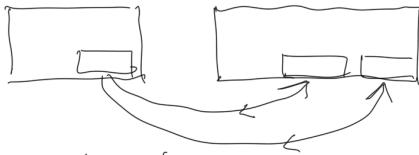
2784 US\$ Obacht: Sehr beweglich
hochspekulativ, es gab schon viele Blasen und
Einbrüche.

- Splitten: Bitcoin-Beträge können auch gesplittet
werden:

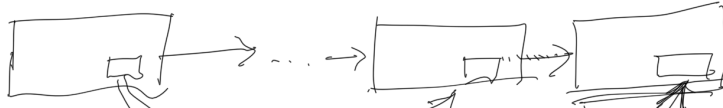


Zu 3. löst das Problem des Mehrfachausgebens einer Münze. Denn:

- innerhalb innerhals eines Blocks kann das geprüft werden:



- genauso innerhalb derselben Kette:



und 3. sagt: nur ein Zweig ist gültig!

Es passiert zwar:

Nakamoto „Falls die Mehrheit der Rechnerkapazität ehrlich ist“ klappt's.



8 Primzahltests

Geg n , ist n prim? Für Zahlen, die als Endziffer 0, 2, 4, 5, 6, 8: Nein interessant nur für Endziffern 1, 3, 7, 9.

• Naiv: Teste für $i=2, 3, 5, 7, 11, \dots, \lfloor \sqrt{n} \rfloor$ ob $\frac{n}{i} \in \mathbb{N}$.

- Ist das nicht effizient? $O(\sqrt{n})$ sub-polynomiell? Nein. Korrekte Eingabegröße: Zahl der Dezimalstellen (oder Binärstellen) von n : $d \approx \log_{10}(n)$ (bzw $\log_2(n) \approx d$)
Also $n \approx 10^d$ (bzw 2^d)
Laufzeit $O(10^{d/2})$ (bzw $O(2^{d/2})$)

Es gibt polynomielle Primzahltests ~~mit~~
(deterministisch) AKS-primality-test

2002: Primes is in P.

In der Praxis werden aber andere Tests benutzt,
oft:

Probabilistische Primzahltests

Finde eine Eigenschaft $E = E(n, a)$, die

- eine Primzahl n haben muß (für alle a)
- eine Nicht-Primzahl n nur mit Wahrscheinlichkeit $p \leq 1$ (bzgl. a) (think: $a^{n-1} \equiv 1 \pmod{n}$)

Teste dann K -mal $E(n, a)$ $\left\{ \begin{array}{l} \text{ggT}(a, n) = 1 \Rightarrow \\ a^{4(n)} \equiv 1 \pmod{n} \end{array} \right\}$
(n fest, a zufällig & unabh.)
• Falls $E(n, a)$ verletzt: Ausgabe „ n ist keine Primzahl“
(dann heißt a Zeuge (für _____))

- Falls $E(n, a)$ immer erfüllt: Ausgabe
„ n ist wahrscheinlich Primzahl“. Wahr mit Wahrsch.
 $1 - p^K$, (n nicht prim: K Runden: p^K)

Daher ist das praktikabel: z.B. $p = \frac{1}{2}$

Wähle z.B. $K = 1000$ oder $K = 10^6$

Irrtum (Ausgabe: „ n ist wahrsch. Primzahl“ obwohl
 n keine ist) ist

$$1 - \left(\frac{1}{2}\right)^{1000} \approx 10^{-300} \quad \left\{ \begin{array}{l} \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \end{array} \right. \quad \left\{ \begin{array}{l} 10^6 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \end{array} \right. \quad 1 - \left(\frac{1}{2}\right)^{10^6} \approx 10^{-300000}$$

Bsp. Fermat-Primzahltest

(s.o. $a^{n-1} \equiv 1 \pmod{n}$ falls n prim)
für alle $1 \leq a \leq n-1$

Also Lemma 8.1 $a^{n-1} \not\equiv 1 \pmod n \Rightarrow n$ nicht prim

Fermat-Primzahltest: n geg., K wählen

• While $i < K$

 • Wähle zufällig $a \in \{2, 3, \dots, n-1\}$

 • falls $a^{n-1} \not\equiv 1 \pmod n$ STOP „ n nicht prim“

 • $i = i + 1$

• Ausgabe „ n wahrsch. Primzahl“

Wie gut ist das?

Antwort 1: Gut. Denn z.B. der Zeuge $a=2$
entlarvt schon viele zusammengesetzt

(vgl. A29 Blatt 8)

- $n = 4$: $2^3 \equiv 8 \not\equiv 1 \pmod 4$; Also 4 nicht prim.
- $n = 6$: $2^5 \equiv 2 \not\equiv 1 \pmod 6$ " 6 " "
- $n = 9$: $2^8 \equiv 4 \not\equiv 1 \pmod 9$ " 9 " "

Problem: Leider gibt es zusammengesetzte
Zahlenⁿ für die 2 kein Zeuge ist, noch
irgendein anderes a mit $2 \leq a \leq n-1$ mit
 $\text{ggT}(a, n) = 1$.

Diese Zahlen wird der Fermattest nicht als
zusammengesetzt entlarven. (Mehr in A30, Bl. 9)

Daher feinere Tests: Solovay-Strassen, Miller-Rabin
(Dazu noch etwas Zahlentheorie: quadratische Reste,
(Legendresymbol, Jacobi symbol)

* *

*