# *Bitcoin:*
# Ein sinnloses Wettrennen von Computern?

## Kryptographische, technische und praktische Hintergründe von Bitcoin

*Klaus Kusche*

*Frühjahr 2024*

# Was ist Bitcoin?

- Eine ***"Krypto-Währung"***
- Eine Menge von

***Regeln, wie Bitcoins entstehen, gespeichert werden und überwiesen werden***

- Ein ***Programm***, das diese Regeln ausführt
  (das Programm ist *kostenlos und Open Source*)
- Ein weltweites ***Netzwerk von Rechnern***, auf denen dieses Programm läuft

# Ziele des Bitcoin-Erfinders (1)

Die Währung soll

***nicht zentral kontrollierbar***
***und nicht von einer Person***
***oder einem Staat beherrschbar sein!***

Eine *"**demokratische**"* Währung *ohne Staatsgrenzen*:

- ***Alle Daten sind weltweit verteilt gespeichert***
- ***Jeder*** kann mitmachen (mit Rechner, Programm und Internet)
- Alle Beteiligten weltweit sind ***gleichberechtigt***
- Das System ist *betrugs- und manipulationssicher*

# Ziele des Bitcoin-Erfinders (2)

Der Besitz der Währung soll

***anonym*** *sein!*

Jede Bitcoin-"Geldbörse" ist ***öffentlich***
(d.h. jeder sieht den Inhalt und die Überweisungen),

aber ***ihr Besitzer ist nirgends gespeichert***
und kann nicht ermittelt werden!

==> Ziele nur teilweise erreicht

**==> *Des Verbrechers Traum!***

# Bitcoin & Kryptographie

- ***"Wallets"*** (= Geldbörsen)
  und *einzelne* Überweisungen:

## *"Public Key"-Verfahren*

*zum "Unterschreiben"*
*und zum Verschlüsseln*

- ***"Blockchain"***
  (= Speicherung *aller* Überweisungen):

## *Kryptographische Hash-Verfahren*

*zum ... (später)*

# "Public Key"-Verfahren (1)

Anderer Name:

***Asymmetrische Verschlüsselungsverfahren***

Weil: Verschlüsseln und Entschlüsseln geschieht mit

***zwei verschiedenen***
*(aber **zusammengehörenden**) Schlüsseln!*

Ein solches ***"Schlüsselpaar"*** besteht aus

- dem ***öffentlichen Schlüssel*** (*jedem* bekannt)
- und dem dazugehörigen ***privaten Schlüssel***
  (nur *einer einzigen Person* bekannt, *geheim*!!!)

# “Public Key”-Verfahren (2)

## Idee dahinter: Nutze *“Einweg-Funktionen”*

- Die Generierung eines ***neuen Schlüsselpaares*** ist

  ***“einfach”*** (nur viel Mathematik)

- Aber die ***Berechnung des privaten Schlüssels*** aus dem dazugehörigen öffentlichen Schlüssel ist

  ***praktisch unmöglich***

  (außer durch Durchprobieren aller Möglichkeiten,
  und das dauert bei großen Zahlen mit hunderten Stellen!)

# “Public Key”-Verfahren (3)

**Beispiel:**

***Produkt*** *zweier sehr* ***großer Primzahlen***

- Das **Produkt** aus den beiden Zahlen zu berechnen ist **leicht** (einfach multiplizieren)
- Aber nur aus dem Produkt wieder die **beiden ursprünglichen Zahlen** zu berechnen ist **sehr mühsam** (faktorisieren riesiger Zahlen???)

==> *Grundlage von RSA,*
*dem ältesten Public-Key-Verfahren*

# “Public Key”-Verschlüsselung

- **Jeder Absender** kann die Daten mit dem

  ***öffentlichen Schlüssel des Empfängers verschlüsseln***

- Nur der “**richtige**” **Empfänger**
  kann die verschlüsselte Nachricht mit

  ***seinem dazugehörenden privaten Schlüssel entschlüsseln***

# “Public Key”-Signatur

- **Nur der Ersteller** eines Dokumentes kann es

  ***mit seinem privaten Schlüssel signieren (“unterschreiben”)***

- **Jeder Empfänger** kann

  ***mit dem öffentlichen Schlüssel des Erstellers Dokument und Signatur prüfen:***

  ==> *Kommt es wirklich von genau diesem Ersteller?*

  ==> *Ist es unverfälscht?*

# “Public Key” in Bitcoin (1)

- Zu ***jedem Wallet*** gehört ein ***Schlüsselpaar***
- Das Schlüsselpaar ist zugleich ***“Kontonummer”*** und Name des Kontos (es gibt *keinen “Inhaber-Namen”*)
- Der ***Besitzer*** des Wallets *(und nur dieser!)* kennt den ***privaten Schlüssel*** des Wallets
- Der ***Besitz des privaten Schlüssels*** ist die ***einzige Identifikation bzw. Legitimation des Besitzers*** gegenüber dem Bitcoin-System

  *(sonst kein Name, kein Identitäts-Dokument, kein Passwort, keine PIN oder TAN ...)*

# “Public Key” in Bitcoin (2)

**Vereinfacht:** ***Überweisungen*** werden mit dem ***privaten Schlüssel des abgebenden Wallets*** signiert

==> ***Nur der Besitzer*** des privaten Schlüssels kann ausgehende Überweisungen erstellen bzw. ***Bitcoins*** aus dem Wallet ***entnehmen***

==> ***Jeder*** kann mit dem dazugehörigen ***öffentlichen Schlüssel prüfen***, ob
- die Überweisung ***wirklich vom Besitzer*** kommt
- und *unverfälscht* ist

(sonst würde die Signatur nicht stimmen)

# “Public Key” in Bitcoin (3)

**Vereinfacht:** Teile der Überweisung sind mit dem ***öffentlichen* Schlüssel des Empfängers** codiert:

==> Nur der ***“richtige” Empfänger***
kann mit seinem ***privaten* Schlüssel**
auf die überwiesenen Bitcoins zugreifen

**Technisch:** Bitcoin verwendet primär
ein *256 bit ECDSA Verschlüsselungsverfahren*
(mit einer sehr speziellen EC = *“Elliptic Curve”*)

# “Public Key” in Bitcoin (4)

- ***“Privater Schlüssel verloren”***

  ==› Alle Bitcoins in diesem Wallet sind

  ***unwiederbringlich verloren!***

  (weil sie niemand mehr überweisen kann)

- ***“Privater Schlüssel gestohlen”***
  *oder öffentlich bekannt geworden*

  ==› Der Dieb bzw. jeder kann

  ***alle Bitcoins*** aus dem Wallet
  ***irgendwohin überweisen!***

# Kryptographische Hashes (1)

Hier: *"**Hash**" = **Prüfsumme** eines Datenblockes*

*"**Kryptographisch**"* = *sicher* = so berechnet, dass man

- ... ***nicht*** gezielt *zu gegebener Prüfsumme einen dazupassenden Datenblock* berechnen kann
- ... ***nicht*** gezielt *zwei Datenblöcke mit derselben Prüfsumme* berechnen kann

==> *"Hash berechnen"* ist eine ***"Einweg-Funktion"***:
- *"Daten gegeben, deren Hash berechnen"* ist ***einfach***
- *"Hash gegeben, dazupassende Daten berechnen"* ist ***unmöglich*** (außer durch *Durchprobieren* aller Daten)

# Kryptographische Hashes (2)

Kryptographische Hashes haben einen sogenannten

***"Lawinen-Effekt":***

Auch wenn sich *nur 1 Bit in den Daten ändert*,
ändern sich durchschnittlich

*die **Hälfte** aller Bits im Hashwert*
*(aber welche Bits sich ändern*
*ist nicht vorhersehbar!)*

==> *Man kann also **nicht die Daten gezielt so ändern**,*
*dass sich nur bestimmte Bits des Hashwertes ändern!*

# Die Blockchain (1)

***Blockchain = "Kette" von Datenblöcken***

**Ziel:** *Manipulationssichere* Speicherung (Archivierung)

- *Neue Daten* werden immer nur *hinten angehängt*
- *Bestehende Daten* werden *nie mehr geändert*

**Verkettung:**

*Jeder Block enthält neben den Daten auch den* ***Hashwert des vorigen Blockes***

(und damit *indirekt* die *Hashwerte aller Blöcke davor*!)

# Die Blockchain (2)

Die gesamte Blockchain (außer dem letzten Block)
ist **manipulationssicher**:

*Ein Bit ändert sich irgendwo*
*==> alle nachfolgenden Hashwerte*
*stimmen nicht mehr!*

Es ist praktisch ***unmöglich***, *nachträglich*
einen ***"gefälschten" Ersatz-Block*** zu berechnen,
der ***denselben Hashwert***
wie der ursprüngliche Block hat!

# Die Bitcoin-Blockchain

... verwendet **SHA-256** und **RIPEMD160** als Hashes

... **speichert** vor allem

***alle* bisher jemals erfolgten Überweisungen**

(jeder einzelne Block enthält
ein paar tausend Überweisungen)

Durch *Nachvollziehen aller bisherigen Überweisungen*
lässt sich berechnen,

***wie viele* noch nicht ausgegebene Bitcoins
*in jedem Wallet* liegen müssen**

# Das “Konsens-Problem” (1)

- Bitcoin wird *weltweit verteilt* gespeichert und berechnet
- Es gibt *keine zentrale Instanz*,
  *niemand ist Chef* oder hat das letzte Wort
- Die *Kommunikation* über das Internet
  ist *verzögert, unsicher und unzuverlässig*
- Im Bitcoin-Netz gibt es *auch Störer und Betrüger*

***Wer entscheidet,***
***wer den nächsten Block anhängen darf?***

***Wie einigt man sich weltweit***
***auf den Inhalt des nächsten Blockes?***

# Das “Konsens-Problem” (2)

Die Wissenschaft nennt das “**Konsens-Problem**”

*Eine hundertprozentige Lösung*
*ist theoretisch **unmöglich**!*

**Aber:**

Die Wissenschaft kennt einige
*sehr gute (und effiziente!) Verfahren*,
die in der Praxis so gut wie immer
ein *korrektes Ergebnis* liefern

# Das Mining-Idee (1)

Bitcoin hat die Wissenschaft *ignoriert*
und verwendet statt wissenschaftlichen Lösungen

***"Proof of Work":***
***Wer am fleißigsten arbeitet, darf anhängen!***

*Genauer: Wer ein* ***"kryptographisches Rätsel"***
***als Erster richtig löst****, darf anhängen*

**Aber:**

Das Rätsel ist ***nicht durch "Hirn" lösbar***,
sondern nur durch ***hirnloses Durchprobieren***
***von Trilliarden von Möglichkeiten***

# Die Mining-Idee (2)

- Wer *zuerst* die richtige Lösung findet

  ***ist reines Glück bzw. Zufall!***

- Wer *mehr Möglichkeiten pro Sekunde prüfen* kann

  ***hat höhere Chancen,***
  ***durch Glück der Erste zu sein!***

**==> Bitcoin ist ein Glücksspiel bzw. Wettrennen mit unfairer Ausgangslage**

(wer *mehr Geld in Hardware* investieren kann
bzw. *billigeren Strom* bekommt, hat höhere Chancen)

# Mining technisch (1)

Das *Ausprobieren vieler Möglichkeiten* nennt man

***"Mining"***

- *Ein paar Bits* in jedem Datenblock sind *frei wählbar* (d.h. sie enthalten keine *"nützlichen"* Daten)
- Für diese Bits *probiert man alle Möglichkeiten*
- *Für jede Möglichkeit* muss man den

***Hash des Blockes berechnen (aufwändig!)***

==> Das ergibt jedesmal einen
*anderen, nicht vorhersehbaren Hashwert*

# Mining technisch (2)

- Man betrachtet den Hashwert als *Zahl*
  (diese Zahl hat ungefähr 80 Stellen!)
- Vorgegeben ist eine *sehr viel **kleinere** Zahl*,

***das "Target"***

- *Gewonnen* hat, wer die freien Bits als Erster *so füllt*,

dass der *Hashwert des Blockes* zahlenmäßig
***kleiner als das Target ist***
(d.h. u.a. *viele führende Nullen* hat)

(die Wahrscheinlichkeit dafür ist *extrem gering*,
umso geringer, je kleiner die Target-Zahl ist)

# Mining-Kollisionen (1)

Problem gelöst? **Nein!**

Was passiert, wenn ***mehrere* Miner**
(*ohne* voneinander zu wissen)
***gleichzeitig* oder knapp nacheinander**
***verschiedene* Lösungen** finden,

d.h. ihren ***neuen Block***
an die Blockchain ***anhängen***?
(die Blockchain hätte dann *zwei Enden*)

# Mining-Kollisionen (2)

## "Weltweite Abstimmung mit den Füßen":

An welchem der beiden neuen Blöcke
*rechnen weltweit mehr Miner weiter*,
d.h. an welchem Ende kommen
***schneller neue Blöcke dazu***?

*Die längere, schneller wachsende Kette gewinnt!*

**Ungefähre Regel:** Es wird derjenige Block als *gültig* anerkannt,
an dem *zuerst 6 weitere Blöcke angehängt* werden.

Der *andere Block* incl. Nachfolge-Blöcken wird *ignoriert bzw. gelöscht*
(die *Überweisungen* im gelöschten Block *gelten nicht*).

# Die Rechenkraft-Attacke

Wer ***über 50 % der weltweiten Mining-Leistung*** kontrolliert, kann ***Bitcoin beliebig manipulieren***:

- Er setzt *weit vor dem aktuellen Ende* der Blockchain an (bei dem Block, ab dem er manipulieren will)
- ***ersetzt*** *diesen Block* durch einen Block *mit anderem Inhalt*
- und berechnet ab diesem Block eine *völlig neue Kette*

Da er *mehr Rechenleistung* als der Rest der Welt hat, wird er *die "echte" Kette in der Länge irgendwann überholen!*

Nach den Bitcoin-Regeln wird *die echte Kette damit ungültig* (alle darin enthaltenen Überweisungen gelten nicht mehr!!!) und *seine Kette gültig!*

# Warum Mining?

**Warum beteiligt man sich** an diesem **"Glücksspiel"?**
(und *zahlt viel Geld* für Spezialhardware, Strom, ...)

Wer als ***Erster*** einen Hash-Treffer findet, ***bekommt***

- Die ***Hashing-Belohnung***
  (derzeit **6,25 Btc = ~300.000 €** pro Block)

  Das sind "***neue***" **Bitcoins** *(aus dem Nichts frisch entstanden)*
- Die ***Überweisungs-Gebühren*** *aller Überweisungen*
  im neuen Block (schwankt stark: Derzeit in Summe 0,1 ... 2 Btc)

  Das sind *"schon vorhandene"* Bitcoins

# Bitcoin & Umwelt (1)

**Alle anderen bekommen *nichts*** und haben

*umsonst und **nutzlos gerechnet***
*und **viel Strom verbraucht**!*

Bei der Vorbereitung des Vortrages:

*Weltweit rund **600.000.000.000.000.000.000***
*Hash-Berechnungen **pro Sekunde***

und nur rund ***alle 10 Minuten "gewinnt" einer***!

# Bitcoin & Umwelt (2)

***Jährlicher Btc-Stromverbrauch: Über 100 TWh !!!***

***= Über 0,5 % des gesamten Welt-Energie-Bedarfs***
(in etwa der *gesamte Stromverbrauch von Holland*),

***= Rund 0,2 % des weltweiten CO2-Ausstoßes***

- Mehr als die Rechenzentren
von *Google, Microsoft & Amazon zusammen*
- Der Stromverbrauch pro Überweisung ist das
*Millionenfache* einer normalen Bank-Überweisung!
- Bei *deutschen Stromkosten* würde
*eine* Bitcoin-Überweisung *knapp 300 Euro* kosten!

# Bitcoin & Umwelt (3)

***"Geklauter Strom"*** für Bitcoin brachte wiederholt das *chinesische Stromnetz* zum *Zusammenbruch*

==> Mining ist in China jetzt generell ***verboten*** (hohe Gefängnis-Strafen!)

**Außerdem:**

Mining-Hardware beanspruchte zeitweise ***über 30 % der gesamten Produktionskapazität von TSMC*** (weltweit größter Halbleiter-Hersteller)!

# Die Entstehung neuer Bitcoins (1)

Die **Anzahl der Bitcoins** ist vom Design her ***endlich***:

- ***Neue*** Bitcoins können

  ***nur als Hashing-Belohnung entstehen!***

  ==> *Niemand* kann Bitcoins *nach Belieben erzeugen!*

- Die Hashing-Belohnung wird

  ***in regelmäßigen Abständen halbiert***

  ==> Die *Belohnung* geht asymptotisch gegen 0
  ==> Die *Anzahl der Bitcoins* geht
  gegen einen *fixen Grenzwert* (rund 21 Mio. Btc)

# Die Entstehung neuer Bitcoins (2)

**Ziel** der Beschränkung:

- ***Keine "Inflation"***

  Inflation war ja ursprünglich
  *"höhere Geldmenge bei gleicher Wirtschaftsleistung"*

- ***Wertsteigerung bestehender Bitcoins***
  durch die *"Gesetze des freien Marktes"*:

  Gleiche "Warenmenge" bei höherer Nachfrage
  *==> Preis bzw. Wert der "Ware" steigt!*

***Umgekehrt: Nachfrage sinkt ==> Wert sinkt!!!***

# Die Mining-Leistung

**Ziel** laut Bitcoin-Regeln:

***In etwa alle 10 Minuten ein neuer Block***

Dafür **2 Stellschrauben:**

- Das ***Target*** (die Grenze für einen erfolgreichen Hash)

  = die **Mining-Schwierigkeit**

- Die ***Überweisungs-Gebühr***

  = **Teil des Mining-Gewinns**

# Das Target

***Alle paar Tage wird das Target nach fixen Regeln neu festgelegt***

Wenn die Target-Schwierigkeit *sinkt*:

==> *Höhere Erfolgs-Wahrscheinlichkeit* beim Mining

==> *Weniger Hash-Versuche* bis zu einem Treffer

Zwei **Folgen:**

- Die *Block-Rate steigt* bei gleicher Mining-Leistung
- Der *Rechenaufwand für einen Gewinn* sinkt
  ==> *Finanzieller Anreiz* erhöht die *Mining-Leistung*

# Die Überweisungs-Gebühr (1)

- Der ***Überweisende*** legt fest,
  ***wie viel Überweisungs-Gebühr***
  er für seine Überweisung zahlt
- Der ***Miner*** wählt aus,
  ***welche Überweisungen***
  er in seinen Block aufnimmt

  ... und welche *nicht*
  (die müssen *noch länger warten*)

==> Die Überweisungs-Gebühren bilden sich
nach den *"Gesetzen des freien Marktes"*

# Die Überweisungs-Gebühr (2)

***Zu wenig Mining-Leistung***
bzw. zu viele Überweisungen:

**==> *Überweisungs-Rückstau, Wartezeit steigt***

==> Überweiser bieten ***mehr Überweisungs-Gebühr***

==> Das ***verbessert ihre Chancen, schnell***
in einen Block aufgenommen zu werden

**==> *Miner verdienen mehr*** an den Überweisungen

==> ***Finanzieller Anreiz*** zum Mining steigt

**==> *Mining-Leistung steigt***

# Bitcoin als Volks-Währung? (1)

- **Zu teuer!**

  ***Überweisungs-Gebühren viel höher*** *als am Konto*

  (durchschnittlich **3-15 € pro Überweisung**,
  zu Stoßzeiten viel höher)

  (werden **steigen**, sobald die Mining-Belohnung gegen 0 geht)

- **Zu langsam!**

  ***Mining-Rate rund 10 Minuten*** pro Block

  (es dauert **1 Stunde**, bis 6 Blöcke dahinter sind)

  (**Bank-Schnellüberweisung** geht in **unter 10 Sekunden**!)

# Bitcoin als Volks-Währung? (2)

- **Zu unzuverlässig!**

  *Jeder Miner kann **frei entscheiden,***
  ***welche Überweisungen** er in seinen Block nimmt*

  ==> **Keine Garantie**,
  **ob und wann** eine Überweisung drankommt!

- **Skaliert nicht** auf *"alle Überweisungen der Welt"!*
  - **Blockchain** wird **zu groß** (derzeit rund 500 GB)
  - Würde **viel zu viel Rechenleistung** brauchen (derzeit rund 300.000 Überweisungen pro Tag)

# *“The End”*

*Fragen?*