Fachhochschule Nordwestschweiz
Hochschule für Technik

Bitcoin …

… lasst es Erdbeeren spriessen

Über den Sprecher …

Name:	Martin Gwerder (martin.gwerder@fhnw.ch)
Anstellung:	Professur für Computersysteme an der FHNW
Arbeitet am:	Institut für Mobile und verteilte Systeme
Schwerpunkte:	Sicherheit und Cloud

BITCOIN RUSSLAND: ERDBEEREN DAS GANZE JAHR ÜBER DANK MINING FARMEN

REDAKTION - 21. FEBRUAR 2018 Teile:

Der russische Oblast (Verwaltungsbezirk) Kaliningrad überlegt, Krypto-Mining in großem Umfang zu organisieren. Als Begleiterscheinung der geplanten Mining Farmen wird Wärme erzeugt, die zur Produktion von Erdbeeren verwendet werden kann. Hinzu kommt, dass auch Leningrad industrielles Krypto-Mining in Betracht zieht.

Heute Abend …

- Ein paar Grundlagen
  - Die Verschlüsselungsarten…
  - Die elektronische Unterschrift
- Digitale Währungen und wie sie funktionieren
  - Die Sache mit dem Vertrauen…
  - Die Blockchain
  - Proof-of-… Häää?
  - Das „schürfen“ von digitalen Münzen
  - Intelligente Verträge?
- Was ist Bitcoin oder Ethereum für Normalsterbliche?

Eine Digitale Unterschrift? Einfach so?

Eine Digitale Unterschrift? Einfach so?

Hiermit bestätige ich, dass ich nichts bestätige.

Eine Digitale Unterschrift? Einfach so?

Mein Name ist Hase und ich weiss von nichts.

Eine Digitale Unterschrift? Einfach so?

Ich schulde jedem Anwesenden 1 Bitcoin.

Die «digitale Unterschrift»

- Bereits unsere «Normale Unterschrift» ist kopierbar
- Kopien im analogen/normalen Umfeld hinterlassen (im Idealfall) wahrnehmbare Spuren
- Wir können es nicht im digitalen Bereich gleich machen. Im digitalen Bereich sind Kopien nicht vom Original unterscheidbar.

Die Verschlüsselungsarten

- Symmetrisch
  - Verschlossen (verschlüsselt) mit einem Schlüssel
  - Umgekehrtes Verfahren und selber Schlüssel für die Entschlüsselung
- Asymmetrisch
  - Verschlossen (verschlüsselt) mit einem Schlüssel
  - Zweites Verfahren und anderer Schlüssel (der zum ersten passen muss) für die Entschlüsselung.
- Hashing
  - Vernichtet die Daten und macht einen Fingerabdruck dieser.

Das Hashing

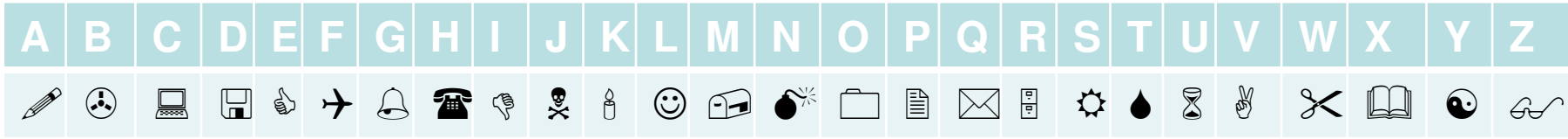
- Hashing erzeugt eine Prüfsumme eines grossen Dokumentes.
- Aus einem Hash kann das Dokument nicht wieder erstellt werden.
- Ein Hash ist typischerweise nur 8-128 Zeichen lang.

→ Ein Hash ist ein «Fingerabdruck» eines Dokumentes

Warnung!

Die folgenden Seiten enthalten Mathematik!!!

Symmetrische Verschlüsselung



- Verschlüsseln: Geheimschrift → 🔔👍☎👍👎📻☼💻☎🎛👎✈💧
- Entschlüsseln: 🔔👍☎👍👎📻☼💻☎🎛👎✈💧 → Geheimschrift

- In heutigen Computersystemen macht man es genau so, aber man fasst typischerweise 32 Zeichen zusammen und ersetzt sie mit anderen 32 Zeichen

  → Die Tabelle beinhaltet 2^{256}Kombinationen (das ist eine Eins mit 77 Nullen).

Asymmetrische Verschlüsselung

- Schlüssel: $Zahl^{Schlüssel\_1^{Schlüssel\_2}} = Zahl\ (mod\ n)$
- Verschlüsseln: $Text^{Schlüssel\_1}\ (mod\ n) = Verschlüsselter\_Text$
- Entschlüsseln: $Verschlüselter\_Text^{Schlüssel\_2}\ (mod\ n) = Text$
- Einfacher:
  - Alles was ich mit Schlüssel 1 verschlüssle, kann ich nur mit Schlüssel 2 entschlüsseln
  - Alles was ich mit Schlüssel 2 verschlüssle, kann ich nur mit Schlüssel 1 entschlüsseln

→ Wenn Sie es nicht (auf Anhieb) verstehen sind sie in guter Gesellschaft ☺. Mathematiker sind etwas seltsam. Oben steht der Beweis.

Wichtiges Prinzip der asymmetrischen Verschlüsselung

- Ein Schlüssel des Schlüsselpaares wird geheim gehalten
- Ein Schlüssel des Schlüsselpaares wird öffentlich gemacht

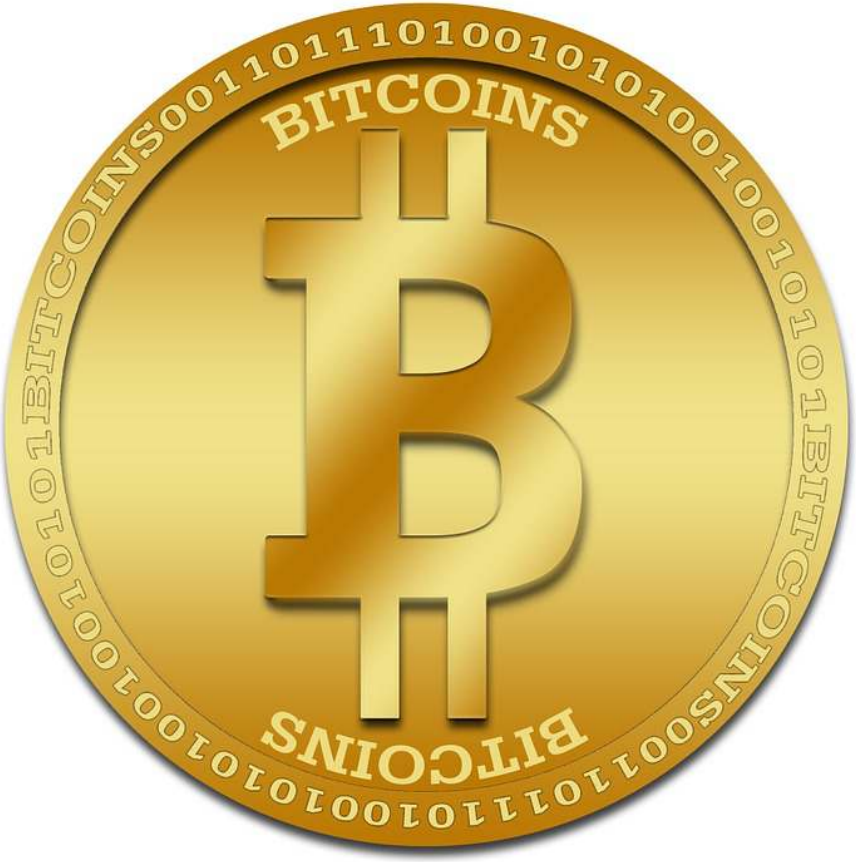
Und die «Digitale Unterschrift»?

- Ich nehme mein Dokument
- Ich berechne davon den Hash (Fingerabdruck)
- Ich Verschlüssle den Hash asymmetrisch mit meinem privaten Schlüssel → Das ist die «Digitale Unterschrift».

Überprüfen:

- Ich nehme das Dokument und berechne den Hash.
- Ich nehme die Unterschrift und entschlüssle sie mit dem öffentlichen Schlüssel. → Wenn jetzt der Hash entsteht heisst das, dass …
  - … das Dokument nicht verändert wurde (sonst hätte sich der Hash geändert)
  - … das derjenige, der das Dokument geschrieben hat, im Besitz des privaten Schlüssels war.

Der Bitcoin

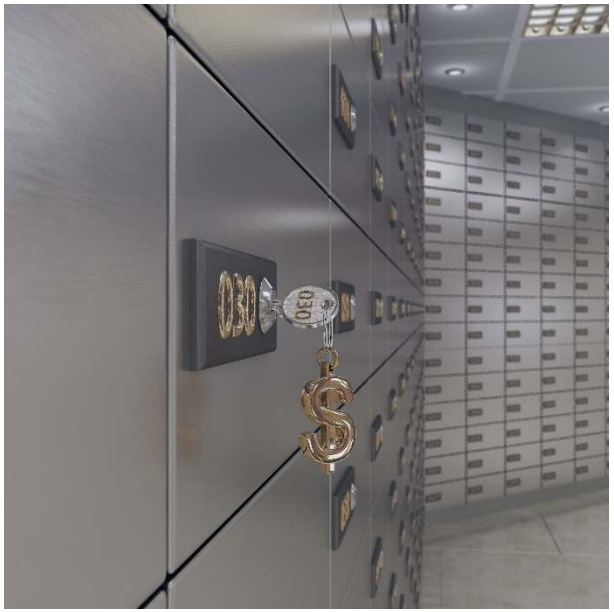


Bitcoin

- Bitcoin ist derzeit die digitale Währung mit dem grössten Handelsvolumen (ca. 60 Milliarden pro Tag)
- Erfunden durch einen Satoshi Nakamoto in 2009 (vermutlich ein Pseudonym)
- Es gibt zwei Sorten von Teilnehmern:
  - Diejenigen, die Zahlungen/Transaktionen machen. (Geld senden oder erhalten)
  - Diejenigen, die Zahlungen/ Transaktionen beglaubigen und neue Münzen in den Umlauf bringen
  - Bitcoin hat keine zentralen Server! Alle, die Transaktionen unterschreiben, sind ein Teil des Netzwerks. → Diesen Vorgang nennt man «Mining»

Was sind «Digitale Währungen»?

- Ein logisches «Etwas» von dem Leute glauben, sie können damit bezahlen.
- Zurzeit gibt es bereits hunderte von solchen «Digitalen Währungen» zu den Bekanntesten gehören:
  - Bitcoin (Volumen derzeit ca. 550K pro Tag)
  - Ethereum Ether (Volumen derzeit ca. 106K pro Tag)
  - LiteCoin (Volumen derzeit ca. 72K pro Tag)
  - Ethereum Classic (Volumen derzeit ca. 44K pro Tag)
  - EOS (Volumen derzeit ca. 38K pro Tag)
  - Bitcoin Cash (Volumen derzeit ca. 36K pro Tag)
  - Ripple (Volumen derzeit ca. 28K pro Tag)
- Coinhills listet derzeit ca. 2800 verschiedene Kryptowährungen
  - Die meisten davon sind aber sehr klein. Nur die Top 600 setzen mehr als ~10000 CHF pro Tag um. Die meisten davon schwanken stark in ihrem Wert.
  - In den letzten 52 Wochen schwankte der Kurs zwischen 900 und 20000 CHF für einen Bitcoin. Bei Ethereum war es zwischen 16 und 1250 CHF.
- Quellen: https://www.coinhills.com/market/volume/100-/ und https://www.finanzen.net/.

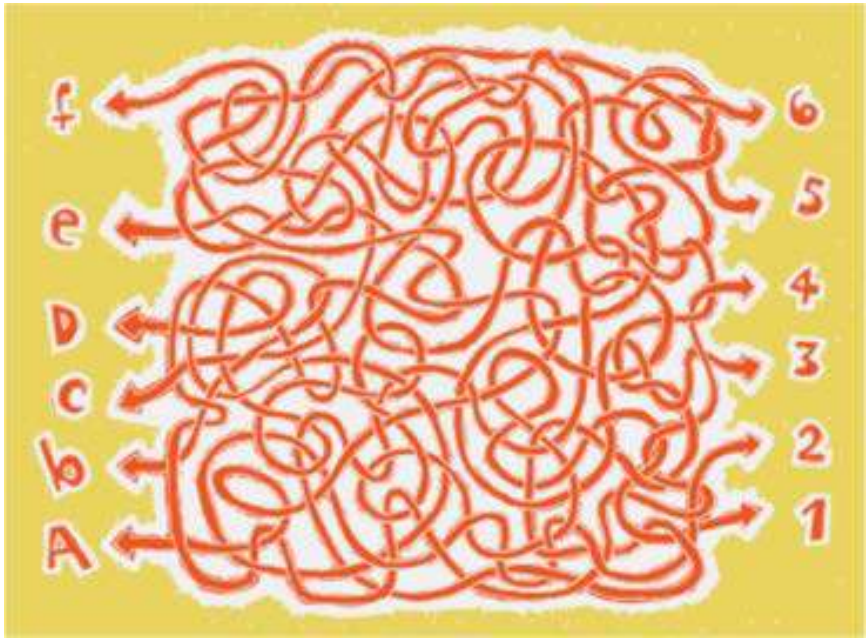


Was ist ein «Bitcoin Block»

- Inhalt
  - Vorgänger (Transaktionen und neue Währungen)
  - Transaktionen (Wer hat seit dem letzten Block an wen Geld bezahlt?)
  - Geld für den Block-Ersteller
    - Neues Geld (dieses Geld wird «geschürft»)
    - Transaktionskosten (Dieses Geld Zahlen die Personen, die Bitcoins überweisen möchten)
  - Kryptopuzzle oder Beweis (Proof-of-…)

Kryptopuzzles und Beweise

- Bitcoin oder Ethereum verwendet einen Proof-of-Work Algrithmus → Man muss ein schwieriges Kryptopuzzle lösen.
  - Das Problem kann
    - CPU-Hard sein (schwierig zu berechnen)
    - Memory-Hard (Viel Arbeitsspeicher Notwendig)
    - IO-Hard (Viele Interaktionen mit externen Speichern notwendig)
- Neu verwendet Ethereum (oder auch Peercoin und Blackcoin) einen Proof-of-Stake Algrithmus → Man muss beweisen, dass man bereits möglichst lange und viel Geld besessen hat.
- Es gibt auch:
  - Proof-of-Burn → Es muss Geld vernichtet werden um einen Block zu unterschreiben.
  - Proof-of-Importance → Eigentumsverhältnisse und ggw. Transaktionshöhe ist wichtig.
  - Proof-of-Stake-Velocity → Eigentum und Transaktions-Frequenz ist wichtig.



Cool … Ich will auch ein Block haben

- Im Durchschnitt werden alle 10 Minuten ein Block generiert.
- Zur erhält man die Transaktionsgebühren (klein) und 12.5 Bitcoin (ca. 120000 CHF)
- Jeder im Netzwerk hat (bei Bitcoin) die selbe Chance pro Rechenleistung einen Block zu finden.
- Es gibt unglaublich viel Rechenleistung im Netz

Consensus Algorithen … oder die Glarner Landsgemeinde

- Jeder kann «Blöcke» erzeugen.
- In einem «Block» werden Transaktionen zusammengefasst.
- Jeder «Block» hat einen vertrauenswerten Vorgänger (und auch dessen Ur-Ur-…-Ur-Enkeln wird vertraut). → Es entsteht eine Kette von Vertrauenswürdigen Blöcken. Das ist die Blockchain
- Jeder kennt die gültigen Regeln für einen «Block». Die Mehrheit wird nur gültige Blöcke akzeptieren.
- Weil jeder nur auf einem vertrauenswürdigen, neuen «Block» aufbaut gibt es mit der Zeit einen Konsens (Wie eine Abstimmung).

Von Ludovic Péron - Eigenes Werk, CC BY-SA 3.0,
https://commons.wikimedia.org/w/index.php?curid=32596829

Wie kann man Bitcoins «schürfen»

- Mit der CPU
  Unrentabel; Die Energie kostet mehr als der zu erwartende Gewinn; Leistung ca. 0.0000003-0.000003 TH/s; Energieeffizienz katastrophal
- Mit einer guten Grafikkarte
  Unrentabel; Leistung ca. 0.00003 TH/s (pro Grafikkarte) ; Energieeffizienz katastrophal
- Mit Spezialisierten USB-Sticks (FPGA oder ASIC basiert)
  möglicherweise knapp rentabel; Leistung 0.001-0.01 TH/s; Preis ca. 50-500 CHF
- Mit spezialisierten Computern
  möglicherweise knapp rentabel; Leistung 0.002-3 TH/s; Preis 300-22'000 CHF

- Netzwerkkapazität derzeit ca. 24'000'000 TH/s
- Wenn Sie eine 50% Chance haben möchten alle 10 Minuten 120'000 CHF zu verdienen (360'000 CHF/h) müssen sie die Hälfte der Rechenkapazität des Netzwerkes besitzen. Das würde 3.5 Miliarden CHF Investition kosten. Ausserdem würde es 2.4 Mio CHF Energie pro Stunde kosten → Bitcoin Mining rechnet sich also nur, wenn sie davon ausgehen, dass der Bitcoinkurs massiv steigt.
- Nebenbei bemerkt: Wer mehr als ~35% des Bitcoin Netzwerks besitzt, dem «gehört» Bitcoin. Das darf nie passieren!
- Derzeit wird mit einer Rendite von 4-14% bei hohem Verlustrisiko gerechnet.

Ist Bitcoins «schürfen Rentabel»?

- Netzwerkkapazität derzeit ca. 24’000’000 TH/s
- Wenn Sie (in der Schweiz) eine 50% Chance haben möchten alle 10 Minuten 120’000 CHF zu verdienen (360’000 CHF/h) müssen sie die Hälfte der Rechenkapazität des Netzwerkes besitzen. Das würde 3.5 Milliarden CHF Investition für Hardware voraussetzen. Ausserdem würde es 2.4 Millionen CHF Energie pro Stunde kosten → Bitcoin Mining rechnet sich in der Schweiz also nur, wenn sie davon ausgehen, dass der Bitcoinkurs massiv steigt.
- Nebenbei bemerkt: Wer mehr als ~35% des Bitcoin Netzwerks besitzt, dem «gehört» Bitcoin. Das darf nie passieren!
- Derzeit wird mit einer Rendite von 4-14% bei hohem Verlustrisiko gerechnet. Kurzfristige gewinne von 100% oder Verluste von 80% scheinen derzeit realisierbar.

Bitcoins und der Schwierigkeitsgrad des Kryptopuzzles

- Der Schwierigkeitsgrad des Puzzles wird vom «Netzwerk» (also allen zusammen) ebenfalls in der Blockchain berechnet. Dies geschieht alle 2016 Blocks.
- Er orientiert sich am Mittelwert der Leistung gemessen über die letzten 2016 Blöcke (wenn das Rätsel im Durchschnitt zu schwierig war, dann wird es leichter gemacht oder umgekehrt)

Intelligente Verträge

- Derzeit unterstützen nur wenige digitale Währungen «Intelligente Verträge».
  - Ethereum
  - Ripple

- Intelligente Verträge sind eigentlich kleine Programme. Sie Regeln, an wen und unter welchen Bedingungen Geld fliesst.

Ein Bitcoin Konto

- Ein Bitcoinkonto können sie selber erfinden. Es sind die Zahlen eines Asymmetrischen Schlüsselpaares.
- Der «öffentliche Schlüssel» ist die Kontonummer.
- Durch Unterschreiben mit dem «privaten Schlüssel» können wir Geld auf dem Konto ausgeben.

- Jeder kann alle Transaktionen der gesamten Blockchain einsehen → Die Kontonummer ist ein Pseudonym für Ihre Identität.

Ein Bitcoinkonto ist (k)ein Bankkonto

Die haben es nicht kapiert!

Warum kann man Bitcoin nicht verbieten oder regulieren?

- Bitcoin wurde «von Grund auf» entwickelt, dass dies nicht funktioniert
  - Wenn es drei oder mehr Menschen auf der Welt gibt, die Bitcoins «Minen» kann irgendwer Zahlungen auf das System machen.
  - Jeder, der Zahlungen macht besitzt die Komplette Blockchain auf seiner Festplatte
- Probleme der Regulierung:
  - Der Besitz der Blockchain könnte illegal sein (viel Spass beim suchen)
  - Der Besitz eines Bitcoin-Kontos könnte illegal sein (viel Spass beim suchen [ausser beim Tattoo])
  - Transaktionen in Bitcoins könnten illegal erklärt werden (auch hier viel Spass beim suchen [ausser beim Tattoo])

Mining-Risiken einmal etwas anders …

- In Island ist Energie sehr günstig.
- Kühlung ist auch einfach.
- Island ist ein Eldorado für Bitcoin-Miner
- Derzeit wurden 4 Rechenzentren «leergeklaut» (600 Rechner)
- Die Polizei hat keine Spur und sucht jetzt die Diebe über den Stromverbrauch

Bitcoin-Hochburg Island: Mining-Equipment im Millionenwert gestohlen

QUELLE: INNO3D

04.03.2018 um 19:45 Uhr **Eine Diebstahlserie der besonderen Art beschäftigt schon seit einigen Wochen die isländische Justiz. Es geht dabei um Mining-Equipment, das zusammengenommen knapp zwei Millionen US-Dollar wert ist. Nun sollen die Diebe über den Stromverbrauch ermittelt werden.**

Quelle: AP (https://apnews.com/55117fb55a714e909fb9aaf08841a5d6/Bitcoin-heist:-600-powerful-computers-stolen-in-Iceland)