Bitcoins

9.10.2015 – Goldschmiede

Jan Lühr, Ramon Waldherr

Inhalt

1. Was ist Bitcoin?
2. SHA-256
3. Sekp256k
4. Das Bitcoin Protokoll

Was ist Bitcoin?

- Elektronisches Zahlungsmittel
- Geschichte:
  - Bitcoin Paper (2008)
  - OpenSource Client (2009)
- Autor
  - Satoshi Nakamoto (satoshin@gmx.com)
  - Unbekannt / Pseudonym

Was ist Bitcoin? (2)

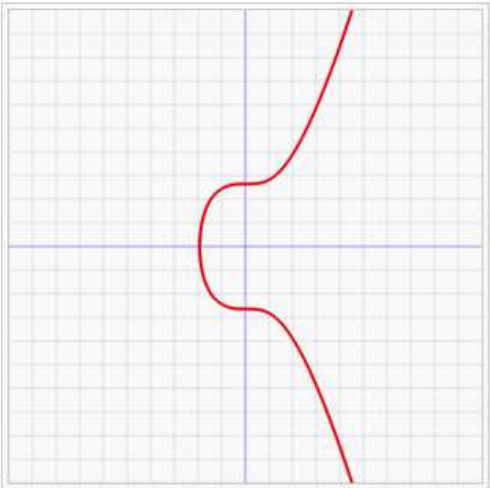
- Idee:
  - Zahlung via Digitaler Signaturen
  - Double-Spending via P2P erkennen
  - Keine Zentrale Kontrollinstanz

- Komponenten
  - Secp256k1
  - SHA-256
  - Bitcoin-Protokoll (Blockchains)

Secp256k1

secp256k1 refers to the parameters of the ECDSA curve used in Bitcoin, and is defined in *Standards for Efficient Cryptography (SEC)* (Certicom Research, http://www.secg.org/sec2-v2.pdf).

secp256k1 was almost never used before Bitcoin became popular, but it is now gaining in popularity due to its several nice properties. Most commonly-used curves have a random structure, but secp256k1 was constructed in a special non-random way which allows for especially efficient computation. As a result, it is often more than 30% faster than other curves if the implementation is sufficiently optimized. Also, unlike the popular NIST curves, secp256k1's constants were selected in a predictable way, which significantly reduces the possibility that the curve's creator inserted any sort of backdoor into the curve.



This is a graph of secp256k1's elliptic curve $y^2 = x^3 + 7$ over the real numbers. Note that because secp256k1 is actually defined over the field Z_p, its graph will in reality look like random scattered points, not anything like this.

Technical details

As excerpted from *Standards*:

The elliptic curve domain parameters over F_p associated with a Koblitz curve secp256k1 are specified by the sextuple T = (p,a,b,G,n,h) where the finite field F_p is defined by:

- p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F
- = $2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$

The curve E: $y^2 = x^3+ax+b$ over F_p is defined by:

- a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
- b = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007

The base point G in compressed form is:

- G = 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798

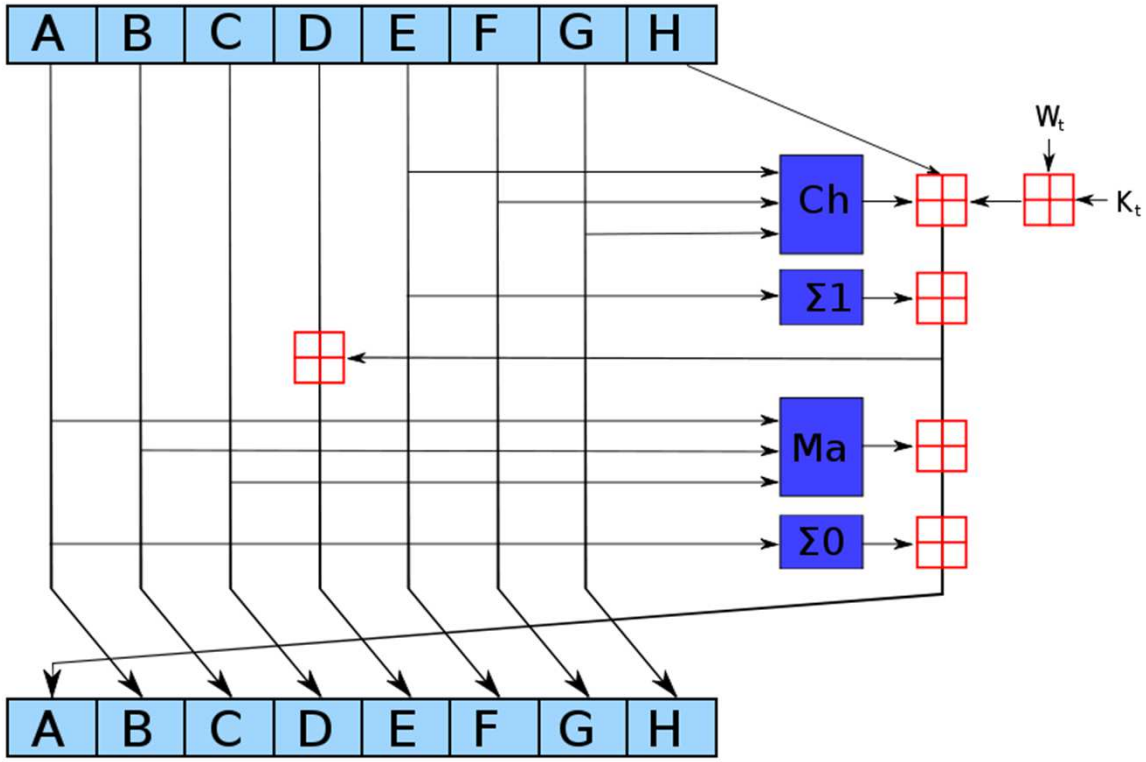
and in uncompressed form is:

- G = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

Finally the order n of G and the cofactor are:

- n = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141
- h = 01

SHA-2



SHA-2

General	
Designers	National Security Agency
First published	2001
Series	(SHA-0), SHA-1, SHA-2, SHA-3
Certification	FIPS PUB 180-4, CRYPTREC, NESSIE
Detail	
Digest sizes	224, 256, 384, or 512 bits
Structure	Merkle–Damgård construction
Rounds	64 or 80

Best public cryptanalysis

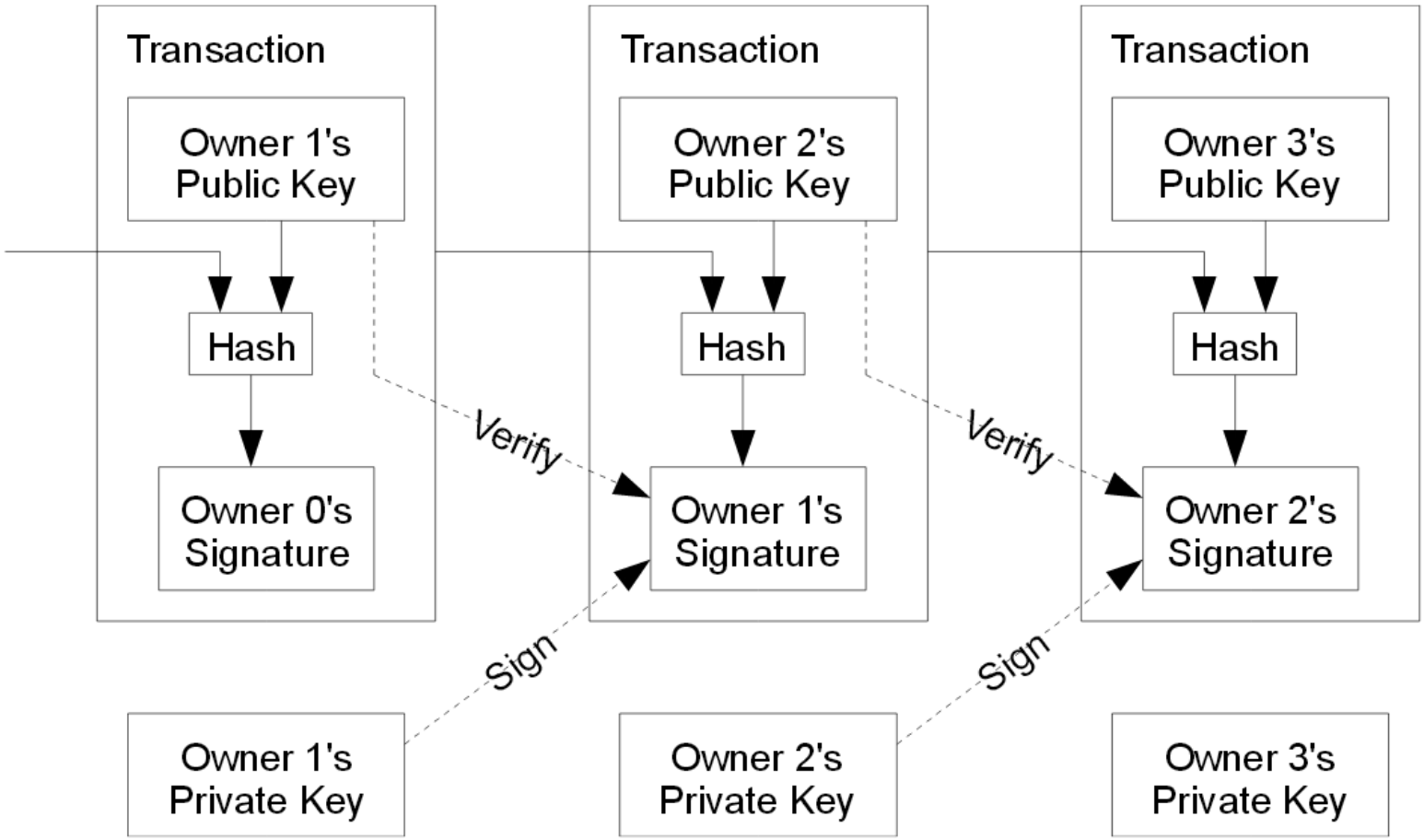
A 2011 attack breaks preimage resistance for 57 out of 80 rounds of SHA-512, and 52 out of 64 rounds for SHA-256.[1]

Pseudo-collision attack against up to 46 rounds of SHA-256.[2]

Quelle:Wikipedia

Das Bitcoin Protokoll

- Was ist eine Bitcoin?



Das Bitcoin-Protokoll(2)

- Die Blockchain