



Blockstream



Blockstream

RESEARCH

Was ist Bitcoin Kryptographie?

Jonas Nick
nickler.ninja

[@n1ckler](https://twitter.com/n1ckler)

2022-09-16

฿TC22



*Was benötigt wird, ist ein elektronisches
Zahlungssystem, das auf kryptografischem
Beweis statt auf Vertrauen basiert [...].*

- Satoshi





Blockstream RESEARCH

- Fokus: Kryptographie & formale Sprachen
 - d.h. wissenschaftliche Publikationen, Spezifikationen (BIPs), Entwicklung von Freier Software
 - für Bitcoin Protokoll, Wallets, Elements/Liquid Sidechain, Lightning Network, Federated E-cash, usw.
- blog.blockstream.com

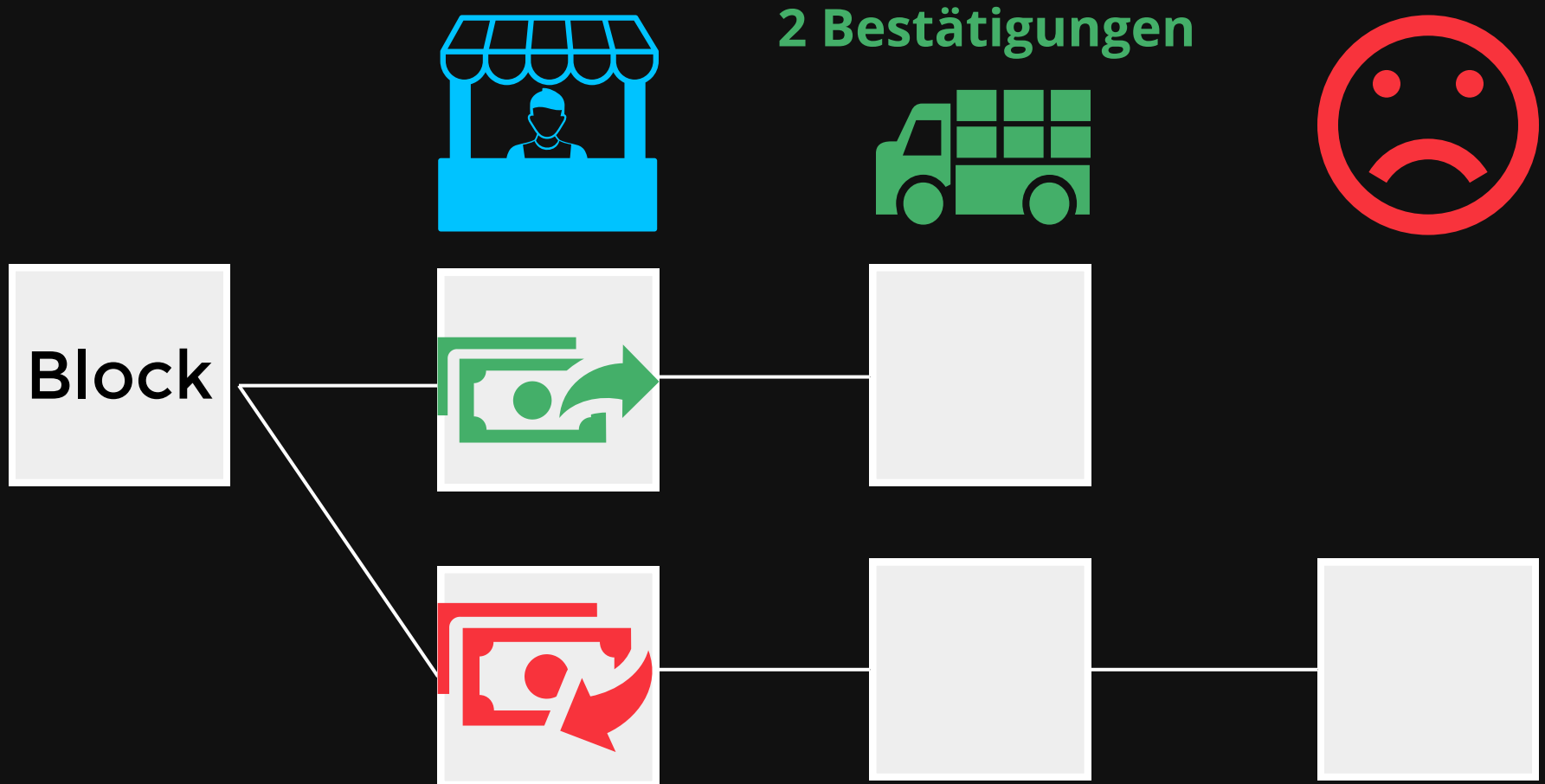
Warm Up

bitcoin_de.pdf

11. Berechnungen

Wir betrachten das Szenario eines Angreifers, der versucht, eine alternative Kette schneller als die ehrliche Kette zu erzeugen. Selbst wenn dies erreicht wird, wird das System nicht für beliebige

Double Spending



Wie viele Bestätigungen soll der Empfänger einer Transaktion abwarten?

Bei 99% Erfolgswahrscheinlichkeit und
20% Hashrate des Angreifers

	Antwort
Nakamoto	7
Rosenfeld	8



Unterschiedliche Modellierung des Angreifers

Ohne Verständnis des Modells ist das Ergebnis wertlos.

Beispielsweise ignoriert das Modell die Frage, ob ein
Angriff eine rationale Strategie ist.

Was ist Kryptographie?

*die Wissenschaftliche Untersuchung von
Verfahren zur Sicherung digitaler
Information, Transaktionen und verteilter
Berechnungen*

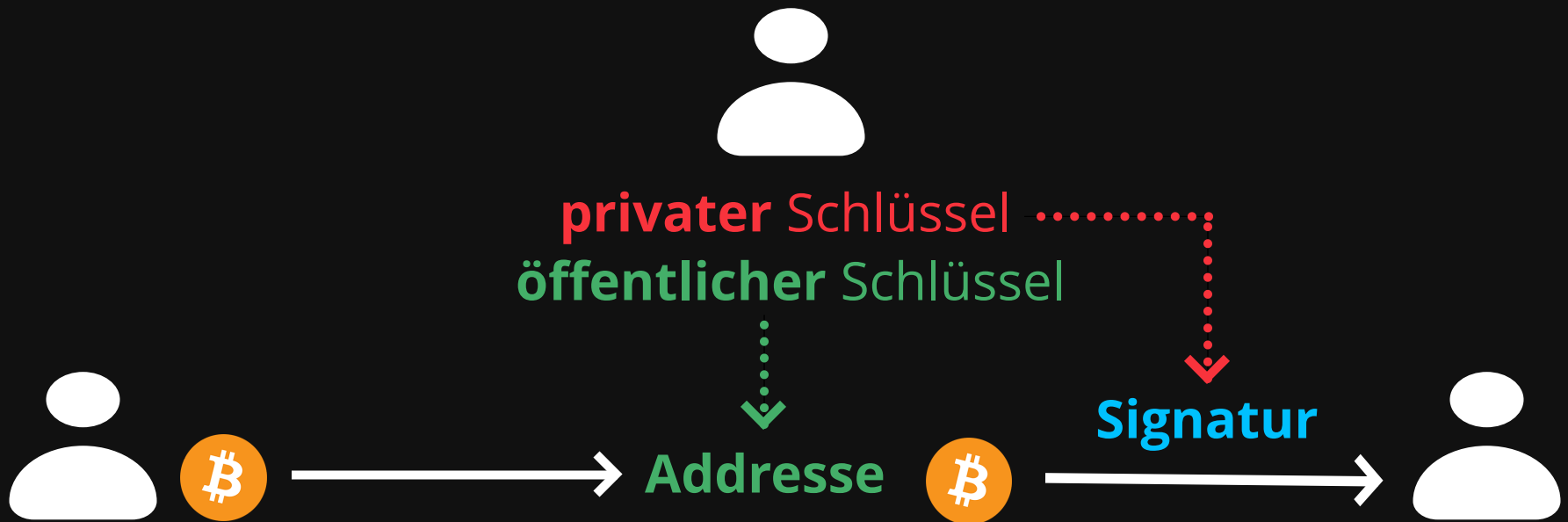
Aus: Introduction to Modern Cryptography, J. Katz, Y. Lindell



Zentrale Rolle spielen Definitionen,
Modelle, Annahmen & präzise
Sicherheitsbeweise

Was sind Signaturen?

In Bitcoin stellen digitale Signaturen sicher, dass nur der Besitzer den Coin ausgeben kann.



Sie bestehen aus drei Komponenten...

Was sind Signaturen?

Definition:

- KeyGen
 - Ausgabe: Schlüsselpaar aus privatem und öffentlichem Schlüssel
- Sign
 - Eingabe: privater Schlüssel und Nachricht
 - Ausgabe: Signatur
- Verify
 - Eingabe: öffentlicher Schlüssel, Nachricht, Signatur
 - Ausgabe: Ja oder Nein

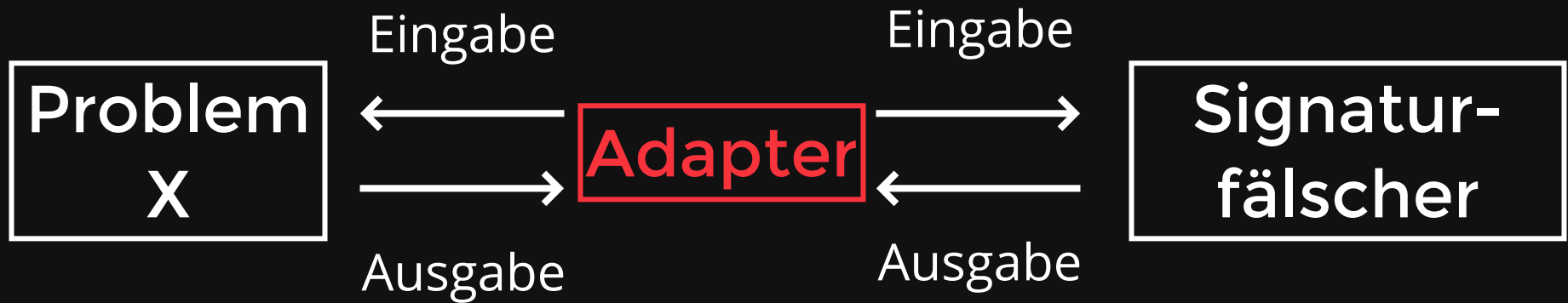
Fälschung: Erstellen einer Signatur für den öffentlichen Schlüssel einer anderen Person

Wann ist ein Signaturverfahren sicher?

Zu beweisen:

- ~~Es ist schwierig eine Signatur zu fälschen~~
- ~~Es dauert sehr, sehr lange eine Signatur zu fälschen~~
- Annahme: es gibt ein **Problem X**, das vermutlich sehr, sehr lange dauert zu lösen
 - Es ist mindestens so schwer eine Signatur zu fälschen wie Problem X zu lösen
 - Oder andersherum: Wenn Problem X schwer, dann ist das Signaturverfahren sicher

Der Sicherheitsbeweis



Gibt es einen Fälscher, so koennen wir Problem X lösen.

Kurz Verschnaufen...



Kein Beweis, Kein Problem?

- Beispiele:
 - **Problem X** gilt als schwer, weil keine effizienten Lösungsansätze bekannt
 - Hash Funktion **SHA-256** hat keinen kompletten Sicherheitsbeweis
 - Signatur-Verfahren **ECDSA** hat Sicherheitsbeweis, aber in ungewöhnlichem Modell
- Aber, neue Verfahren ohne Beweis: Skepsis!
 - Erste Versionen von **half-aggregation, discreet-log contracts, pay-to-contract** unsicher
 - **BIP 32** (HD-Wallets) komplizierter als nötig

Zurück zur echten Welt



Bsp.: "Sei $P \in \mathbb{G}$ " "Sei P eine Anordnung von 33 bytes" `unsigned char P[33];`

Spezifikation / Bitcoin Improvement Proposal (BIP):

- Von mathematischen Objekten zu Bits & Bytes
- Ziel: ermöglicht kompatible Implementationen
- Spezifikation der Spezifikationen: [BIP 2](#)
- Unklare Spezifikationen führen zu [Schwachstellen in Implementationen](#)
- In Zukunft idealerweise: [Formale Spezifikationen](#), die beweisbar korrekte implementationen ermöglichen

Zurück zur echten Welt



Bsp.: "Sei $P \in \mathbb{G}$ " "Sei P eine Anordnung von 33 bytes" `unsigned char P[33];`

Implementation:

- Soll natürlich korrekt sein
- Frei von Seitenkanälen, z.B Korrelation von privatem Schlüssel und Rechenzeit

CPU-BUG HERTZBLEED

Erstmals Seitenkanalangriff über CPU-Frequenzen gelungen

Die Frequenz von x86-CPUs hängt von den verarbeiteten Daten ab. Durch gezielte Taktänderungen lassen sich Seitenkanäle zum Ausleiten von Schlüsseln finden.



in Pocket speichern



merken



15. Juni 2022, 12:47 Uhr, Sebastian Grüner

**Was ist Bitcoin
Kryptographie?**

(Multiparty-)
Payment Channels

Sidechains

Federated
E-Cash

off-chain
("Layer 2")

optional, Settlement auf Base Layer

on-chain
(Base Layer)

muss jeder Bitcoin Knoten validieren,
Konsens



Kryptographie

Bitcoin Kryptographie



**Konsens ist
veränderlich**

Benötigt Konsens der Bitcoin community, daher

- etablierte Annahmen
- effizient
- "einfach" zu analysieren und implementieren



Kryptographie

Bitcoin Kryptographie

Layer 2 Kryptographie

Kryptographie, die

- auf Bitcoin Base Layer aufbaut
- dort aber nicht praktikabel wäre
- bessere Effizienz & Überwachungsresistenz ermöglicht
- z.B. Multisignaturen, Blinde Signaturen, Zero-Knowledge Beweise beinhaltet

Fallstudie: Post-Quanten Kryptographie

Für Quantencomputer ist Problem X theoretisch nicht schwer. In der Praxis aber fragwürdige Bedrohungslage.

Post-Quanten Krypto...

- ... benötigt neuartige Annahmen
- ... hat niedrige Effizienz
- ... hat teilweise hohe Komplexität

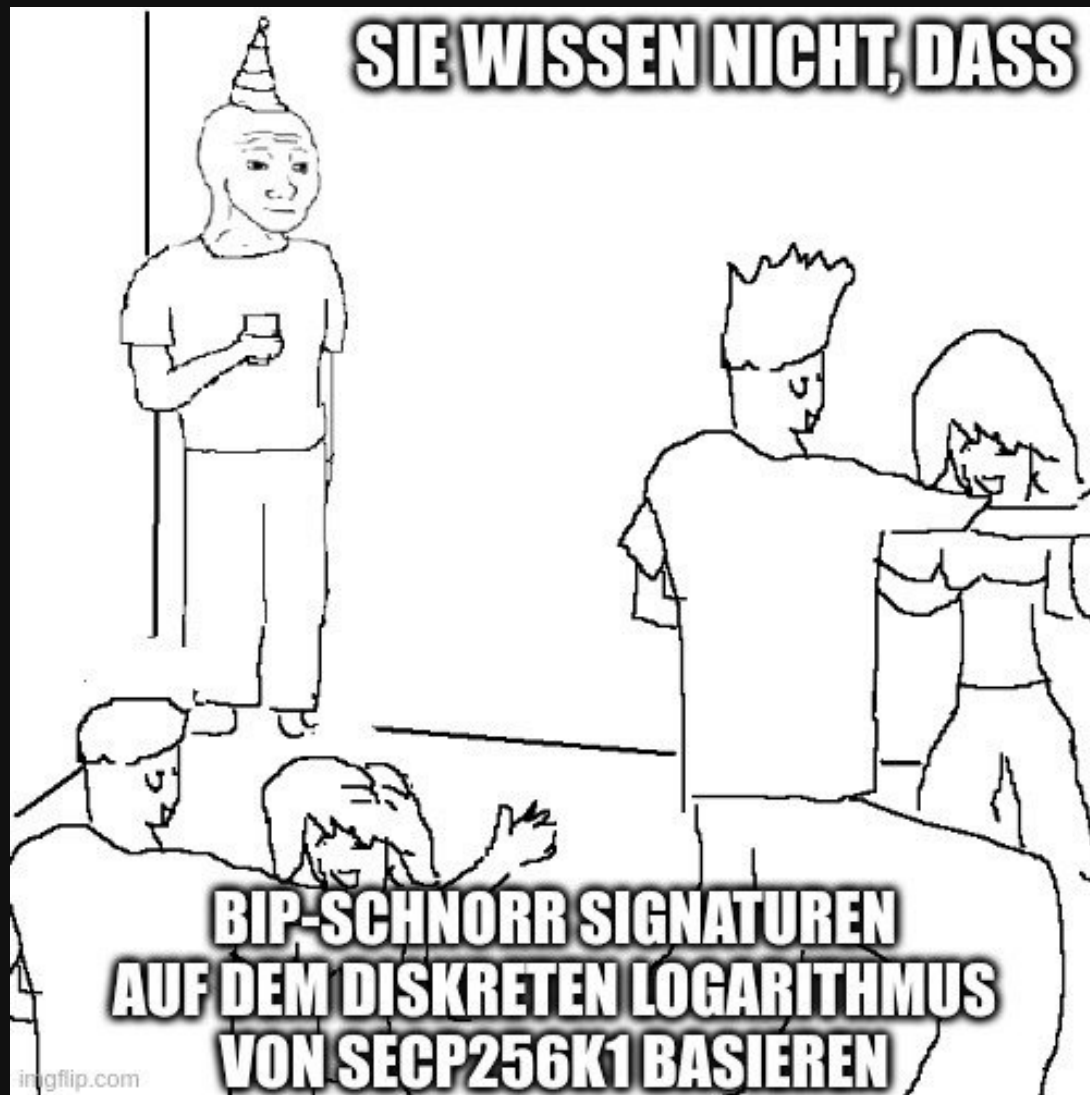
"Manche Leute scheinen nicht die Möglichkeit in Betracht zu ziehen, dass die NSA Post-Quanten Krypto sabotiert".

MAN KANN NICHT EINFACH

BITCOIN QUANTENSICHER MACHEN

Ausblick

- Bitcoin Kryptographie:
 - Weitere Fortschritte im Bereich Resilienz (z.B. Sicherheitsbeweise, bessere Spezifikationen, sicherer Code)
 - Selbst mit Beschränkung auf heutige Annahmen sind signifikante Verbesserungen des Bitcoin Protokolls möglich
 - Was als sicher gilt, ändert sich im Lauf der Zeit und damit auch was konsensfähig ist. Bitcoin Kryptographie
- Layer 2 Kryptographie:
 - Weites Feld mit vielen offenen Fragen für Theorie & Praxis



Folien auf nickler.ninja/slides