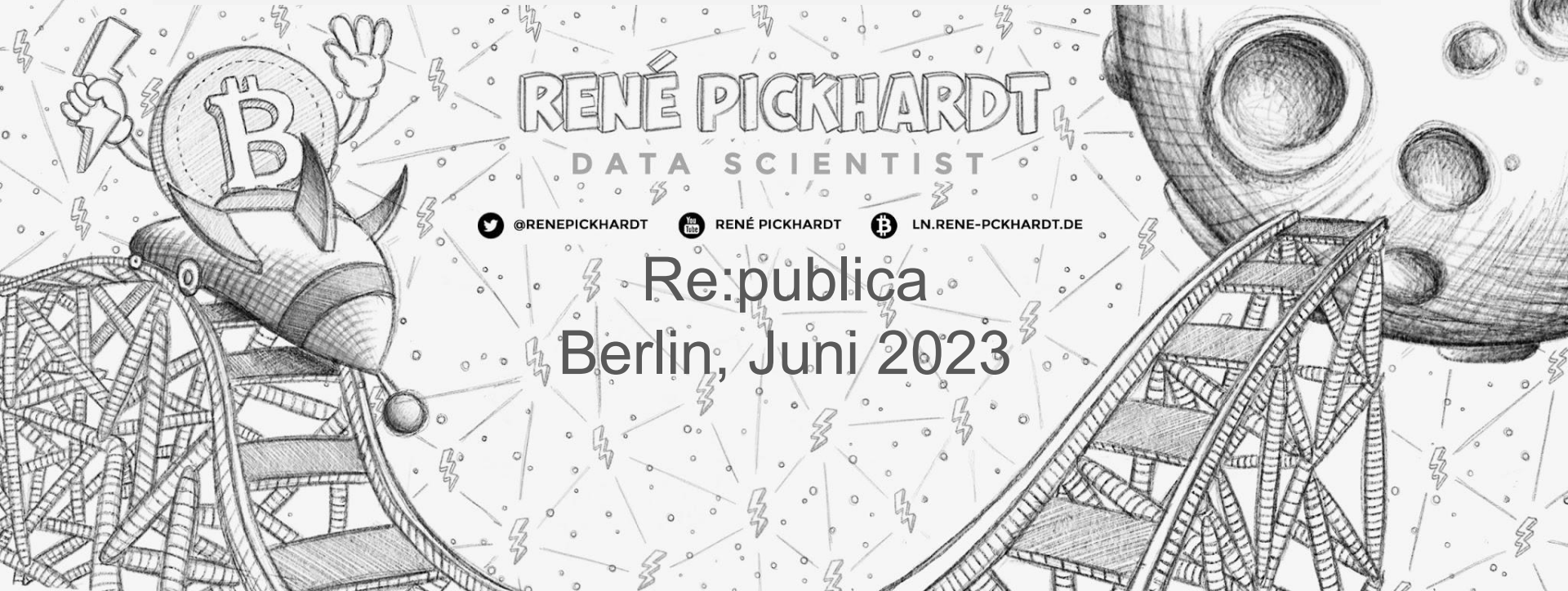
Don't trust, verify! Kann der Bitcoin seine Versprechen - aus Sicht eines Open Source Developers - einhalten?



Re:publica

Berlin, Juni 2023

Disclaimer

Nach 5 Jahren als Open Source Entwickler ist dieser Vortrag mein **subjektiver** Eindruck über den Status Quo, sowie Probleme und Herausforderungen mit dem Governance Modell von Bitcoin.

Es besteht keinerlei Anspruch auf Vollständigkeit oder Korrektheit. Der Vortrag spiegelt lediglich nach bestem Wissen und Gewissen mein aktuelles Verständnis über das Bitcoin Projekt.

Die Ankündigung des Vortrags lässt sich unter folgender URL finden:
https://re-publica.com/de/session/dont-trust-verify-kann-der-bitcoin-seine-versprechen-aus-sicht-eines-open-source

Motivation für den Talk

Rene Pickhardt
@renepickhardt

I am considering becoming more vocal criticizing #bitcoin ₿ and the #LightningNetwork ...

As a researcher I find sound and substatial criticism extremely important.

Unfortnunatly most critics do (even if they underdtand the fundamentals of the technology) a terrible job... 1/2

Tweet übersetzen

9:10 vorm. · 11. Juni 2022

Tweet-Statistiken anzeigen

57 Retweets **11** Zitate **982** „Gefällt mir"-Angaben **41** Lesezeichen

Motivation für den Talk

Rene Pickhardt
@renepickhardt

I am considering becoming more vocal criticizing #bitcoin and the #LightningNetwork ...

As a researcher I find sound and substatial criticism extremely important.

Unfortnunatly most critics do (even if they underdtand the fundamentals of the technology) a terrible job... 1/2

Tweet übersetzen

9:10 vorm. · 11. Juni 2022

Tweet-Statistiken anzeigen

57 Retweets **11** Zitate **982** „Gefällt mir"-Angaben **41** Lesezeichen

Rene Pickhardt
@renepickhardt

Most #bitcoin critics (that I'm aware of) focus on already debunked / fixed or minor problems, make use of adhominem arguments or whataboutism. By useing strong language & conflicting #bitcoin with the actual #cryptobros they seem to be focused on narrative instead of debate 2/2

Tweet übersetzen

9:10 vorm. · 11. Juni 2022

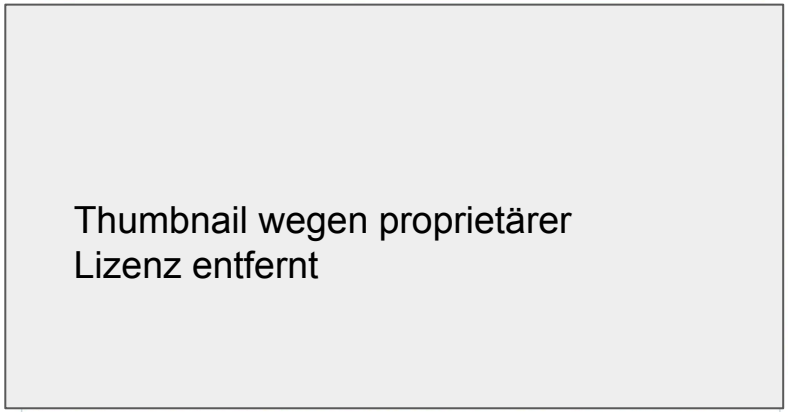
Tweet-Statistiken anzeigen

9 Retweets **3** Zitate **416** „Gefällt mir"-Angaben **3** Lesezeichen

Versuch den Diskurs zu führen

Spektrum @spektrum · 17. Okt. 2022

Kaum ein Thema spaltet so sehr wie der Bitcoin, doch ein ausgewogener Diskurs fehlt. Leider liegt auch @maithi_nk bei ihrer ZDF-Sendung zu dem Thema manchmal daneben, erklärt der Bitcoin-Entwickler @renepickhardt.



spektrum.de

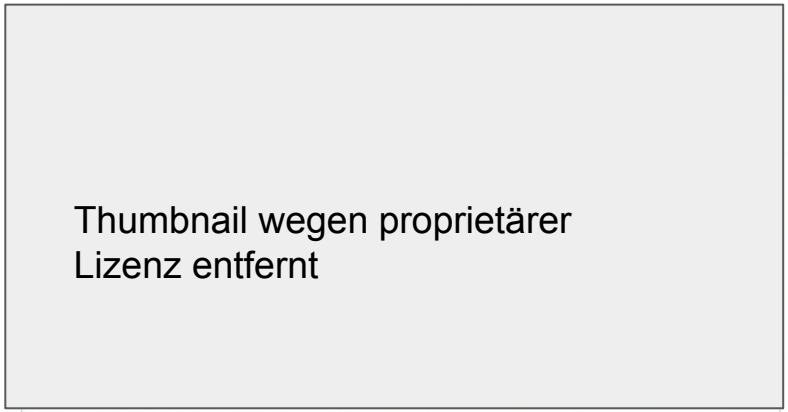
Kryptowährung: Eine freie Menschheit braucht den Bitcoin

Kaum ein Thema spaltet so sehr wie Bitcoin, doch ein ausgewogener Diskurs fehlt. Ein Gastbeitrag

FIfF macht bei den Ad Hominem Attacken mit

Spektrum @spektrum · 17. Okt. 2022

Kaum ein Thema spaltet so sehr wie der Bitcoin, doch ein ausgewogener Diskurs fehlt. Leider liegt auch @maithi_nk bei ihrer ZDF-Sendung zu dem Thema manchmal daneben, erklärt der Bitcoin-Entwickler @renepickhardt.



spektrum.de

Kryptowährung: Eine freie Menschheit braucht den Bitcoin

Kaum ein Thema spaltet so sehr wie Bitcoin, doch ein ausgewogener Diskurs fehlt. Ein Gastbeitrag

Einige Accounts, denen du folgst, markieren diese*n Tweeter*in oft mit „Gefällt mir“

Forum Informatik f. Frieden & ges. Verantwortung
@FIfF_de

So eine unsinnige Aussage. Wir wollen doch keine „ausgewogene Diskussion“ zwischen Runderde, Hohlerde und Flacherde?

Schaut mal hier fahrplan22.bits-und-baeume.org/bitsundbaeume/... und versteht, warum Euer Autor #Gesellschaft überhaupt nicht versteht und zudem einem gefährlichen Kult anhängt.

fahrplan22.bits-und-baeume.org

Die Nicht-Nachhaltigkeit von Blockchain & Web3 Bits & B...

Sie wird gefeiert als revolutionäre neue Technik, die die Wirtschaft und Gesellschaft umkrempeln wird so wie ...

10:54 nachm. · 17. Okt. 2022

1 Zitat **4** „Gefällt mir“-Angaben

Ziele des Vortrags

1. Brücken bauen für eine zukünftig sachlichere Debatte
    a. Ja, ich bin Bitcoin Entwickler / Wissenschaftler und ja, ich finde Bitcoin durchaus gut
    b. Ich bin ein ganz gewöhnlicher Mathematiker mit Interesse an gesellschaftlichen Themen
        i. 6 Jahre Institut für Web Science and Technologies (Master Web Science mit entwickelt)
        ii. Spitzenkandidat der Piratenpartei 2017
        iii. Aktivist für freies Wissen
        iv. Ausbau Gewaltschutz-Programme für männliche Opfer häuslicher Gewalt
2. Exemplarisch Probleme aufzeigen, die ich im Bezug auf Bitcoin relevant finde
    a. Keinen Anspruch auf Vollständigkeit
    b. Ggf. sind meine Prioritäten durch Betriebsblindheit und "Innensicht" verschoben
    c. Habe nur noch 25 Minuten, deswegen
        i. bleibt der Fokus heute bei Problemen
        ii. Auslassen hinreichend bekannter Kritik (z.B. Energieverbrauch)

Verbreitete Erzählungen & Versprechen über Bitcoin

1. Bitcoin sei dezentral und niemand könne das System kontrollieren
2. Bitcoin sei unveränderbar
3. Es gäbe nur 21 Millionen Münzen - Bitcoin sei ein rares Gut.
4. Bitcoin funktioniere ohne Vertrauen
5. Menschen seien souverän in der Lage ihre eigenen Coins zu verwalten

Ausgelassen mangels Zeit:

Frage, ob das Lightning Netzwerk global p2p Bitcoin Zahlungen skalieren kann?

Bitcoin P2P e-cash paper

Satoshi Nakamoto satoshi at vistomail.com
Fri Oct 31 14:10:00 EDT 2008

- Previous message: Fw: SHA-3 lounge
- **Messages sorted by:** [date] [thread] [subject] [author]

```
I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the
    network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract.  A purely peer-to-peer version of electronic cash would
```

https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

Wie dezentral ist Bitcoin tatsächlich?

- Rollen im Bitcoin Netzwerk
  - Bitcoin Miner
  - Bitcoin Developer
  - Bitcoin Nodes
  - Bitcoin Service Provider
  - Verbraucherinnen und Verbraucher

- Was haben alle gemeinsam?
  - Sprechen das gleiche Protokoll
    - D.h. sie haben **Konsens** über das Protokoll

Was passiert, wenn der Konsens verloren geht?

- Fork / Chain split
- 2017 entstanden wegen Uneinigkeit über notwendige (?) Protokolländerungen mehrer Forks
- Welche Version ist dann der echte / eigentliche Bitcoin?
- Wer entscheidet das eigentlich auf welche Art und Weise?

Wodurch entsteht der Konsens über das Protokoll?

- Erwartungsgemäß entsteht **technischer Konsens** durch eine Spezifikation
- Bitcoin Core gilt als die Referenzimplementierung und die Spec
  - Satoshis initialer Vorschlag auf Kritik zum Whitepaper
    - https://www.metzdowd.com/pipermail/cryptography/2008-November/014858.html
  - Vermutlich historischer Kontext: Weiterentwicklung von Satoshis Implementierung
  - Philosophie: Code is the Law
- Wer entscheidet, warum ausgerechnet Bitcoin Core das Protokoll definiert?
  - Darüber gibt es bis zum Konflikt ein auf **Meritokratie** basierenden **sozialen Konsens**
- Ist Meritokratie das beste Governance Model?

Implikation für die (Weiter-) Entwicklung von Bitcoin Core

- Hohe Verantwortung?
- Authorative Funktion?
- Entscheidungshoheit?
- Deutungshoheit?

Beispiel: Inflations-Bugfix im Jahr 2018

- Bitcoin Core Versionen 0.15.X, 0.16.0, 0.16.1 and 0.16.2 betroffen
- Miner waren technisch in der Lage den Wert doppelt ausgegebener Münzen für sich zu beanspruchen
  a. Erinnerung: Bitcoin hatte das Double Spend Problem gelöst
  b. Konsequenz: Geldmenge könnte - wenn Miner das nutzen - beliebig wachsen
- In anderen Worten:
  a. In diesem Zeitfenster war Bitcoin technisch nicht auf 21 Mio Münzen begrenzt
     i. Jedoch war dieser Bug (Feature?) unbemerkt und wurde nicht ausgenutzt
     ii. Daher zunächst praktisch kein Problem
  b. Zurückändern auf das 21 Mio Münzen Limit bedürfte einer (**technischen**) Konsensänderung
- Änderung der technischen Konsensregeln braucht Software Update
  a. In einem dezentralen Peer 2 Peer Netzwerk ohne auto update, alert keys, zentrale Autorität

  → Viel Erfolg

How to P2P Konsensänderung in Windeseile

Timeline for September 17, 2018: (all times UTC)

- 14:57 anonymous reporter reports crash bug to: Pieter Wuille, Greg Maxwell, Wladimir Van Der Laan of Bitcoin Core, deadalnix of Bitcoin ABC, and sickpig of Bitcoin Unlimited.
- 15:15 Greg Maxwell shares the original report with Cory Fields, Suhas Daftuar, Alex Morcos and Matt Corallo
- 17:47 Matt Corallo identifies inflation bug
- 19:15 Matt Corallo first tries to reach slushpool CEO to have a line of communication open to apply a patch quickly
- 19:29 Greg Maxwell timestamps the hash of a test-case which demonstrates the inflation vulnerability (a47344b7dceddff6c6cc1c7e97f1588d99e6dba706011b6ccc2e615b88fe4350)
- 20:15 John Newbery and James O'Beirne are informed of the vulnerability so they can assist in alerting companies to a pending patch for a DoS vulnerability
- 20:30 Matt Corallo speaks with slushpool CTO and CEO and shares patch with disclosure of the Denial of Service
- 20:48 slushpool confirmed upgraded
- 21:08 Alert was sent to Bitcoin ABC that a patch will be posted publicly by 22:00
- 21:30 (approx) Responded to original reporter with an acknowledgment
- 21:57 Bitcoin Core PR 14247 published with patch and test demonstrating the Denial of Service bug
- 21:58 Bitcoin ABC publishes their patch
- 22:07 Advisory email with link to Bitcoin Core PR and patch goes out to Optech members, among others
- 23:21 Bitcoin Core version 0.17.0rc4 tagged

September 18, 2018:

- 00:24 Bitcoin Core version 0.16.3 tagged
- 20:44 Bitcoin Core release binaries and release announcements were available
- 21:47 Bitcointalk and reddit have public banners urging people to upgrade

September 19, 2018:

- 14:06 The mailing list distributes an additional message urging people to upgrade by Pieter Wuille

Quelle: https://bitcoincore.org/en/2018/09/20/notice/

TL;DR: How to P2P Konsensänderung in Windeseile

- Habe hohe Expertise
- Sei gut vernetzt
- Verstecke es in dem Bugfix einer DoS Attacke
- Kommuniziere mit den größten Service Providern / Minern
- Verwendung von open source software, so dass dein Handeln geprüft werden kann
- Vor allem aber:
  a. Vertrauen
  b. Sozialer Konsens
  c. Agiere in Good Faith
  d. Check and balance

Wie unveränderbar ist Bitcoin?

- Wir haben gesehen, dass **technische** Konsensänderungen möglich sind
  - https://bitcoincore.org/en/2018/09/20/notice/

  - Ähnliches Beispiel aus 2010:
    i. https://en.bitcoin.it/wiki/Value_overflow_incident
  - Integer Overflow Bug für timestamps im Block Header wird kommen
    i. https://en.bitcoin.it/wiki/Block_timestamp
    ii. https://en.wikipedia.org/wiki/Year_2038_problem

- Interessanter: Wie lässt sich **sozialer** Konsens verändern?
  - Populismus
  - Gezielte PR
  - Social Engineering

Gibt es tatsächlich nur 21 Millionen Bitcoin?

- Unklar, weil unbekannte Bugs oder 0-day Attacken existieren könnten
  - Aber: Metakonsens, solche Bugs würden wohl schnell Konsens für ein Update finden
  - Allerdings: What happened to "Code is the law"?
- Protokoll-Veränderungen werden durchaus vorgeschlagen
  - Tail emission für Bitcoin: Unendliche Ausgabe von Coins, um Miner zu vergüten
    - https://petertodd.org/2022/surprisingly-tail-emission-is-not-inflationary
- Was ist mit Paper Bitcoins?
  - Service Provider halten Bitcoins für fremde Menschen
  - Möglichkeit zum Fractional Reserve Banking
    - Service Provider gehen immer wieder Pleite (Mt. Gox, FTX,...)
  - Bankrun ermöglicht Menschen zwar ihre Coins zu holen
    - Wer zu spät kommt hat Pech (Not your Keys, Not your Coins)
    - Block Confirmation times lassen Bankrun in Zeitlupe ablaufen

Klappt Bitcoin ohne Vertrauen & souveräne Teilnahme?

- Theoretisch ja
  - Praktisch nur für eine kleiner Gruppe von Menschen mit Spezialwissen
- Andernfalls vertrauen Menschen in vielen Fällen z.B:
  - Entwicklerinnen und Entwicklern
  - Software
  - Hardware (Wallet) Hersteller
  - Server Hosting Services
  - Möglicherweise Bitcoin / Lightning Service Provider

https://bitcoinblog.de/2019/07/01/prinzipiell-basiert-bitcoin-halt-doch-auf-vertrauen/

Aber Rene, mit all den Problemen: Warum doch Bitcoin?

- Ich finde Netzneutralität wichtig
  - Ähnlich erscheint mir ein neutrales Geldsystem erstrebenswert

- Technisch ist mir kein stärkerer Eigentumstitle als Digitale Signaturen bekannt

- Einige Beispiele für die Nützlichkeit von Bitcoin
  - Edward Snowden kaufte Server-Infrastruktur für NSA Leaks mit Bitcoin
    - https://www.youtube.com/clip/Ugkxw7DGoz1iE2KxhFAPHy_YAMk99Qd1c0-R
  - Julian Assange & Wikileaks
    - https://www.coindesk.com/markets/2014/09/16/assange-bitcoin-and-wikileaks-helped-keep-each-other-alive/
  - Ukraine Krieg:
    - https://www.tagesschau.de/wirtschaft/finanzen/kryptowaehrungen-ukrainekrieg-101.html

Ein Paar Gedanken zum Schluss

- Hey Gesellschaftswissenschaftler*innen, ist die **Interaktion** von **sozialem** mit **technischem** Konsens nicht etwas, das erforschenswert ist?
- Warum wird in der Re:publica Bubble Bitcoin eigentlich eher stark abgelehnt?
  a. Kommt gerne auf mich zu und erklärt es mir, ich verstehe es nämlich nicht
- Mich nervt dieses ganze gehype und overselling von Bitcoin auch total
  a. Natürlich gibt es offene Fragen und Probleme
     i. In der Realität sind die auch ganz schön kompliziert
     ii. Wir Open Source Devs stellen uns denen auch so gut wie wir das können
- Allerdings läuft und funktioniert Bitcoin seit über einem Jahrzehnt
  a. Wir werden den Bitcoin wohl kaum stoppen bzw. beenden können
  b. Daher bitte mehr Debatte, was wir mit Bitcoin machen und wie wir damit umgehen wollen
     i. Insbesondere glaube ich, dass gute Regulation nur durch guten Diskurs möglich ist

Hörtipp: Die Debatte mit Mai Thi ging weiter

https://www.youtube.com/watch?v=L-T8NoCBe5k&pp

Vielen Dank für Euer Interesse an dem Thema

- https://ln.rene-pickhardt.de
- Github & Twitter: @renepickhardt
- Ich freue mich auf respektvollen Diskurs
- Danke an Christoph Floßmann für hilfreiche Diskussionen & Feedback