Bitcoin Zeitreise

Von den Cypherpunks bis zum Lightning Network

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Bitcoin ist ein bargeldähnliches elektronisches Zahlungssystem

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

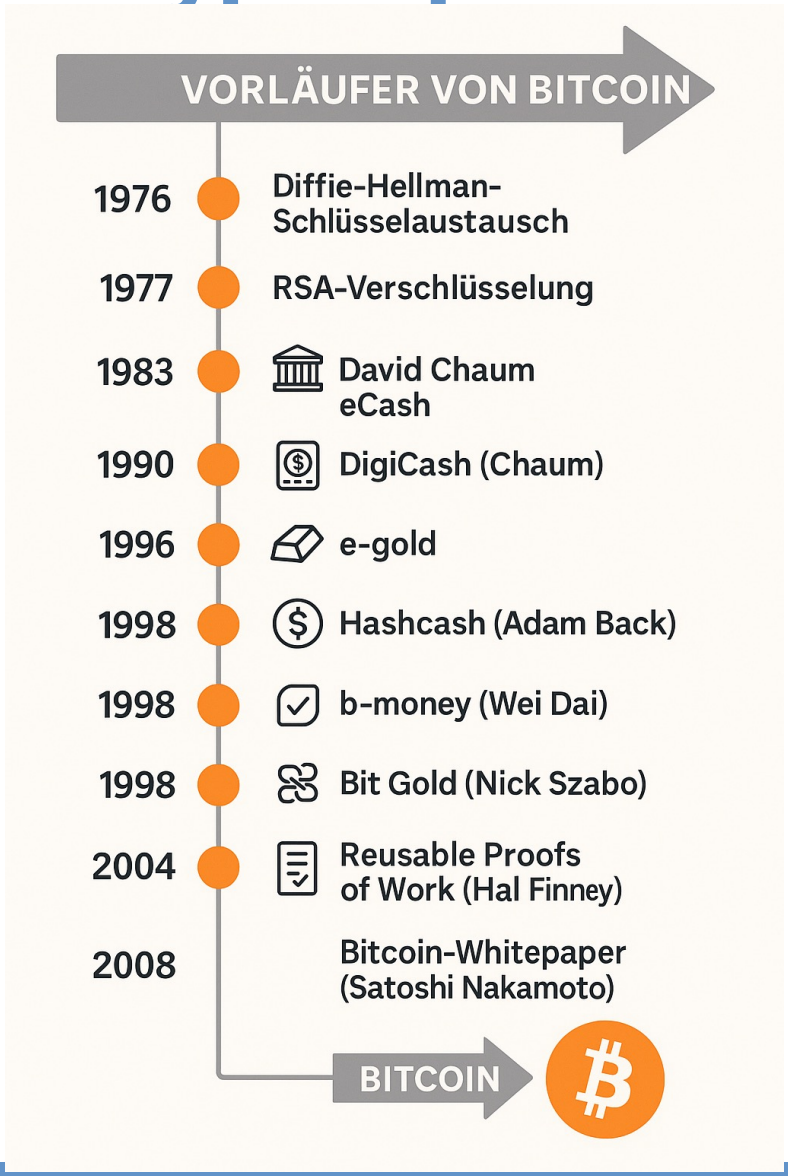
Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

- Payment: 12x
- Transaction(s): über 60x
- Store of Value oder Spekulation wird nirgendwo erwähnt

1980er-1990er: Cypherpunk & Vorläufer

Cypherpunk – Digitales Zahlungsmittel

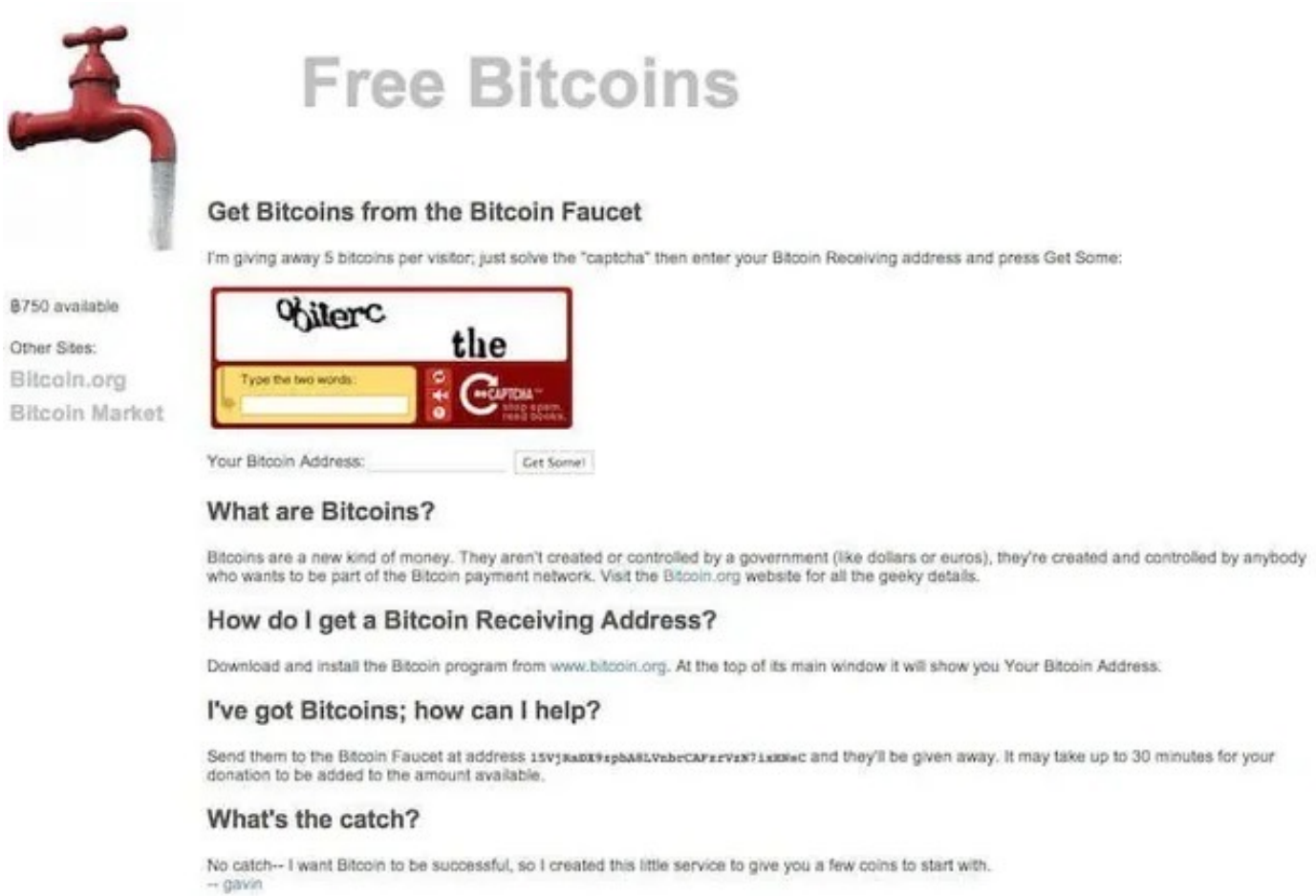


- ohne Staat und Banken
- Privatsphäre und Anonymität
- Freiheit und Zensurresistent
- Dezentral

2010:
Erste Anwendungen

Juni 2010 – Bitcoin Faucet

5 Bitcoin for Free



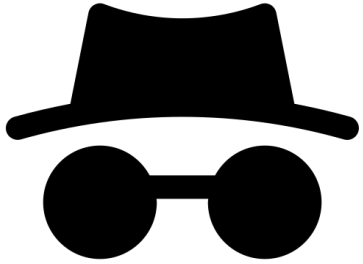
22. Mai 2010 – Pizza Day

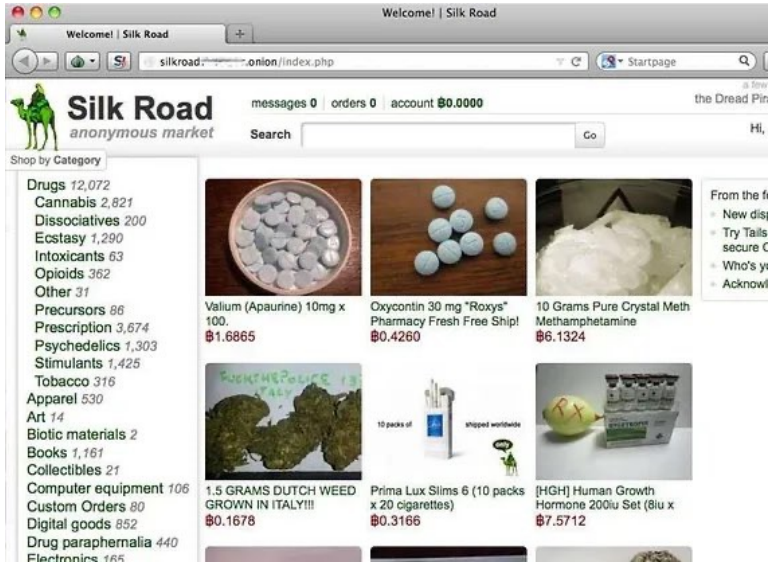
2 Pizzen für
10.000 BTC

1 BTC = $0,0041

2010-2016:
„Kriminelles Internetgeld“

2011 bis 2016 “kriminelles“ Internet Money im Darknet





- 2011–2013: Silk Road machte Bitcoin als Zahlungsmittel im Darknet bekannt.
- 2013–2017: Bitcoin blieb trotz der Schließung von Silk Road die Hauptwährung im Darknet.
- Ab 2017: Übergang zu Privacy-Coins (Monero, Zcash)
- Heute: Keine Bitcoin Zahlungen im Darknet

2013-2018:
Aufstieg im Clearnet

2013 bis 2018 Aufstieg von Bitcoin im Clearnet

- 2013–2014: Erste Akzeptanzwelle
- Grenzüberschreitendes, schnelles Zahlungsmittel für digitale Güter, Reisen und E-Commerce
- Übergang von Bitcoin als Nischenexperiment zum global beachteten Zahlungsmittel

Ende 2017: Spekulationsobjekt statt Zahlungsmittel

Dezember 2017 – Der große Hype

Bitcoin Preisexplosion

- Anfang 2017 Bitcoin Kurs bei $1.000
- Dezember 2017 Bitcoin Kurs bei $10.000
- Medienhype & ICO-Boom

Probleme auf der Bitcoin Blockchain

- Volatilität
- Hohe Transaktionsgebühr
- Lange Bestätigungszeiten

Konsequenz:

Bitcoin nicht mehr praktisches Zahlungsmittel, sondern digitales Gold / Spekulationsobjekt

- Onchain-Zahlungen nicht mehr attraktiv
- Online-Händler deaktivieren Bitcoin Zahlungen
- Bitcoin wird Wertaufbewahrungsmittel
- Neue Lösungen werden gesucht

2018-2020: Store of Value („Digitales Gold“)

Bitcoin als Store of Value

Ab 2017: Bitcoin wurde vom Zahlungsmittel zum Store of Value (Wertaufbewahrungsmittel)

August 2020: Michael Saylor / MicroStrategy beginnen in das beste Wertaufbewahrungsmittel in der Geschichte zu investieren.

Bitcoin Onchain

- Für tägliche Zahlungen **nicht** geeignet
- Geeignet als Wertaufbewahrungsmittel
- Geeignet für größere Transfer & Settlement

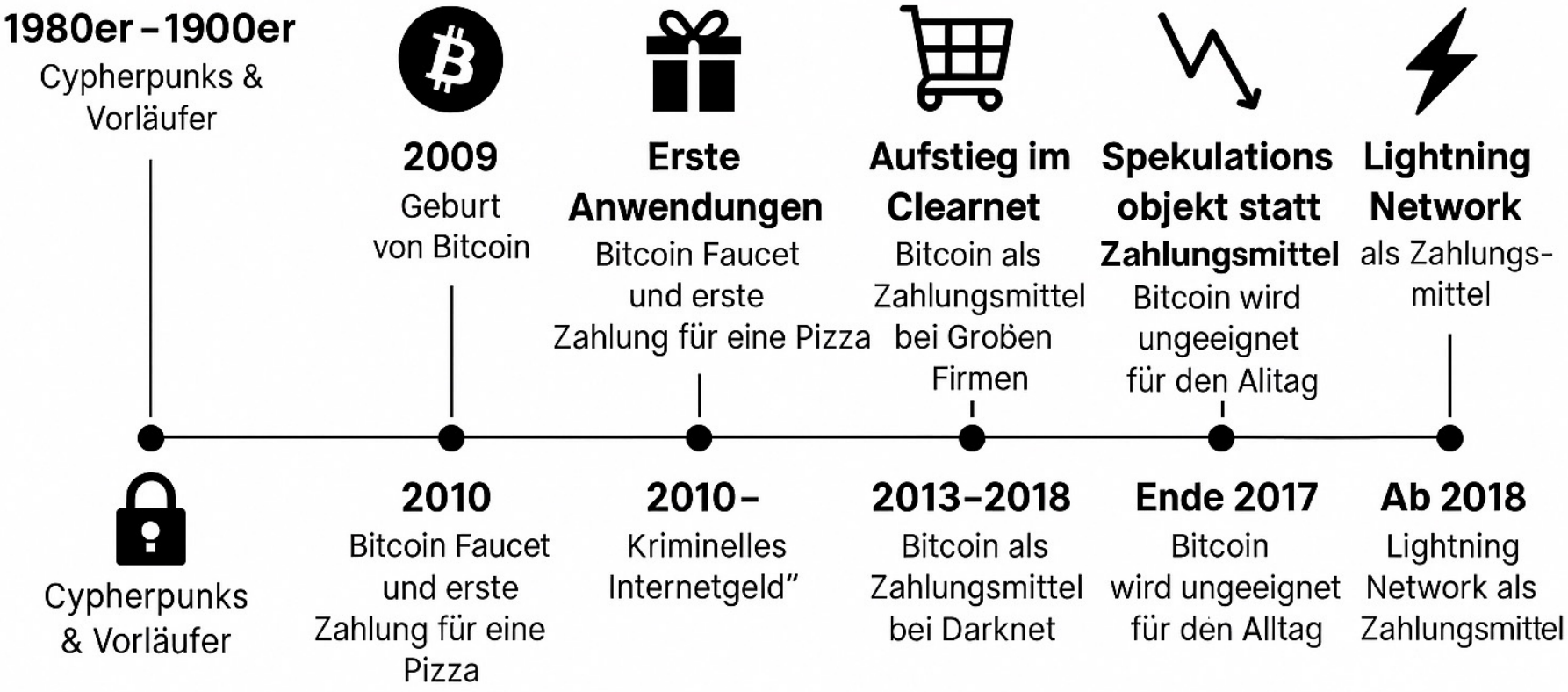
Ab 2018:
Lightning Network als Zahlungsmittel

Lightning als Zahlungsmittel

- 2015: Lightning Network Whitepaper
- 2016-2017: Erster Prototyp und SegWit Aktivierung
- 2018: Start Lightning in der Praxis
- 2018: Wallet of Satoshi
- 2021: Globaler Durchbruch als Bitcoin Zahlungsnetzwerk

Bitcoin ist
Wertaufbewahrungsmittel (Onchain)
+
Zahlungsmittel (Lightning)

ZEITACHSE VON DEN CYPHERPUNKS BIS ZUM LIGHTNING NETWORK



coinpages

https://coinpages.io

coincharge

https://coincharge.io

coinsnap

https://coinsnap.io

YouTube

https://youtube.com/@coincharge

Bitcoin Bundesverband

Jens Leinert

jens@leinert.com

https://leinert.com

https://x.com/leinert

https://linkedin.com/in/leinert/