Bitcoin
Pengar
Blockkedjeteknik

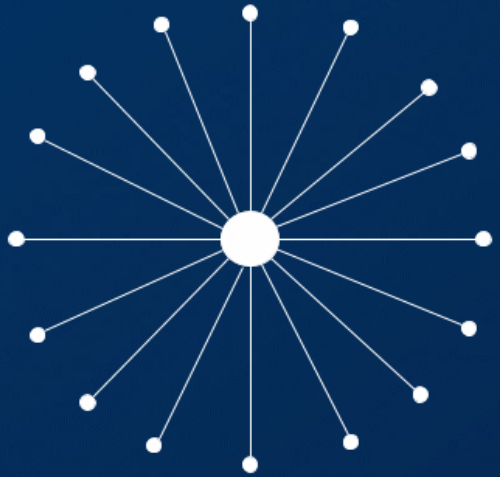
-Hur det fungerar och
vad vi kan förvänta oss

Robert Högberg

Svenska
Bitcoinföreningen

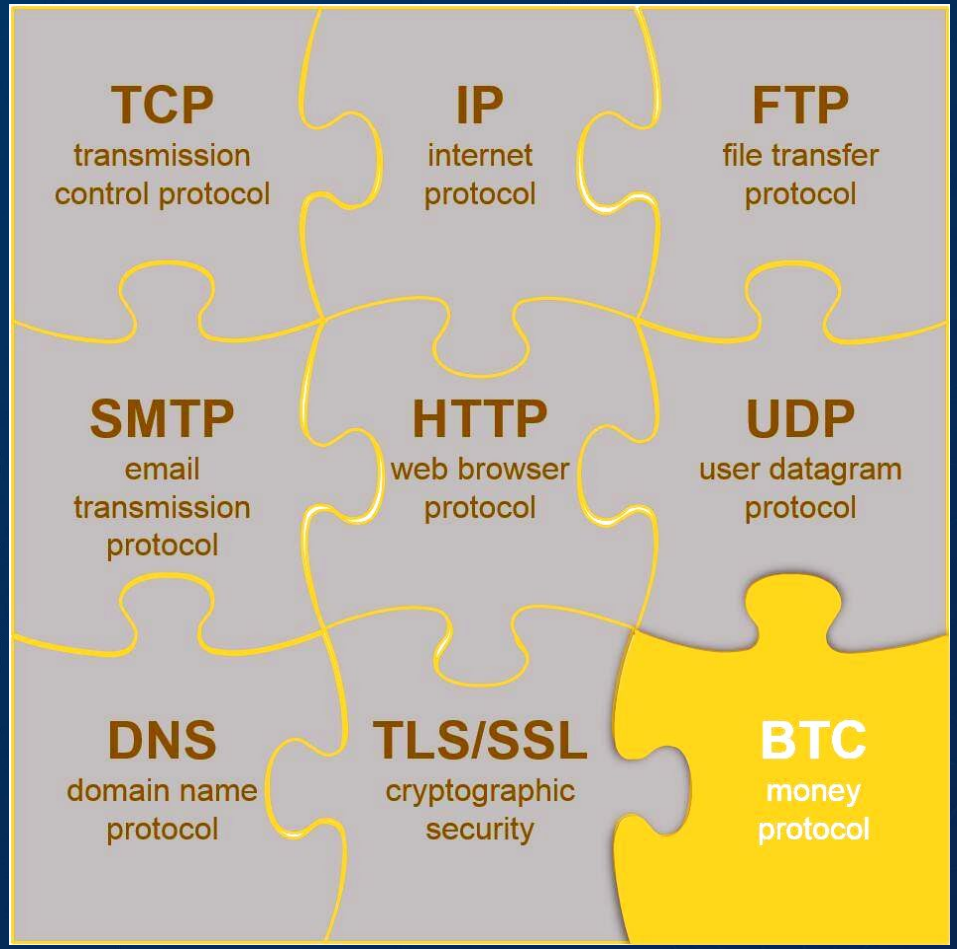
Stödja och uppmuntra en
bred användning av
Bitcoin i Sverige

Vad är blockkedjeteknik?



Centraliserat

Decentraliserat


TCP
transmission control protocol
IP
internet protocol
FTP
file transfer protocol
SMTP
email transmission protocol
HTTP
web browser protocol
UDP
user datagram protocol
DNS
domain name protocol
TLS/SSL
cryptographic security
BTC
money protocol

Tillämpningar av blockkedjeteknik

- Digitala tillgångar
  - Valutor, aktier, äganderätter, andra finansiella instrument
  - Nycklar, certifikat, licenser, identitetshandlingar
- Permanent verifierbar dokumentation
- Smarta kontrakt
- Smarta ägodelar
- Säker elektronisk röstning
- Decentraliserade autonoma organisationer (DAOs)

Pusselbitar för att bygga en decentraliserad global valuta

- Ett öppet globalt decentraliserat kommunikationsnätverk
- Peer-to-peer fildelningsteknik
- Öppen källkod
- Stark kryptering
- En inbyggd incitamentsstruktur som garanterar decentralisering, säkerhet och tillväxt

Internet 1960 -

- Packet-Switching (1961)
- ASCII (1963)
- ARPANET (1969)
- Email @ (1972)
- TCP/IP (1982)
- SMTP (1982)
- WWW (1989)
- HTML (1993)

Öppen källkod 1983 -

- GNU (1983)
- GPL (1989)
- Linux (1991)
- Open Source Initiative (1998)
- Git (2005)
- Android (2008)

Stark kryptering 1970 -

- Data Encryption Standard (1975)
- Diffie-Hellman key exchange (1976)
- RSA (1977)
- Elliptic Curve Cryptography (1985)

p2p fildelningsteknik 1999 -

- Napster (1999)
- BitTorrent (2001)

Satoshi Nakamoto skapar Bitcoin

"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"

Bitcoin: A Peer-to-Peer Electronic Cash System

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

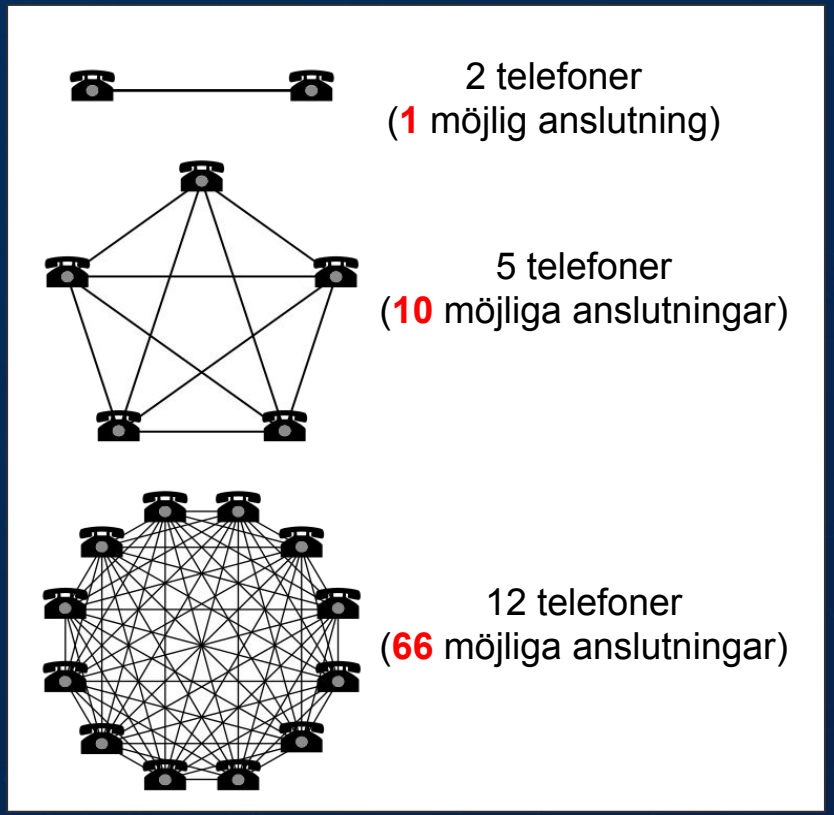
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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.

31 October 2008

3 January 2009

Hur Bitcoin fick ett värde

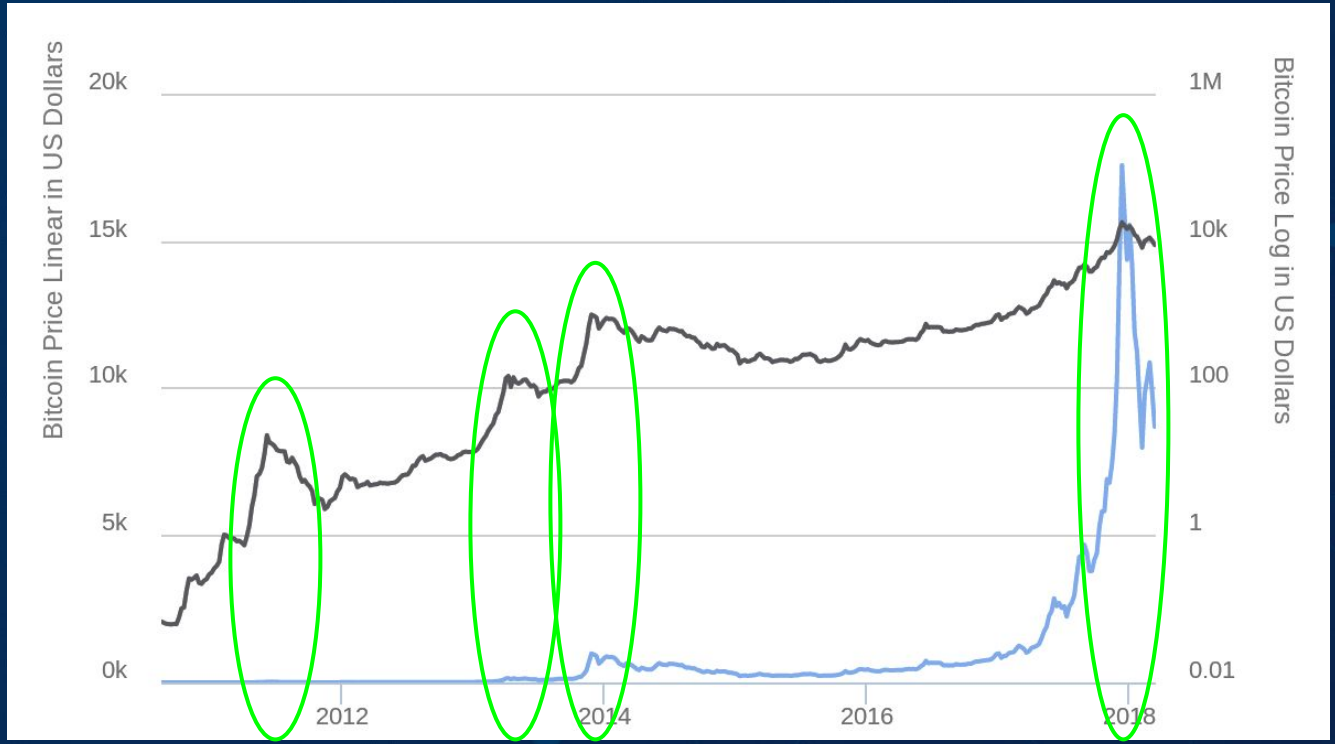
- Subjektiv värdering
- Nätverkseffekter (n^2)
  - Metcalfe's lag
- Fler användare
  ➡️ mer värde
  ➡️ fler användare



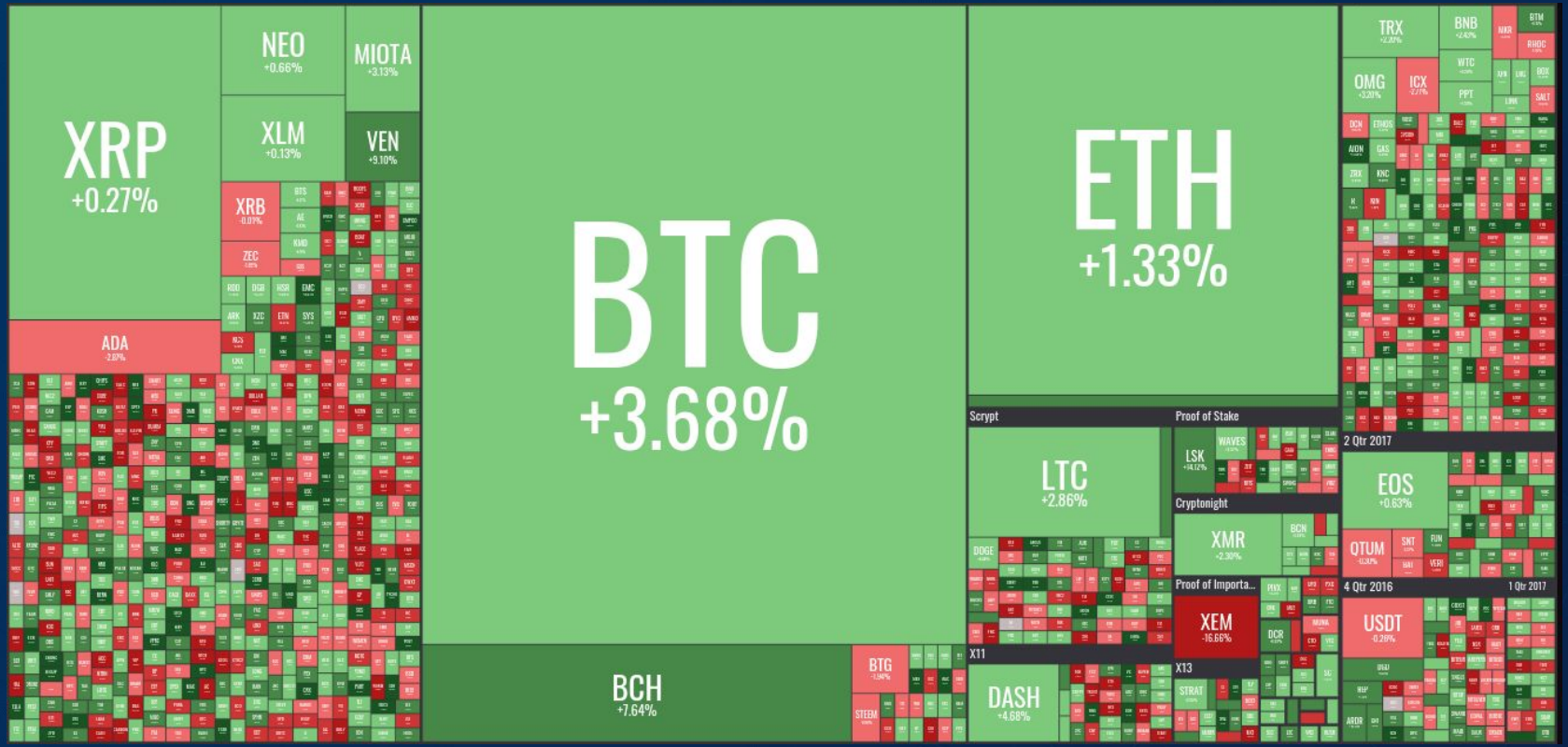
Bitcoins historiska prisutveckling 2010-2019

I mars månad ($)

2010 = 0,05
2011 = 0,80
2012 = 5
2013 = 40
2014 = 500
2015 = 300
2016 = 400
2017 = 1100
2018 = 8200
2019 = 3900
2020 = **?**



Bitcoin + Altcoins



Pengar

Bytesmedel

Mått på värde

Lagring av värde

Pengars historia

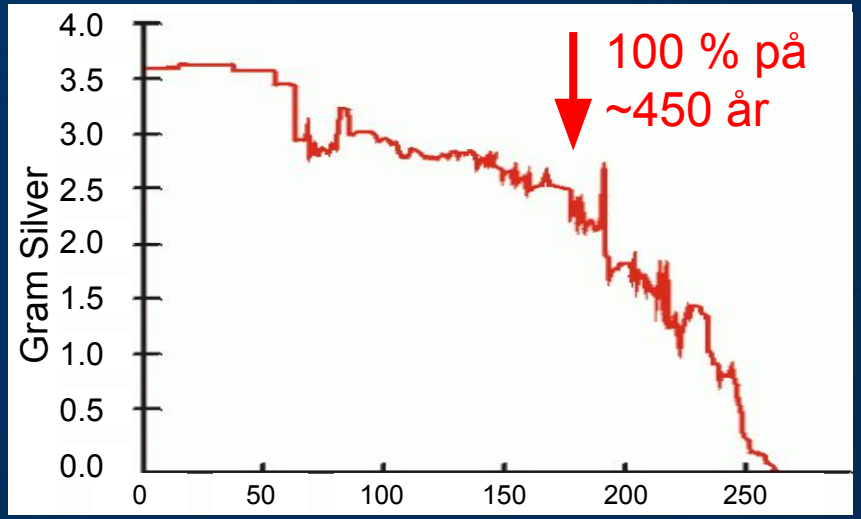
- Byteshandel
- Varupengar
- Ädelmetaller
- Sedlar
  - Guldmyntfot
  - Fiat
- Betalkort/Kreditkort
- Bitcoin

Skuldbaserat

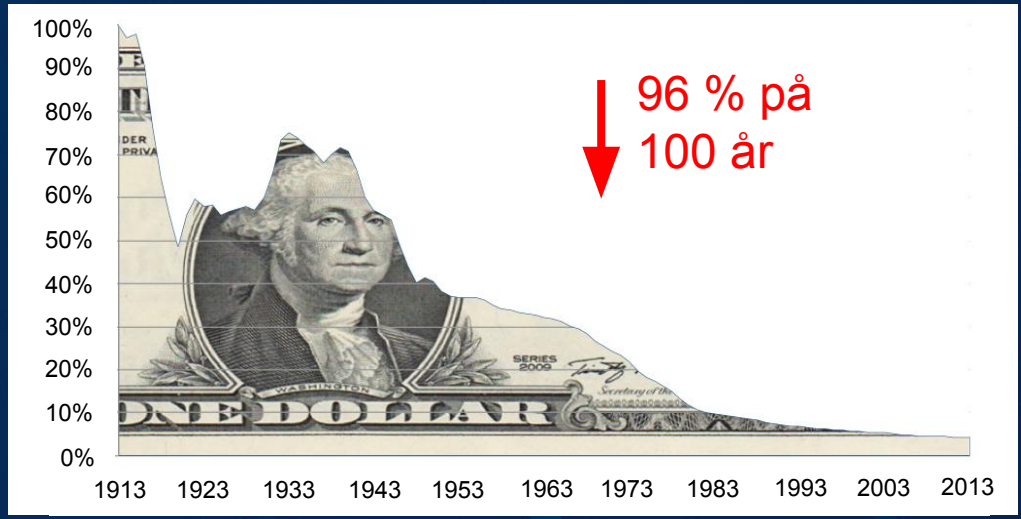
Abstraktion

Utspädning av valutors värde

Silver (g) i Romersk Denarius



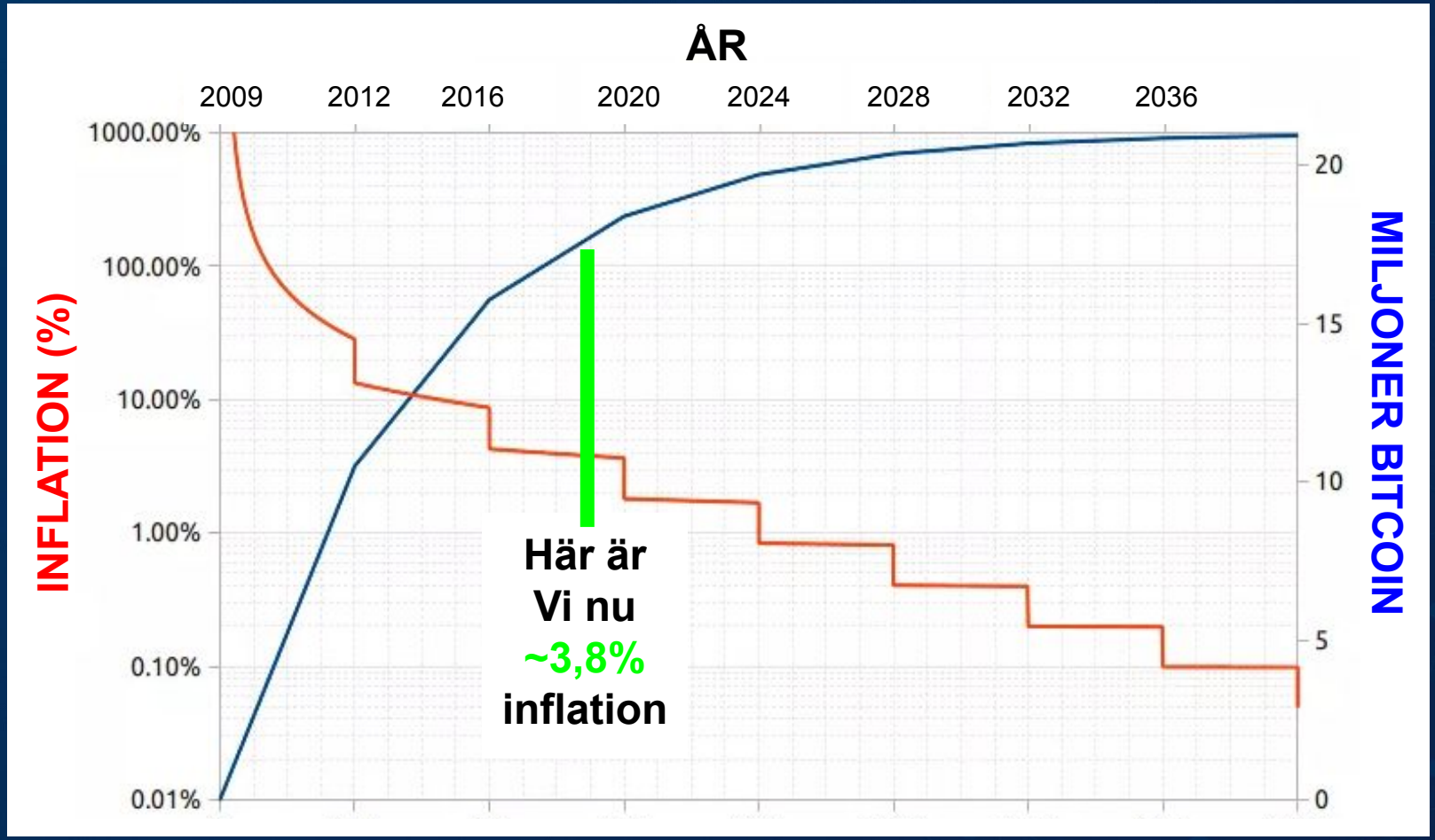
Köpkraft för US dollar (KPI) 1913-2013



2 % inflation / år = halvering på 35 år

Dold skatt!

Bitcoins penningpolitik



Pengars egenskaper

	Bitcoin	Guld	Fiat
Begränsad mängd	A+	A	F
Hållbarhet	B	A+	C
Flyttbarhet	A+	D	B
Delbarhet	A+	C	B
Verifierbarhet	A+	B	B
Fungibilitet	B	A+	A+
Utbredd användning	D	C	A
Historik	D	A+	C
Censurresistens	A	B	C
Kan programmeras	A	-	-

Bitcoin kan ge ekonomisk suveränitet

- Inga tredjeparter
- Inga mellanhänder
- Ingen kontroll eller censur
- Opt-in & Opt-out
- Ingen manipulation av räntor och valutamängd
- Ingen dold eller automatisk beskattning

Politiska och samhällsekonomiska implikationer

- Snabbare, billigare och säkrare finansiella transaktioner
- Minskade trösklar in på den globala marknaden
- Ökad ekonomisk autonomi för individer och organisationer globalt
- Individer i utvecklingsländer kan få tillgång till finansiella tjänster med säkrare överföringar

Risker

- Tekniken och utvecklingen är fortfarande i ett tidigt skede!
- Kryptovalutor kan underlätta för olaglig handel utanför statlig kontroll
- Då transaktioner på blockkedjan är irreversibla är det ett tacksamt betalningsmedel att använda för bedragare som vill lura människor på pengar. Ingen mellanliggande betalningförmedlare som kan hantera tvister
- Kryptovalutor kan underlätta för utpressare och kidnappare att få betalt (tex via ransomware-virus)
- Bitcoins konsensusalgoritm "proof-of-work" förbrukar omfattande mängder elektricitet som vissa anser inte är försvarbara ur ett hållbarhetsperspektiv