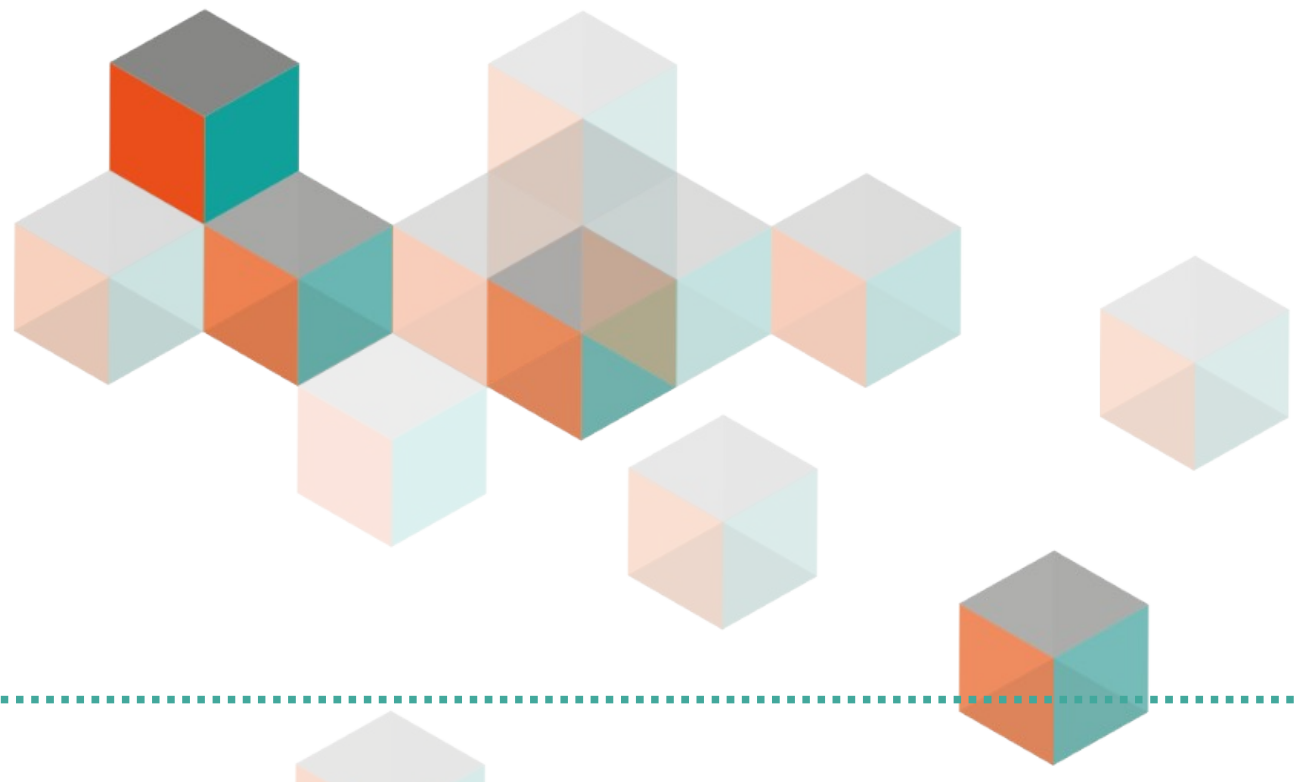


# Bitcoins: Endlich Geld im Sinne von Hayek?

**... oder warum sich Liberale oft noch schwer mit der Kryptowährung tun**



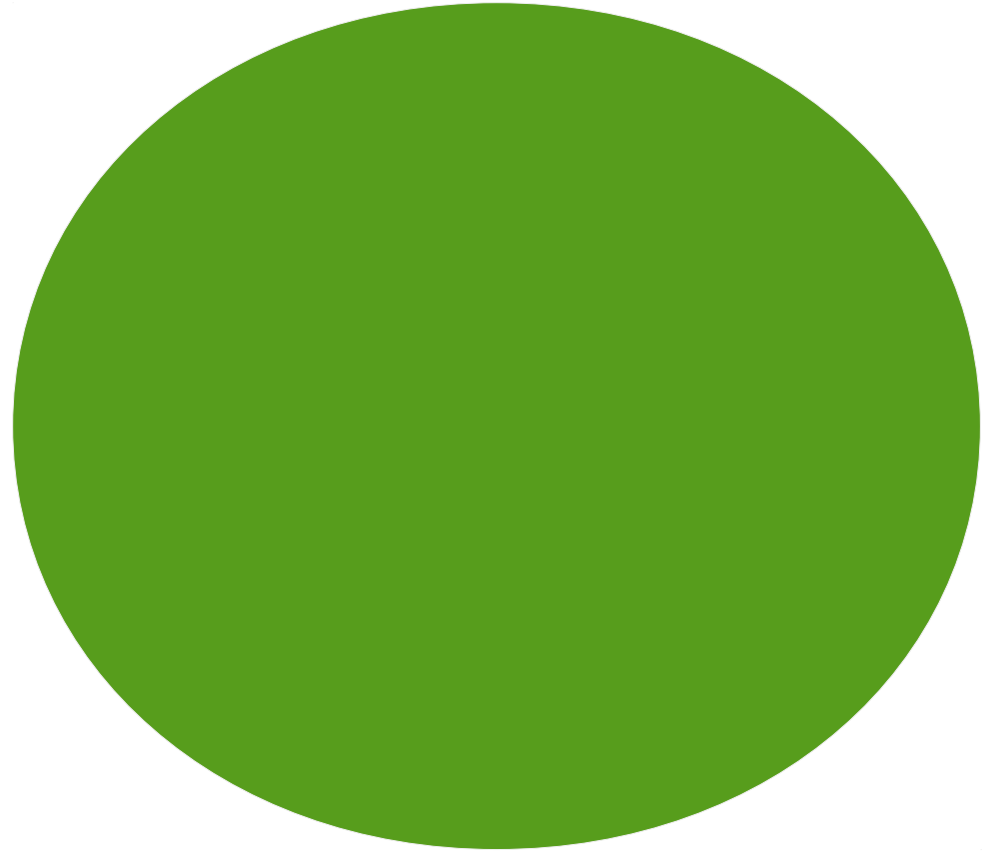
# Blockchain

- . Grundbücher
- . Supply Chain
- . Medizinische Daten
- . Gutscheine
- . Internet der Dinge
- . Fleisch
- . Identität
- . Energie
- . und so weiter und so fort



# Blockchain

- . Pressemitteilungen, Projekte, Startups, Investitionen, Veranstaltungen, Ankündigungen, Kooperationen, Allianzen, Vorträge, Arbeitspapiere ...
- . realisierte Projekte



# Bitcoin

Dezentrale, privat herausgegebene Währung mit limitierter Geldmenge, deren Kaufkraft (Wert) allein auf dem Markt bestimmt wird, die so beschaffen ist, dass weder Staaten noch Banken Guthaben einfrieren oder Transaktionen blockieren können, und die ausschließlich aufgrund freiwilligen Handelns benutzt und akzeptiert wird.



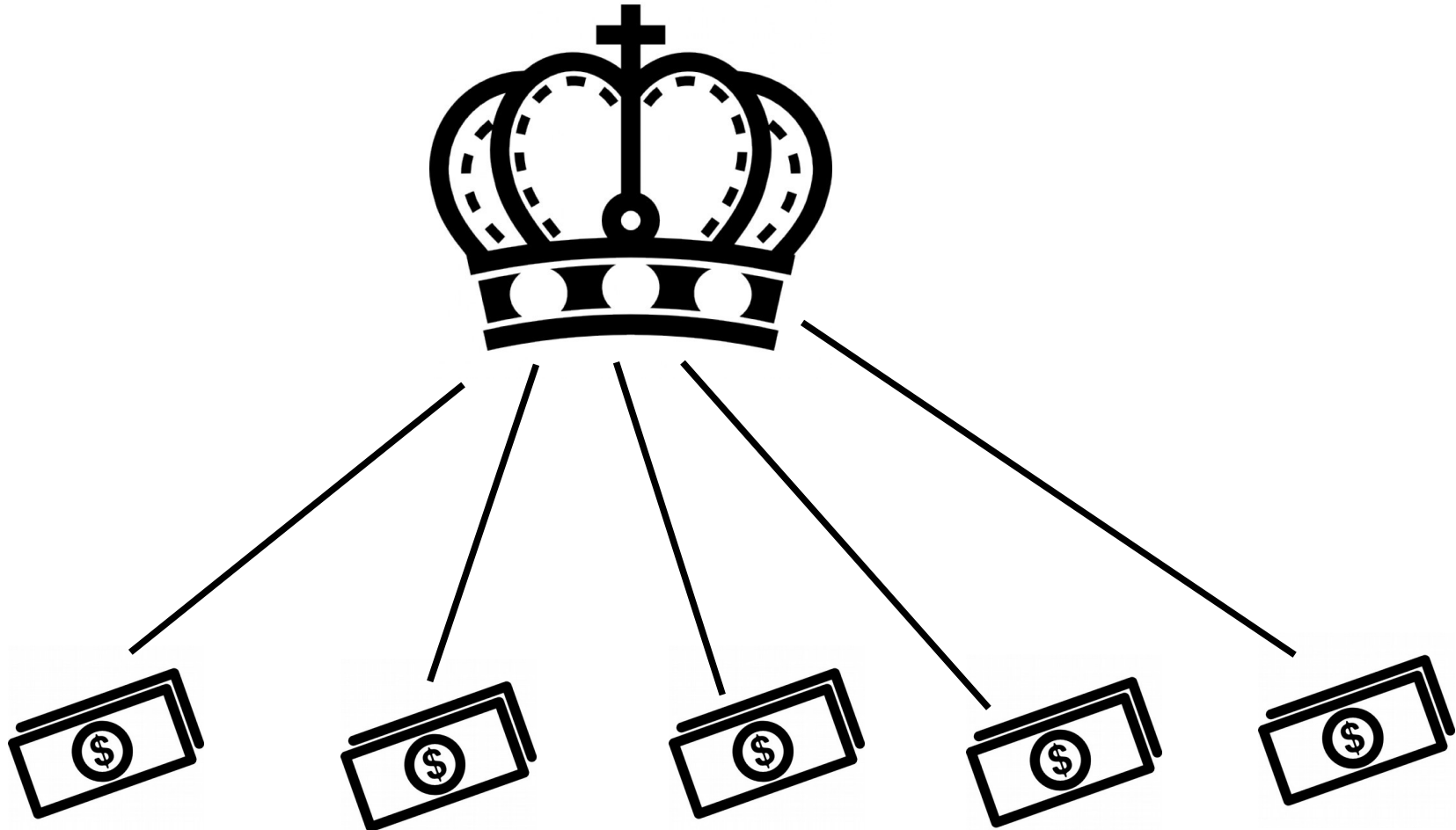
# 4.000 v. Chr. - 2009 n. Chr.



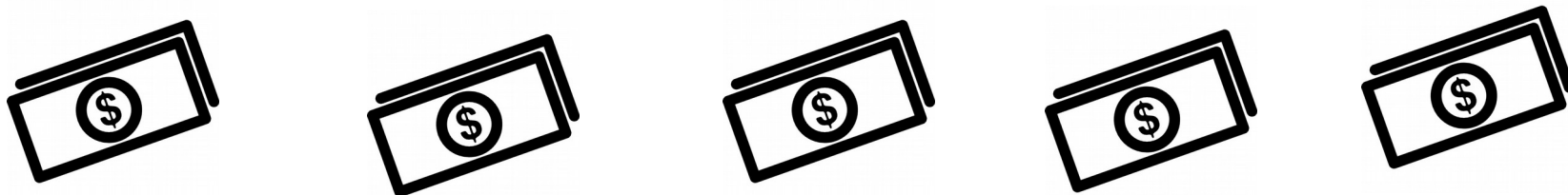
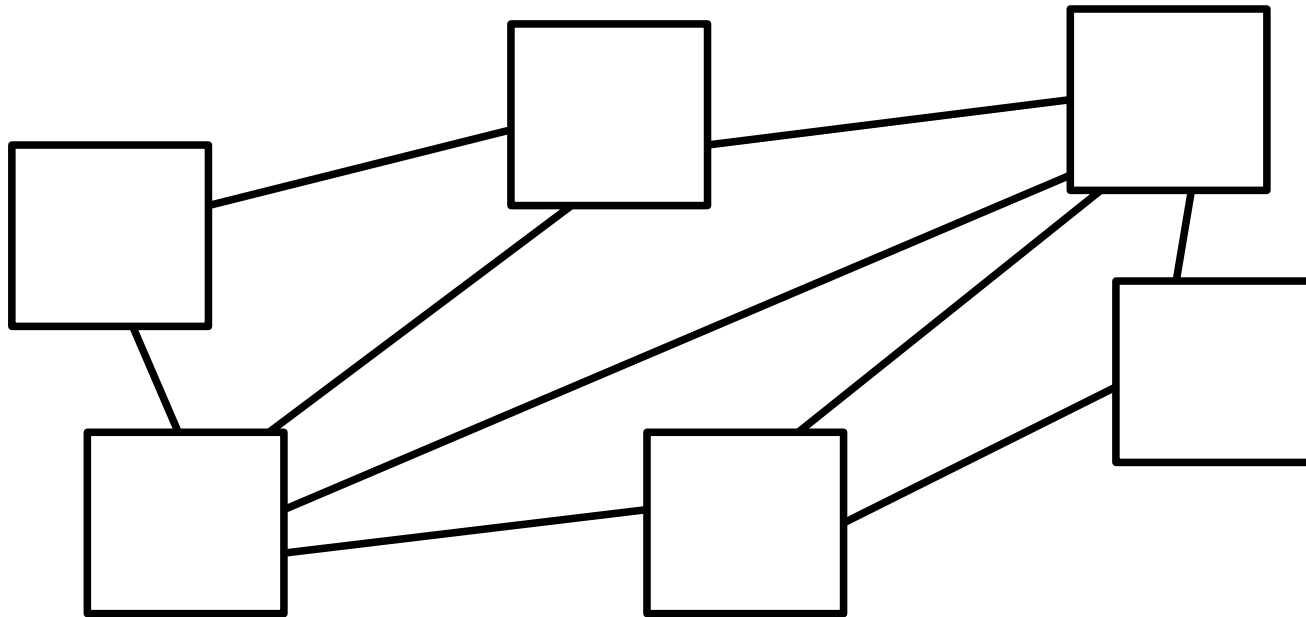
# 2009: Bitcoin



# Geldschöpfung: 4.000 v. Chr. - 2009 n. Chr.

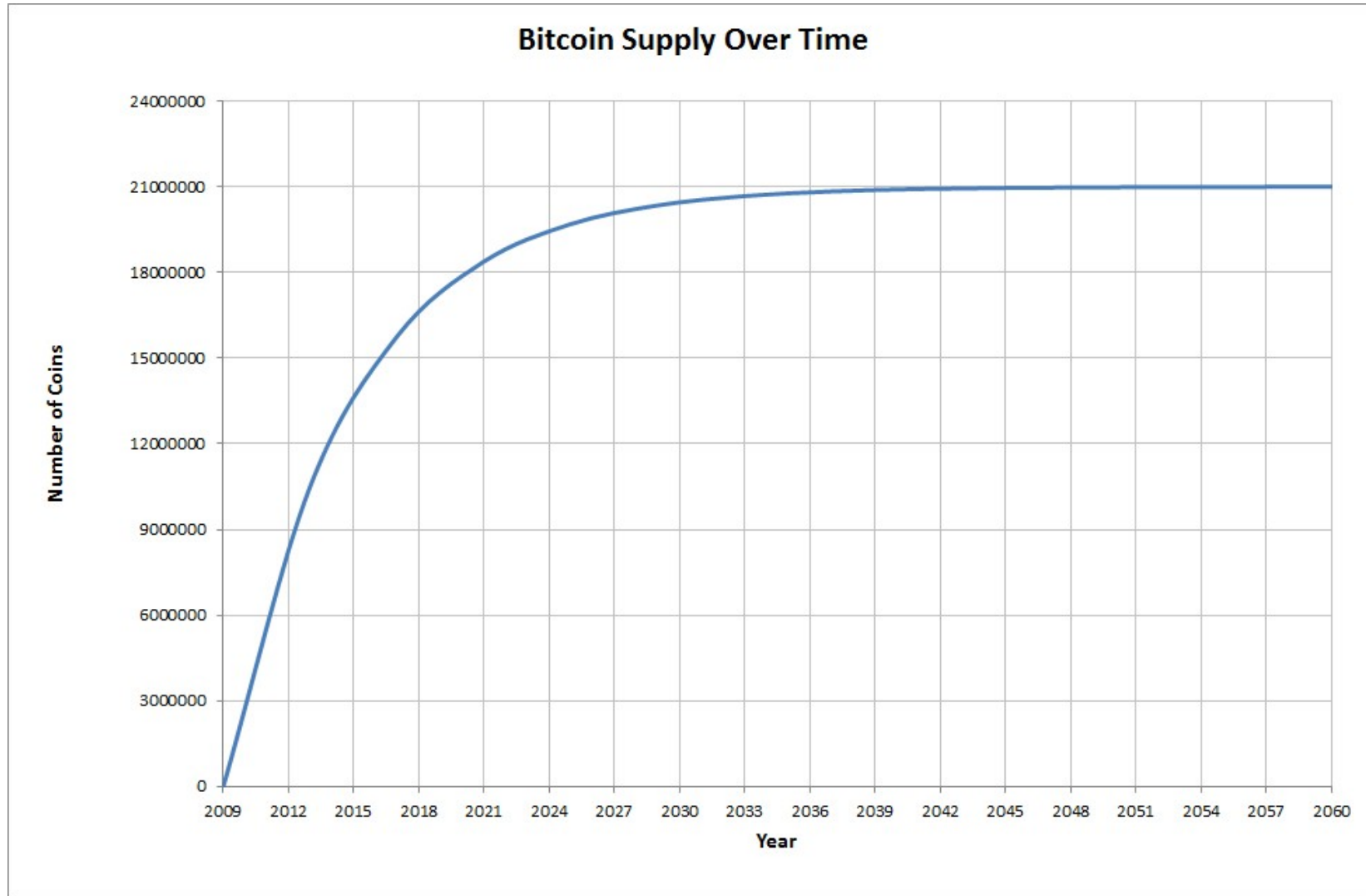


# Geldschöpfung: ab 2009 n. Chr.





# Geldschöpfung: ab 2009 n. Chr.



# Warum Bitcoin?

- . wertstabil
- . autonom
- . pseudonym
- . international
- . schnell & günstig



# Finanzmärkte ohne Banken

- . **Altcoin-Börsen:** Shapeshift (~600 Mio \$ / Tag), Poloniex (~25 Mio. \$ / Tag)
- . **Crowdfunding:** Etherem (20 Mio. \$), DAO (150 Mio. \$), Lisk (5 Mio. \$)
- . **Kredite:** BTCJam, BitBond, Loanbase
- . **Darknetmarkets:** ~ 20 Mio. \$ / Tag



# Von Hayek bis Schäffler

Dezentrale, privat herausgegebene Währung mit limitierter Geldmenge, deren Kaufkraft (Wert) allein auf dem Markt bestimmt wird, die so beschaffen ist, dass weder Staaten noch Banken Guthaben einfrieren oder Transaktionen blockieren können, und die ausschließlich aufgrund freiwilligen Handelns benutzt und akzeptiert wird.



- . Hayek, Denationalisierung des Geldes
- . Baader, Geldreform
- . Eckert, Alles Gold der Welt
- . Schäffler, Nicht mit unserem Geld



# Satoshi

. Bitcoin: A p2p electronic cash system  
(2009)



# Geldreform

**Bitcoin:**

- . größtes liberales monetäres Projekt aller Zeiten?
- . dezentrale Geldreform



# Warum nicht **Thema Nr. 1** bei **Liberalen?**

Vermutungen:

- . Technologie (Kryptographie, dezentrale Netzwerke)
- . kein Edelmetall (Mises' Progressions-Theorem)



# Keine **Krypto-Piraten**

- . Nur ein Videospiel? Linden-Dollar, Geld aus Civilization?
- . Zwei Technologien: Kryptographie + Dezentrale Netze
- . Kryptographie ist Mathematik:  
Asymmetrische Kryptographie, Adresse  
+ priv. Key





# Sicherheit

Imagine you built a perfect computer; forget about GHash and Megahertz.

You built a computer which used the absolute minimum amount of energy theoretically possible to record a change in a single bit [1 to 0 or 0 to 1].

We are talking about the limits of thermodynamics; nothing more efficient is even possible.

Now imagine you used most of the natural resources in our star system to construct a dyson sphere and covered the entire surface of this sphere with a single star system sized super computer.

Now imagine you could keep this supercomputer cooled at roughly absolute zero and could do so without expending any additional energy.

If you had that and captured (with no inefficiency or loss) the entire energy output of our star (not just in a day or week but continually until it burned out) you couldn't COUNT to  $2^{256}$  before you ran out of energy.

Keep in mind this is simply counting.

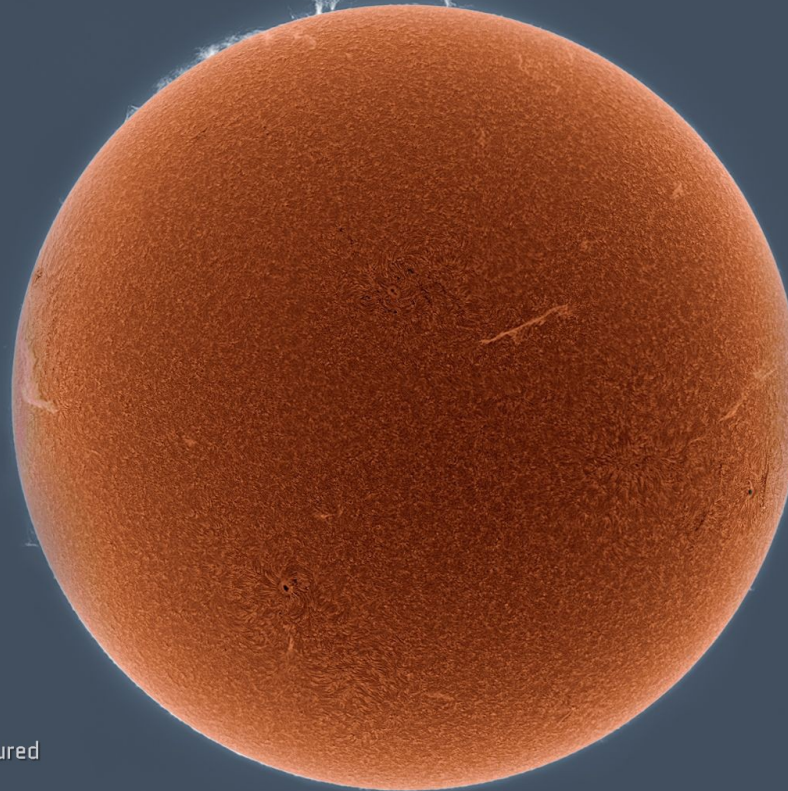
Just counting, not hashing, not comparing, not performing lookups just counting 1 .. 2 .. 3 .. ....  $2^{256}-1$ .

These numbers have nothing to do with the technology of the devices; they are the maximums that thermodynamics will allow.

And they strongly imply that brute-force attacks against 256-bit keys will be infeasible *until computers are built from something other than matter and occupy something other than space.*

Bitcoin — Your money is secured by the laws of the universe.

BITCOIN  
IN CRYPTO NOS CONFIDIMUS

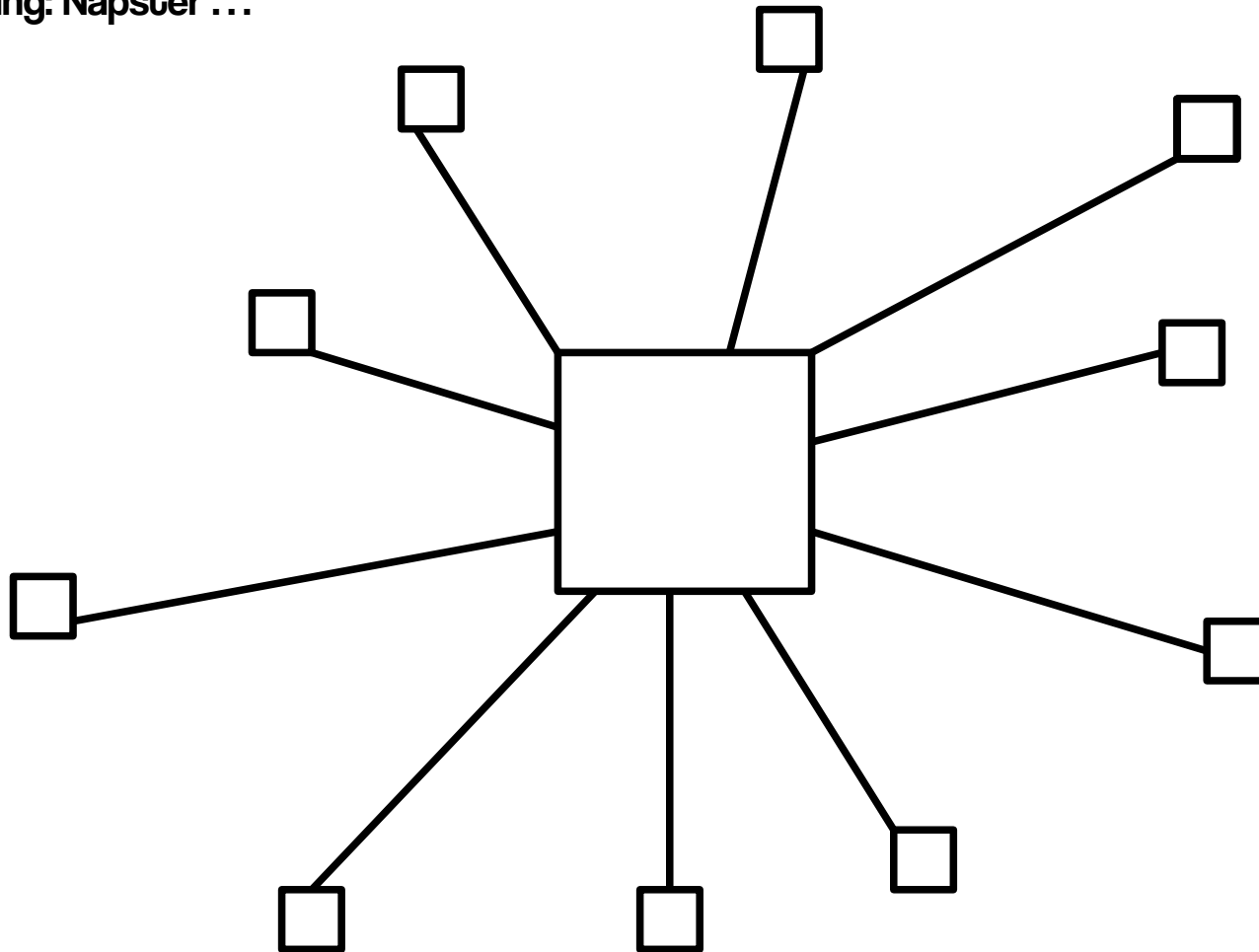


**Perfekter Computer, bedeckt gesamte Oberfläche der Sonne, dennoch nicht möglich, Schlüssel zu brechen, bevor Energie erschöpft ist.**



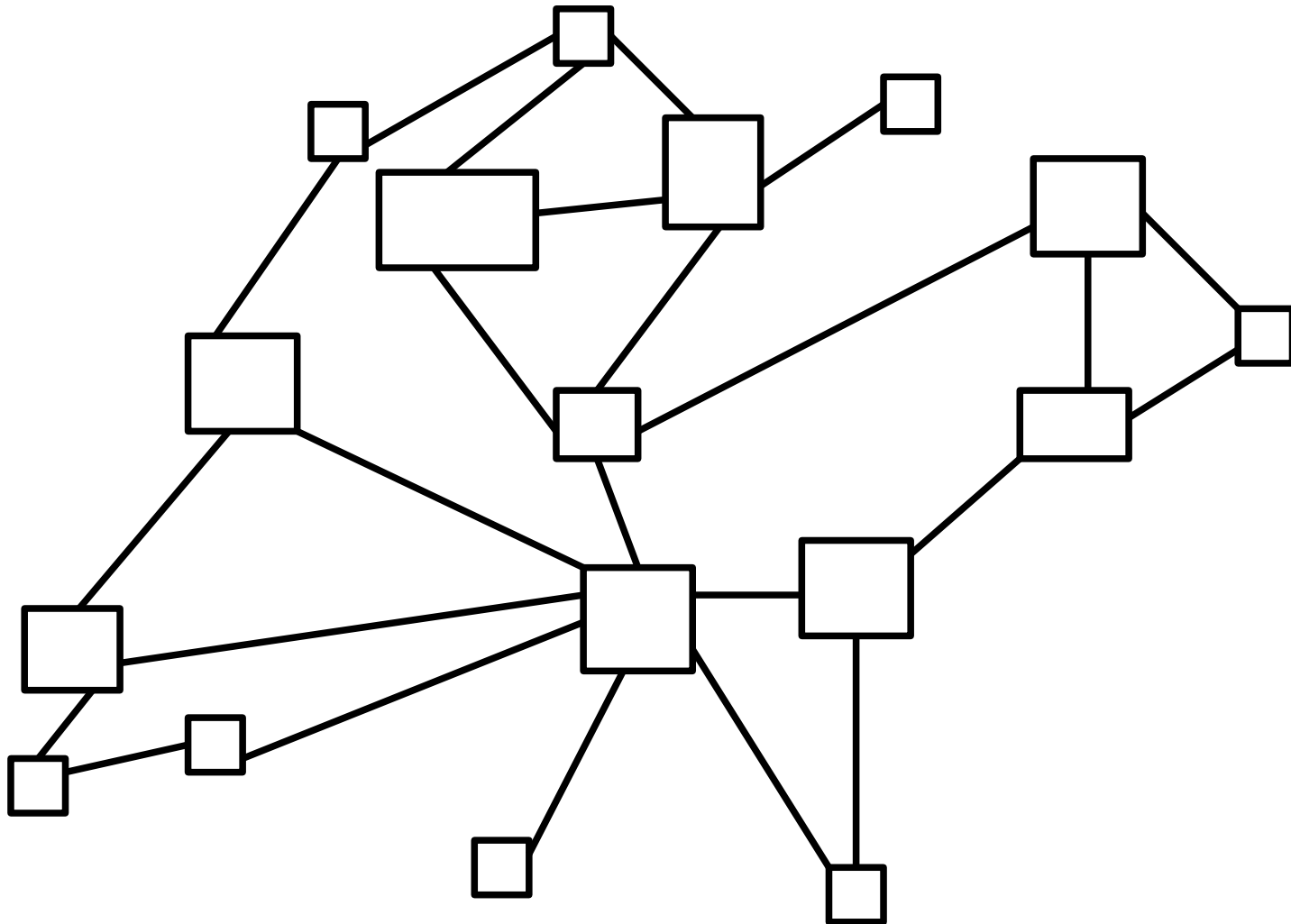
# Dezentrale Netze

. Filesharing: Napster ...



# Dezentrale Netze

- . BitTorrent
- . Kazaa
- . Emule



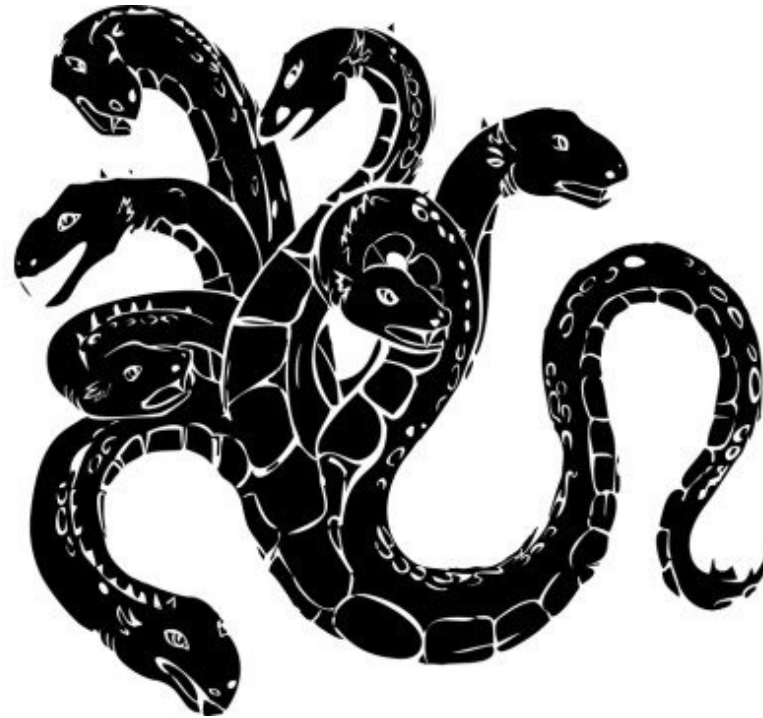
# Dezentrale Netze

## Bitcoin

- . überträgt dezentrales Prinzip auf Geld
- . Geld = Guthaben in Kontenbuch (Blockchain)
- . jeder Knoten prüft Kryptographie + Guthaben
- . Miner synchronisieren Kontobücher + erhalten dafür Bitcoins

## Ergebnis

- . niemand kann Bitcoin abschalten
- . niemand kann Bitcoins fälschen
- . niemand kann Transaktionen rückgängig machen
- . seit 8 Jahren ohne Ausfall ohne Hack



# Kein Edelmetall

- . inherenter Wert?
- . Regressionstheorem?

**„Wie kann man Geld aus einem Computer-Code erzeugen? Das erschien mir absurd, wie eine Techno-Version der Alchemie. Geld musste aus Gütern entstehen, die im Tauschhandel genutzt werden. Das hatte Carl Menger bewiesen. Wenn Bitcoin einen Wert hat, dann muss das ein Error sein, oder das Ergebnis von gutem Marketing, wie bei jedem Ponzi-Schema ... dennoch ist Bitcoin Geld. Es wird jeden Tag benutzt. Man kann es auf den Börsen in Echtzeit sehen. Es ist kein Märchen. Es ist echt.“**

**– Jeffrey Tucker**



# Kein Edelmetall

„Stell' dir vor, es gibt ein Metall, das so knapp ist wie Gold, aber die folgenden Eigenschaften hat: langweilig grau in der Farbe, kein guter Leiter von Strom, nicht besonders fest, aber auch nicht besonders weich, nicht nützlich für irgendwelche praktischen oder dekorativen Zwecke und, als die eine, spezielle, magische Eigenschaft: Es kann über einen Kommunikations-Kanal transportiert werden ...“

– Satoshi

„Der ursprüngliche Wert des Bitcoins ist an das an ihn angehängte Payment-Netzwerk gebunden. Das ist der Nutzwert, auf den sich Mises bezieht. Er liegt nicht in der Währungseinheit, sondern vielmehr in dem brillanten und innovativen Zahlungsnetzwerks. Bitcoin ist auf genau dieselbe Weise entstanden wie jede andere Währung, von Salz zu Gold. Leute fanden das Payment-System nützlich, und die damit verbundene Rechnungseinheit war transportabel, teilbar, fungibel, haltbar und knapp.“

– Jeffrey Tucker

---

# Zum Abschluss

## Wichtige Zitate von Wence Caesares (Xapo):

**„Was findest du am Bitcoin toll?“**

**- „Dass es sich mehr wie ein Kreuzzug als wie ein wirtschaftliches Phänomen.“**

**„Ich denke, Bitcoin ist wie eine Schwangerschaft: es ist egal, wie mächtig und reich du bist, es dauert 9 Monate, bis du ein Baby bekommst. Genauso ist es egal, wie intelligent du bist und wieviel du über Technologie und Finanzen weißt – es dauert etwa 6 Monate, bis du Bitcoin verstehst und umfasst.“**

**„Ich sage immer, dass die zweitdümme Sache, die man derzeit machen kann, ist, mehr Bitcoin zu besitzen, als man sich leisten kann zu verlieren, und dass es die dümmste Sache ist, keine Bitcoins zu besitzen.“**

