Bitcoin angreifen

für billig

Optimierungen für 51% Angriffe

START

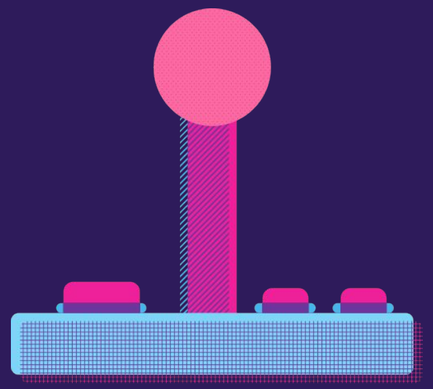
Credits

Die Theorie hinter der Präsentation basiert auf der Arbeit von Justin Drake

Wichtigste Quelle:

Youtube-Interview mit CompassMining:

v=o8Mg4hzJaFg



Vielen Dank an SlidesCarnival für das Präsentationstemplate

Kapitel

1

Warum minen?

Warum machen die das?

2

51% - ja und?

Hashen ist Macht!

3

Anleitung

Nicht zu Hause ausprobieren…

Warum?

Deshalb minen Miner

Warum machen die das?

Profit

- Miner bekommen für “gefundene Blöcke” eine Belohnung + TX-Fees
- **Das Geschäft muss profitabel sein**

- Höherer Bitcoin-Preis
  -> mehr Hashrate
- Höherer Reward (inkl. Fees)
  -> mehr Hashrate

- Und umgekehrt

Ideologie

- Manche Miner sind nicht profitorientiert
- “Echte Bitcoiner”
- Insbesondere kleine Miner aus der Bitcoin Community, ohne Firma oder ETF

- Der Anteil ist nicht bekannt, aber wahrscheinlich klein

CapEx und OpEx

CapEX

- Capital Expense (Beschaffungskosten)
- Hardware-Kauf, z.B. Mining-ASICs, Transformatoren, Kabel, Hallen, Grundstück, etc...
- **Angreifer optimieren für niedrige CapEX**

OpEx

- Operational Expense (Betriebskosten)
- Strom, Miete, Steuern
- Für Mining-Firmen ist dies der entscheidende Kostenanteil
- Grund: Abschreibungszeit für Mining Hardware ca. 5 Jahre
- **Miner optimieren für niedrige OpEx**

51%?

Hashen ist Macht

Blockproduktion

Der Rhytmus

- Bitcoin erzeugt ca. alle 10 Minuten einen neuen Block
- Der Finder bekommt eine Belohnung

- Wer 50% der Hashrate hat, findet durchschnittlich jeden zweiten Block

- Belohnung: 6,25 BTC
- Ab ca. 31.05.24: 3,125 BTC

Das Maß

- Gemessen in TH/s Terra-Hashes pro Sekunde

- Terra = 1.000.000.000.000 (eine Billion) Hashes pro Sekunde

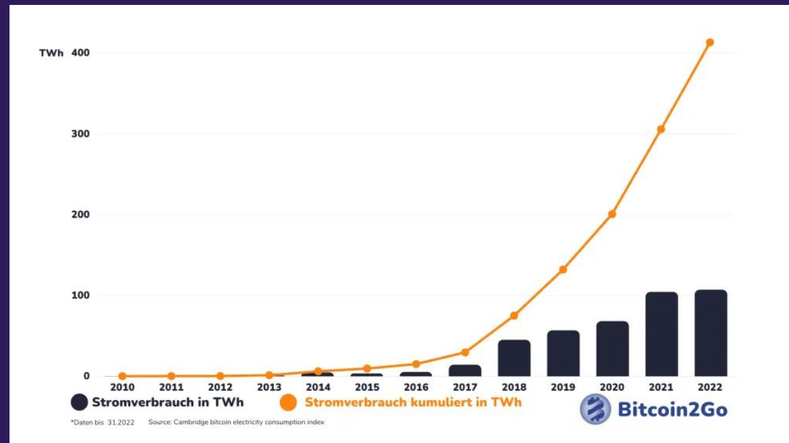
- Derzeit ca. 550 Millionen TH/s

Die Technik

- Spezialhardware, die Hashes erzeugt

- Die Hardware muss gekauft werden

- Der Betrieb kostet Strom: ca. 100TWh / Jahr (0.4-0.5% des weltweiten Verbrauchs)



Sicherheits-Budget

Das Sicherheits-Budget ist der Betrag, den man aufwenden muss,
um >51% der Hash-Rate zu erreichen.

SB = Hashrate x Kosten pro Hash

Sicherheits-Verhältnis

(Security-Ratio, SR)

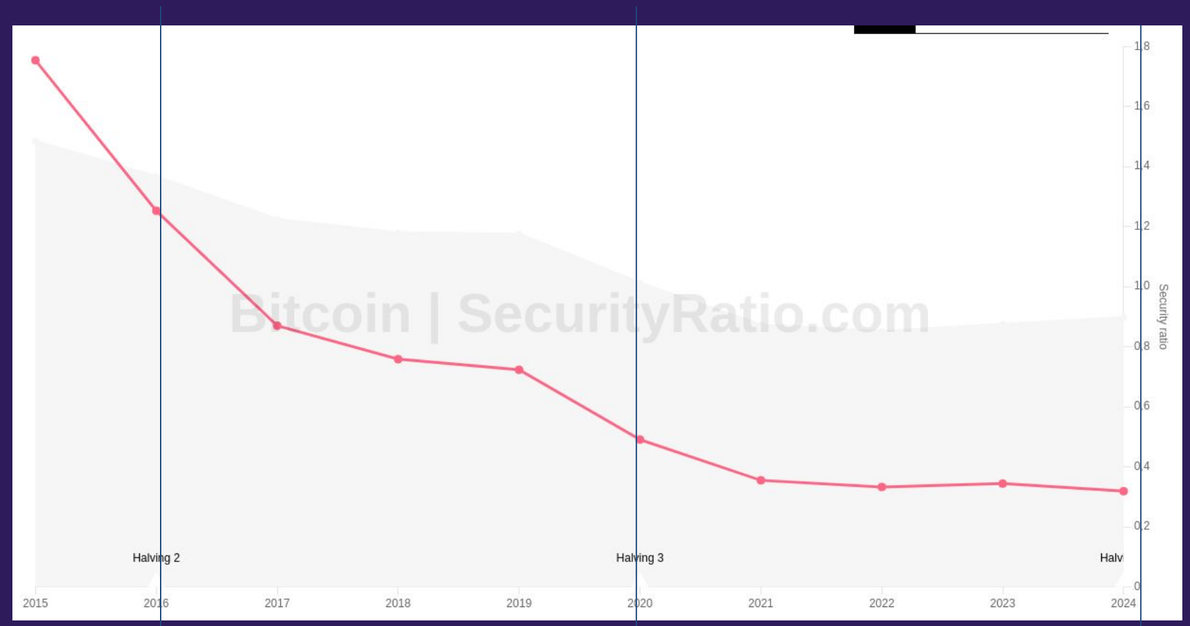
Verhältnis zwischen Marktkapitalisierung und Belohnungen

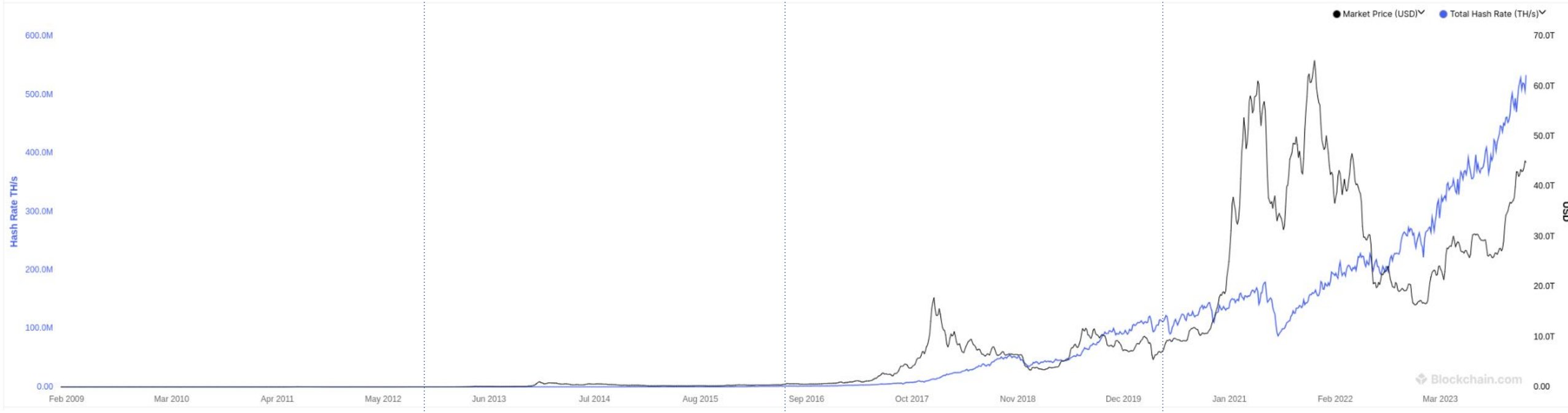
Halbiert sich mit jedem Halvening

SR = Belohnungen / Marktkapitalisierung

Aktuell ca. 0.3

$$\text{Security ratio (SR)} = \frac{\text{Total Block rewards}}{\text{Total Circulation supply}} * 1\,000\,000$$




Market Price (USD)
Total Hash Rate (TH/s)
Hash Rate TH/s
600.0M
500.0M
400.0M
300.0M
200.0M
100.0M
0.00
70.0T
60.0T
50.0T
40.0T
30.0T
20.0T
10.0T
0.00
USD
Feb 2009
Mar 2010
Apr 2011
May 2012
Jun 2013
Jul 2014
Aug 2015
Sep 2016
Oct 2017
Nov 2018
Dec 2019
Jan 2021
Feb 2022
Mar 2023
Blockchain.com

Naiver Brute-Force Angriff

Die Rechnung

- Aktuelle Hash-Rate: 550M TH/s [1]
- Hardware kaufen: 15,- $/TH
  (Einzelpreis, inkl. Profit, keine Rabatte, kein Übertakten)

Mining Hardware	Hashrate	Power Consumption (Watts)	Price (USD)
Bitmain Antminer S19 XP Hyd (255Th)	255Th/s	5304	$4,150+
Bitmain Antminer S19 XP (140Th)	140TH/s	3010	$3,999+
Canaan Avalon Made A1366	130TH/s	3250	$5,499+
MicroBT Whatsminer M50S	126TH/s	3276	$2,999+
MicroBT WhatsMiner M56S	212TH/s	5500	$4,300+

Quelle: koinly.io

Daraus lässt sich ein *naives* Security-Budget ableiten:

15 x 550M = 8.25 Milliarden $

Zum Vergleich: Elon Musk hat Twitter für 40 Milliarden $ gekauft

Hashen ist Macht: 51% kann...

Regeln ändern

- Soft-Forks im Alleingang
- Hard-Forks im Alleingang

100% Blockkontrolle

- God-Mode: Welche Blöcke existieren
- Nur auf eigene Blöcke aufbauen

Zensur

- Transaktionen auswählen
- Verteidiger zensieren

Double-Spending

- kaum relevant
- Außer: Cross chain / Lighting

Der Angreifer ist im Vorteil

Zeitwahl

Ortswahl

Waffenwahl

CapEx vs. OpEx

Kleines Risiko /
nichts zu verlieren

Selbstverstärkung

rationale Miner verkaufen Hardware,
rationale Holder verkaufen Bitcoin

Recycling / Griefing

Vertrauensbruch
/ Story kaputt

Kaum Stromkosten

Sicherheit und Preis /
TX-Gebühren eng verknüpft

Die Spieler

Ehrlicher Miner

Hält sich an immer
an die Regeln

Rationaler Miner

Handelt immer im
Eigeninteresse

Böser Miner / Angreifer

Will zerstören und die
Welt brennen sehen

Motivation:
Gewinn, Angst

Anleitung

Nicht zu Hause ausprobieren…

Unser Team

Wer sind wir?

Ein Nationalstaat, der Angst vor
Bitcoin hat -> Böser Miner

Was haben wir vor?

Agenda: Bitcoin killen
5 Jahre Zeit, 40 Milliarden $ Budget

Der PLAN

Vorbereiten

60% Hashrate erlangen

Warten

Angreifer-Vorteile maximieren

Angreifen

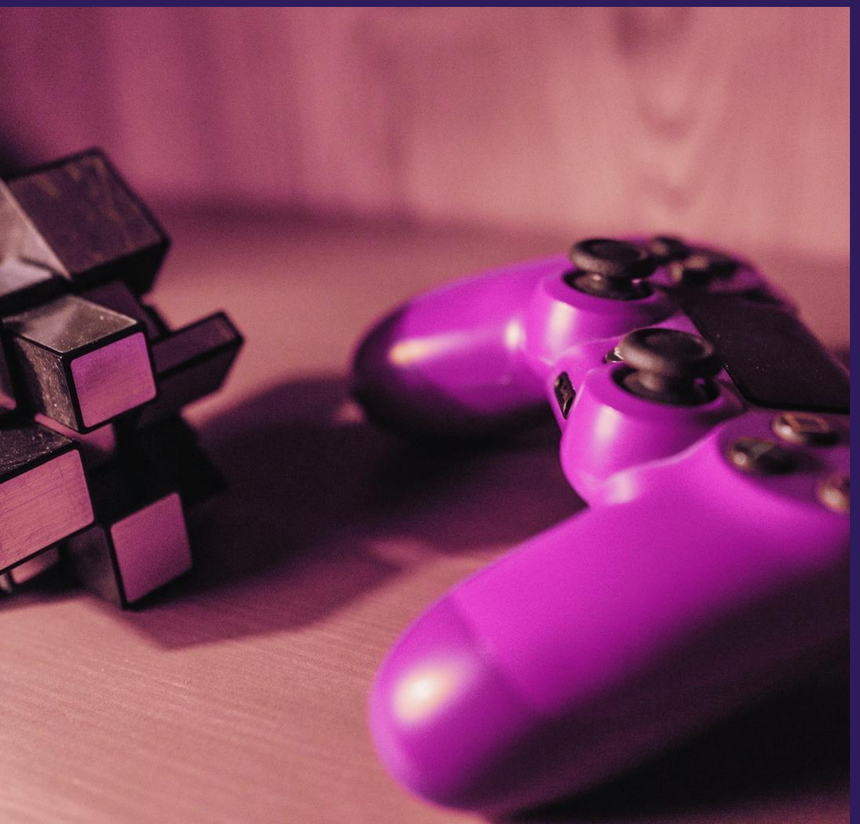
Angreifen, manipulieren, mobben

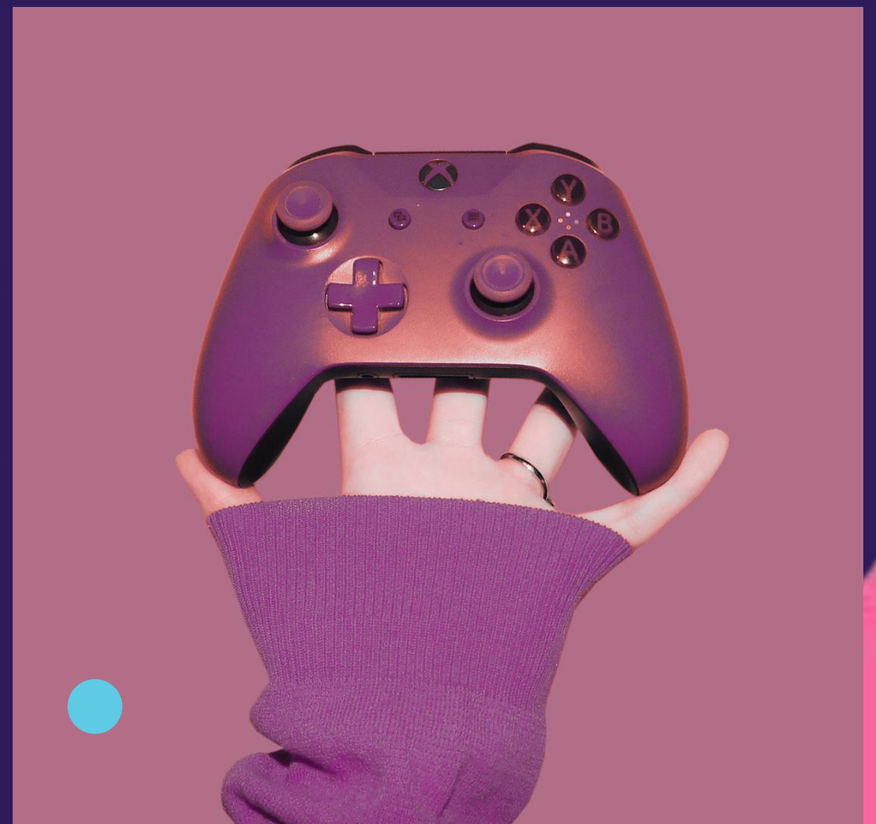
Sichern

Sieg sichern, sabotieren, Gewinn abschöpfen

Vorbereiten

Wir machen uns bereit





Alte Hardware kaufen

- **Billig zu haben**
  CapEx optimiert
- **Unauffällig**
  “Stupid shitcoiner”
- **Nahe an EOL**
  Kann aber übertaktet werden (+30-50%)

Unrentable Mining-Farmen kaufen

Finanzielle Probleme

Machen kein Profit, bereit zu verkaufen, kurz nach Halvening, im Bärenmarkt, …

Off-Shore

Ideologisches Alignment simulieren, knapp über Marktpreis bieten

Weiter betreiben

Kaum profitabel aber auch kaum Kosten

2x Hashrate Faktor

Bestehende Hashrate wird gekapert + Übertakten

-> ⅓ reicht bereits

Schlachtfeld wählen

Hemisphären-Arbitrage

Südhalbkugel -> Winter wenn Sommer in Texas (Kühlung, etc…)

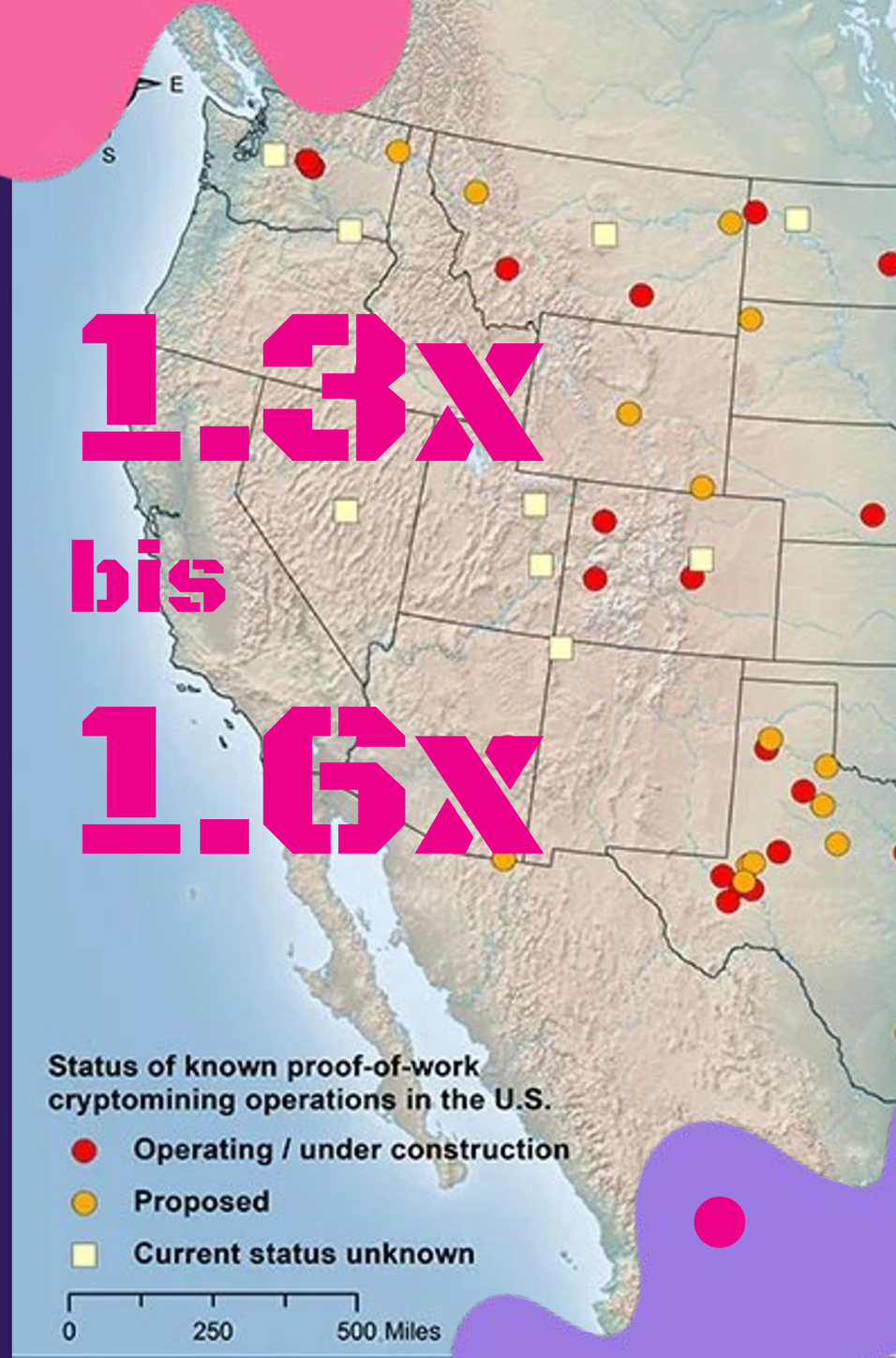
Miner in Texas drosseln im Sommer

Klima-Arbitrage

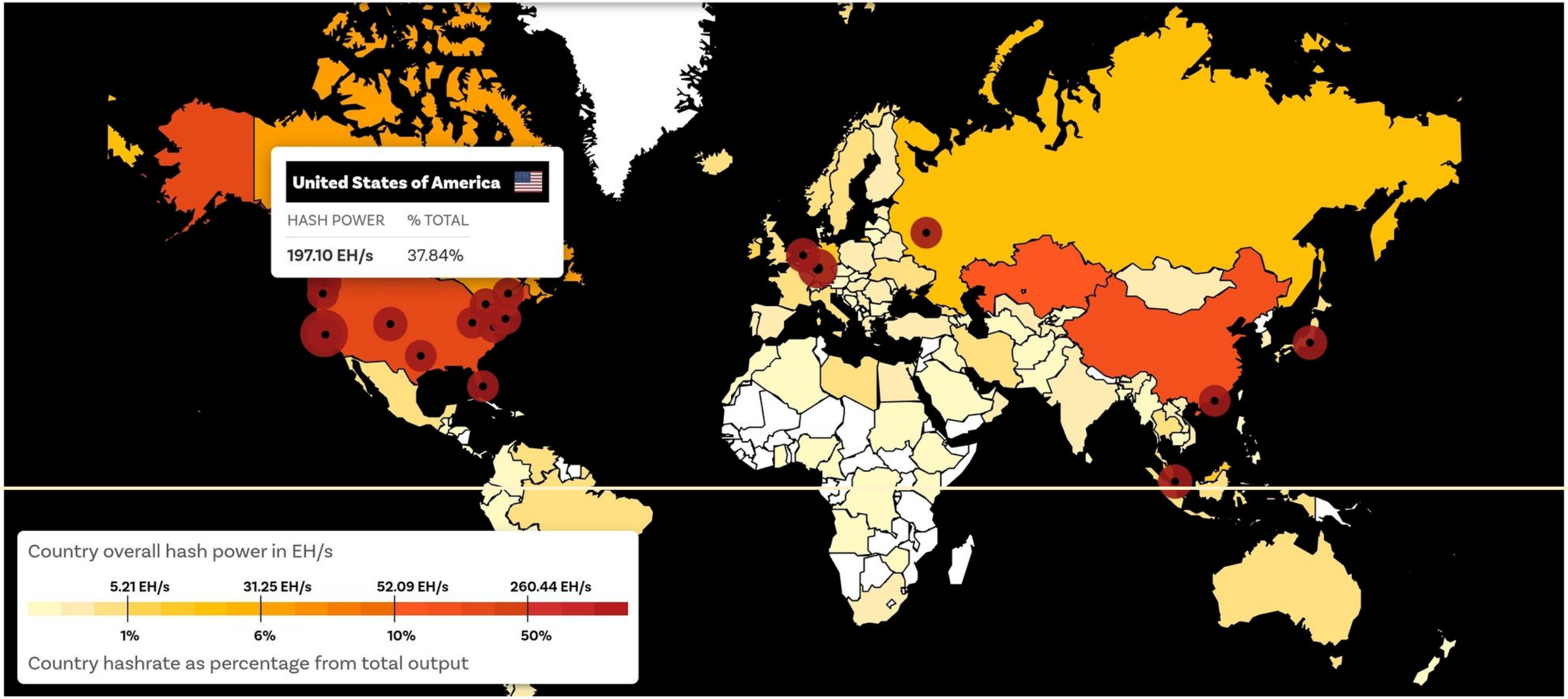
Zu viel Energie im Winter (Touristen-Hotspot, Wasserkraft, …)

Politische Arbitrage

Whäle ein Land, dass das Vorhaben gutheißt



The Chain Bulletin | **Bitcoin Mining Map**



Boutique ASIC Hersteller kaufen

Optimierung

Spitzenleistung statt Niedrig-Energie

Alte Technik nutzen

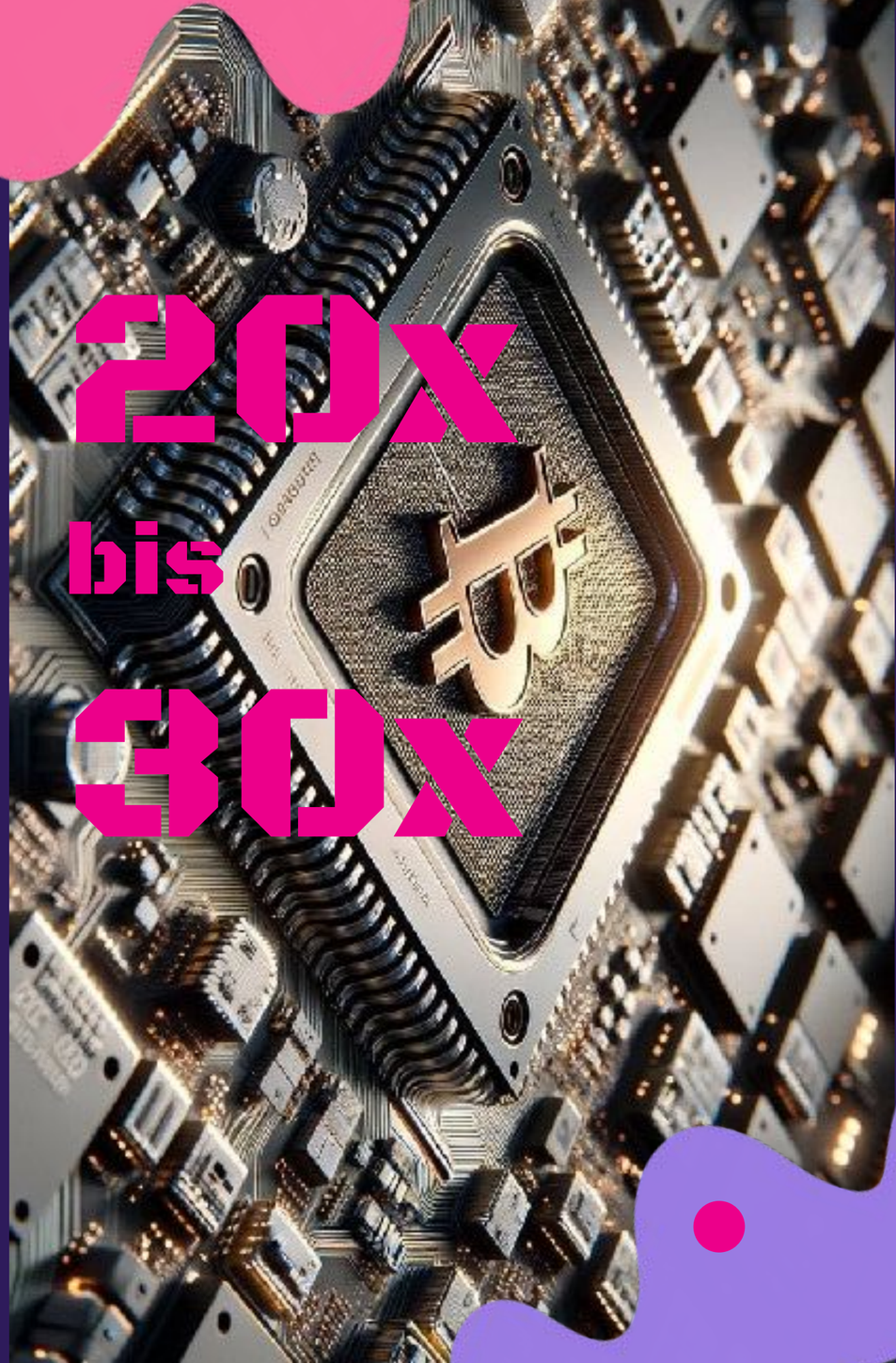
z.B. 28nm,
optimiert for CapEx

SHA256 anpassen

Hohe Hashrate präferieren (anderer Quadrant)
-> 20-30x

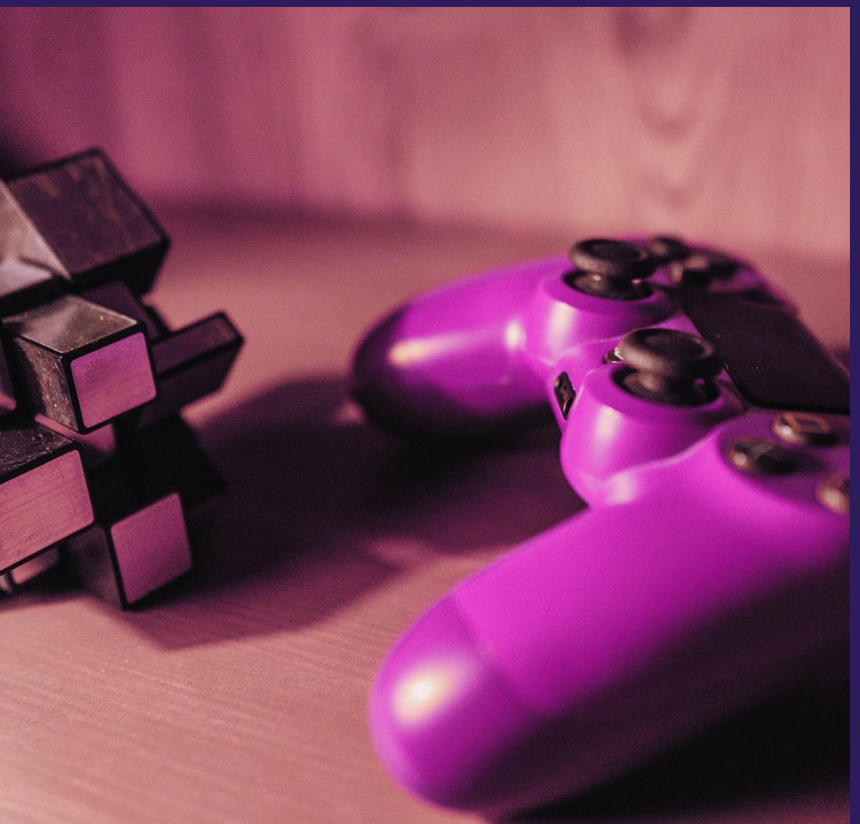
Bei hohem Sicherheits-Budget

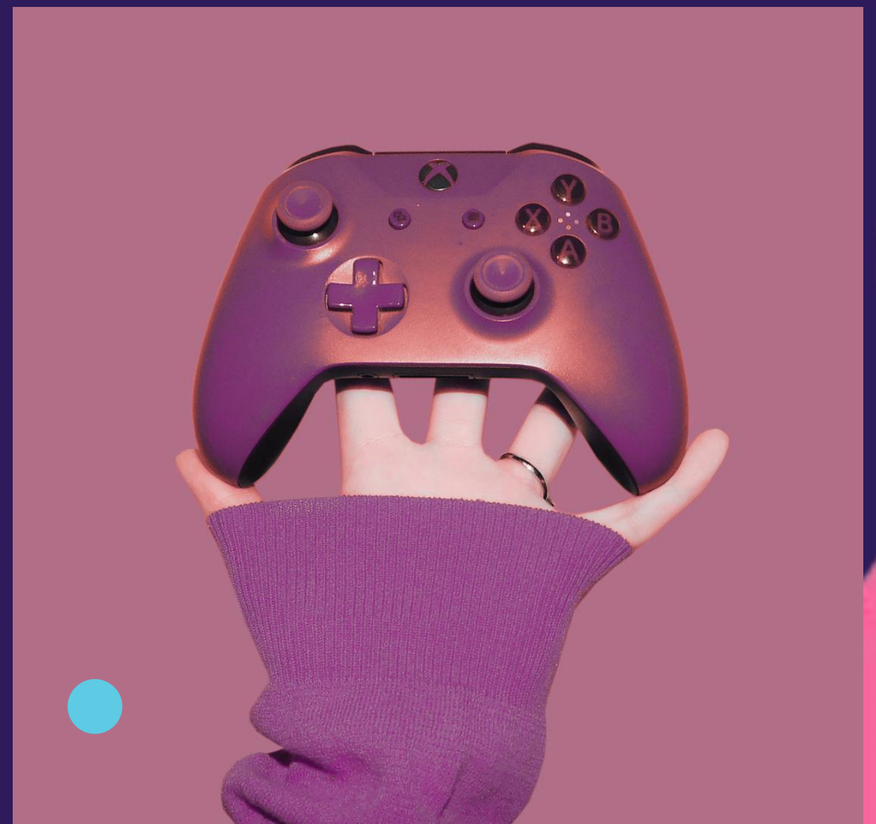
z.B. 100 M



Warten

Allzeit bereit





Wenn der Feind schläft...

Spezial-Firmware

Firmware für starkes Overclocking entwickeln

Schwacher Markt

Angreifen, wenn Miner unter Stress stehen, Hardware kaufen, wenn die Belohnung sich halbiert

Big Short vorbereiten

1% der BTC MarketCap mit 100x genügt

Denkfabrik

Um weitere Optimierungen zu finden

Replacement-Attack

Eigene Hashrate (auch mit Verlust) drückt fremde Hashrate vom Markt (nicht mehr profitabel)

Wenn der Feind nicht mehr schläft...

Angriff ankündigen

Um den Bitcoin-Preis zu drücken -> Stress für Miner

Allianzen schmieden

Gemeinsam angreifen und Strategien entwickeln

Credible commitment

100M in Ethereum Smart Contract -> Proof of 1000 empty Blocks bekommt Belohnung

Verkaufspirale

- Farm Erpressung
- Commitment Erpressung

Wer zuerst geht, macht am wenigsten Verlust

Ergebnis

Kosten stark gedrückt, z.B. um den Faktor 2-4

Realistisches Budget: 2-4 Milliarden USD

(statt 8.25 Milliarden)

Angriff!!!

Booste dich!

Alle Miner los!

Overclocking 20-30%

Ortsvorteil

Günstige Spitzenleistung, nicht: günstige Dauerleistung

Mobbe sie!

Miner-Mobbing

Miner Wallets einfrieren
+ 0,0 BTC Belohnung
-> Shut down
-> ASICS aufkaufen

Einbahnstraßen-Angriff

Exchanges:
Nur hin, nie zurück

Double-Spend

Break Lighting-Channels
Wrapped Bitcoin

Spawn Camp Angriff

Droppe deine Hash-Rate, warte auf meiner, greife wieder an

Up/Down, Up/Down

Manipulation

Schnipp/Schnapp

Miner Sabotage
100k pro Anlage

Vertrauen

Commitment einsammeln

Kirmes-Angriff

Auf Transformatoren schießen
100k pro Anlage

Profitiere

Shorts Ausführen

0.5% of Market-Cap ist genug (1-4M) um alle Kosten reinzuholen

Clear out Lightning

Censor Fraud Proofs

Parallelr Angriffsplan

1

Boosting!

Im Sommer untertakten die Miner -> 20-30%

2

Mobbing!

Zuerst: Delaying (10%)

Dann: nur eigene Blöcke

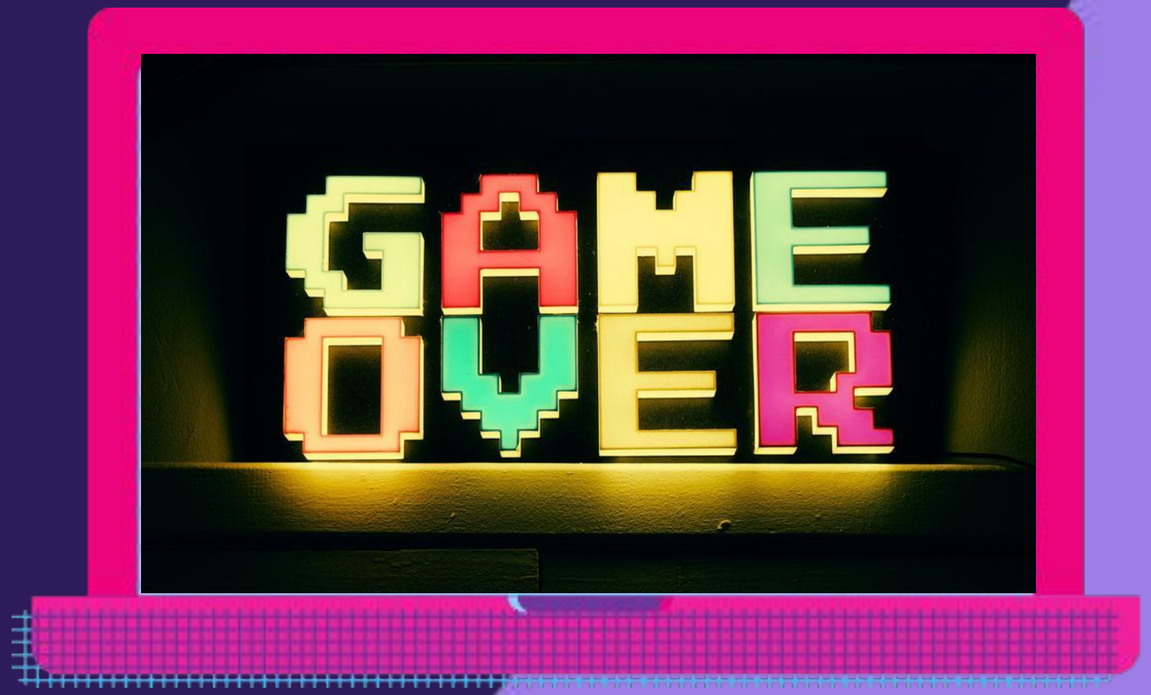
3

Manipulation!

Censor Money

Schnipp-Schnapp

Thank you!



Sichern

… und Kosten reduzieren

Billige Hardware aufkaufen, Angriff verstärken (massive Spawn Camp)

Später: Transformatoren, Klimatechnik, etc… verkaufen.

Muhahaha!

Diskussion

MENU

Verteidigung

Koordinieren

- Counter-Selfish-Mine
- Overclock, too

- Alles schwach, weil der Angreifer keine Koordinierung benötigt und nur ein wenig mehr Budget

Veränderung

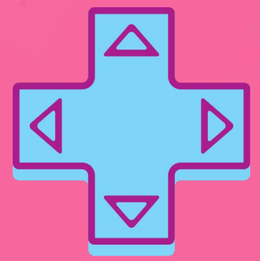
- PoS
- Tail issuance
- More expressive
- Fee smoothing
- Checkpoints
- Neuer Hash Algo
- Secret Switch

Bitcoin sterben lassen

- UTXO-Set als Ethereum Roll-Up auferstehen lassen

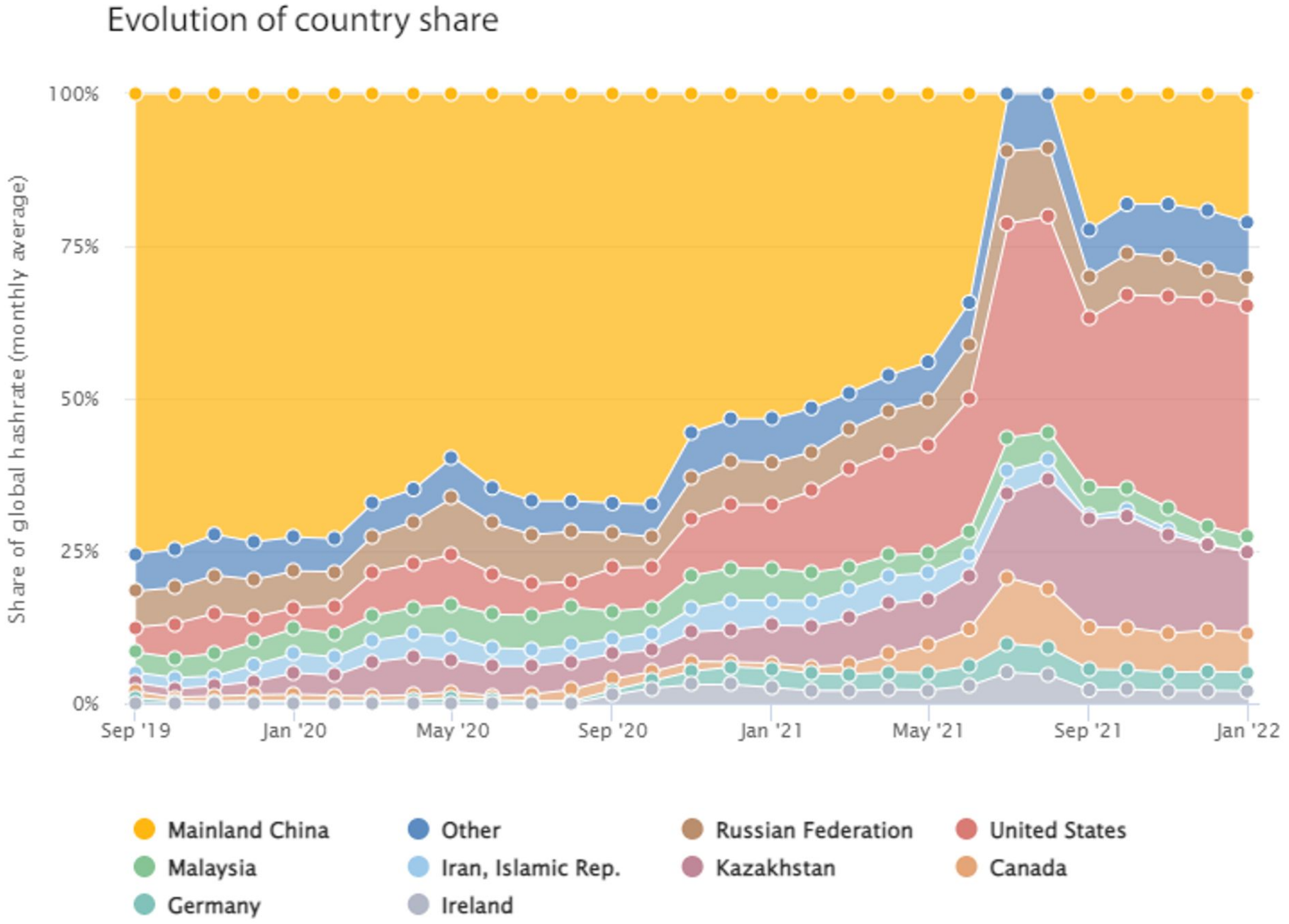
Ordinals Lieben Lernen

- Höhere TX Einnahmen

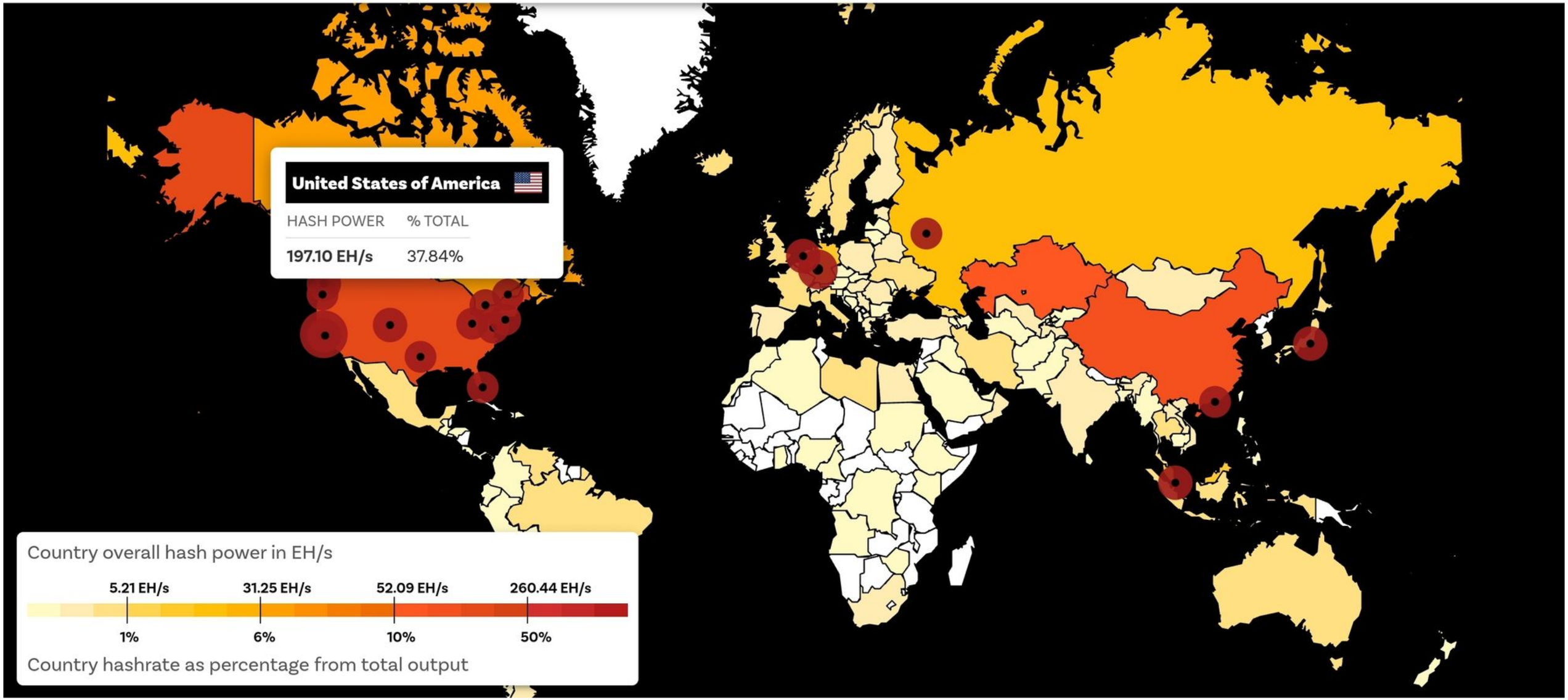


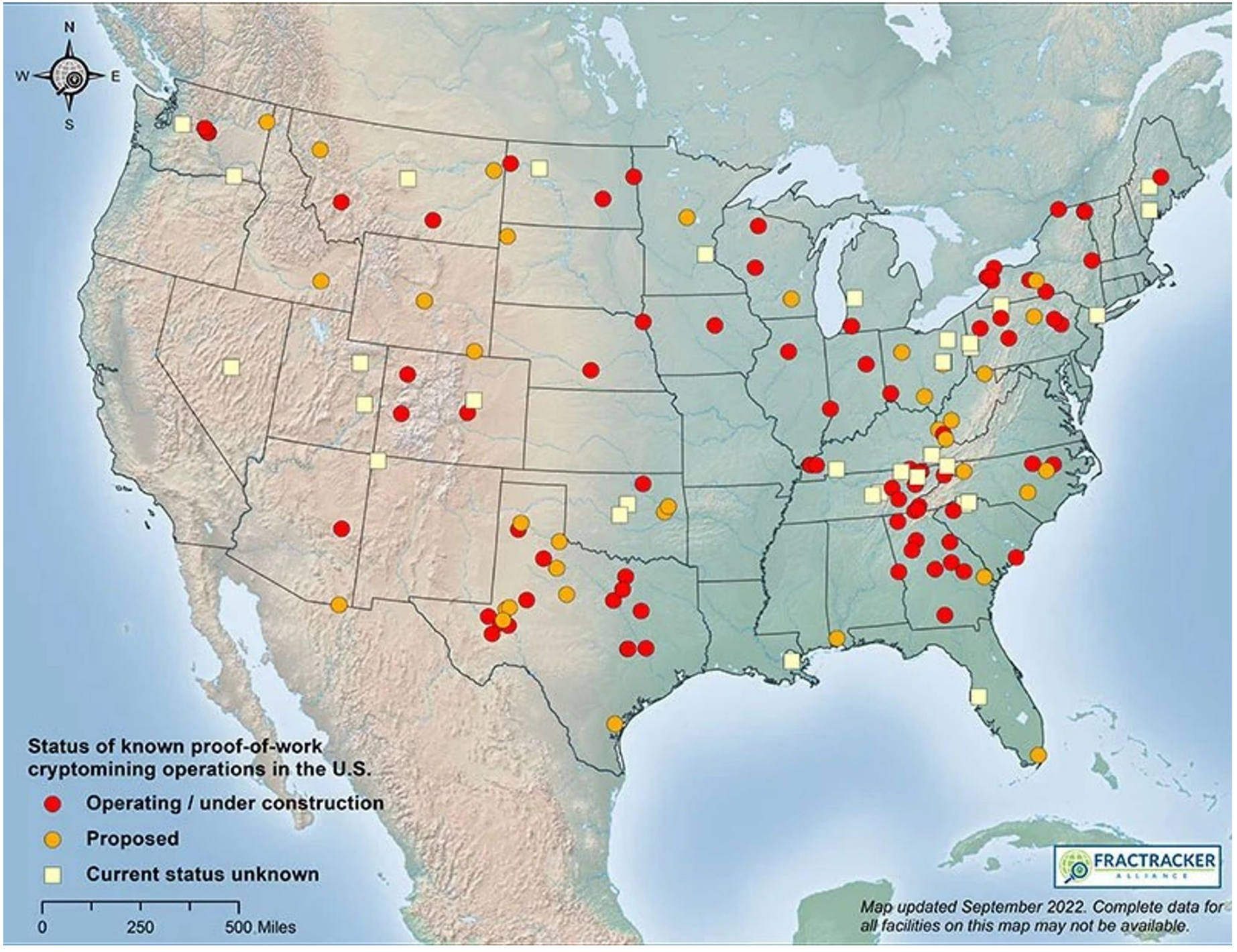
@j6sp5r on X/Twitter

Halving	Date	Block Reward
1	2009-01-03	50.000000
2	2012-11-28	25.000000
3	2016-07-09	12.500000
4	2020-05-11	6.250000
5	2024-05-08	3.125000
6	2028-05-05	1.562500
7	2032-05-03	0.781250
8	2036-04-30	0.390625
9	2040-04-27	0.195312
10	2044-04-25	0.097656
11	2048-04-22	0.048828
12	2052-04-19	0.024414
13	2056-04-17	0.012207
14	2060-04-14	0.006104


Evolution of country share
Share of global hashrate (monthly average)
100%
75%
50%
25%
0%
Sep '19
Jan '20
May '20
Sep '20
Jan '21
May '21
Sep '21
Jan '22
Mainland China
Other
Russian Federation
United States
Malaysia
Iran, Islamic Rep.
Kazakhstan
Canada
Germany
Ireland

The Chain Bulletin | **Bitcoin Mining Map**




N
W
E
S
Status of known proof-of-work cryptomining operations in the U.S.
Operating / under construction
Proposed
Current status unknown
0
250
500 Miles
FRACTRACKER ALLIANCE
Map updated September 2022. Complete data for all facilities on this map may not be available.

Bitcoin over time