

฿฿฿

฿฿

฿

Bitcoin Puzzle



Alexander Thurn  
Software-Entwickler  
alex@feuerware.com



← → ⌛ beatthehodler.feuerware.com ⭐

# Beat the HODLer

2014 0%	2015 0%	2016 0%	2017 0%	2018 0%
2019 0%	2020 0%	2021 0%	2022 0%	2023 0%
2024 0%	17-20 0%	21-24 0%	14-24 0%	BTC 0%

?

github.com/alexanderthurn/beatthehodler

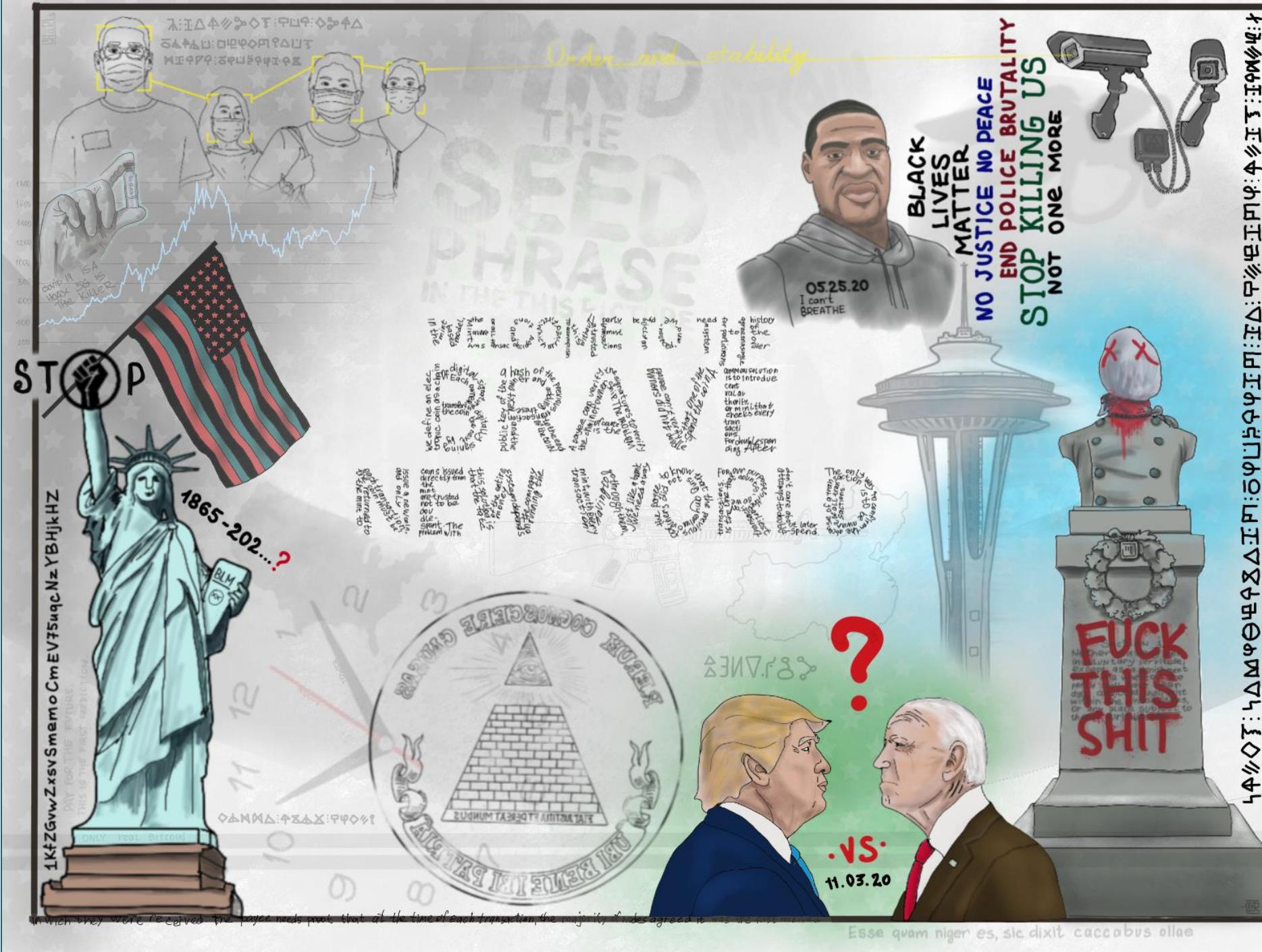
# Bitcoin Puzzle(s)

- 0,2 BTC Bildpuzzle
- 5 BTC Schnitzeljagd
- “**1000 BTC-Challenge**”
- Viele weitere Puzzles



# 0.2 BTC Puzzle

“The seedphrase  
is in the picture”



# Hinweise 0.2 BTC

<https://mempool.space/address/1KfZGvwZxsvSmemoCmEV75uqcNzYBHjkHZ>

## Hinweise zur Entschlüsselung

- 'Moon' (Mond) und 'Tower' (Turm) befinden sich auf den **Zeigern der Uhr**.
- 'Food' (Essen) befindet sich auf der **Seattle Space Needle**.
- 'Breathe' (Atmen) befindet sich auf **George Floyds Brust** sowie auf dem **Hals der Statue**.
- **Rune 1 (Oben links)** ist auf Russisch: "Я надеюсь что сюда будут присыпать много биткоинов" und bedeutet übersetzt: "**Ich hoffe, dass viele Bitcoins hierher geschickt werden.**"
- **Rune 2 (Unten links)** ist auf Russisch: "Сумма двух чисел" und bedeutet übersetzt: "**Summe von zwei Zahlen.**"
- **Rune 3 (Über Trump)** ist in Bills Chiffre und bedeutet übersetzt: "**Dienstag**".
- **Rune 4 (Lang, rechts)** ist auf Russisch: "Здесь зашифрованы биткоины на чёрный день номер X" und bedeutet übersetzt: "**Hier sind verschlüsselte Bitcoins für einen verregneten Tag Nummer X.**"
- 'This' (Dies/Dieses) ist wahrscheinlich ein **Seed-Wort**, da es in "This is the first prediction" (Dies ist die erste Vorhersage), "Fuck this shit" und "Find the seed phrase in the this picture" (Finde die Seed-Phrase in diesem Bild) wiederholt wird.
- **'Subject'** (Subjekt/Thema) ist auf der **Statue rechts unterstrichen**.
- Mithilfe von Forensically oder Photoshop enthüllt der Sockel der Freiheitsstatue "**Only Bitcoin**" unter "**Only real Bitcoin**", was wahrscheinlich bedeutet, dass '**Real**' (Echt) ein **Seed-Wort** ist.
- Das Latein unten links bezieht sich auf "**The Pot Calling The Kettle Black**" (Der Topf nennt den Kessel schwarz), wobei '**Black**' (Schwarz) auch in Bezügen zur Black Lives Matter-Bewegung wiederholt wird, daher ist es wahrscheinlich ein **weiteres Wort**.

~~5~~ 1.25  
BTC  
Puzzle



GSMG.IO 5 BTC PUZZLE CHALLENGE



[1GSMG1JC9wtdSwfwApgj2xcmJPawx7prBe](https://mempool.space/address/1GSMG1JC9wtdSwfwApgj2xcmJPawx7prBe)

[https://mempool.space/address/  
1GSMG1JC9wtdSwfwApgj2xcmJP  
Awx7prBe](https://mempool.space/address/1GSMG1JC9wtdSwfwApgj2xcmJPawx7prBe)

# 1000 BTC-Challenge

- 989,04 BTC
- ~~256~~ 160 Teil-Puzzles
- 82 gelöst (73 BTC gewonnen bisher, 10.11.2025)
- Autor unbekannt



15.01.2015

Tx mit  
32,896 BTC und  
256 Outputs

<https://mempool.space/tx/08389f34c98c606322740c0be6a7125d9860bb8d5cb182c02f98461e5fa6cd15>

**BurtW**  
Legendary  


December 28, 2015, 03:28:19 PM

---

<https://blockchain.info/tx/08389f34c98c606322740c0be6a7125d986>

Does look like someone placed an interesting puzzle in the blockchain for us.

It appears to me to be a game of some sort: if you crack the sequence you can get the BTC.

# Technik



## Private Key

- Damit kann man was überweisen



PRIVATE KEY

## Public Key:

- Damit kann man sehen was drauf ist



## Wallet-Adresse:

- Damit kann man sehen was drauf ist



ADDRESS

## Private Key

- WIF-Komprimiert:  
KwDiBf89QgGbjEhKnhXJuH7LrciVrZi3qYjgd9M7rFU73sVHnoWn
- Legacy (WIF-Unkomprimiert):  
5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreAnchuDf
- Adresse:
  - Legacy: 1BgGZ9tcN4rm9KBzDn7KprQz87SZ26SAMH
  - Segwit (P2SH): 3JvL6Ymt8MVWiCNHC7oWU6nLeHNJKLZGLN
  - Segwit (P2WPKH): bc1qw508d6qejaxtdg4y5r3zarvary0c5xw7kv8f3t4

# Private Key

WIF-Komprimiert:  
KwDiBf89QgGbjEhKnhXJuH7L  
rciVrZi3qYjgd9M7rFU73sVHno  
Wn



Private Key

Zahl

1 bis  $2^{256}$



*1 bis*

115.792.089.237.

316.195.423.570.

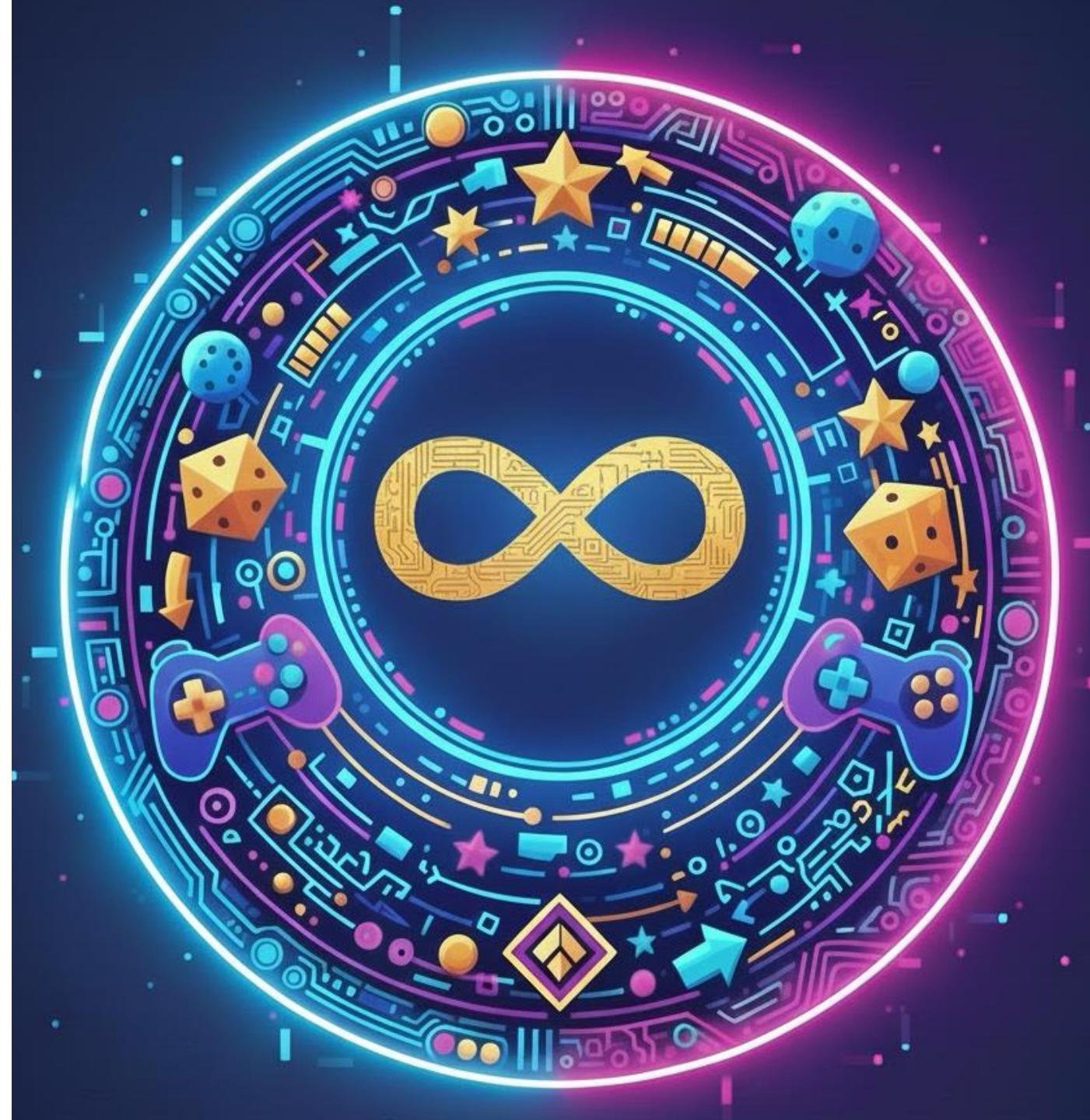
985.008.687.907.

853.269.984.665.

640.564.039.457.

584.007.913.129.

639.936



00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000

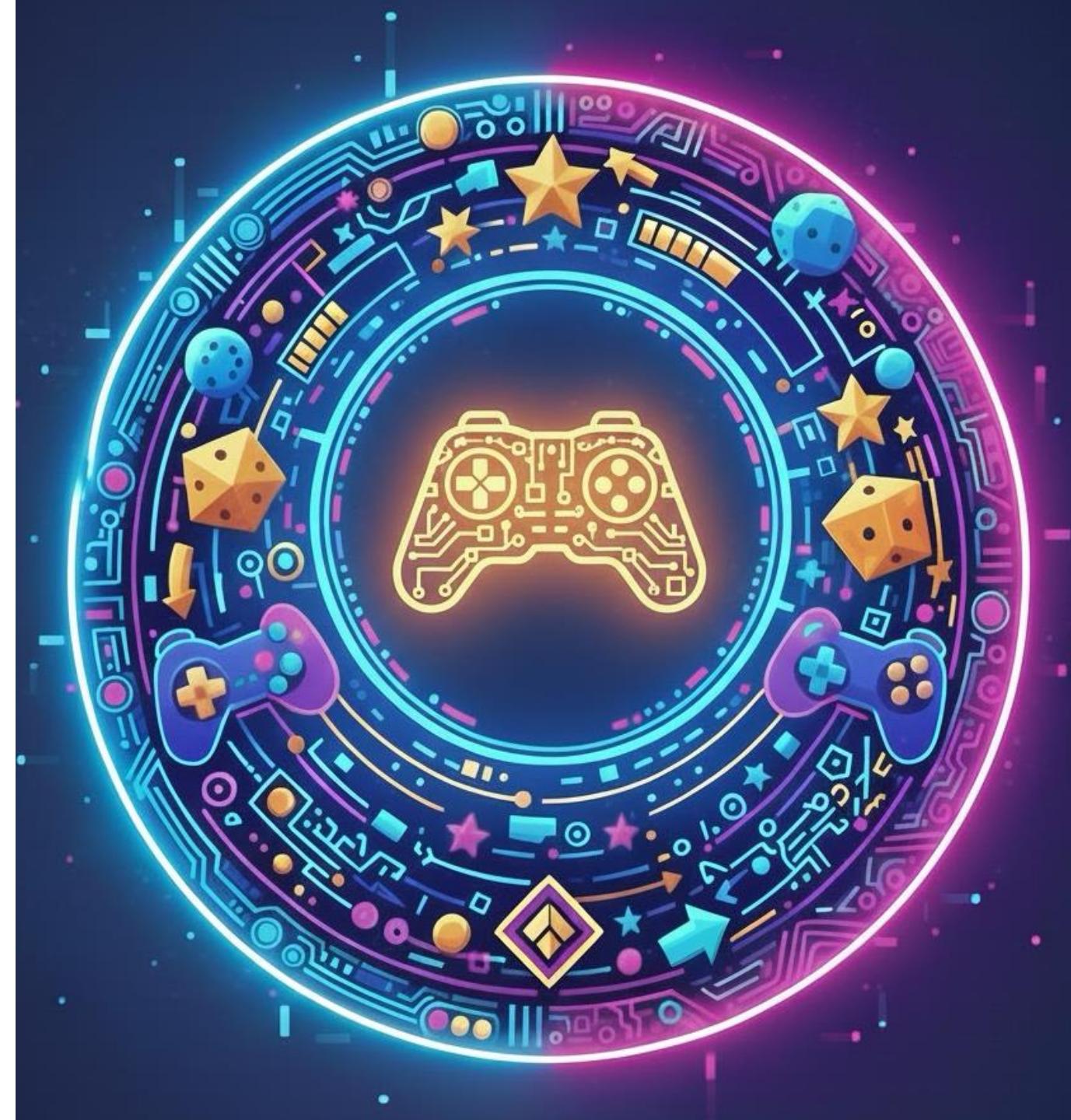
00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000001

# Spiel



28.12.2015

**Bulista** (OP)

Member



For example:

Address 2:

KwDiBf89QgGbjEhKnhXJuH7LrciVrZi3qYjgd9M7rFU74sHUHy8S  
1CUNEBjYrCn2y1SdiUMohaKUi4wpP326Lb

BigInteger PVK value: 3

Hex PVK value: 3

28.12.2015

Address 1, pvk decimal value: 1  
Address 2, pvk decimal value: 3  
Address 3, pvk decimal value: 7  
Address 4, pvk decimal value: 8  
Address 5, pvk decimal value: 21  
Address 6, pvk decimal value: 49  
Address 7, pvk decimal value: 76

# Bits



# Ziel-Adressen bekannt

<https://mempool.space/tx/08389f34c98c606322740c0be6a7125d9860bb8d5cb182c02f98461e5fa6cd15>

mempool.space		Explore the full Bitcoin ecosystem	🔍		
⚡	1Czoy8xtddvcGrEhUUCZDQ9QqdRfKh697F	32.90000000 BTC	↗		
1BgGZ9tcN4rm9KBzDn7KprQz87SZ26SAMH	0.00100000 BTC	↗	1CUNEBjYrCn2y1SdiUMohaKUi4wpP326Lb	0.00200000 BTC	↗
19ZewH8Kk1PDbSNdJ97FP4EiCjTRaZMZQA	0.00300000 BTC	↗	1EhqbyUMvvs7BfL8goY6qcPbD6YKfPqb7e	0.00400000 BTC	↗
1E6NuFjCi27W5zoXg8TRdcSRq84zJeBW3k	0.00500000 BTC	↗	1PitScNLyp2HCygzadCh7FveTnfmpPbfp8	0.00600000 BTC	↗
1McVt1vMtCC7yn5b9wgX1833yCcLXzueeC	0.00700000 BTC	↗	1M92tSqNmQLYw33fuBvjmeadirh1ysMBxK	0.00800000 BTC	↗
1CQFwcjw1dwhtkVWBttNLDtql7ivBonGPV	0.00900000 BTC	↗	1LeBZP5QCwwgXRtmUVTVrraqPUokyLHqe	0.01000000 BTC	↗
1PgQLmst3Z314JrQn5TNiys8Hc38TcXJu	0.01100000 BTC	↗	1DBaumZxUkM4qMQRt2LVWyFJq5kDtSZQot	0.01200000 BTC	↗
<a href="#">Show all (244 remaining)</a>					

# Brute Force

Finde den Private Key für eine bekannte Bitcoin Adresse mit n Bit Sicherheit

FOR a=1 TO  $2^n$ :

1.b = SECP256k1(a)

2.c = SHA256(b)

3.d = RIPEMD160(c)

4.e = '\x00' + d

5.f = SHA256(SHA256(e))

6.g = BASE58\_ENCODE(e + the first 4 bytes of f)

[https://  
btcpuzzle.info  
/de/puzzle](https://btcpuzzle.info/de/puzzle)

# Spiel

- <https://btcpuzzle.info/de/tools/visual-puzzle-hunter?page=5>

Visueller Puzzlejäger - BTC Puzzles

btcpuzzle.info/de/tool... +

256-Bit Bitcoin privater Schlüsselerzeuger

(Alle Schlüsse)

Löschen Zufällig

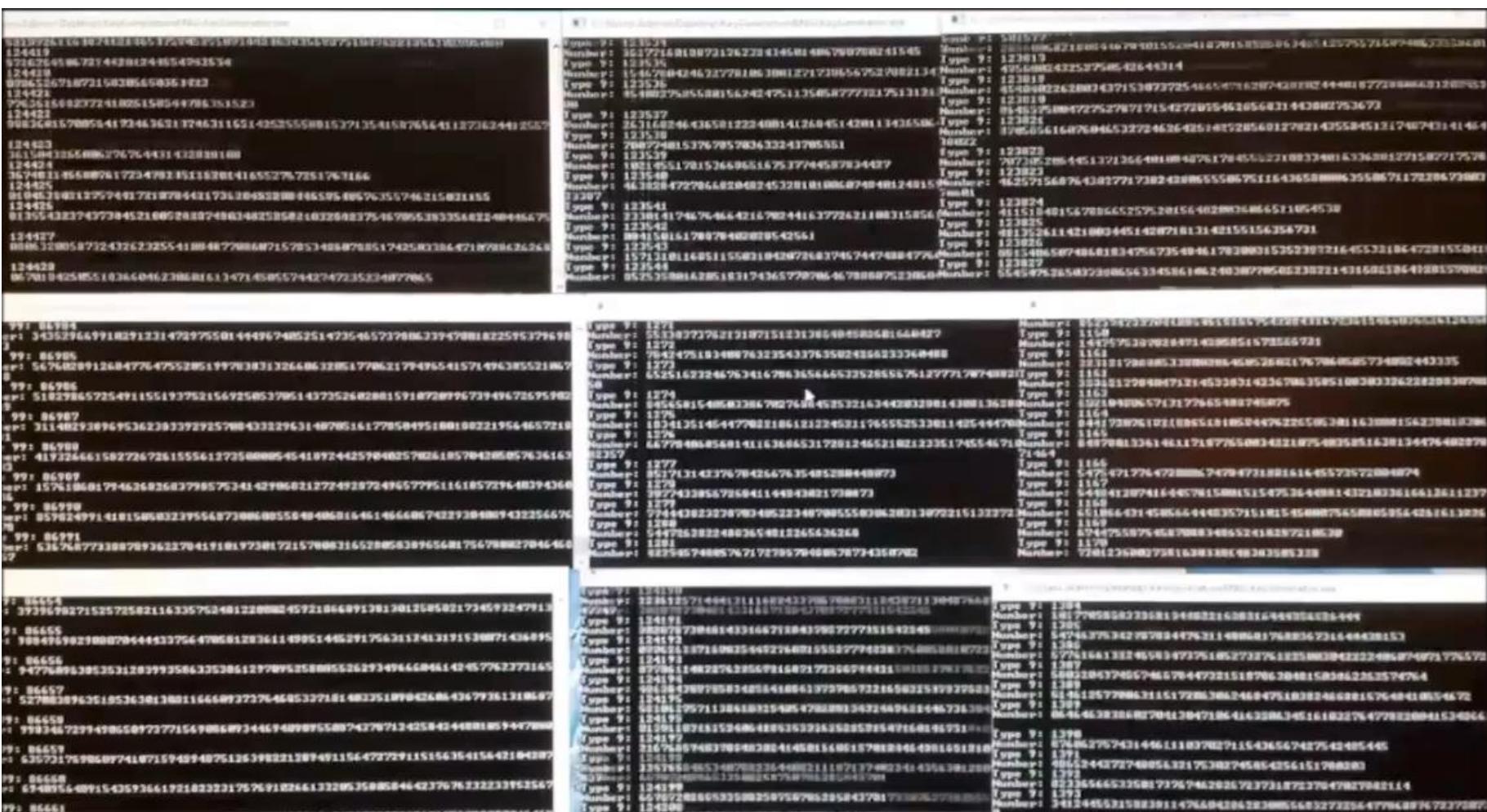
Daten teilen

Privacy - Terms

27.12.2015

## Bullista:

# Private-Key- Brute-Force- Programm



GPU-Benchmark für Bitcoin-Puzzle x +

btcpuzzle.info/de/benchmark

**BTCPUZZLE**

Puzzles Schlüssel Cloud Search Werkzeuge Andere bc1q...xj7a

Swap Spend \$87033.99

[IMPORTANT] All clients must be updated to the new version! 1/4

# GPU-Benchmark für Bitcoin-Puzzle

Entdecken Sie die Bereichs-/Range-Scan-Leistung von Grafikkarten.

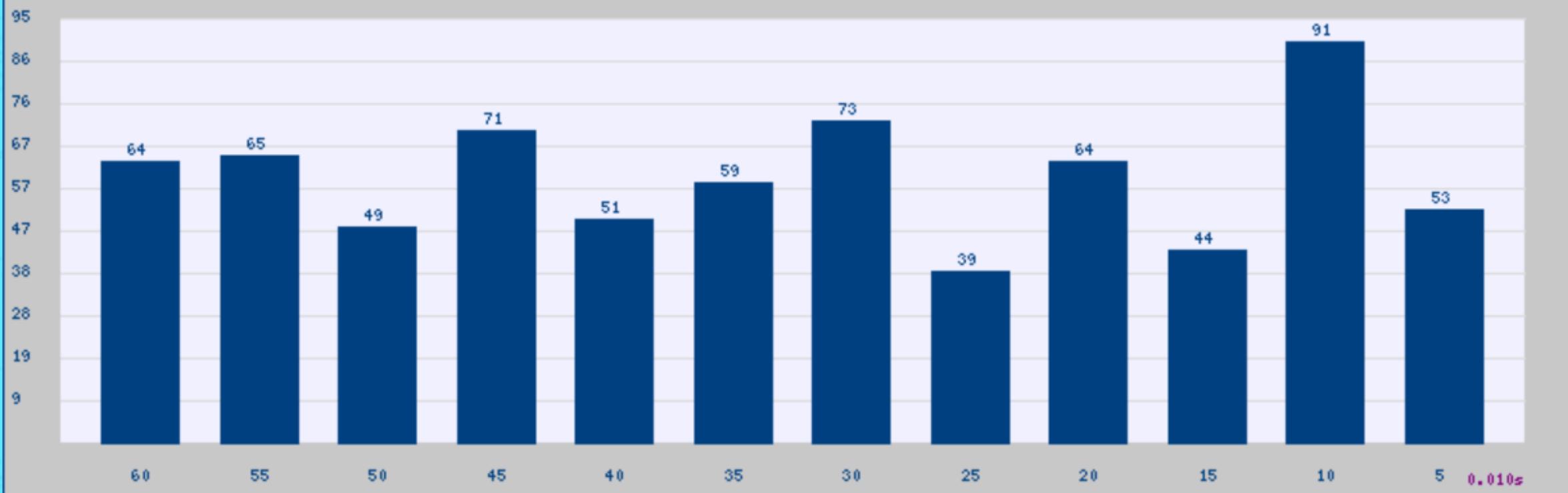
#	Geschwindigkeit/(sek)
RTX 5090	<b>8.06 Bkeys /sek</b>
RTX 4090	<b>5.96 Bkeys /sek</b>
RTX 4090 D	<b>4.64 Bkeys /sek</b>
RTX 5080	<b>4.52 Bkeys /sek</b>
RTX 4080 SUPER	<b>3.69 Bkeys /sek</b>
RTX 4080	<b>3.49 Bkeys /sek</b>

Privacy - Terms

Login

Don't have an account? Sign up now.

Last 60 Minutes (719 ranges, 790.55 Trillion Keys, 219.60 BK/s)



This site was created to collectively solve bit 66 of the Bitcoin puzzle challenge.

# Historie

- 11.07.2017
  - Umschichtung #161 - #256 in niedrigere Ranges
- 31.05.2019
  - Public Key exponiert für #65, #70, #75, #80, #85, #90, #95, #100, #105, #110, #115, #120, #125, #130, #135, #140, #145, #150, #155, #160
- 16.04.2023
  - Ungelöste Preisgelder 100x.
    - Puzzle #69 hat jetzt 6,9 BTC statt 0,069 BTC
    - Puzzle #160 hat 16 BTC

Bitcoin Puzzle Liste - BTC Pu x +

btcpuzzle.info/de/puzzle

Puzzles Schlüssel Cloud Search Werkzeuge Andere bc1q...xj7a

**Puzzle 68**  $(2^{67}) \dots (2^{68})$  %49

1MVDYgVaSN6iKKEsbzRUAYFrYJadLYZvvZ **Gelöst**  
T 00bebb3940cd0fc1491

**Letzter Schnappschuss**

Scan [1] Scan [2]

**Puzzle 69**  $(2^{68}) \dots (2^{69})$  %0

19vkiEajfhuz8bs8Zu2jgmC6oqZbWqhkhG **Gelöst**  
T 00101d83275fb2bc7e0c

**Letzter Schnappschuss**

Scan [1] Scan [2]

**Puzzle 70**  $(2^{69}) \dots (2^{70})$  %64

19YZECXj3SxEZMoUeJ1yiPsw8xANe7M7QR **Gelöst**  
T 00349b84b6431a6c4ef1

Scan [1] Scan [2]

**Puzzle 71**  $(2^{70}) \dots (2^{71})$

1PWo3JeB9jrGwfHDNpdGK54CRas7fsVzXU **Ungelöst**  
**Q Dem Pool beitreten**

Scan [1] Scan [2]

**Puzzle 72**  $(2^{71}) \dots (2^{72})$

1JTK7s9YVVywmf5XUH7RNhHJH1LshCaRFR **Ungelöst**  
**Q Dem Pool beitreten**

Scan [1] Scan [2]

**Puzzle 73**  $(2^{72}) \dots (2^{73})$

12VVRNPi4SJqqUTsp6FmqDqY5sGosDtysn4 **Ungelöst**  
**Q Dem Pool beitreten**

0BTC  
6.80032562BTC  
\$0.00 (27 txs)

0BTC  
6.90036533BTC  
\$0.00 (24 txs)

0BTC  
0.70071362BTC  
\$0.00 (7 txs)

7.10020628BTC  
0BTC  
\$618,025.81 (15 txs)

7.20014379BTC  
0BTC  
\$626,724.71 (6 txs)

7.30013849BTC  
0BTC  
\$635,428.58 (6 txs)

Privacy - Terms

# Public Key Exposure



Bitcoin Puzzle Liste - BTC Pu... +

btcpuzzle.info/de/puzzle

**BTCPUZZLE**

Puzzles   Schlüssel   Cloud Search   Werkzeuge   Andere ▾ bc1q...xj7a ▾

Puzzle 125 $(2^{124}) \dots (2^{125})$	%77	1PXAyUB8ZoH3WD8n5zoAthYjN15yN5CVq5 <span style="color: green;">Gelöst</span>	0BTC 12.50004706BTC \$0.00 (8 txs)
Puzzle 126 $(2^{125}) \dots (2^{126})$		1AWCLZAjKbV1P7AHvaPNCKiB7ZWVDMxFiz <span style="color: green;">Ungelöst</span>	12.6BTC 0BTC \$1,096,746.34 (3 txs)
Puzzle 127 $(2^{126}) \dots (2^{127})$		1G6EFyBRU86sThN3SSt3GrHu1sA7w7nzi4 <span style="color: green;">Ungelöst</span>	12.7BTC 0BTC \$1,105,450.67 (3 txs)
Puzzle 128 $(2^{127}) \dots (2^{128})$		1MZ2L1gFrCtkkn6DnTT2e4PFUTHw9gNwaj <span style="color: green;">Ungelöst</span>	12.8BTC 0BTC \$1,114,155.01 (3 txs)
Puzzle 129 $(2^{128}) \dots (2^{129})$		1Hz3uv3nNzzBVMXLGadCucgjiCs5W9vaGz <span style="color: green;">Ungelöst</span>	12.9BTC 0BTC \$1,122,859.34 (3 txs)
Puzzle 130 $(2^{129}) \dots (2^{130})$	%62	1Fo65akq8s8iquMt6weF1rku1moWVEd5Ua <span style="color: green;">Gelöst</span>	0BTC 13.00013257BTC \$0.00 (15 txs)
Puzzle 131 $(2^{130}) \dots (2^{131})$		16zRPnT8znwq42q7XeMkZUhb1bKqgRogyy <span style="color: green;">Ungelöst</span>	13.1BTC 0BTC \$1,140,268.02 (3 txs)

Scan [1] Scan [2]   Scan [1] Scan [2]

Privacy - Terms

# Warum das Ganze?



$$2^1 = 2$$

$$2^2 = 4$$

$$2^3 = 8$$

$$2^4 = 16$$

$$2^5 = 32$$

$$2^6 = 64$$

$$2^7 = 128$$

Wieviel Bits  
sind heute  
**SICHER?**

$2^{250}$

$2^{251}$

$2^{252}$

$2^{253}$

$2^{254}$

$2^{255}$

$2^{256}$

Wie sicher ist  
Bitcoin?

$$2^1 = 2$$

$$2^2 = 4$$

$$2^3 = 8$$

$$2^4 = 16$$

$$2^5 = 32$$

$$2^6 = 64$$

$$2^7 = 128$$

Wieviel Bits  
sind heute  
**UNSICHER?**

Und wie  
schnell ging  
es?

$$2^{250}$$

$$2^{251}$$

$$2^{252}$$

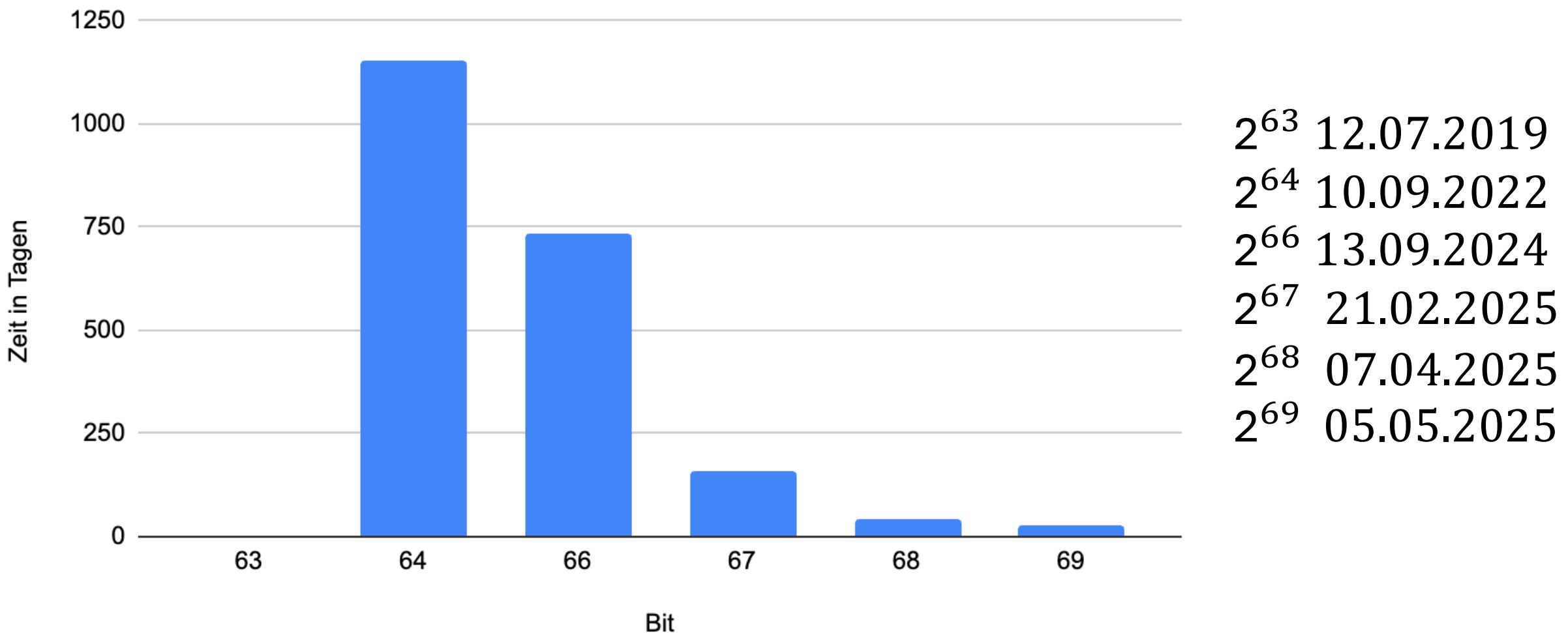
$$2^{253}$$

$$2^{254}$$

$$2^{255}$$

$$2^{256}$$

## Dauer zur Lösung seit vorherigem



Vielen Dank  
für die  
Aufmerksamkeit

Vortrag als PDF

