DAS ETHEREUM NETZWERK UND SEINE MONETÄRE STRATEGIEN

rfl

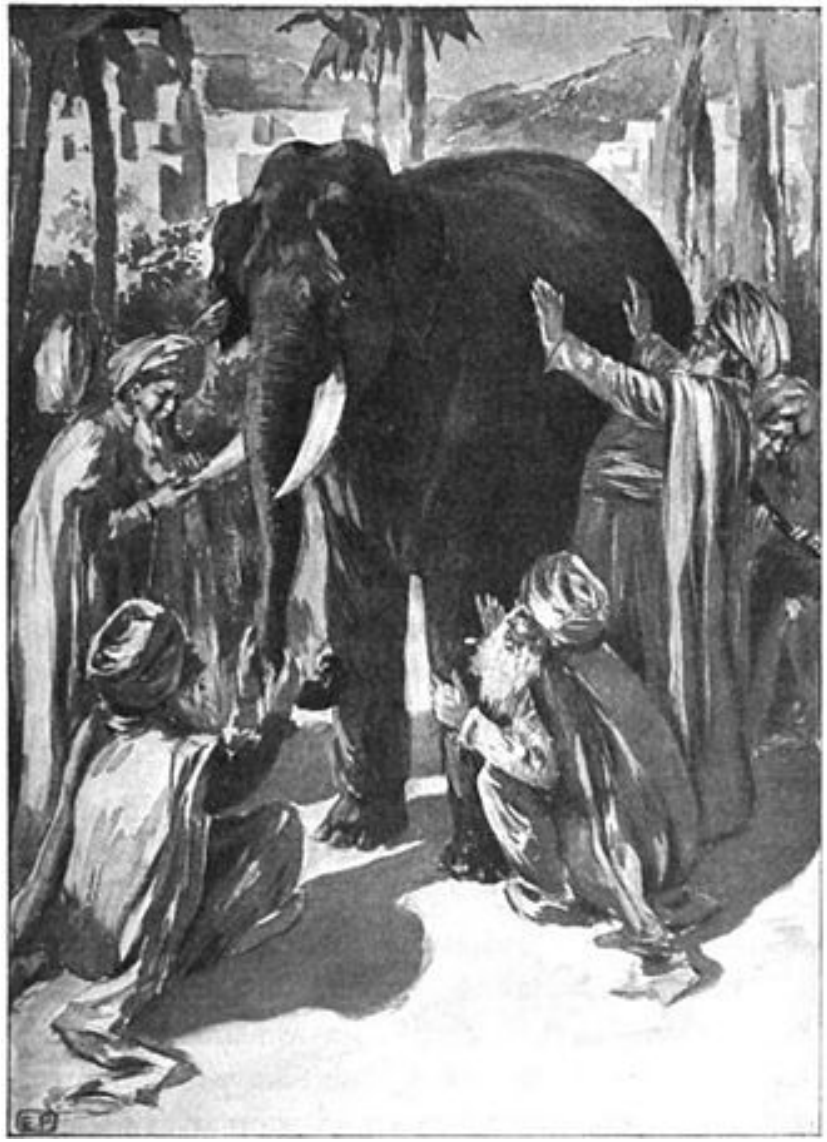
somewhere

2024-11-03

Folien

https://code.flipdot.org/rfl/talks

WAS IST ETHEREUM?



https://en.wikipedia.org/wiki/Blind_men_and_an_elephant

ETHEREUM IST ...

- eine Idee
- ein Soziales Netzwerk
- eine Blockchain
- ein Geld des Internets

ETHEREUM IST ...

- eine Idee
- ein Soziales Netzwerk
- eine Blockchain
- ein Geld des Internets

ETHEREUM IST ...

- eine Idee
- ein Soziales Netzwerk
- eine Blockchain
- ein Geld des Internets

ETHEREUM IST ...

- eine Idee
- ein Soziales Netzwerk
- eine Blockchain
- ein Geld des Internets

ETHEREUM IST EINE IDEE

Anfänge:

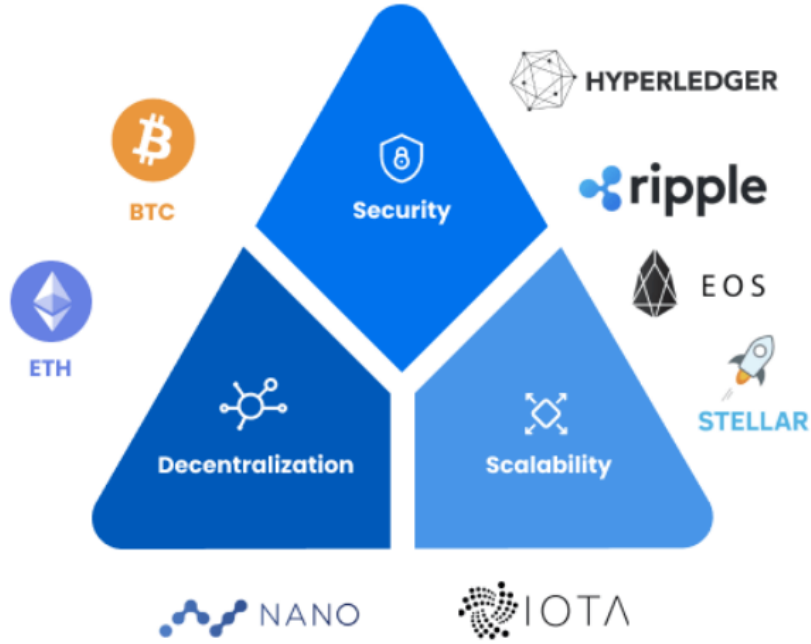
- Bitcoin (2009)
- Whitepaper (2013)
- Stiftung Ethereum (2014)
- Genesisblock (2015)

Ziele:

- Dezentralisierung
- Unzensierbarkeit
- Transparenz
- Benutzbarkeit

Ziele:

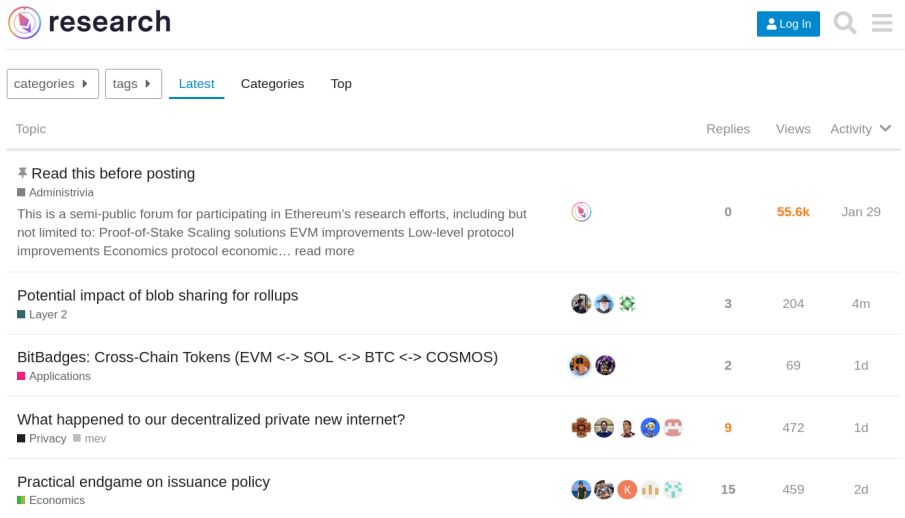
- Dezentralisierung
- Unzensierbarkeit
- Transparenz
- Benutzbarkeit



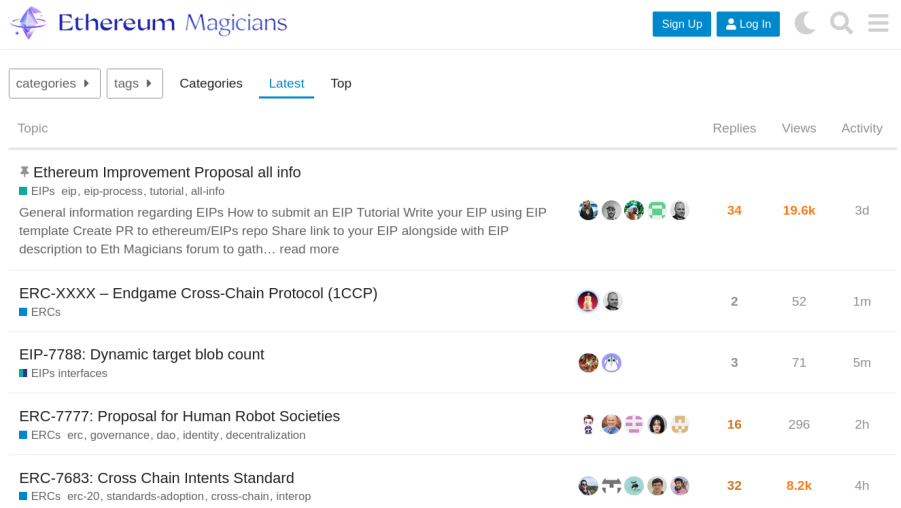
https://learn.swyftx.com/blockchain/blockchain-trilemma

ETHEREUM IST EIN SOZIALES NETZWERK

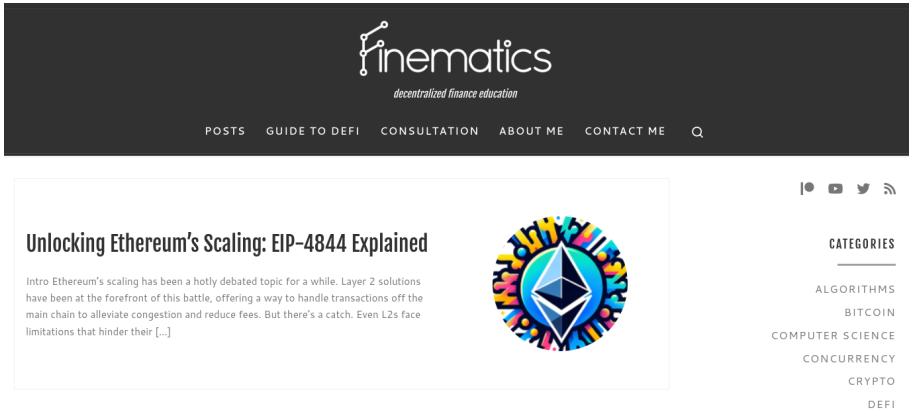
- Foren
- Blogs
- Social-Media Beiträge
- Konferenzen
- Verbesserungsdiskussionen



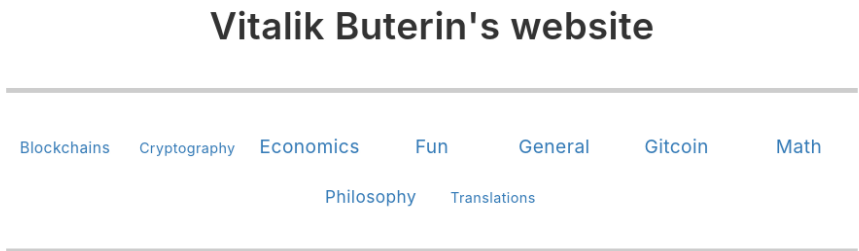
- Foren
- Blogs
- Social-Media Beiträge
- Konferenzen
- Verbesserungsdiskussionen



- Foren
- Blogs
- Social-Media Beiträge
- Konferenzen
- Verbesserungsdiskussionen



- Foren
- Blogs
- Social-Media Beiträge
- Konferenzen
- Verbesserungsdiskussionen



HAUPTAKTEURE

- Kern-Entwicklerteam (offen nach Eignungsphase)
- Podcaster
- Benutzer durch Social-Media Beiträge
- Ethereum Stiftung (eher selten)

VERBESSERUNGSDISKUSSIONEN

- engl. EIP = Ethereum Improvement Proposal
- Variabler Umfang, kann alles Mögliche enthalten
  - von utopischen Visionen
  - über Mathematischen Beweise
  - bis zu ausführlichen Vorbereitung der Änderungen
- Diskussionen werden nahezu vollständig offen im Internet geführt
- Einigung unter den Hauptakteuren führt zur Änderung
- Mitunter auch nicht möglich, dann eventull Spaltung der Systeme

BEISPIEL

Standards Track: Core

EIP-1559: Fee market change for ETH 1.0 chain

Authors	Vitalik Buterin (@vbuterin), Eric Conner (@econoar), Rick Dudley (@AFDudley), Matthew Slipper (@mslipper), Ian Norden (@i-norden), Abdelhamid Bakhta (@abdelhamidbakhta)
Created	2019-04-13
Requires	EIP-2718, EIP-2930

Table of Contents

ETHEREUM IST EINE BLOCKCHAIN

COMPUTERCODE

- Unterschied zwischen Spezifikation und Anwendung
- es gibt nur eine Spezifikation, aber unzählige Anwendungen in den verschiedensten Programmiersprachen
- Anzahl der Programmierer der Spezifikationen < 100

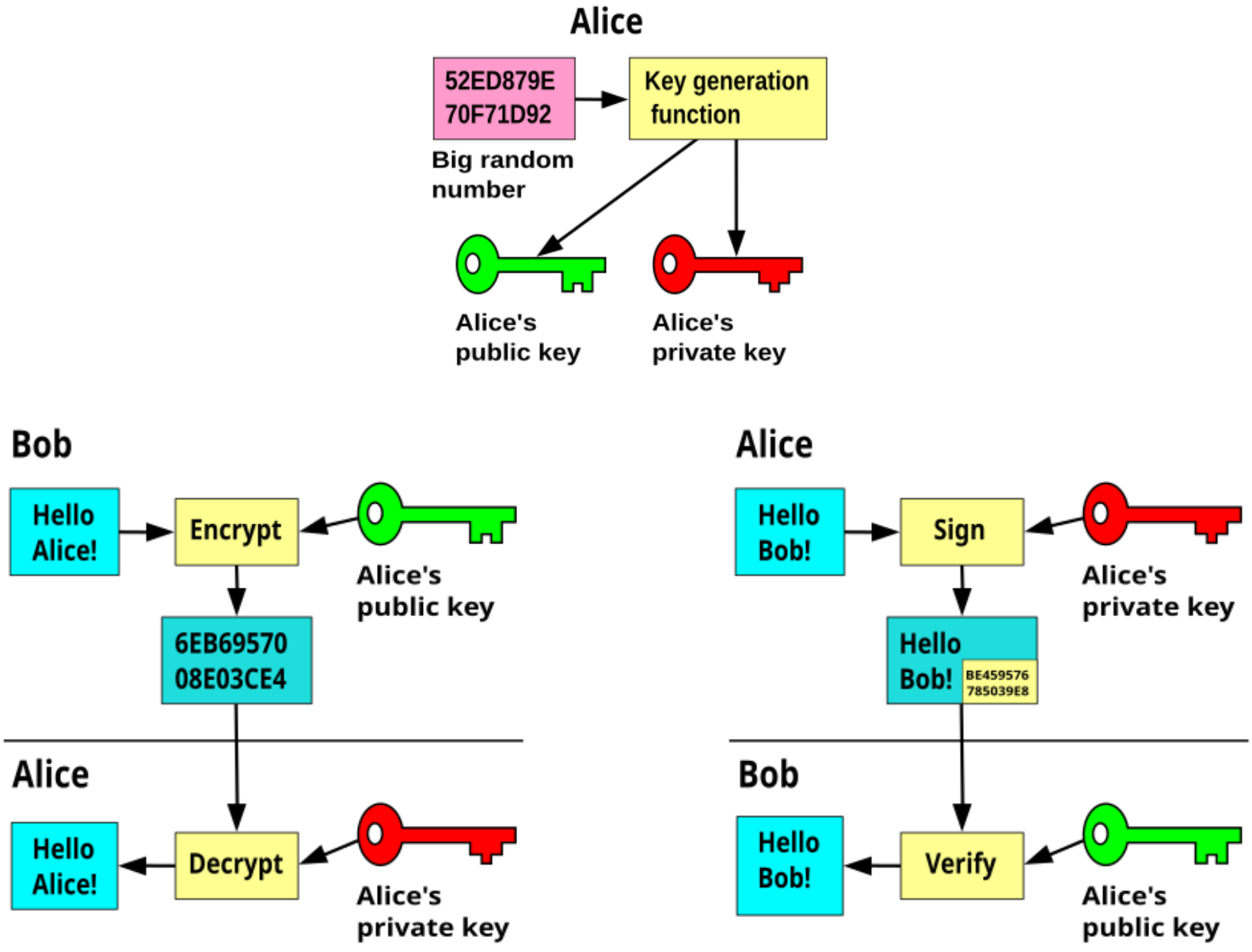
  `https://github.com/ethereum/consensus-specs`
- Anzahl der Programmierer der Anwendungen > 20000

  z.B. `https://github.com/ethereum/go-ethereum`
- Automatische Tests, ob Anwendungen die Spezifikationen erfüllen

Man will ...

- Zustände ausfallsicher speichern
- nur zulässige Änderungsvorgänge unfälschbar durchführen
- alles für Beobachter transparent nachvollziehbar

INTERLUDE: PUBLIC KEY KRYPTOGRAPHIE



https://en.wikipedia.org/wiki/Public-key_cryptography

LEDGER

- Sammlung von allen “Wer hat was?” Aussagen
- Adresse ist gleich öffentlicher Schlüssel
- Wallet verwaltet geheimen Schlüssel
- Nur Eigentümer des geheimen Schlüssels kann Transfer initialisieren

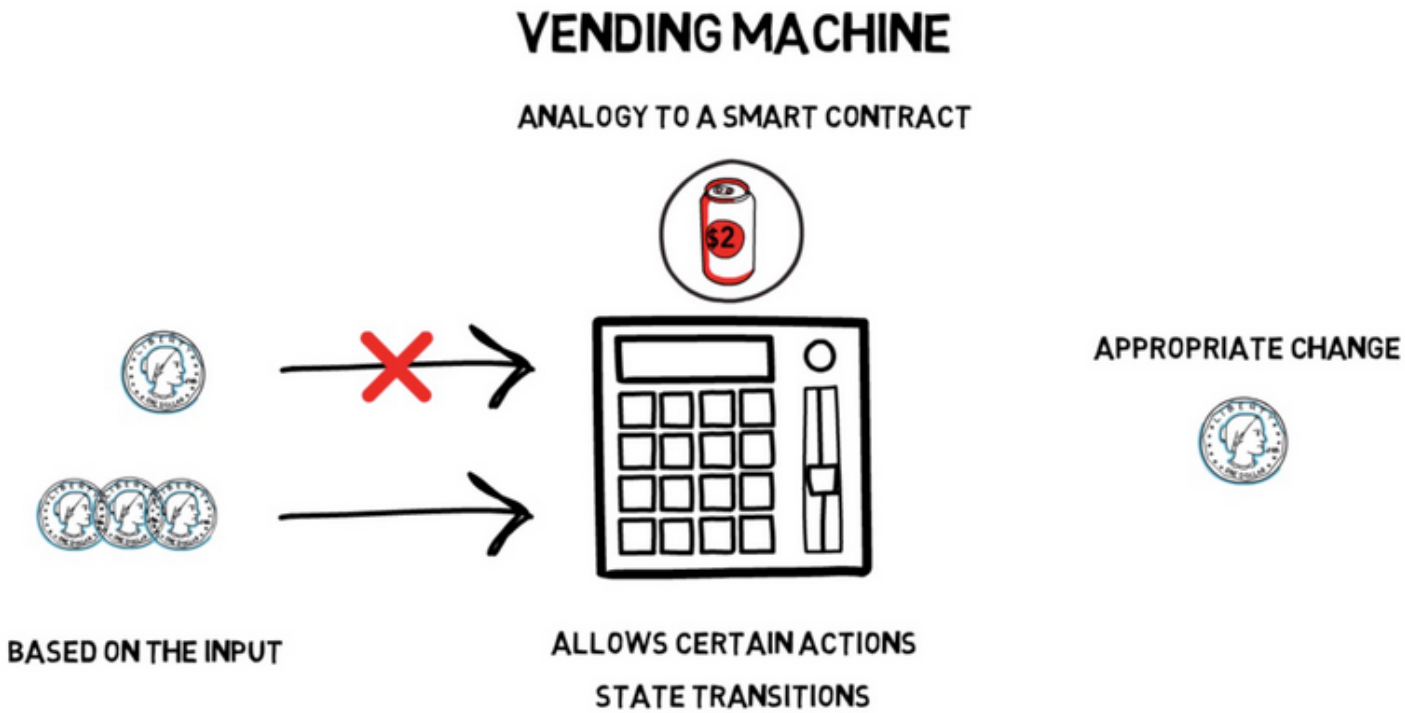
TRANSAKTIONEN

Statt Alice gibt Bob 5 Euro heißt es nun:


```
{
   "accessList":[ ⋯ ],
   "blockHash":"0x479c9dca8a806183261d7b3c2c69844a1a5cb3eae7e10b4d8298f3c6cf207346",
   "blockNumber":15499910,
   "chainId":"0x1",
   "from":"0x1ecc89fd4fc4ded8543204854ab4596aec69eb47",
   "gas":134434,
   "gasPrice":149358907014,
   "hash":"0x6582df4448ce1eb37b5c3365fe869ce43282eda92d78f2a6e0e7ad065deea081",
   "input":"0x0000001000000000000000000000000000000000000000000000000000000000d006824c000
   "maxFeePerGas":154096481318,
   "maxPriorityFeePerGas":138636083893,
   "nonce":4205,
   "r":"0x423ff6d0f848e83b7b46572956e28a4b72ceb8b10f6f68d9b378e0e0de9f1b94",
   "s":"0x712e01d03c25d8f75179e9232b56d45f943a05f7f51ee318b7ad1946806ada4",
   "to":"0xbeefbabeea323f07c59926295205d3b7a17e8638",
   "transactionIndex":2,
   "type":"0x2",
   "v":"0x0",
   "value":15499910
}
```

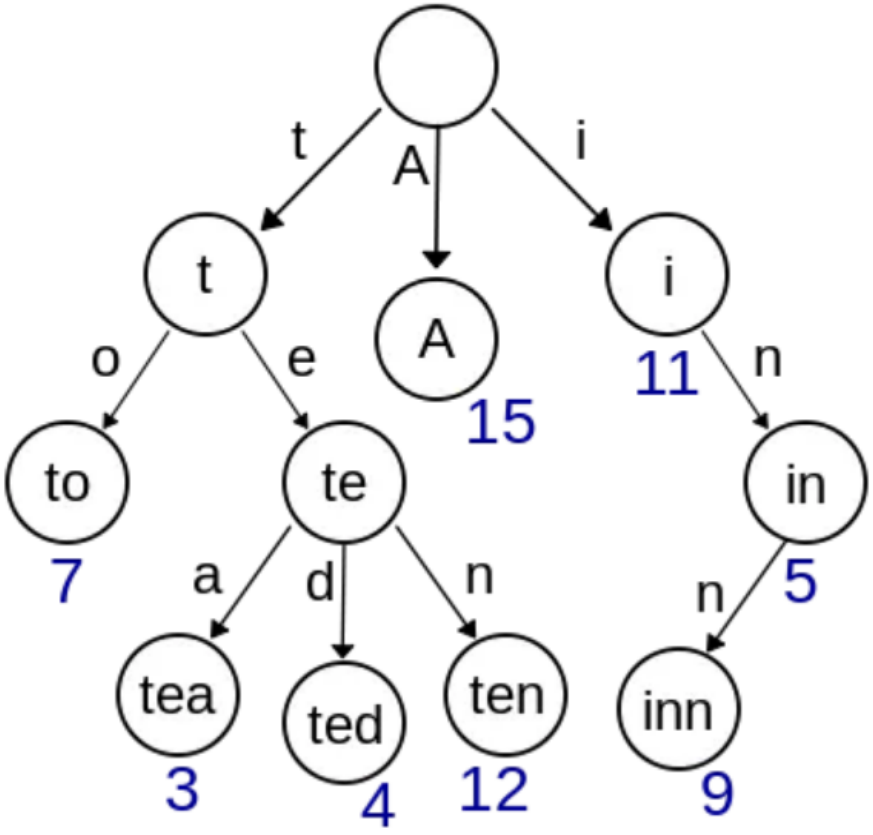

https://inevitableeth.com/home/ethereum/blockchain/transaction

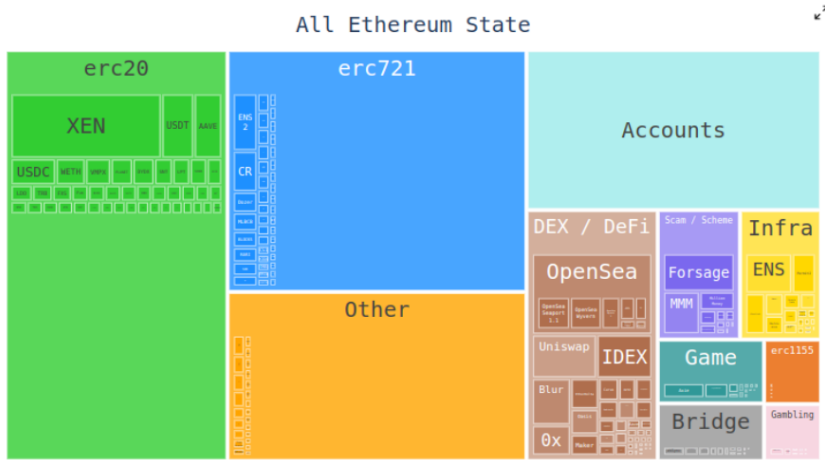
SMART CONTRACTS



https://finematics.com/smart-contracts-explained/

STORAGE





https://vitalik.eth.limo/general/2024/10/23/futures4.html

https://medium.com/codechain/modified-merkle-patricia-trie-how-ethereum-saves-a-state-e6d7555

EVM

- EVM = ethereum virtual machine
- EVM ist Turing-vollständig
- Halting-Problem ist unentscheidbar

```
stored_num: int128

@external
def store_num(num: int128):
  self.stored_num = num

@external
def get_num() -> int128:
  return self.stored_num

@public
def perform_operations(x: int128, y: int128) -> (int128, int128, int
   sum = x + y
  difference = x - y
  product = x * y
  return (sum, difference, product)

@public
def compare_values(x: int128, y: int128) -> bool:
  return x > y
```

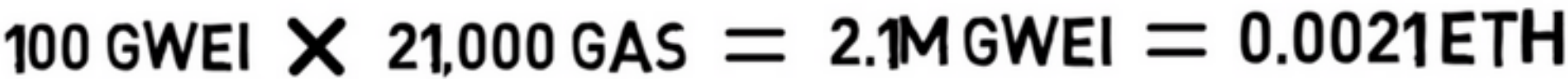
https://whiteboardcrypto.com/vyper-signed-integers/

GAS

- Synthetisches Verbrauchsgut
- verhindert nicht-endende Berechnungen
- Jeder Berechnungsschritt kostet Gas
- Rückabwicklung bei unzureichender Vorsorge
- Entkopplung Transaktionskosten von ETH-Preis

GAS

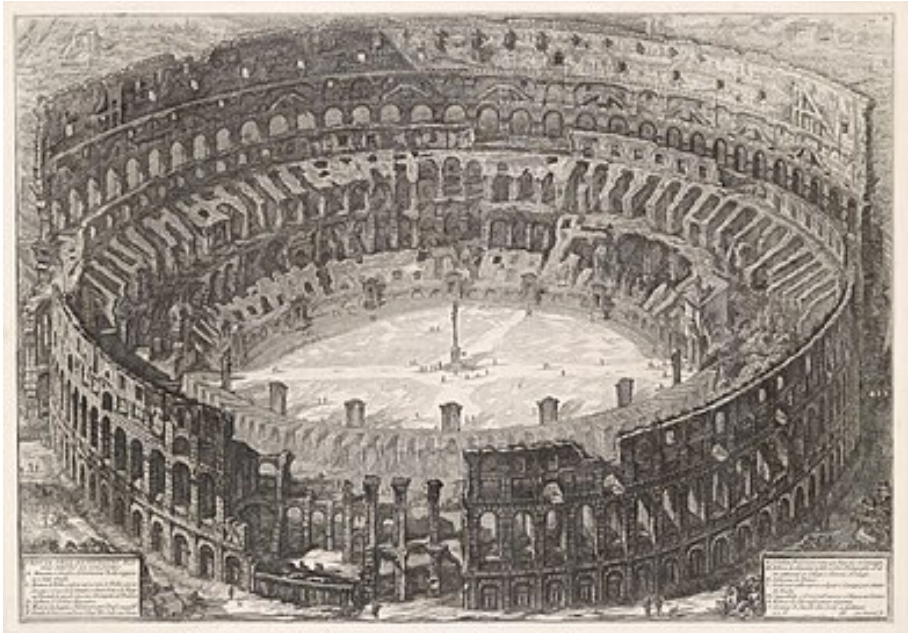
- Synthetisches Verbrauchsgut
- verhindert nicht-endende Berechnungen
- Jeder Berechnungsschritt kostet Gas
- Rückabwicklung bei unzureichender Vorsorge
- Entkopplung Transaktionskosten von ETH-Preis



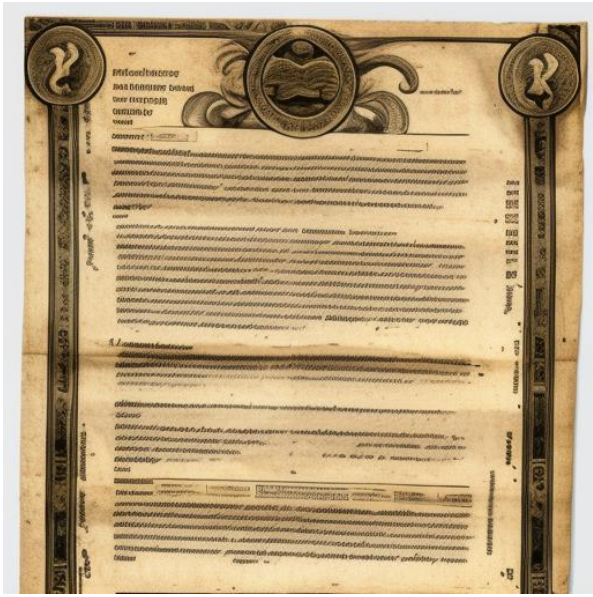
https://finematics.com/what-is-gas-ethereum-high-transaction-fees-explained/

ETHEREUM IST EIN GELD DES INTERNETS (?)

PROOF OF STAKE (- METAPHER)



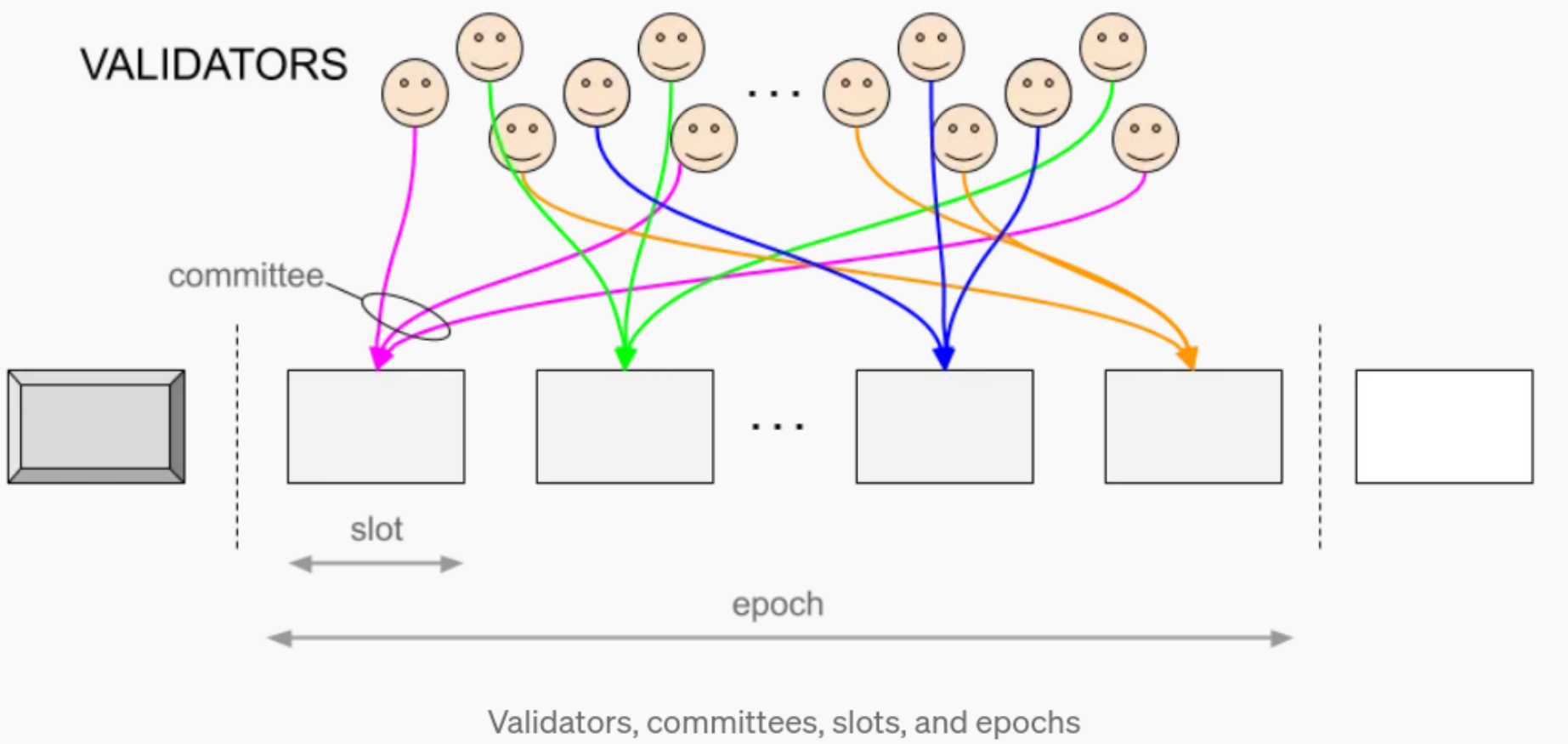
https://en.wikipedia.org/wiki/Colosseum



https://picsart.com/ai-image-generator/

prompt: an ancient looking scroll for obtaining the rights of a validator in a proof of stake system

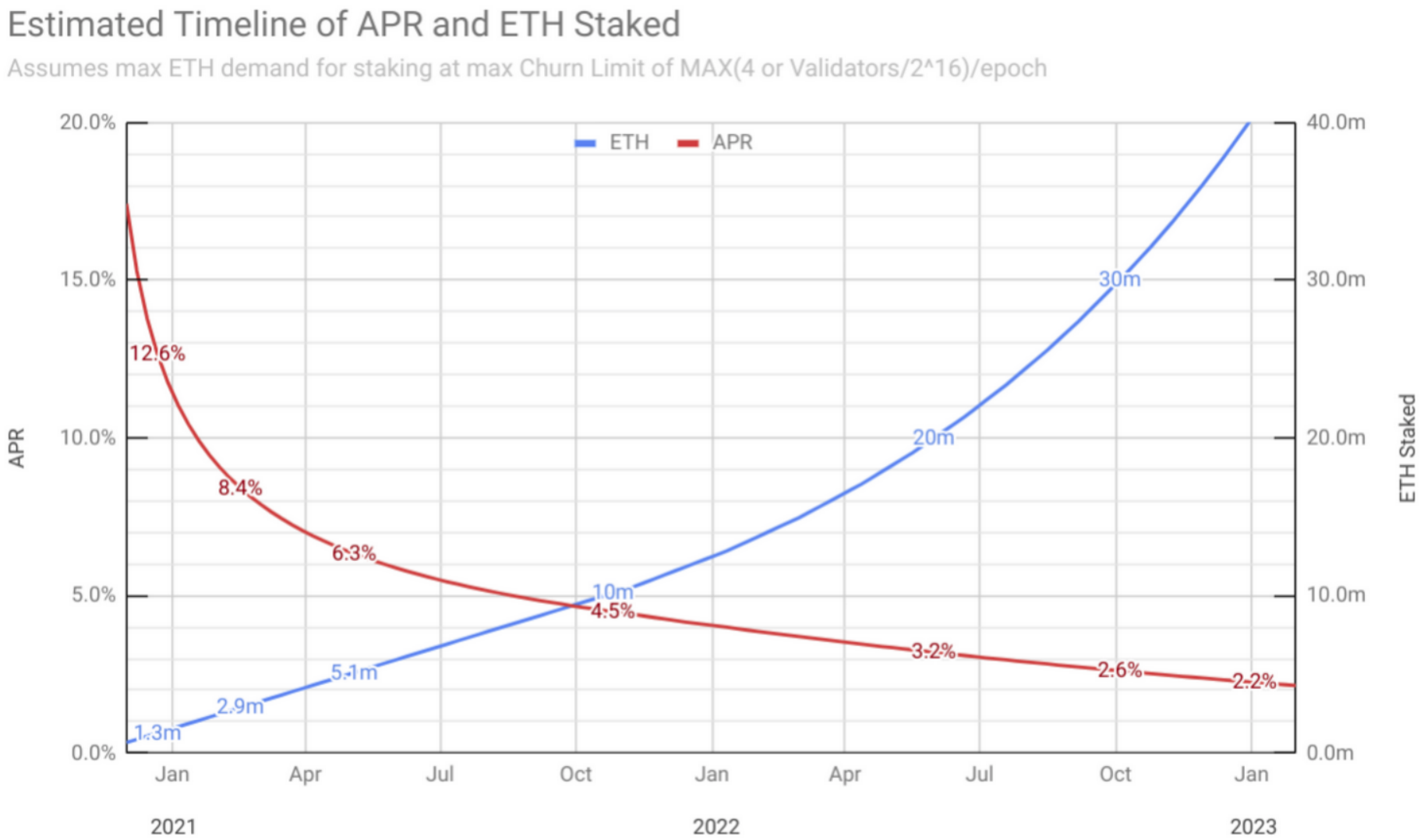
PROOF OF STAKE (ETWAS MEHR DETAILS)



Validators, committees, slots, and epochs

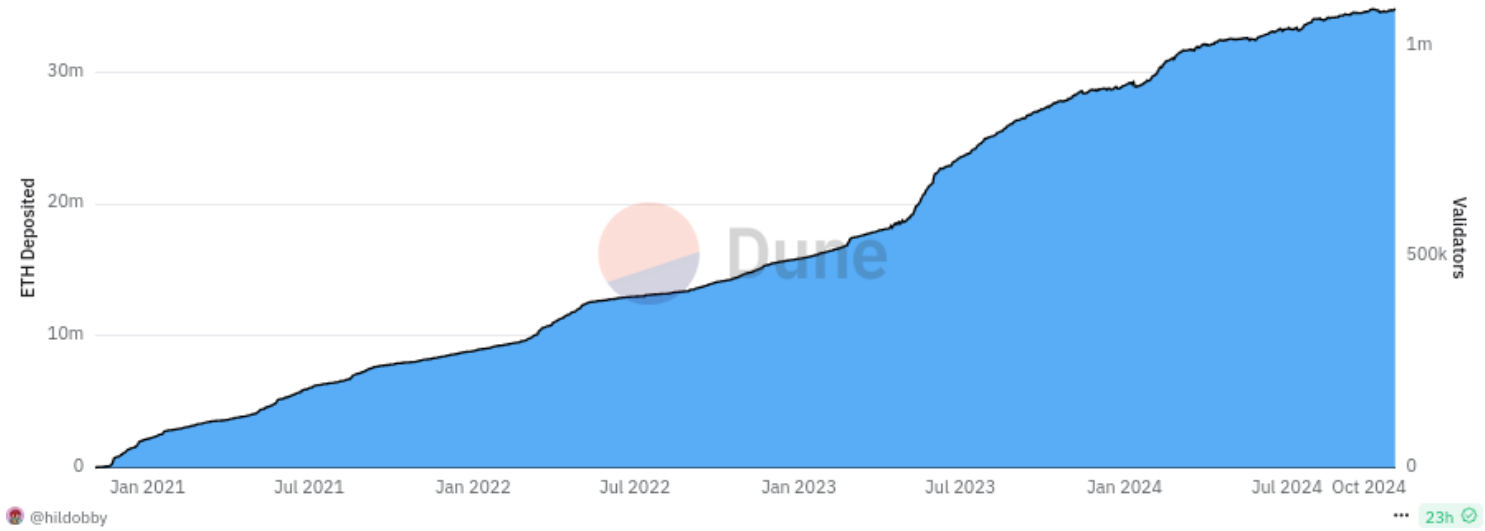
https://medium.com/coinmonks/eth2-0-phase-0-basics-for-new-contributors-8a0a22bc38c7

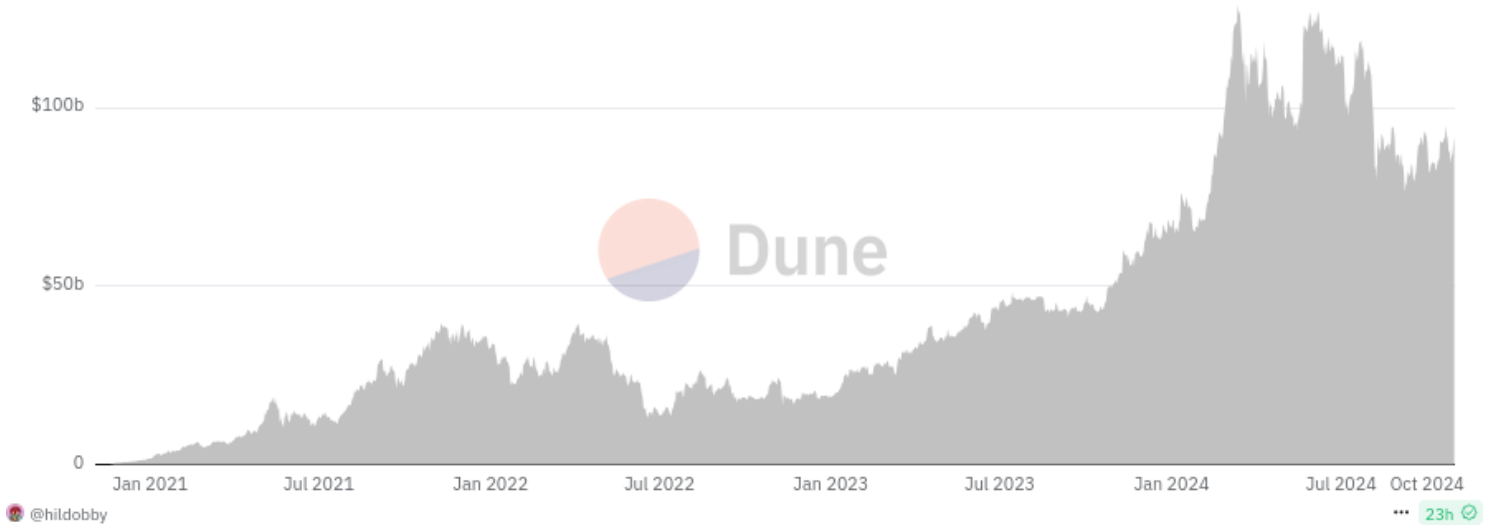
RENDITE FÜR VALIDIERUNG - ~~INFLATION~~ ISSUANCE



https://old.reddit.com/r/ethstaker/comments/k9wf4x/estimated_timeline_of_apr_and_eth_staked/

STATISTIKEN

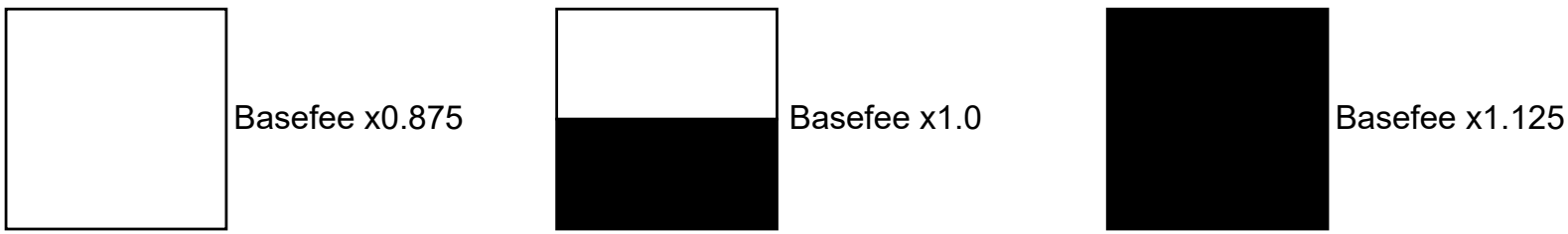




https://dune.com/hildobby/eth2-staking

EIP1599

- Transaktionspreis = Basispreis + Prioritätspreis
- ETH des Basispreises wird vernichtet
- ETH des Prioritätspreises bekommt der Blockbauer
- Basispreis ist abhängig von vorheriger Blockgröße

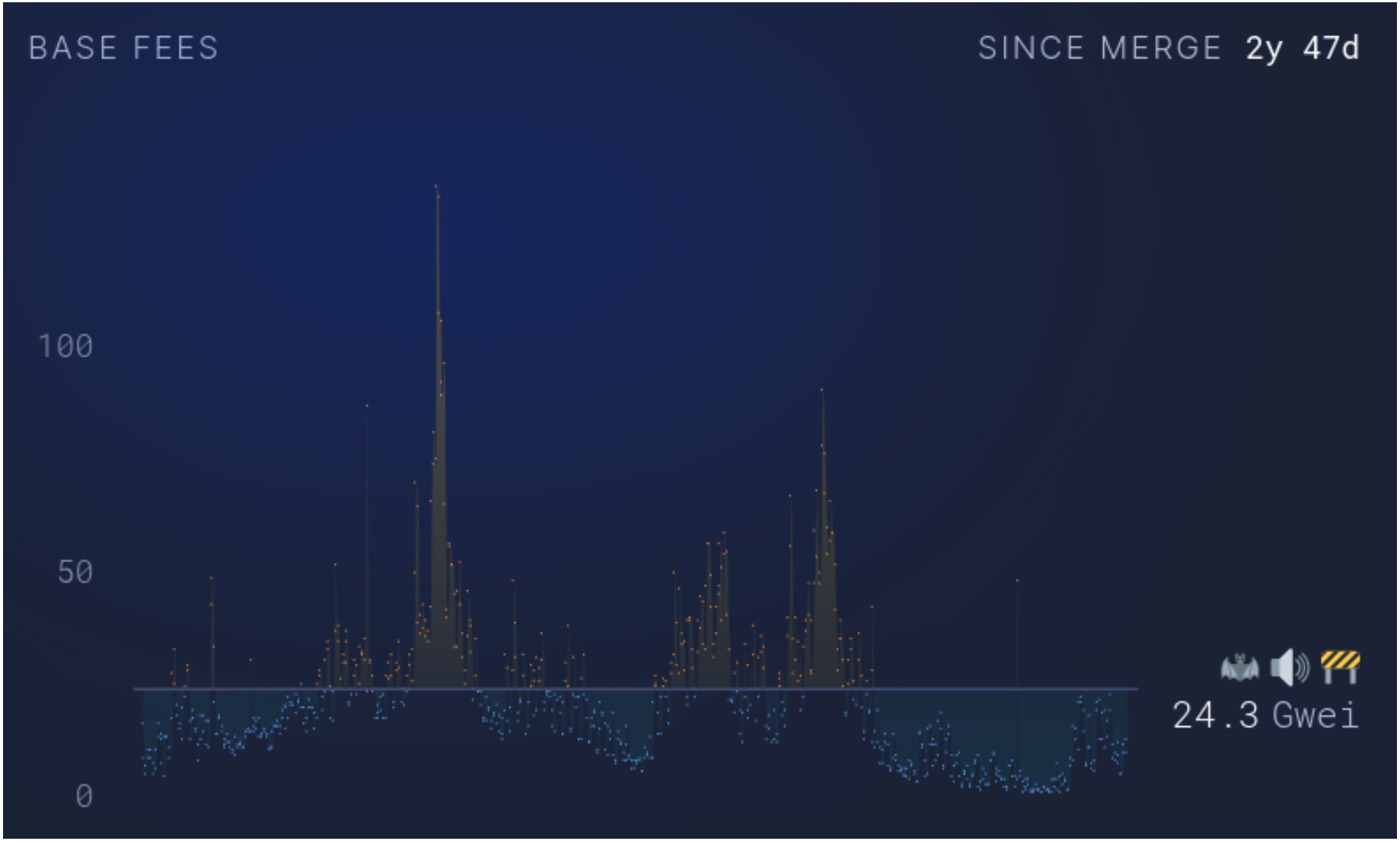


BASEPREIS BEISPIEL

Block Number	Included Gas	Fee Increase	Current Base Fee
1	15M	0%	100 gwei
2	30M	0%	100 gwei
3	30M	12.5%	112.5 gwei
4	30M	12.5%	126.6 gwei
5	30M	12.5%	142.4 gwei
6	30M	12.5%	160.2 gwei
7	30M	12.5%	180.2 gwei
8	30M	12.5%	202.7 gwei

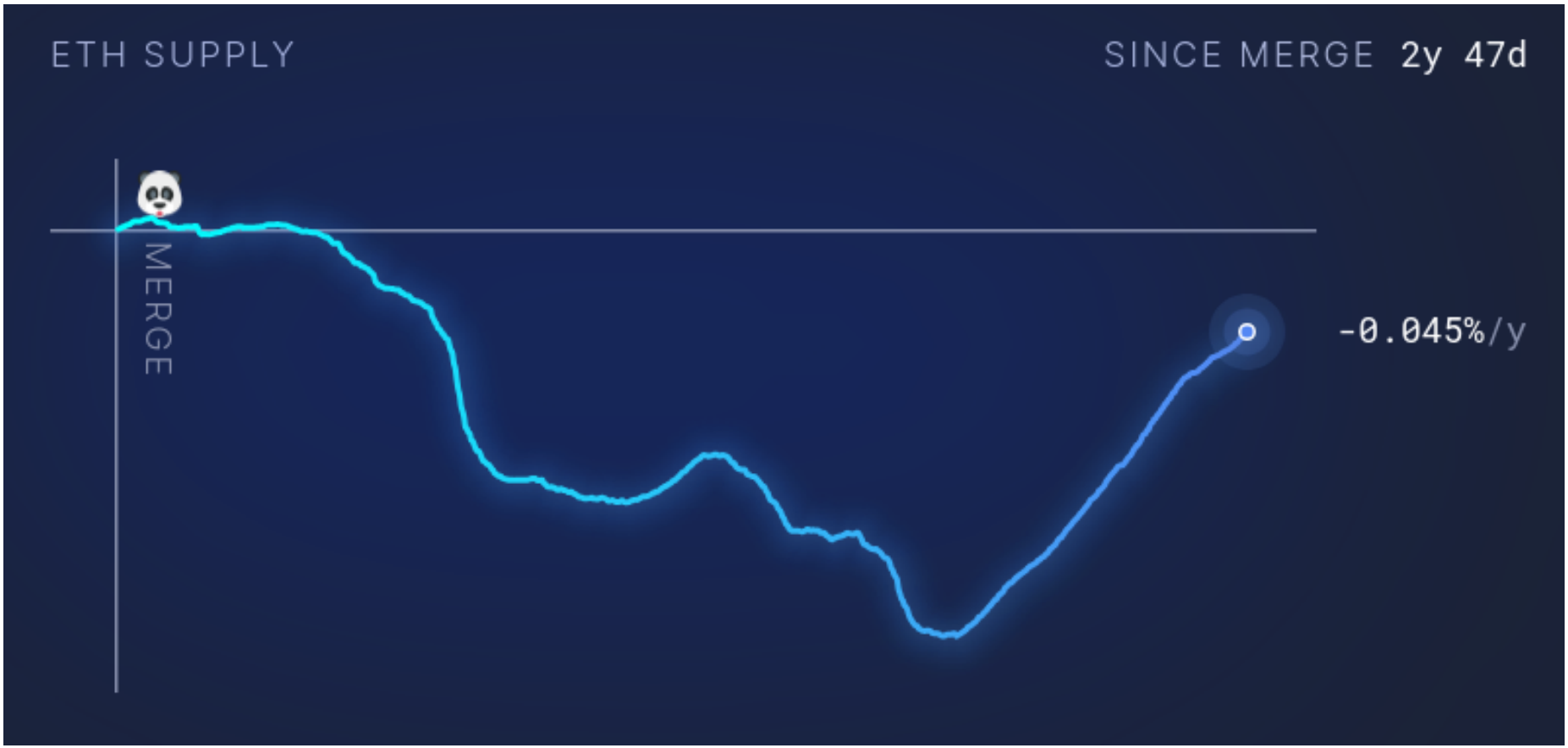
https://ethereum.org/en/developers/docs/gas/

STATISTIKEN



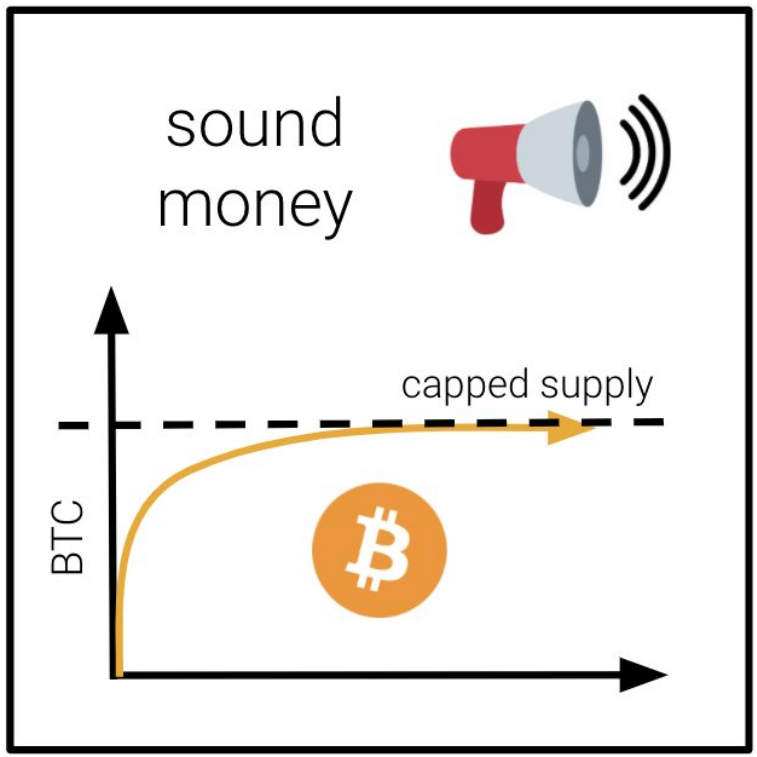
https://ultrasound.money/

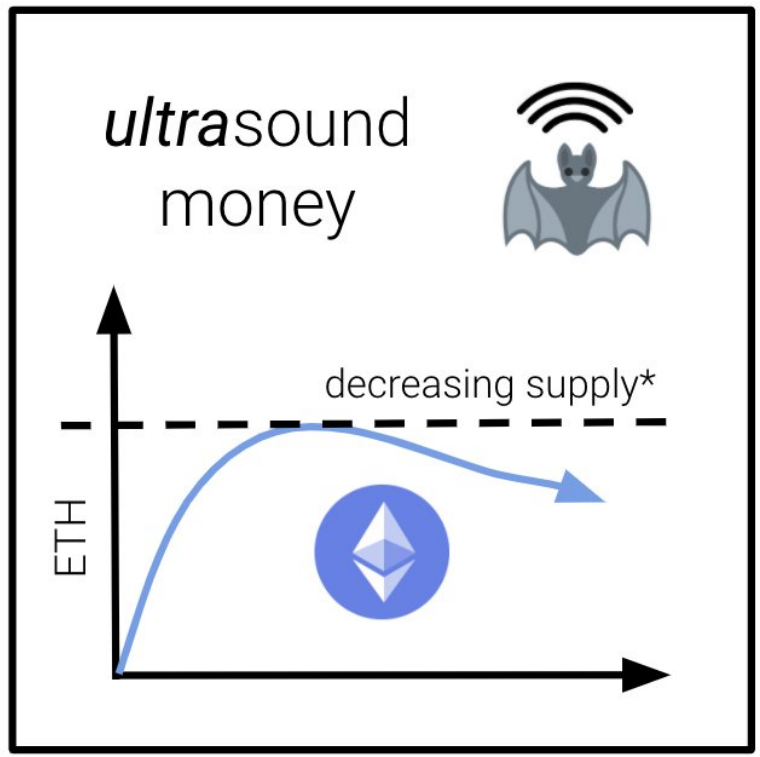
STATISTIKEN



https://ultrasound.money/

DAS ULTRA SOUND MONEY MEME





*if fee burn (EIP 1559) greater than inflation

https://twitter.com/drakefjustin/status/1304064879662227456

SKALIERUNG

- Gas Ziel: 15.000.000 (halb voller Block)
- Gas pro Transaktion: 21.000
- ergibt theoretisches Maximum von 59.5 TPS
- nicht erreicht wegen Konkurrenz durch Smartcontracts
- im Vergleich andere Zahlungssysteme
  - Bitcoin 7TPS
  - Ethereum (praktisch) 13 TPS
  - Visa ~1,700 TPS (nach eigener Aussage)
  - Mastercard ~5,000 TPS (nach eigener Aussage)

ROLLUPS (-METAPHER)

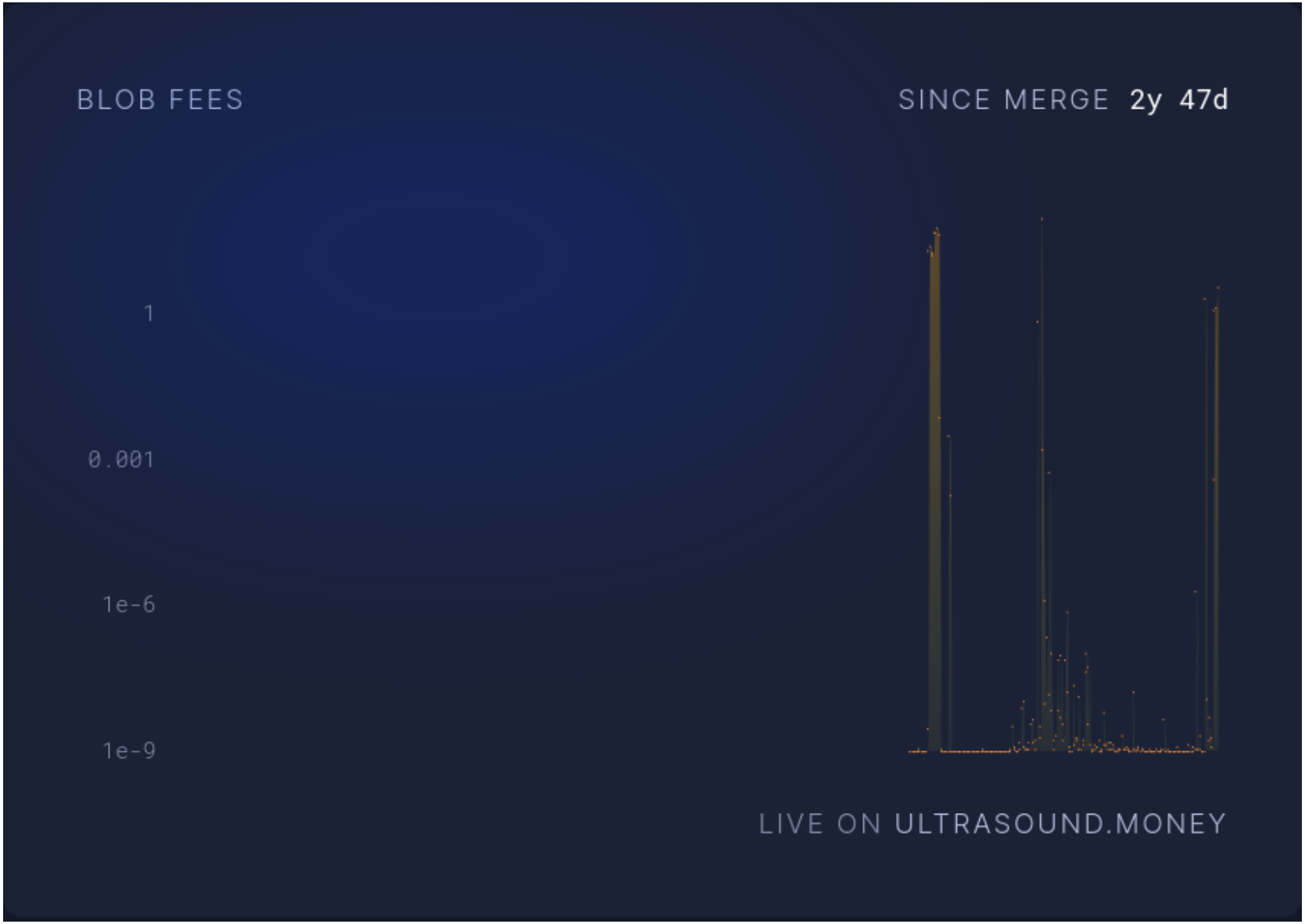
Ethereum als eine stark befahrene Autobahn und Transaktionen als Autos (Erklärung erdacht durch ein LLM). Rollups Vorgang:

- Sammeln von Transaktionen: Anstatt dass jedes Auto (Transaktion) auf der Hauptautobahn (Ethereum) fährt, werden sie auf einem Parkplatz (Rollup) gesammelt.
- Verarbeitung außerhalb der Kette: Die Transaktionen werden in diesem separaten Bereich verarbeitet, abseits der Autobahn.
- Komprimierung: Nach der Verarbeitung wird eine *mathematisch äquivalente* Zusammenfassung aller dieser Transaktionen erstellt, fast wie eine Liste der Autos, die durchgefahren sind.
- Rückmeldung: Diese Zusammenfassung wird dann an das Ethereum-Netzwerk gesendet und nimmt dabei viel weniger Platz ein, als wenn jedes Auto einzeln auf der Autobahn gefahren wäre.

EIP4844

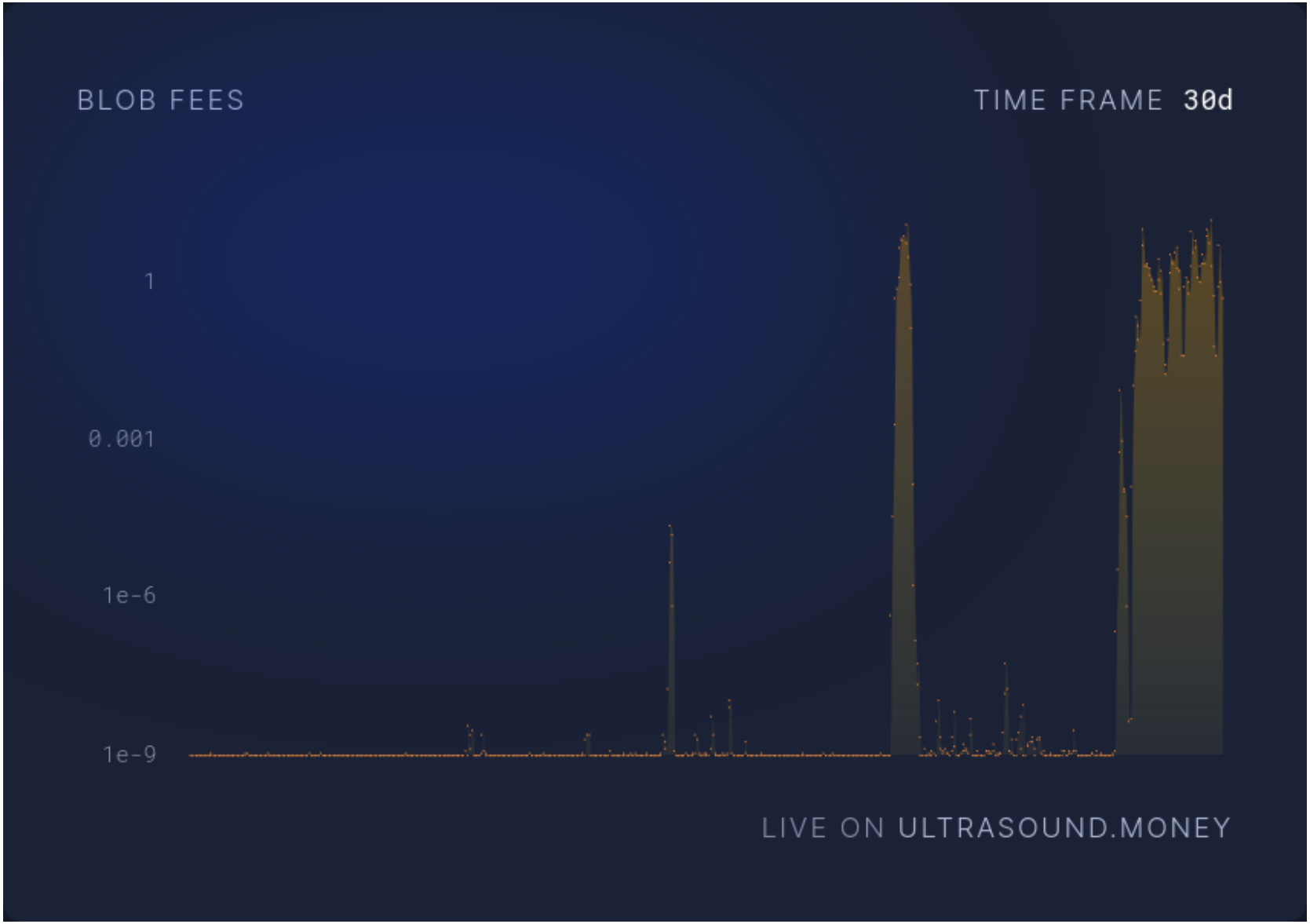
- Spezieller Speicherplatz für Rollups
- für die Zusammenfassung der einzelnen Tansaktionen
- BLOBS = Binary Large Object
- Ziel: 3 BLOBS pro Block, 6 maximal
- Preisfindung mit EIP1559 ähnlichem Prozess
- erst Anfang des Jahres eingeführt

BLOB STATISTIKEN



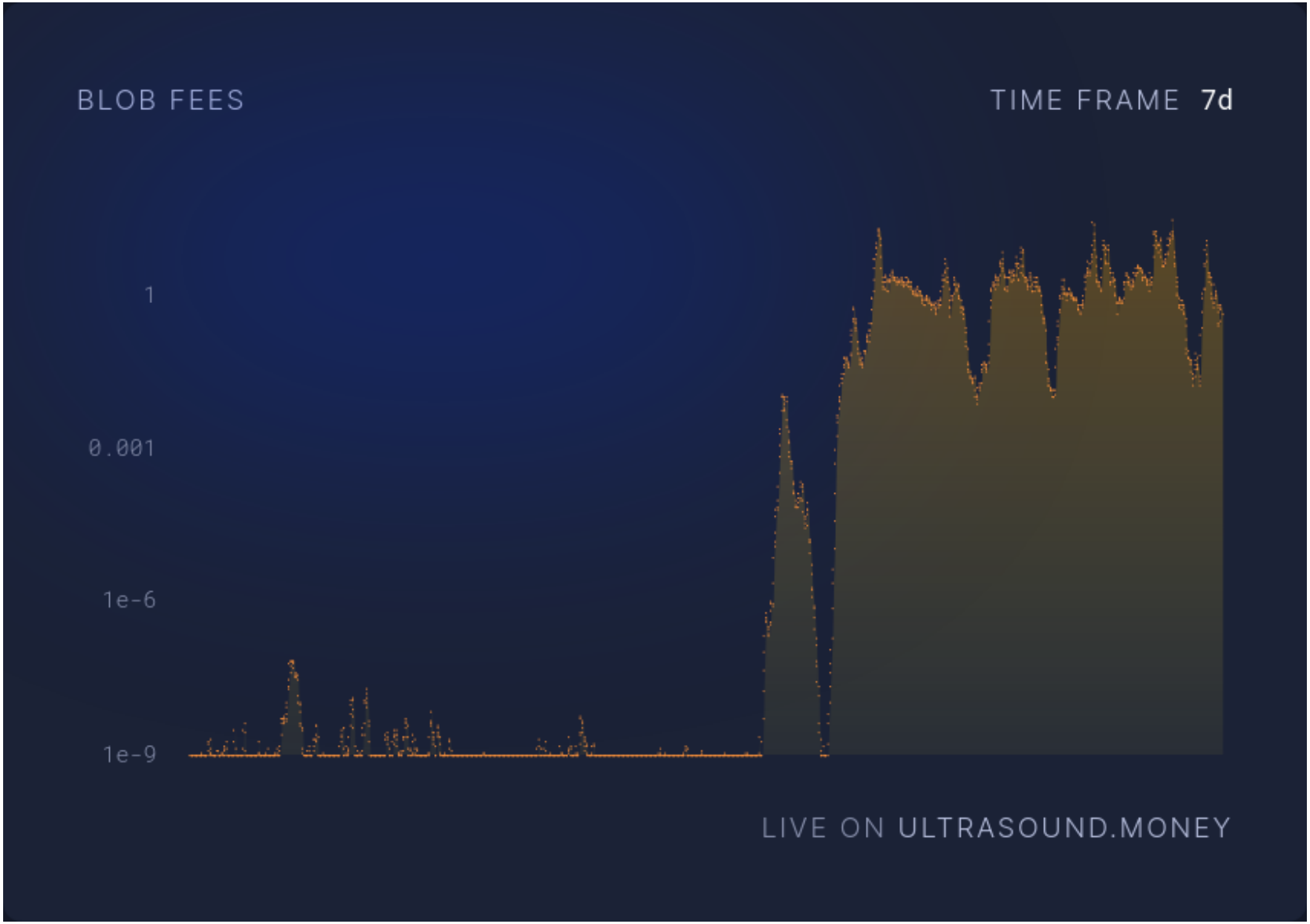
https://ultrasound.money/

BLOB STATISTIKEN



https://ultrasound.money/

BLOB STATISTIKEN



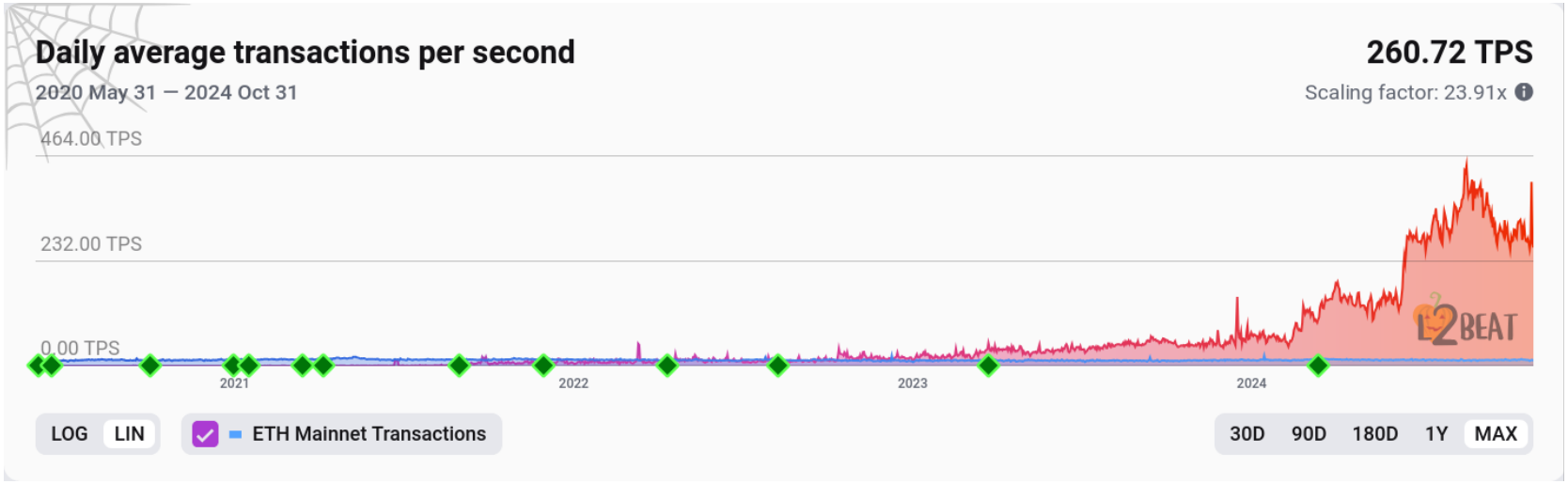
https://ultrasound.money/

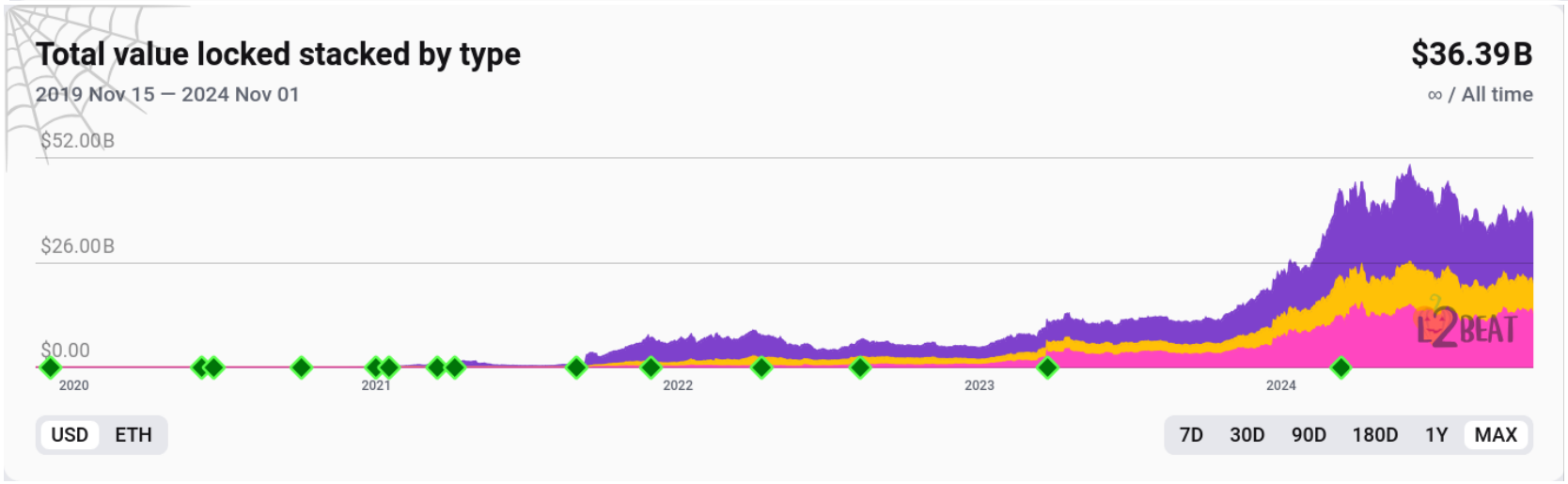
ROLLUPS STATISTIKEN

#	NAME	PAST DAY TPS	MAX TPS	30D COUNT	DATA SOURCE
1	Base	78.23	80.76 on 2024 Oct 30	175.19M ▲17.6%	Blockchain RPC
2	Taiko	45.28	45.50 on 2024 Oct 26	71.44M ▲10.3%	Blockchain RPC
3	Arbitrum One	21.30	58.97 on 2023 Dec 16	55.37M ▼13.1%	Blockchain RPC
4	Gravity	17.83	69.45 on 2024 Aug 19	71.10M ▼35.4%	Blockchain RPC
5	Ethereum	12.56	22.69 on 2024 Jan 14	34.53M ▼4.14%	Blockchain RPC
6	OP Mainnet	8.74	11.28 on 2024 Mar 27	23.54M ▼16.4%	Blockchain RPC
7	World Chain	6.20	8.48 on 2024 Oct 18	9.01M ▼5.55%	Blockchain RPC
8	Blast	5.61	27.34 on 2024 Aug 21	18.40M ▼22.0%	Blockchain RPC
9	Mantle	3.79	25.47 on 2023 Dec 27	9.49M ▼6.33%	Blockchain RPC
10	Linea	3.25	55.69 on 2024 Mar 31	7.02M ▼3.11%	Blockchain RPC

https://l2beat.com/

ROLLUPS STATISTIKEN





https://l2beat.com/

AUSBLICK: AKTUELLE DISKUSSIONEN

- Maximum Stake Target
- MEV Burn (vgl Bonusslide)
- Enshrined Rollup
- Multidimensional Gaspricing
- State Expiry
- Quantumresistant Cryptography

Vielen Dank für eure Aufmerksamkeit

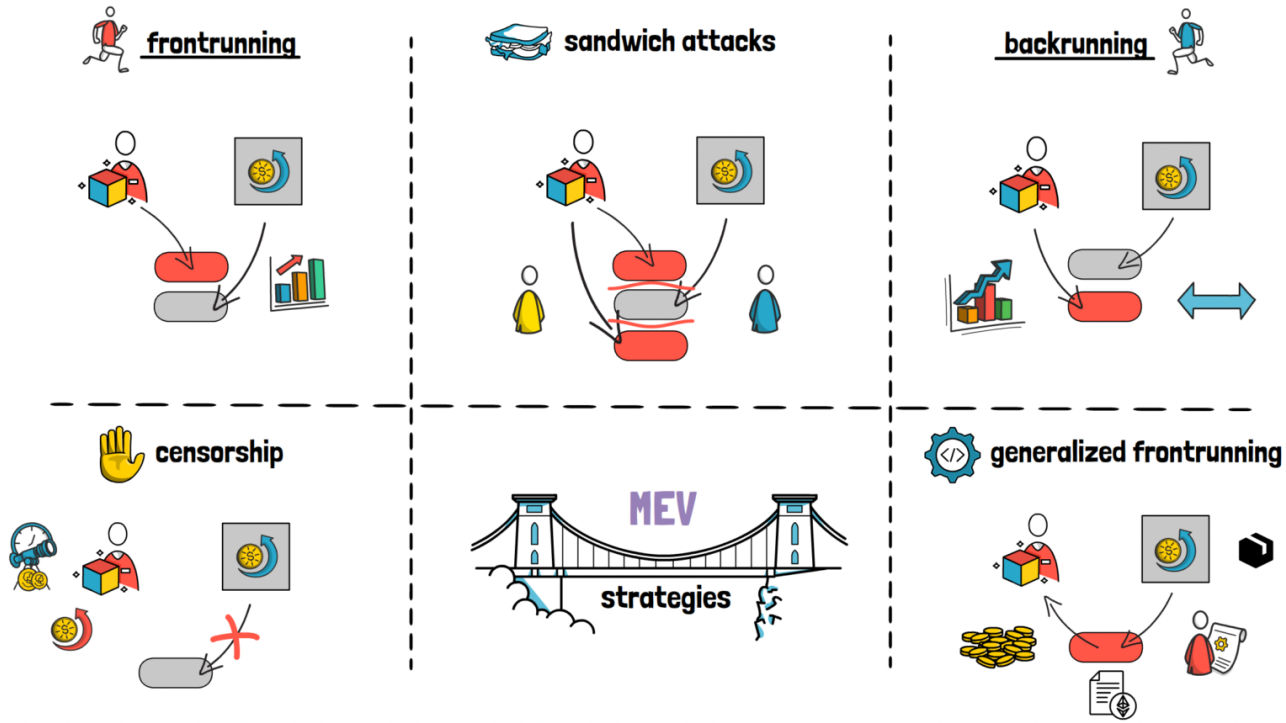
✉ rfl@flipdot.org

[m] @rfl:flipdot.org

rfl@social.flipdot.org

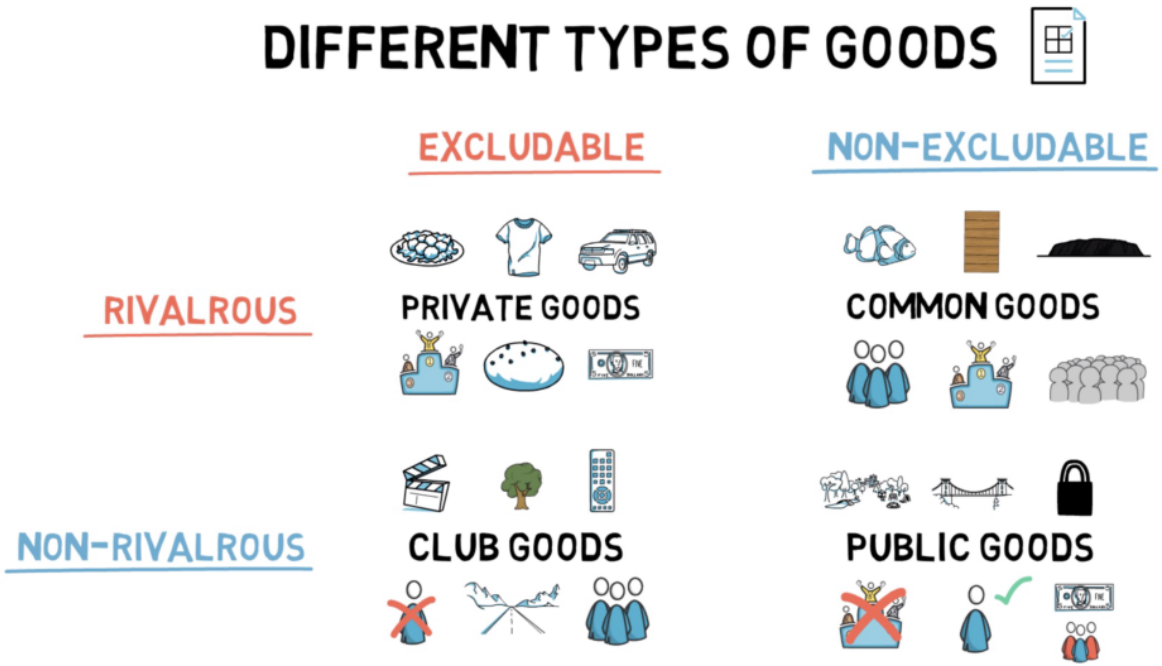
BONUS: ÖKONOMISCHE RENTE

- in der Community bekannt als MEV = Maximal Extractable Value
- allgemein: Abfolge der Transaktionen ist wichtig
- Gewinne werden mitunter als Diebstahl an der Gemeinschaft gesehen



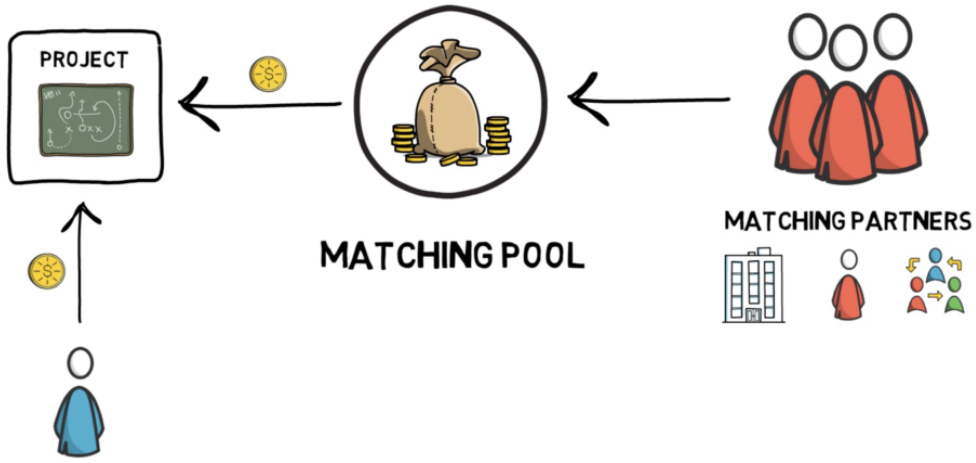
https://finematics.com/decoding-mev-past-present-future/

BONUS BONUS: QUADRATISCHE FÖRDERUNG



https://finematics.com/quadratic-funding-explained/

BONUS BONUS: QUADRATISCHE FÖRDERUNG



$10,000 MATCHING POOL

$v_i^p\left(\left(\sum_j \sqrt{c_{ij}^p}\right)^2\right) - c_i^p$

	A	B	C
FUNDING	$1000	$1000	$1000
NR. OF CONTRIBUTORS	5 ($200 EACH)	2 ($500 EACH)	20 ($50 EACH)
MATCHED AMOUNT	$1,851.85	$740.74	$7,407.41
% OF INITIAL AMOUNT	~185%	~74%	~740%

https://finematics.com/quadratic-funding-explained/