

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:

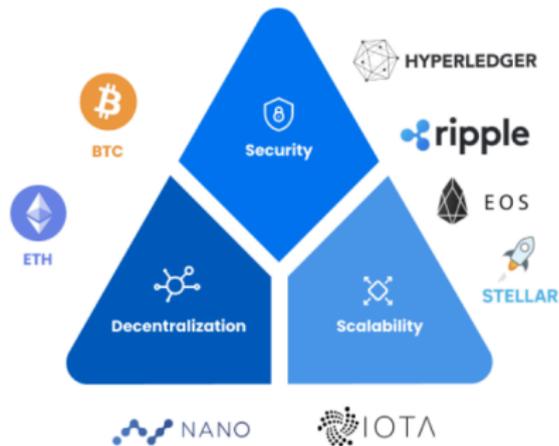
- Bitcoin (2009)
- Whitepaper (2013)
- Stiftung Ethereum (2014)
- Genesisblock (2015)

Ziele:

- Dezentralisierung
- Unzensurbarkeit
- Transparenz
- Benutzbarkeit

Ziele:

- Dezentralisierung
- Unzensurierbarkeit
- Transparenz
- Benutzbarkeit



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

ETHEREUM IST EIN SOZIALES NETZWERK

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

research

categories tags Latest Categories Top

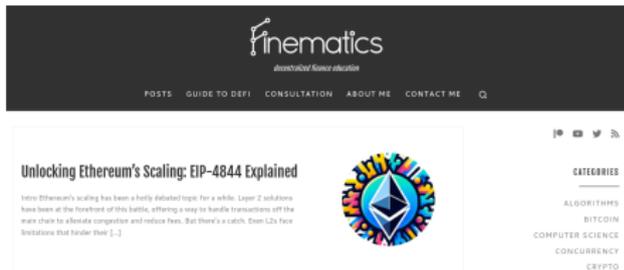
Topic	Replies	Views	Activity
<p>Read this before posting</p> <p>Administrators</p> <p>This is a semi-public forum for participating in Ethereum's research efforts, including but not limited to: Proof-of-Stake Scaling solutions EVM improvements Low-level protocol improvements Economics protocol economic... read more</p>	0	55.6k	Jan 29
<p>Potential impact of blob sharing for rollups</p> <p>Layer 2</p>	3	204	4m
<p>BitBadges: Cross-Chain Tokens (EVM <-> SOL <-> BTC <-> COSMOS)</p> <p>Applications</p>	2	69	1d
<p>What happened to our decentralized private new internet?</p> <p>Privacy # new</p>	9	472	1d
<p>Practical endgame on issuance policy</p> <p>Economics</p>	15	459	2d

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

The screenshot shows the Ethereum Magicians forum interface. At the top, there is a navigation bar with the site logo, a 'Sign Up' button, a 'Log In' button, and icons for a search and a menu. Below the navigation bar, there are tabs for 'categories', 'tags', 'Categories', 'Latest', and 'Top'. The main content area is a table of forum topics.

Topic	Replies	Views	Activity
<p> Ethereum Improvement Proposal all info</p> <p>ERCs · eip-process, tutorial, all-info</p> <p>General information regarding EIPs How to submit an EIP Tutorial Write your EIP using EIP template Create PFE to etherscan/EIPs repo Share link to your EIP alongside with EIP description to Eth Magicians forum to geth... read more</p>	34	18.0k	3d
<p>ERC-XXXX – Endgame Cross-Chain Protocol (LCCP)</p> <p>ERCs</p>	2	52	1m
<p>EIP-7788: Dynamic target blob count</p> <p>EIPs intention</p>	3	71	5m
<p>ERC-7777: Proposal for Human Robot Societies</p> <p>ERCs · erc, governance, dao, identity, decentralization</p>	16	296	2h
<p>ERC-7683: Cross Chain Intents Standard</p> <p>ERCs · erc-20, standards-adoption, cross-chain, intent</p>	32	6.2k	4h

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



The screenshot shows the website 'Kinematics' with the tagline 'decentralized finance education'. The navigation menu includes 'POSTS', 'GUIDE TO DEFI', 'CONSULTATION', 'ABOUT ME', 'CONTACT ME', and a search icon. The main content area features an article titled 'Unlocking Ethereum's Scaling: EIP-4844 Explained' with a sub-headline: 'Intro: Ethereum's scaling has been a hotly debated topic for a while. Layer 2 solutions have been at the forefront of this battle, offering a way to handle transactions off the main chain to alleviate congestion and reduce fees. But there's a catch. Even L2s face limitations that hinder their [...]'. To the right of the article is a colorful circular graphic with an Ethereum logo in the center. On the far right, there are social media icons and a 'CATEGORIES' section listing: ALGORITHMS, BITCOIN, COMPUTER SCIENCE, CONCURRENCY, CRYPTO, and DEFI.

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

Vitalik Buterin's website

[Blockchains](#) [Cryptography](#) [Economics](#) [Fun](#) [General](#) [Bitcoin](#) [Math](#)
[Philosophy](#) [Translations](#)

2024 Oct 29

[Possible futures of the Ethereum protocol, part 6: The Splurge](#)

2024 Oct 26

[Possible futures of the Ethereum protocol, part 5: The Purge](#)

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 eventuell 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

- Simple Summary
- Abstract
- Motivation
- Specification
- Backwards Compatibility
 - Block Hash Changing
 - GASPRICE
- Security Considerations
 - Increased Max Block Size/Complexity
 - Transaction Ordering
 - Miners Mining Empty Blocks
 - ETH Burn Precludes Fixed Supply
- Copyright

ETHEREUM IST EINE BLOCKCHAIN

COMPUTERCODE

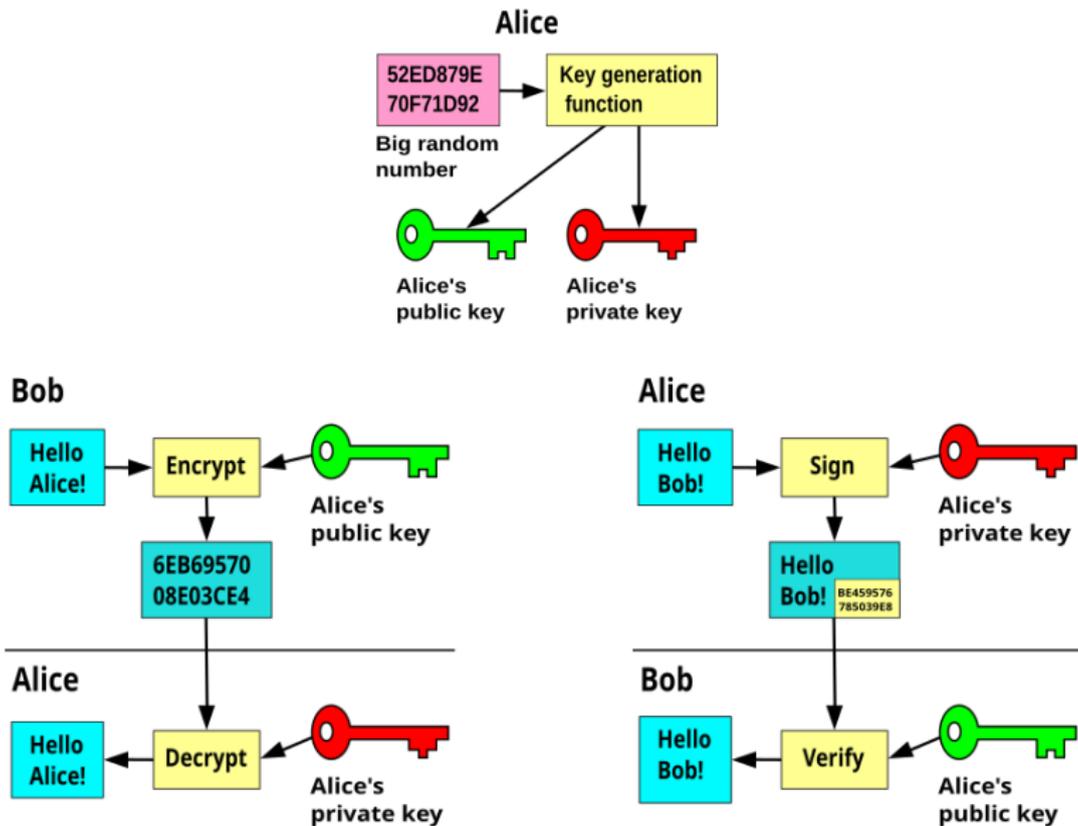
- Unterschied zwischen Spezifikation und Anwendung
- es gibt nur eine Spezifikation, aber unzählige Anwendungen in den verschiedensten Programmiersprachen
- Anzahl der Programmierer der Spezifikationen < 100
<https://github.com/ethereum/consensus-specs>
- Anzahl der Programmierer der Anwendungen > 20000
z.B. <https://github.com/ethereum/go-ethereum>
- Automatische Tests, ob Anwendungen die Spezifikationen erfüllen

GRUNDLAGEN

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:

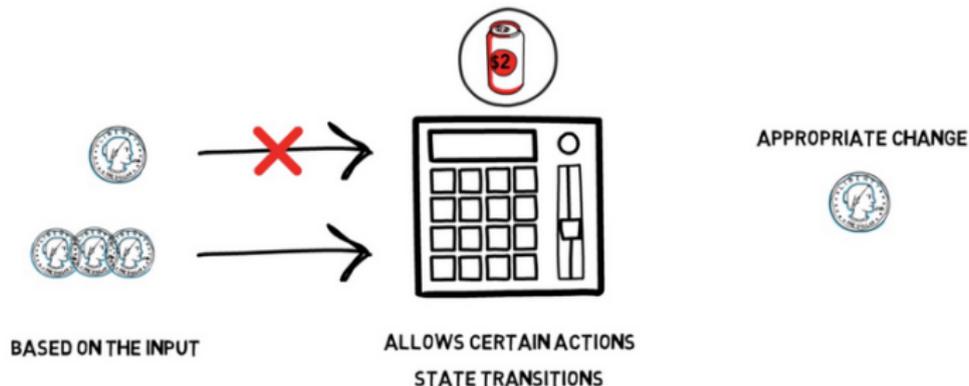
```
{
  "accessList": [
    {
      "address": "0x1eccc89fd4fc4ded8543204854ab4596aec69eb47",
      "storageKeys": [
        "0x0000000000000000000000000000000000000000000000000000000000000000"
      ]
    }
  ],
  "blockHash": "0x479c9dca8a806183261d7b3c2c69844a1a5cb3eae7e10b4d8298f3c6cf207346",
  "blockNumber": 15499910,
  "chainId": "0x1",
  "from": "0x1eccc89fd4fc4ded8543204854ab4596aec69eb47",
  "gas": 134434,
  "gasPrice": 149358907014,
  "hash": "0x6582df4448ce1eb37b5c3365fe869ce43282eda92d78f2a6e0e7ad065deea081",
  "input": "0x0000000100000000000000000000000000000000000000000000000000000000d006824c000",
  "maxFeePerGas": 154096481318,
  "maxPriorityFeePerGas": 138636083893,
  "nonce": 4205,
  "r": "0x423ff6d0f848e83b7b46572956e28a4b72ceb8b10f6f68d9b378e0e0de9f1b94",
  "s": "0x712e01d03c25d8f75179e9232b56d45f943a05f7f51ee318b7ad1946806ada4",
  "to": "0xbeefbabeaa323f07c59926295205d3b7a17e8638",
  "transactionIndex": 2,
  "type": "0x2",
  "v": "0x0",
  "value": 15499910
}
```

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

SMART CONTRACTS

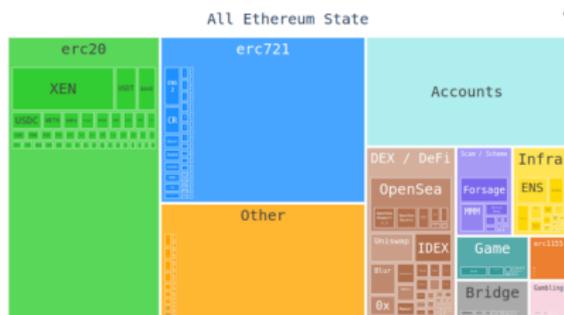
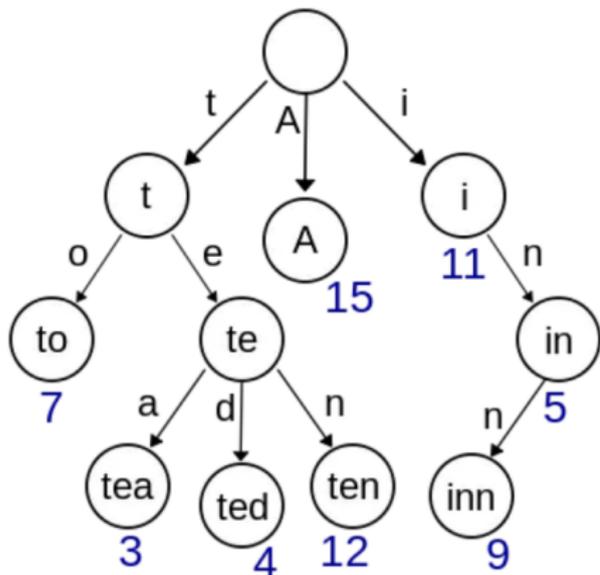
VENDING MACHINE

ANALOGY TO A SMART CONTRACT



<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, int128):
    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

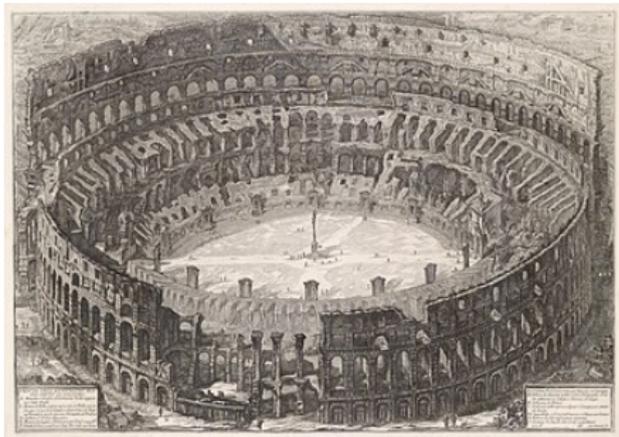
$$100 \text{ GWEI} \times 21,000 \text{ GAS} = 2.1 \text{ MGWEI} = 0.0021 \text{ ETH}$$

<https://finematics.com/>

what-is-gas-ethereum-high-transaction-fees-explained/

ETHEREUM IST EIN GELD DES INTERNETS (?)

PROOF OF STAKE (- METAPHER)

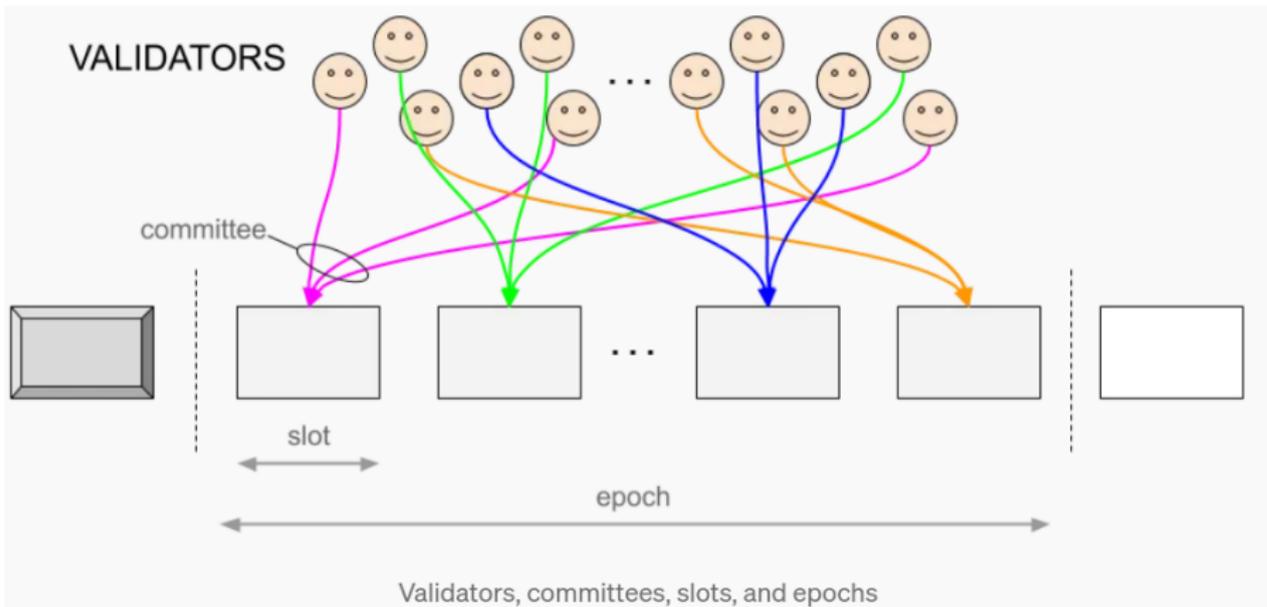


<https://en.wikipedia.org/wiki/Colosseum>



<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)



<https://medium.com/coinmonks/>

eth2-0-phase-0-basics-for-new-contributors-8a0a22bc38c7

RENDITE FÜR VALIDIERUNG - INFLATION ISSUANCE

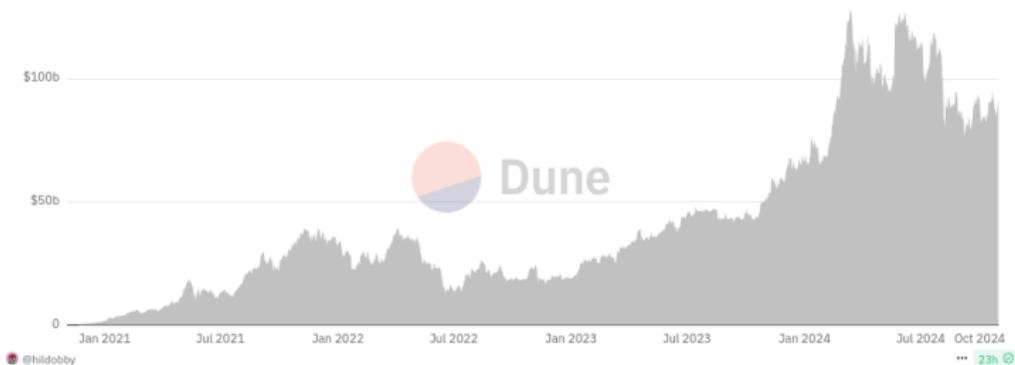
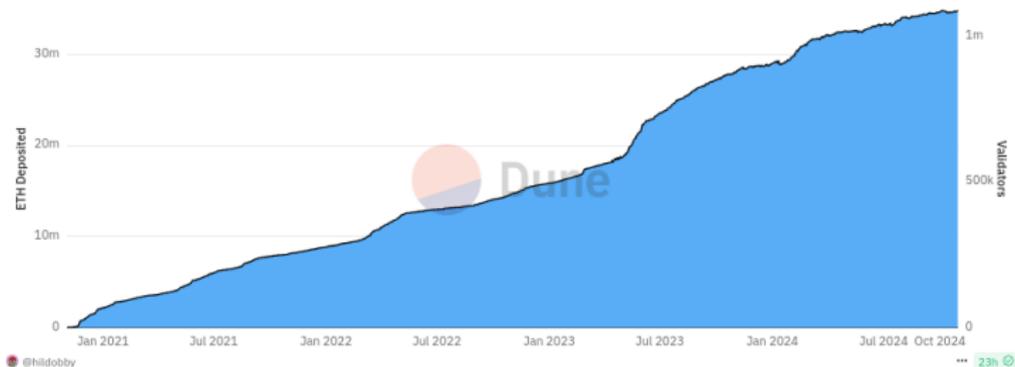
Estimated Timeline of APR and ETH Staked

Assumes max ETH demand for staking at max Churn Limit of $\text{MAX}(4 \text{ or } \text{Validators}/2^{16})/\text{epoch}$



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



Basefee x0.875



Basefee x1.0



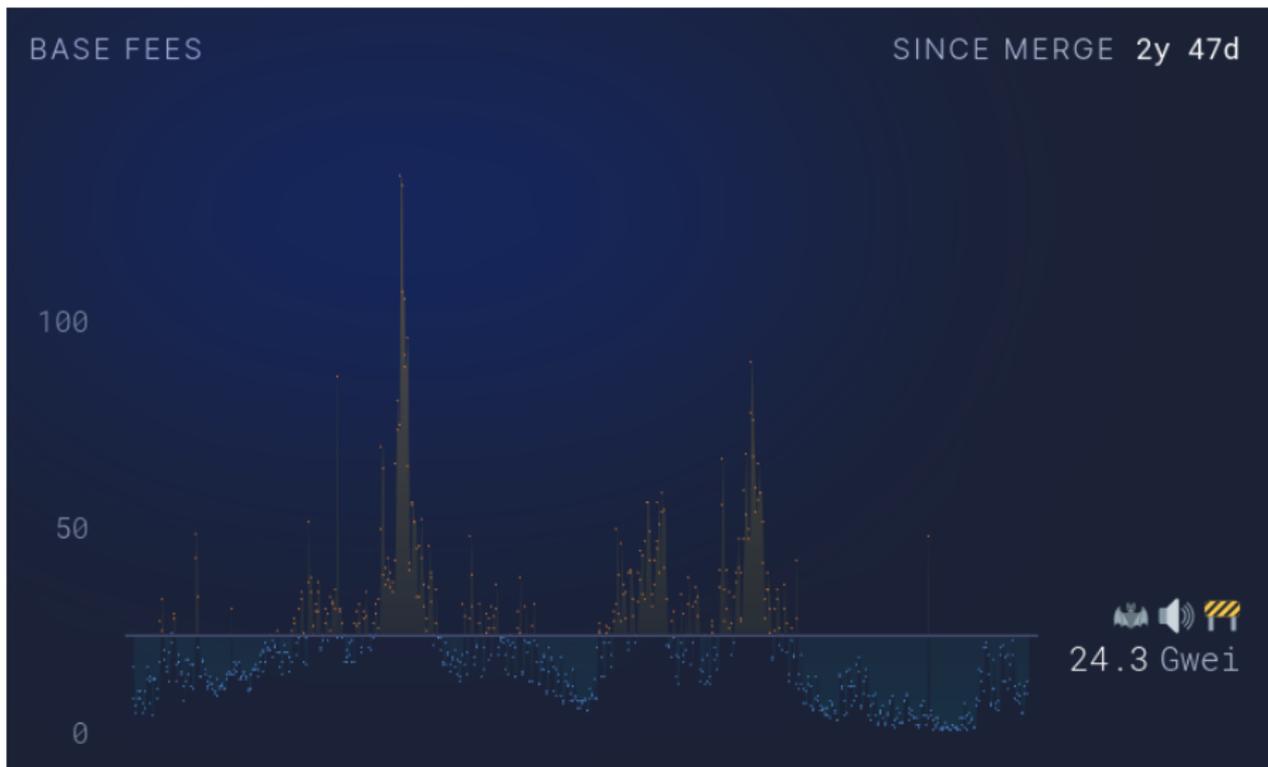
Basefee x1.125

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

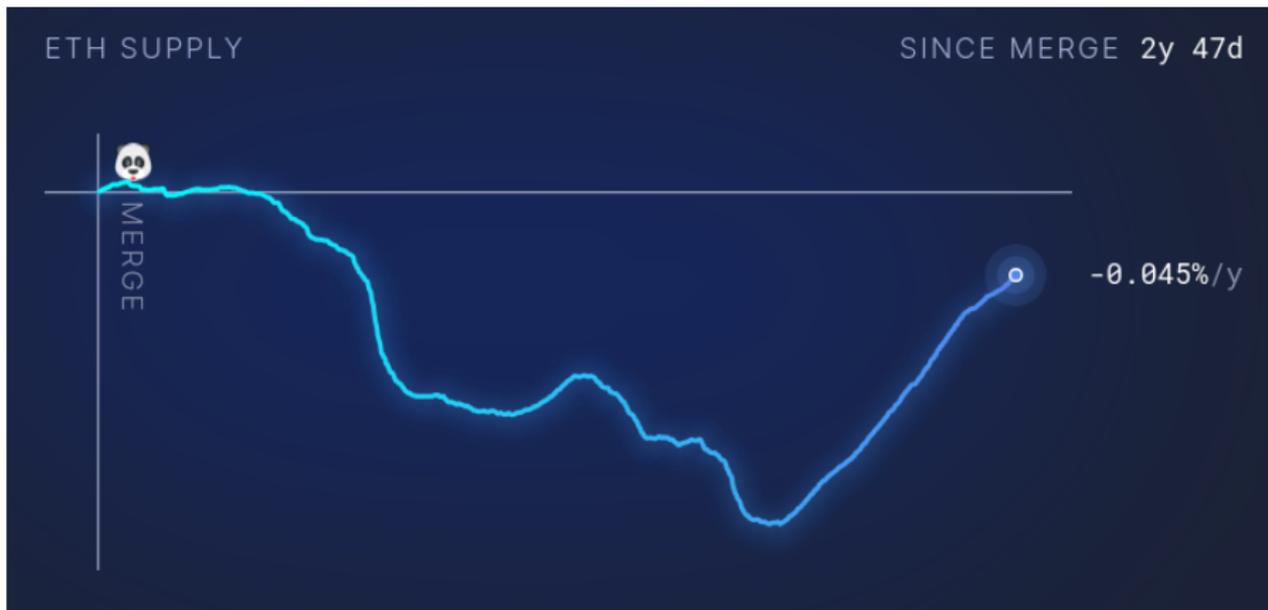
<https://ethereum.org/en/developers/docs/gas/>

STATISTIKEN



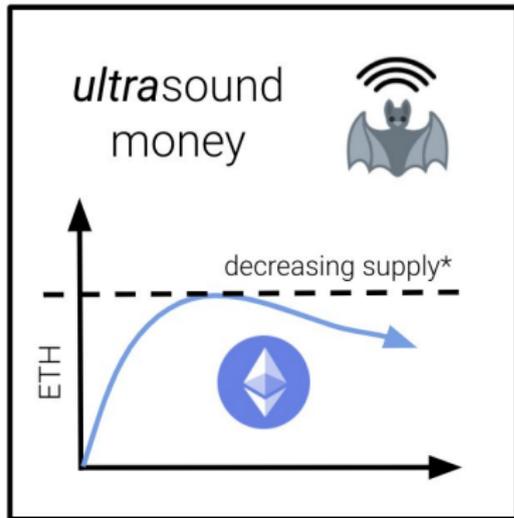
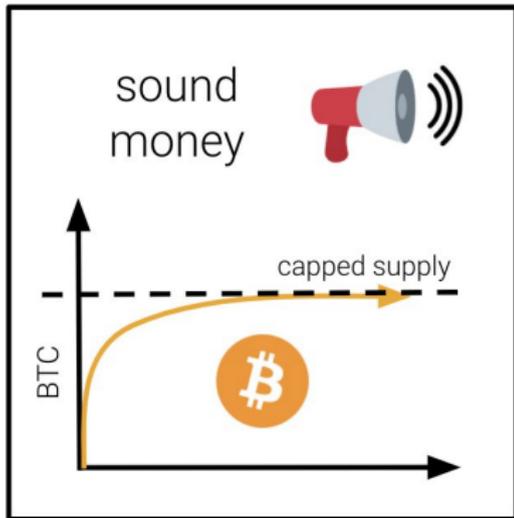
<https://ultrasound.money/>

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)

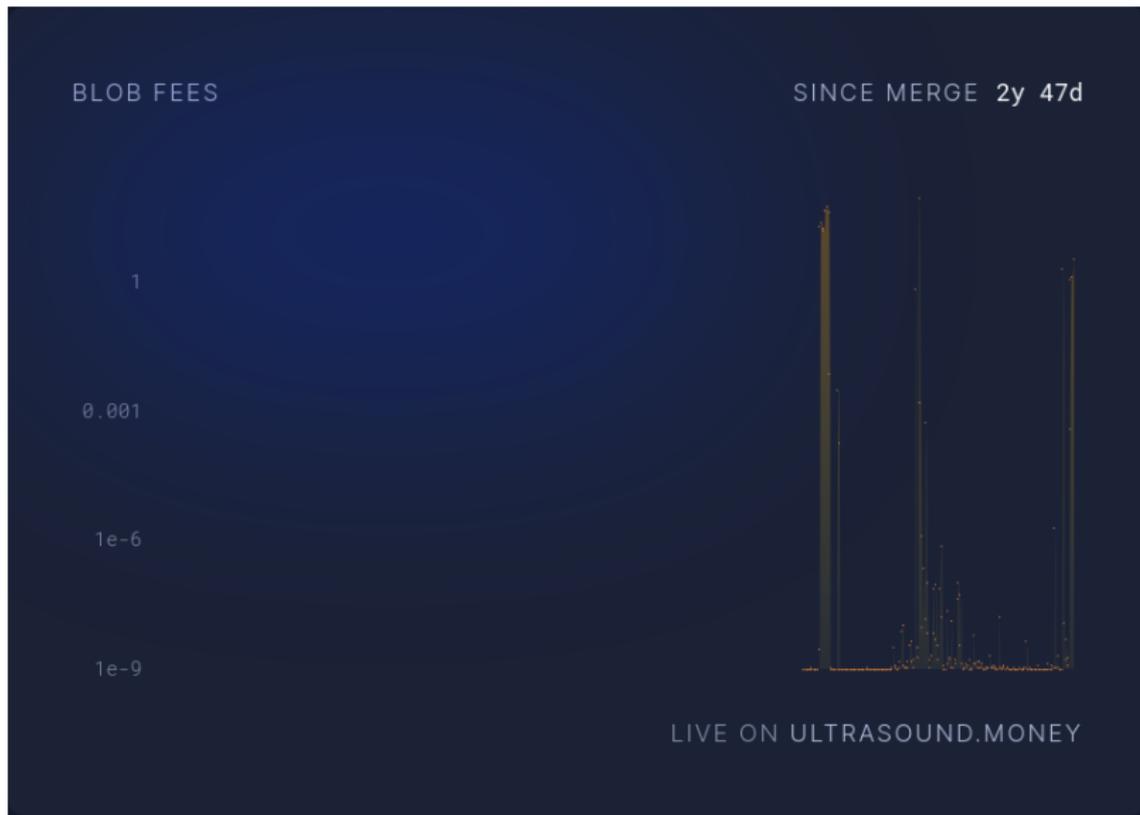
Ethereum als eine stark befahrene Autobahn und Transaktionen als Autos (Erklärung erdacht durch ein LLM). Rollups Vorgang:

- 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

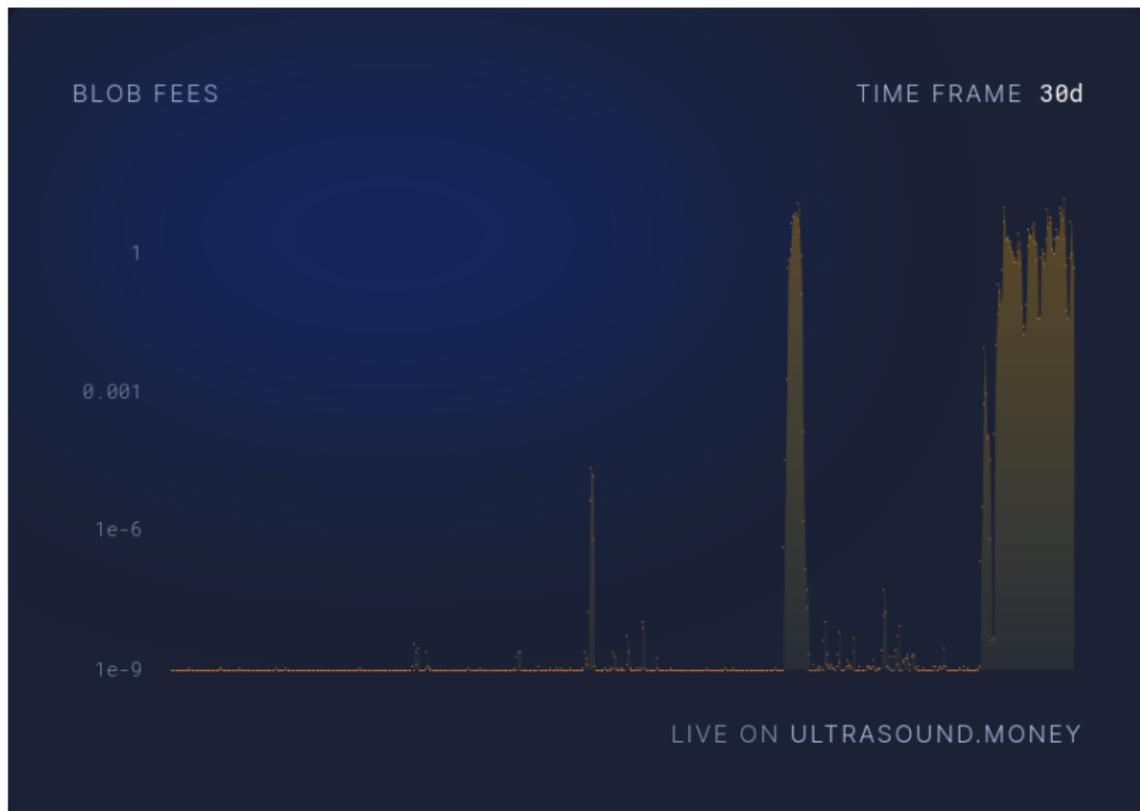
- Spezieller Speicherplatz für Rollups
- für die Zusammenfassung der einzelnen Tansaktionen
- BLOBS = Binary Large Object
- Ziel: 3 BLOBS pro Block, 6 maximal
- Preisfindung mit EIP1559 ähnlichem Prozess
- erst Anfang des Jahres eingeführt

BLOB STATISTIKEN



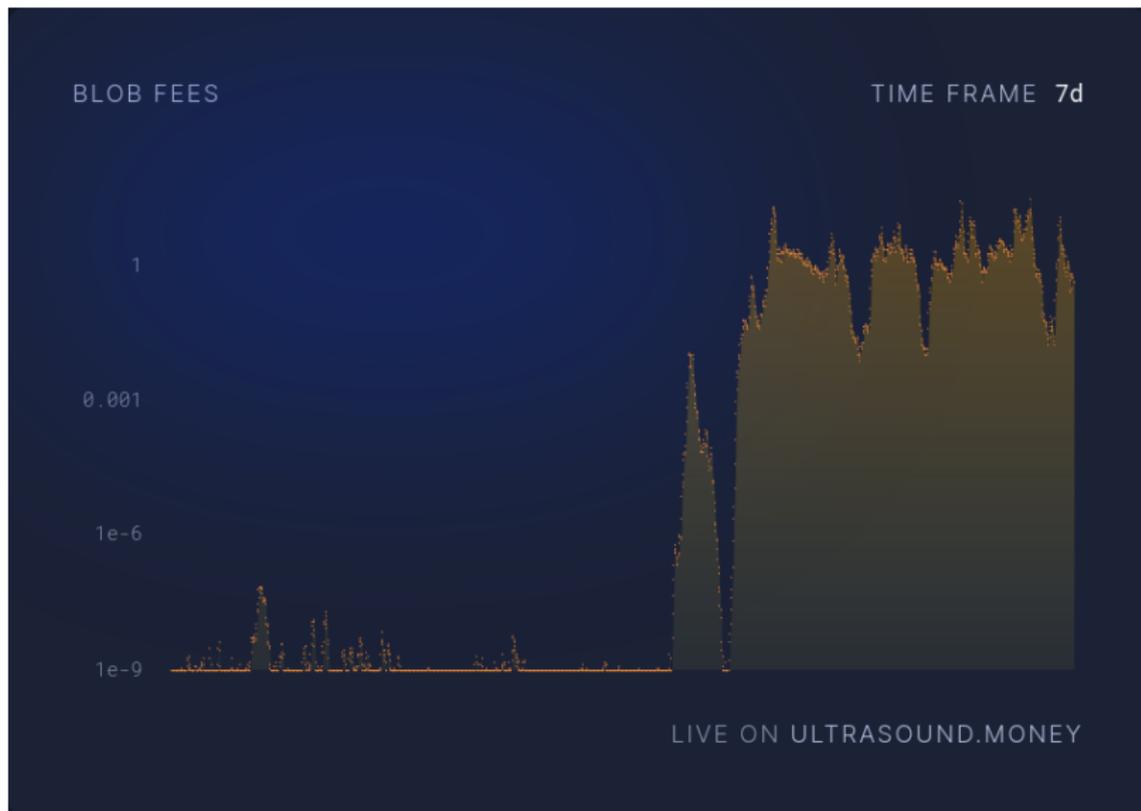
<https://ultrasound.money/>

BLOB STATISTIKEN



<https://ultrasound.money/>

BLOB STATISTIKEN



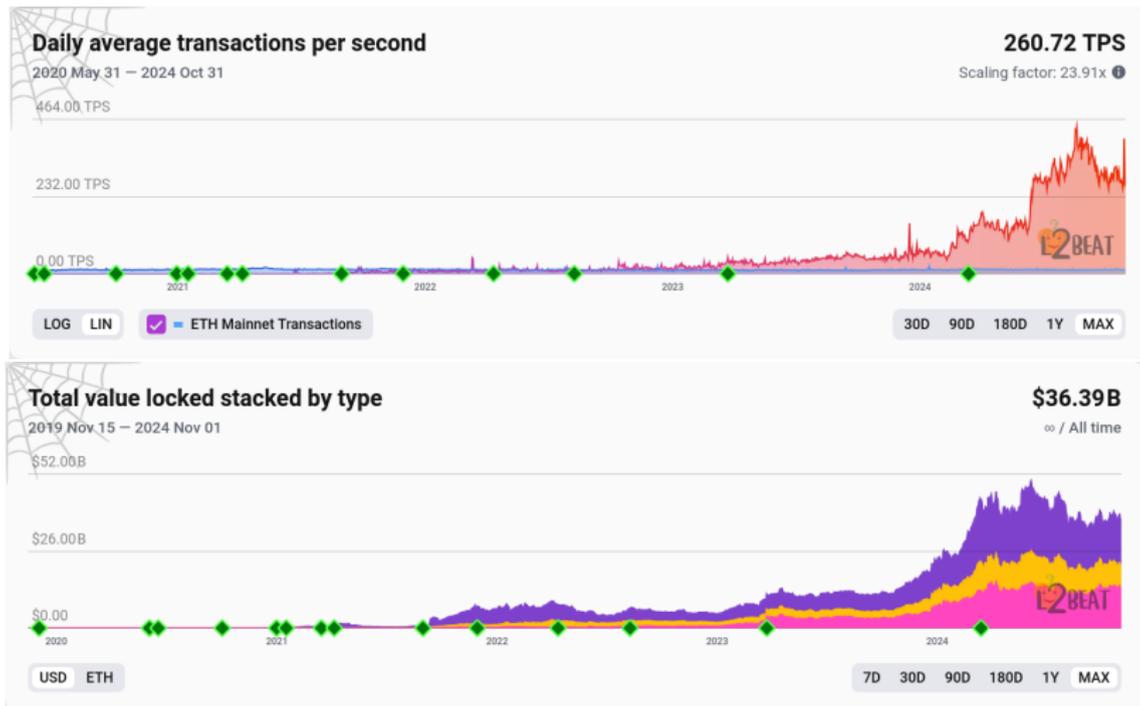
<https://ultrasound.money/>

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 Bonuslide)
- Enshrined Rollup
- Multidimensional Gaspricing
- State Expiry
- Quantumresistant Cryptography

Vielen Dank für eure Aufmerksamkeit

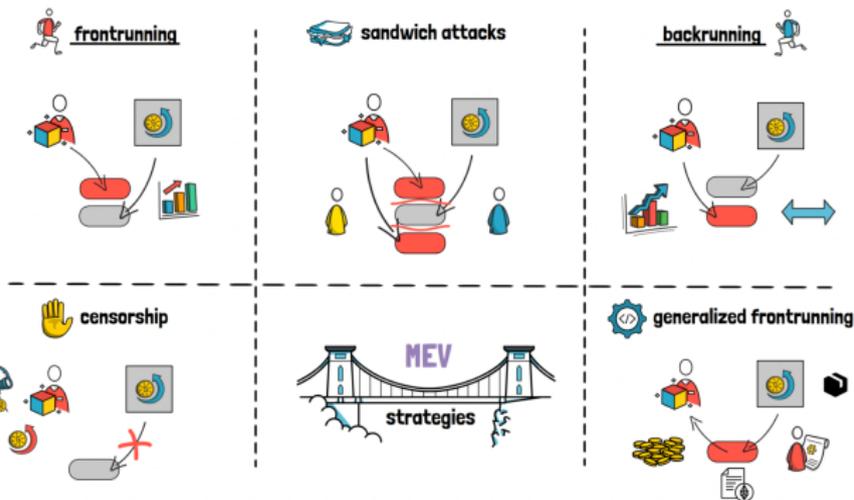
✉ rfl@flipdot.org

[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/>

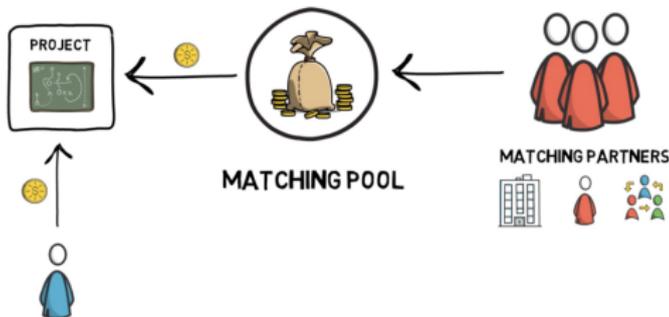
BONUS BONUS: QUADRATISCHE FÖRDERUNG

DIFFERENT TYPES OF GOODS



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

BONUS BONUS: QUADRATISCHE FÖRDERUNG



\$10,000 MATCHING POOL 

	A	B	C 
$v_i^p / ((\sum \sqrt{G_i^p}))^2 - c_i^p$			
FUNDING	\$1000	\$1000	\$1000
NR. OF CONTRIBUTORS	5 <small>(\$200 EACH)</small>	2 <small>(\$500 EACH)</small>	20 <small>(\$50 EACH)</small>
 MATCHED AMOUNT	\$1,851.85	\$740.74	\$7,407.41
% OF INITIAL AMOUNT	-185%	-74%	-740%