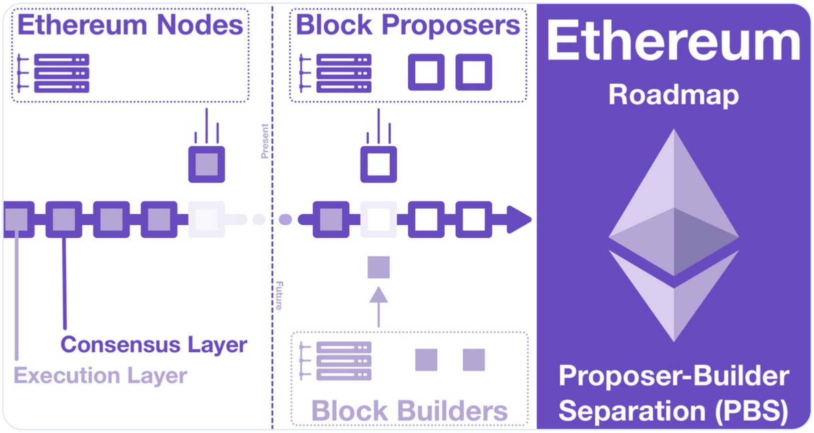
Haym @SalomonCrypto

Sep 15 • 27 tweets • SalomonCrypto/status/1570557757190983680

(1/26) @ethereum Roadmap: Proposer-Builder Separation

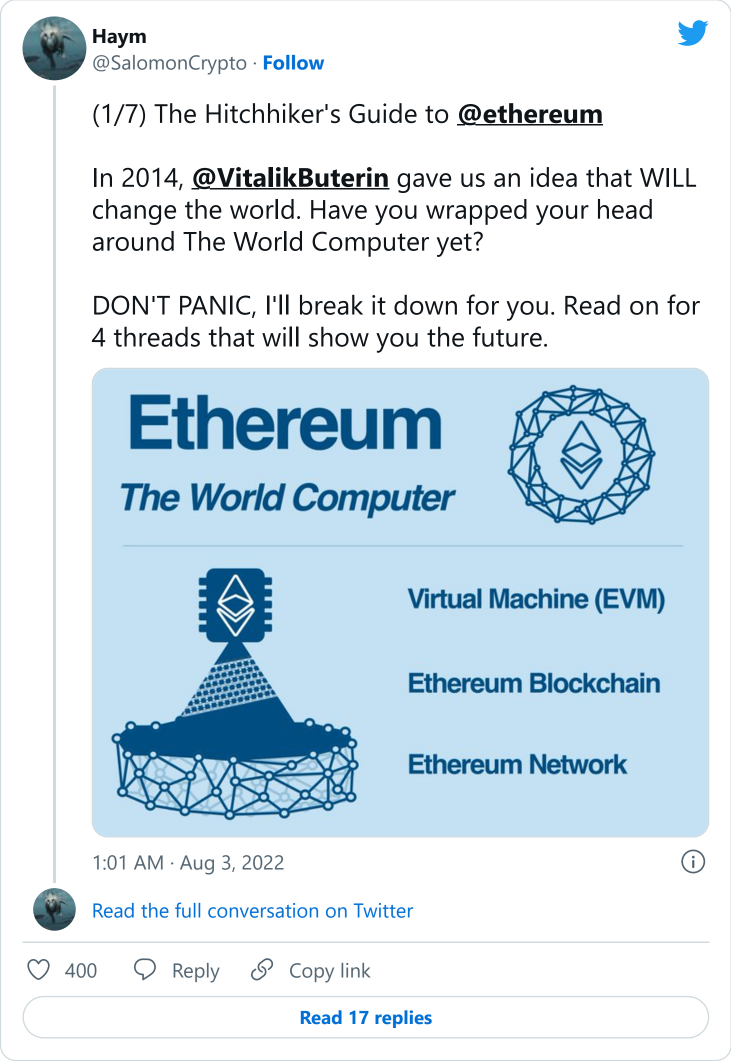
The Merge was successful, $ETH is Proof of Stake! As the era of miners closes, we find ourselves entering a new meta: the age of MEV

Your guide to existential threat facing Ethereum... and the plan to vanquish it



(2/26) @ethereum is the World Computer, a globally shared utility that exists between a network of 1,000s of computers, each running a local version of the Ethereum Virtual Machine (EVM).

Anyone can access the World Computer by submitting a transaction to the network.



Haym
@SalomonCrypto · **Follow**

(1/7) The Hitchhiker's Guide to **@ethereum**

In 2014, **@VitalikButerin** gave us an idea that WILL change the world. Have you wrapped your head around The World Computer yet?

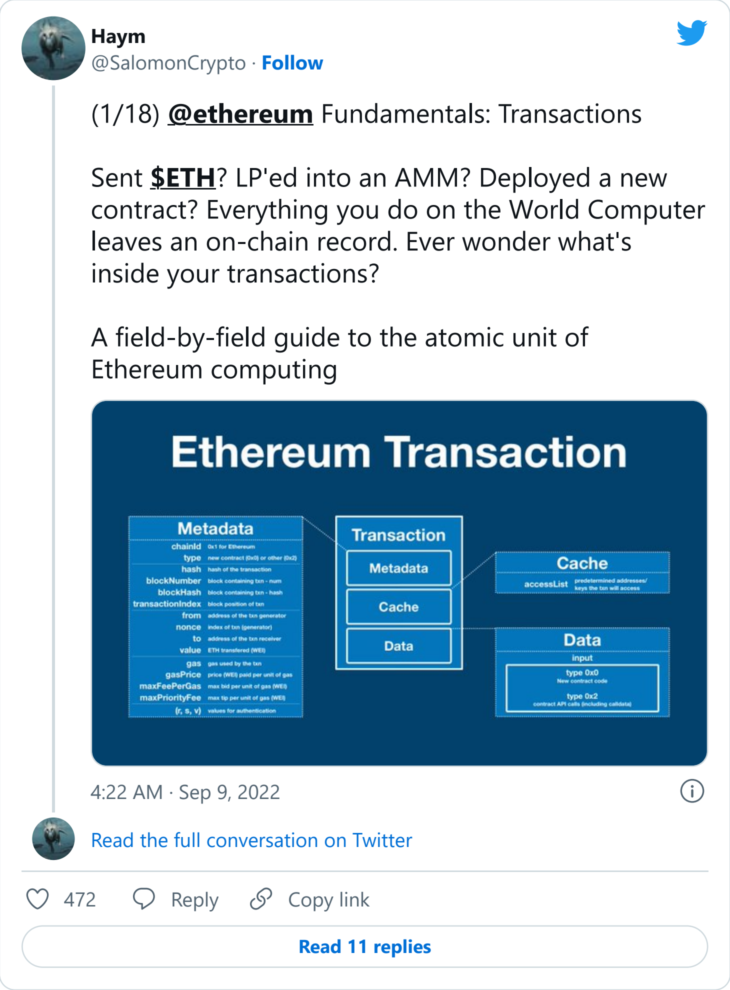
DON'T PANIC, I'll break it down for you. Read on for 4 threads that will show you the future.

1:01 AM · Aug 3, 2022

Read the full conversation on Twitter

(3/26) Holistically, an @ethereum transaction is an instruction for the World Computer. Transactions are irreversible and atomic (they execute completely or they fail).

To use the World Computer, users create a transaction and sends it to the mempool.



Haym
@SalomonCrypto · Follow

(1/18) **@ethereum** Fundamentals: Transactions

Sent **$ETH**? LP'ed into an AMM? Deployed a new contract? Everything you do on the World Computer leaves an on-chain record. Ever wonder what's inside your transactions?

A field-by-field guide to the atomic unit of Ethereum computing

Ethereum Transaction
Metadata
chainId 0x1 for Ethereum
type new contract (0x0) or other (0x2)
hash hash of the transaction
blockNumber block containing txn - num
blockHash block containing txn - hash
transactionIndex block position of txn
from address of the txn generator
nonce index of txn (generator)
to address of the txn receiver
value ETH transfered (WEI)
gas gas used by the txn
gasPrice price (WEI) paid per unit of gas
maxFeePerGas max bid per unit of gas (WEI)
maxPriorityFee max tip per unit of gas (WEI)
(r, s, v) values for authentication
Transaction
Metadata
Cache
Data
Cache
accessList predetermined addresses/ keys the txn will access
Data
input
type 0x0
New contract code
type 0x2
contract API calls (including calldata)

4:22 AM · Sep 9, 2022

Read the full conversation on Twitter

472
Reply
Copy link
Read 11 replies

(4/26) The mempool is a public database of pending transactions, each with their own instructions for the World Computer.

In order to build a new block and progress the blockchain (and therefore the World Computer), @ethereum nodes select pending transactions from the mempool.

(5/26) This method has important benefits (decentralized, transparent, censorship resistant, etc) but also a critical weakness: the public nature of the mempool.

From this setup comes the existential risk of crypto: MEV.

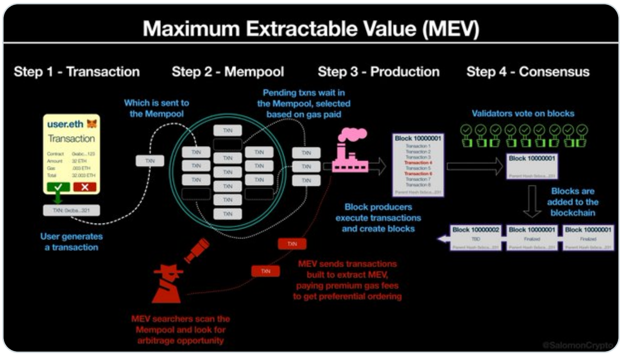
(6/26) In November 2020, @thegostep posted "Flashbots: Frontrunning the MEV crisis" and introduced the community to Maximum Extractable Value (MEV).

In its most basic incarnation, MEV is a form of arbitrage.

Haym
@SalomonCrypto · **Follow**

(1/15) MEV 101

This time with drawings!!!


Maximum Extractable Value (MEV)
Step 1 - Transaction
Step 2 - Mempool
Step 3 - Production
Step 4 - Consensus
user.eth
Transaction
Contract
Amount
32 ETH
Gas
.003 ETH
Total
32.003 ETH
TXN: 0xcba...321
User generates a transaction
Which is sent to the Mempool
TXN
Pending txns wait in the Mempool, selected based on gas paid
Block producers execute transactions and create blocks
Block 10000001
Transaction 1
Transaction 2
Transaction 3
Transaction 4
Transaction 5
Transaction 6
Transaction 7
Transaction 8
Validators vote on blocks
Blocks are added to the blockchain
Block 10000002
TBD
Finalized
MEV searchers scan the Mempool and look for arbitrage opportunity
MEV sends transactions built to extract MEV, paying premium gas fees to get preferential ordering
@SalomonCrypto

1:31 AM · Jun 26, 2022

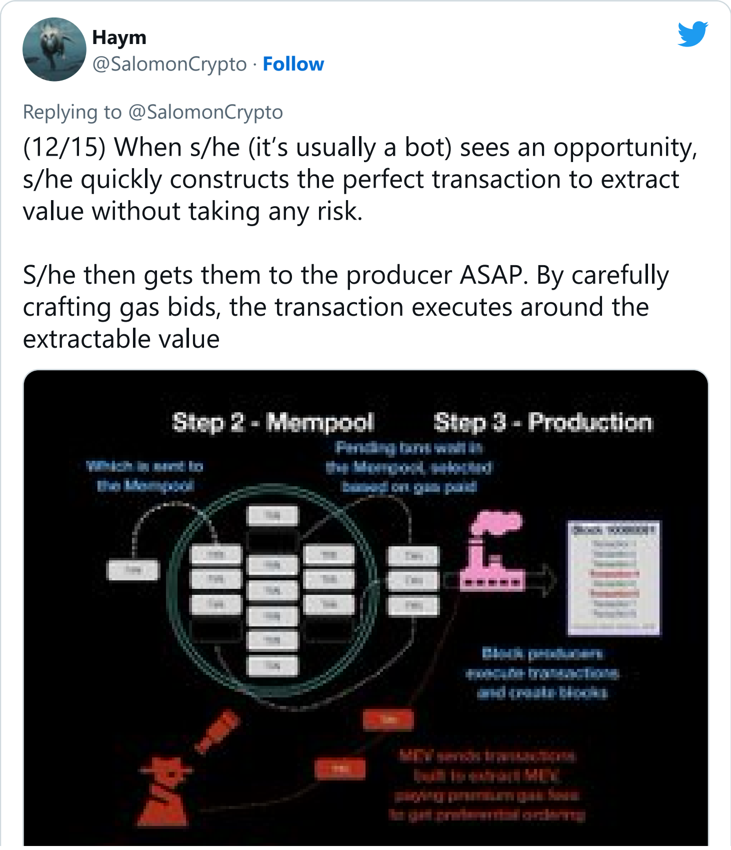
Read the full conversation on Twitter

1.1K Reply Copy link

Read 24 replies

(7/26) Imagine a bot that is closely watching the mempool for pending txns. Suddenly, a pending txn with a HUGEEEE $ETH market buy appears.

The bot, knowing the pending txn will raise the price of $ETH, quickly buys $ETH, waits for the txn and then immediately sells it.



Haym
@SalomonCrypto · Follow

Replying to @SalomonCrypto

(12/15) When s/he (it's usually a bot) sees an opportunity, s/he quickly constructs the perfect transaction to extract value without taking any risk.

S/he then gets them to the producer ASAP. By carefully crafting gas bids, the transaction executes around the extractable value

Step 2 - Mempool
Step 3 - Production
Which is sent to the Mempool
Pending txns wait in the Mempool, selected based on gas paid
Block producers execute transactions and create blocks
MEV sends transactions built to extract MEV paying premium gas fees to get preferential ordering

(8/26) The result:

MEV bot - bought before a huge txn drove up the price of $ETH and sold immediately after, locking in a profit.

Whale - revealed his hand early and had to buy $ETH at a higher price because of the MEV bot.

The bot extracted value from the whale.

(9/26) This example is perhaps the most basic type of MEV; from here, things get exotic very quickly.

While MEV is a very diverse category, there is a common through line: MEV is the value that can be captured by a participant with privileged knowledge or access to a system.

Haym
@SalomonCrypto · **Follow**

(1/21) What exactly IS MEV? How should you understand it?

Let’s dive into its deep history, the current context and the exciting future ahead!

9:22 PM · Jun 17, 2022

Read the full conversation on Twitter

(10/26) In our example, that includes the detailed knowledge of the mempool and the ability to manipulate the order of transactions. The bot uses these levers to extract value.

But what if you didn't need these indirect levers? What if you could just build the block yourself?

(11/26) An @ethereum node is a computer responsible for operating the World Computer and progressing the blockchain. (Under Proof of Stake) the blockchain progresses when a block proposer (selected randomly) submits a new block to the network

First they need to build that block

(12/26) The naive approach to block building is to scan the mempool for the txns with the highest priority fees. Each txn is picked in descending order until the block is filled up.

A less naive node might notice some opportunities as its building.

(13/26) Remember our huge $ETH buy? Maybe no one noticed and so as it's building a block, the node can slip in a txn to capture the arbitrage.

Or maybe some did notice and submitted the arbitrage txn and the node might just decide to ignore that txn and put their own in.

(14/26) Nodes do not have to respect the mempool when they are building blocks; each one is able to select txns as it sees fit.

Some nodes are going to build baseline-blocks, other nodes are going to play more aggressive.

A few will be WAYYY better than anyone else.

(15/26) Consider the implications of being better at building blocks. Lets imagine 2 nodes: naive builder (NB) and MEV builder (MB)

- NB and MB will have the same costs & opportunity to build blocks
- MB will earn more yield than NB
- MB's stake will grow faster than NB's stake

(16/26) As of yesterday, @ethereum is a Proof of Stake chain.

What does it mean to have a Proof of Stake chain where some nodes (can) earn more than others?

Centralization is inevitable.

Haym
@SalomonCrypto · Follow

Welcome to Proof of Stake

```
:42:53.002 INFO Ready for the merge                     current_difficulty: 58750003716598352816469, terminal_total_
6:42:59.749 INFO New block received                      root: 0x810a00400a80cdffc11ffdcf17ac404ac4dba215b95221955a9d
6:42:59.954 INFO
           ,,,                                          ,,,         ,,,
:        ;'   ',                                     ;'   ^;      ;'   ',
$$$$$$$s       ;                                     ;     s$$$$$$$s     ;
$$$$$$$$$s  ,'   ooooooooo.    .oooooo.    .oooooo..o    ,   ss$$$$$$$$$$s  ,'
$$$$$$$$$$       `888   `Y88. d8P'  `Y8b d8P'    `Y8   ;s$$$$$$$$$$$$$$$
$$$$$$$$$$$$      888   .d88'888      888Y88bo.          $$$$$$$$$$$$$$$$$$
Y$$$Y""W$$$$$     888ooo88P' 888      888 `"Y8888o.    $$$$P""Y$$$Y""W$$$$$
"LFG"q  $$$$$     888        888      888     `"Y88b   $$$$  p"LFG"q  $$$$$
$$$$$.  $$$$      888        `88b    d88'oo     .d8P   $$$$  .$$$$$.  $$$$
$$$$$$$$$$       o888o        `Y8bood8P' 8""88888P'     $$DcaU$$$$$$$$$$
$"*"$$$Y"                                                  "Y$$$"*"$$$Y"
"$b.$$"                                                        "$b.$$"

o.                    .   o8o                        .                 .o8
88.                 .o8   `"'                      .o8                "888
888.     .ooooo. .o888oooooo oooo    ooo .oooo.  .o888oo .ooooo.  .oooo888
`888.   d88' `"Y8  888   `888  `88.  .8' `P  )88b   888  d88' `88bd88' `888
o8888.  888        888    888   `88..8'   .oP"888   888  888ooo888888   888
  `888. 888   .o8  888 .  888    `888'   d8(  888   888 .888    .o888   888
 o8888o`Y8bod8P'  "888"o888o      `8'    `Y888""8o  "888"`Y8bod8P'`Y8bod88P"

e: beacon
6:42:59.954 INFO Proof of Stake Activated                slot: 4700013, service: beacon
6:42:59.954 INFO                                         Terminal POW Block Hash: 0x55b11b918355b1ef9c5db810302ebad0b
6:42:59.957 INFO                                         Merge Transition Block Root: 0x810a00400a80cdffc11ffdcf17ac4
:42:59.957 INFO                                          Merge Transition Execution Hash: 0x56a9bb0302da44b8c0b3df54
```

7:03 AM · Sep 15, 2022

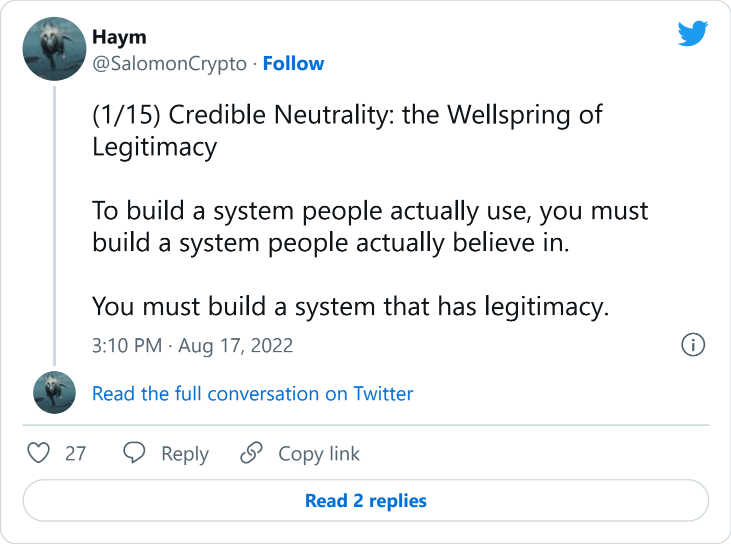
79 Reply Copy link

Read 1 reply

(17/26) Centralization is the anathema of @ethereum. The World Computer is built on a single core principle: decentralization.

From decentralization flows credible neutrality.

From credible neutrality comes global dominance.



Haym
@SalomonCrypto · Follow

(1/15) Credible Neutrality: the Wellspring of Legitimacy

To build a system people actually use, you must build a system people actually believe in.

You must build a system that has legitimacy.

3:10 PM · Aug 17, 2022

(18/26) By its very nature, block building will always reward those with the most resources. Faster connections, better algorithms and smarter people will always outcompete vanilla builders.

Rather than leveling the playing field, we just send the pros the major leagues.

(19/26) This is what an @ethereum block looks like. At the highest level, it can be thought of as having 3 sections: admin, consensus and execution.

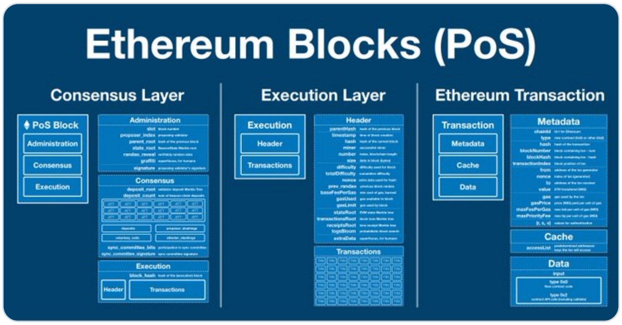
A node must propose a new block with all 3 parts... but there's no reason the node must build the whole block.

Haym
@SalomonCrypto · **Follow**

(1/21) **@ethereum** Fundamentals: PoS Blocks

In less than 1 week, the Ethereum blockchain will Merge with the Beacon Chain and the World Computer will transition from PoW to PoS. The blockchain will never be the same.

A field-by-field guide to on-chain future.



10:28 PM · Sep 9, 2022

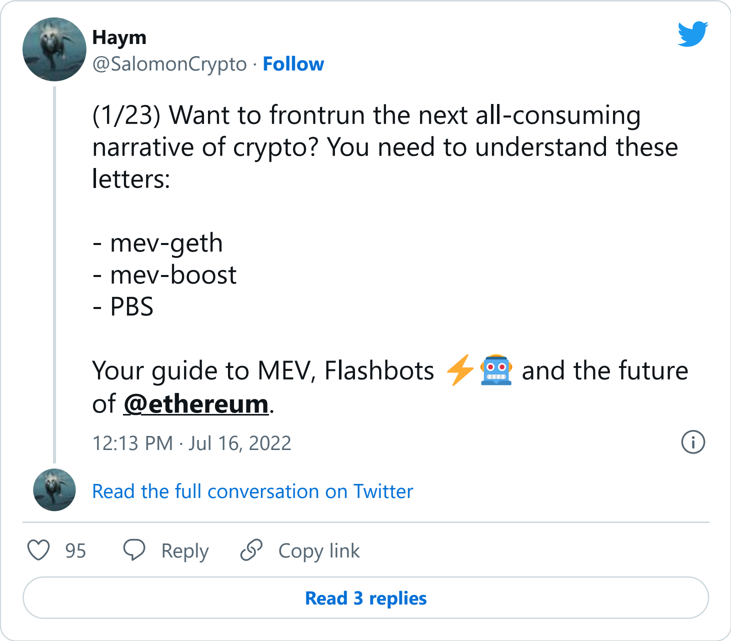
Read the full conversation on Twitter

471 Reply Copy link

Read 36 replies

(20/26) The team at Flashbots gave us a vision: highly specialized block builders. Each one will be a well resourced expert, finding MEV as aggressively as possible

They will compete to build the most attractive blocks in the hopes that the next proposing node picks their bundle



(1/23) Want to frontrun the next all-consuming narrative of crypto? You need to understand these letters:

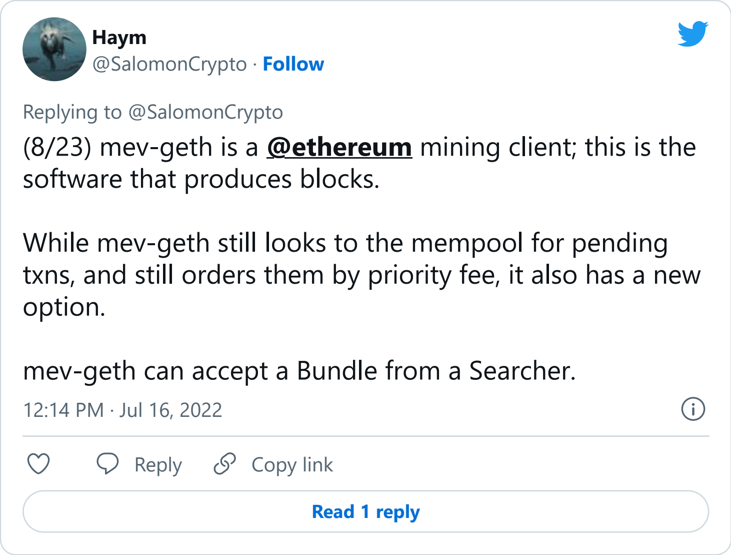
- mev-geth
- mev-boost
- PBS

Your guide to MEV, Flashbots ⚡🤖 and the future of @ethereum.

12:13 PM · Jul 16, 2022

(21/26) Phase 1: mev-geth, which provided a private channel for block builders to send txn bundles/blocks to nodes with upcoming proposals.

Rather than find MEV themselves, these nodes can access the channel and pick the highest profit opportunity.



Replying to @SalomonCrypto

(8/23) mev-geth is a @ethereum mining client; this is the software that produces blocks.

While mev-geth still looks to the mempool for pending txns, and still orders them by priority fee, it also has a new option.

mev-geth can accept a Bundle from a Searcher.

12:14 PM · Jul 16, 2022

(22/26) Phase 2: mev-boost, which adapts mev-geth for Proof of Stake and extends it by creating a two sided marketplace.

Any node can access mev-boost for extra MEV yield and any block builders can submit bundles.

Haym
@SalomonCrypto · Follow

Replying to @SalomonCrypto

(15/23) They say "v2 is always what the founder originally had in mind."

mev-boost is a middleware in which validators can sell their blockspace to not just Flashbots, but to other builders as well.

writings.flashbots.net
Why run mev-boost? | Flashbots
This article explains the benefits of mev-boost to the network and to validators, node operators, and staking pools.

12:14 PM · Jul 16, 2022

(23/26) This new architecture allow has incredible benefits:

- nodes get equal access to MEV
- block builders get many more bundles/blocks
- block builders can specialize and centralize without affecting the decentralization of @ethereum

(24/26) mev-boost is a huge step towards solving the problem, but it still rests on centralization through Flashbots and some implicit trust assumptions.

Thus, the endgame of Flashbots is to fold itself directly into @ethereum. The endgame of the World Computer is Enshrined PBS.

(25/26) mev-boost is a piece of additional software that bolts PBS on top of @ethereum, but the long term plan is to enshrine it into the World Computer by building it into the core protocol specs.

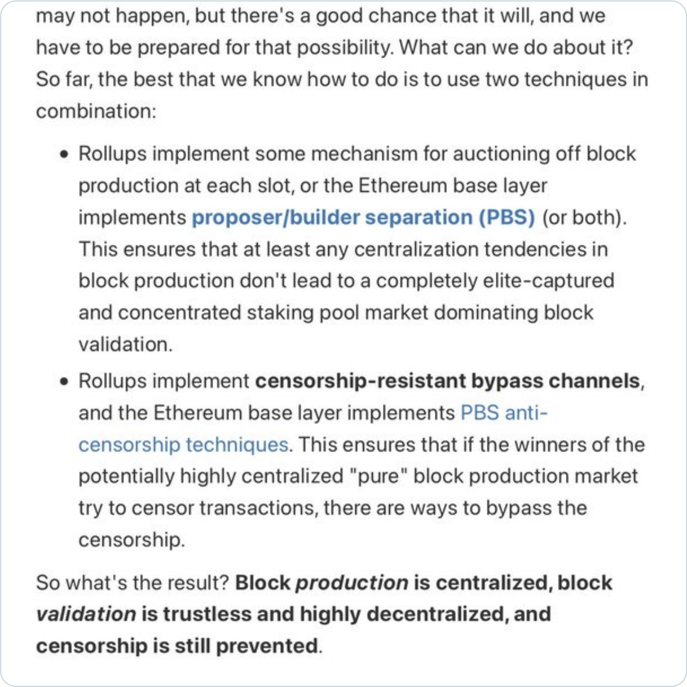
Haym
@SalomonCrypto · **Follow**

Replying to @SalomonCrypto

(18/23) PBS is so big that it's eventually going to be folded directly into **@ethereum**'s core infrastructure.

Check out **@VitalikButerin**'s endgame post.

vitalik.ca/general/2021/1...



may not happen, but there's a good chance that it will, and we have to be prepared for that possibility. What can we do about it? So far, the best that we know how to do is to use two techniques in combination:

- Rollups implement some mechanism for auctioning off block production at each slot, or the Ethereum base layer implements **proposer/builder separation (PBS)** (or both). This ensures that at least any centralization tendencies in block production don't lead to a completely elite-captured and concentrated staking pool market dominating block validation.
- Rollups implement **censorship-resistant bypass channels**, and the Ethereum base layer implements PBS anti-censorship techniques. This ensures that if the winners of the potentially highly centralized "pure" block production market try to censor transactions, there are ways to bypass the censorship.

So what's the result? **Block *production* is centralized, block *validation* is trustless and highly decentralized, and censorship is still prevented**.

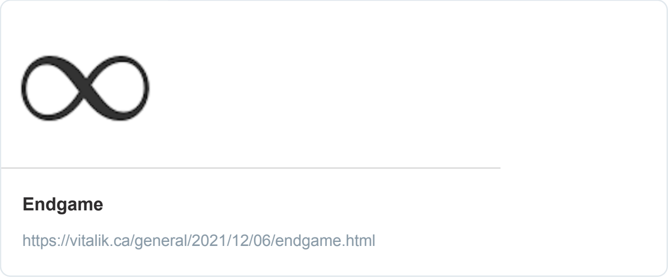
12:14 PM · Jul 16, 2022

♡ 2 Reply Copy link

Read 1 reply

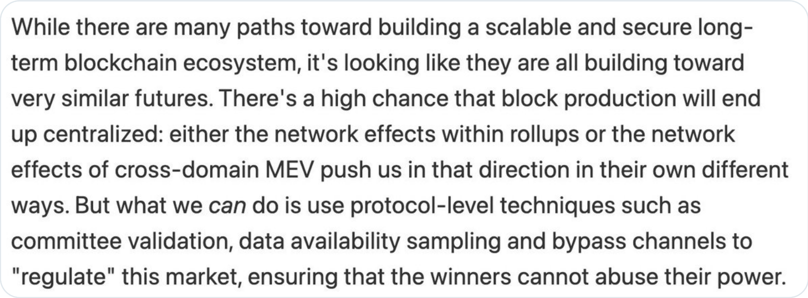
(26/26) And so, we are charting a course towards a decentralized @ethereum that has centralized block production; a cutthroat game of MEV transformed into fair access for all nodes.

This is @VitalikButerin's Ethereum Endgame.



Endgame

https://vitalik.ca/general/2021/12/06/endgame.html



While there are many paths toward building a scalable and secure long-term blockchain ecosystem, it's looking like they are all building toward very similar futures. There's a high chance that block production will end up centralized: either the network effects within rollups or the network effects of cross-domain MEV push us in that direction in their own different ways. But what we *can* do is use protocol-level techniques such as committee validation, data availability sampling and bypass channels to "regulate" this market, ensuring that the winners cannot abuse their power.

Like what you read? Help me spread the word by retweeting the thread (linked below).

Follow me for more explainers and as much alpha as I can possibly serve.

Haym
@SalomonCrypto · **Follow**

(1/26) **@ethereum** Roadmap: Proposer-Builder Separation

The Merge was successful, **$ETH** is Proof of Stake! As the era of miners closes, we find ourselves entering a new meta: the age of MEV

Your guide to existential threat facing Ethereum... and the plan to vanquish it

11:38 PM · Sep 15, 2022

Read the full conversation on Twitter

• • •