CS251 Fall 2023

(cs251.stanford.edu)

(1) Maximal Extractable Value, (2) NFT Marketplaces

Dan Boneh

HW#3 posted

Where we are in the course

- How consensus protocols work
- **Bitcoin**: the UTXO model, and the Bitcoin scripting language
- **Ethereum** (the blockchain computer): the EVM and Solidity

Current topic: **decentralized finance**

on-chain: exchanges, stablecoins, today: MEV

Next: privacy on the blockchain, scaling the blockchain,
and interoperability across blockchains

Decentralized Finance (DeFi)

- **Permissionless**: any financial instrument can be implemented and deployed with a few lines of Solidity code

(a centralized system could refuse to deploy a competing service)

- **Transparent**: Dapp code and Dapp state are public

$\Longrightarrow$ Anyone can inspect and verify

- **Composable**: Dapps can call one another

ERC-20 standard enables interoperability (6 functions)

Why DeFi? Failures of the existing financial system

- **Cross border inefficiency**:

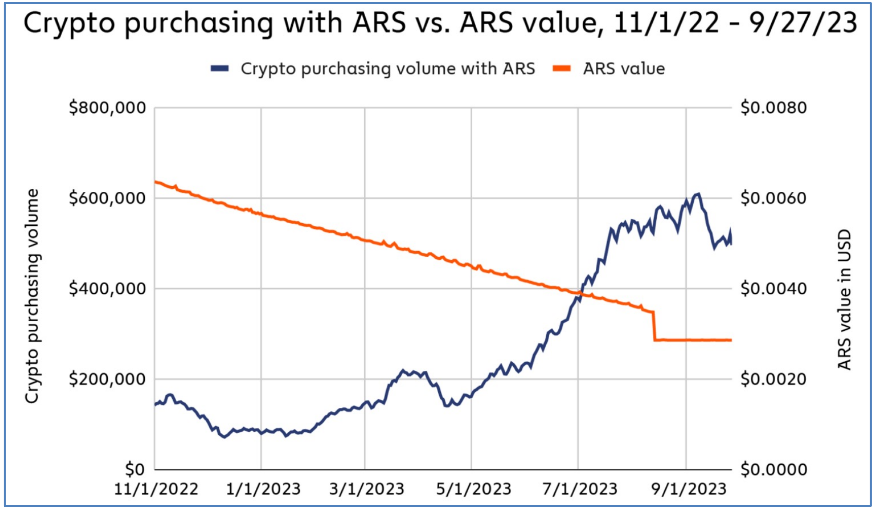
  send $10 to south america ⇒ 36% fees

- **The high cost of being poor in america:**

  In 2019, **5.4 percent** of US households were unbanked

- **Economies with an unstable fiat currency**

Why DeFi? Failures of the existing financial system



USDC/USDT daily purchasing volume
in Argentina during inflation

> “As crypto adoption has grown,
> lots of people [in Argentina] will now
> get their paycheck and immediately
> put it into USDT or USDC.”
>
> Alfonso Martel Seward, Lemon Cash

https://www.chainalysis.com/blog/latin-america-cryptocurrency-adoption/

Maximal Extractable Value (MEV)

Searchers

Ethereum gives rise to a new type of business: **searchers**

- **Arbitrage:** Uniswap DAI/USDC exchange rate is 1.001
  whereas at Sushiswap the rate is 1.002

  ⇒ a searcher posts Tx to equalize the markets and profits

- **Liquidation**: suppose there is a liquidation opportunity on Aave

  ⇒ a searcher posts a liquidation Tx and profits

- Many other examples … often using a sequence of Tx (a bundle)

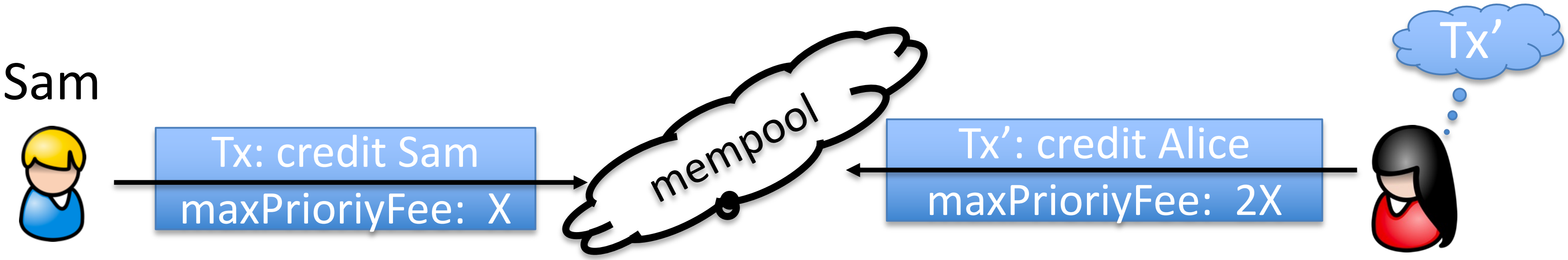
The MEV problem

What happens when a searcher posts a Tx to the mempool?

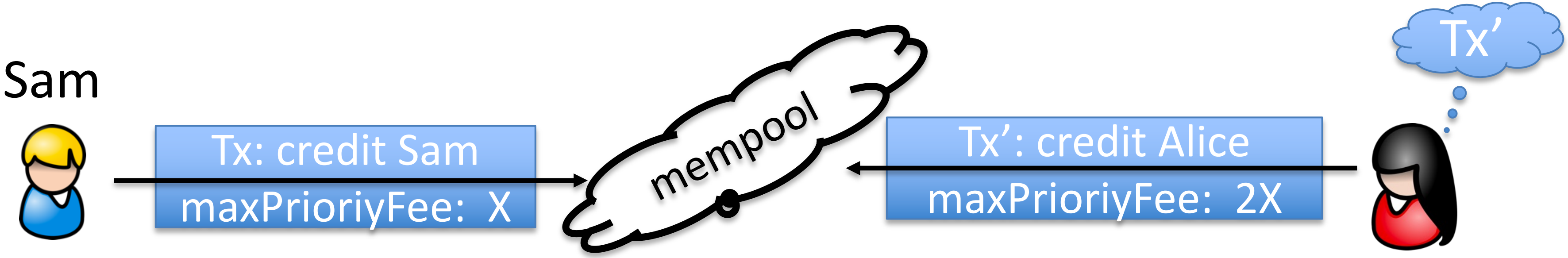
- **Validator:** create a new Tx' with itself as beneficiary, and place it before Sam's Tx in the proposed block

- **Another searcher:** create a new Tx' with itself as beneficiary, and posts it with a higher *maxPrioriyFee*

⇒ this action is now mostly automated by copy-paste bots



The MEV problem



Sam

Tx: credit Sam

maxPrioriyFee: X

mempool

Tx': credit Alice

maxPrioriyFee: 2X

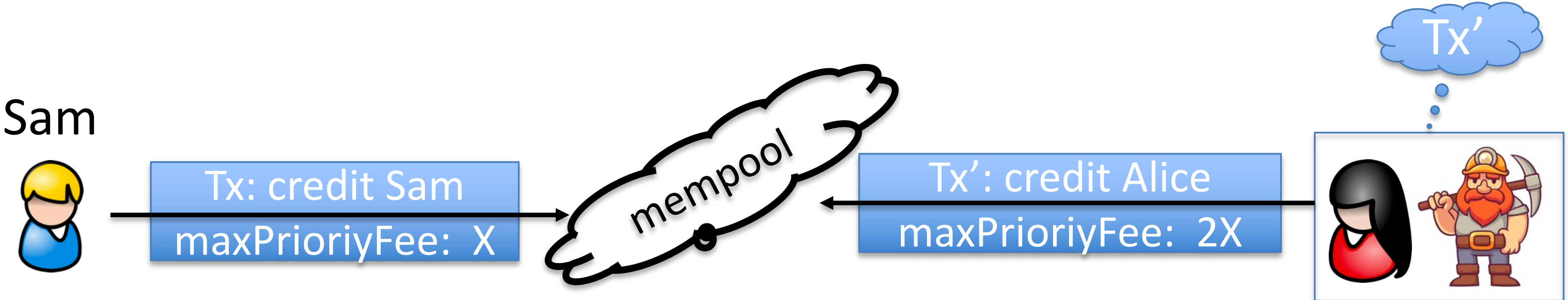
Tx'

The result harms honest users

Price Gas Auctions (PGA): many searchers compete

- Repeatedly submit a Tx with higher and higher *maxPriorityFee* until a validator chooses one … happens within a few seconds

⇒ causes congestion (lots of Tx in mempool) and high gas fees



Sam

Tx: credit Sam
maxPrioriyFee: X

mempool

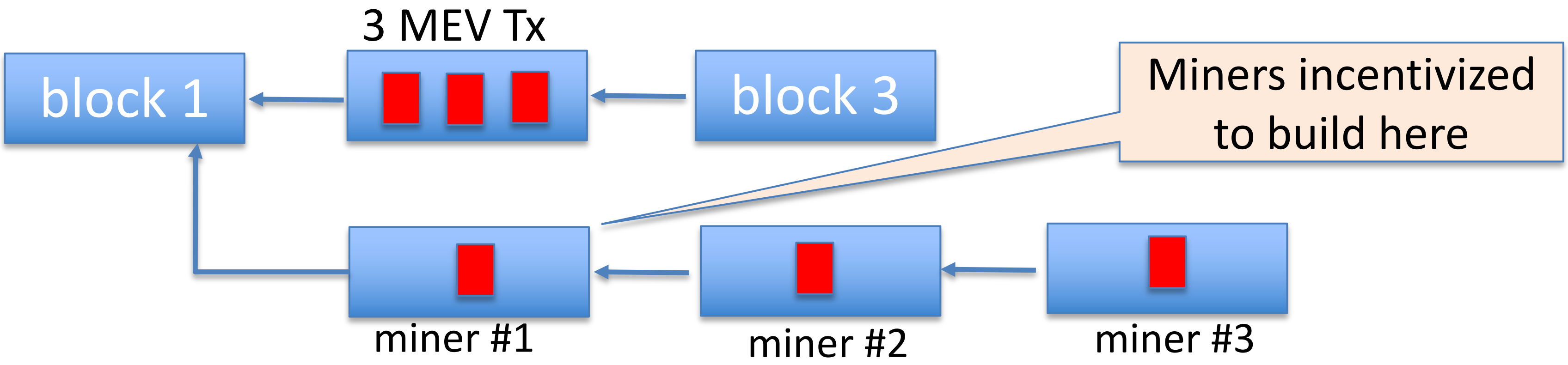
Tx’: credit Alice
maxPrioriyFee: 2X

Tx’

The result harms consensus

Undercutting attack on <u>longest-chain</u> consensus (not Ethereum):

Rational miner: can cause a re-org by taking one MEV Tx for itself and leave two for other miners



The problem: MEV Tx generate extra revenue for miners, higher than block rewards

The result causes centralization

Validators can steal MEV Tx from searchers ⇒ **Private mempools**

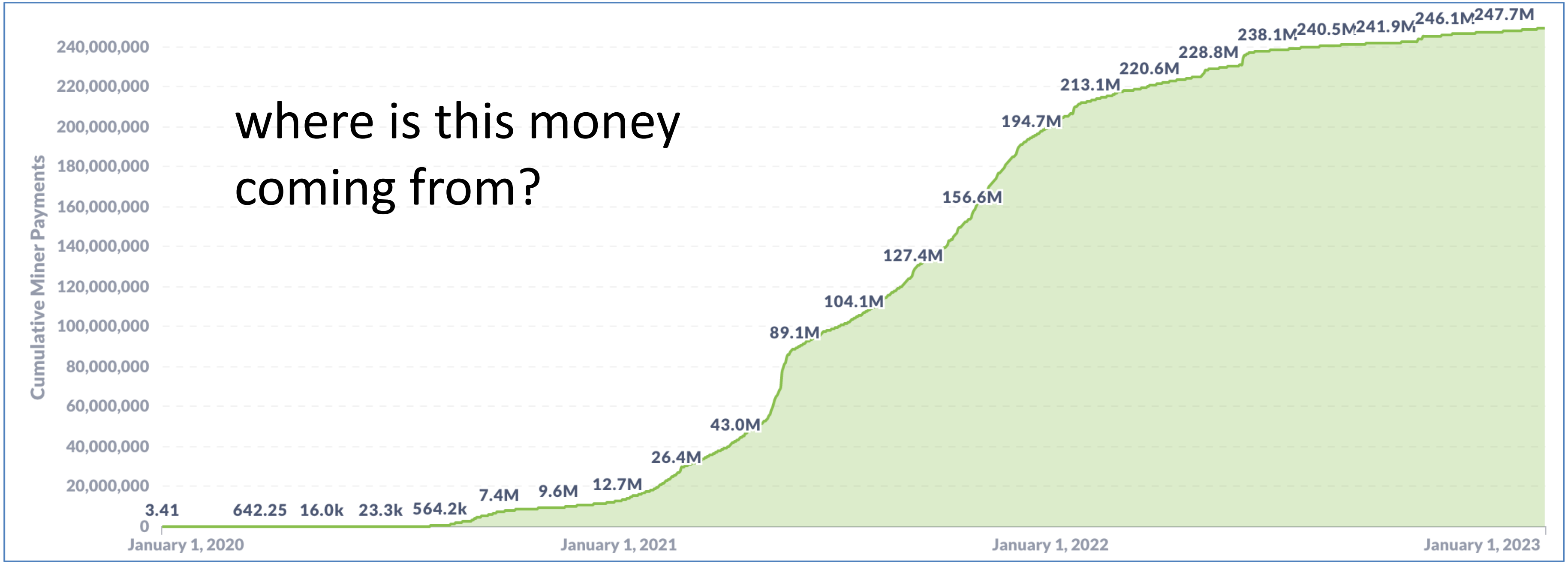
Searchers only send Tx to a validator they trust
(have a business relation with)

These validators do not propagate Tx to the network,
but put them in blocks themselves

In the long run: a few validators will handle the bulk of all Tx

How big are MEV rewards?

Cumulative MEV payments to validators since Nov. 2020: ($247M)

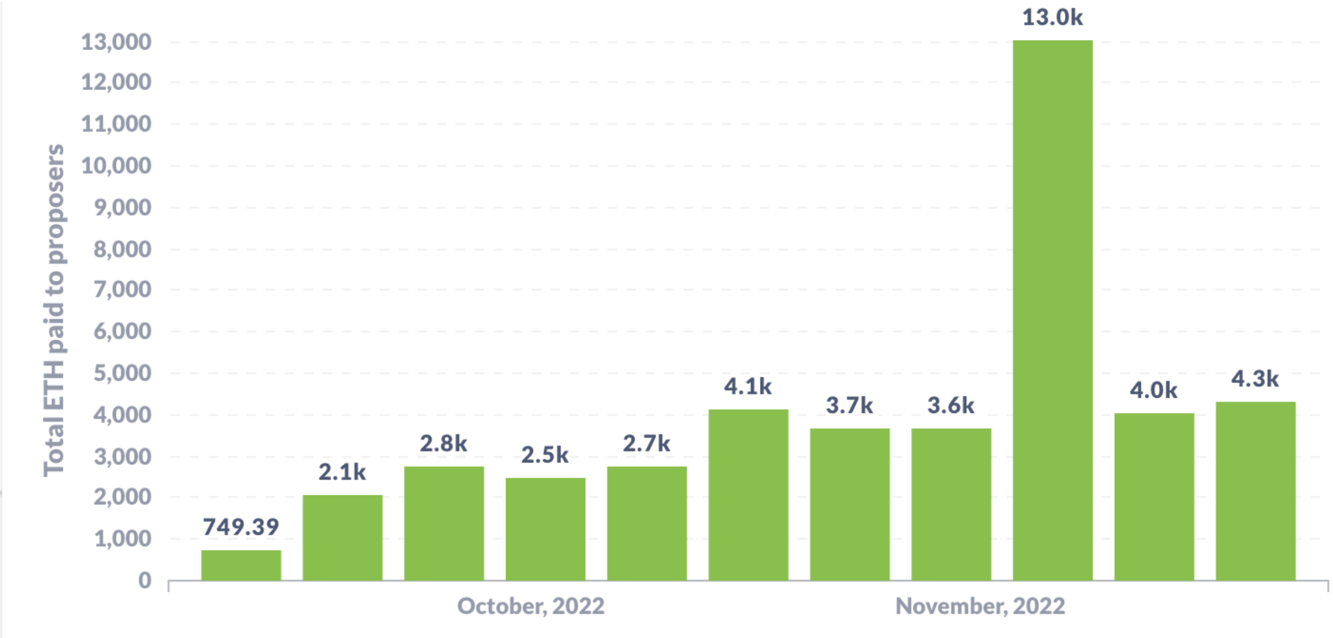


where is this money coming from?

source: explore.flashbots.net

How big are MEV rewards?

Weekly MEV amount paid to validators (in ETH):



source: transparency.flashbots.net

What to do??

Two options

Option 1:

- Accept MEV is unavoidable; minimize its harm to the ecosystem

  ⇒ Flashbots

Option 2:

- Try to prevent some MEV, by removing the block proposer's choice in ordering Tx in a block. (mostly in research papers)

Option 1: Proposer Builder Separation (PBS)

Goals:

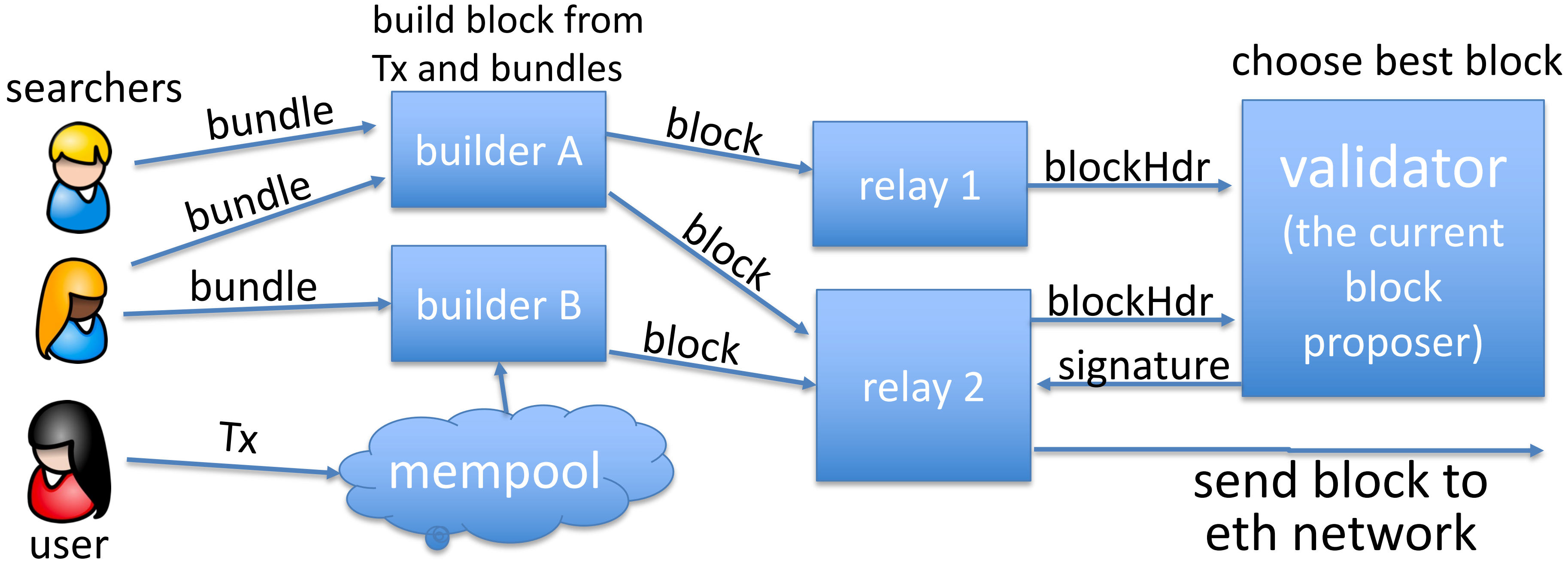
- Eliminate price gas auctions in the public mempool
  - Instead, create an off-chain market for searchers to compete on the position of their bundles in a block
- Prevent validator concentration: make it possible for every validator to earn MEV payments from searchers

Current PBS implementation: **MEV-boost**

The participants in PBS (as in MEV-boost)

Users have Tx and searchers have bundles (sequence of Tx)

- searcher wants its bundle posted in a block unmodified



MEV-boost

Builder: collects bundles and Tx, builds a block   (≈300 bundles/block)

- includes a MEV offer to validator (feeRecipient)

Relay: collects blocks, chooses block with max MEV offer

- sends block header (and MEV offer) to block proposer
- Can’t expose Tx in block to proposer (proposer could steal Tx)

Proposer: chooses best offer and signs header with its staking key

⇒ Then Relay sends block to network, making it public

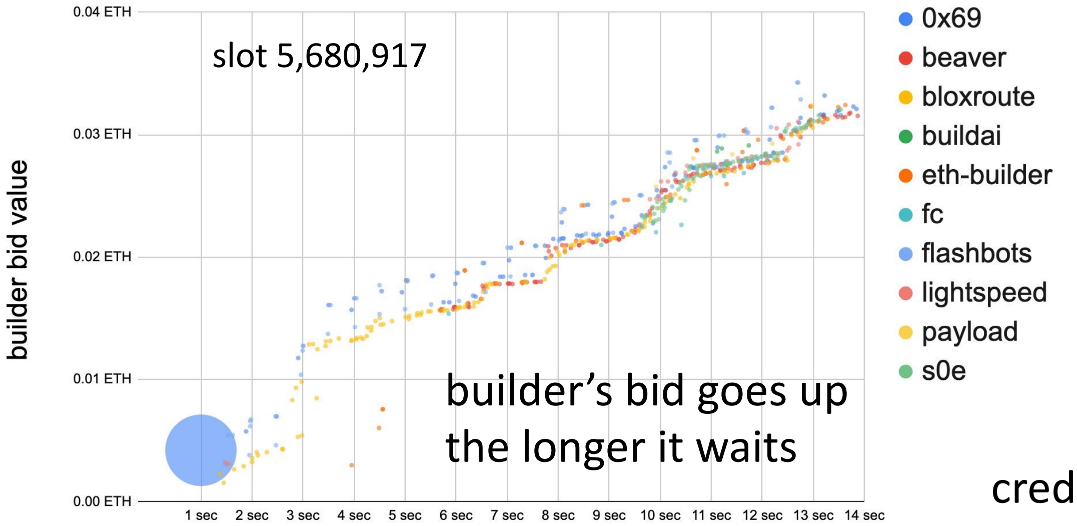
⇒ Now, proposer cannot steal MEV (would be exposed to slashing)

https://writings.flashbots.net/searching-post-merge

Many block options per slot

A relay might receive 500 blocks per slot from builders

- Each builder might send 20 blocks to relay for one slot
- Why? The longer builder waits the more MEV opportunities …



slot 5,680,917

builder's bid goes up the longer it waits

credit: Justin Drake and Shea Ketsdever

Operating relays

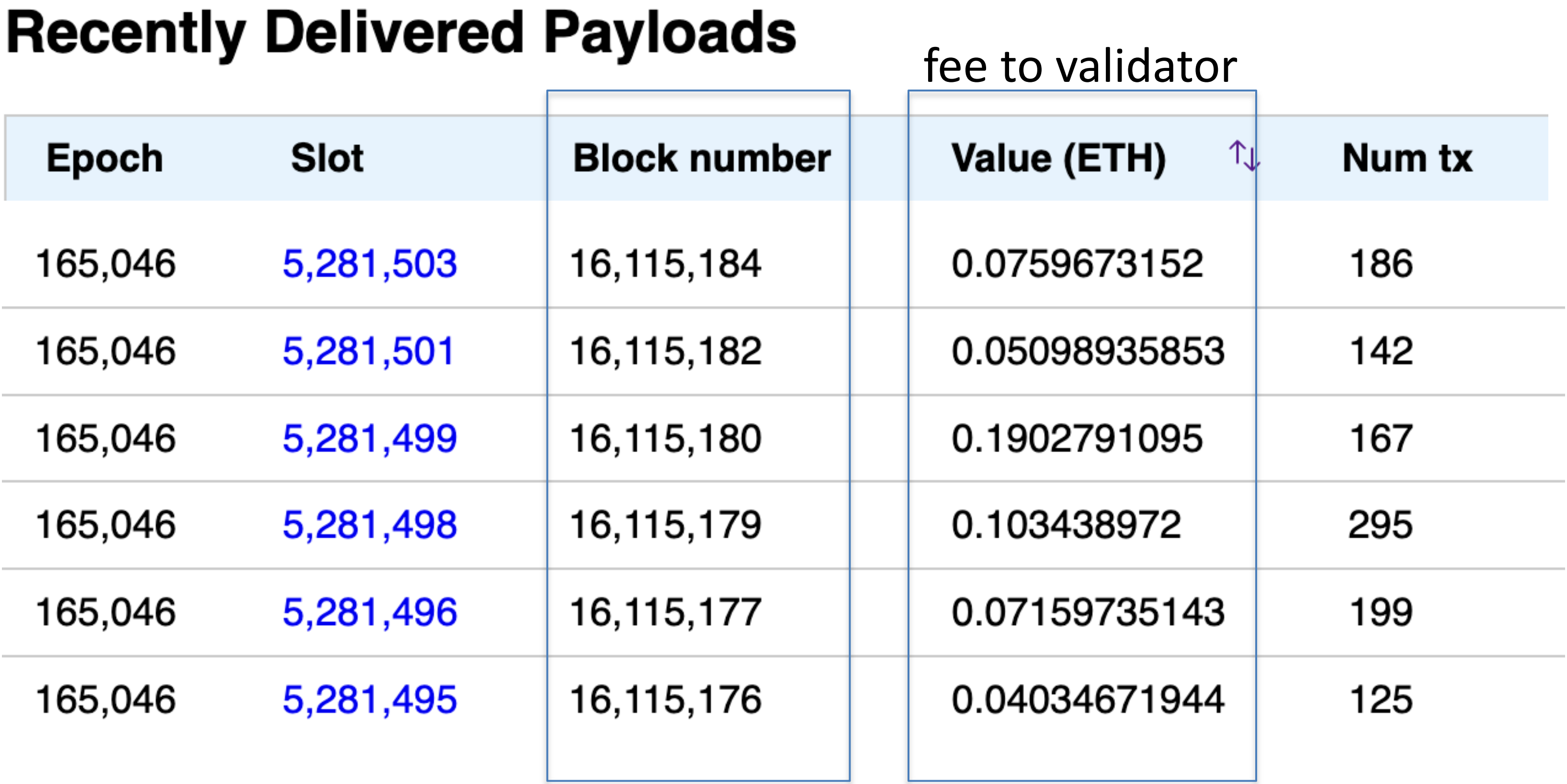
Flashbots: Filters out OFAC sanctioned addresses,
aims to maximize validator payout
(so that many validators will work with it)

BloXroute: no censorship, aims to maximize validator payout

UltraSound: not for profit, non censoring

…

An example: flashbots relay

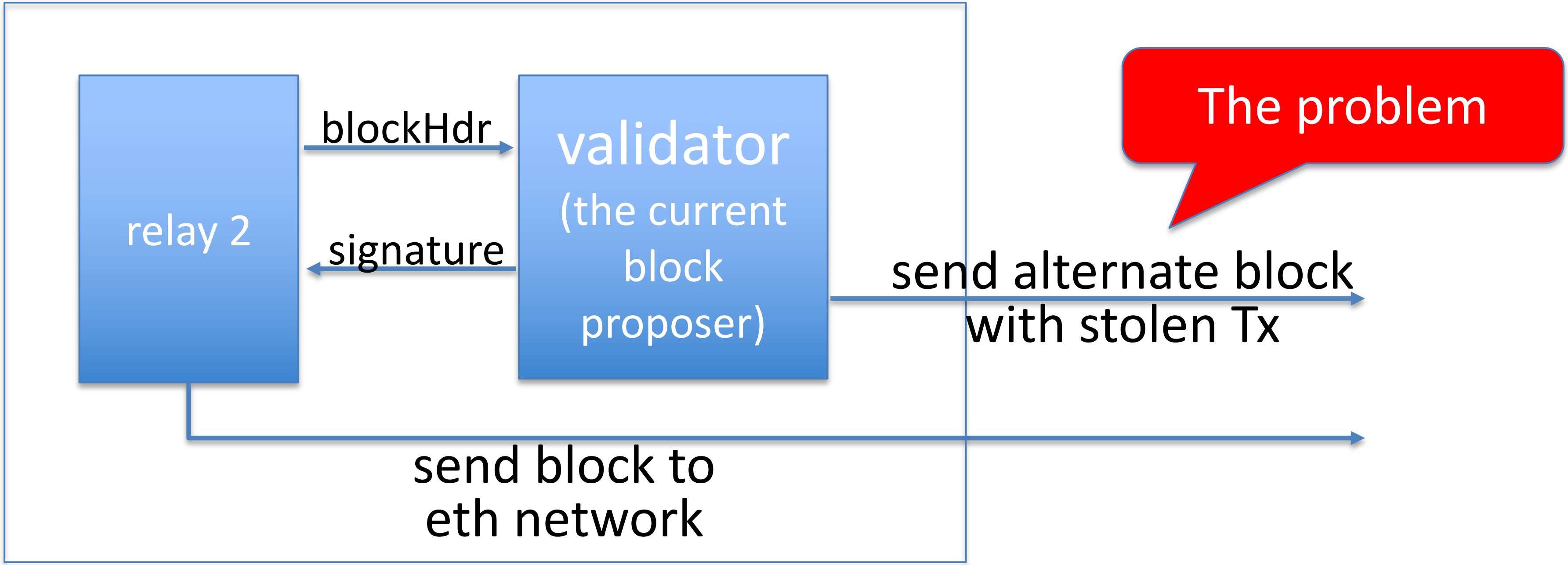


Recently Delivered Payloads

fee to validator

Epoch	Slot	Block number	Value (ETH) ↑↓	Num tx
165,046	5,281,503	16,115,184	0.0759673152	186
165,046	5,281,501	16,115,182	0.05098935853	142
165,046	5,281,499	16,115,180	0.1902791095	167
165,046	5,281,498	16,115,179	0.103438972	295
165,046	5,281,496	16,115,177	0.07159735143	199
165,046	5,281,495	16,115,176	0.04034671944	125

The race problem


relay 2
blockHdr
signature
validator
(the current block proposer)
send alternate block with stolen Tx
send block to eth network
The problem

Block proposer will be slashed (why?) ⇒ Lose 1 ETH

… but can gain much more in stolen MEV.

Are we done? Not quite …

Builder concentration: three builders build 75% of all blocks !!

- Clear centralization in the builder market
- Enables censorship by builders

(builder0x69,beaverbuild,Flashbots)

Proposers hold all the power (first price auction among builders)

⇒ Most MEV profits flow to block proposers

MEV-boost is not designed for cross-chain MEV

- For cross-chain arbitrage, no atomicity guarantee for bundle

The next step: SUAVE

Goals:

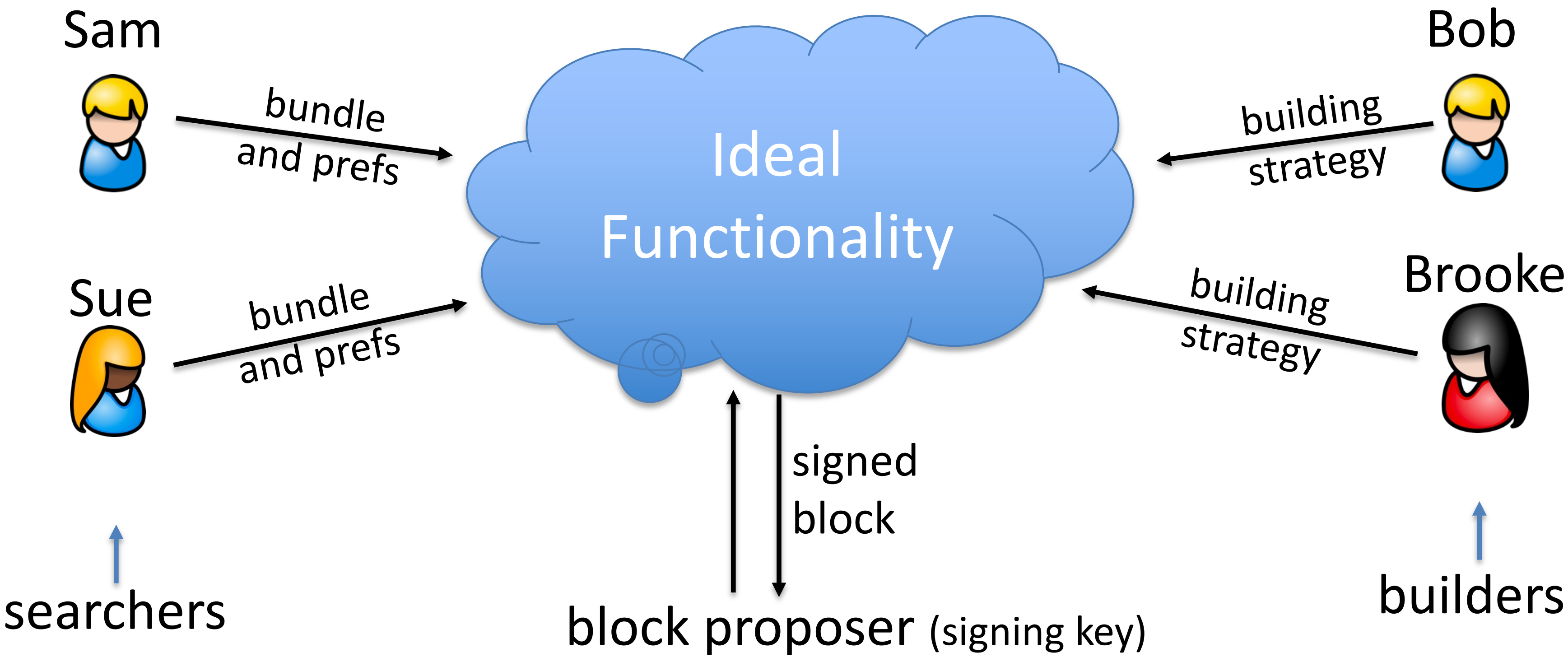
- Tx should be private (encrypted) until signed by block proposer

  ... but should be available to all block builders to build blocks

Seems contradictory! crypto to the rescue:

⇒ requires a massive MPC or secure HW enclaves

The SUAVE Multiparty Computation



Sam

bundle and prefs

Sue

bundle and prefs

searchers

Ideal Functionality

signed block

block proposer (signing key)

Bob

building strategy

Brooke

building strategy

builders

Option 2:
Fair Ordering of Transactions

Can we reduce MEV?

1. **Randomize transactions before executing**
   Downside: spamming with identical extracting transaction

2. **Time-Based Order-Fairness**

3. **Blind Order-Fairness**

4. **Trusted execution environments (TEEs)** to order transactions
   Downside: hardware assumption

5. **More ideas? Your idea here …**

Aequitas: Time-Based Order-Fairness

Basic idea: if most validators received tx1 before tx2, then tx1 should precede tx2 in the final ordering.

The problem of **Condorcet cycles**:

- validator #1: [tx1, tx2, tx3]
- validator #2: [tx2, tx3, tx1]
- validator #3: [tx3, tx1, tx2]

Two received (tx1 before tx2) AND two received (tx2 before tx3) AND two received (tx3 before tx1)

⇒ No ordering !!

A possible solution: reject entire cycle if Tx in cycle conflict.

[Kelkar-Zhang-Goldfeder-Juels 2020]

Aequitas: Time-Based Order-Fairness

Block-Fair-Ordering protocol:

1. Miners broadcast their order preferences.
2. Build a graph of transactions:
   1. Vertices = transactions present in a large number of orderings,
   2. Edge(tx1 → tx2) if tx1 comes before tx2 in most orderings.
3. Collapse strongly connected components to a single vertex.
4. Topologically sort vertices.
5. Final an ordering that respects the sort.

[Kelkar-Zhang-Goldfeder-Juels 2020]

More Time-Based Order-Fairness Protocols

- Problem: Advantages searchers with better connectivity
- High communication: $\boldsymbol{O(n^3)}$.

Themis: same goals as Aequitas, but only $\boldsymbol{O(n^2)}$ communication.

"Themis: Fast, Strong Order-Fairness in Byzantine Consensus" by Kelkar-Deb-Long-Juels-Kannan 2021

A different approach: **blind order-fairness**

Blind order fairness: three phases:

- **Commit transactions**:
  users send **commitments** to their transactions
  (Tx data remains hidden from block proposer)

- **Order commitments**:
  block proposer orders commitments into a block.

- **Reveal transactions**:
  once block is finalized commitments are revealed
  (by validators or "automatically"). Too late to steal MEV.

Blind Order-Fairness

Construction #1: threshold encryption (Osmosis chain):

- Setup: validators generate pk, threshold share a secret key sk
- **Commit (tx):** users send $ct \leftarrow$ Encrypt(pk, Tx)
- **Reveal** (by validators): once block is finalized:

  Validators jointly decrypt ct: Tx ← Decrypt(sk, ct)

Reiter-Birman, 1994
Cachin-Kursawe-Petzold-Shoup, 2001

Blind Order-Fairness

Construction #2: timed-commitments

- **Commit (tx):** user sends $ct \leftarrow \mathrm{TimeCommit}(\mathrm{Tx})$

- **Reveal** (by anyone):
  - Anyone can open the commitment ct using ten minutes of sequential computation … by then block is finalized.

Note: need a batch timed-commitment to avoid 10 mins per Tx !

More ideas needed!

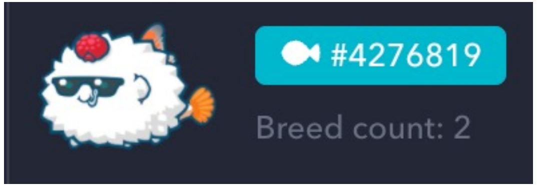
An active area of research

New topic: the World of NFTs

Digital assets (NFTs)

Example digital assets: (ERC-721)

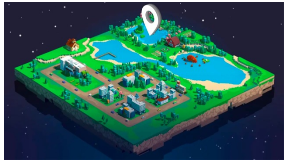
- Gaming assets: axies, DFK Heroes, …
- Memberships: Proof collective (access to events)
- Domain names: ENS
- Sports collectible: NBA top shots
- Virtual worlds: plots in a virtual land
- Art



#4276819

Breed count: 2

NBA top shots



Digital assets (NFTs)

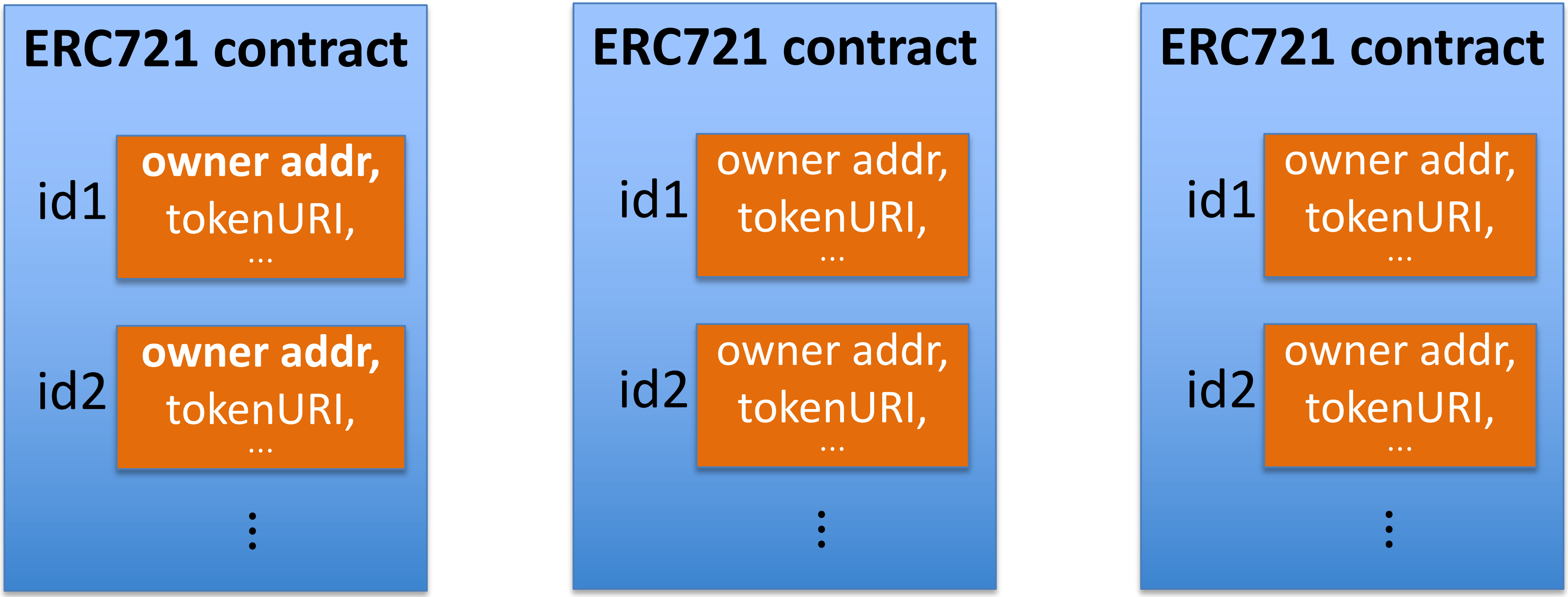
No two NFTs are the same: they are not mutually exchangeable

- NFTs are defined by their: history, utility, appearance, etc.

Why not manage in a central DB?

- Blockchain ensures long-term ownership, until sale.
- Provides a trusted record of provenance (forgeries are evident)

The ERC-721 standard



ERC721 contract

id1 **owner addr,** tokenURI, …

id2 **owner addr,** tokenURI, …

⋮

NFT collection

ERC721 contract

id1 owner addr, tokenURI, …

id2 owner addr, tokenURI, …

⋮

Another NFT collection

ERC721 contract

id1 owner addr, tokenURI, …

id2 owner addr, tokenURI, …

⋮

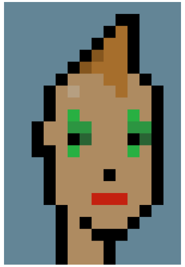
NFT collection

The ERC-721 standard (subset)

```
mapping (uint256 => address)   internal   idToOwner;

function safeTransferFrom(
      address _from,  address _to,  uint256 _tokenId,  bytes data)

function approve(address _approved, uint256 _tokenId)

function setApprovalForAll(address _operator, bool _approved)

function ownerOf(uint256 _tokenId) returns (address);
```

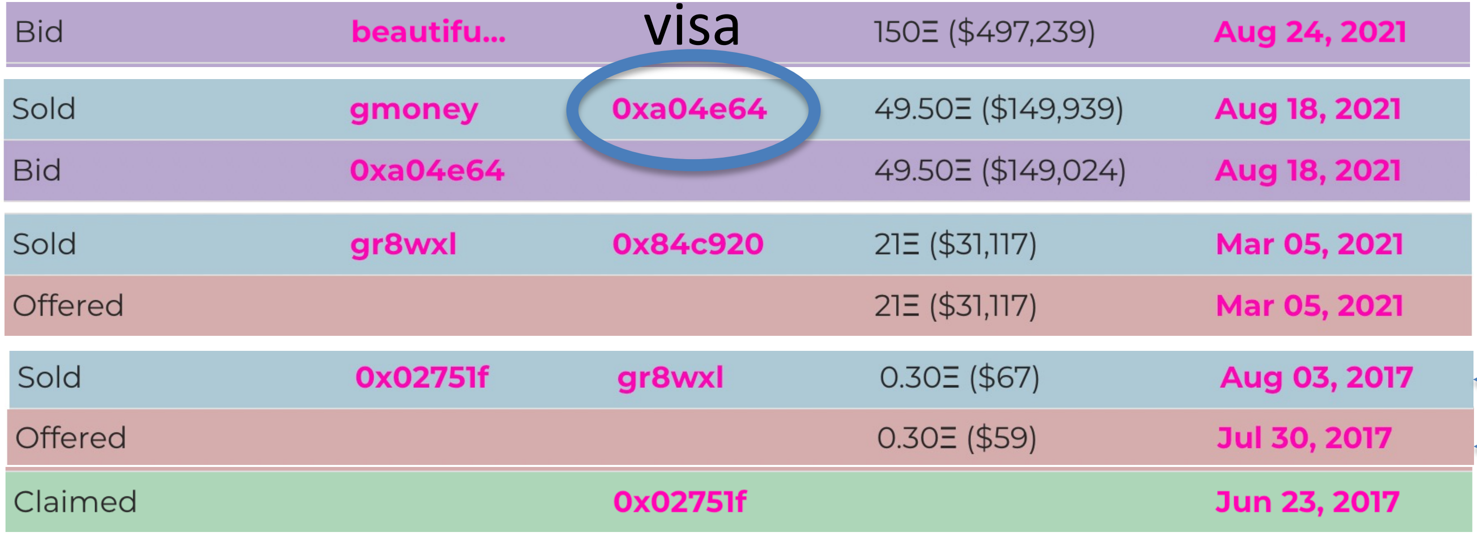
Example: CryptoPunks (2017, predates ERC-721)

10,000 total CryptoPunks. Managed by contract at Ethereum address 0xb47e3cd8DF8… (250 lines of solidity)



#7610

on-chain marketplace:



visa

Bid	beautifu…		150Ξ ($497,239)	Aug 24, 2021
Sold	gmoney	0xa04e64	49.50Ξ ($149,939)	Aug 18, 2021
Bid	0xa04e64		49.50Ξ ($149,024)	Aug 18, 2021
Sold	gr8wxl	0x84c920	21Ξ ($31,117)	Mar 05, 2021
Offered			21Ξ ($31,117)	Mar 05, 2021
Sold	0x02751f	gr8wxl	0.30Ξ ($67)	Aug 03, 2017
Offered			0.30Ξ ($59)	Jul 30, 2017
Claimed		0x02751f		Jun 23, 2017

buy offer

sold!

sell offer

https://www.larvalabs.com/cryptopunks/details/7610

The NFT ecosystem

Fractional ownership: buy a fraction of an NFT with a large group

- such as an expensive gaming asset (a spaceship)
- control it with the group (governance, collaborative work)

Lending/borrowing an NFT: (enabled by extensions to ERC-721)

- Lend a gaming NFT or a domain name for someone to use
- Try-before-you-buy experience

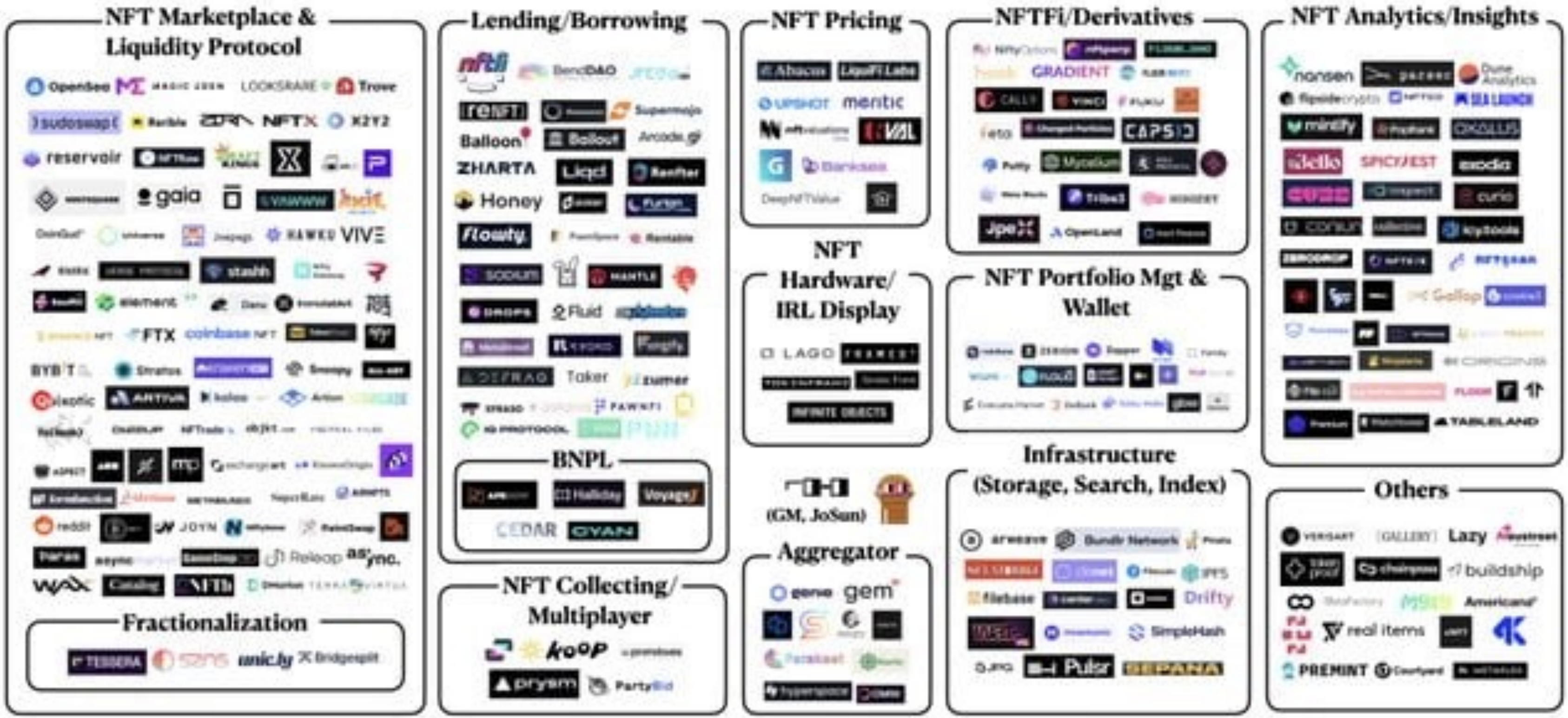
Use an NFT as collateral for a loan (need continuous price estimates)

NFT derivatives markets, NFT pricing services

GBV

The NFTFi Ecosystem

@0xminion
@alexgedevani



Caveats:

- Not all encompassing. Does not include a few big verticals that also touch NFTs: Photography, Music, Fashion, Metaverse, Reputation/Identity
- Some products overlap in multiple areas but are only listed once. Some in stealth are adding competing products in adjacent markets
- Have not mapped all chains supported. Ethereum leads in activity but most products will go multichain

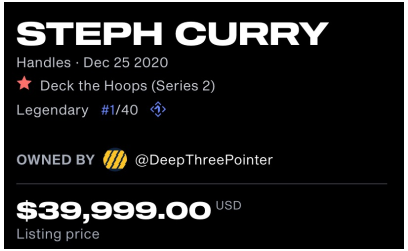
Aug 2022

Royalties

With ERC-721 it is quite easy to code up any royalty plan:

- example: on every sale of asset, send 1% royalty to creator.

(think: NBA Top Shots)



STEPH CURRY

Handles · Dec 25 2020

★ Deck the Hoops (Series 2)

Legendary #1/40

OWNED BY @DeepThreePointer

$39,999.00 USD

Listing price

<u>Problem</u>: not hard to bypass this policy.

- Custodial marketplace owns the asset

  ⇒ shows on its web site that asset belongs to Bob

- When Bob sells asset to Carol, marketplace updates its web site.

  No on-chain Tx ⇒ no royalty payment to creator

Gaming Guilds

Inter-game financial institutions (Yield Guild Games)

What is it:

Source capital from LPs (by issuing a token)

⇒ Buy up swathes of virtual land and in-game items,

⇒ Generate revenue by **leasing** assets to players,

⇒ Pay LPs dividends,

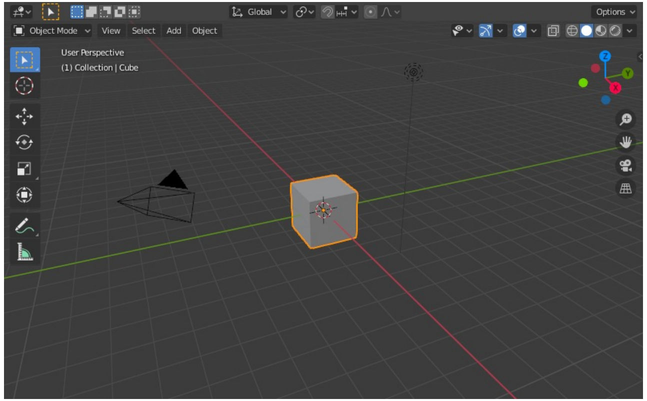
⇒ Accrue capital gains on the underlying assets.

Develop Virtual Land?

Successful platforms leverage the creativity of their users (UGC)

- NFTs let creators own, maintain, and control their creations

Challenge for everyone: turn a cube into a digital city.



=>

END OF LECTURE

Next lecture: The regulatory landscape