

A dark endgame

Sebastian Bürgel (HOPR Association)

Who do most Ethereum users trust today?

* not disrespectful, thank you for running infrastructure that we're all too lazy to run ourselves!



What does “trust” even mean?

Trust to not censor you

- ✓ FOSS
- ✓ standardization
- ✓ retail hardware requirements

Trust to deliver correct data

- ✓ run your own node
- ✓ light client verification (can we pls start using this?! Shout-out: kevlar.sh)

Trust to not track your every move

- ✗ strong full-stack privacy (including data transport)

Lack of full stack privacy today

Application layer:

 Tracking & other web2.0 ugliness

Execution layer:

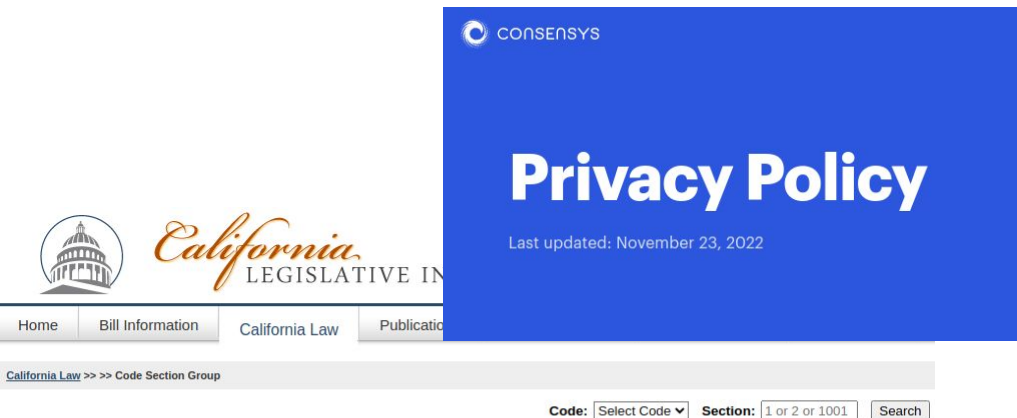
 On-chain privacy (ongoing: Tornado, zkBob, Umbra, Nocturne, Railgun, Aztec, etc)

 P2P leaks (solvers, builders, indexers)


Consensus layer:

 Validators are not private (and SSLI does not fix that)

The old world tries to enforce privacy



The screenshot shows the California Legislative Information website. A blue overlay with the text "CONSENSYS Privacy Policy" is centered on the page. Below the overlay, the website's navigation bar is visible, including "Home", "Bill Information", "California Law", and "Publications". The California State Capitol logo and the text "California LEGISLATIVE INFORMATION" are also present.

web3privacy <small>now</small>			PERSONAL INFORMATION COLLECTION	
From You	Automatically	From Third Parties		
Unique Identifiers <ul style="list-style-type: none">• account number• including Ethereum wallet address• or other similar identifiers Communications and Interactions <ul style="list-style-type: none">• records of your contact details• communications• interactions• our responses	Device and Browsing Information <ul style="list-style-type: none">• device identifiers• log information• network connectivity information. Transaction Data <ul style="list-style-type: none">• monitor and collect transactions Activities and Usage <ul style="list-style-type: none">• activity information	Not specified Personal information		
total: min 13 various data types are collected				

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

CIVIL CODE - CIV

DIVISION 3. OBLIGATIONS [1427 - 3273.55] (Heading of Division 3 amended by Stats. 1988, Ch. 160, Sec. 14.)

PART 4. OBLIGATIONS ARISING FROM PARTICULAR TRANSACTIONS [1738 - 3273.55] (Part 4 enacted 1872.)

TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100] (Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3.)

[1798.100](#). General Duties of Businesses that Collect Personal Information

DECENTRALIZE ALL THE THINGS!



**TRUST ALL RANDOS ON THE INTERNET TO NOT
DATA HARVEST EVERYTHING THEY CAN ABOUT ME AND
NOT USE IT AGAINST ME IN THE WORST POSSIBLE WAY?!**



Connecting to a non-private EL allows randos on the internet to

- Link all your Ethereum accounts
- Link your accounts to off-chain identities
- See all data that you will see, even before you

→ Your IP address is your primary identifier on a non-private EL!

How to screw users in a yolo-decentralized non-private web3

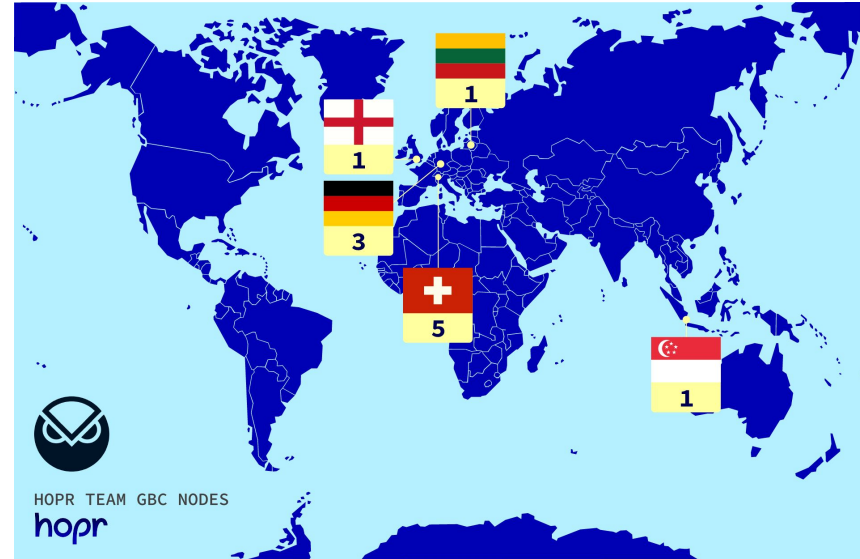
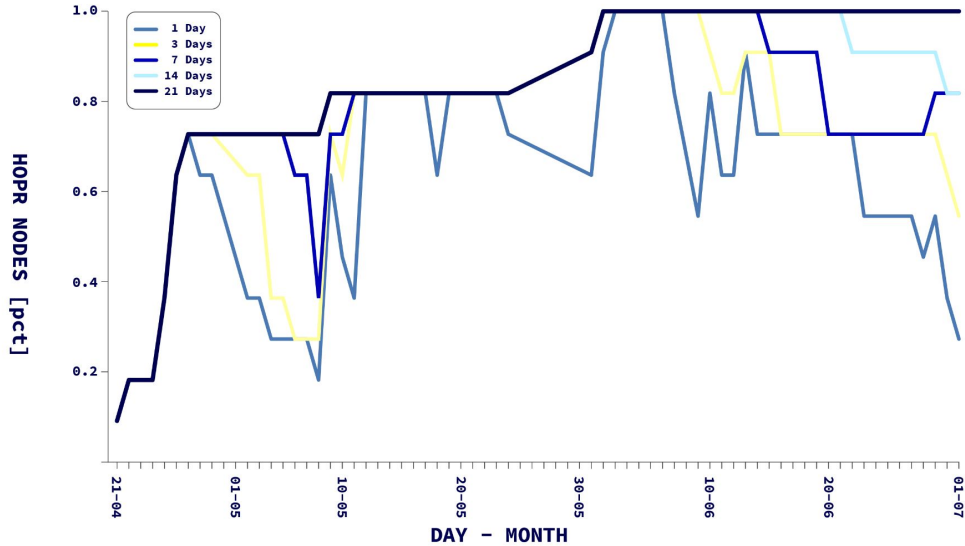
Example: fully decentralized app.uniswap.eth (without regards for privacy)

Infrastructure: ENS + IPFS + TheGraph + Pokt

1. Identify active users by harvesting IPFS DHT queries
2. Predict next action of user by harvesting TheGraph queries
3. Frontrun mempool by harvesting eth_estimateGas or eth_sendRawTransaction calls

* not disrespectful, all example infrastructure projects are aware of these issues and working towards solutions

What about CL privacy?



<https://medium.com/hoprnet/proof-of-stake-validator-sniping-research-8670c4a88a1c>

<https://github.com/hoprnet/lighthouse>

...but is privacy really a problem and is anyone going to ever exploit this?!



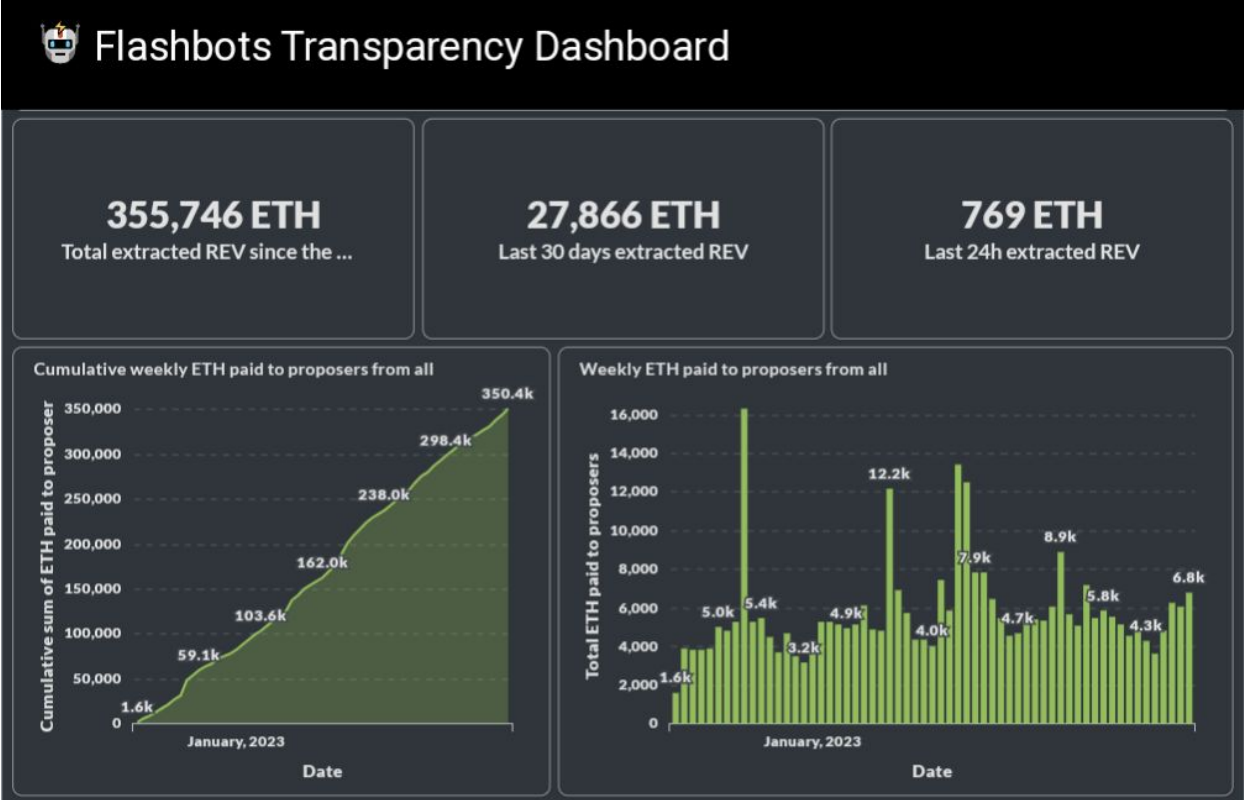
Today's sad state of Ethereum [d]app privacy:

* to be clear: Uniswap, this is a disgrace, especially for an IPFS deployment!

```
▼ Request Payload view source
{
  "api_key": "00000000000000000000000000000000",
  "events": [...],
  "op": "api_key: \"00000000000000000000000000000000\"",
  "events": [...],
  "0": {
    "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
    "sess": {
      "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
      "device_model": "Linux",
      "event_id": 20,
      "event_type": "$identify",
      "insert_id": "f0009217-b814-478f-950d-359ad170a26a",
      "language": "en-US",
      "library": "amplitude-ts/1.6.1",
      "os_name": "Chrome",
      "os_version": "119.0.0.0",
      "platform": "Web",
      "session_id": 1700267349438,
      "time": 1700267883150
    },
    "user_properties": {
      "$set": {
        "wallet_address": "0x288867c8C5A8E20F8aac5A031578067E2312f"
      }
    },
    "1": {
      "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
      "sess": {
        "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
        "device_model": "Linux",
        "event_id": 28,
        "event_type": "$identify",
        "insert_id": "777d3cee-fe10-410a-9259-c987fe03bec7",
        "language": "en-US",
        "library": "amplitude-ts/1.6.1",
        "os_name": "Chrome",
        "os_version": "119.0.0.0",
        "platform": "Web",
        "session_id": 1700267883338,
        "time": 1700267883338
      },
      "user_properties": {
        "$set": {
          "wallet_version": "MetaMask/v11.4.1"
        }
      }
    },
    "2": {
      "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
      "sess": {
        "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
        "device_model": "Linux",
        "event_id": 28,
        "event_type": "$identify",
        "insert_id": "777d3cee-fe10-410a-9259-c987fe03bec7",
        "language": "en-US",
        "library": "amplitude-ts/1.6.1",
        "os_name": "Chrome",
        "os_version": "119.0.0.0",
        "platform": "Web",
        "session_id": 1700267883338,
        "time": 1700267883338
      },
      "user_properties": {
        "$set": {
          "wallet_version": "MetaMask/v11.4.1"
        }
      }
    },
    "3": {
      "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
      "sess": {
        "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
        "device_model": "Linux",
        "event_id": 28,
        "event_type": "$identify",
        "insert_id": "777d3cee-fe10-410a-9259-c987fe03bec7",
        "language": "en-US",
        "library": "amplitude-ts/1.6.1",
        "os_name": "Chrome",
        "os_version": "119.0.0.0",
        "platform": "Web",
        "session_id": 1700267883338,
        "time": 1700267883338
      },
      "user_properties": {
        "$set": {
          "wallet_version": "MetaMask/v11.4.1"
        }
      }
    },
    "4": {
      "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
      "sess": {
        "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
        "device_model": "Linux",
        "event_id": 28,
        "event_type": "$identify",
        "insert_id": "777d3cee-fe10-410a-9259-c987fe03bec7",
        "language": "en-US",
        "library": "amplitude-ts/1.6.1",
        "os_name": "Chrome",
        "os_version": "119.0.0.0",
        "platform": "Web",
        "session_id": 1700267883338,
        "time": 1700267883338
      },
      "user_properties": {
        "$set": {
          "wallet_version": "MetaMask/v11.4.1"
        }
      }
    },
    "5": {
      "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
      "sess": {
        "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
        "device_model": "Linux",
        "event_id": 28,
        "event_type": "$identify",
        "insert_id": "777d3cee-fe10-410a-9259-c987fe03bec7",
        "language": "en-US",
        "library": "amplitude-ts/1.6.1",
        "os_name": "Chrome",
        "os_version": "119.0.0.0",
        "platform": "Web",
        "session_id": 1700267883338,
        "time": 1700267883338
      },
      "user_properties": {
        "$set": {
          "wallet_version": "MetaMask/v11.4.1"
        }
      }
    },
    "6": {
      "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
      "sess": {
        "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
        "device_model": "Linux",
        "event_id": 28,
        "event_type": "$identify",
        "insert_id": "777d3cee-fe10-410a-9259-c987fe03bec7",
        "language": "en-US",
        "library": "amplitude-ts/1.6.1",
        "os_name": "Chrome",
        "os_version": "119.0.0.0",
        "platform": "Web",
        "session_id": 1700267883338,
        "time": 1700267883338
      },
      "user_properties": {
        "$set": {
          "wallet_version": "MetaMask/v11.4.1"
        }
      }
    },
    "7": {
      "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
      "sess": {
        "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
        "device_model": "Linux",
        "event_id": 28,
        "event_type": "$identify",
        "insert_id": "777d3cee-fe10-410a-9259-c987fe03bec7",
        "language": "en-US",
        "library": "amplitude-ts/1.6.1",
        "os_name": "Chrome",
        "os_version": "119.0.0.0",
        "platform": "Web",
        "session_id": 1700267883338,
        "time": 1700267883338
      },
      "user_properties": {
        "$set": {
          "wallet_version": "MetaMask/v11.4.1"
        }
      }
    },
    "8": {
      "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
      "sess": {
        "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
        "device_model": "Linux",
        "event_id": 28,
        "event_type": "$identify",
        "insert_id": "777d3cee-fe10-410a-9259-c987fe03bec7",
        "language": "en-US",
        "library": "amplitude-ts/1.6.1",
        "os_name": "Chrome",
        "os_version": "119.0.0.0",
        "platform": "Web",
        "session_id": 1700267883338,
        "time": 1700267883338
      },
      "user_properties": {
        "$set": {
          "wallet_version": "MetaMask/v11.4.1"
        }
      }
    },
    "9": {
      "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
      "sess": {
        "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
        "device_model": "Linux",
        "event_id": 28,
        "event_type": "$identify",
        "insert_id": "777d3cee-fe10-410a-9259-c987fe03bec7",
        "language": "en-US",
        "library": "amplitude-ts/1.6.1",
        "os_name": "Chrome",
        "os_version": "119.0.0.0",
        "platform": "Web",
        "session_id": 1700267883338,
        "time": 1700267883338
      },
      "user_properties": {
        "$set": {
          "wallet_version": "MetaMask/v11.4.1"
        }
      }
    }
  }
}

▼ Request Payload view source
{
  "api_key": "00000000000000000000000000000000",
  "events": [...],
  "op": "api_key: \"00000000000000000000000000000000\"",
  "events": [...],
  "0": {
    "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
    "sess": {
      "device_id": "6495f7ef-4728-498a-afef-2ee204241762",
      "device_model": "Linux",
      "event_id": 40,
      "event_type": "Swap Quote Received",
      "insert_id": "894fc3cf-588c-4168-b9ca-19323c52b07c",
      "language": "en-US",
      "library": "amplitude-ts/1.6.1",
      "os_name": "Chrome",
      "os_version": "119.0.0.0",
      "platform": "Web",
      "session_id": 1700267349438,
      "time": 1700267531054
    },
    "event_properties": {
      "routing": "classic",
      "type": 0,
      "ura_request_id": "25626a8f-0e60-4e27-8c73-fd2b349cf5e"
    },
    "allowed_slippage": 5,
    "allowed_slippage_basis_points": 500,
    "chain_id": 1,
    "estimated_network_fee_usd": 7.319149504259753,
    "method": "ROUTING_API",
    "minimum_output_after_slippage": "26.5795",
    "origin": "https://app.uniswap.org",
    "page": "swap-page",
    "price_impact_basis_points": 4142,
    "quote_latency_milliseconds": 2317,
    "routing": "classic",
    "swap_quote_block_number": "18595188",
    "token_in_address": "NATIVE",
    "token_in_amount": 0.001,
    "token_in_amount_max": "0.001",
    "token_in_detected_tax": 0,
    "token_in_symbol": "ETH",
    "token_out_address": "0xF5581dFeFD0F0e4aeC526bE659CFaB1f8",
    "token_out_amount": 27.908476506275623,
    "token_out_amount_min": "26.579501434548212272",
    "token_out_detected_tax": 0,
    "token_out_symbol": "HOPR",
    "type": 0,
    "ura_quote_block_number": "18595188",
    "ura_request_id": "25626a8f-0e60-4e27-8c73-fd2b349cf5e"
  }
}
```

Data harvesting MVP on Ethereum



Data harvesting in prod by Ethereum's most desired next users

Bloomberg

More Hedge Funds Are Shorting Oil as Negative Sentiment Spreads

Julia Fanzeres

Mon, November 13, 2023 at 10:18 PM GMT+1 · 1 min read

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach

Whistleblower describes how firm linked to former Trump adviser Steve Bannon compiled user data to target American voters

How hedge funds use satellite images to beat Wall Street—and Main Street

MAY 28, 2019 | BY LAURA COUNTS

Berkeley Haas research finds there may be a dark side to the rise of "alternative data" in capital markets



Mempool data harvesting is a ~\$1b market today.

Full-stack web3 data harvesting will be a billion \$ opportunity soon.

Strong privacy tech is our primary insurance policy to prevent exploitation of every single web3 user.

How do we fix the lack of privacy today

Application layer:

- 🤪 Tracking & other web2.0 ugliness
→ defend core values of Ethereum, and yes, point out problems, starting with Uniswap!

Execution layer:

- 🤪 On-chain privacy (ongoing: Tornado, zkBob, Umbra, Nocturne, Railgun, Aztec, etc)
→ use them, integrate them and provide legal assurance for devs that privacy is not evil!
- 🤪 P2P leaks (solvers, builders, indexers)
→ mixnets are great - we're working on that at HOPR and use them for RPC middleware RPCCh.net

Consensus layer:

- 🤪 Validators are not private (and SSLI does not fix that)
→ use P2P privacy on CL as well (but latency issues are hard!)