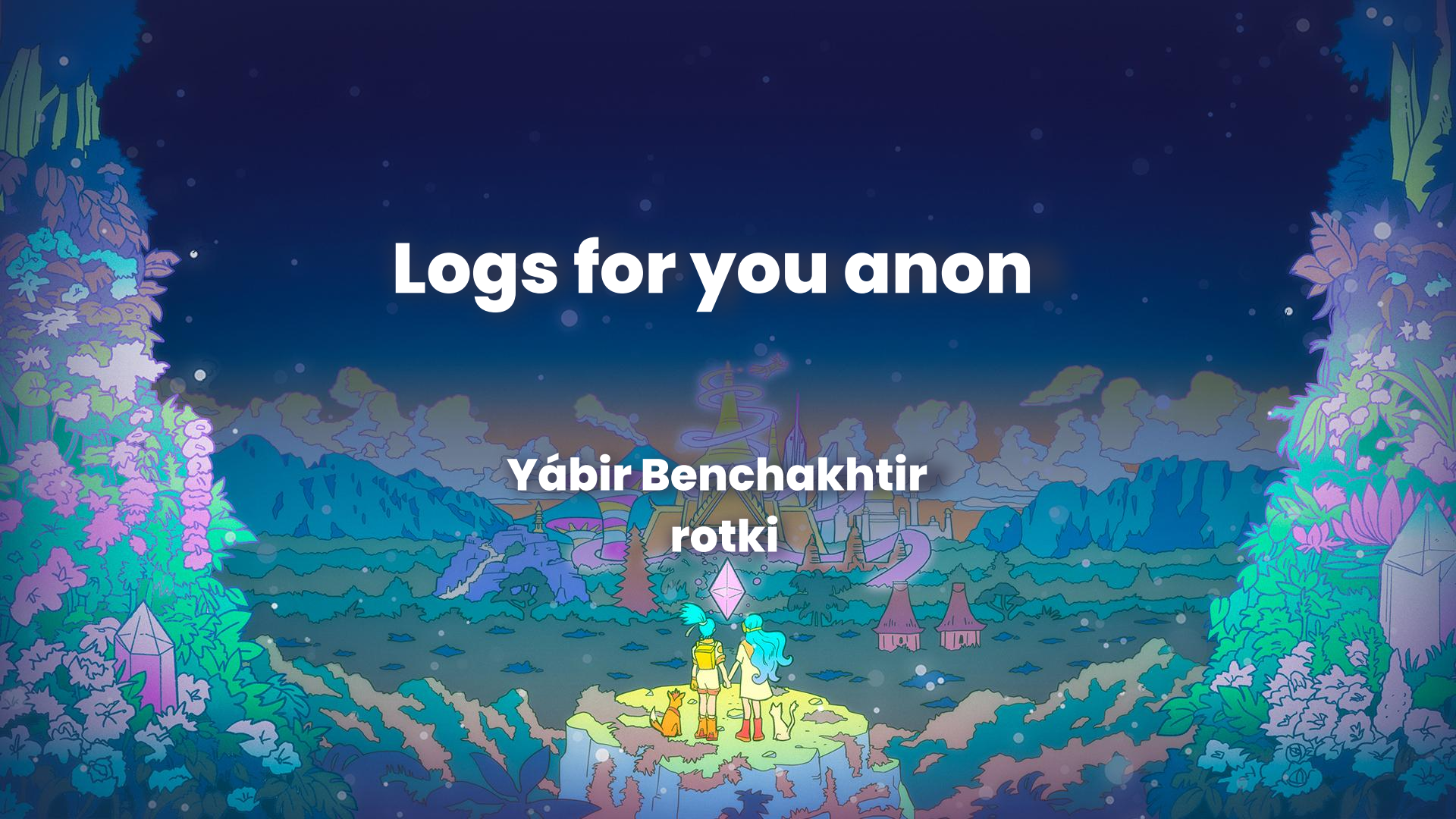
Logs for you anon

Yábir Benchakhtir
rotki



What are logs

- Logs are information emitted by the contract.
- They can be consumed by apps
- There is no limit (afaik) in the amount of logs, only the blocksize

They contain:

1. They have topics (ordered data) up to 4 entries. The first one is always the signature of the event and then the others can be used for indexing and faster searches.
2. A non limited amount of hex data. It requires more effort to parse but is cheaper
3. The address of the contract that emits the event

0xC7...8a13 called depositWithExpiry on MAYAChain_Router

6 Explorers

Details | Token transfers | User operations | Internal txns | Logs | State | Raw trace

Address Tether: USDT Stablecoin 73

Decode input data

Method id	ddf252ad
Call	Transfer(address indexed from, address indexed to, uint256 value)

Name	Type	Indexed?	Data
from	address	true	0xC74D832ac65683FD5D29FE1fFA40D30514198a13
to	address	true	0xe3985E6b61b814F7Cdb188766562ba71b446B46d
value	uint256	false	3000000000

Topics

0 0xddf252ad1be2c89b69c2b068fc378daa952ba7f163c4a11628f55a4df523b3ef

1 Hex 0x000000000000000000000000c74d832ac65683fd5d29fe1ffa40d30514198a13

2 Hex 0x000000000000000000000000e3985e6b61b814f7cdb188766562ba71b446b46d

Data

0x00000000000000000000000000000000000000000000000000000000b2d05e00

https://eth.blockscout.com/tx/0x1ba6a8139b96aabda412128d76bac92f6f825ca38dbc10bb3ba07364371f7d09?tab=logs

Transaction	`0x50c00e9cecc846808c809cc04010403c18b056cc94c062748eb07e2450a06638`			15/06/941 01:43:00
GAS FEE `0xb080...7638`		< 0.01 ETH > 0.25 €	Burned < 0.01 ETH for gas	
SWAP `0xb080...7638`		< 810.20 DAI 745.33 €	Swap < 810.20 DAI in LlamaZip	
SWAP `0xb080...7638`		< 0.26 ETH 750.82 €	Receive < 0.26 ETH as the result of a swap in LlamaZip	
Transaction	`0xb0e040b404a84010e29028204e0862c842c076045ee8963ce0e09620a688dac4`			03/11/926 23:46:10
GAS FEE `0x56d0...6eb0`		< 0.01 ETH > 0.66 €	Burned < 0.01 ETH for gas	
APPROVAL `0x56d0...6eb0`		OP	Revoke OP spending approval of `0x56d0...6eb0` by `0xee70...3034`	
SWAP `0x56d0...6eb0`		< 20.10 OP 66.30 €	Swap < 20.10 OP in LlamaZip	
SWAP `0x56d0...6eb0`		< 0.02 ETH 66.03 €	Receive < 0.02 ETH as the result of a swap in LlamaZip	

Section 1

The problem

Two big problems

- The user pays for creating the log events
- The networks has to store the log events of every transaction

Gas Spent on Events (L30D) Gas Spent on Events (L30D, ETH)

1,271Ξ

Gas Spent on Events (L30D)

@alvin ··· 2mo

Gas Spent on Events (L30D) Gas Spent on Events (L30D, $)

$3,069,640

Gas Spent on Events (L30D)

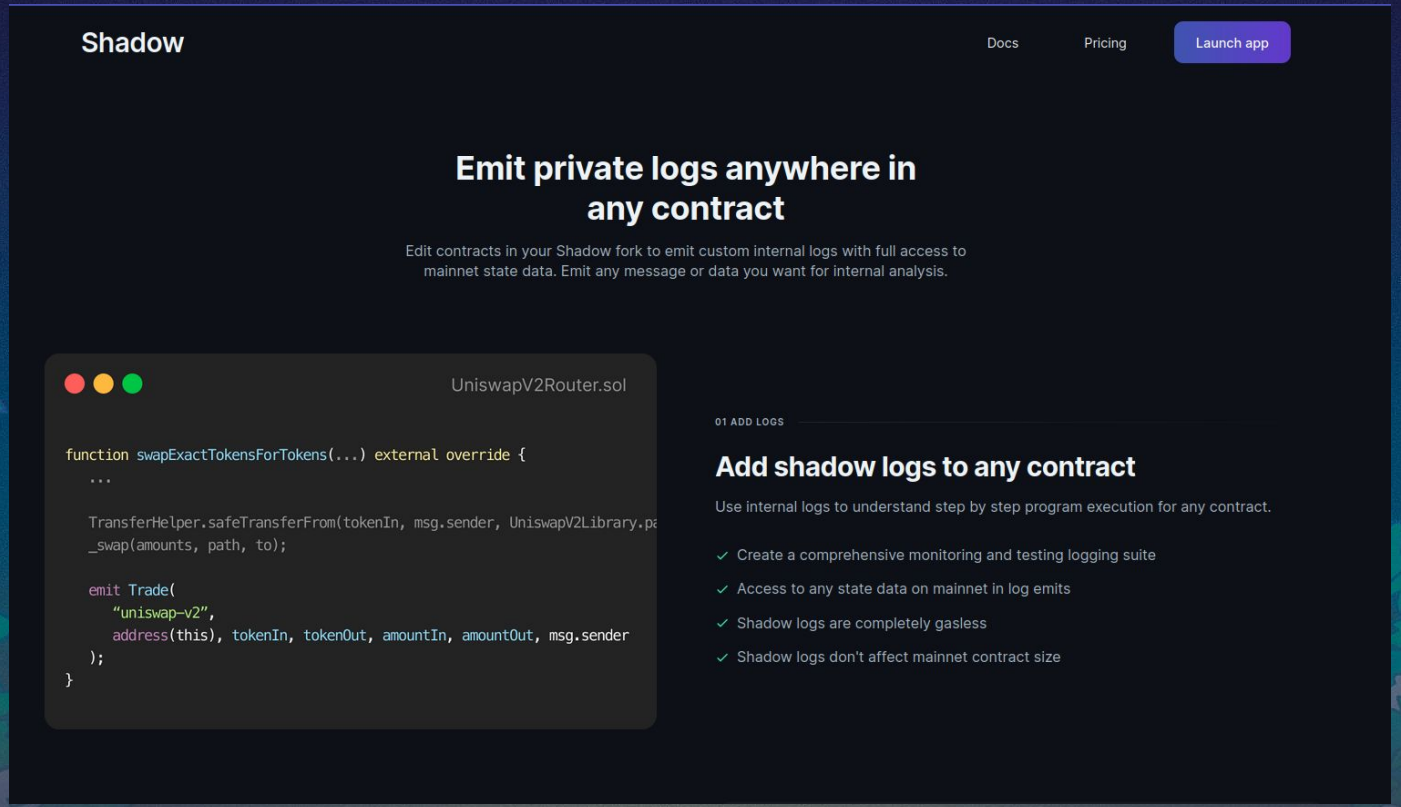
@alvin ··· 2mo

https://dune.com/alvin/gas-costs-of-events

Section 2

So what can we do?

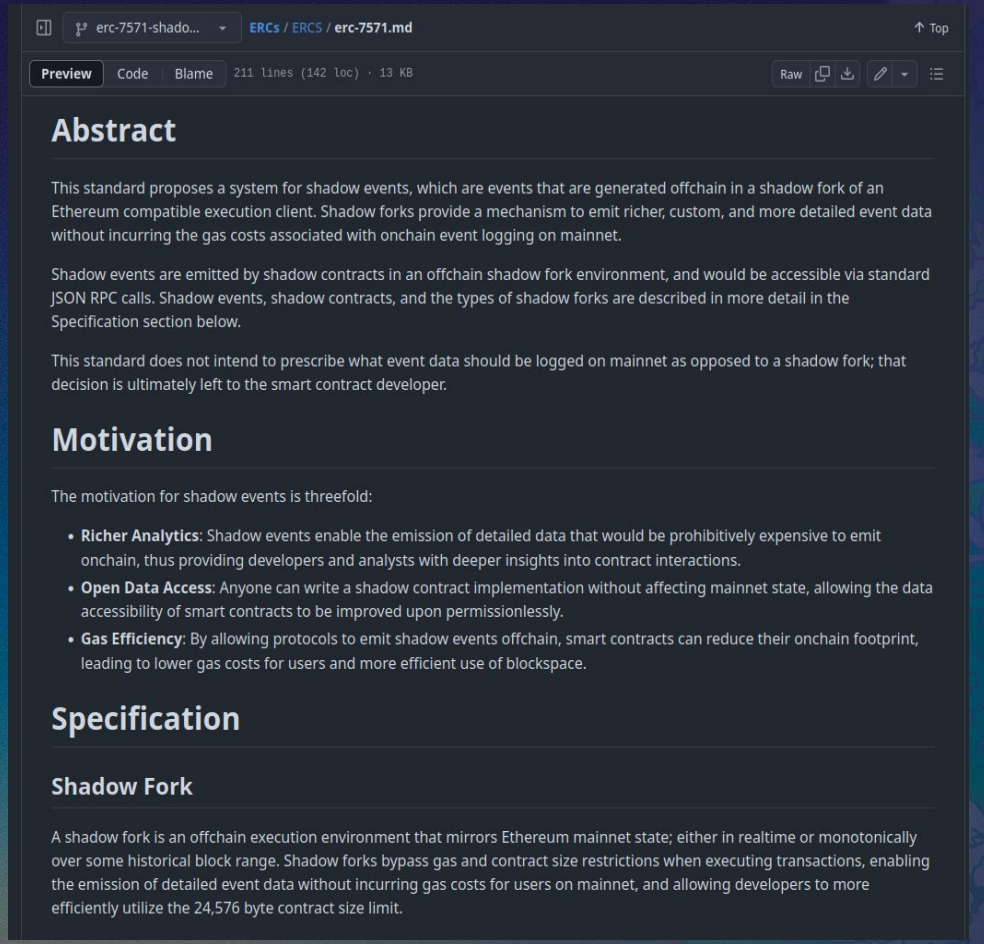
Of course we remove the logs



ERC 7571

- Standard definition so everyone can use it
- Can be adopted by the community
- Hasn't had much conversation recently

https://ethereum-magicians.org/t/erc-7571-shadow-events/17134



erc-7571-shado... ERCs / ERCS / erc-7571.md ↑ Top

Preview Code Blame 211 lines (142 loc) · 13 KB Raw

Abstract

This standard proposes a system for shadow events, which are events that are generated offchain in a shadow fork of an Ethereum compatible execution client. Shadow forks provide a mechanism to emit richer, custom, and more detailed event data without incurring the gas costs associated with onchain event logging on mainnet.

Shadow events are emitted by shadow contracts in an offchain shadow fork environment, and would be accessible via standard JSON RPC calls. Shadow events, shadow contracts, and the types of shadow forks are described in more detail in the Specification section below.

This standard does not intend to prescribe what event data should be logged on mainnet as opposed to a shadow fork; that decision is ultimately left to the smart contract developer.

Motivation

The motivation for shadow events is threefold:

- **Richer Analytics**: Shadow events enable the emission of detailed data that would be prohibitively expensive to emit onchain, thus providing developers and analysts with deeper insights into contract interactions.
- **Open Data Access**: Anyone can write a shadow contract implementation without affecting mainnet state, allowing the data accessibility of smart contracts to be improved upon permissionlessly.
- **Gas Efficiency**: By allowing protocols to emit shadow events offchain, smart contracts can reduce their onchain footprint, leading to lower gas costs for users and more efficient use of blockspace.

Specification

Shadow Fork

A shadow fork is an offchain execution environment that mirrors Ethereum mainnet state; either in realtime or monotonically over some historical block range. Shadow forks bypass gas and contract size restrictions when executing transactions, enabling the emission of detailed event data without incurring gas costs for users on mainnet, and allowing developers to more efficiently utilize the 24,576 byte contract size limit.

Section 3

But is that good?

Some considerations

Users pay for information that they benefit from

Users use tools like rotki, zerion, aave and many other frontends. They all consume logs

Ethereum scalability

- In archive mode is ~600GB for geth
- If at any point it becomes a problem the information can be sharded and distributed

Data ownership

Information is not in the node anymore

In this case, users require access to external sources to retrieve information useful for them.

we are suppose to be cypherpunk!

Section 4

But there are also good things

Improve old contracts

When there is missing information you should ask the developers so they fix it in different iterations of the protocol.

- Liquity liquidations

- Gnosis xDAI bridge

https://www.univ3.xyz/contracts/0x88e6a0c2ddd26feeb64f039a2c41296fcb3f5640

We need a balance

Take home messages:

- We need some logs, everybody uses them for users
- It's okay to have extra information in the shadow logs


Thank you!
Yábir Benchakhtir
rotki
@yabirgb