
The verge is (not) going
to break your contracts!
Hadrien Croubois (Amxx)
OpenZeppelin

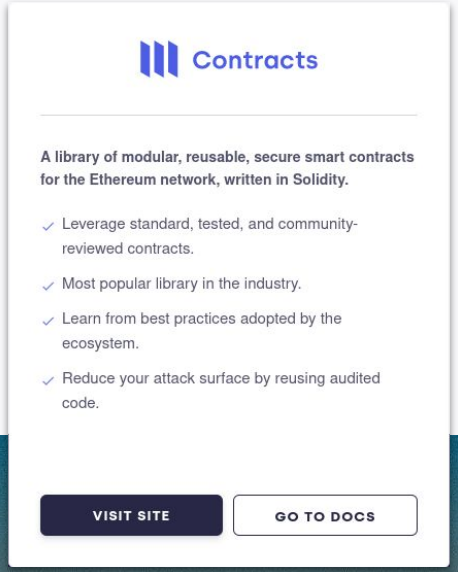
OpenZeppelin's thesis

- There will be a **trillion dollar open economy** built on blockchains and **powered by smart contracts**
- This new, open economy will be **built by teams of creative people developing new applications used by billions of people**
- These teams **will need a set of tools, products and services** to make sure that what they are building is **safe and reliable**
- OpenZeppelin will be a **leading provider of these solutions**, allowing teams to **build faster with lower risk**

Contracts

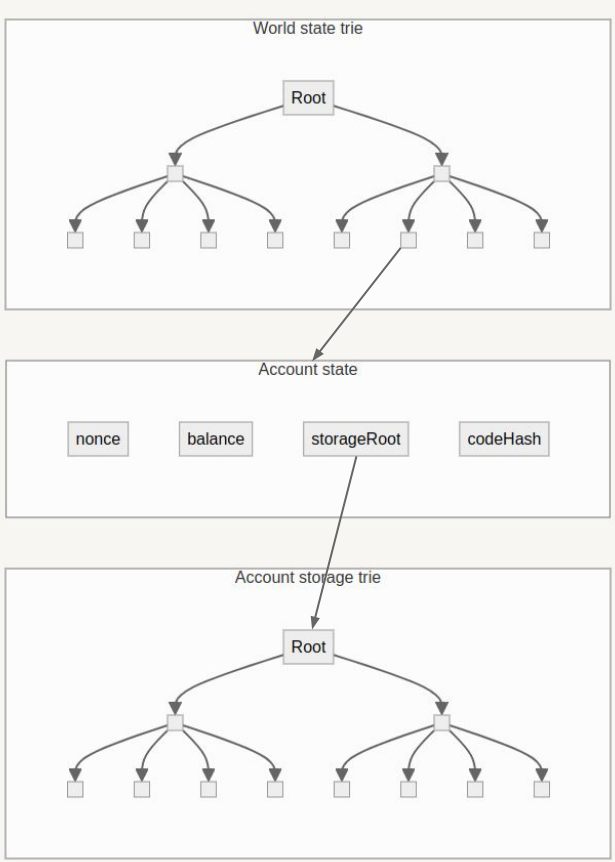
@openzeppelin/contracts@5.1.0

@openzeppelin/contracts-upgradeable@5.1.0



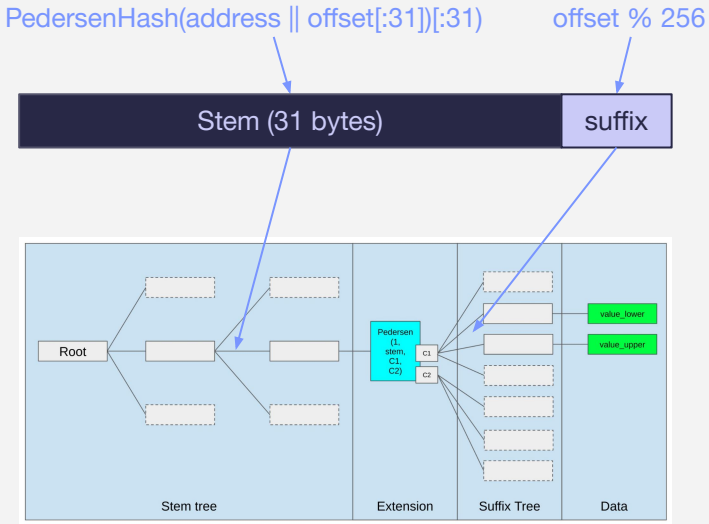
Section 1

How is the verge going to affect devs?



How is smart contract state stored?

- **Each account comes with a storage trie**
- **Used for persistent data**
  ERC-20 balances, ERC-721 ownership, everything
- **Storage is divided in slots**
  Each account has 2^{256} slots available
- **Slots must be “warmed up” before use**
  You only pay the warm-up price once per tx
- **All slots are identical**



That all changes with the verge

- **All storage in the same (verkle) trie**
- **Position in that shared trie is a combination of account and offset (“slot number”)**
- **Slots are gathered in buckets (aka extensions)**
  For a given account, consecutive slots are in the same bucket (up to 256 slots)
- **Buckets are “warmed up”, not slots**
  So reusing slots in a given bucket is efficient

Here's the timeline.

Dencun

March 13th 2024

Pectra

~ April 2025

The Verge

~2026?

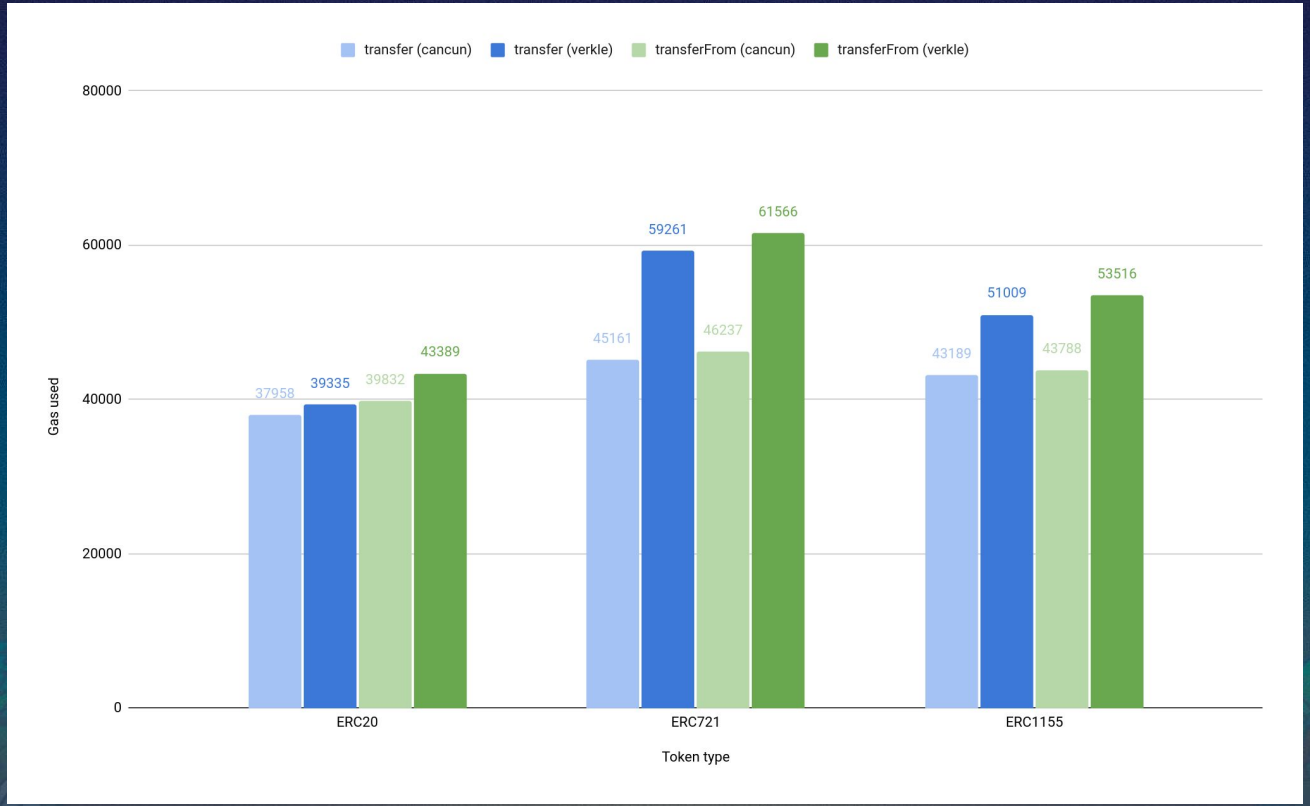
Section 2

How will it impact existing contracts?

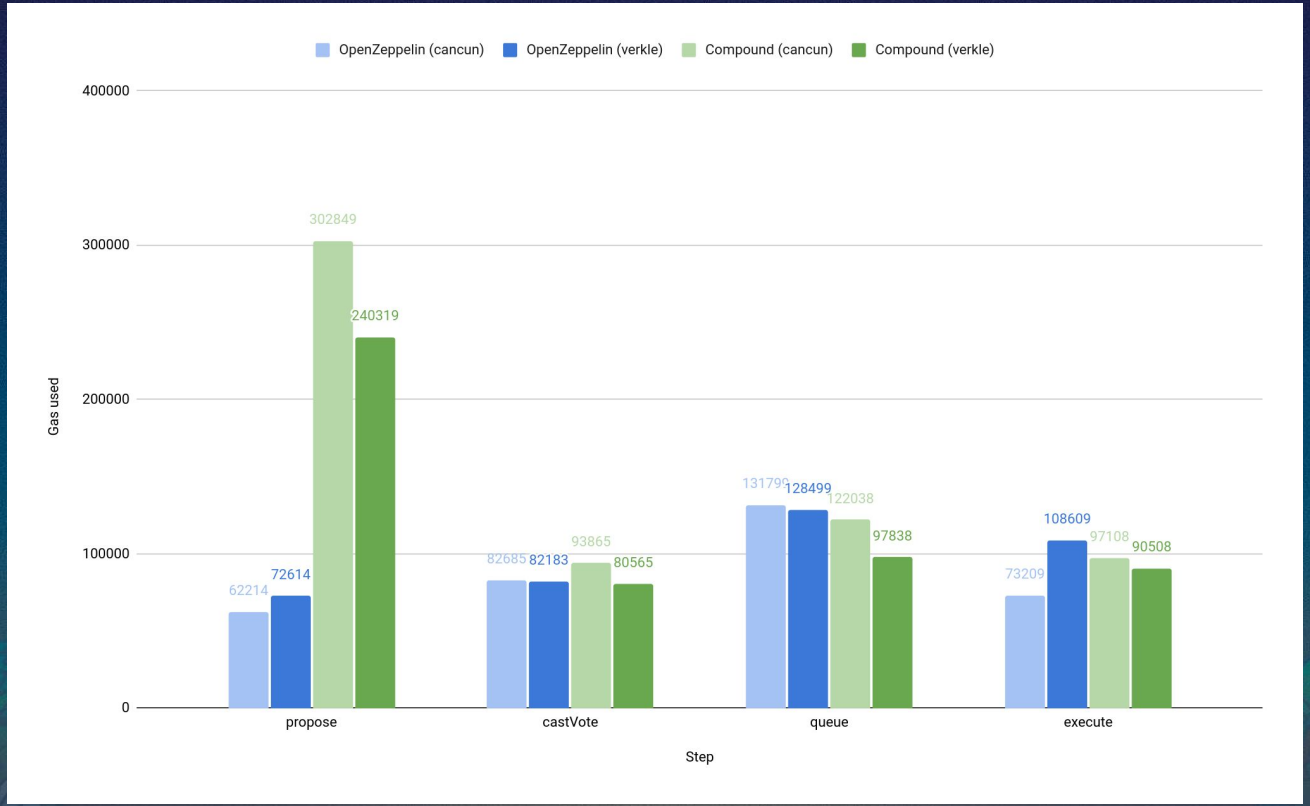
Disclaimer

Gas numbers shown in this presentation are NOT final.
Verkle implementation is still in progress.

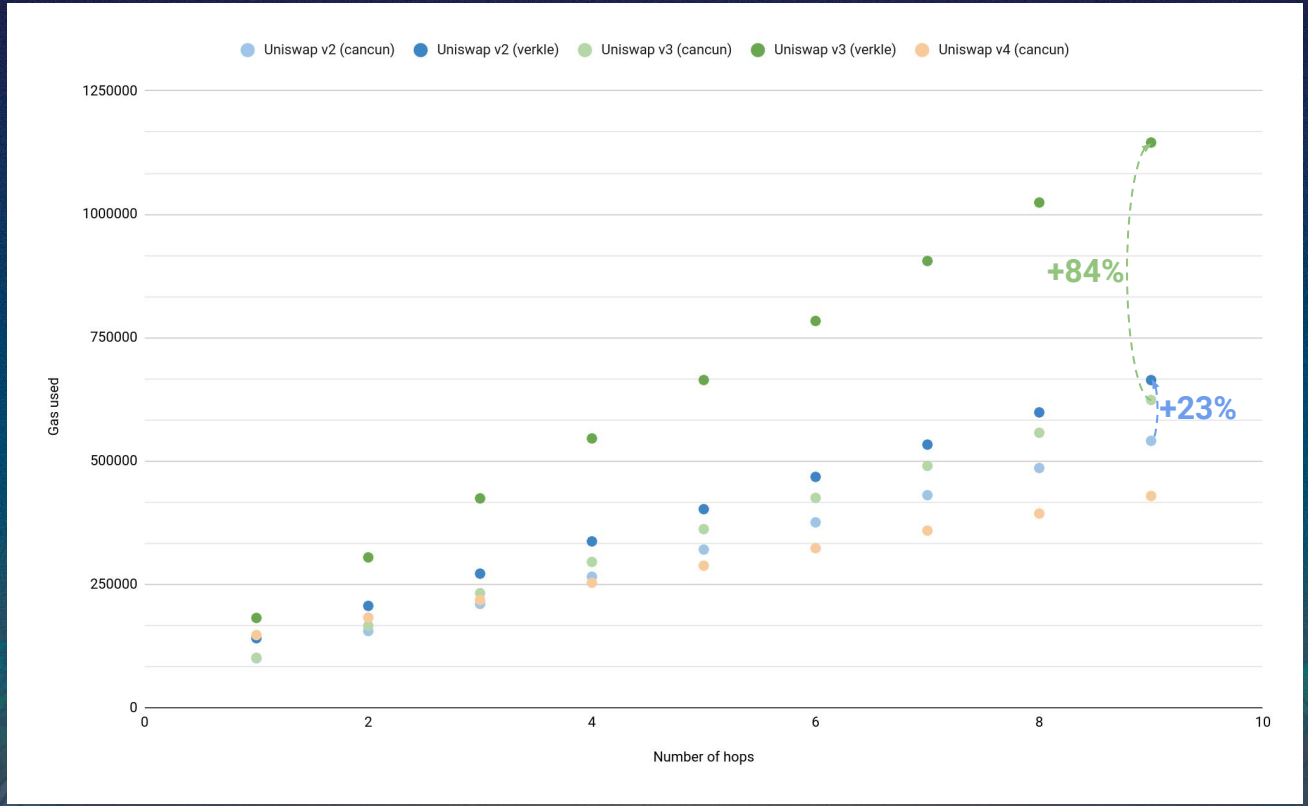
Common tokens



Governance (with Timelock)



Token swaps

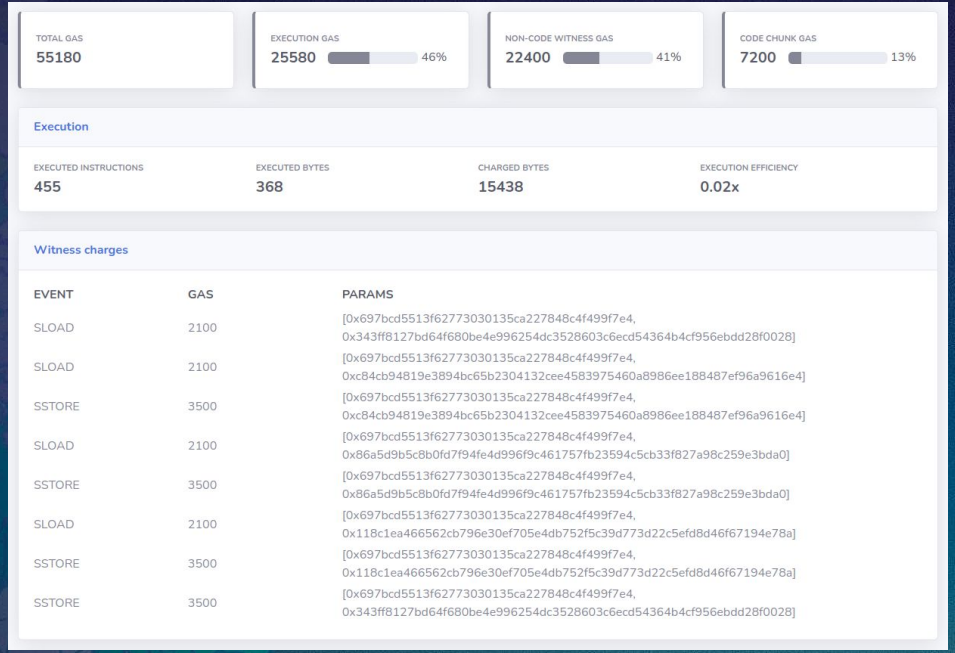


Section 3

Smart contract design for a Verkle-EVM

34 contracts/token/ERC721/ERC721.sol

```
@@ -25,13 +25,19 @@ abstract contract ERC721 is Context, ERC165, IERC721, IERC721Metadata, IERC721Er
25 25      // Token symbol
26 26      string private _symbol;
27 27
28    -    mapping(uint256 tokenId => address) private _owners;
   28 +    struct TokenDetails {
   29 +        address owner;
   30 +        address approval;
   31 +    }
29 32
30    -    mapping(address owner => uint256) private _balances;
   33 +    struct AccountDetails {
   34 +        uint256 balance;
   35 +        mapping(address => bool) operators;
   36 +    }
31 37
32    -    mapping(uint256 tokenId => address) private _tokenApprovals;
   38 +    mapping(uint256 tokenId => TokenDetails) private _tokens;
33 39
34    -    mapping(address owner => mapping(address operator => bool)) private _operatorApprovals;
   40 +    mapping(address owner => AccountDetails) private _accounts;
35 41
36 42      /**
37 43       * @dev Initializes the contract by setting a `name` and a `symbol` to the token collection.
@@ -58,7 +64,7 @@ abstract contract ERC721 is Context, ERC165, IERC721, IERC721Metadata, IERC721Er
58 64          if (owner == address(0)) {
59 65              revert ERC721InvalidOwner(address(0));
60 66          }
61    -        return _balances[owner];
   67 +        return _accounts[owner].balance;
62 68      }
63 69
64 70      /**
@@ -128,7 +134,7 @@ abstract contract ERC721 is Context, ERC165, IERC721, IERC721Metadata, IERC721Er
128 134       * @dev See {IERC721-isApprovedForAll}.
129 135       */
130 136      function isApprovedForAll(address owner, address operator) public view virtual returns (bool) {
131   -        return _operatorApprovals[owner][operator];
   137 +        return _accounts[owner].operators[operator];
132 138      }
```



TOTAL GAS	EXECUTION GAS	NON-CODE WITNESS GAS	CODE CHUNK GAS
55180	25580 46%	22400 41%	7200 13%

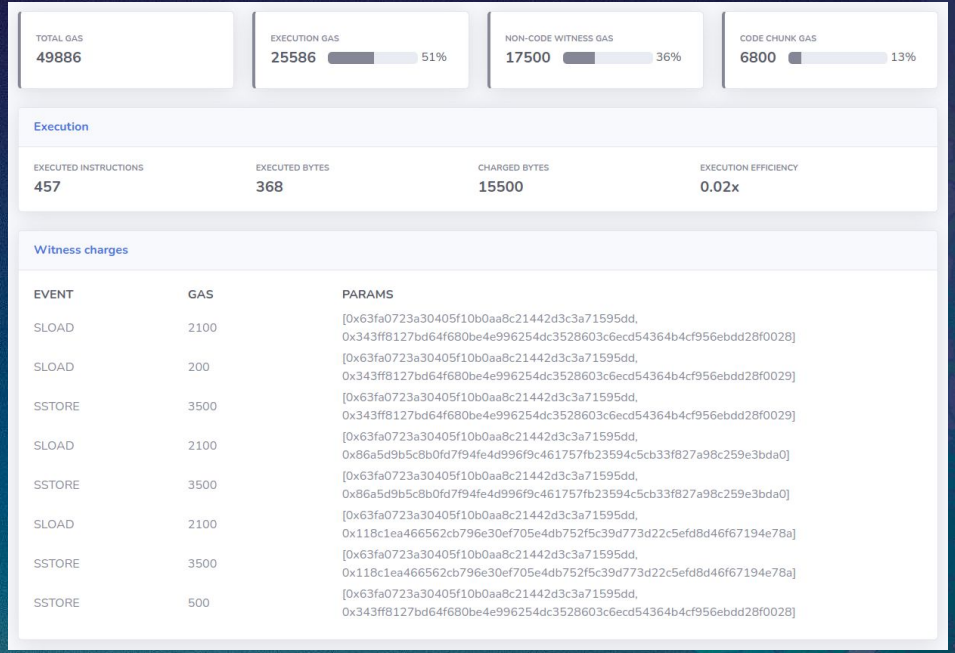
Execution

EXECUTED INSTRUCTIONS	EXECUTED BYTES	CHARGED BYTES	EXECUTION EFFICIENCY
455	368	15438	0.02x

Witness charges

EVENT	GAS	PARAMS
SLOAD	2100	[0x697bcd5513f62773030135ca227848c4f499f7e4, 0x343ff8127bd64f680be4e996254dc3528603c6ecd54364b4cf956ebdd28f0028]
SLOAD	2100	[0x697bcd5513f62773030135ca227848c4f499f7e4, 0xc84cb94819e3894bc65b2304132cee4583975460a8986ee188487ef96a9616e4]
SSTORE	3500	[0x697bcd5513f62773030135ca227848c4f499f7e4, 0xc84cb94819e3894bc65b2304132cee4583975460a8986ee188487ef96a9616e4]
SLOAD	2100	[0x697bcd5513f62773030135ca227848c4f499f7e4, 0x86a5d9b5c8b0fd7f94fe4d996f9c461757fb23594c5cb33f827a98c259e3bda0]
SSTORE	3500	[0x697bcd5513f62773030135ca227848c4f499f7e4, 0x86a5d9b5c8b0fd7f94fe4d996f9c461757fb23594c5cb33f827a98c259e3bda0]
SLOAD	2100	[0x697bcd5513f62773030135ca227848c4f499f7e4, 0x118c1ea466562cb796e30ef705e4db752f5c39d773d22c5efd8d46f67194e78a]
SSTORE	3500	[0x697bcd5513f62773030135ca227848c4f499f7e4, 0x118c1ea466562cb796e30ef705e4db752f5c39d773d22c5efd8d46f67194e78a]
SSTORE	3500	[0x697bcd5513f62773030135ca227848c4f499f7e4, 0x343ff8127bd64f680be4e996254dc3528603c6ecd54364b4cf956ebdd28f0028]

transferFrom on a “Normal ERC-721”



TOTAL GAS	EXECUTION GAS	NON-CODE WITNESS GAS	CODE CHUNK GAS
49886	25586 51%	17500 36%	6800 13%

Execution

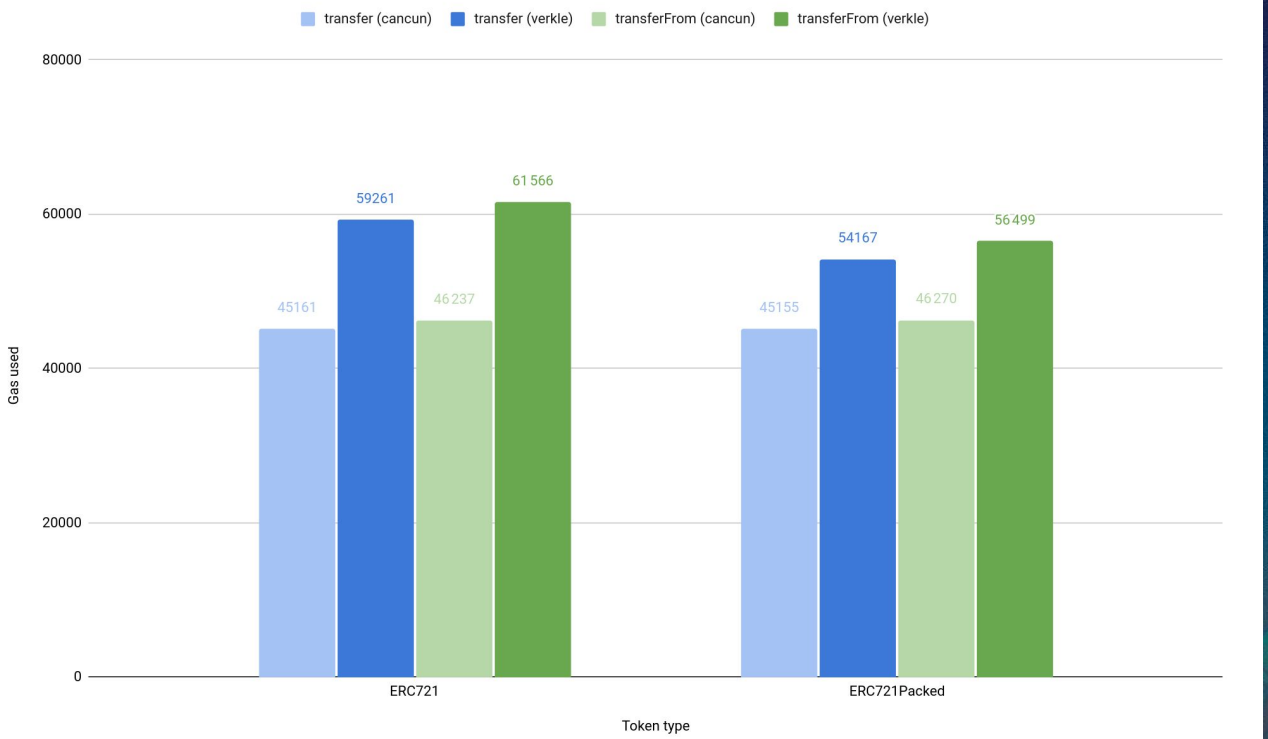
EXECUTED INSTRUCTIONS	EXECUTED BYTES	CHARGED BYTES	EXECUTION EFFICIENCY
457	368	15500	0.02x

Witness charges

EVENT	GAS	PARAMS
SLOAD	2100	[0x63fa0723a30405f10b0aa8c21442d3c3a71595dd, 0x343ff8127bd64f680be4e996254dc3528603c6ecd54364b4cf956ebdd28f0028]
SLOAD	200	[0x63fa0723a30405f10b0aa8c21442d3c3a71595dd, 0x343ff8127bd64f680be4e996254dc3528603c6ecd54364b4cf956ebdd28f0029]
SSTORE	3500	[0x63fa0723a30405f10b0aa8c21442d3c3a71595dd, 0x343ff8127bd64f680be4e996254dc3528603c6ecd54364b4cf956ebdd28f0029]
SLOAD	2100	[0x63fa0723a30405f10b0aa8c21442d3c3a71595dd, 0x86a5d9b5c8b0fd7f94fe4d996f9c461757fb23594c5cb33f827a98c259e3bda0]
SSTORE	3500	[0x63fa0723a30405f10b0aa8c21442d3c3a71595dd, 0x86a5d9b5c8b0fd7f94fe4d996f9c461757fb23594c5cb33f827a98c259e3bda0]
SLOAD	2100	[0x63fa0723a30405f10b0aa8c21442d3c3a71595dd, 0x118c1ea466562cb796e30ef705e4db752f5c39d773d22c5efd8d46f67194e78a]
SSTORE	3500	[0x63fa0723a30405f10b0aa8c21442d3c3a71595dd, 0x118c1ea466562cb796e30ef705e4db752f5c39d773d22c5efd8d46f67194e78a]
SSTORE	500	[0x63fa0723a30405f10b0aa8c21442d3c3a71595dd, 0x343ff8127bd64f680be4e996254dc3528603c6ecd54364b4cf956ebdd28f0028]

transferFrom on a “Packed ERC-721”

ERC-721 Packed



Section 4

Conclusion

The verge:

- is NOT going to break you contracts
- will impact the gas costs of all contracts, including the “old” ones.
- should be taken into consideration when designing/optimizing you next contracts!

You can act now:

- avoid “persistent” storage (transient can help)
- use contiguous storage
  - favor arrays to mapping
  - consolidate mappings using structs
  - store the length of the arrays at the first position (see my EthCC talk)
- (if possible) align your structs with extensions
  - see ERC-7201
- change the language/compiler.

Thank you!

Hadrien Croubois

OpenZeppelin

hadrien@openzeppelin.com

@Amxx

https://shared.hadriencroubois.com/slides/Devcon2024-verge.pdf