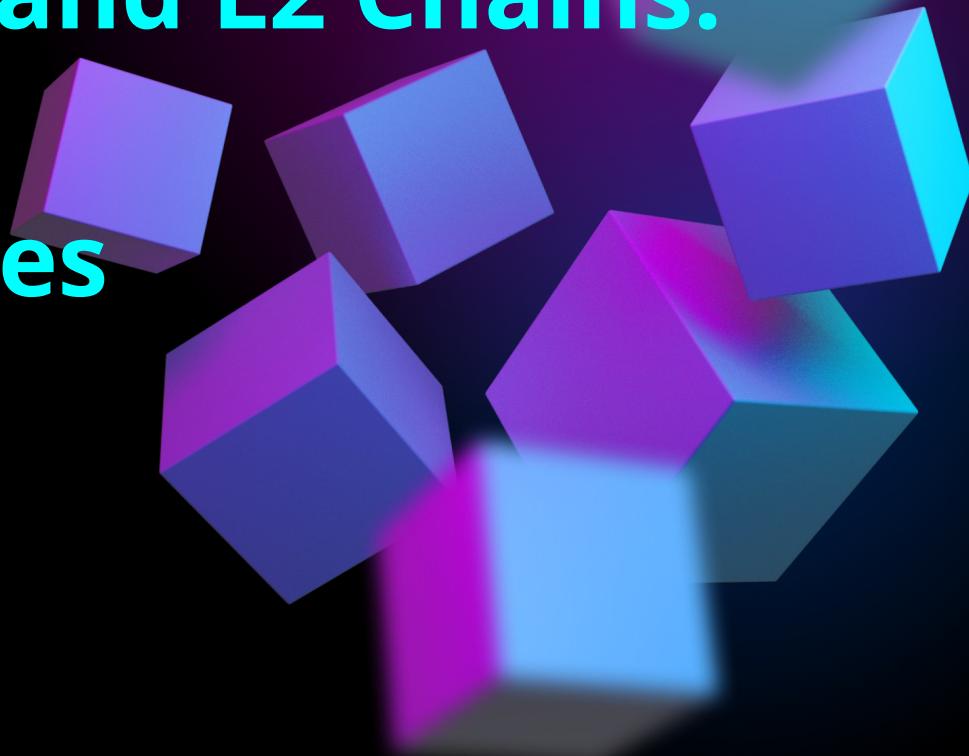


Deploying to L1 and L2 Chains: the Differences and Best Practices

Michal Převrátil & Jan Kalivoda

EthPrague 2023





Hi 

Michal Převrátil

Lead developer of security tooling for
Ethereum @ Ackee Blockchain

- Woke 

- Tools for Solidity



@AckeeBlockchain
ackeeblockchain.com



Hi



Jan Kalivoda ([jaczkal.eth](https://twitter.com/jaczkal))

Ethereum Tech Lead @ Ackee Blockchain

Twitter [@jaczkal](https://twitter.com/jaczkal)



@AckeeBlockchain
ackeeblockchain.com



About us

Blockchain security audits

Development of open source security tools

Onboarding developers to blockchain



@AckeeBlockchain
ackeeblockchain.com

We work with



Our latest work - Solady

- 1 high, 1 medium issue
- 11 findings in total
- 3 auditors
- PR with unit and fuzz tests in Woke

vectorized.eth · @optimizoor · 30. 5. ...

Super big thanks to [@Rockaway_X](#) and [@AckeeBlockchain](#) for completing the first Solady audit!

Extremely grateful for their generosity and keen eyes. 🐱

New version with fixes coming soon.

Vectorized/solady

#445 **Audit by RockawayX <> Ackee**

0 comments 0 reviews 1 file +0 -0

Vectorized · May 30, 2023 · 1 commit

github.com

Audit by RockawayX <> Ackee by Vectorized · Pull Request #445...
Description H1: ERC-1155 _setApprovalForAll emits incorrect owner
Fix ERC1155 internal _setApprovalForAll event If you don't use the...

EVM chains (in)compatibility



ethereum



AVALANCHE



BNB CHAIN



ARBITRUM



Key differences across L1s and L2s

- access lists (EIP-2930)
- tx fee models (EIP-1159 `maxFeePerGas` and `maxPriorityFeePerGas` vs `gasPrice`)
- precompiled contracts (identity, hashing functions, elliptic curve operations)
- `PUSH0` support (EIP-3855)

Key differences across L1s and L2s (continued)

- different decimals of the same token (**USDT** & **USDC** have 18 decimals on BSC)
- block production speed may not be constant and may significantly differ
 - do not rely on `block.number` for timing
- different **token0/token1** order on Uniswap-like AMMs
 - **USDC/WETH** on Polygon but **WETH/USDC** on Optimism

token0

```
function token0() external view returns (address);
```

Returns the address of the pair token with the lower sort order.

token1

```
function token1() external view returns (address);
```

Returns the address of the pair token with the higher sort order.

L2 specific differences

- sequencer may go offline use Chainlink's sequencer uptime feed
- opcodes:
 - COINBASE, DIFFICULTY, NUMBER, TIMESTAMP, ORIGIN, CALLER (most L2s)
 - SELFDESTRUCT replaced by SENDALL (Polygon zkEVM)
- zkSync:
 - custom compiler
 - CREATE, CREATE2 bytecode must be known ahead of time, different address derivation method
 - SELFDESTRUCT, CALLCODE, PC, EXTCODECOPY forbidden
 - memory expansion differences
 - there's more => <https://era.zksync.io/docs/dev/building-on-zksync/contracts/differences-with-ethereum.html>

Deployments using Woke

Woke



- LSP server and static analysis tool
 - public API for custom vulnerability detectors and printers soon
- development and testing framework
 - **pytypes** - code completions and type checking
 - integrated property based fuzzer
 - supports multiple L1 and L2 chains
 - automatically uses access lists, gas estimates
- VS Code integration through **Tools for Solidity** extension



Tools for Solidity

Ackee Blockchain  ackeeblockchain.com |  2,072 installs |  (9) | Free

Advanced Solidity support and vulnerability detectors developed by Ackee Blockchain



```
pip3 install woke

# import existing account (private key) or create new one
woke accounts import deployment
woke accounts new deployment

git clone https://github.com/Ackee-Blockchain/ethprague-2023-workshop-deployments.git
cd ethprague-2023-workshop-deployments

npm ci
woke init pytypes
woke run scripts/deploy.py
```



scripts/deploy.py

```
from woke.deployment import *
from pytypes.contracts.Dummy import Dummy

@default_chain.connect("https://rpc2.sepolia.org")
def main():
    a = Account.from_alias("deployment")
    default_chain.set_default_accounts(a)

    dummy = Dummy.deploy()
    print(dummy)
```

ackeeblockchain.com

<https://t.ly/5pSs>



ackee | blockchain
security

<https://github.com/Ackee-Blockchain/ethprague-2023-workshop-deployments>

Email hello@ackeeblockchain.com

Twitter [@AckeeBlockchain](https://twitter.com/AckeeBlockchain)

Telegram [@josef_ackee](https://t.me/josef_ackee)