

SWC-116: Block values as a proxy for time

Lorenz Kofler and Jonas Fischer

13 October 2023

1 Infos

There is neither a lower nor an upper bound on the number of pages. Assume that the reader is familiar with Ethereum and Smart Contracts, and just write what is necessary. It is a technical report, not an essay, so stick to the facts. As a sign of professionalism, proofread the paper and eliminate spelling and grammatical errors. You may use chatGPT or a similar tool to polish the paper, but take care that it does not introduce nonsense.

Write the paper in English. Typeset it in L^AT_EX. The document class `article` is fine, but you may use fancier formatting if you prefer. See the source of this document for an example.

For Solidity code, add the line `\usepackage{solidity}` to your preamble and wrap the code in a `solidity` environment, like below.

```
1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.20;
3 contract HelloWorld {
4     string public greet = "Hello World!";
5 }
```

The citation information for the papers in the TUWEL course is provided in the file `seminar.bib`. Add any further papers that you want to cite. Cite only the papers that you really need. Currently, `seminar.bib` contains the following references.

References

- [1] Lexi Brent, Anton Jurisevic, Michael Kong, Eric Liu, Francois Gauthier, Vincent Gramoli, Ralph Holz, and Bernhard Scholz. Vandal: A scalable security analysis framework for smart contracts. *arXiv*, 2018.