SWC-116: Block values as a proxy for time

Lorenz Kofler and Jonas Fischer

13 October 2023

1 Introduction

This report deals with a weakness in Solidity smart contracts, which is called "block values as a proxy for time". This weakness is described in the Smart Contract Weakness Classification (SWC) registry under the number 116.
The weakness comes from the attempt of developers to introduce time depended functionality in their smart contracts, by reading the values block.timestamp or block.number [1].
But because Ethereum is decentralized, this information is controlled by miners. There is no restriction how the miners have to set the timestamp. It only needs to be higher then the timestamp of the previous block [2].

$$H_s > P(H)_{H_s} \tag{1}$$

The timestamp of the block H_s in 1 must be greater then the timestamp of the previous block $P(H)_{H_s}$ [3].

2 Examples

2.1 Example1 - Game

```
1     function play() public {
2         require(now > 1521763200 && neverPlayed == true);
3         neverPlayed = false;
4         msg.sender.transfer(1500 ether);
5     }
```

Source: NCC Group - Time manipulation [4]

3 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 LaTeX. 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.

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

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] Smart Contract Weakness Classification, *Block values as a proxy for time*. [Online]. Available: https://swcregistry.io/docs/SWC-116/

[2] N. Veloso, "Conkas: A modular and static analysis tool for ethereum bytecode," 2021. [Online]. Available: https://www.semanticscholar.org/paper/Conkas:-A-Modular-and-Static-Analysis-Tool-for-Veloso/425e474177885f9ac9e57d44e8e2386d13f9c87d

[3] Wood, Garvin and other, "Ethereum: A secure decentralised generalised transaction ledger berlin version 2bcdb2d – 2023-08-25," *Ethereum project yellow paper*, vol. 151, no. 2014. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[4] NCC Group, *Time manipulation*. [Online]. Available: https://dasp.co/#item-8