MICHAL ZALECKI.com

TOOPLOOX

FREE SAMPLE

Ethereum: 30 Tips & Tricks

FOR SOLIDITY DEVELOPERS

by Michał Załęcki

MICHAŁ ZAŁĘCKI

×

Table of Contents

#CONTENTS#CON

Tips

#3 #SOLIDITY#3#S

Tip #3
What's the difference between SHA-3 and Keccak256?

In Solidity, the sha3 function is an alias for keccak256 function and uses Keccak, the winning algorithm in the NIST competition for SHA-3 hash function. In many libraries or different programming languages, sha3 usually implements the SHA-3 FIPS 202 standard which is different from Keccak. Before standardization, NIST changed the padding parameter which results in a different output.

In the next Solidity version, aliases sha3 and suicide are going to be forbidden.

```
keccak256("The quick brown fox jumps over the lazy dog");
// 0x4d741b6f1eb29cb2a9b9911c82f56fa8d73b04959d3d9d222895df6c0b28aa15
```

```
const { sha3_256, keccak_256 } = require("js-sha3");
sha3_256("The quick brown fox jumps over the lazy dog");
// 69070dda01975c8c120c3aada1b282394e7f032fa9cf32f4cb2259a0897dfc04
keccak_256("The quick brown fox jumps over the lazy dog");
// 4d741b6f1eb29cb2a9b9911c82f56fa8d73b04959d3d9d222895df6c0b28aa15
```

#17#FUNCTION_S

Tip #17
How to compute the function selector and test the exception?

To test the exception in Solidity, for example, while writing unit tests in Solidity, you have to use the address.call. You can assert for raised exceptions as address.call returns false when the call failed and true otherwise. To use the address.call function, you have to pass a function selector which are the first 4 bytes of Keccak hash of the function signature.

```
bytes4 signature = bytes4(keccak256(“transferOwnership(address)”));
bool result = address(ownable).call(signature, address(this));
Assert.equal(result, false, “non-owner can call transfer ownership”);
```

The other way to obtain a function selector is to access the selector member of the function. It’s easier and makes refactoring simpler as you change argument type once but doesn’t work for overloaded functions.

```
bytes4 signature = ownable.transferOwnership.selector;
```

#26 #SOLIDITY #26

Tip #26
How to highlight Solidity syntax on GitHub?

At the time of writing, GitHub doesn't support syntax highlighting in *.sol files by default. If you want to improve readability of your pull requests, add the .gitattributes file to your repository with the following content.

```
*.sol linguist-language=Solidity
```

CONTINUE READING...

#FULL_VERSION#

Get the full version

www.michalzalecki.com

MICHAŁ ZAŁĘCKI X TOOPLOOX

#REVIEWS#OPINI

Full version reviews

"I was amazed how Michal was able to put a lot of knowledge in form of short, easy to digest tips. I think it's essential read for any blockchain developer."

– **Krzysztof Kaczor**, Engineering At MakerDAO

"This book is an essence of the most useful hints in Solidity for Ethereum Blockchain. On almost 50 pages you will find everything from an address definition, through transactions details, to Smart Contracts functions."

– **Kamil Lelonek**, Elixir Software Engineer

"So many great tips that it's difficult to not read all of them at once. Clear, concise and informative. Definitely worth reading!"

– **Sebastian Muszyński**, Front-End Web Developer