eth-hash Documentation

Release 0.7.0

The Ethereum Foundation

Mar 01, 2024

CONTENTS

The Ethereum hashing function, keccak256, sometimes (erroneously) called sha3

CHAPTER

ONE

CONTENTS

1.1 Quickstart

1.1.1 Choose a hashing backend

If you're not sure, choose "pycryptodome" because it supports pypy3.

You can find a full list of each currently supported backend in *eth_hash.backends*.

1.1.2 Install

Put the backend you would like to use in brackets during install, like:

```
python -m pip install "eth-hash[pycryptodome]"
```

1.1.3 Compute a Keccak256 Hash

```
>>> from eth_hash.auto import keccak
>>> keccak(b'')
b"\xc5\xd2F\x01\x86\xf7#<\x92~}\xb2\xdc\xc7\x03\xc0\xe5\x00\xb6S\xca\x82';{\xfa\xd8\x04]\
↪x85\xa4p"
```

You may also compute hashes incrementally

```
>>> from eth_hash.auto import keccak
>>> preimage = keccak.new(b'part-a')
>>> preimage.update(b'part-b')
>>> preimage.digest()
b'6\x91l\xdd50\xd6[\x7f\xf9B\xff\xc9SW\x98\xc3\xaal\xd9\xde\xdd6I\xb7\x91\x9e\xf4`pl\x08'
```

The preimage object returned may be copied as well.

```
>>> from eth_hash.auto import keccak
>>> preimage = keccak.new(b'part-a')
>>> preimage_copy = preimage.copy()
>>> preimage.update(b'part-b')
>>> preimage.digest()
b'6\x91l\xdd50\xd6[\x7f\xf9B\xff\xc9SW\x98\xc3\xaal\xd9\xde\xdd6I\xb7\x91\x9e\xf4`pl\x08'
>>> preimage_copy.update(b'part-c')
```

(continues on next page)

(continued from previous page)

```
>>> preimage_copy.digest()
b'\xffcy45\xea\xdd\xdf\x8e(\x1c\xfcF\xf3\xd4\xa1S\x0f\xdf\xd8\x01!\xb2(\xe1\xc7\xc6\xa3\
↪x08\xc3\n\x0b'
```

1.1.4 Select one of many installed backends

If you have several backends installed, you may want to explicitly specify which one to load. You can specify in an environment variable, or at runtime.

Specify backend by environment variable

```
$ ETH_HASH_BACKEND="pysha3" python
>>> from eth_hash.auto import keccak
# This runs with the pysha3 backend
>>> keccak(b'')
b"\xc5\xd2F\x01\x86\xf7#<\x92~}\xb2\xdc\xc7\x03\xc0\xe5\x00\xb6S\xca\x82';{\xfa\xd8\x04]\
↪x85\xa4p"
```

Specify backend at runtime

```
>>> from eth_hash.backends import pysha3
>>> from eth_hash import Keccak256
>>> keccak = Keccak256(pysha3)
>>> keccak(b'')
b"\xc5\xd2F\x01\x86\xf7#<\x92~}\xb2\xdc\xc7\x03\xc0\xe5\x00\xb6S\xca\x82';{\xfa\xd8\x04]\
↪x85\xa4p"
```

1.2 eth_hash.backends package

1.2.1 Submodules

1.2.2 eth_hash.backends.auto module

class eth_hash.backends.auto.**AutoBackend**

Bases: BackendAPI

keccak256(*in_data: bytearray | bytes*) → bytes

preimage(*in_data: bytearray | bytes*) → PreImageAPI

1.2.3 eth_hash.backends.pycryptodome module

class eth_hash.backends.pycryptodome.**CryptodomeBackend**

Bases: BackendAPI

keccak256(*prehash: bytearray | bytes*) → bytes

preimage(*prehash: bytearray | bytes*) → PreImageAPI

class eth_hash.backends.pycryptodome.**CryptodomePreimage**(*prehash: bytes*)

Bases: PreImageAPI

copy() → *CryptodomePreimage*

digest() → bytes

update(*prehash: bytes*) → None

eth_hash.backends.pycryptodome.**keccak256**(*prehash: bytearray | bytes*) → bytes

eth_hash.backends.pycryptodome.**preimage**(*prehash: bytearray | bytes*) → PreImageAPI

1.2.4 eth_hash.backends.pysha3 module

class eth_hash.backends.pysha3.**PySha3Backend**

Bases: BackendAPI

keccak256(*prehash: bytearray | bytes*) → bytes

preimage(*prehash: bytearray | bytes*) → PreImageAPI

class eth_hash.backends.pysha3.**Pysha3Preimage**(*prehash: bytes*)

Bases: PreImageAPI

copy() → *Pysha3Preimage*

digest() → bytes

update(*prehash: bytes*) → None

eth_hash.backends.pysha3.**keccak256**(*prehash: bytearray | bytes*) → bytes

eth_hash.backends.pysha3.**preimage**(*prehash: bytearray | bytes*) → PreImageAPI

1.2.5 Module contents

A collection of optional backends that implement hashing.

You must manually select and install the backend you want. If the backend is not installed, then trying to import the module for that backend will cause an `ImportError`.

See *Choose a hashing backend* for more.

1.3 eth_hash package

1.3.1 eth_hash.auto module

1.3.2 eth_hash.main module

class eth_hash.main.**Keccak256**(*backend: BackendAPI*)

Bases: object

new(*preimage: bytearray | bytes*) → PreImageAPI

1.4 Release Notes

1.4.1 eth-hash v0.7.0 (2024-03-01)

Internal Changes - for eth-hash Contributors

- Merge template updates, notably adding py312 support and testing docs build for all formats (#57)

1.4.2 eth-hash v0.6.0 (2024-01-10)

Breaking Changes

- Drop python 3.7 support (#53)

Internal Changes - for eth-hash Contributors

- Merge project template updates, notably use `pre-commit` for linting and change the name of `master` branch to `main` (#53)
- Correct booleans in `pyproject.toml` and add test for presence of `eth_hash.__version__` attribute (#55)

1.4.3 eth-hash v0.5.2 (2023-06-07)

Internal Changes - for eth-hash Contributors

- remove unused docs deps, bump version of remaining (#48)
- merge updates from the python project template (#51)

1.4.4 eth-hash v0.5.1 (2022-11-09)

Features

- Add support for Python 3.11 (#45)

1.4.5 eth-hash v0.5.0 (2022-07-20)

Performance improvements

- Prefer pysha3 backend by default (#42)

1.4.6 eth-hash v0.4.0 (2022-07-06)

Features

- Add support for Python 3.8, 3.9, 3.10 (#40)

Deprecations and Removals

- Drop support for Python 3.5 and 3.6 (#39)

Miscellaneous changes

- #40, #41

1.4.7 eth-hash v0.3.3 (2022-06-30)

Performance improvements

- Keccak backend was initialized every time it was called. Now it's initialized only the first time it's called. (#36)

Internal Changes - for eth-hash Contributors

- Prune `venv` files from the release via MANIFEST.in (#38)

1.4.8 eth-hash v0.3.2 (2021-09-03)

Miscellaneous changes

- Drop eth-utils requirement, to fix dependency cycle (#33)

1.4.9 eth-hash v0.3.1 (2021-01-21)

Bugfixes

- Bugfix to export type annotations (#28)

1.4.10 eth-hash v0.3.0 (2021-01-20)

Features

- Export type annotations, for use in importing projects (#29)

Internal Changes - for eth-hash Contributors

- Import 3 years worth of template updates (#29)

1.4.11 v0.2.0

Released September 5, 2018

- set *pycryptodome* version to *>=3.6.6,<4* to fix a recently discovered vulnerability

1.4.12 v0.1.4

Released May 28, 2018

- Ensure the auto backend is pickleable (#19)

1.4.13 v0.1.3

Released May 14, 2018

- The pycryptodome backend now allows `update()`, then `digest()`, then `update()`.

1.4.14 v0.1.2

Released Apr 2, 2018

- You can now import eth-hash without a backend, it won't fail until trying to generate a hash

1.4.15 v0.1.1

Released Mar 15, 2018

- upgrade pycryptodome to v3.5.1+
- performance improvements with preimage
- Better docs and tests

1.4.16 v0.1.0

Released Feb 28, 2018

- Add support for `bytearray` input to keccak
- Add support for incrementally building hash results

1.4.17 v0.1.0-alpha.3

Released Feb 7, 2018

- Add pycryptodome backend support
- Add pysha3 backend support
- Can specify backend in environment variable `ETH_HASH_BACKEND`
- New *Quickstart* docs

1.4.18 v0.1.0-alpha.2

Released Feb 6, 2018

- Bugfix pypy3 reference in pypi

1.4.19 v0.1.0-alpha.1

- Launched repository, claimed names for pip, RTD, github, etc

CHAPTER

TWO

INDICES AND TABLES

- genindex
- modindex

PYTHON MODULE INDEX

e

INDEX