**Сравнительный анализ функций хеширования**

|  |  |  |  |
| --- | --- | --- | --- |
| **Характеристика** | **MD5** | **SHA-2** | **Blake2** |
| **Год создания** | 1991 | 2001 | 2012 |
| **Длина хеша** | 128 бит | SHA-224 (224 бит), SHA-256 (256 бит), SHA-384 (384 бит), SHA-512 (512 бит) | Различные варианты (от 1 до 512 бит) |
| **Размер блока** | 512 бит | 512 бит | Варьируется в зависимости от варианта (от 1 до 1024 бит) |
| **Размер внутреннего состояния** | 128 бит | SHA-224 (224 бит), SHA-256 (256 бит), SHA-384 (384 бит), SHA-512 (512 бит) | 1024 бит |
| **Скорость хеширования** | Высокая | В зависимости от варианта - высокая | Высокая |
| **Структура алгоритма** | Меркла — Дамгора | Меркла — Дамгора | Не определена |
| **Достоинства** | Быстрый, широко используется | Высокая стойкость, широко используется, нет серьезных известных уязвимостей | Высокая скорость, гибкость, отсутствие коллизий в обычных условиях |
| **Недостатки** | Уязвим к коллизиям | Немного медленней предшественника | Нет широкой стандартизации |
| **Примечания** | Не рекомендуется для криптографических целей из-за уязвимостей | Широко используется, рекомендуется для криптографических целей | Широко применяется в различных областях, в том числе в блокчейне |