УДК 004.31 DOI: 10.18698/2541-8009-2020-03-585

# ОБЗОР АЛГОРИТМОВ ХЕШИРОВАНИЯ НА ПЕРСОНАЛЬНОМ КОМПЬЮТЕРЕ

**Р.А. Бушуев** presentman@bk.ru
SPIN-код: 4704-2637

**А.В. Марченко** mart0n@mail.ru
SPIN-код: 2567-4813

**МГТУ им. Н.Э. Баумана, Москва, Российская Федерация**

**Аннотация**

*Рассмотрены основные алгоритмы хеширования для майнинга, описаны их характеристики и предложен лучший вариант алгоритма хеширования на персональном компьютере (с определенными техническими параметрами). Представлены описания функций хеширования, приведены результаты и примерные показания их работы. Проделанная работа позволит ознакомиться с наиболее часто встречающимися алгоритмами майнинга, типами майнинга, а также углубиться в тему криптовалют, ознакомившись с их разновидностями. Приведенные практические результаты не только позволят проанализировать рынок криптовалют и майнинга в целом, но и дадут понимание того, как вычисления влияют на технические параметры устройства.*

**Ключевые слова**

*Майнинг, криптовалюта, пул, хеширование, алгоритм, биржа, хешрейт, блокчейн*

Поступила в редакцию 13.02.2020


Существует множество разновидностей криптовалют (виртуальных монет) [1], а также алгоритмов хеширования, которые позволяют их «добывать». Каждая пятая новая монета имеет огромный спрос и волатильность цены, зависящую от капитализации. К капитализации относится как денежное вложение, так и вложение в вычислительные устройства, которые используют свою мощность для реализации алгоритмов хеширования.

*Основная цель статьи* — оценить весь процесс майнинга и ознакомиться с основными терминами в этой сфере.

Эффективность алгоритмов будем рассматривать как прибыльность в виртуальных монетах (криптовалюта). Для приобретения данных монет или обмена ими существуют разные средства:

– криптобиржи (биржи, где можно обменивать, продавать, покупать криптовалюту);

– криптокошельки (в отличие от криптобирж, тут торговать и обмениваться нельзя);

– обменники (покупка/продажа осуществляется через специальный интернет-сервис);

– мобильные приложения (все делается через специальный интернет-сервис);

– майнинг (способ получения новых блоков (монет) криптовалюты посредством осуществления компьютером определенных криптографических, математических и других видов вычислений);

– блокчейн-игры, в которых можно выигрывать разные криптовалюты.

Рынок криптовалют стремительно растет, ведь хеширование дает большие перспективы в возможности шифровать информацию в различных сферах. На примере имеющегося оборудования рассмотрим основные алгоритмы майнинга, которые отличаются своим эффективным вычислением блокчейн-блоков [2] с помощью вычислительной мощности процессора видеокарт. Таким образом, вырабатываемая мощность компьютера или вычислительного устройства, которая служит для шифрования, вознаграждается; естественно, чем больше вознаграждение, тем эффективнее алгоритм, в качестве награды выплачивается определенная криптовалюта, такой процесс называется майнингом. С технической точки зрения выделяют несколько типов майнинга [3], различающихся использованием:

1) центрального процессора (CPU) — здесь для вычислений задействована мощность компьютерного процессора;

2) графических видеокарт (GPU), когда для вычислений используется мощность видеокарты;

3) интегральных схем специального назначения (ASIC) — это отдельное самостоятельное устройство, вся мощность которого используется только для вычислений.

Помимо этого майнинг подразделяют на три вида:

1) соло-майнинг [4] — когда майниг-оборудование работает над блоками самостоятельно, ни с кем не разделяя «добытую» монету;

2) майнинг через пулы — несколько единиц оборудования в сети работают над складыванием блоков, сложив их, делят «добытую» сумму. Криптографические блоки складываются путем хеширования. Хеш — это специальный алгоритм кодирования различных данных (картинки, аудиофайлы, коды, тексты). Хеширование работает следующим образом: из исходных данных генерируется буквенная и цифровая последовательность определенной длины. Из них и складываются блоки;

3) облачный майнинг — майнер платит деньги какой-либо компании за оборудование.

Для «добычи» той или иной криптовалюты нужен определенный алгоритм. Краткое описание самых популярных алгоритмов [5] и их валют представлено в таблице.

**Основные алгоритмы майнинга и их описание**

| Алгоритм | Описание | Валюты |
|---|---|---|
| SHA-256 | Сокращение SHA расшифровывается как «безопасный расчет хеша». Этот вычислительный метод обеспечивает неизменность информации в криптографическом наборе данных. Информация зашифрована или закодирована, поэтому находится в безопасности, и получить доступ могут только те люди, у которых есть код. Работает с данными, разбитыми на фрагменты по 512 бит (64 байт), криптографически смешивает их и выдает 256-битный (32 байта) хеш [6] | Bitcoin, Steemit, DigiByte, Peercoin, Namecoin, Terracoin, PetroDollar и др. |
| Dagger-Hashimoto (Ethash) | Алгоритм Виталия Бутерина, который использует направленные ациклические графики для одновременного достижения быстрых вычислений в памяти | Ethereum, EthereumClassic, Expanse, Ubiq, Pirl, Musicoin, Metaverse, SOILcoin, Bowhead и др. |
| X11 | Предусматривает 11 раундов применения различных хеш-функций (blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd, echo) | Dash, Pura, Memetic, TransferCoin, HyperStake, 365Coin и др. |
| Keccak | Алгоритм стандарта SHA-3 имеет структурную конструкцию «губки», где все вводные данные сначала как бы впитываются и суммируются по узлу с инвариантами состояния, затем внутри криптографической губки создаются многосерийные перестановки и на выходе «выжимается» зашифрованный результат | Nexus, SmartCash, CreativeChain, MaxCoin |
| ECDSA | Алгоритм с открытым ключом для создания цифровой подписи | Ripple |
| CryptoNight | Использует функцию привязки памяти, которая не может быть легко конвейерной. Из-за требований к объему оперативной памяти, данный алгоритм не применяется в ASIC-чипах | Monero, ByteCoin, Dashcoin, CryptoNoteCoin, Sumokoin, DigitalNote, Intensecoin, Electroneum и др. |
| Blake2 | Основан на шифре ChaCha/Salsa20 [7] и специально оптимизирован для использования в качестве альтернативы алгоритма MD5 [8], т. е. в облачных сервисах, программном обеспечении и т. п. | Siacoin |
| Scrypt | Использует большой объем оперативной памяти (памяти со случайным доступом). Память в Scrypt используется для хранения большого вектора псевдослучайных битовых последовательностей, генерируемых в начале алгоритма. После создания вектора его элементы запрашиваются в псевдослучайном порядке и комбинируются друг с другом для получения ключа | Litecoin, Dogecoin, Syscoin, BelaCoin, Einsteinium, Potcoin, ViaCoin, DNotes и др. |

*Окончание таблицы*

| | | |
|---|---|---|
| Lyra2RE | Характеризуется уменьшенным потреблением электроэнергии. Это цепной алгоритм, построенный на таких функциях, как Keccak, Skein, Groestl, Blake и Lyra2 | Verge, ZCoin, Vertcoin, Zoin, Unitus, Hexx, Crypto и др. |
| NIST5 | Представляет собой смесь алгоритмов BLAKE, Grøstl, JH, Keccak, Skein [9] | Electra, CoinonatX, Powercoin, NamoCoin, Bulwark и др. |
| NeoScrypt | Имеет криптографическое решение с интенсивным использованием памяти | VIVO, Phoenixcoin, Feathercoin, Guncoin, Orbitcoin, DESIRE и др. |
| Equihash | Уникальный алгоритм, который должен позволить осуществлять майнинг, используя для этого стандартные домашние компьютеры. Сегодня нагрузка на сеть распределена неравномерно, Equihash призван исправить данную оплошность [10] | Bitcoin Gold, Zcash, Komodo, ZClassic, ZenCash, Hush, BitcoinZ, Zero, Bitgem и др. |

Если алгоритмы до сих пор актуальны, они развиваются, объединяются, расширяются, то некоторые из валют, перечисленных в таблице, из-за волатильности рынка могли перестать существовать.

Заметим, что некоторые алгоритмы, такие как ECDSA, blake2b, награждают только одной единственной валютой, данные алгоритмы основаны на MD5 [7], или Message Digest 5 — это 128-битный алгоритм хеширования, разработанный в начале 1990-х годов. Данный алгоритм является уязвимым и постепенно алгоритмом SHA.

В соответствии с краткими описаниями алгоритмов можно сказать, что все они достаточно схожи. Суть их разновидности лишь в сложности расчета блоков, ведь при работе над ними максимально используется ресурс устройства, чтобы максимально быстро обработать транзакцию. Для расчета сложности майнинга применяют формулу

$$\text{difficulty} = \frac{\text{difficulty\_1\_target}}{\text{current\_target}},$$

где difficulty — сложность; target — 256-битное число. Difficulty_1_target может принимать различные значения. Обычно это хеш, 32 первых бита которого являются нулями, остальную часть составляют цифры и буквы.

Реализовывать алгоритмы хеширования можно на любом устройстве — главное, чтобы это устройство было способно обработать заданный алгоритм, если возникнут сбои в работе или алгоритм окажется слишком сложным, данная операция будет прервана, а в худшем случае вычислительное устройство перегреется. В рассматриваемом случае в качестве оборудования возьмем три видеокарты с разными характеристиками: две из них с процессором NVIDIA

GTX 1060 памятью 6 Гб и одну с процессором GTX 1050 памятью 4 Гб. Для подбора подходящих к оборудованию алгоритмов можно воспользоваться онлайн-сервисами, такими как What to mine, специальными калькуляторами или бенчмарками пулов. На основе опыта использования разных видов майнинга можно утверждать, что основным и наглядным для примера будет майнинг на пуле Nicehash [11].

Почему именно этот тип майнинга и этот пул?

Во-первых, на пулах не нужно следить за прибыльностью алгоритмов, если алгоритм невыгоден или сложен для данной системы, пул автоматически переходит на другой алгоритм.

Во-вторых, помимо наглядного интерфейса, показывающего, какой алгоритм запущен (рис. 1), высвечивается командное окно (рис. 2), где можно увидеть не только алгоритмы, которые реализуются в реальном времени, но и их хешрейт [12], а также отработанные транзакции.

| | | | |
|---|---|---|---|
| **GPU#1** | Nist5 | 33.172 MH/s | 0.00010006 |
| **GPU#2** | DaggerHashimoto (Dual) | 11.025 MH/s | 0.00004768 |
| **GPU#2** | Decred (Dual) | 264.603 MH/s | 0.00000305 |
| **GPU#3** | NeoScrypt | 694.840 kH/s | 0.00009863 |

**Рис. 1.** Фрагмент интерфейса

```
core | Algorithm 'nist5' total speed: 33.190606 MH/s
core | Algorithm 'daggerhashimoto_decred' total speed: 10.993019 MH/s & 263.837509 MH/s
core | Algorithm 'neoscrypt' total speed: 695.861272 kH/s
algo-nist5 | New job_0 '00000023cca02e20', diff=0.1
algo-nist5 | New job_0 '00000023cca05322', diff=0.1
core | Algorithm 'nist5' total speed: 33.170082 MH/s
core | Algorithm 'daggerhashimoto_decred' total speed: 11.023829 MH/s & 264.575617 MH/s
core | Algorithm 'neoscrypt' total speed: 695.818960 kH/s
net | Share #11 accepted
net | Share #23 accepted
algo-nist5 | New job_0 '00000023cca05cb6', diff=0.1
net | Share #24 accepted
algo-neoscrypt | New job_0 '00000025d68a9ca0', diff=0.125
core | Algorithm 'nist5' total speed: 33.156066 MH/s
core | Algorithm 'daggerhashimoto_decred' total speed: 11.063757 MH/s & 265.535022 MH/s
core | Algorithm 'neoscrypt' total speed: 696.064713 kH/s
algo-nist5 | New job_0 '00000023cca0b7ba', diff=0.1
net | Share #25 accepted
core | Algorithm 'nist5' total speed: 33.142234 MH/s
core | Algorithm 'neoscrypt' total speed: 695.812996 kH/s
```

**Рис. 2.** Командное окно

В-третьих, выводимые в личном кабинете сервиса Nicehash графики статистики (рис. 3) дают понять, какой алгоритм для имеющихся мощностей подходит больше всего и какой доход он обеспечивает.

Анализируя статистику, можно заметить, что самым прибыльным алгоритмом является Nist5. Данный алгоритм используется чаще всего, поскольку при его реализации температура и энергопотребление оборудования имеют низкие значения, а хешрейт при этом не ниже, чем у других алгоритмов.

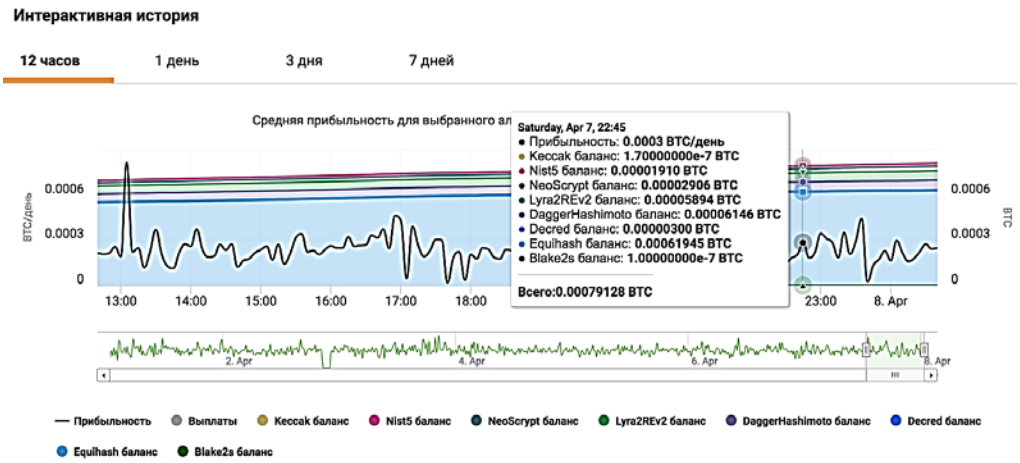


**Рис. 3.** Статистика доходности алгоритмов

Сравнение алгоритмов Nist5 и Equihash по температуре, энергопотреблению и другим характеристикам выполнено на рис. 4.

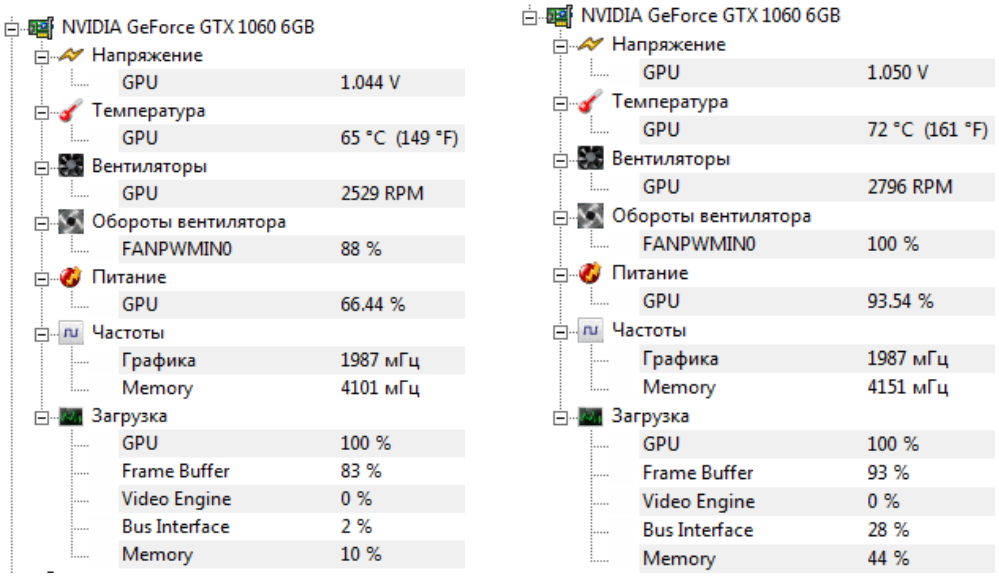


**Рис. 4.** Сравнение алгоритмов Nist5 и Equihash

В составе Nist5 [9] входят такие алгоритмы, как BLAKE, Grøstl, JH, Keccak, Skein. Согласно статистике, показанной на рис. 3, можно обнаружить алгоритм Keccak, работает отдельно, когда Nist5 занят или падает в эффективности.

Подводя итоги, отметим, что эффективность вычислений зависит от следующих параметров:

1) мощности и производительности оборудования;

2) выбора вида и типа майнинга;

3) корректности подбора алгоритмов.

Если говорить о заработке, то стоит также учитывать факторы роста и убытка криптовалюты, поскольку себестоимость монет может изменяться, что приведет к росту дохода или убыткам.

**Литература**


[1] Тян Н.Г., Замотаева Е.В. Перспективы развития рынка блокчейн. *Современные условия взаимодействия науки и техники*. Уфа, Омега-Сайнс, 2017, с. 121–124;

[2] Iansiti M., Lakhani K.R. The truth about blockchain. *Harv. Bus. Rev.*, 2017, vol. 95, no. 1, pp. 118–127.

[3] Арянова Т. Гайд по майнингу: всё, что нужно знать о добыче криптовалют. *ru.ihodl.com: веб-сайт*. URL: https://ru.insider.pro/tutorials/2017-09-07/gajd-po-majningu-vsyo-chto-nuzhno-znat-o-dobyche-kriptovalyut/ (дата обращения: 18.12.2019).

[4] Когда соло-майнинг выгоднее, чем добыча в пуле? *crypto-fox.ru: веб-сайт*. URL: https://crypto-fox.ru/faq/solo-majning/ (дата обращения: 18.12.2019).

[5] Алгоритмы майнинга криптовалют — таблица 2018 и краткое описание. mining-*cryptocurrency.ru: веб-сайт*. URL: https://mining-cryptocurrency.ru/algoritmy-kriptovalyut/ (дата обращения: 18.12.2019).

[6] Майним Bitcoin с помощью бумаги и ручки. *habrahabr.ru: веб-сайт*. URL: https://habrahabr.ru/post/258181/ (дата обращения: 18.12.2019).

[7] Blake2 – fast secure hashing. *blake2.net: веб-сайт*. URL: https://blake2.net (дата обращения: 18.12.2019).

[8] Хэш-функция MD5. *habr.com: веб-сайт*. URL: https://habr.com/ru/sandbox/26876/ (дата обращения: 18.12.2019).

[9] Perlner R., Burr W.E., Turan M.S., et al. Third-round report of the SHA-3 cryptographic hash algorithm. NIST, 2012.

[10] Алгоритм Equihash. *cryptocoins.group: веб-сайт*. URL: http://cryptocoins.group/equihash (дата обращения: 18.12.2019).

[11] Что такое Хешрейт: характеристики и сервисы для анализа. *altcoinlog.com: веб-сайт*. URL: https://altcoinlog.com/chto-takoe-hashrate (дата обращения: 18.12.2019).

[12] About Nicehash. *nicehash.com: веб-сайт*. URL: https://www.nicehash.com/about (дата обращения: 18.12.2019).



**Бушуев Роман Андреевич** — магистрант кафедры «Системы обработки информации и управления «, МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

**Марченко Антон Васильевич** — магистрант кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

**Научный руководитель** — Ковалева Наталья Александровна, старший преподаватель кафедры «Системы обработки информации и управления», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.



**Ссылку на эту статью просим оформлять следующим образом:**

Бушуев Р.А., Марченко А.В. Обзор алгоритмов хеширования на персональном компьютере. *Политехнический молодежный журнал*, 2020, № 03(44). http://dx.doi.org/10.18698/2541-8009-2020-03-585

# OVERVIEW HASHING ALGORITHMS ON A PERSONAL COMPUTER

**R.A. Bushuev** presentman@bk.ru
SPIN-code: 4704-2637

**A.V. Marchenko** mart0n@mail.ru
SPIN-code: 2567-4813

**Bauman Moscow State Technical University, Moscow, Russian Federation**

## Abstract

*The basic hashing algorithms for mining are considered, their characteristics are described and the best version of the hashing algorithm on a personal computer (with certain technical parameters) is proposed. Descriptions of hash functions are presented, results and approximate indications of their work are given. The work done will allow you to get acquainted with the most common mining algorithms, types of mining, as well as delve deeper into the topic of cryptocurrencies and their varieties. The given practical results will allow you not only to analyze the cryptocurrency market and mining in general, but also to understand how calculations affect the technical parameters of the device.*

## Keywords

*Mining, cryptocurrency, pool, hashing, algorithm, exchange, hashrate, blockchain*

Received 13.02.2020


## References

[1] Tyan N.G., Zamotaeva E.V. [Development prospects for blockchain market]. Sovremennye usloviya vzaimodeystviya nauki i tekhniki [Today conditions of interaction between science and technics]. Ufa, Omega-Sayns Publ., 2017, pp. 121–124 (in Russ.).

[2] Iansiti M., Lakhani K.R. The truth about blockchain. *Harv. Bus. Rev*., 2017, vol. 95, no. 1, pp. 118–127.

[3] Aryanova T. Gayd po mayningu: vse, chto nuzhno znat' o dobyche kriptovalyut [Mining guide: everything you should know about cryptocurrency mining]. *ru.ihodl.com: website* (in Russ.). URL: https://ru.insider.pro/tutorials/2017-09-07/gajd-po-majningu-vsyo-chto-nuzhno-znat-o-dobyche-kriptovalyut/ (accessed: 18.12.2019).

[4] Kogda solo-mayning vygodnee, chem dobycha v pule? [When is solo mining more beneficial than pool mining?] *crypto-fox.ru: website* (in Russ.). URL: https://crypto-fox.ru/faq/solo-majning/ (accessed: 18.12.2019).

[5] Algoritmy mayninga kriptovalyut — tablitsa 2018 i kratkoe opisanie [Algorithms of cryptocurrency mining: 2018 table and brief summary]. *mining-cryptocurrency.ru: website* (in Russ.). URL: https://mining-cryptocurrency.ru/algoritmy-kriptovalyut/ (accessed: 18.12.2019).

[6] Maynim Bitcoin s pomoshch'yu bumagi i ruchki [Bitcoin mining by means of paper and pen]. *habrahabr.ru: website* (in Russ.). URL: https://habrahabr.ru/post/258181/ (accessed: 18.12.2019).

[7] Blake2 – fast secure hashing. *blake2.net: website*. URL: https://blake2.net (accessed: 18.12.2019).

[8] Khesh-funktsiya MD5 [MD5 cash function]. *habr.com: website* (in Russ.). URL: https://habr.com/ru/sandbox/26876/ (accessed: 18.12.2019).

[9] Perlner R., Burr W.E., Turan M.S., et al. Third-round report of the SHA-3 cryptographic hash algorithm. NIST, 2012.
[10] Algoritm Equihash [Equihash algorithm]. *cryptocoins.group: website* (in Russ.). URL: http://cryptocoins.group/equihash (accessed: 18.12.2019).
[11] Chto takoe Kheshreyt: kharakteristiki i servisy dlya analiza [What is hash rate: characteristics and services for analysis]. *altcoinlog.com: website* (in Russ.). URL: https://altcoinlog.com/chto-takoe-hashrate (accessed: 18.12.2019).
[12] About Nicehash. *nicehash.com: website*. URL: https://www.nicehash.com/about (accessed: 18.12.2019).

**Bushuev R.A.** — Master's Degree Student, Department of Information Processing Systems, Bauman Moscow State Technical University, Moscow, Russian Federation.

**Marchenko A.V.** — Master's Degree Student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

**Scientific advisor** — Kovaleva N.A., Senior Lecturer, Department of Information Processing Systems, Bauman Moscow State Technical University, Moscow, Russian Federation.

**Please cite this article in English as:**
Bushuev R.A., Marchenko A.V. Overview hashing algorithms on a personal computer. *Politekhnicheskiy molodezhnyy zhurnal* [Politechnical student journal], 2020, no. 03(44). http://dx.doi.org/ 10.18698/2541-8009-2020-03-585.html (in Russ.).