электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

**УДК 004.75**

# Добыча криптовалюты в домашних условиях

***Калистратов А.П.**, студент*
*Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,*
*кафедра «Системы обработки информации и управления»*

*Научный руководитель: Румянцева Е.И.,доцент*
*Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана*
*bauman@bmstu.ru*

## 1. Введение

Для того, чтобы иметь представление о предметной области, в начале статьи определим, что такое криптовалюта. Криптовалюта – электронное средство расчета, попросту, деньги. Криптовалюта не зависит от материальных благ, т.е., фактически ничем не обеспечена, в отличие от традиционных денежных средств, например, доллара. При этом самостоятельно эту валюту выпустить нельзя, т.к., она эмитируется посредством совершения сложных математических расчетов. Криптографическое происхождение валюты защищает ее пользователей и от мошенничества, т.к., для перевода также необходимо произвести сложные математические операции с непредсказуемым и уникальным результатом. Используя криптовалюту, возможно создание экономики, недоступную для контроля внешними силами. В данной статье в качестве примера криптовалюты используется Биткоин (Bitcoin).

Bitcoin – популярная криптовалюта, широко используемая по всему миру. Большинство пользователей пользуются специальным ПО – биткоин-кошельками для накопления и перевода валюты другим пользователям. Каждый кошелек содержит в себе историю транзакций между всеми кошельками с момента создания системы. Это делает Биткоин распределенной системой, защищенной от мошенничества.

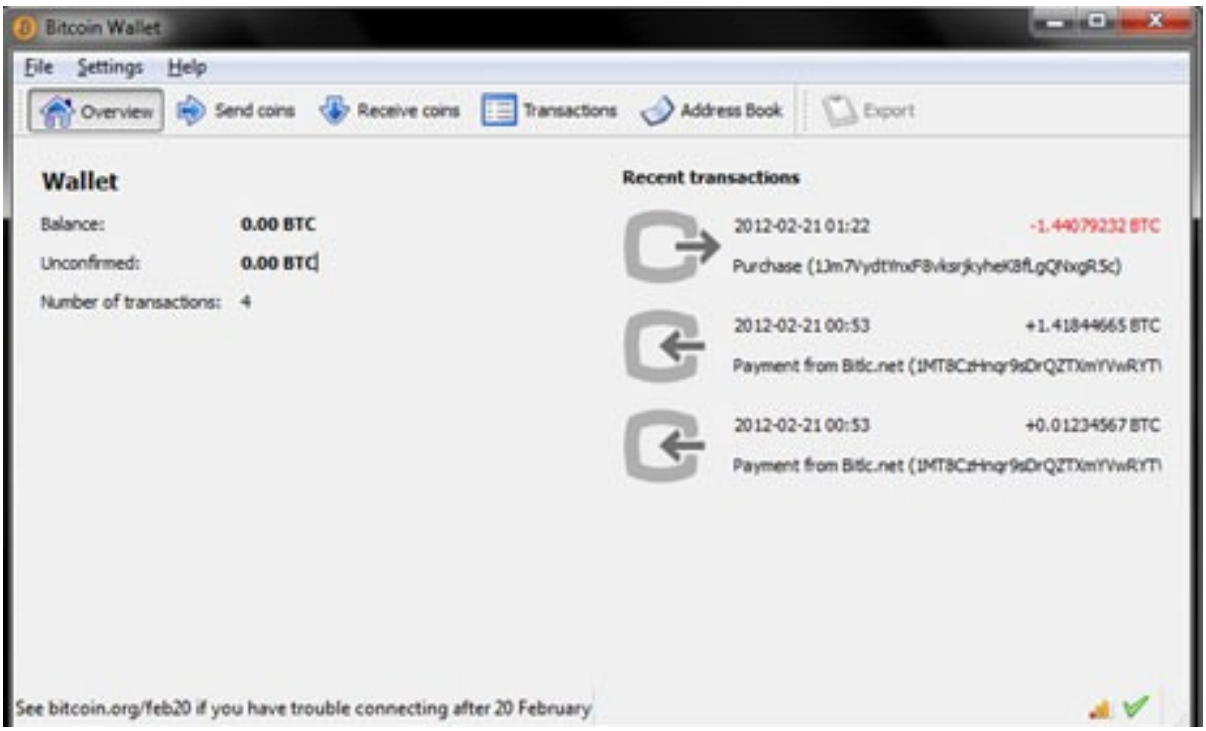


Рис. 1. Биткоин-кошелек

## 2. Добыча криптовалюты

Количество биткоинов конечно, при этом новые биткоины можно получить только с помощью майнинга. Майнинг – процесс эмиссии биткоинов посредством решения крайне сложной математической задачи. Сама задача заключается в преобразовании массива данных произвольного размера в блок данных фиксированного размера с помощью определенной функции (хэш-функции). При этом в полученном блоке данных содержится информация о транзакциях, произведенных в системе с момента создания предыдущего блока данных. Также особенностью полученного блока данных является его уникальность – при внесении малейшего изменения в исходный массив данных меняется и блок, получаемый в результате. При этом, проверить хэш (результат работы) можно за доли секунды. На принципе проверки результата работы (proof-of-work) основана работа сети биткоинов.

Т.к., необходимый блок данных невозможно предугадать или как-то вычислить, процесс майнинга заключается в переборе всех возможных вариантов. Пользователь, первым подобравший подходящий вариант, получает вознаграждение в виде перевода определенного (уменьшающегося со временем) количества биткоинов.

Система биткоинов задумана саморегулирующейся, т.е., при увеличении вычислительной мощности машин сети повышается и количество усилий, требуемых для создания «выигрышного» набора данных. Обратное тоже верно – при уменьшении

продуктивности сети параметр «сложность» понижается. Сложность отвечает за требования, предъявляемые к хэшам и пересчитывается каждые 2016 вознаграждений.

В общем и целом, желающие получить максимальное вознаграждение должны задействовать максимальные вычислительные мощности для работы в системе. Со временем количество биткоинов, получаемое за подбор «выигрышного» хэша уменьшается. На данный момент вознаграждение составляет 25 биткоинов (при старте системы вознаграждение составляло 50 биткоинов)

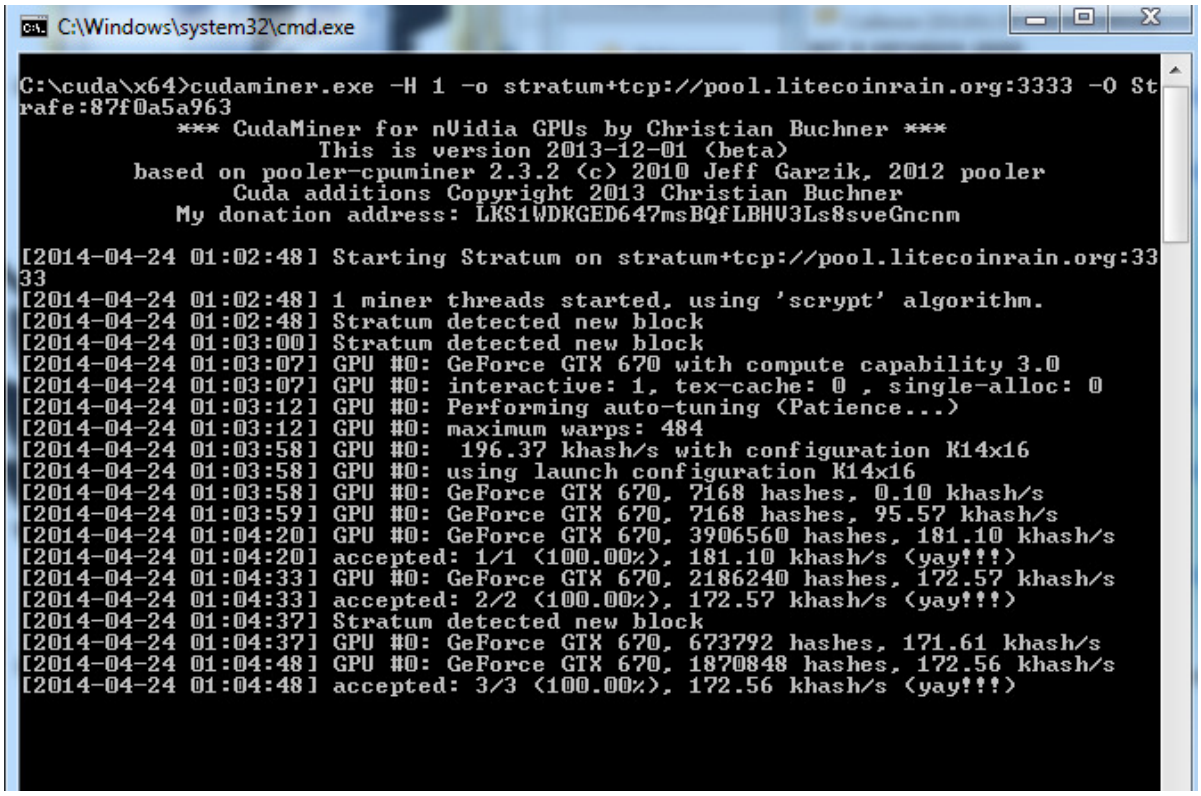


Рис. 2. Интерфейс майнера для ПК

### 3. Приспособления для майнинга в домашних условиях

Для майнинга биткоинов на ПК используются специальные программы – майнеры. Для каждого способа майнинга используется свой софт, друг от друга принципиально ничем не отличающийся. При низкой сложности сети можно майнить и с помощью CPU (центрального процессора), но этот способ оправдан лишь в самом начале, т.к., майнинг подразумевает параллельные вычисления, к которым CPU не приспособлен. Довольно быстро процессоры перестают окупать даже электричество, потребляемое в процессе работы.

К примеру, в единицу времени CPU может выполнитть 4 операции, в то же время, GPU (графический процессор) может выполнить 3200 операций. Компьютеры, предназначенные для майнинга биткоинов и оснащенные мощными графическими процессорами, называются биткоин-фермами. В то же время, биткоин-ферма может использоваться и как рабочий\домашний компьютер, а майнить в свободное от взаимодействия с пользователем время. В таблице ниже приведена примерная конфигурация фермы для использования в домашних условиях.

Примерная конфигурация фермы, пригодной для игр и работы

| Компонент | Модель | Цена |
|---|---|---|
| Корпус | CoolerMaster HAF 932 | $140 |
| БП | PC Power & Cooling Silencer Mk II 950W, 80 PLUS Silver Certified | $120 |
| Материнская плата | MSI P67A-GD65 | $173 |
| Процессор | Intel Core i7-2700K | $340 |
| ОЗУ | G.SKILL ECO Series 8GB | $55 |
| Видеокарта | Radeon HD 6990 | $734 |
| Охлаждение | CoolerMaster Hyper212+ | $40 |
| Жесткий диск | Seagate 1TB 7200RPM HDD | $70 |
| Оптический привод | ASUS DVD-RW | $22 |
| Клавиатура | LITE-ON SK-1788/BS PS/2 Keyboard | $8 |
| Мышь | V7 M30P20-7N PS/2 Mouse | $7 |
| Монитор | LG IPS231P-BN Black 23" 6ms IPS | $250 |
| Всего | | $1949 |

Также применяются различные специализированные устройства, такие как FPGA (ППВМ, программируемая пользователем вентильная матрица) и ASIC (ИССН, интегральная схема специального назначения), но они предназначены для добычи биткоинов в промышленных масштабах, так что в этой статье они упомянуты лишь для сравнения с домашней биткоин-фермой.

### 4. Выгоден ли майнинг

Сравнение способов майнинга представлено в виде рисунка 3. Из него видно, что наиболее эффективными являются как раз-таки промышленные инструменты добычи –

ASIC, FPGA. Плюс GPU - универсальность , их можно использовать для разных криптовалют без изменения характеристик фермы, в то время как специфическое железо можно использовать только для одной валюты, к примеру, для биткоина.

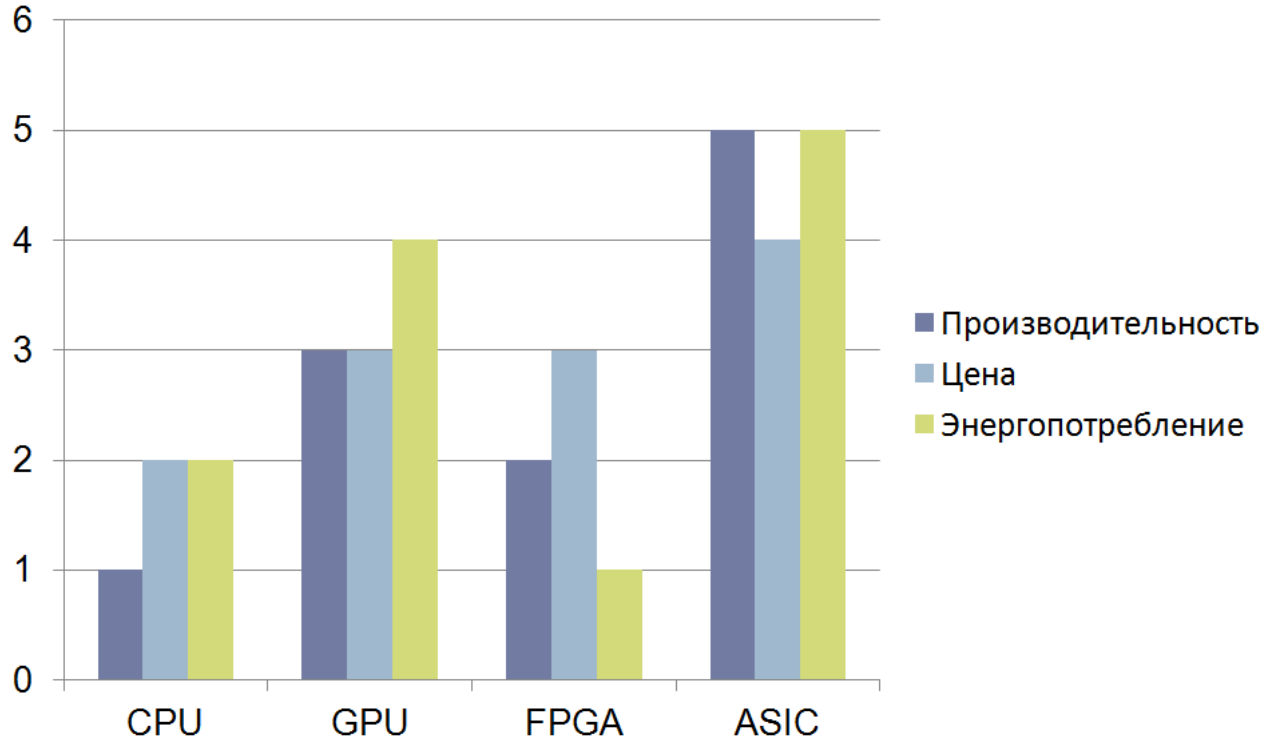


Рис. 3. Примерное сравнение оборудования для майнинга

На рисунке 4 представлено сравнение 4 типичных конфигураций ферм, значительно различающихся по стоимости – две специально для майнинга и две для домашнего использования с майнингом в свободное время. Наиболее рентабельно использовать конфигурацию дешевого майнера, компенсировав это их числом. Они окупят себя, но доход принесут небольшой. Дорогие фермы содержать более рискованно, т.к., несмотря на большую прибыль, они будут очень долго окупать себя из-за высокой стоимости (более 3000$). Домашние конфигурации содержать специально для майнинга и вовсе невыгодно, т.к., при нынешних сложности и курсе биткоина они едва окупят затраты на электричество.

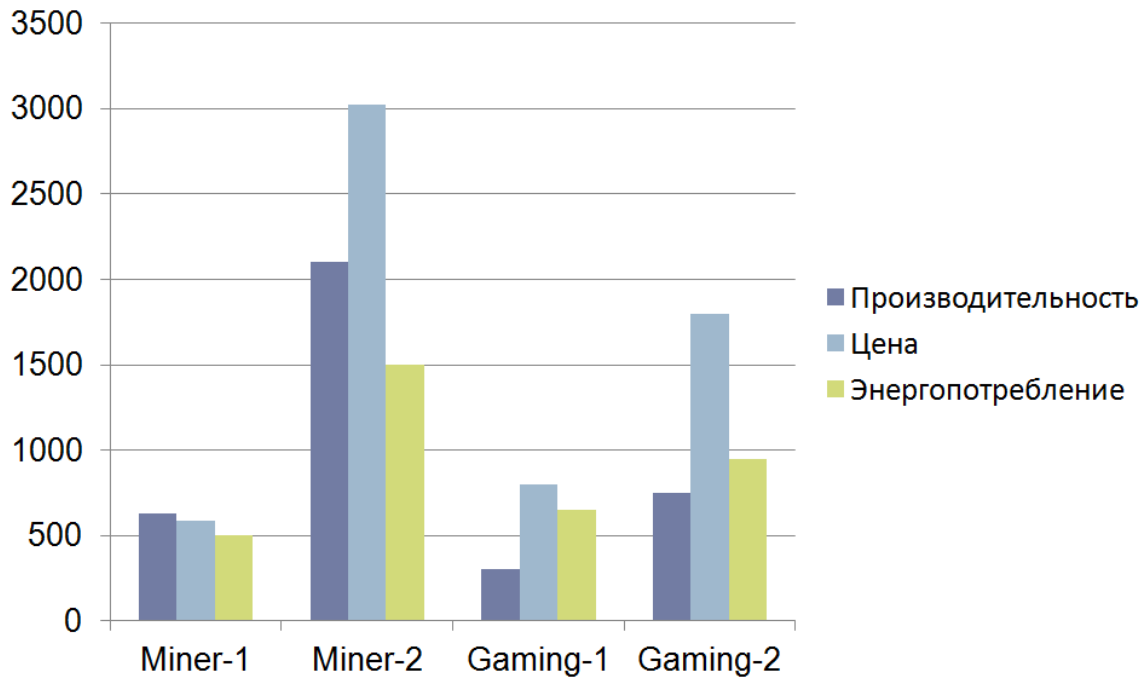


Рис. 4. Сравнение биткоин-ферм

## 5. Заключение

В заключение хочется подчеркнуть, что, несмотря на то, что добыча биткоинов ранее являлась крайне выгодным занятием, резкое увеличение сложности вычислений свело на нет выгоду от добычи биткоинов с помощью обычных компьютеров – на данный момент такой способ добычи перестал окупать себя даже в случае наличия бесплатного электричества. Возможно, стоит попробовать себя в добыче непопулярной криптовалюты, но в этом случае под вопросом ее рыночная стоимость, а, как было упомянуто в начале статьи, без интереса инвесторов стоимость криптовалюты стремится к нулю.

## Список литературы

1. Bitcoin mining profitability calculator. Available at: http://www.bitcoinx.com/profit/, accessed 23.04.2014.
2. Bitcoincharts: financial and technical data related to the Bitcoin network.
3. Available at: http://bitcoincharts.com/, accessed 23.04.2014.
4. Graf K.S. On the origins of Bitcoin: Stages of monetary evolution. Available at: http://konradsgraf.com/storage/On%20the%20Origins%20of%20Bitcoin%20Graf%2003.11.13.pdf, accessed 23.04.2014.
5. Andrychowicz M, Dziembowski S., Malinowski D., Mazurek L. Secure Multiparty Computations on Bitcoin. Available at: http://eprint.iacr.org/2013/784, accessed 23.04.2014.