

УДК 004.75

Home mining of cryptocurrency

*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. Introduction

To begin with, we have to define, what cryptocurrency is. Cryptocurrency is a digital medium of exchange. Cryptocurrency does not depend on material wealth. Fundamentally, cryptocurrencies are specifications regarding the use of currency which seeks to incorporate principles of cryptography to implement a distributed, decentralized and secure information economy. In this article, I use Bitcoin as an example because it is the most popular cryptocurrency.

Bitcoin is a web platform that enables us to use completely digital money. From a user's perspective, Bitcoin is nothing more than a mobile app or a computer program that provides a personal Bitcoin wallet and allows sending and receiving currency. This is how Bitcoin works for most of the users.

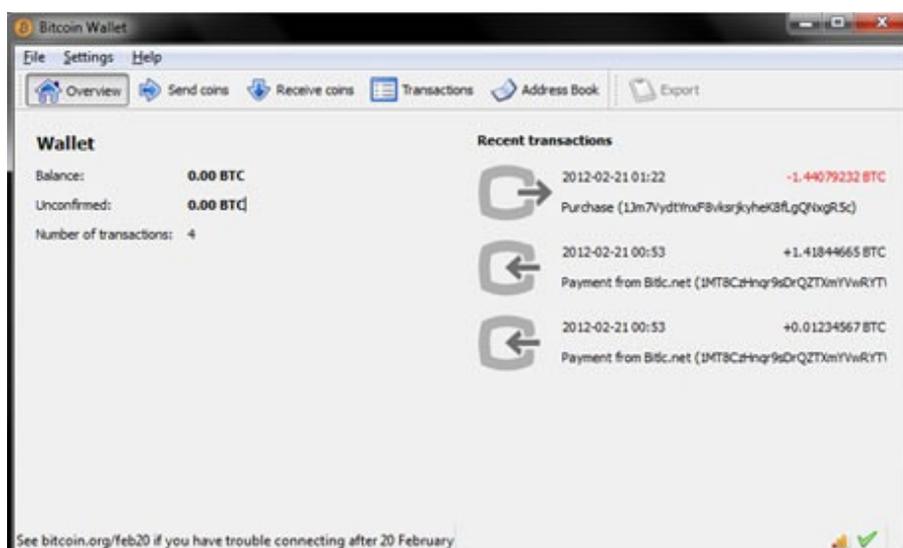


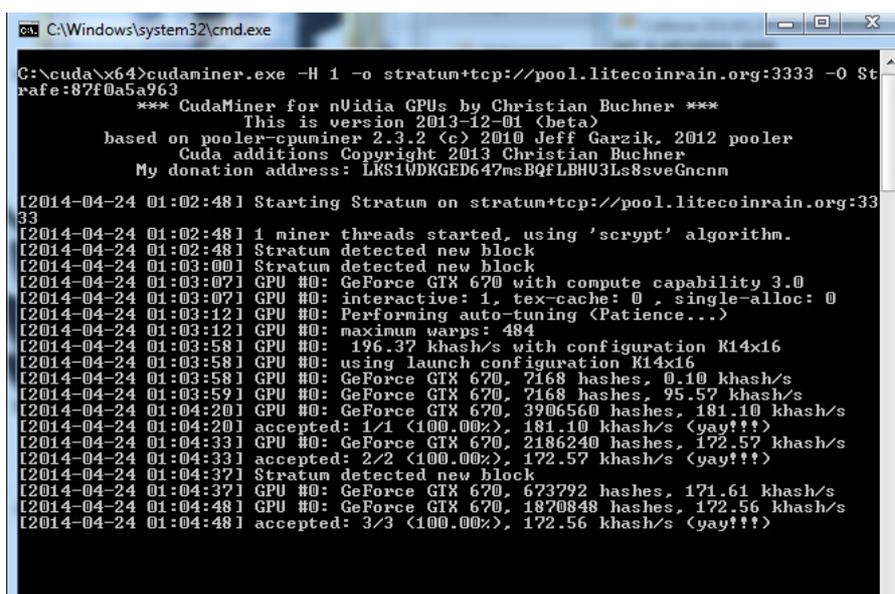
Fig. 1. Bitcoin wallet

2. Principles of mining

Mining allows the initial supply of Bitcoins to be distributed without a centralized authority. Basically, the user can obtain bitcoins by solving hashes with his PC. A hash algorithm turns an arbitrarily-large amount of data into a fixed-length hash. The same hash will always result from the same data, but modifying the data by even one bit will completely change the hash. Like all computer data, hashes are large numbers, and are usually written as hexadecimal

The difficulty consists in finding out how long does it take to find a hash below a given target. The Network contains a constantly raising «difficulty factor» which is a conditional value that determines how hard it is to find a «winning» hash.

So the basic concept of Bitcoin mining is that there's a little chunk of each block that contains meaningless random data, and Bitcoin miners take all the data in the current block, shuffle up that random chunk and calculate the hash of the whole thing. Once the network confirms the solution, the miner is rewarded with a number of Bitcoins.



```
C:\Windows\system32\cmd.exe
C:\cuda\64>cudaminer.exe -H 1 -o stratum+tcp://pool.litecoinrain.org:3333 -O Strafe:87f@a5a963
*** CudaMiner for nVidia GPUs by Christian Buchner ***
      This is version 2013-12-01 (beta)
based on pooler-cpuminer 2.3.2 (c) 2010 Jeff Garzik, 2012 pooler
      Cuda additions Copyright 2013 Christian Buchner
My donation address: LKS1WDRKGED647msBQFLBHU3Ls8sveGncnm

[2014-04-24 01:02:48] Starting Stratum on stratum+tcp://pool.litecoinrain.org:3333
[2014-04-24 01:02:48] 1 miner threads started, using 'scrypt' algorithm.
[2014-04-24 01:02:48] Stratum detected new block
[2014-04-24 01:03:00] Stratum detected new block
[2014-04-24 01:03:07] GPU #0: GeForce GTX 670 with compute capability 3.0
[2014-04-24 01:03:07] GPU #0: interactive: 1, tex-cache: 0, single-alloc: 0
[2014-04-24 01:03:12] GPU #0: Performing auto-tuning (Patience...)
[2014-04-24 01:03:12] GPU #0: maximum warps: 484
[2014-04-24 01:03:58] GPU #0: 196.37 khash/s with configuration K14x16
[2014-04-24 01:03:58] GPU #0: using launch configuration K14x16
[2014-04-24 01:03:58] GPU #0: GeForce GTX 670, 7168 hashes, 0.10 khash/s
[2014-04-24 01:03:59] GPU #0: GeForce GTX 670, 7168 hashes, 95.57 khash/s
[2014-04-24 01:04:20] GPU #0: GeForce GTX 670, 3906560 hashes, 181.10 khash/s
[2014-04-24 01:04:20] accepted: 1/1 (100.00%), 181.10 khash/s <yay!!!>
[2014-04-24 01:04:33] GPU #0: GeForce GTX 670, 2186240 hashes, 172.57 khash/s
[2014-04-24 01:04:33] accepted: 2/2 (100.00%), 172.57 khash/s <yay!!!>
[2014-04-24 01:04:37] Stratum detected new block
[2014-04-24 01:04:37] GPU #0: GeForce GTX 670, 673792 hashes, 171.61 khash/s
[2014-04-24 01:04:48] GPU #0: GeForce GTX 670, 1870848 hashes, 172.56 khash/s
[2014-04-24 01:04:48] accepted: 3/3 (100.00%), 172.56 khash/s <yay!!!>
```

Fig. 2. Miner interface

3. Mining equipment

Over time the users used various types of hardware to mine blocks. Early Bitcoin client versions allowed users to use their CPUs to mine. As the network hashrate grew with more power efficient GPU miners the amount of Bitcoin's produced by CPU mining became lower than the cost of power to operate the CPUS.

A CPU core can execute 4 32-bit instructions per clock, whereas a GPU like the Radeon HD 5970 can execute 3200 32-bit instructions per clock. CPUs and GPUs form a mining rig –

computer which is built and operated to mine bitcoins. On the other hand, a rig can be a computer that fills other needs, such as gaming, and mine only part-time. I have made a configuration (see the table) for a typical multipurpose mining rig just as an example.

Field programmable gate array (FPGA) and application-specific integrated circuit (ASIC) are the devices which were designed especially for the purpose of mining. For the amount of power they consume, they are vastly faster than all the previous technologies. But, unlike mining rigs, one can't use them for anything but mining.

Typical mining-gaming configuration

Component	Description	Price
Chassis	CoolerMaster HAF 932	\$140
Power Supply	PC Power & Cooling Silencer Mk II 950W, 80 PLUS Silver Certified	\$120
Motherboard	MSI P67A-GD65	\$173
CPU	Intel Core i7-2700K	\$340
Memory	G.SKILL ECO Series 8GB	\$55
Graphics card	Radeon HD 6990	\$734
Heat Sink Fan	CoolerMaster Hyper212+	\$40
Storage	Seagate 1TB 7200RPM HDD	\$70
Media Drive	ASUS DVD-RW	\$22
Keyboard	LITE-ON SK-1788/BS PS/2 Keyboard	\$8
Mouse	V7 M30P20-7N PS/2 Mouse	\$7
Display	LG IPS231P-BN Black 23" 6ms IPS	\$250
Total		\$1949 + s/h/t

4. Profitable mining

I've made a comparison of mining hardware, it's shown in figure 3. 1 means low value and, vice versa, 5 means the highest results. So, as we can see, typical computers lack efficiency, but if bitcoins suddenly turn to nothing, you will still have valuable hardware. In my study I don't mean FPGAs and ASICs to be used as home miners, so I'd rather not dwell upon their efficiency and pay-off periods.

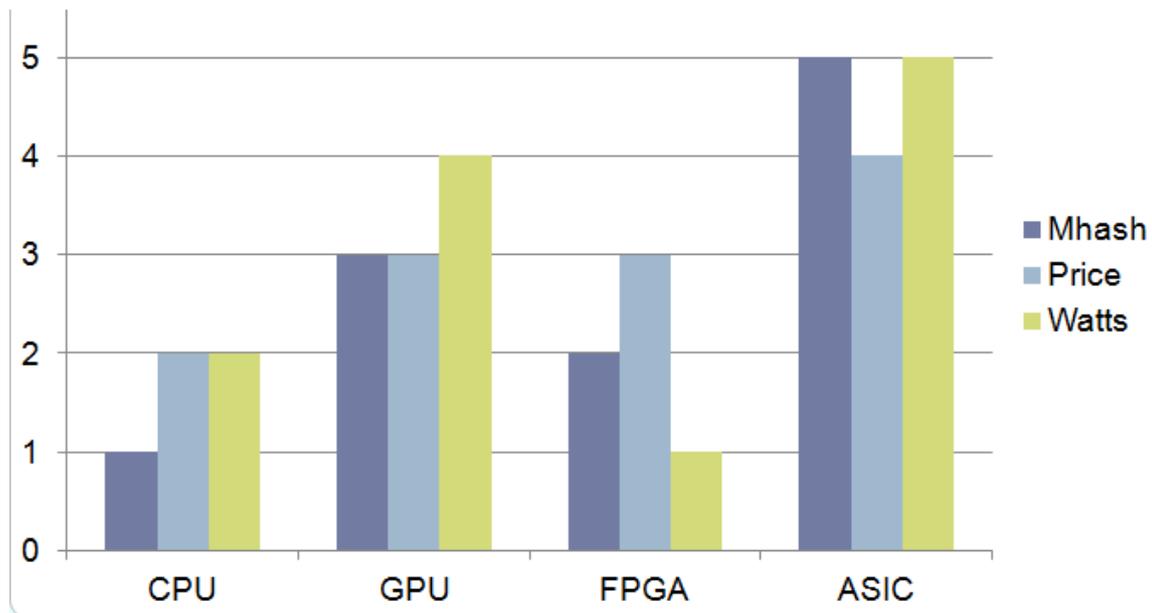


Fig. 3. Approximate comparison of mining hardware

Figure 4 presents a comparison of 4 typical miner configurations – two designed for mining and two for gaming with ability of part-time mining. The most coin-efficient is Miner-1, but its overall hash output is low, so the payoff will be sufficient, but the income will be low. With Miner-2 situation is quite opposite – the profit of mining is high, but the payoff period is longer than Miner-1’s one. Gaming configurations are not very profitable anymore, so even if one has free electricity, the gaming-mining rigs will likely never pay for themselves at this point.

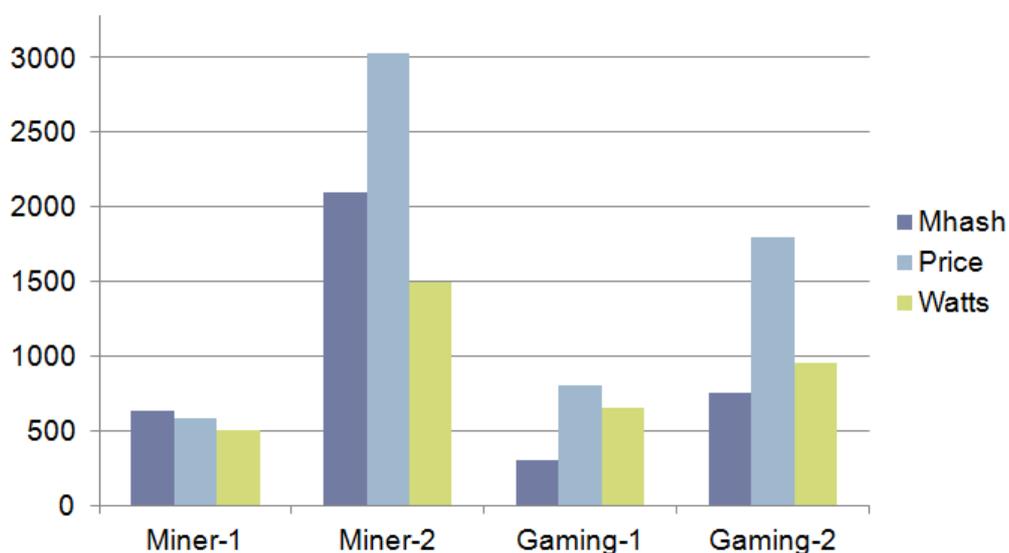


Fig. 4. Comparison of mining rigs

5. Conclusion

I'd like to state that home mining can bring some profits, but considering the present-day combination of the development level of cryptocurrency and mining technology, buying into expensive mining rigs or special hardware such as ASICs is a risky thing – bitcoin stock exchanges are stagnating, difficulty raises constantly and so does the payoff period.

References

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.