Raspberry PI jako koparka bitcoinów

Kryptowaluty coraz odważniej wkraczają do naszego życia. Bitcoin – najbardziej popularna z nich nie tylko została niedawno oficjalnie uznana w Europie za walutę, a nie towar, co ułatwia transakcje, ale też bywa akceptowana przez rosnącą liczbę firm. Pod pewnymi względami przypomina też złoto – jego zasoby są ograniczone i trzeba je wydobywać. Tyle, że zamiast przesiewać grunt na Alasce czy kopać kilofem pod ziemią, można to robić za pomocą komputera w domowym zaciszu. Takim komputerem może być nawet Raspberry PI, będący w posiadaniu wielu Czytelników.

Raspberry PI nie ma dużej mocy obliczeniowej i samo w sobie nie będzie dobrym komputerem do wydobywania bitcoinów ani innych kryptowalut. Natomiast pobiera mało mocy, jest niewielkie i niedrogie, dlatego może stanowić świetny kontroler niektórych koparek bitcoinów. Ponadto popularność tego komputera sprawiła, że Raspberry PI można znaleźć w wielu domach, czasem zupełnie niewykorzystane, stąd stanowi użyteczny przykład implementacji koparki bitcoinów.

Jak funkcjonuje Bitcoin?

We wstępie wypada wyjaśnić, jak funkcjonuje Bitcoin, gdyż o ile wiele osób orientuje się, że jest to kryptowaluta, którą można przelewać z konta na konto i wymieniać w kantorach internetowych na waluty narodowe, ale mało kto zna technikalia z tym związane, a nawet często można spotkać się z błędnymi informacjami na temat sposobu działania Bitcoina.

Bitcoin to tak naprawdę protokół kryptograficzny, który został opracowany tak, by mógł pełnić rolę waluty internetowej. Do podstawowych założeń Bitcoina należało zapewnienie by:

- Nie był to pieniądz fiducjarny, który można by było „drukować" w nieskończoność.
- Użytkownicy mogli sobie swobodnie przesyłać określone ilości waluty.
- Stan kont poszczególnych użytkowników nie był kontrolowany przez żadną pojedynczą jednostkę, tylko by był kontrolowany wspólnie, elektronicznie, przez społeczność użytkowników.

Wszystkie powyższe cechy zapewnia opracowany algorytm. Użytkownicy tworzą swoje konta samodzielnie (z użyciem odpowiedniego programu), poprzez generację pary w postaci klucza prywatnego i klucza publicznego. Klucze te służą do podpisywania i sprawdzania zleceń transakcji oraz stanowią numery kont (klucz publiczny). Na początku nowe konto jest puste i można na nie jedynie przyjmować przelewy, a więc tak samo jak w zwykłym banku. Jeśli ktoś, kto posiada na swoim koncie bitcoiny zechce przesłać na nowe konto pewną kwotę, zgłasza informację o takiej transakcji, podpisując ją odpowiednio swoimi kluczami. Zgłoszenie trafia do puli transakcji, które czekają na zatwierdzenie. Pula ta jest publicznie dostępna – wszystkie wykonane transakcje są jawne dla dowolnego użytkownika Internetu. W efekcie da się prześledzić przepływy bitcoinów pomiędzy kontami, choć to, do kogo należą dane konta nie jest jawne – nie ma to znaczenia dla poprawności działania algorytmu.

Znaczenie ma natomiast zatwierdzanie transakcji. Samo zgłoszenie transakcji społeczności nie oznacza jeszcze, że jest ona poprawna i faktycznie została wykonana. Trzeba m.in. sprawdzić, czy na danym koncie znajduje się określona liczba bitcoinów i czy zgłoszona transakcja nie kłóci się w żaden sposób z innymi zgłoszonymi. Sprawdzenie to wykonywane jest przez społeczność, która pobiera transakcje pogrupowane w bloki. Sprawdzaniem zajmuje się bardzo wiele osób jednocześnie, z użyciem wielu komputerów. Aby uniknąć oszustw

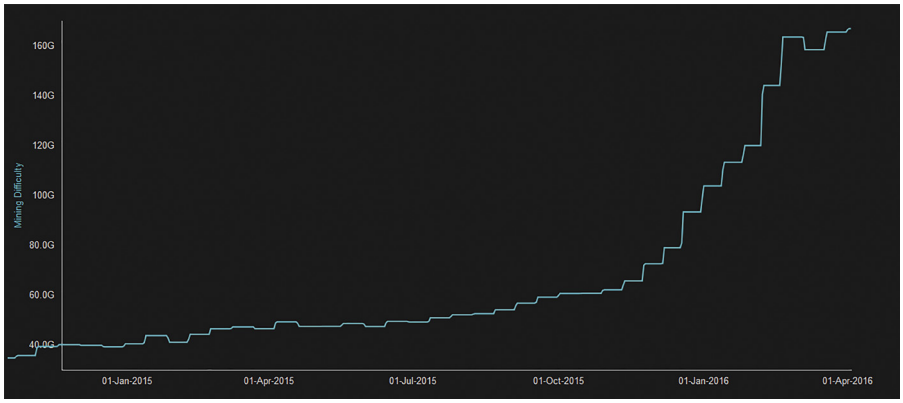
na tym etapie, pomyślne sprawdzenie bloku transakcji wymaga dodatkowo rozwiązania pewnej złożonej obliczeniowo zagadki. Czas rozwiązania zagadki zależy od posiadanej mocy obliczeniowej oraz od szczęścia, w efekcie czego pierwszymi, którzy rozwiążą zagadki dla kolejnych bloków transakcji są różne osoby (grupy osób). To właśnie ta osoba, która jako pierwsza znajdzie i zgłosi rozwiązanie tworzy nowy punkt odniesienia dla kolejnych bloków transakcji. Dlaczego jednak ktoś w ogóle miałby poświęcać moc obliczeniową swoich komputerów, by wykonywać takie obliczenia? Powodem jest nagroda w postaci nowych bitcoinów, które powstają wraz z każdym zatwierdzonym blokiem transakcji i trafiają na konto znalazcy rozwiązania zagadki. Dlatego właśnie zatwierdzanie transakcji jest nazywane jednocześnie kopaniem – wydobywa się nowe zasoby waluty, którymi następnie można swobodnie dysponować. W ten właśnie sposób powstały wszystkie bitcoiny będące w obiegu.

Tu warto jeszcze wspomnieć o ograniczeniu łącznej liczby bitcoinów. Wielkość nagrody jest bowiem z góry ograniczona i zmienia się zgodnie z określonym planem. Początkowo każdemu nowemu, zatwierdzonemu blokowi transakcji towarzyszyło wygenerowanie 50 bitcoinów. Z czasem liczba ta jest zmniejszana o połowę. Algorytm mówi bowiem, że suma bitcoinów przelewanych na konta w bloku transakcji nie może być większa niż powiększona o X suma bitcoinów na kontach, z których wykonywane są transakcje zgłoszone w danym bloku. X natomiast jest zależne od liczby dotąd zatwierdzonych bloków transakcji. Początkowo X wynosiło 50 BTC, obecnie wynosi 25 BTC, szacuje się, że za kilka miesięcy liczba bloków wzrośnie do poziomu, w którym X zmniejszy się do 12,5 BTC, a z czasem X spadnie praktycznie do zera (poniżej 10^{-8} BTC). Rekompensatą dla malejącego „wydobycia" bitcoinów są prowizje, tj. reszty z przelewanych kwot. Jeśli jeden użytkownik, mając na swoim koncie 1,01 BTC chce przelać na inne konto 1 BTC i nie wskaże żadnego dodatkowego konta, na które miałaby trafić reszta z tej transakcji, zgodnie z wcześniej podaną zasadą, osoba która rozwiąże zagadkę zatwierdzania danego bloku transakcji może podać swoje konto, na które trafi ta reszta wraz z nowowydobytymi X bitcoinami. Harmonogram zmniejszania się liczby bitcoinów nagrody został pokazany w **tabeli 1**.

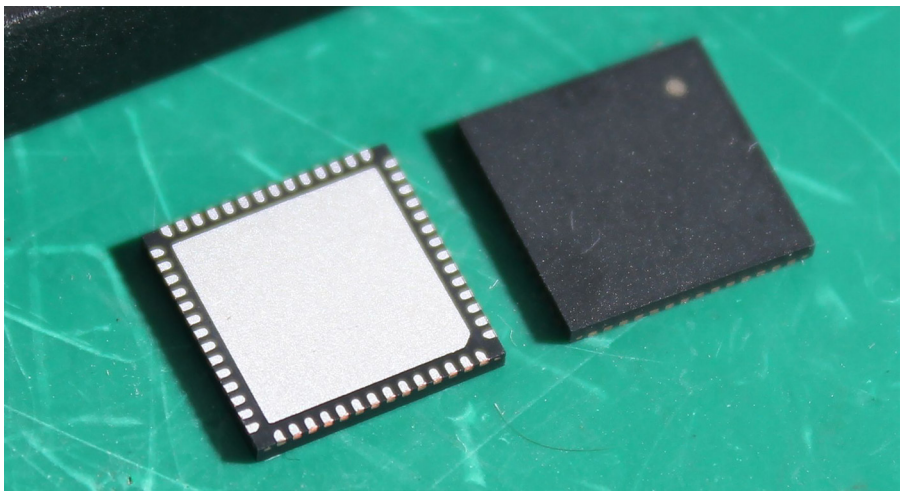
Zagadka, czyli obliczanie skrótów

Co sprawia, że zatwierdzenie bloku transakcji nie jest łatwe i wymaga niemałej mocy obliczeniowej? Odpowiada za to konieczność znalezienia takiego ciągu znaków, który po dodaniu do zatwierdzanego bloku transakcji spowoduje że hash (skrót) tego połączenia danych będzie pasował do ustalonego schematu. Skrót obliczany jest z użyciem funkcji SHA-256, a ustalony schemat wskazuje wartość, która musi być większa od wyliczonego skrótu. W praktyce sprowadza się to przede wszystkim do tego, by wyliczony skrót zaczynał się od odpowiedniej liczby zer. Ponieważ SHA-256, tak jak i inne funkcje skrótu, jest względnie łatwa do policzenia, ale nie jest znana funkcja odwrotna, znajdywanie ciągu znaków, który po uzupełnieniu bloku będzie dawał odpowiedni wynik po przetworzeniu za pomocą SHA-256 wymaga wielu żmudnych prób. Oznacza to, że praca tzw. koparki bitcoinów polega na ciągłym obliczaniu funkcji SHA-256 z użyciem kolejnych ciągów dodatkowych znaków i porównywaniu jej z zadanym kryterium. Tę czynność będzie wykonywać Raspberry PI i w razie sukcesu, zgłaszać obliczony hash w odpowiednie miejsce, by inni użytkownicy bitcoinów uznali fakt przelewu prowizji i nowych bitcoinów na podane przez zgłaszającego konto, tj. by kolejne obliczenia transakcji odnosiły się do właśnie tego zatwierdzonego bloku.

Warto jeszcze wspomnieć o samym schemacie, decydującym o trudności znalezienia pasującego do założeń skrótu SHA-256. Trudność zmienia się co 2016 bloków, a każdy blok ma nie więcej niż 1 MB długości. Twórcy Bitcoina przyjęli,



Rysunek 1. Zmiana poziomu trudności zatwierdzania bloków. Wyraźnie widać wzrost trudności w okresie ostatnich kilku miesięcy



Fotografia 2. Układ ASIC BitMain BM1380

Fotografia 3. AntMiner U1, w którym użyto układ BM1380

że zatwierdzenie każdego bloku powinno trwać średnio 10 minut. Oznacza to, że w ciągu godziny powinno dać się zatwierdzić 6 bloków, w ciągu doby 144 bloki, a w ciągu tygodnia: 1008 bloków. 2016 to liczba bloków, jakie powinny być zatwierdzone w ciągu dokładnie dwóch tygodni. Ponieważ nie da się z góry przewidzieć, jak wiele osób zaangażuje się w zatwierdzanie transakcji, ani jak postęp technologiczny wpłynie na szybkość pracy komputerów realizujących to zadanie, trudność zmienia się na podstawie porównania czasu, który faktycznie potrzebny był na zatwierdzenie 2016 bloków z okresem 2 tygodni. Jeśli w praktyce obliczenia zajęły mniej czasu, trudność powinna wzrosnąć (a więc liczba od której obliczony skrót SHA-256 ma być mniejszy – spaść). Analogicznie – jeśli zatwierdzanie 2016 bloków trwało dłużej, trudność powinna zmaleć, a liczba porównywana ze skrótami SHA-256 – wzrosnąć.

Dzięki tym ograniczeniom da się w przybliżeniu ustalić tempo przyrostu liczby bitcoinów w obrocie, a więc i tempo wydobywania. Ponadto, jeśli okaże się, że liczba osób chętnych do zatwierdzania transakcji zmaleje, czas rozwiązywania zagadek wrośnie, a więc trudność w niedługim czasie zostanie obniżona, co znowu może zachęcić nowe osoby do zaangażowania się w kopanie.

Sprzętowo czy programowo?

Szybkość obliczania skrótów SHA-256 oczywiście zależy od dostępnej mocy obliczeniowej. Klasyczna, programowa realizacja tego algorytmu dla bloków wielkości ok 1 MB pozwala obliczać około 66 milionów skrótów na sekundę na procesorze Intel Core i7 3930K, a więc topowym CPU z przed kilku lat. Dla porównania, pierwsze Raspberry PI z układem BCM2835, a więc rdzeniem ARM1176JZF-S, taktowanym zegarem 800 MHz miało wydajność 0,2 MHash/s (czyli 330-krotnie mniejszą niż wspomniany wcześniej Core i7), zbliżoną do starszych modeli Intel Pentium III. Wzrost wydajności można uzyskać korzystając z jednostek GPU. Przykładowo karta graficzna AMD Radeon 7970 umożliwia obliczanie rzędu 700 MHash/s, w zależności od taktowania zegara. W jaki więc sposób małe Raspberry PI może konkurować z jakimikolwiek innymi systemami? Może w oparciu o układy ASIC.

Skuteczne wydobywanie bitcoinów jest równoznaczne z zarabianiem pieniędzy, co wykorzystali inwestorzy, finansując projektowanie specjalistycznego sprzętu. Obecnie wartość jednego bitcoina to około 420 USD, a nagrodą za znalezienie poprawnego skrótu każdego bloku jest 25 BTC. Do tego trzeba doliczyć prowizje za transakcje, które wynoszą średnio ok. 0,17 BTC na blok. Oznacza to, że każde pomyślne rozwiązanie zagadki jest nagradzane kwotą rzędu 10,5 tysiąca dolarów i dzieje się to z założenia, średnio raz na 10 minut. A więc statystycznie każdego dnia budżet na nagrody dla górników wynosi półtora miliona dolarów. Jest to kwota zdecydowanie godna powalczenia, ale by móc konkurować, konieczne jest zastosowanie znacznie bardziej wydajnych narzędzi niż karty graficzne.

Jednymi z takich urządzeń są specjalistyczne „koparki" AntMiner firmy Bitmain. Ich najnowsze wersje są zbudowane w oparciu o układy BM1385, również zaprojektowane przez inżynierów Bitmaina. BM1385 to układy ASIC czwartej generacji, wyprodukowane przez Taiwan Semiconductor Manufacturing Company (TSMC) w procesie 28 nm. BM1385 jest w pełni autorskim projektem, a więc dla zwiększenia wydajności nie zastosowano w nim gotowych, uniwersalnych bloków. Wymaga zasilania napięciem 0,66 V i ma wydajność 32,5 GHash/s, pobierając przy tym jedynie 7 W mocy. Porównując tę wartość ze wspomnianym Radeonem 7970, pokazuje się, że pojedynczy ASIC jest w stanie uzyskać 46-krotnie większą wydajność przy 30-krotnie mniejszym zużyciu energii.

Tabela 1. Harmonogram przyznawania nagród za poprawne obliczenie skrótu bloku z podziałem na ery, rozpoczynające się z określonymi numerami bloków. Dzięki malejącej nagrodzie nie ma możliwości emitowania nowych bitcoinów w nieskończoność

Okres (tzw. era)	Początkowy numer bloku	Nagroda za blok [BTC]	Suma nagród w danym okresie [BTC]	Procent z docelowej liczby bitcoinów wprowadzonych do obiegu
1	0	50	10500000	50,00%
2	210000	25	5250000	75,00%
3	420000	12,5	2625000	87,50%
4	630000	6,25	1312500	93,75%
5	840000	3,125	656250	96,88%
6	1050000	1,5625	328125	98,44%
7	1260000	0,78125	164062,5	99,22%
8	1470000	0,390625	82031,25	99,61%
9	1680000	0,1953125	41015,625	99,80%
10	1890000	0,09765625	20507,8125	99,90%
11	2100000	0,04882812	10253,9052	99,95%
12	2310000	0,02441406	5126,9526	99,98%
13	2520000	0,01220703	2563,4763	99,99%
14	2730000	0,00610351	1281,7371	99,99%
15	2940000	0,00305175	640,8675	100,00%
16	3150000	0,00152587	320,4327	100,00%
17	3360000	0,00076293	160,2153	100,00%
18	3570000	0,00038146	80,1066	100,00%
19	3780000	0,00019073	40,0533	100,00%
20	3990000	0,00009536	20,0256	100,00%
21	4200000	0,00004768	10,0128	100,00%
22	4410000	0,00002384	5,0064	100,00%
23	4620000	0,00001192	2,5032	100,00%
24	4830000	0,00000596	1,2516	100,00%
25	5040000	0,00000298	0,6258	100,00%
26	5250000	0,00000149	0,3129	100,00%
27	5460000	0,00000074	0,1554	100,00%
28	5670000	0,00000037	0,0777	100,00%
29	5880000	0,00000018	0,0378	100,00%
30	6090000	0,00000009	0,0189	100,00%
31	6300000	0,00000004	0,0084	100,00%
32	6510000	0,00000002	0,0042	100,00%
33	6720000	0,00000001	0,0021	100,00%
34	6930000	0	0	100,00%

Fotografia 4. AntMiner U3 – urządzenie nowszej generacji, ale wciąż korzystające z portu USB

W oparciu o układy serii BM138x firma Bitmain przygotowała wiele różnych modeli koparek, z czego trzy oferowane są w wersji z interfejsem USB: AntMiner U1, AntMiner U2+ i AntMiner U3. Wszystkie z nich można podłączyć do Raspberry PI, a wykorzystując dodatkowy HUB USB, jedno RPI może obsługiwać wiele takich koparek jednocześnie. Nie ma obaw o przepustowość interfejsu USB ani Ethernetu – fakt że rozmiar bloków do przetwarzania nie przekracza 1 MB sprawia, że wąskim gardłem jest tak czy inaczej liczenie skrótów algorytmem SHA-256.

Aktualnie spośród wymienionych, bezpośrednio od producenta można kupić jedynie AntMinera U3, opartego o starszą generację scalaka: układ BM1382. AntMiner U3 zawiera 4 takie układy i ma sumaryczną wydajność 63 GHash/s, przy czym wymaga zewnętrznego zasilania napięciem 12 V, pobierając przy tym ok 4,5 A prądu. AntMinery mają zintegrowane (najczęściej aktywne) systemy chłodzenia i są bardzo łatwe w użyciu oraz kompatybilne ze sobą – to samo oprogramowanie będzie poprawnie funkcjonować z poszczególnymi modelami. W przypadku omawianego projektu wykorzystano najstarszą wersję AntMinera – U1, wyposażonego w jeden układ BM1380. Jest to także ASIC (obudowa QFN56), standardowo zasilany napięciem 0,75 V, co przy taktowaniu zegarem 200 MHz pozwala mu na obliczanie z wydajnością 1,6 GHash/s. Zwiększenie napięcia do 1,1 V pozwala względnie stabilnie podnieść taktowanie do 350 MHz, co daje wydajność rzędu 2,8 GHash/s. W praktyce podobno, przy zapewnieniu odpowiedniego chłodzenia, da się go zmusić do pracy z taktowaniem 500 MHz, uzyskując 4 GHash/s. Taktownie ustawia się programowo, a regulacja napięcia wymaga podmiany rezystorów na płytce drukowanej AntMinera.

Tabela 2. Parametry konfiguracyjne włączające obsługę poszczególnych koparek w programie cgminer. Dostępność poszczególnych opcji może zależeć od wersji oprogramowania

Opcja	Obsługiwane urządzenia
--enable-ants1	AntMiner S1
--enable-ants2	AntMiner S2
--enable-avalon	Avalon
--enable-avalon2	Avalon2/3
--enable-avalon4	Avalon4/4.1/6
--enable-bab	BlackArrow Bitfury
--enable-bflsc	Układy ASIC firmy BFL
--enable-bitforce	Układy FPGA firmy BitForce
--enable-bitfury	Układy ASIC firmy BitFury
--enable-bitmain	Układy BitMain w trybie Multi Chain
--enable-bitmine_A1	Układy ASIC serii Bitmine.ch A1
--enable-blockerupter	ASICMINER BlockErupter Tube/Prisma
--enable-bmsc	Układy BitMain w trybie Single Chain
--enable-cointerra	Układy ASIC firmy Cointerra
--enable-drillbit	Układy ASIC Drillbit BitFury
--enable-hashfast	Hashfast
--enable-icarus	Icarus/Block Erupter
--enable-klondike	Klondike
--enable-knc	Koparki firmy KnC
--enable-minion	Układ Minion BlackArrow
--enable-modminer	Układy FPGA firmy ModMiner
--enable-sp10	Spondoolies SP10
--enable-sp30	Spondoolies SP30
--enable-libsystemd	Obsługa Watchdoga i powiadomień

Listing 1. Przykładowy plik konfiguracyjny programu cgminer

```
{
„pools” : [
    {
        „url” : „http://stratum.antpool.com:3333”,
        „user” : „Nazwa_uzytkownika”,
        „pass” : „Haslo”
    }
]
,
    „api-listen” : true,
    „api-port” : „4028”,
    „expiry” : „120”,
    „failover-only” : true,
    „log” : „5”,
    „no-pool-disable” : true,
    „queue” : „2”,
    „scan-time” : „60”,
    „worktime” : true,
    „shares” : „0”,
    „kernel-path” : „/usr/local/bin”,
    „api-allow” : „0/0”,
    „bmsc-options” : „115200:0.57”,
    „bmsc-freq „ : „0981”
}
```

Właściwy projekt

Po tym długim wstępie można zabrać się do wykonywania projektu. W podstawowej wersji jest on bardzo łatwy w realizacji.

Na Raspberry PI należy zainstalować system Raspbian, a następnie doinstalować potrzebne oprogramowanie. Dobrym wyborem będzie dosyć uniwersalny program **cgminer**, dostępny bezpłatnie z Internetu. Aktualnie najnowszą wersją jest 4.9. Wymaga on jednak zestawu bibliotek, dostępnych w ramach repozytorium Raspbiana. By je zainstalować należy w linii poleceń wpisać:

```
sudo apt-get update
sudo apt-get install build-
essential libusb-1.0-0-dev
libusb-1.0-0 libcurl4-openssl-
dev libncurses5-dev libudev-dev
```

Następnie można pobrać **cgminera** poleceniem:

```
wget http://ck.kolivas.org/apps/
cgminer/4.9/cgminer-4.9.0.tar.bz2
```

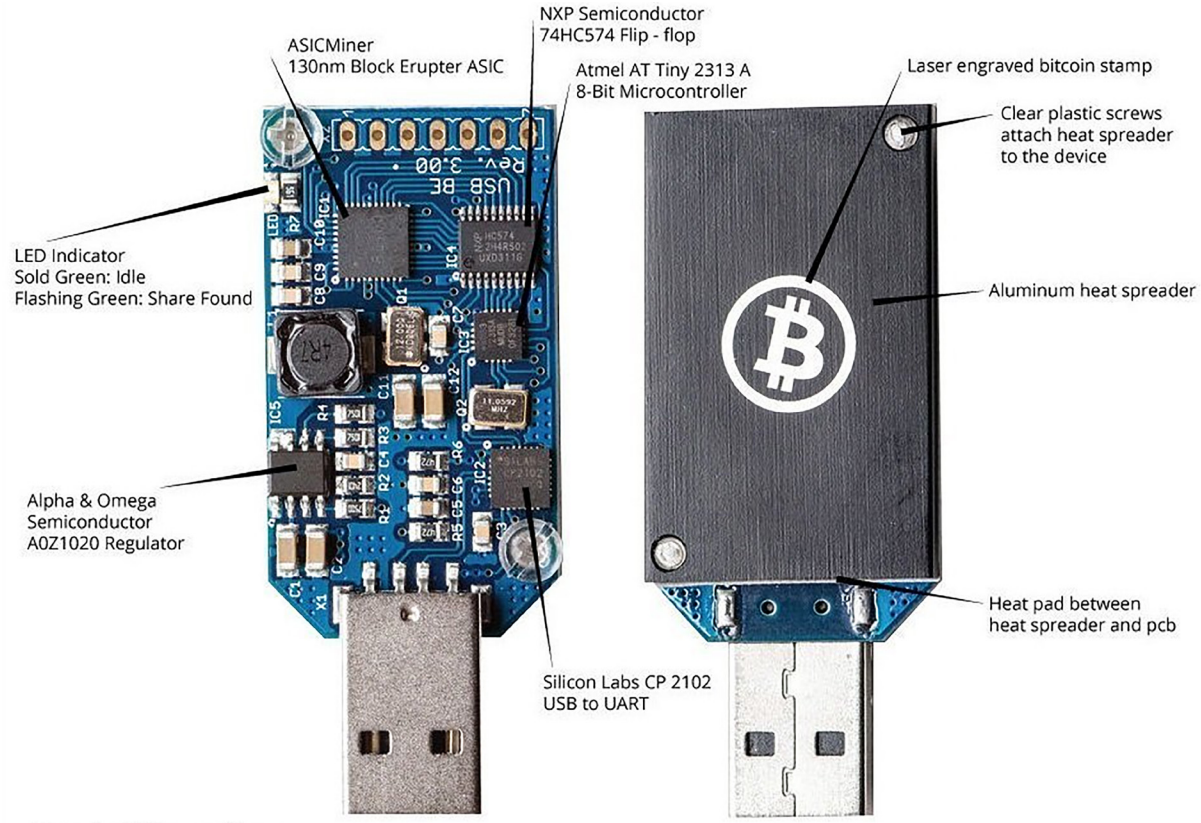
Program ten trzeba samodzielnie skompilować – do tego właśnie potrzebne były programy z repozytorium Raspbiana. Plik z programem należy rozpakować:

```
tar xvf cgminer-4.9.0.tar.bz2
```

po czym należy przejść do powstałego w ten sposób katalogu, dokonać konfiguracji zależnej od wybranego urządzenia kopiącego i całość skompilować oraz zainstalować. Służą do tego kolejno wydawane polecenia:

```
cd cgminer-4.9.0/
./configure --enable-bmsc
sudo make
sudo make install
```

Parametr **--enable-bmsc** włącza obsługę koparki AntMiner U1 oraz jej zaawansowanych ustawień. W przypadku innych



Fotografia 5. Budowa koparki USB, w której użyto układ Block Erupter

urządzeń kopiących należy zastosować odpowiednie inne opcje, zgodnie z **tabelą 2**.

Pozostaje podłączyć nabyte koparki USB do Raspberry PI – najlepiej z użyciem zasilanego z zewnątrz koncentratora i… zarejestrować się w grupie „górników”.

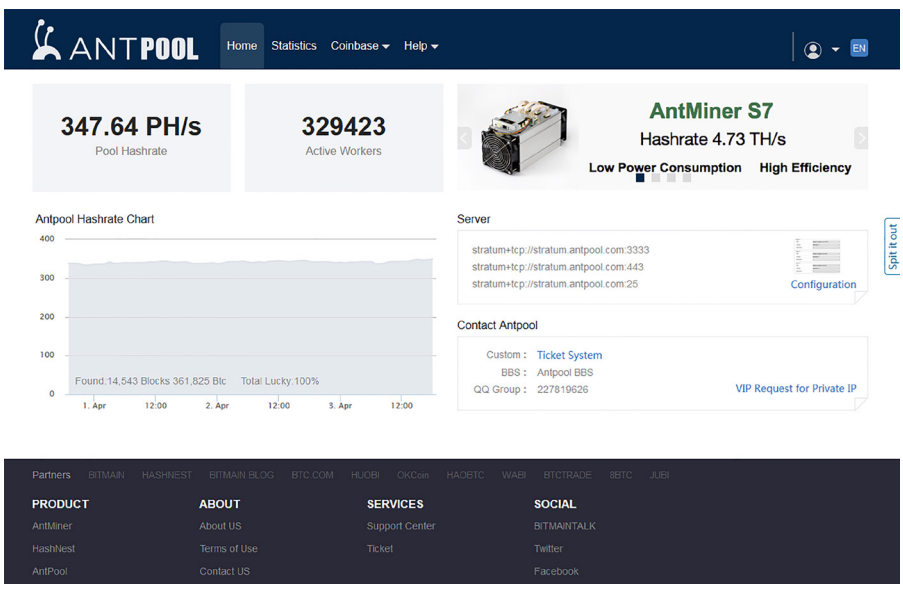
Grupy kopiące

Ostatnia z wymienionych czynności może wydawać się dziwna, ale wystarczy chwila obliczeń, by zdać sobie sprawę z jej zasadności. Kopanie bitcoinów to w pewnym sensie gra, gdyż w ogólności nie jest ważne, ile pracy włożyło się w znajdywanie skrótu przetwarzanego bloku transakcji, a jedynie kto pierwszy znalazł poprawny skrót. Tylko ta osoba wygrywa, a pozostali zaczynają od początku. Zwycięzca bierze wszystko, przy czym statystycznie na dobę przypada 144 zwycięzców (mogą się oni powtarzać). W praktyce oznacza to, że aby móc cokolwiek zarobić na kopaniu bitcoinów, konieczne jest posiadanie ogromnej mocy obliczeniowej, lub przynależność do społeczności, która wspólnie kopie, dzieląc się następnie wygranymi.

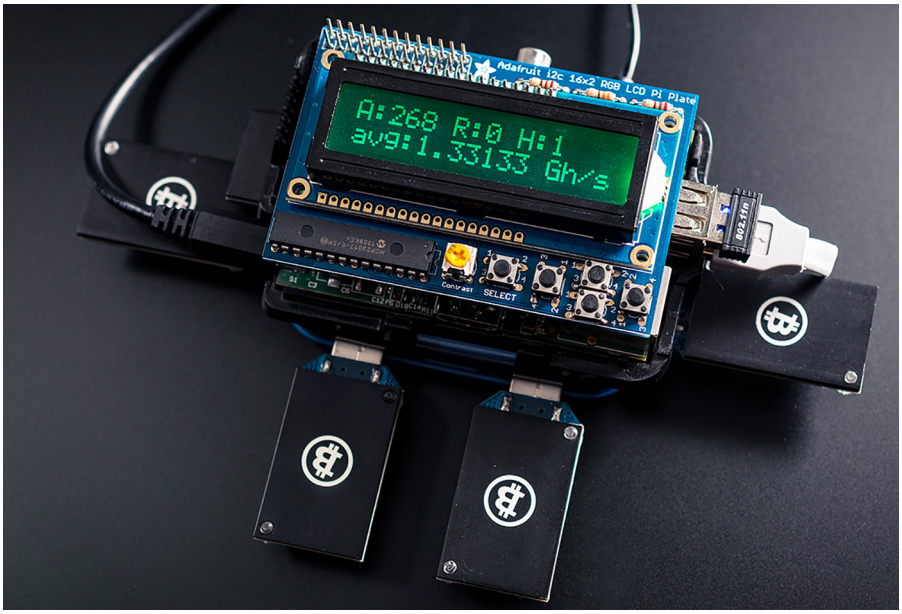
Jedną z takich społeczności jest grupa AntPool, która w trakcie powstawania tego artykułu wygrywała około 28% nagród za bloki, a więc około 40 razy dziennie. Liczba ta przekłada się na ponad 1000 bitcoinów nagród na dzień, a więc przychód przekraczający 420 tysięcy dolarów. Grupa AntPool została założona przez firmę Bitmain, a więc twórcę wspomnianych w artykule AntMinerów. Na rzecz AntPool pracuje około 330 tysięcy maszyn, które dzielą między sobą zadanie obliczania skrótów oraz dzielą się wygranymi. Podział zależny jest od wkładu mocy obliczeniowej użytkownika; łącznie w przypadku AntPool wynosi ona obecnie około 350 PHash/s, a grupa pomyślnie rozwiązała od początku swojej działalności ponad 14,5 tysiąca zagadek.

Tabela 3. Wartości parametru --bmsc-freq programu cgminer i odpowiadające im częstotliwości taktowania układu BM1380

Wartość parametru --bmsc-freq	Taktowanie [MHz]
0581	150
0681	175
4F02	193
0781	200
0881	225
0981	250
0A81	275
0B81	300
0C81	325
0D81	350
0E81	375
0F81	400
5081	425
5181	450
5281	475
5381	500



Rysunek 6. Strona internetowa grupy AntPool



Fotografia 7. Raspberry PI z modułami Block Erupter i wyświetlaczem LCD, przystosowane do kopania bitcoinów

Z mocami obliczeniowymi na poziomie 350 PHash/s trudno samodzielnie konkurować, a tego rzędu wydajność mają właśnie liderzy, którzy regularnie jako pierwsi odkrywają poprawne skróty bloków. Oprócz AntPool, do najsilniejszych grup należą BW Pool, BitFury, BTCChina i F2Pool. Pozostałe grupy znajdują poprawne rozwiązania tylko okazyjnie, dlatego warto dołączyć do jednej z popularnych grup. By to zrobić, w wielu przypadkach wystarczy zarejestrować się na stronie danej grupy. Zarejestrowany użytkownik otrzymuje namiary na serwer oraz swój login i hasło, potrzebne do uruchomienia **cgminera** w taki sposób, by uczestniczył w pracach grupy.

Wydobywanie

Mając już wszystkie potrzebne dane oraz sprzęt można przystąpić do prac. W tym celu należy uruchomić program **cgminer** z uprawnieniami roota, w następujący sposób:

```
sudo ./cgminer -o adres_grupy
-u nazwa_użytkownika -p hasło.
```

Oczywiście, podając w odpowiednich miejscach właściwy adres serwera grupy, nazwę użytkownika i hasło do konta w grupie. W przypadku AntMinerów można jeszcze określić m.in. taktowanie zegara układu (wartości parametru dla AntMinera U1 podano w **tabeli 3**). Przykładowo, podwyższenie taktowania do 250 MHz wymaga wywołania komendy z parametrem **--bmsc-freq 0981**.

Dla ułatwienia, zbiór ustawień (parametrów wywołania) można zapisać w pliku konfiguracyjnym, a następnie wywołać program **cgminer** z parametrem **--config adres_pliku_konfiguracyjnego**. Przykładowy plik pokazano na **listingu 1**.

Warto zwrócić uwagę na opcje **--api-listen**, **--api-port** i **--api-allow**, które pozwalają na pobieranie aktualnych danych z **cgminera** i np. prezentowanie ich z użyciem innych programów. Zostało to wykorzystane w dobry sposób w projekcie opracowanym przez Collina Cunninghama z firmy Adafruit, który w oparciu o cztery moduły Block Erupter wykorzystał Raspberry PI do kopania na rzecz grupy Slush Pool. Dodatkowo użył on alfanumerycznego wyświetlacza LCD 2×16, zintegrowanego z prostą klawiaturą, na którym prezentuje dane na temat pracy urządzenia. Informacje te są pobierane właśnie z API programu **cgminer**, za pomocą oddzielnego skryptu. Szczegółowy opis tego projektu można znaleźć pod adresem: *https://goo.gl/x6XDsc*.

Podsumowanie

Na koniec warto się zastanowić nad opłacalnością kopania bitcoinów. Sprawa nie jest łatwa, gdyż zależy od wielu czynników. Podstawowe znaczenie ma sam kurs BTC/PLN, który się mocno zmienia. Istotny jest też kurs USD/PLN, gdyż urządzenia do kopania bitcoinów są produkowane głównie w Azji i sprzedawane za dolary. To sprawia, że właściwie nie wiadomo, ile w rzeczywistości w przyszłości warte będą nagrody.

Drugim problemem jest silnie rosnąca w ostatnich miesiącach konkurencja. O ile już w połowie ubiegłego roku wiele osób twierdziło, że nie opłaca się zatwierdzać transakcji bictoinowych, to od tego czasu trudność wzrosła około 4-krotnie. Podobnie wzrosła też moc obliczeniowa grup zaangażowanych w wydobywanie. A to oznacza, że o ile przynależy się wciąż do dobrej grupy, wartość udziałów w zysku, przy zachowaniu tej samej koparki, spadła w ciągu tego okresu ok. 4-krotnie. Szczęśliwie spadły też ceny wprowadzanych na rynek modułów kopiących, a ich wydajność zdecydowanie wzrosła. Spadł też przelicznik kosztu energii względem wydajności. Ma to dosyć istotny wpływ, gdyż praca koparek non-stop powoduje względnie duże zużycie energii, mające istotny wpływ na opłacalność całego przedsięwzięcia. Są jednak głosy, że jeśli ktoś ma energię elektryczną „za darmo", to wykopywanie bitcoinów zawsze jest opłacalne – choć z punktu widzenia inwestora, czas zwrotu włożonego kapitału może wydawać się zbyt długi, by miało to sens.

W końcu całkiem blisko na horyzoncie pojawia się spadek nagrody. W trakcie pisania tego artykułu liczba istniejących bloków Bitcoin przekracza już 405 tysięcy, co oznacza, że za niecałe 15 tysięcy bloków nagroda zmaleje o połowę. Powinno to się zdarzyć w połowie lipca i biorąc pod uwagę wagę tej zmiany, trudno ocenić, jak zareagują zaangażowane w Bitcoina grupy. Może się zdarzyć tak, że wiele osób zrezygnuje z kopania, co z czasem spowoduje istotne zmniejszenie trudności. Innym skutkiem może być spowolnienie zatwierdzania transakcji, w efekcie czego użytkownicy Bitcoina zaczną oferować większe prowizje. Jednakże ażeby nadrobić 25 BTC różnicy pomiędzy aktualną a przyszłą nagrodą, musieliby statystycznie podnieść prowizje 130-krotnie, do poziomu ok. 0,02 BTC. Wynika to z faktu, że aktualnie średnio w jednym bloku gromadzone jest ok. 1200 transakcji, a średnia wartość prowizji na transakcję to poniżej 0,00015 BTC. Przy aktualnym kursie prowizja statystycznie utrzymuje się na poziomie ok. 6 centów, a musiałaby ok. 8 dolarów, jeśli kurs pozostałby stały, a przychody „górników" miałyby pozostać na dotychczasowym poziomie.

Być może dla czytelników EP lepszym interesem będzie jednak nie tyle samodzielne kopanie bitcoinów, czym przecież może zająć się ktokolwiek, ale wykorzystanie wiedzy zawodowej do samodzielnego zaprojektowania nowocześniejszych, bardziej wydajnych koparek.

Marcin Karbowniczek, EP