Uniwersytet Wrocławski

Matematyka na UWr - studia pełne możliwości

Bitcoin - analiza kryptowaluty

Ziemowit Rzeszotnik

Wrocław 2014

1 Wstęp

Co to jest bitcoin? Idea bitcoina opiera się na procesie tworzenia nowych bitcoinów na podstawie istniejących bitcoinów. W bardzo dużym uproszczeniu proces ten wygląda następująco. Wyobraźmy sobie, że istniejący bitcoin to pewien skończony ciąg znaków, na przykład

btc1

Aby na jego podstawie wytworzyć nowego bitcoina należy dopisać do tego istniejącego pewien losowy ciąg znaków, na przykład

btc1.blablabla

a nastepnie sprawdzić jaki jest wynik nałożenia na ten nowy ciąg ustalonej funkcji haszującej. Funkcja hashująca działa tak jak każda zwykła funkcja. Na przykład oryginalna funkcja haszująca SHA-1 nałożona na nasz ciąg btc1.blablabla daje wynik

37c26876f504a59e1ccef7a6ff91b414d2190b67

Nowy bitcoin powstaje wtedy, gdy tak otrzymany wynik zgadza się z pewnym wyznaczonym celem. Zazwyczaj ten cel to ustalona ilość zer na początku takiego wyniku. Na przykład ustalmy, że założony cel to przynajmniej jedno zero na początku wyniku. W tym wypadku btc1.blablabla nie jest nowym bitcoinem. A co jest? Na przykład to

btc1.20c1e0f09

albo to

btc1.16e96d912

W istocie, po nałożeniu funkcji haszującej SHA-1 na btc1.20c1e0f09 otrzymujemy wynik

0007cd7871741d9e327f0385713c6e11c2d407ce

natomiast ciąg btc1.16e96d912 daje równie dobry wynik

00009dfad8179a25398d05fee0385aacdcc43560

Po uzyskaniu nowych bitcoinów możemy ich użyć jako pożywkę do produkcji następnych bitcoinów. Na przykład ciąg btc1.16e96d912 może zostać przedłużony o kolejny losowy ciąg znaków dając

btc1.16e96d912.73a79e22

co spełnia nasz ustalony cel, bo po nałożeniu funkcji haszującej na btc1.16e96d912.73a79e22 otrzymujemy wynik

000ecc0de5ab3eee290be723a5ad408389fe88d0

i tak dalej.

2 Nomenklatura

W celu ułatwienia analizy bitcoina należy przedstawić odpowiednie nazewnictwo i przy okazji dostarczyć trochę głębszych wyjaśnień odnośnie tej kryptowaluty.

W dużym uproszczeniu możemy przyjąć, że cały proces kreacji bitcoinów rozpoczyna się od *bloku genesis*

btc1

Jest to początkowy *blok bitcoinów*, który jest wart 50 bitcoinów (w skrócie 50 btc). Te 50 btc może być przekazane innej osobie w ramach transakcji. Aby zatwierdzić tą transakcję, do bloku bitcoinów dodaje się dane nowego właściciela. Zakładając, że te dane to NW1 otrzymujemy

btc1:NW1

i dopiero teraz staramy sie znaleźć pewien losowy ciąg znaków, który chcemy dopisać do powyższego ciągu. Ten losowy ciąg znaków określa się mianem *nonce*. W naszym prostym przykładzie kolejnym blokiem bitcoinów, który realizuje *cel* jest

btc1:NW1.241821ebb

W istocie, po nałożeniu funkcji haszującej SHA-1 na powyższy ciąg otrzymujemy

000c54a78984097dfa4443ad95edf78855eeb7e5

Funkcja haszująca jest funkcją, która po nałożeniu na skończony ciąg znaków daje wynik będący innym ciągiem znaków. Ten wynik nosi nazwę *hasz*. Hasz w naszym przykładzie realizuje cel, jeśli zgodzimy się, że ten cel to przynajmniej dwa zera na początku hasza. Cel jednak może się zmieniać. Im więcej musimy uzyskać zer, tym większa staje się *trudność*. Poszukiwanie nonce tak aby hasz osiągał cel wymaga czasu oraz odpowiedniej mocy obliczeniowej. Osoba, która pierwsza zgłasza dobre rozwiązanie staje się właścicielem zgłoszonego bloku bitcoinów. Ilość bitcoinów przypisywana do nowych bloków zmniejsza się w czasie (średnio co 4 lata ilość ta zmniejsza się o połowę).

Załóżmy, że wskazany blok btc1:NW1.241821ebb został odkryty przez osobę G1 oraz, że jest to blok 50 bitcoinów. W naszym przykładzie mamy więc już dwóch właścicieli bitcoinów. NW1 ma 50 btc posiadając blok btc1 oraz G1 ma 50 btc posiadając blok btc1:NW1.241821ebb. Te bitcoiny mogą być przekazane dalej w ramach kolejnych transakcji. NW1 może przekazać swoje bitcoiny NW2, czyli poprosić o potwierdzenie ciągu

btc1:NW2

Osoba G2 może potwierdzić taki ciąg produkując nowy blok bitcoinów

btc1:NW2.1ece8d6f9

Podobnie G1 może przekazać swoje bitcoiny NW3, czyli poprosić o potwierdzenie ciągu

btc1:NW1.241821ebb:NW3

Osoba G3 może potwierdzić taki ciąg produkując nowy blok bitcoinów

btc1:NW1.241821ebb:NW3.89e698fade

itd.

3 Notatka

Bitcoin nie stanowi zagrożenia dla standardowego systemu walutowego. Wynika to ze struktury tej kryptowaluty. Struktura ta opiera się na zastąpieniu banku centralnego użytkownikami, którzy produkują tą kryptowalutę we własnym zakresie. Transakcje dokonywane bitcoinami zostają przeprowadzone tylko wtedy, gdy uzyskają potwierdzenie wynikające z procesu produkcji nowych bitcoinów. Proces ten polega na poszukiwaniu kolejnych bloków bitcoinów. Produkcja nowych bloków bitcoinów jest więc warunkiem koniecznym do przeprowadzania transakcji w tej kryptowalucie.

Przyczyny dla których bitcoin nie może konkurować z tradycyjnymi walutami są następujące:

A. Wspomniana konieczność produkcji nowych bloków bitcoinów do przeprowadzania transakcji istniejącymi bitcoinami.

B. Ograniczenia sprzętowe dla produkcji bitcoinów.

C. Koszty energii elektrycznej ponoszonej przy produkcji bitcoinów.

D. Zmniejszanie nagrody producentów bitcoinów o połowę w terminach określonych przez twórców bitcoina (średnio co 4 lata).

E. Zbyt duża wrażliwość bitcoina na spadek jego wartości wobec walut standardowych.

F. Konieczność ciągłej popularyzacji bitcoina w celu utrzymania jego wartości.

G. Niskie parametry rynkowe bitcoina.

H. Zbyt duża awaryjność występująca w środowisku bitcoina.

I. Brak organów gwarantujących pokrywalność tej kryptowaluty.

Podstawową przyczyną, dla której bitcoin ma minimalne szanse, by awansować do miana waluty, jest jednak brak możliwości prowadzenia polityki monetarnej w stosunku do tej kryptowaluty. Strukturalne problemy bitcoina wskazane powyżej świadczą o tym, że grozi mu seria szoków, na które nie będzie mógł odpowiednio reagować. Standardowe waluty są ręcznie sterowane, co pozwala na utrzymywanie ich względnej stabilności w różnych sytuacjach rynkowych. Założenia monetarne bitcoina zostały zaplanowane z góry kilka lat temu i wbudowane w kod źródłowy tej kryptowaluty. Jej jedyną możliwością reakcji na szoki rynkowe jest zwiększenie awaryjności systemu (znikające bitcoiny), lub zwiększone wysiłki w celu popularyzacji tego niedoskonałego tworu. Poważna zmiana kodu bitcoina jest ostatecznością, która zniszczy czar zagwarantowany przez jej twórców.

Należy jednak zaznaczyć, że bitcoin otwiera pierwszą generację kryptowalut. Następne rozwiązania w tej dziedzinie już się pojawiają. Nie można więc wykluczyć, że mimo swych początkowych problemów kryptowaluty zostaną z nami na dłużej. Ponadto model biznesowy wielu kryptowalut jest silny o tyle, że opiera się na anonimowości użytkowników umożliwiającej nabywanie nielegalnych towarów i usług hazardowych. W ostatecznym rozrachunku kolejne generacje kryptowalut mogą więc doprowadzić do konieczności wypuszczenia własnej kryptowaluty przez jeden z uznanych banków centralnych. Na razie jednak, nie widać takiej wyraźnej potrzeby.

4 Uzasadnienie

4.1 A. Konieczność produkcji

Bitcoin od początku oparł się na ideologii kontry wobec działalności banków centralnych. Sam fakt stworzenia takiej moralnej podbudowy dla tej kryptowaluty może napawać niepokojem. i to wcale nie dlatego, że banki centralne powinny być pod ochroną. Po prostu dobry produkt nie potrzebuje ideologii. Jego funkcjonalność i niezawodność powinny być głównymi atutami, a wyparcie konkurencji, jedynie efektem ubocznym realizacji tych atutów.

Jednym z podstawowych założeń bitcoina odróżniającym go od walut standardowych jest oganiczenie ilości bitcoinów, które można wyprodukować. Aby zrozumieć ten schemat musimy wrócić do uprzednio przedstawionych pojęć. Produkcja bitcoinów odbywa się blokowo. Każdy producent chce jako pierwszy znaleźć nowy blok bitcoinów, aby stać się właścicielem wyprodukowanych w ten sposób bitcoinów. Ilość bitcoinów przypisywana do nowych bloków zmienia się w czasie. Każdy z pierwszych 210 000 bloków ma przypisaną wartość 50 bitcoinów. Każdy z kolejnych 210 000 bloków ma przypisaną wartość 25 bitcoinów (czyli mniejszą o połowę). Każdy z następnych 210 000 bloków ma przypisaną wartość 12,5 bitcoinów itd. Możemy więc łatwo obliczyć całkowitą ilość bitcoinów możliwą do uzyskania w tym schemacie

$$210\,000 \cdot 50 + 210\,000 \cdot 25 + 210\,000 \cdot 12,5 \cdots =$$

$$210\,000 \cdot \sum_{n=0}^{\infty} 50 \cdot \left(\frac{1}{2}\right)^n = 210\,000 \cdot 100 = 21\,000\,000$$

W sumie można więc wyprodukować 21 milionów bitcoinów. A w skończonym czasie – trochę mniej. Dla wygody możemy myśleć, że każdy blok bitcoinów jest swoistego rodzaju banknotem. Wówczas proces produkcji bitcoinów może być porównany do drukowania serii banknotów o określonych nominałach. Najpierw drukowane są banknoty o nominale 50 btc (o numerach seryjnych od 1 do 210 000)[1], potem drukowane są banknoty o nominale 25 btc (o numerach seryjnych od 210 001 do 420 000), nastepnie drukowane sa banknoty o nominale 12,5 btc itd. Proces ten nigdy się nie kończy i po pewnym czasie drukowane są banknoty o nominale prawie zerowym.

Konieczność produkcji nowych bloków bitcoinów (nawet tych o prawie zerowej wartości nominalnej) wynika z tego, w jaki sposób procesowane są transakcje dokonywane bitcoinami. Prośby o przeprowadzenie transakcji zgłaszane są do systemu. Producenci bitcoinów wybierają kilka z tych próśb i na ich podstawie próbują wygenerować nowy blok bitcoinów, który potwierdzi te transakcje. Czas potrzebny na wygenerowanie nowego bloku bitcoinów jest tak ustalony, że wynosi średnio 10 minut. Aby transakcja została uznana za pewną potrzeba sześciu takich potwierdzeń. Do całkowitego przeprowadzenia transakcji potrzeba więc około godziny. Niestety, ten czas może zostać przekroczony i to znacznie. Na przykład w przypadku, gdy ilość procesowanych transakcji jest duża. Wówczas bowiem maleją szanse na to, że dana transakcja zostanie wybrana do potwierdzenia w procesie produkcji bitcoinów. Nie jest to jednak bieżące zmartwienie bitcoina. System tej kryptowaluty jest w stanie procesować 7 transakcji na sekundę (średnio). To ograniczenie wynika z tego, że każda transakcja jest plikiem tekstowym, który ma pewien rozmiar wyrażony w bajtach. Ten rozmiar ogranicza ilość transakcji, które można potwierdzić nowym blokiem bitcoinów. Obecnie jest to około 4200 transakcji (stan na połowę 2014 r.). Tak więc średnio co 10 minut 4200 transakcji może uzyskać potwierdzenie. Jednak w rzeczywistości średnio zaledwie 400 transakcji uzyskuje swoje potwierdzenie co 10 minut. Obecnie ilość dziennych transakcji wynosi około 60 tys.

[1] Albo od 0 do 209 999, tak jak to się dzieje z bitcoinem.

Widać więc, że daje to 416 transakcji na 10 minut i system nie powinien mieć żadnych problemów z ich potwierdzeniem. Tak jednak nie jest. Wynika to z tego, że producenci bitcoinów mają dużo swobody przy wyborze transakcji do potwierdzenia. Zamiast pobierać pewną ustaloną ilość transakcji według kolejności ich zgłaszania producenci mogą wybrać w zasadzie to co chcą, np. jedną transakcję i to w dodatku tylko swoją. Ten schemat ma na celu zmuszenie pozostałych użytkowników tej kryptowaluty do wnoszenia specjalnych opłat transakcyjnych. Jeśli dany użytkownik chce uzyskać pewność, że jego transakcja zostanie wybrana do potwierdzenia, to musi wnieść opłatę wyrażona w bitcoinach na tyle wysoką, aby była atrakcyjna dla producentów bitcoinów. Opłata ta nie jest częścią kodu źródłowego bitcoina, tylko umowną daniną, która może się zmieniać w czasie. Im wyższa danina, tym lepsza gwarancja, że będzie ona atrakcyjna dla producenta bitcoinów. Obecnie zalecane są opłaty rzędu 0,0005 btc.[2]

Warto zaznaczyć, że w celu przeprowadzenia transakcji wystarczy, że zostanie ona potwierdzona tylko przez jeden nowy blok bitcoinów. Kolejne pięć wymaganych potwierdzeń polega jedynie na odczekaniu, aż za pierwszym blokiem potwierdzającym daną transakcję pojawi się pięć nowych bloków potwierdzających inne transakcje. Stres związany z wciśnięciem danej transakcji do procesu produkcji bitcoinów jest więc jednorazowy.

O wiele większy stres dotyka jednak producentów bitcoinów. Odkrywca nowego bloku bitcoinów musi czekać na 100 (a nawet 120) nowych bloków zanim może puścić wyprodukowane bitcoiny w obieg. Jeśli więc producent wytworzy nowy blok bitcoinów o wartości nominalnej 25 btc, to musi czekać około 20 godzin zanim te 25 btc będzie do jego dyspozycji. Ten fakt jeszcze bardziej uświadamia producentom tej kryptowaluty konieczność ciągłej produkcji nowych bloków bitcoinów.

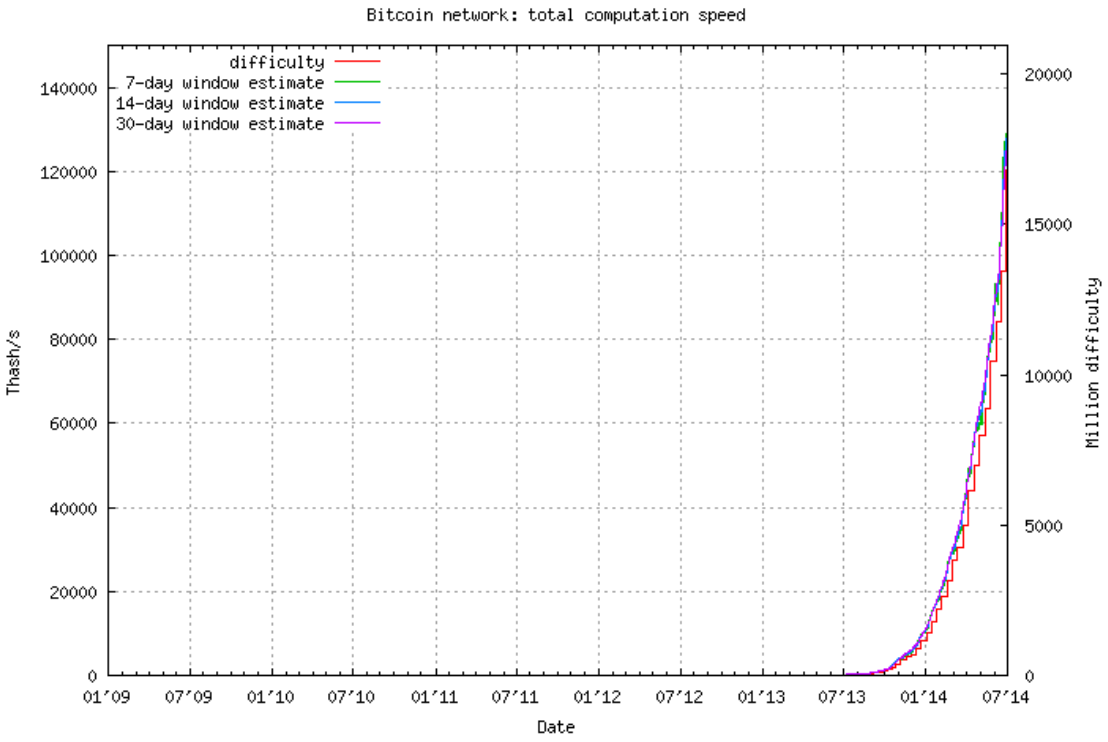
Według twórców bitcoina ta presja na ciągłą produkcję oraz stopniowe zmniejszanie ilości bitcoinów przypisywanej nowym blokom doprowadzi jedynie do tego, że po pewnym czasie producenci nowych bloków będą się zaspokajać tylko opłatami transakcyjnymi. Z perspektywy użytkownika nie będącego producentem oznacza to ryzyko rosnących opłat transakcyjnych oraz *de facto* prawie całkowite uzależnienie od producentów tej kryptowaluty. Pod tym względem użytkownicy bitcoinów znajdują się w o wiele gorszej sytuacji niż użytkownicy walut standardowych oraz osoby inwestujące w środki trwałe.

4.2 B. Ograniczenia sprzętowe

Pierszy blok bitcoinów pojawił się w styczniu 2009 r. W początkowym okresie nowe bloki bitcoinów w istocie mogły być wytwarzane przez zwykłe domowe komputery w ich wolnym czasie zgodnie z sugestiami twórców tej kryptowaluty. Wraz z upływem czasu produkcja bitcoinów zaczęła wymagać specjalistycznego sprzętu trudniącego się jak najszybszym nakładaniem funkcji haszującej. Użytkownicy tego sprzętu posługują się wskaźnikiem tej szybkości wyrażonej w ilości uzyskiwanych haszów na sekundę. Wskaźnik ten jest o tyle istotny, że można go zastosować zbiorczo wobec wszystkich producentów bitcoinów. W ten sposób uzyskuje się informację odnośnie szybkości z jaką cała sieć generująca bitcoiny wykonuje konieczne obliczenia (czyli nakłada funkcję haszującą dostając wynik zwany haszem). Obecnie szybkość ta wynosi około 120 PetaHash/s. Oznacza to, że cała sieć bitcoinów oblicza $120 \cdot 10^{15}$ haszów na sekundę. Rok temu wskaźnik ten wynosił jedynie około 130 MegaHash/s, czyli prawie tysiąc razy mniej[3] (patrz Rys.1).

[2] Głębszym powodem dla ograniczenia ilości potwierdzanych transakcji oraz wprowadzenia opłat transakcyjnych jest próba sprowadzenia rozmiaru nowych bloków bitcoinów do jak najmniejszej ilości bajtów.

[3] Dane na ten temat sa dostępne na stronie blockchain.info/en/charts/hash-rate.



Rys.1 Wzrost szybkości obliczeń wykonywanych przez sieć generującą bitcoiny.[4]

Warto zaznaczyć, że eksponencjalny wzrost szybkości obliczeń wykonywanych przy generacji bitcoinów nie wynika z tego, że wraz z upływem czasu obrabianie rosnącej ilości danych wymaga więcej mocy obliczeniowej. Ten eksponencjalny wzrost wynika tylko i wyłącznie z rosnącej ilości osób chętnych do tego, aby produkować bitcoiny.

Nabywcy specjalistycznego sprzętu do produkcji bitcoinów zazwyczaj łączą swoje siły tworząc konglomeraty produkcyjne. W tych konglomeratach zyski z produkcji bitcoinów są dzielone w zależności od mocy obliczeniowej sprzętu włączanego przez danego członka do konglomeratu.

W chwili obecnej produkcja bitcoinów przestaje być opłacalna dla osób, które pragną zainwestować w specjalistyczny sprzęt do produkcji bitcoinów. Stan na połowę 2014 r. wskazuje, że inwestycja tego typu wymaga kilku tysięcy USD[5] i po roku generuje stratę tego samego rzędu.[6]

Rynek produkcji bitcoinów jest bardzo rozwinięty, co wskazuje na to, że idea produkowania "własnych pieniędzy" jest jedną z głównych atrakcji bitcoina. Na tym rynku obecne są firmy dostarczające lub udostępniające sprzęt do produkcji bitcoinów oraz osoby płacące za te usługi. Płatności przyjmowane są zarówno w bitcoinach jak i w zwykłych walutach, ale ceny są wyrażane w uznanych walutach standardowych. Dane płynące z rynku świadczą o tym, że wiele już zrealizowanych usług na dostarczenie sprzętu do produkcji bitcoinów zostało zawartych w czasie gdy cena bitcoina w USD była wyższa niż obecnie. Część z tych usług

[4] Źródło: bitcoin.sipa.be.

[5] USD to dolar amerykański.

[6] Strona tradeblock.com/mining dostarcza danych na temat sprzętu do produkcji bitcoinów wraz z kalkulatorem pozwalającym ocenić zyskowność z inwestycji w dany sprzęt. Podobne dane można znaleźć na stronie bitcoinwisdom.com/bitcoin/calculator.

zostało zrealizowanych z opóźnieniem, lub wcale, co spowodowało zbiorowe pozwy sądowe w stosunku do niektórych producentów tego sprzętu.

Powyższe dane wskazują na to, że w chwili obecnej rynek producentów bitcoinów został nasycony (a nawet przesycony). Aby zdać sobie sprawę z rozmiaru strat osób, które dopiero niedawno zainwestowały w produkcję bitcoinów należy przeanalizować jeszcze jeden wskaźnik.

Wraz z malejącymi zyskami producentów bitcoinów wynikającymi z podziału tego zysku na coraz więcej osób stworzono możliwość inwestycji w usługi produkcyjne bez konieczności inwestycji w sprzęt. Inwestor zakupuje jedynie udziały w procesie produkcji bitcoinów wykonywanym przez producenta sprzedającego te udziały. Udziały te są wyrażone we wpomnianych jednostkach. Jeden udział to 1 GigaHash/s (w skrócie: 1 GH/s). Inwestor kupuje więc moc obliczeniową wyrażoną w gigahaszach na sekundę. Wskaźnik, który obrazuje straty lub zyski takich inwestorów, to cena jednego udziału wyrażona w bitcoinach (lub przeliczona na USD). Rynek tych usług otworzył się pod koniec października 2013. Na początku listopada 1 GH/s kosztował 0,1 btc (jedną dziesiątą bitcoina). Od tej pory cena stopniowo spadała i na początku maja 2014 ustabilizowała się na poziomie 0,007 btc dając stratę rzędu 93%. Podobne zachowanie odnotowała cena tej mocy obliczeniowej wyrażona w dolarze. Na przełomie listopada i grudnia 2013 cena 1 GH/s wynosiła około 70 USD, a na początku maja br. spadła do 3 USD odnosząc stratę rzędu 96%. Od tego momentu cena ta podniosła się na poziom 4 USD.

Tego typu katastrofa nie powinna dziwić. Gdyby produkcja bitcoinów w istocie przynosiła krociowe zyski, to producenci sprzętu do generowania bitcoinów sami by go używali do produkcji kryptowaluty, a nie wystawiali na sprzedaż. Warto też przypomnieć, że tego typu wymagania sprzętowe nie są wcale konieczne. Sieć bitcoin w obecnym stanie ciągle mogłaby funkcjonowac w oparciu o laptopy i smartfony. Schemat działania bitcoina jednak na to nie pozwala. Wraz ze wzrostem chętnych do produkcji bitcoinów wzrasta moc obliczeniowa sieci. Im większa moc, tym szybciej rodzą się nowe bloki bitcoinów. W tym momencie kod źródłowy bitcoina zwiększa trudność produkcji nowych bloków, tak aby średnio były generowane co dziesięć minut. Im większa trudność, tym więcej mocy obliczeniowej potrzeba na to by wygrać wyścig o nowy blok bitcoinów. Widać więc do czego doprowadził ten schemat. Oczywiście nie jest to krach oznaczający koniec bitcoina. Jest to jednak mała lekcja ekonomii:

Dogmat. *W warunkach wolnej konkurencji i wolnego handlu zyski z produkcji towarów nasycających popyt dążą do zera.*

Wolny rynek sprawia, że wraz z nasyceniem popytu cena równowagi między podażą i popytem ustala się na poziomie nieznacznie wyższym niż koszty. Dotyczy to nie tylko cen towarów, ale również cen usług, o ile usługi te są w stanie nasycić popyt. Ta lekcja nie oznacza, że wraz z postępem wolnego rynku będziemy pracować prawie za darmo, a wszystko będzie kosztować tyle co nic. Wynika to z tego, że niektóre kluczowe produkty (np. żywność, węgiel, ropa, gaz, cement) są szybko zużywalne i nasycenie popytu wymaga ich ciągłego odtwarzania dając nadzieję na pojawienie się inflacji cen. Podobnie jest z usługami komunalnymi, remontowymi czy naprawczymi. Powyższy dogmat pozwala jednak zrozumieć naturalną presję deflacyjną, bezrobocie, coraz mniej trwałe produkty, kartele cenowe, dotacje rolnicze, wspieranie przemysłu samochodowego, ciągłą pogoń za nowymi technologiami, wojny patentowe oraz krach na rynku produkcji zarówno paneli słonecznych jak i bitcoina.

Warto podkreślić, że w tym momencie nie ma już odwrotu od balansowania opłacalności dalszej produkcji bitcoinów na poziomie zero. Utrzymanie ceny bitcoina w stosunku do walut standardowych na stałym poziomie lub ich spadek oznaczać będzie straty na tej produkcji. Wzrost ceny bitcoina spowoduje zaś napływ nowych chętnych do produkcji gwarantując ciągłą marginalizację zysków z dalszej produkcji bitcoinów.

Prawdziwe niebezpieczeństwo leży jednak w rejonie, który nie jest dostępny do przeanalizowania. Ze względu na anonimowość każdego użytkownika bitcoina, który ukrywa swoją tożsamość pod wieloma adresami, nie jest możliwe, aby ocenić jak duża ilość bitcoinów znajduje się w rękach ich producentów (oraz w rękach producentów sprzętu do generacji bitcoinów). Jeśli ta ilość jest duża w porównaniu z ilością utrzymywaną przez pozostałych użytkowników bitcoina, to krach na rynku produkcji rodzi ryzyko krachu ceny bitcoina w stosunku do walut standardowych. Jeśli w istocie producenci bitcoinów sami zatrzymują wyprodukowaną kryptowalutę, to rachunek zysków i strat z procesu produkcji zaczyna się opierać tylko na ich przeszłej produkcji, ze względu na to, że jak wiemy, dalsza produkcja jest już nieopłacalna. Aby więc nie ponieść strat na całym procesie produkcji, producenci bitcoinów w końcu będą musieli upłynnić wygenerowany produkt. Oczywiście nawet w tym scenariuszu pojawia się problem decyzyjny, nie jest bowiem jasne w którym momencie dokonać takiego upłynnienia. Cena bitcoina może przecież jeszcze wzrosnąć.

Największą niewiadomą staje się zatem ilosc bitcoinów utrzymywana przez producentów sprzętu do generacji bitcoinów, którzy przyjmują płatności za ten sprzęt w bitcoinach. Produkcja wirtualnych bitcoinów generuje realne koszty ze względu na zużycie energii elektrycznej potrzebnej do zasilenia i chłodzenia sprzętu.[7] Koszty chłodzenia zależą od temperatury panujacej na zewnątrz otoczenia w którym umieszczany jest sprzęt i trudno je ocenić. Koszty zasilenia zależą od cen energii elektrycznej obowiązujących w terenie, gdzie podłączany jest sprzęt.[8] Ograniczenia sprzętowe polegają na tym, że producenci sprzętu do generacji bitcoinów obecnie nie są w stanie zejść poniżej pewnej granicy zużycia energii elektrycznej. Ta granica to pół wata potrzebne na uzyskanie mocy obliczeniowej w wysokości 1 GH/s. Zamówiony wcześniej sprzęt do generacji bitcoinów jest ciągle dostarczany odbiorcom. Nieopłacalność dalszej produkcji bitcoinów z dużym prawdopodobieństwem może jednak doprowadzić do spadku dalszych zamówień na sprzęt. Kłopoty producentów tego sprzętu (np. CoinTerra, Butterfly Labs, HashFast) mogą zaś skutkować koniecznością upłynnienia posiadanych przez nich bitcoinów.

4.3 C. Koszty energii

Konieczność produkcji oraz ograniczenia sprzętowe stawiają bitcoina przed zadaniem, aby wykazać, że nie jest pułapką inwestycyjną na producentów tej kryptowaluty. Dojście bitcoina do bariery opłacalności jego dalszej produkcji nie jest czymś nieoczekiwanym. W listopadzie 2013 roku na forum bitcointalk.org pojawiło się ostrzeżenie użytkownika AJJ wraz z wyliczeniami wskazującymi na to, że inwestycja w moc obliczeniową do produkcji bitcoinów przyniesie straty. To ostrzeżenie nie trafiło do wszystkich i w rezultacie po pół roku straty w tą inwestycję przekroczyły 90%. W podobnym tonie i czasie, choć zupełnie niezależnie, wypowiada się użytkownik swansontec na portalu forums.butterflylabs.com/bitcoin-discussion/. Jego wyliczenia wskazują na to, że przy stabilnej cenie bitcoina w stosunku do walut standardowych moc obliczeniowa sieci generującej bitcoiny jest ograniczona. Stosując bieżące dane[9] tok tego rozumowania jest następujący.

Zgodnie z kodem źródłowym nowe bloki bitcoinów są generowane średnio co 10 minut. Dziennie daje to 144 bloki. Obecna ilość bitcoinów przypisywana do nowego bloku wynosi 25 btc. Załóżmy scenariusz pewnej stabilnej ceny bitcoina wobec dolara. Na przykład 650 USD

[7] Do tego należy jeszcze dodać koszty podłączenia sprzętu do sieci internetowej.

[8] W kwietniu br. odnotowano pierwszy w Holandii przypadek kradzieży prądu w celu produkcji bitcoinów. Bardzo ciekawy artykuł *Bitcoins: Made in China* Tima Swansona z maja br. (dostępny na stronie ofnumbers.com) sugeruje, że tego typu akty darmowej produkcji bitcoinów zachodzą w Chinach na dużą skalę dzięki odpowiednim koneksjom.

[9] blockchain.info

za 1 btc. To daje łączne dzienne dochody producentów bitcoinów na poziomie 2 340 000 USD. Biorąc pod uwagę dochody producentów pochodzące z opłat transakcyjnych możemy to zaokrąglić do 2,4 miliona USD. Dane dotyczące dziennych dochodów z produkcji bitcoinów dostępne są również na stronie blockchain.info/en/charts/miners-revenue. Wskazują one, że w przeciągu ostatnich 5 miesięcy dochody te w istocie oscylują wokół 2,4 mil. USD. Na godzinę daje to 100 tys. USD.

Wiedząc, że godzinne dochody wszystkich producentów bitcoinów wynoszą 100 tys. USD musimy zbadać ile energii elektrycznej można nabyć za tą kwotę. Przyjmując, że 1 kWh (jedna kilowatogodzina) kosztuje 0,15 USD dostajemy 100 000/0,15 = 666 666,666... watów, czyli 667 megawatów.

Teraz wreszcie możemy oszacować maksymalną moc obliczeniową sieci generującej bitcoiny. Umowną jednostką tej mocy jest 1 GH/s (jeden GigaHash na sekundę). Sprzęt do generowania bitcoinów musi mieć pewną dolną granicę zużycia energii elektrycznej. Obecnie wynosi ona 0,5 wata dla uzyskania mocy obliczeniowej w wysokości 1 GH/s. Dzieląc 667 megawatów przez 0,5 watów na GH/s otrzymujemy 1 334 MegaGigaHash/s, czyli 1 334 miliony GH/s lub w skrócie 1 334 PetaHash/s, co daje około 1,3 ExaHash/s.

Do niedawna sieć generująca bitcoiny posługiwała się mocą 0,13 ExaHash/s, czyli dziesięciokrotnie mniejszą od wskazanej powyżej granicy. Obecnie moc ta stara się ustabilizować na poziomie 0,11 ExaHash/s, ale nie jest jasne, czy ta stabilizacja będzie trwała. Ponownie dane do tej niewiadomej znajdują sie w rękach producentów sprzętu do generacji bitcoinów. Łączna moc obliczeniowa sprzętu uruchamianego i produkowanego oraz przewidywany czas funkcjonowania sprzętu uruchomionego to zmienne, które zadecydują o dalszym losie mocy obliczeniowej sieci generującej bitcoiny oraz o przyszłej cenie 1 GH/s.

4.4 D. Zmniejszanie nagrody

Od początku 2009 r. do końca 2012 r. wyprodukowano 10,5 miliona bitcoinów, czyli dokładnie połowę wszystkich bitcoinów możliwych do wygenerowania. Wszystkie bloki bitcoinów wygenerowane w tej pierwszej serii miały przypisaną wartość 50 bitcoinów (50 btc). Wraz z wyprodukowaniem bloku o numerze 210 000, co nastąpiło 28 listopada 2012 r., rozpoczęto produkcję drugiej serii bloków, w której wartość przypisywana nowym blokom zmniejszyła się o połowę. Użytkownicy bitcoina uczcili ten moment zastanawiajac się, jak zmniejszenie nagrody dla producentów bitcoinów wpłynie na cenę tej kryptowaluty. Cena ta nie zmieniła się znacznie oscylując w granicach 13 USD do końca 2012 roku. Później jednak nastąpił 10-krotny wzrost tej ceny, który utrzymał się do października 2013 r. Do końca 2013 roku cena wzrosła jeszcze 5-krotnie i przez pierwszą połowę br. utrzymała się na poziomie 650 USD.

Obecnie każdy nowy blok bitcoinów ma przypisaną wartość 25 btc. Zmniejszanie ilości bitcoinów przypisywanych do każdego nowego bloku następuje mniej więcej co cztery lata. Kolejne zmniejszenie tej nagrody powinno nastąpić w 2016 roku. Wówczas skończy się generowanie drugiej serii bloków i rozpocznie generowanie trzeciej serii, w której każdy nowy blok będzie miał wartość 12,5 btc. Ze względu na obecne trudności na rynku produkcji bitcoinów można się zastanowić, co takie zmniejszenie nagrody będzie oznaczać dla tego rynku.

Po pierwsze warto ocenić, kiedy to zmniejszenie nastąpi. Według portalu bitcoinclock.com obecne estymacje wskazują na połowę sierpnia 2016 r. Rozmija się to trochę z początkowymi przewidywaniami zawartymi na stronie en.bitcoin.it/wiki/Controlled_supply, gdzie datę tego wydarzenia oszacowano na koniec 2016 r. W istocie, od 28 listopada 2012 r. do końca

pierwszej połowy 2014 r. wygenerowano prawie 2,5 miliona nowych bitcoinów. Ponieważ tempo tej produkcji jest stałe, możemy oszacować, że połowa wszyskich bitcoinów dostępnych w bieżącej drugiej serii zostanie wygenerowana do połowy sierpnia 2014 r.[10] Oznacza to, że pierwsza połowa bieżącej serii bloków zostanie wyprodukowana w przeciągu 20,5 miesięcy (od końca listopada 2012 do połowy sierpnia 2014). Przy utrzymaniu dotychczasowego tempa produkcji nowych bloków koniec bieżącej serii powinien więc nastapić po upływie kolejnych 20,5 miesięcy, czyli około pierwszego maja 2016 r.

Tempo generowania bitcoinów produkowanych w bieżącej serii bloków jest prawie stałe (patrz blockchain.info/en/charts/total-bitcoins) i wynosi około 128,9 tys. btc na miesiąc, czyli około 4240 btc dziennie (zakładając, że miesiąc ma średnio 365/12 = 30,4 dni). Bitcoiny są więc produkowane nieco szybciej niż planowano. Kod źródłowy stara się wymusić, aby nowe bloki były generowane średnio co 10 minut. Daje to 144 bloki dziennie, czyli 3600 btc dziennie. Różnica między osiąganą dzienną produkcją oraz tą planowaną jest dosyć duża i wynosi około 640 btc, czyli trochę ponad 1/6 planu.

Wyjaśnienie tego fenomenu może być następujące. Kod źródłowy zmienia trudność produkcji bitcoinów co 2016 bloków (około dwa tygodnie) w oparciu o długość czasu w jakim zostało wyprodukowane 2016 ostatnich bloków. Kod źródłowy jednak nie jest w stanie ustawić tej nowej trudności na poziomie, który odpowiednio weźmie pod uwagę przyszły wzrost mocy obliczeniowej sieci produkującej bitcoiny. Producenci mają więc około dwóch tygodni na to, aby korzystając z ciągłego przyrostu mocy obliczeniowej produkować kolejne bloki szybciej, niż planuje to kod źródłowy. Potem trudność znajdowania nowych bloków znowu zostaje dostosowana i wraz z napływem nowych mocy obliczeniowych znowu pokonana przez producentów. Odchylenie produkcji bitcoinów o 1/6 od planu jest więc pewną miarą szaleństwa panującego na rynku produkcji bitcoinów. Jeśli to szaleństwo się skończy i wraz z dojściem do połowy produkcji bieżącej serii bloków moce obliczeniowe sieci wreszcie się ustalą, to produkcja drugiej połowy tej serii zajmie dwa lata potwierdzając przewidywania portalu bitcoinclock.com.

Podsumowując, kolejne zmniejszenie nagrody producentów bitcoinów powinno nastąpić między majem i sierpniem 2016 r. Ograniczenia sprzętowe polegające na kosztach zasilania i chłodzenia maszyn posiadających tak dużą moc obliczeniową oraz długi czas oczekiwania producentów bitcoinów na dostarczenie nowego sprzętu powinny spowodować upadek przemysłu produkcji tych maszyn najpóźniej jesienią przyszłego roku. Produkcja bitcoinów osiągnęła próg opłacalności, z którego już się nie podniesie. Przypomnijmy, że nawet ewentualny wzrost wartości bitcoina spowoduje dalszy napływ chętnych do produkcji bitcoinów gwarantujący utrzymanie nieopłacalności tej produkcji. Grono chętnych do produkcji "własnych pieniędzy" może jeszcze rosnąć przez rok w oparciu o naiwność takich inwestorów, bądź ich nadzieje na wzrost wartości bitcoina. Zmniejszenie nagrody producentów bitcoinów o połowę w lecie 2016 r. jest na tyle wymierne i bolesne, że musi skutecznie odstraszyć takich potencjalnych inwestorów na kilka miesięcy przed tym wydarzeniem.

Jest bardzo prawdopodobne, że twórcy bitcoina nie planowali tak kuriozalnych i astronomicznych kosztów oraz wymagań do produkcji tej kryptowaluty. W teorii, zmniejszanie mocy obliczeniowej sieci produkującej bitcoiny skutkować będzie zmniejszaniem trudności do produkcji nowych bloków. Tego typu efekt był widoczny na przełomie 2011 i 2012 roku. Nie jest jednak jasne, czy takie ewentualne zmniejszanie mocy obliczeniowej będzie trwałe i to na tyle, aby znacznie ograniczyć koszty generowania bitcoinów i zmniejszyć wymagania sprzętowe. Przewidywany krach na rynku produkcji tego sprzętu mógłby w tym pomóc. Bitcoin ma przecież możliwość, by opierać się na sieci tworzonej z tabletów i smartfonów.

[10] Ilość bitcoinów dostępnych w drugiej serii wynosi 5,25 miliona. W połowie sierpnia br. powinniśmy ujrzeć, że całkowita ilość wygenerowanych bitcoinów wyniesie 13,125 mil.

Filozofia tej kryptowaluty nie pozwala jednak na wymuszenie tych minimalnych wymagań sprzętowych.

Jak widać, do tej pory jedną z głównych atrakcji bitcoina była możliwość emitowania własnej "waluty", co skończyło się dramatycznym napływem emitentów. Wraz z odejściem tej atrakcji dalszy los bitcoina będzie zależeć od jego ceny wobec walut standardowych.

4.5 E. Wrażliwość na cenę

Siła waluty standardowej opiera się na rozmiarach i kondycji gospodarki posługujacej się tą walutą jako oficjalnym środkiem płatniczym. Dodatkowymi elementami wpływającymi na kurs walut standardowych jest napływ bądź odpływ inwestorów z innych stref walutowych oraz polityka monetarna banków centralnych. Warto zaznaczyć, że duże banki centralne starają się zapobiegać sytuacjom, w których emitowana przez nie waluta znacznie zyskuje na wartości wobec innych walut. Taki wzrost wartości ma negatywny wpływ na globalną konkurencyjność gospodarki firmującej się taką silną walutą. Znaczny spadek wartości waluty również nie jest pożądany, ale o ile utrzymany jest w ryzach, to na dłuższą metę wspomaga gospodarkę posiadajacą tą słabą walutę. Co więcej, niedawno ukute pojęcie "wojen walutowych" świadczy o tym, że banki centralne mogą pożądać spadku kursu swej własnej waluty wobec innych walut w celu wsparcia własnej strefy gospodarczej.

Bitcoin nie jest i nigdy nie będzie walutą z tego względu, że nie posiada powyżej opisanego wsparcia gospodarczego i spadek jego ceny wobec walut standardowych za bardzo zagraża jego istnieniu. Główni użytkownicy waluty standardowej zyskują na konkurencyjności w przypadku spadku wartości swej oficjalnej waluty. W podobnej sytuacji użytkownicy bitcoina nie zyskują nic, prócz możliwości taniego nabycia bitcoinów, które mogą dalej tracić na wartości.

Przypomnijmy, że ponad połowa wszystkich możliwych do wyprodukowania bitcoinów została wygenerowana w czasach, gdy ich wartość nie przekraczała 13 USD. Od tego momentu wartość bitcoina wrosła 50 razy. Jest to bardzo pokaźny zysk. Obecnie na rynku mamy już 5/8 wszystkich możliwych do wyprodukowania bitcoinów, a ich cena swobodnie utrzymuje się ponad poziomem 500 USD. Gdyby było jasne, że w przyszłości japoński jen będzie się trwale osłabiać wobec dolara, to nie byłyby to złe wiadomości dla jena. Kursy na tokijskiej giełdzie poszłyby w górę. Gdyby zaś było jasne, że w przyszłości kurs bitcoina wobec USD będzie się trwale obniżać, to mogłoby to wywołać panikę nagłej wyprzedaży bitcoina.

Ze względu na brak odpowiedniego wsparcia gospodarczego bitcoin nie może być traktowany jako waluta. Nie powinien być również traktowany jako standardowy walor investycyjny. W istocie, nabywając standardowe walory inwestycyjne takie jak akcje, czy obligacje inwestor utrzymuje pewne gwarancje w razie spadku ceny tych walorów. W przypadku spadku cen akcji inwestor ciagle zachowuje udziały danej spółki. Spadek cen może więc doprowadzić do wykupienia udziałów i przejęcia kontroli nad spółką. W przypadku spadku cen obligacji inwestor może czekać do momentu zapadalności tych wierzytelności i nawet w obliczu bankructwa dłużnika domagać się częściowego zaspokojenia w procesie upadłościowym.

Inwestycja w bitcoina bardziej przypomina inwestycję w kontrakty terminowe. Tego typu inwestycje są traktowane jako szczególny rodzaj hazardu. Kupując kontrakt terminowy na pewien towar można zyskać, gdy towar zyska na wartości i stracić gdy towar straci na wartości. Tego typu kontrakty opierają się jednak na cenach ustalonych towarów, które mają pewne dolne ograniczenia. Na przykład cena stali może tylko nieznacznie spaść poniżej kosztów jej produkcji. Inwestycja w bitcoina to hazard czysty. Co więcej, wiele wskazuje na

to, że bitcoin ma w sobie cechy żetonu do globalnej gry w kasynie.

Tego typu podejście należy uzasadnić, albowiem może być ono odpowiednią podstawą do dolnego oszacowania ceny bitcoina.

Po pierwsze, nie jest prawdą, że produkcja bitcoinów to rozwiązywanie matematycznie skomplikowanych problemów kryptograficznych. Produkcja bitcoinów, to proces czysto losowy. Polega on na wielokrotnym nałożeniu funkcji haszującej i każdorazowym sprawdzeniu, czy wynik tej operacji osiąga pożądany cel. Proces ten jest więc analogiczny do wielokrotnego rzutu monetą, tak aby w końcu osiągnąć serię odpowiedniej ilości orłów pod rząd. Maszyny produkujace bitcoiny wykonują mnóstwo takich operacji w bardzo krótkim czasie, czyli w naszej analogii są to maszyny do "szybkiego rzucania monetą", a nie zaawansowane mózgi elektronowe do rozwiązywania matematycznych problemów kryptograficznych. W tej analogii cała trudność w uzyskiwaniu bitcoinów sprowadza się do tego, że kod źródłowy wymaga dłuższych serii orłów pod rząd (np. 5, 10, 15 itd.). Podobnie, cała łatwość w uzyskiwaniu bitcoinów sprowadza się do tego, że kod źródłowy wymaga krótszych serii orłów pod rząd (np. 5, 2, 1). Nie warto chyba dodawać, że "rozwiązywanie" tego typu "problemów" ma zerową wartość matematyczną.[11]

Po drugie, dziesięciokrotny wzrost wartości bitcoina na przełomie 2012 i 2013 roku zbiega się w czasie z popularyzacją serwisu SatoshiDice, który był pierwszym serwisem oferującym hazard internetowy oparty na płatnościach w bitcoinach. Ten wzrost wartości bitcoina osiągnał swój szczyt w maju 2013 r. wraz z ograniczeniem dostępu do tego serwisu użytkownikom z USA z przyczyn prawnych. Kolejny pięciokrotny wzrost wartości bitcoina pod koniec 2013 roku może być tłumaczony intensywnym rozwojem innych portali oferujących usługi hazardu internetowego w oparciu o płatności w bitcoinach. Strona en.bitcoin.it/wiki/Category:Gambling listuje obecnie około 40 kasyn internetowych, 7 portali pokerowych i ponad 20 portali do gry w kości. Wszystkie te portale operują traktując bitcoin jako żeton do gry.

Po trzecie, na liście najpopularniejszych adresów używanych do transakcji bitcoinów sam serwis SatoshiDice zajmuje ponad 20 czołowych pozycji. We wspomnianym okresie popularyzacji serwis ten generował około 50% dziennego obrotu liczonego ilością transferów[12]. Istnieją sugestie, że zbiorowy udział serwisów internetowych oferujących tego typu hazard nadal utrzymuje poziom 50% dziennego obrotu bitcoina.[13]

Po czwarte, bitcoin z założenia miał posiadać wszystkie cechy umożliwiające użycie go do hazardu, który w wielu krajach jest nielegalny: anonimowość użytkowników, brak organu odpowiedzialnego za emisję, łatwość transferu, nieodwracalność transferu, bezpieczeństwo przechowania i łatwość wymiany na waluty standardowe. Ze względu na kłopoty z legalizacją standardowy hazard internetowy narażony jest na nieuczciwość klientów, którzy po przegranym zakładzie starają się anulować swoją transakcję dokonaną w celu obstawienia zakładu. Nieodwracalność transferu bitcoinów może być więc udogodnieniem dla serwisów oferujących hazard internetowy w oparciu o standardowe waluty. Niestety bitcoin prawdopodobnie zmarnował tą szansę ze względu na niedopełnienie innych założeń, czyli bezpieczeństwa przechowania i łatwości wymiany na waluty standardowe. Jak dobrze wiadomo, wielu użytkowników utraciło swoje "bezpieczne" bitcoiny na różnych giełdach wymiany.

Powyższe podejście pozwala, przynajmniej połowicznie, ocenić potencjał dalszego wzrostu ceny bitcoina oraz dostarcza ograniczeń co do jej spadku.

[11] Dużą wartością eksperymentalną byłoby jedynie stwierdzenie, że tego typu masowy hazard daje wygrane odbiegające od przewidywań statystycznych.

[12] Co jest różne od obrotu liczonego wielkością transferów, czyli ilością transferowanych bitcoinów.

[13] www.pbs.org/newshour/updates/bitcoin-gambling-sites-fly-regulatory-radar/

Według danych firmy *H2 Gambling Capital* globalny rynek hazardu internetowego osiąga roczne zyski między 30 i 40 miliardów USD. Dla uproszczenia przyjmijmy, że jest to 36,5 miliarda USD, co daje 100 milionów USD na dzień. Dzienny obrót bitcoinami wyrażony w USD również jest bliski tej wartości (średnia z II kwartału 2014 r. wynosi około 50 mil. USD). Serwisy internetowe oferujące hazard w bitcoinach generują swe zyski zachowując około 1-2% bitcoinów, którymi obracają. Zyski te stanowią więc w przybliżeniu najwyżej 1 milion USD dziennie. To daje zaledwie 1% rynku wszystkich usług hazardu internetowego. Oczywiście można wierzyć, że w takim razie bitcoin ma szansę na to, aby ten udział zwiększyć 100 razy. Wydaje się to jednak mało realne. *Q1 2014 Online Gambling Quarterly report* opublikowany przez MECN stwierdza, że zdaniem ekspertów tej dziedziny hazardu bitcoin ma bardzo mały potencjał na zwiększenie swego udziału w zyskach osiąganych z hazardu internetowego.[14]

Jest to o tyle istotne, że serwisy oferujące hazard w bitcoinie dostarczają jedynego sensownego wsparcia dla ceny tej kryptowaluty. W sytuacji drastycznego spadku cen, te serwisy jako jedyne mogą zacząć skupować bitcoiny w celu utrzymania swej dalszej działalności. Pozostałe podmioty gospodarcze przyjmujące bitcoiny jako formę płatności nie mają żadnego interesu w skupie bitcoinów. Z ich perspektywy przyjmowanie bitcoinów jest formą reklamy, na której mogą stracić, tak jak na przyjęciu usług serwisów oferujących zakupy grupowe. Bitcoinowe serwisy hazardowe jako jedyne potrzebują bitcoinów w celach biznesowych, po to aby wypłacać wygrane swym użytkownikom.[15] Aby utrzymać swój dzienny zysk na poziomie 1 miliona USD serwisy te mogą liczyć na maksymalny obrót w wysokości 21 milionów bitcoinów dziennie[16] (obecnie te obroty są około 200 razy mniejsze). Zakładając, że zyski z działalności tych serwisów wynoszą 1% obrotów daje to 0,2 mil. btc w cenie 1 mil. USD czyli 5 dolarów za bitcoina. Poniżej tej granicy cenowej utrzymanie zysków tych serwisów na poziomie 1 mil. USD dziennie nie będzie już możliwe. Dzięki temu cena 5 USD za 1 btc stanowi minimalne wsparcie dla ceny bitcoina wobec dolara. Po tej cenie wszystkie bitcoiny można wykupić za około 100 milionów USD ratując bitcoinowe serwisy hazardowe, które w naszym modelu osiągają roczne zyski na poziomie 365 milionów USD.

Aby zrozumieć obecne ceny bitcoina wystarczy powtórzyć powyższe rozumowanie stosując bieżącą skalę obrotów. Wynosi ona około 100 tys. btc dziennie, czyli ok. 200 razy mniej niż powyższe 21 mil. To daje cenę 200 razy większą, niż wyliczone uprzednio 5 USD. Dzięki temu uzyskujemy cenę 1 000 USD za 1 btc, czyli około 2 razy wyższą niż obecnie.

Przyjmując że w istocie istnieje potencjał, aby bitcoinowe serwisy hazardowe generowały roczny zysk rzędu 365 milionów USD, możemy potraktować bitcoiny jako swoistego rodzaju udziały w tym biznesie hazardowym. To daje możliwość bardziej realnej wyceny bitcoina. Przedsięwzięcie generujące stały roczny zysk Z może być wycenione metodą dyskontowanych przepływów pieniężnych. W tej metodzie przyszłe przepływy pieniężne są zmniejszane, aby odpowiednio ująć straty wynikające z ich oddalenia w czasie. Najprostrza metoda tego typu, to kapitalizacja prosta. Zakłada się w niej, że inwestor żąda pewnego dyskonta R (z reguły jest to 10%) i wycenia przepływy, które nastąpia po n latach według łatwego do zrozumienia równania: $(1+R)^n \cdot$cena n-tego przepływu$= Z$. Sumując ceny wszystkich przyszłych przepływów otrzymujemy więc

$$\text{cena} = \sum_{n=1}^{\infty} \frac{Z}{(1+R)^n} = \frac{Z}{R}.$$

Zgadzając się na standard $R = 0,1$ widzimy, że w uproszczeniu metoda kapitalizacji prostej

[14] www.isa-guide.de/english-news/articles/110657.html

[15] Warto dodać, że ci użytkownicy (czyli gracze) również dostarczają określonego popytu na bitcoiny wspierając ich cenę.

[16] Przy założeniu, że obrót wszystkimi dostępnymi bitcoinami odpowiednio wydłuży czas potwierdzenia transakcji.

polega na tym, aby stały roczny zysk pomnożyć przez 10 i taki wynik przyjąć jako cenę przedsięwzięcia generującego te zyski. W naszym przypadku cena bitcoinowego biznesu hazardowego wynosi więc 3 650 milionów USD. Traktując wszystkie 21 milionów bitcoinów jako swoiste udziały w tym biznesie[17] otrzymujemy, że cena jednego bitcoina to 3 650/21=173,8 USD, czyli około 3 razy niższą od obecnej.

Zakładając, że dotychczasowe wzrosty cen bitcoina związane były z wykorzystaniem jego atutu hazardowego, otrzymujemy dosyć nikły potencjał dalszego wzrostu ceny tej waluty. Oprócz skonsumowania atutu polegającego na atrakcyjności produkcji bitcoinów blednie więc również atut inwestycyjny bitcoina. Ze względu na to, że ponad połowa bitcoinów została wyprodukowana w czasie, gdy ich cena była 50 razy niższa niż obecnie, istnieje dosyć duże ryzyko chęci realizacji tych zysków. Jedyne serwisy potrzebujące bitcoinów do prowadzenia swej działalności są zbyt młode i nie zdążyły wygenerować odpowiednich zysków, aby zagwarantować obecną cenę bitcoina w najbliższej przyszłości. Utrzymanie ceny bitcoinów powyżej obecnych poziomów zależeć więc będzie od dalszej popularyzacji tej kryptowaluty z nadzieją na przedłużenie wzrostów jej ceny, co oddali ryzyko realizacji zysków z inwestycji w bitcoina.

4.6 F. Konieczność popularyzacji

Popularność bitcoina wynikająca z potraktowania go jako żeton do uprawy gier hazardowych zdaje się osiągać swoje granice odzwierciedlone w stabilności cen bitcoina wobec USD. Popularność ta nie jest duża i może zostać łatwo zmniejszona przez ukłony legislacyjne wobec przemysłu hazardowego posługującego się standardowymi walutami. Jest bardzo prawdopodobne, że bitcoin zdołał już wykorzystać prawie wszystkie swoje atuty (produkcyjny, hazardowy, inwestycyjny). Natomiast ze względu na swój atut hazardowy bitcoin praktycznie nie ma szans na pełną legalizację jako środek płatniczy. Co gorsza, istnieje ryzyko delegalizacji bitcoina w niektórych krajach. To może zaniepokoić producentów, którzy ponieśli realne koszty przy produkcji bitcoinów i prawdopodobnie zatrzymali część wyprodukowanej kryptowaluty w celach inwestycyjnych. W rozsądnym scenariuszu wraz z upływem czasu bitcoinowe serwisy hazardowe oraz ich użytkownicy będą stopniowo przejmować wyprodukowane bitcoiny po obecnych cenach. Przypomnijmy jednak, że bitcoiny są stale produkowane, co zwiększa ich podaż. Dalsza popularyzacja tej kryptowaluty staje się więc drogą do zwiększenia popytu, który mógłby utrzymać obecne ceny.

Kroki podejmowane przez promotorów bitcoina nie mogą jednak powielić sukcesu serwisów oferujących zakupy grupowe. W tym przypadku dostarczyciele usług i towarów detalicznych zostali zmuszeni do masowego korzystania z tych serwisów. Ten przymus opierał się na tym, że ze względu na niższą cenę klienci wybierali tylko tych dostarczycieli, którzy oferowali zakupy w systemie grupowym. Bitcoin nie jest w stanie stworzyć takiego przymusu. Kawiarnia przyjmująca płatności w bitcoinach może zyskać kilku nowych klientów. Osoby nie używające bitcoinów nic jednak nie stracą, gdy pójdą do innej kawiarni, która przyjmuje tylko zwykłe płatności.

Model popularyzacji bitcoinów może się za to oprzeć na świadczeniu usług i fantów dla osób używających bitcoina w celach hazardowych. Tego typu model funkcjonuje w świecie standardowego przemysłu hazardowego. W skrócie, za posiadane bitcoiny użytkownik może przedostać się do hotelu, tam otrzymac kilka fantów i pewną kwotę standardowej waluty, którą później (średnio) przegra w pobliskim kasynie.

[17] Oczywiście nie są to prawdziwe udziały pozwalające na otrzymanie porcji zysku z działalności tego biznesu.

Udana popularyzacja bitcoina, która pozwoli producentom bitcoinów na wyjście z tego biznesu bez szwanku może jednak wywołać nieoczekiwane skutki. Bitcoiny mogą pogłębić swoje nielegalne zastosowania. Na przykład zostać zaakceptowane jako bezpieczny sposób na przekazywanie pieniędzy w ramach korupcji. Osoba korumpowana może bowiem pozwolić sobie na oczekiwanie, aż przekazane bitcoiny zostaną potwierdzone i wymienione na walutę standardową. Tego typu proceder jest praktycznie niewykrywalny, co może tłumaczyć łatwość z jaką propagatorzy bitcoina zdobywają nowych zwolenników akceptacji tej kryptowaluty.

Akceptacja bitcoina w społecznościach lokalnych może też wyzwolić atut socjalny tej kryptowaluty, czyli użycie jej zgodnie z obiecanym przeznaczeniem. Osoby wykonujące drobne prace oraz sprzedające własne produkty mogą wykorzystywać bitcoiny do prowadzenia swej działalności w szarej nieopodatkowanej strefie.

Bitcoin posiada jednak kilka ograniczeń, które będą hamować jego popularyzację.

Przypomnijmy, że bitcoiny produkowane są w blokach, które zawierają i potwierdzają informacje o dokonanych transakcjach. Wszyskie wyprodukowane bloki ustawiane są zgodnie z kolejnością ich produkcji tworząc tzw. *łańcuch bloków*. Łańcuch ten zawiera potwierdzenia wszystkich transakcji dokonanych bitcoinami i stanowi jądro tej kryptowaluty. Dla niektórych ten łańcuch bloków jest genialnym rozwiązaniem, które jak wielka księga wieczysta spisuje wszystkie ruchy bitcoinów i będzie rosnąć w nieskończoność, tak aby każdy mógł się do niej dopisać. Dla innych ten łańcuch bloków stanowi beznadziejne i brzydkie rozwiązanie problemu przekazywania "waluty" w formie informacji. Pełny użytkownik bitcoina musi mieć dostęp do całego łańcucha, który jest aktualizowany na bieżąco. Budzi to duże wątpliwości natury praktycznej. Aby w pełni używać bitcoina należy utrzymywać informacje o wszystkich przeszłych transakcjach wszystkich użytkowników bitcoina na całym świecie. Normalna waluta nie ma takich ograniczeń.

Kwestia rozmiaru łańcucha bloków jest na tyle drażliwa, że użytkownicy bitcoina uważają ją za zamkniętą. Łańcuch ma obecnie rozmiar około 19 GB (19 gigabajtów) i wykazuje lekką tendencję do wzrostu kwadratowego. Warto zaznaczyć, że ten wzrost jest odnotowywany nawet w sytuacji stabilnego wolumenu transakcji w bitcoinach. Wzrost popularności bitcoina i wzrost wolumenu transakcji mogą spowodować, że rozmiar łańcucha bloków zacznie rosnąć zbyt szybko. Zwiększona ilość transakcji będzie też rzutować na czas potrzebny do ich potwierdzenia. Bitcoin w swej obecnej formie nie gwarantuje odpowiednich możliwości technicznych do poradzenia sobie ze wzrostem popularności. W rezultacie, promotorzy bitcoinów oferują uproszczone procedury do nabywania, przechowywania i wydawania bitcoinów, co odbija się na bezpieczeństwie tej kryptowaluty.

Nierozwiązanie kwestii bezpieczeństwa i utrata zaufania wielu dotychczasowych użytkowników bitcoina jest poważnym hamulcem dla jego popularyzacji. Tajemnicze zniknięcie 650 tysięcy bitcoinów zdeponowanych przez użytkowników na giełdzie wymiany Mt. Gox odstrasza od bitcoina i podkreśla kłopoty z jego wymienialnością na waluty standardowe. Pokazuje również, że łańcuch bloków jest słabym rozwiązaniem. W przypadku kradzieży bitcoinów sprawca zostawia swój ślad, czyli informację na jakie adresy zostają przesyłane kradzione bitcoiny. Jest to więc zwykła transakcja, która w efekcie potwierdzenia nowymi blokami bitcoinów trafia na zawsze do łańcucha bloków. Wykrycie procederu kradzieży jest więc możliwe, ale anulowanie tych transakcji jest utrudnione. Proste anulowanie tych transakcji oznacza anulowanie wszystkich transakcji, które zostały potwierdzone kolejnymi blokami. Aby tego uniknąć, należy chwilowo zatrzymać proces produkcji bitcoinów. Anulować kwestionowane transakcje i znów uruchomić produkcję bitcoinów w celu ponownego potwierdzenia pozostałych transakcji. W tym rozwiązaniu część bloków zostaje zniszczona przynosząc straty ich producentom i wytwarzając nawis transakcji wymagających potwierdzenia. Ze względu

na decentralizację emisji bitcoinów tego typu rozwiązanie nie jest stosowane i łańcuch bloków pieczętuje takie akty kradzieży.

Podsumowując, bitcoin jako produkt może się okazać nieatrakcyjny, lub nawet uciążliwy dla osób, które nie mają potrzeby operowania w szarej strefie.

4.7 G. Parametry rynkowe

Cena bitcoina wobec USD osiagnęła swoje maksimum 1250 USD pod koniec listopada 2013 roku. Kilka dni potem cena trwale spadła poniżej 1000 USD. Przyczyną tego ograniczenia cenowego była decyzja centralnego banku Chin (z dnia 5 grudnia 2013 r.) nakładajaca poważne ograniczenia w obrocie bitcoinem. Zgodnie z tą decyzją chińskie instytucje finansowe nie mogą kupować ani sprzedawać bitcoinów, podawać cen w bitcoinach oraz oferować jakichkolwiek produktów i usług związanych z bitcoinem.

Ta decyzja jest o tyle istotna, że ponad połowa wszystkich bitcoinów wymienianych na waluty standardowe znajduje się w rękach osób posługujących się chińską walutą. W istocie, zgodnie z danymi bitcoincharts.com/charts/volumepie/ pekińska giełda OKCoin ma udział 56% w globalnym obrocie bitcoinami notowanym na wszystkich giełdach wymiany tej kryptowaluty na waluty standardowe. Kolejne 5% udziału posiada szanghajska giełda BTC China. Obie te giełdy mogą używać tylko chińskiej waluty i innych kryptowalut. W sumie 62% wszystkich bitcoinów wymienianych na światowych giełdach jest wymieniana na chińska walutę. Wymiana bitcoinów na USD ma udział dwukrotnie mniejszy i wynosi 27%. Wymiana na pozostałe waluty ma udział 11%, w tym jedynie około 3% przypada na euro.

Tak duży udział chińskiej waluty w globalnej wymianie bitcoinów na waluty standardowe wymaga pogłębionej analizy.

Obrót notowany na światowych giełdach wymiany bitcoinów nie jest duży. W II kwartale br. wartość wszystkich transakcji bitcoinami wyniósła około 50 milionów USD dziennie. Obrót na wszystkich giełdach wymiany bitcoinów nie powinien więc przekraczać 50 mil. USD dziennie. Udział chińskiej waluty w tym obrocie to najwyżej 30 mil. USD dziennie.

Powyższe obroty są bardzo niskie. Wg. BIS w zeszłym roku średni dzienny obrót na rynku wymiany walut standardowych wyniósł 5,3 biliona USD, jest to więc około 200 tysięcy razy więcej niż ewentualne 50 milionów USD średniego dziennego obrotu na rynku walutowym bitcoina.

Mimo tych niskich obrotów wymiany chińskiej waluty na bitcoiny należy pamiętać, że bank centralny Chin stosuje dosyć twardą politykę izolacji swojej waluty od innych walut standardowych. Dlatego, nie tylko chęć ochrony swoich obywateli, lecz również swojej waluty są cytowane jako przyczyny wprowadzenia ostrych restrykcji wobec bitcoina przez Ludowy Bank Chin.

Najpopularniejszą walutą światową jest USD ze względu na rozmiar i siłę gospodarki USA oraz uwarunkowania polityczno-historyczne. Rozmiar gospodarki Chin jest porównywalny, lecz chińska waluta nie podlega wolno-rynkowej wymianie na inne waluty standardowe (co ma swoje uzasadnienie, lecz powoli niszczy partnerów handlowych Chin). Bitcoin może być więc traktowany jako specyficzny pas transmisyjny umożliwiający taką wymianę na drobną i ryzykowna skalę.

Waluta emitowana przez bank centralny Chin nosi nazwę *renminbi*. Podstawowa jednostka tej waluty to *yuan*. Yuan używany jest w Chinach kontynentalnych i oznaczany jako CNY.

Oprócz tego yuan może byc transferowany do Hong Kongu otrzymując skrót CNH. Wymiana CNY na CNH podlega pewnym restrykcjom. Dodatkowo Hong Kong posiada swoją własną wymienialną (i dosyć popularną) walutę *dolar hongkoński* oznaczaną jako HKD. Ze względu na swą strukturę dolar ten może być utożsamiany z USD. Kurs wymiany HKD na USD jest prawie stały i wynosi 7,75 HKD za 1 USD. W związku z tym restrykcje przy wymianie yuanów na HKD muszą być podobne jak przy wymianie na USD. Oczywiście z wyjątkiem czarnego rynku wymiany yuanów w Hong Kongu.

To czy bitcoin może włączyć się w tą grę wymiany zależy od nastawienia organów rezydujących w chińskich terytoriach. Do tej pory nie miał takich możliwości. W maju br. taka możliwość została jednak stworzona wraz z otworzeniem hongkońskiej giełdy ANX (Asia Nexgen Bitcoin Exchange) na handel kluczowymi walutami światowymi. Oczywiście główną atrakcją tej giełdy jest możliwość wymiany bitcoinów na chińską walutę CNY. Inne akceptowane waluty to: AUD, CAD, CHF, EUR, GBP, HKD, JPY, NZD, SGD oraz USD. Na razie handel tymi walutami jest w fazie rozruchu. Na każdej z tych walut dzienny obrót wymiany na bitcoina jest prawie identyczny. Trudno jednak ocenić, czy wiodące chińskie giełdy kryptowalut zapewnią swoim użytkownikom odpowiednie bezpieczeństwo oraz otrzymają stałe przyzwolenie na operowanie w yuanie umożliwiając bitcoinowi skorzystanie na minimalnej odwilży w chińskiej polityce monetarnej.[18]

Warto również podkreślić, że prawdziwa skala operacji w bitcoinach jest trudna do oceny. Kluczową kwestią jest średni dzienny obrót bitcoinami. Strona blockchain.info podaje całkowity obrót, który średnio waha się między milionem i połową miliona btc dziennie. Niestety bitcoin działa w ten sposób, że osoba dokonująca transakcji najpierw przesyła pewna kwotę bitcoinów, a potem otrzymuje resztę w bitcoinach. Całkowity obrót zlicza obie części tej transakcji. Jeśli dana osoba przesyła 1 btc i otrzymuje 0,9 btc reszty dokonując transakcji przesłania 0,1 btc, to realny obrót wynosi 0,1 btc, a całkowity obrót wynosi 1,9 btc. Dane dotyczące całkowitego obrotu są więc przetwarzane tak, aby szacunkowo określić obrót realny (patrz blockchain.info/pl/charts/esti- mated-transaction-volume). Nie jest jasne na ile te szacunki są poprawne. Strona bitcoincharts.com dostarcza jednak bardziej szczegółowych danych dotyczących obrotu na giełdach wymiany bitcoina. Według tych danych średni dzienny obrót na tych giełdach w przeciągu ostatnich 30 dni wyniósł około 100 tys. btc dziennie. Daje to około 50-60 milionów USD dziennego obrotu na rynku wymiany btc na waluty standardowe (o ile włączymy do nich niezbyt wymienialnego yuana).

Dla bezpieczeństwa możemy też skoncentrować się na całkowitym obrocie i przyjąć, że wynosi 1 milion btc dziennie. Nawet jeśli ten obrót trafia w całości na giełdy wymiany btc, to otrzymujemy 500-600 milionów USD dziennego obrotu na tych giełdach. Jest więc to kropla 20 tysięcy razy mniejsza niż cały ocean rynku FOREX, który wg. danych BIS w ubiegłym roku miał 5,3 biliona dolarów dziennych obrotów.

Sama kapitalizacja bitcoina jest bardzo mizerna i wynosi zaledwie 8 miliardów dolarów. Dla porównania, w marcu br. Unicredit ogłosił kwartalną stratę w wysokości około 20 miliardów dolarów. Zniknięcie wszystkich bitcoinów w jeden dzień można więc ocenić jako mniejszą stratę finansową niż srogie kichnięcie dużego banku europejskiego.

W obecnym stanie bitcoin wraz z przylegajacymi i konkurencyjnymi kryptowalutami jest prawie niewidoczny z perspektywy rynku finansowego.

[18] Ponieważ kwestia urynkowienia yuana jest bardzo poważna, istnieje możliwość, że ta potencjalna korzyść bitcoina zniknie wraz z włączeniem yuana do koszyka SDR (patrz internet).

4.8 H. Duża awaryjność

Duża awaryjność panująca w środowisku usług związanych z bitcoinem jest czynnikiem, który znacznie ogranicza możliwość popularyzacji tej kryptowaluty. Poniższe kalendarium tych awarii nie jest pełne, lecz pozwala zrozumieć skalę tego problemu.

15.08.2010 - Wykorzystanie luki w protokole bitcoina i wygenerowanie przez użytkownika dwóch fałszywych transakcji opiewających w sumie na ponad 184 milionów bitcoinów. W celu anulowania tych transakcji łańcuch bloków został rozszczepiony.

13.06.2011 - Użytkownik allinvain oświadcza, że z jego wirtualnego portfela ukradziono 25 tys. btc informując tym samym o pierwszej kradzieży kryptowaluty.

19.06.2011 - Haker wykrada dane użytkowników giełdy wymiany bitcoinów Mt. Gox, łamie hasła części tych użytkowników i składa zamówienie na sprzedaż dużej ilości bitcoinów powodując spadek ich wartości do 0,01 USD.

26.07.2011 - Polska giełda wymiany bitcoinów Bitomat traci 17 tys. btc w wyniku błędu administratora, a potem zostaje przejęta przez giełdę Mt. Gox.

05.08.2011 - Jeden z pierwszych dostarczycieli uproszczonych procedur do obrotu bitcoinami MyBitcoin ogłasza upadłość w związku z utratą ponad 78 tys. btc w wyniku ataku hakerskiego.

05.10.2011 - Giełda wymiany bitcoinów Bitcoin7 po kilku miesiącach działalności ogłasza swe zamknięcie w wyniku ataku hakerskiego i utraty ponad 5 tys. btc.

13.02.2012 - Druga co do wielkości (w tamtym czasie) giełda wymiany bitcoinów Tradehill ogłasza swe zamknięcie ze względów prawnych (nie ujawniając strat poniesionych przez jej użytkowników).

02.03.2012 - Firma Linod dostarczająca usług w chmurze obliczeniowej zostaje zaatakowana przez hakerów. Ich celem są klienci firmy Linod, którzy wykorzystują jej serwery do obsługi własnych serwisów internetowych związanych z bitcoinami. Największe straty ponosi firma Bitcoinica (ponad 43 tys. btc) oferująca kontrakty do spekulacji dotyczących kursu btc wobec USD. W sumie straty klientów firmy Linod wyniosły ok. 47 tys. btc.

11.04.2012 - Bitcoinowy serwis hazardowy Betcoin zgłasza kradzież 3 tys. btc.

20.04.2012 - Użytkownik Tony76 oferujący tanie narkotyki na stronie Silk Road nie dostarcza towaru i uchodzi z ok. 20-30 tys. btc.

12.05.2012 - Ponowny atak hakerski na serwis Bitcoinica. W sumie skradzionych zostaje 38,5 tys btc. W tym około 20 tys. btc pochodzących od właściciela giełdy wymiany bitcoinów BitMarket.eu, który używał bitcoinów klientów swej giełdy do uprawy hazardu finansowego oferowanego przez serwis Bitcoinica.

13.07.2012 - Kolejny atak hakerski na serwis Bitcoinica. Tym razem ginie 40 tys. btc utrzymywanych przez ten serwis na koncie giełdy Mt. Gox. Dwa tygodnie później Bitcoinica zostaje zamknięta i postawiona w stan likwidacji.

17.08.2012 - Upada piramida finansowa Bitcoin Savings and Trust oferująca tygodniowy zysk w wysokości 7% zainwestowanych bitcoinów. Jej twórca Trendon Shavers defrauduje ok. 250 tys. btc i zostaje pociągnięty do odpowiedzialności przez Securities and Exchange Commission.

04.09.2012 - Nowojorska giełda wymiany bitcoinów Bitfloor zarejestrowana przez rządowe biuro Financial Crimes Enforcement Network zgłasza kradzież 24 tys. btc.

06.10.2012 - Nagłe zamknięcie giełdy GLBSE (Global Bitcoin Stock Exchange) oferującej możliwość inwestycji w firmy związane z bitcoinem (straty inwestorów nie są znane).

11.03.2013 - Błędy w protokole bitcoina powodują rozszczepienie łańcucha bloków.

03.04.2013 - Kolejny dostarczyciel uproszczonych procedur do obrotu bitcoinami Instawallet zostaje zaatakowany i zamyka swą działalność nie informując o poniesionych stratach (ok. 35 tys. btc).

02.10.2013 - FBI zamyka serwis Silk Road będący miejscem wymiany bitcoinów na nielegalne towary. Około 30 tys. btc należących do użytkowników serwisu zostaje przejęte przez FBI. Kilka tygodni potem ok. 144 tys. btc zostaje przejęte od aresztowanego właściciela tego serwisu Rossa Ulbrighta. Kontestuje on jednak legalność zajęcia jego własnych bitcoinów przez FBI.

11.08.2013 - Użytkownicy bitcoinów korzystający z aplikacji Android dowiadują się, że aplikacja ta nie dostarcza odpowiedniego bezpieczeństwa dla obrotu bitcoinami narażając użytkowników na utratę bitcoinów.

26.10.2013 - Znika chińska giełda bitcoinów Global Bond Limited generując straty jej użytkowników w wysokości 30 mil. yuanów (ok. 5 milionów USD).

04.11.2013 - Bankructwo firmy Alydian (związanej z przewodniczącym Bitcoin Foundation) oferującej inwestycje w produkcję bitcoinów.

27.01.2014 - Zamknięcie nowojorskiej giełdy wymiany bitcoinów Bitinstant w związku z aresztowaniem jej współzałożyciela i dyrektora Charliego Shrema. Był on również członkiem założycielem Bitcoin Foundation. Został aresztowany pod zarzutem prania brudnych pieniędzy przy użyciu serwisu Silk Road.

28.02.14 - Giełda wymiany bitcoinów Mt. Gox wnioskuje o bankructwo (ochronę przed wierzycielami) po utracie ok. 650 tys. btc swoich użytkowników. Dyrektor i współwaściciel tej giełdy Mark Karpelès jest również członkiem założycielem Bitcoin Foundation.

Warto dodać, że ze względu na brak prawnej ochrony użytkownicy tracący swoje bitcoiny mają trudności z ich odzyskaniem, lub nawet wszczęciem śledztwa oraz innych kroków prawnych w przypadku utraty bitcoinów. Ponadto istnieją podejrzenia, że niektóre akty kradzieży bitcoinów nie były dokonywane przez hakerów, lecz przez osoby związane z dostarczycielami usług opartych na bitcoinie.

Anonimowość użytkowników bitcoina oraz brak osób odpowiedzialnych za zarządzanie tą kryptowalutą jest więc zarówno atutem jak i poważną bolączką bitcoina.

4.9 I. Brak organów

O ile anonimowość użytkowników bitcoina może być cechą pożądaną przez osoby operujące w szarej strefie, to brak osób gwarantujących pokrywalność tej kryptowaluty jest cechą fatalną.

W teorii, bitcoin miał nie wymagać zarządzania, tylko rozprzestrzeniać się zdobywając nowych użytkowników. W praktyce wymagało to stworzenia odpowiedniego oprogramowania implementujacego protokół bitcoina, który mógł być pobierany przez potencjalnych użytkowników

tej kryptowaluty. Twórca pierwszych wersji tego oprogramowania nadal ukrywa się pod pseudonimem Satoshi Nakamoto. Warto zauważyć, że od stycznia 2009 do grudnia 2010 Satoshi Nakamoto stworzył 23 wersje tego oprogramowania poczynając od wersji 0.1.0, a kończąc na wersji 0.3.19. Niektóre z tych zmian były wymuszone koniecznością wprowadzenia poprawek do oprogramowania. Niestabilność oprogramowania oferowanego użytkownikom jest standardowym problemem całej branży dostarczającej tego typu produkty. Oprogramowanie implementujące protokół bitcoina nie jest żadnym ewenementem i wymaga ciągłego monitoringu przez grupę osób mogących wprowadzać konieczne zmiany. Ta grupa to tzw. deweloperzy bitcoina. Po roku 2010 Satoshi Nakamoto usunął się z dalszej realizacji projektu bitcoina przekazując pałeczkę innym deweloperom oraz opiekunom bitcoina. Bez wątpienia najważniejszą funkcję w tej grupie pełnią osoby uprawnione do ogłoszenia alertu dla użytkowników bitcoina, w sytuacji wykrycia krytycznych problemów zagrażających funkcjonowaniu oprogramowania implementujacego protokół bitcoina. Wg. portalu en.bitcoin.it/wiki/Alerts osoby uprawnione do podniesienia alertu to Satoshi Nakamoto (twórca bitcoina) Gavin Andresen (deweloper bitcoina) oraz Michael Marquardt (opiekun bitcoina). Gavin Andresen jest członkiem założycielem Bitcoin foundation oraz należy do grona głównych deweloperów bitcoina. Wg. portalu bitcoin.org/en/development jest to grono o nastepującym składzie: Wladimir J. van der Laan,[19] Gavin Andresen, Jeff Garzik, Gregory Maxwell oraz Pieter Wuille. Wg. portalu en.bitcoin.it/wiki/People Michael Marquardt opiekuje się bitcoinem jako założyciel portalu blockexplorer.com oraz forum bitcointalk.org.

Wymienione osoby mają pewną dozę władzy nad bitcoinem. Nie są jednak odpowiedzialne za dostarczenie jakichkolwiek gwarancji w zakresie wartości generowanej kryptowaluty. W istocie, wartość bitcoina jest umowna i nikt nie może być obarczony odpowiedzialnością, gdy spadnie do zera. Paradoksalnie, producenci sprzętu generującego bitcoiny w przypadku znacznego opóźnienia w dostawie sprzętu mogą być pozwani o straty wynikające z utraty możliwości wygenerowania bitcoinów o dużej wartości rynkowej. Jeśli jednak w okresie opóźnienia wartość tych bitcoinów byłaby prawie zerowa, to strona pozywająca nie ma już możliwości by wykazać utracony zysk.

5 Synteza

Bitcoin ma dużą wartość edukacyjną. Mimo iż nigdy nie będzie walutą, bo nie ma oparcia w rzeczywistej gospodarce, to w skali mikro przedstawia model wolnego rynku finansowego odrywającego się od realnej gospodarki.

Ta wolność objawia się w minimalnej ilości ograniczeń nałożonych na bitcoina przez jego twórców. Ograniczenie główne, czyli stopniowanie procesu produkcji skończonej ilości tej kryptowaluty, nie zapobiegło eksplozji nadprodukcji bitcoinów. Ta nadprodukcja jest widoczna w szybkości produkowania nowych bitcoinów, która obecnie jest o 1/6 większa od zaplanowanej.

Ogromna ilość osób chętnych do produkcji tej kryptowaluty doprowadziła do marginalizacji zysków z produkcji bitcoinów. Przewidywany krach na rynku produkcji bitcoinów może zaś doprowadzić do krachu wartości bitcoina w stosunku do walut standardowych, powielając znany z historii los walut oderwanych od gospodarki.

Brak innych ograniczeń wobec bitcoina pokazał natomiast zasadność regulacji rynku finansowego. Ryzyko kontrahenta w środowisku bitcoina jest tak ogromne, że odstrasza jej potencjalnych użytkowników.

[19] Obecny lider zespołu deweloperów bitcoina, bitcoinfoundation.org/2014/04/07/bitcoin-core-maintainer-wladimir-van-der-laan/

W świecie bitcoina mamy upadające banki i giełdy, piramidy finansowe, zwykłe oszustwa i malwersacje oraz absurdalną pogoń za zyskiem. Są to standardowe objawy wolnego rynku finansowego. W przypadku rynku opartego na uznanej walucie upadające banki i giełdy są ratowane, piramidy finansowe są likwidowane w zarodku, oszustwa i malwersacje są ścigane z urzędu, a absurdalna pogoń za zyskiem przekształca się w działania ochraniające zdobyty kapitał. Bitcoin pokazuje, czemu te działania są konieczne.

Pozostałe kryptowaluty są efektem marginalizacji zysków z produkcji bitcoina i ich parametry rynkowe są zbyt niskie, by warto było o nich wspominać. Z perspektywy rynku finansowego, o wiele większe parametry bitcoina również nie zasługują na uwagę.

Bitcoin może funkcjonować jako moneta, której jedną stroną jest drobny handel, a drugą mikro FOREX. Jej dalsze istnienie jest jednak zagrożone rosnącą ilością danych, które obciążaja system transakcyjny bitcoina oraz przewidywanym krachem na rynku produkcji tej kryptomonety.

Najbardziej prawdopodobnym scenariuszem dla dalszego losu bitcoina staje się zatem: samolikwidacja i ewentualna wymiana promocyjna na nową lepszą kryptowalutę, lub przejęcie potencjału tej technologii przez uznanego emitenta centralnego.