

Bitcoin dla początkujących

30 września 2013

Zrozumienie Bitcoina wymaga zrozumienia ograniczeń naszych możliwości wyobrażenia sobie przyszłości, jaką może stworzyć rynek.

Na przykład, gdyby trzydzieści lat temu ktoś powiedział, że elektroniczny tekst – znaki przelatujące przez powietrze i lądujące w spersonalizowanych skrzynkach odbiorczych posiadanych przez każdego z nas, które możemy sprawdzać, kiedy tylko chcemy, o każdej porze dnia i nocy – zastąpi przesyłki polecone, powiedzielibyście pewnie, że to niemożliwe.

Jakby nie patrzeć, nawet Jetsonowie nie mieli e-maili. Elroy przynosił do domu uwagi od nauczyciela na kartce papieru. Mimo to e-mail w dużej mierze zastąpił przesyłki polecone, tak samo jak SMS-y, portale społecznościowe, komunikatory, a nawet wideopoczta przez VoIP zastępują tradycyjne telefony.

Okazuje się, że przyszłość bardzo trudno sobie wyobrazić, zwłaszcza gdy przedsiębiorcy specjalizują się w zaskakiwaniu nas wynalazkami. Rynek zawsze potrafi przechytrzyć nawet największych marzycieli, a są oni na pewno mądrzejsi niż intelektualiści, którzy wciąż powtarzają: to i to jest niemożliwe.

Tak samo jest dzisiaj. A co, jeśli zasugeruję, że pieniądz elektroniczny może w końcu zastąpić rządowy pieniądz papierowy? Wiadomo, że potrzebujemy zmiany.

ROZWIĄZYWANIE PROBLEMÓW BAJT PO BAJCIE

Pieniądz we współczesnych czasach zaczynał jako złoto i srebro kontrolowane przez posiadaczy i użytkowników. Następnie politycy się do niego dorwali – i patrzcie, co zrobili. Dziś pieniądz nie jest zakorzeniony w niczym, a jego wartość podlega zachciankom polityków, biurokratów od spraw

pieniężnych i gospodarce planowej. Ten system nie jest zbyt nowoczesny, biorąc pod uwagę obecny świat, w którym rynek kieruje innowacjami w innych aspektach naszego życia codziennego.

Może to tylko kwestia czasu. Nie można zaprzeczyć stronie praktycznej: gracze potrzebowali żetonów, którymi mogliby handlować. Cyfrowe nieruchomości musiały być kupowane i sprzedawane. Pieniądz stawał się coraz bardziej spekulatywny wraz z cyfrowymi przelewami, bankowymi systemami komputerowymi i kartami sieciowymi umożliwiającymi przemieszczanie się „pieniędzy”. Cały świat powoli migrował do sfery cyfrowej, ale tradycyjne pieniądze były przywiązane do ziemi, do skarbców należących do rządów lub kontrolowanych przez nie.

Maniacy komputerowi zajęli się pracą nad tym problemem w latach 90. i stworzyli wiele prototypów – Ecash, bit gold, RPOW, b-money, ale każdy z nich załamywał się z tego samego powodu. Ich dostawa nie mogła być ograniczona, a nikt nie mógł wymyślić, jak spowodować, by niemożliwe było podwójne lub potrójne wydawanie. Zazwyczaj powtarzalność to wspinała rzecz. Możesz wysłać mi zdjęcie i nadal je mieć. Możesz wysłać mi piosenkę i nie stracić swojej. Internet umożliwił nieskończone kopiowanie, co jest świetne, jeśli chodzi o media i SMS-y lub nawet przedmioty (dzięki drukowaniu 3D). Jednakże powtarzalność nie jest cechą, która służy środkowi wymiany.

Jakby nie było, waluta jest nieprzydatna, jeśli nie jest ograniczona, a jej reproduktywność starannie kontrolowana. Pomyśl o systemie waluty złotej. Na świecie jest określona ilość złota, która zaczyna okres eksploatacji tylko dzięki ciężkiej pracy i realnym wydatkom. Złoto musi być wydobywane. Kiedy mam uncję, ty nie możesz mieć jej w tym samym czasie. Jak taki sam system może być odtworzony w sferze cyfrowej? Jak można przypisać nazwy do zamiennego cyfrowego dobra i upewnić się, że te nazwy będą zupełnie przyklejone do danej własności?

PODĄŻAJ ZA PIENIĘDZMI

W końcu to się stało. W 2008 roku człowiek znany jako „Satoshi Nakamoto” stworzył Bitcoina. Nie był pierwszym, który rozwiązał problem podwójnego wydawania. Zrobiła to waluta zwana e-gold, ale wadą była centralna jednostka u władzy, której użytkownicy musieli zaufać. Bitcoin usunął ten znaczący defekt, umożliwiając „górnikom”, by sami sprawdzali rejestr transakcji. Spowodował, że każdy użytkownik ściągnął księgę handlową wszystkich możliwych bitcoinów po to, żeby wszystkie uprawnienia mogły być sprawdzone i nieużywane więcej niż raz w tym samym czasie. Każda moneta miała właściciela, a system nie mógł być oszukany.

Następnie Nakamoto opracował system wydobywania, który stara się naśladować system waluty złotej. Równania, jakie musisz rozwiązać, stają się trudniejsze z biegiem czasu. Pierwsi twórcy mieli łatwo, tak jak wcześni wydobywcy złota, którzy mogli wyławiać je z rzeki, podczas gdy później musieli wydobywać je już z gór. Nakamoto ustanowił limit monet, jakie mogą być wydobyte (21 milionów do 2140 roku). (Nowa moneta jest obecnie wydobywana co mniej więcej 20 sekund, a transakcje odbywają się co sekundę).

Upublicznił i udostępnił swój kod wszystkim godnym zaufania. A system płatności wykorzystywał najbardziej zaawansowane szyfrowanie z kluczami jawnymi, widocznymi dla wszystkich i systemem szyfrującym, który sprawia, że jego połączenie do klucza prywatnego jest niemożliwe do wykrycia.

Nikt nie będzie władać systemem – wszyscy będą mogli nim władać. To właśnie oznacza upubliczniony kod źródłowy. Jest to ta sama dynamika, która spowodowała, że WordPress stał się elektrownią w społeczności software. Nie ma potrzeby dla kontroli finansowej Bitcoin. Zaufanie, anonimowość, szybkość, ścisłe prawa własnościowe i możliwość wprowadzenia zastosowań dla istniejącej już infrastruktury sprawiły, że jest to system doskonały.

Bitcoin wystartował 1 listopada 2008 roku. Aby w pełni docenić

znaczenie tego faktu, należy wziąć pod uwagę tamte czasy. Cała polityczna i finansowa władza była w załamaniu na pełną skalę. Rynki nieruchomości upadły, ciągnąc w dół bilanse dużych banków. Banki inwestycyjne pozbywały się zabezpieczeń hipotecznych z wyjątkową prędkością. Statki transportowe nie mogły opuścić wybrzeży, bo nie były w stanie znaleźć poręczycieli dla swoich papierów ubezpieczeniowych. Przez chwilę wydawało się, że świat się kończy. Republikanie władali Białym Domem, ale nieprawdopodobne rzeczy wciąż się działy. Rząd i banki centralne zdecydowały się na ratowanie całego systemu, wydając i tworząc biliony w nowych papierowych banknotach, by wypełnić skarbce.

Było jasne, że rządowy pieniądz upadał. Cyfrowa alternatywa musiała powstać. Ale co nadało bitcoinowi jego wartość? Istniało kilka czynników. Nie był związany z żadną z istniejących walut, więc mógł mieć płynny kurs ustalany zgodnie z ludzką oceną. Został stworzony z konkretów: tych jedynek i zer, które napędzały światową gospodarkę rynkową. Podczas gdy jedynek i zera mogą być reprodukowane do nieskończoności, nowe monety nie mogły, a to dzięki systemowi, w którym moneta i jej klucz publiczny były ściśle kontrolowane, a księga rachunkowa uaktualniana przy każdej transakcji. Poprawność zapisów mogły być ciągle sprawdzane dzięki natychmiastowej konwersji na inne waluty, podobnie jak na towary i usługi. Ten model wydawał się nieprzenikliwy – pierwsza cyfrowa waluta rozwiązująca wszystkie problemy, które doprowadziły do zagłady poprzednich prób.

MÓJ WŁASNY BITCOIN

Przyśpieszmy w czasie do marca 2013 roku. Stałem się dumnym posiadaczem mojego pierwszego bitcoina. Mój portfel istniał na moim smartfonie. Zaledwie trzy lata temu kilka wspaniałych aplikacji zajmowało się walutami. Mimo, że jestem trochę technologicznie zorientowany, nie jestem żadnym geniuszem i mam całkowitą pewność, że to by mnie przerosło. Ale w ten oto sposób cyfrowe instytucje stały się bardziej przyjazne

użytkownikowi. Przy tej samej okazji, gdy zostałem posiadaczem bitcoina, użyłem bankomatu Bitcoin. Włożyłem kilka banknotów, przyłożyłem mój cyfrowy portfel do skanera i poczułem wibrację na moim smartfonie. Fizyczne stało się cyfrowe. Pięknie.

Jednak nadal zastanawiałem się, co właściwie mogę zrobić z tym wszystkim. Wtedy konsumencki świat produktów Bitcoin pojawił się przede mną. Nie mówimy tu tylko o Silk Road – stronie, która stała się znana z umożliwiania łatwego, anonimowego kupna i sprzedaży narkotyków. Sklepy Bitcoin są wszędzie. Istnieją też usługi, które możesz kupić z każdej strony z interfejsem Bitcoin. Mówono o bitcoinowych rynkach transakcji terminowych. Chodziły plotki, że niektóre firmy wejdą na giełdę używając bitcoinów, tym samym omijając całkowicie SEC. Zastosowania są niesamowite.

ŚWIĘTE SZCZYPCE

Mimo wszystko, jestem dotykowcem. Muszę doświadczać rzeczy. Wszedłem więc na jedną z tych stron. Kupiłem pierwszy produkt jaki widziałem (dlaczego? – nie wiem). Były to szczypce do zaciskania kabli elektrycznych. Podałem swój adres wysyłkowy i pojawiła się informacja, że trzeba zapłacić. To był moment, na który czekałem. Kod QR – ten śmieszny kwadratowy wzorek, który wygląda jak kod kreskowy 3-D – wyskoczył na ekranie. Podniosłem mój „portfel” i zeskanowałem go. W mniej niż 2 sekundy transakcja została dokonana. To było prostsze niż system zamawiania przez jedno kliknięcie Amazona. Moje serce biło szybciej. Wyskoczyłem z krzesła, zaśpiewałem i zatańczyłem wokół pokoju. W jakiś sposób zrozumiałem to całkowicie po raz pierwszy: to właśnie przyszłość.

Szczypce dotarły dwa dni później i mimo to, że nie mam do czego ich używać, bardzo je cenię.

Bitcoin już wystartował, gdy uderzył niespodziewany kryzys na Cyprze. Rząd mówił o zajmowaniu depozytów bankowych jako sposobie na pomoc całemu systemowi. Podczas tego okresu

bitcoiny w zasadzie podwoiły swoją wartość. Reportaże prasowe twierdziły, że ludzie wycofywali walutę państwową i zamieniali ją, nie tylko na Cyprze, ale i w Hiszpanii, Włoszech i wszędzie indziej. Cena bitcoinów w dolarach wzrosła. Mówiąc innymi słowami, cena towarów i usług w bitcoinach malała. Tak, to ten straszliwy system, który potępiany jest przez mainstreamowych ekonomistów jako „deflacja”. Słynny keynesista Paul Krugman poszedł nawet dalej mówiąc, że najgorszą rzeczą w Bitcoinie jest to, że ludzie gromadzą je, a nie wydają, tym samym powtarzając system waluty złotej, którego nienawidzi najbardziej!

OBSESJA I URAZ

Moje własne doświadczenie z Bitcoin podczas tego czasu nasiliło się. Zacząłem dzwonić do przyjaciół na Skypie, skanować ich kody QR i wymieniać waluty. Zacząłem wciągać innych w moją obsesję opartą na moim doświadczeniu – musisz posiadać, by uwierzyć. Po jednym całym dniu kupowania, sprzedawania i używania bitcoinów, miałem dziwne uczucie żalu, że muszę zapłacić za taksówkę w starych zwykłych dolarach.

Jak zdobyć bitcoiny? Proces może być trochę skomplikowany. Możesz znaleźć na localbitcoin.com osobę w okolicy, która wymieni twoje pieniądze na bitcoiny. Zazwyczaj takie wymiany dokonują się przy dużych premiach od 10 do 50 procent, zależnie od tego, jak konkurencyjny jest lokalny rynek. To zrozumiałe, że ludzie mają opory przed zrobieniem tego, nieważne jak bezpieczna jest transakcja. Jest coś podejrzanego w spotkaniu z nieznajomym w całodobowej kawiarni w celu dokonania niezwyklej wymiany cyfrowej waluty.

Bardziej konwencjonalnym sposobem jest znalezienie jednego z wielu sprzedawców w Internecie, podpięcie swojego konta bankowego i kupowanie. Ten proces może zająć kilka dni. Wtedy, kiedy zaczynasz przesyłać swoje środki, możesz być zaskoczony limitami na rynku, które obecnie istnieją. Portale internetowe racjonują sprzedawanie bitcoinów, na podstawie dostępności,

biorąc pod uwagę tylko wysoki popyt. Może zając 10 dni lub więcej, by z nieposiadacza stać się posiadaczem. Ale kiedy już je masz, możesz ruszać. Wysyłanie i otrzymywanie pieniędzy nigdy nie było prostsze.

WĄTPLIWOŚCI?

W czasie pisania tego tekstu, jedna moneta bitcoin kosztowała 88,249 dolarów (cena następnie wzrosła do 250 dolarów, po czym opadła znów do mniej więcej 90 dolarów w momencie publikacji – przyp. red. Freeman). Zaledwie trzy lata temu wynosiła 0,14 dolara. Wielu ludzi patrzy na rynek walut i myśli: „to na pewno bańka spekulacyjna”. To może być prawda, choć nie musi. Ludzie wymieniają niestabilne, puste pieniądze na coś z prawdziwym aktem własności, co nie może zostać zduplikowane. Każdy wie, ile dokładnie bitcoinów istnieje w dowolnym momencie. Każdy może obserwować transakcje odbywające się w czasie rzeczywistym. Cena bitcoina może iść w górę i w dół, i to jest w porządku, ale nie ma prawdziwych spekulacji, które są endogenne dla rynku Bitcoina.

Czy to piramida finansowa? Cechą charakterystyczną piramidy finansowej jest to, że więcej osób niż jedna ma takie same roszczenia do tych samych pieniędzy lub towarów. To fizycznie niemożliwe w Bitcoinie. Sposób, w jaki program jest zaprojektowany, przewiduje reżim surowego prawa własnościowego bez wyjątków. Na początku marca pojawiła się niewielka przeszkoda w systemie, kiedy nowe monety były zatwierdzone przez jedną grupę programistów, a przez inną nie. Pojawiło się rozwidlenie w systemie. Ceny zaczęły opadać. Programiści szybko pracowali, by rozwiązać konflikt, i w końcu system oraz ceny wróciły do normy. Taka jest zaleta upublicznionego kodu źródłowego.

A co z poczuciem niepewności niektórych ludzi co do tego, że kilkoro programistów, na własną rękę, może stworzyć nową walutę? Jeśli spojrzycie na to, co mówił austriacki teoretyk monetarny Carl Menger, to wskazywał on na podobny proces,

dzięki któremu powstała waluta złota. Żadna nowa waluta nie jest początkowo używana przez wszystkich. Na początku korzystają z niej tylko „najbardziej wnikliwe, zdolne i oszczędne jednostki”. Ich pomysłyne działanie jest następnie naśladowane przez innych. Innymi słowy, powstanie pieniądza wymaga przedsiębiorczości – to znaczy bycia otwartym na możliwość odkrywania i dostarczenia czegoś nowego.

LEWIATAN ŁYPIE OKIEM

A co z interwencją rządu? Nie ma wątpliwości, że będą podejmowane takie działania. Już teraz agencje rządowe wyrażają pewien stopień zniecierpliwienia co do tego, co może się stać. Jednak rządy nie były w stanie kontrolować gospodarki gotówkowej. Byłoby niewyobrażalnie bardziej trudne kontrolować cyfrową walutę, bez banku centralnego, z szyfrowaniem i milionem użytkowników każdego dnia. Taka kontrola byłaby nie do pomyślenia.

Kiedyś pomyślałem, że e-booki zastąpią książki papierowe, był absurdem. Kiedy po raz pierwszy patrzyłem na wczesne generacje e-czytników, śmiałem się i szydziłem. Teraz szukam nowego domu dla moich papierowych książek i ściągam setki e-booków. W ten oto sposób rynek nas zaskakuje. Technologia bez gospodarki planowej spełnia marzenia.

Możliwe, że Bitcoin upadnie. Może to tylko pierwsza generacja. Może tysiące ludzi zostanie ogołoconych już przy pierwszej okazji. Ale czy nadchodzi cyfryzacja pieniędzy? Oczywiście. Czy znajdą się jacyś sceptycy? Oczywiście. Jednak w tym przypadku nie mają władzy. Rynek będzie robił to, co robi, budując przyszłość, czy się z tym zgadzamy lub rozumiemy to w pełni, czy nie. Przyszłość się nie zatrzyma.

Autor: Jeffrey A. Tucker

Tłumaczenie: Maja Świrko

Źródło oryginalne: [Freeman](#)

Źródło polskie: [Instytut Misesa](#)