Czym jest Bitcoin? Co w tym takiego nowego?

Bitcoin jest zdecentralizowaną cyfrową walutą peer to peer. Wykorzystuje zaawansowaną matematykę i kryptografię krzywej eliptycznej, a także globalnie replikowaną księgę publiczną o nazwie Blockchain. Bitcoin został opracowany w 2008 roku i po raz pierwszy wprowadzony przez Satoshi Nakamoto w 2009 roku. Satoshi jest uważany za pseudonim, a społeczność Bitcoinów nie słyszała od niego nic od 2010 roku. To historia pochodzenia godna fabuły komiksu: tajemnicza kryptografia, geniusz rozwija zupełnie nową walutę, która może zmienić globalny krajobraz finansowy, publikuje białą księgę wyjaśniającą technologię, a następnie całkowicie znika z dyskusji, ponieważ zaczyna zyskiwać akceptację. Jest kilka rzeczy, które Bitcoin osiąga, co wcześniej nie było możliwe w e-walucie.

OK. Jakie są te rzeczy?

Bitcoin uniemożliwia (lub prawie uniemożliwia) dokonywanie podwójnych transakcji - innymi słowy, gdy pieniądze opuszczają twoją własność, nie są już twoje. Było to ogromne wyzwanie związane z cyfrową walutą, ponieważ na przykład, gdy wysyłasz znajomemu plik muzyczny, jak to zrobić, aby plik już nie istniał na twoim komputerze? Podczas transakcji w walucie cyfrowej konieczne jest, aby pieniądze pozostawiały w twoich rękach i trafiały do strony odbierającej - użytkownik nie może mieć możliwości wydawania pieniędzy więcej niż raz. Jest to jeden z powodów, dla których bitcoin jest często opisywany przez prasę jako „gotówka cyfrowa" - posiadacz ma nad nim pełną kontrolę i trwale traci kontrolę, gdy daje go innej stronie. Transakcje są nieodwracalne. Bitcoin zapewnia również niemal natychmiastowe (w ciągu 10 do 30 minut) niezaprzeczalne potwierdzenie, że twoje pieniądze zostały odebrane lub wysłane. Nie martw się o odbite czeki. Bitcoin również jest niemożliwy do podrobienia; transakcja gotówkowa lub transakcja złotem może zawierać fałszywe rachunki lub fałszywe złoto. Nie ma czegoś takiego jak fałszywy Bitcoin. Ponadto nie ma przedłużonego okresu rozliczeniowego. Gdy transakcja zostanie potwierdzona przez akceptowalną liczbę węzłów w sieci, pieniądze są naprawdę twoje. I wreszcie, ponieważ wszystkie transakcje są wymienione w globalnej księdze publicznej znanej jako Blockchain, Bitcoin zapewnia nieocenioną obronę przed bzdurami „wielkiego kapelusza, bez bydła". Innymi słowy, jeśli planujesz robić interesy z kimś, kto twierdzi, że ma X pieniędzy - zamiast wierzyć na słowo lub rodzaj zegarka, który nosi lub jeździ samochodem, lub jego historię kredytową itp.,

osoba fizyczna może po prostu podać adres publiczny, aby zobaczyć jej saldo. W ciągu kilku sekund wiesz, czy strona ma pieniądze, czy nie.

Bitcoin nie ma wewnętrznej wartości, dlaczego ludzie go akceptują jako walutę?

Nic we wszechświecie fizycznym nie ma wartości „wewnętrznej". Złoto jest metalem, który ludzie uznali za wartość transakcyjną ze względu na jego niedobór i interesujące właściwości fizyczne (nie utlenia się, ładny i ciężki, wygląda ładnie, dobrze przewodzi prąd). Dolar amerykański jest kartką papieru lub cyframi popartymi jedynie „wiarą i kredytem" rządu USA - w publicznym zaufaniu, że rząd może spłacić swoje długi i wywiązać się z wszelkich zobowiązań. Kiedy ludzie twierdzą, że Bitcoin nie ma wewnętrznej wartości, zwykle próbują powiedzieć: „Nie lubię Bitcoina". I dobrze jest mieć osobiste preferencje dotyczące czegoś, o ile uznajesz, że twoja osobista wiara nie pokrywa się z rzeczywistą wartością waluty. Bitcoin ma wartość, ponieważ ludzie chcą go kupować i sprzedawać po określonej cenie. Ten rynek jest płynny dzięki wielu wymianom.Bitcoin jest również akceptowany przez coraz większą liczbę firm i pracowników jako formę płatności. Słyszałem w mediach opowieści grozy o kradzieży, zagubieniu monet itp.

Myślałem, że to jest bezpieczne?

Bitcoin to prawdziwie cyfrowa gotówka. Gdybyś zostawił plecak wypełniony gotówką w centrum handlowym, a jeśli ten plecak miałby zabrać jakiś nieznajomy, to już nie byłby twój. Podobnie, gdybyś podłożył milion dolarów pod kuchenną podłogę, a twój dom spłonął, nie miałbyś już tych pieniędzy. Kto trzyma klucze prywatne do monet w portfelua, kontroluje te monety. Gdy klucze prywatne zostaną zgubione lub zniszczone, pieniądze zostaną utracone. Cóż, to nie brzmi zabawnie. Przypomnij mi, dlaczego to dobrze? Nie ma organu centralnego, żadnej firmy ani rządu. Jeśli kupujesz coś za pomocą karty kredytowej, jeśli nie jesteś zadowolony (na przykład produkt nie dotrze zgodnie z obietnicą), możesz odwołać się do firmy obsługującej karty i zainicjować ewentualne obciążenie zwrotne. Zapewnia to konsumentom warstwę komfortu, a komfort jest finansowany z wysokich opłat transakcyjnych kupców (nawet 2 do 3 procent całkowitej kwoty), a także takich rzeczy jak opłaty roczne, wysokie stopy procentowe itp. Bank musi zapłacić za koszty wsparcia, jak również odpowiedzialność finansową (koszty obciążenia zwrotnego, nieautoryzowane transakcje, kradzież tożsamości i tak dalej). Ponadto bank musi płacić koszty marketingu, aby utrzymać rentowność. Z Bitcoinem, podobnie jak z pocztą

elektroniczną, nie ma żadnej firmy. Jest to globalny protokół wysyłania i odbierania pieniędzy. Koszty transakcji to niewielki ułamek istniejących opłat za transakcje bankowe. Nieodwracalny charakter Bitcoinów obniża koszty, ponieważ akceptanci nie ponoszą ryzyka obciążeń zwrotnych ani nieuczciwych transakcji. Czy pierwsi użytkownicy nie dostali dużo monet ze względną łatwością? Jak to jest sprawiedliwe? Czym różni się to od „piramidy”? Tak, górnicy (ci, którzy uruchamiają oprogramowanie na swoich komputerach, aby utrzymać funkcjonowanie sieci Bitcoin) generują monety z biegiem czasu - na początku monety te były produkowane ze względną łatwością i z czasem coraz mniej monet jest produkowanych, a proces staje się bardziej trudny. Podobnie pierwsi użytkownicy mogli kupować monety już za 0,01 USD. Warto zauważyć, że Bitcoin nie zawsze był złotym standardem e-waluty. Jeszcze w maju 2010 r. 10 000 monet mogło ci kupić pizzę. A górnicy byli uważani przez wielu za łatwowiernych kretynów, rozdających cenne zasoby komputerowe w zamian za „fałszywe pieniądze internetowe”, których nikt nie akceptował ani o które nie dbał. To naturalne, że ci, którzy ryzykują stworzenie lub posiadanie Bitcoinów na wczesnym etapie procesu, powinni zobaczyć zwrot z „inwestycji”. Wiele z tych osób nie gromadziło monet, ale raczej kupowało je przez Internet lub sprzedawało po cenach znacznie poniżej dzisiejszej wartości rynkowej - gdy coś kosztuje 0,01 USD, cena 10 USD wydaje się atrakcyjna. Istnieją dowody na to, że własność monet jest mniej skoncentrowana niż na początku. Ponadto każdy może zostać górnikiem lub kupić monety. Nie był to zamknięty klub z wtajemniczonymi - po prostu większość społeczeństwa nie wierzyła w ten pomysł

Czy możesz wyjaśnić, jak to jest sprawiedliwe? Niektórzy ludzie mają o wiele więcej niż inni.

Bitcoin jest matematycznie czysty i każdy może odczytać kod źródłowy, który sprawia, że system działa. Nie jest zastrzeżony i żadna osoba ani jednostka nie może nadmuchać rynku, tworząc nowe monety z powietrza (jak zrobiłby to bank centralny). Utworzenie Bitcoina odbywa się według matematycznego „harmonogramu” i do połowy następnego stulecia uzupełni 21 milionów monet. Niedobór ten gwarantuje, że siła nabywcza jednostki i jej przechowywana wartość nie zostaną osłabione decyzją polityka, by wydrukować więcej waluty (to jest pomysł przynajmniej). Nikt nie może zdecydować się na wydrukowanie większej liczby bitcoinów.

Czy pierwsi użytkownicy będą bogaci?

Na podstawie moich badań z pewnością możliwe jest, że pierwsi odbiorcy staną się miliarderami - jeśli Bitcoin stanie się światowym standardem dla transakcji cyfrowych w taki sam sposób, w jaki e-mail stał się światowym standardem komunikacji cyfrowej, taki wynik nie jest śmieszny. Możliwe jest również, że pierwsi użytkownicy stracą do 100% swojej „inwestycji", jeśli Bitcoin zostanie zagrożony w krytyczny sposób lub jeśli zainteresowanie opinii publicznej szybko zmieni się na nieznany jeszcze alternatywny protokół. Oprócz odwołania jako alternatywy dla kart Visa, MasterCard i PayPal, niektórzy użytkownicy Bitcoinów twierdzą, że pomaga to chronić ich pieniądze przed inflacją. Czy możesz wyjaśnić, o co tu chodzi? Inflacja jest jednym z najstarszych problemów, przed którymi stoi każda waluta wydana przez rząd lub organ centralny. Starożytni Rzymianie to zrobili, Chińczycy to zrobili, Amerykanie (i prawie wszyscy inni) robią to dzisiaj. Prowokowanie inflacji jest bardzo kuszące dla establishmentu, ponieważ pozwala na a) subtelny podatek od bogactwa obywateli b) finansowanie projektów publicznych - dróg, opieki zdrowotnej, wojen - które w innym przypadku byłyby ekonomicznie niemożliwe do zrealizowania. Artykuł z popularnego bloga finansowego Zero Hedge sprzed kilku lat podsumowuje całkiem dobrze praktykę dewaluacji waluty, ściśle związaną z inflacją:

„… Jak większość monetarystów wie zbyt dobrze, to Rzymianie zaangażowali się w pierwszy akt dobrowolnej dewaluacji waluty - rozwodnienie, poprzez stopniowe zmniejszanie zawartości srebra (tak, nawet wtedy waluty były wspierane przez metale szlachetne: i zgadnij, co - żadne CDO do kwadratu, sześciennego lub kwadratowego, nie zostały stworzone przez lokalne biuro Goldmanus Sachus) aż do momentu, gdy osiągnie zero. .. i imperium rzymskiego już nie było. Jak na ironię, prawie 100% dewaluacja waluty w czasach rzymskich zajęła nieco ponad 2 wieki. Porównuje to nieco korzystne dla 97% spadku siły nabywczej amerykańskiej waluty od początku istnienia Rezerwy Federalnej„. Więc, jak widzisz, to, co dziś robi nasz rząd, rzadko kwalifikuje się jako nowa praktyka. Starożytni Rzymianie, niestety, nie miał Internetu i zdecentralizowanej waluty, aby zabezpieczyć się przed rozwodnieniem waluty. Jeśli masz 1000 dolarów na koncie bankowym, nadal masz 1000 dolarów na tym koncie w przyszłym roku - ale rzeczywista wartość tych pieniędzy, siła nabywcza, może się zmniejszyć zasadniczo. Kiedy Rezerwa Federalna zdecyduje się wydrukować więcej pieniędzy, istnieje większa podaż dolara za taką samą ilość popytu, dlatego twoje pieniądze stają się nieco mniej specjalne, warte trochę mniej, co jednak pomaga rządowi i innym dłużnikom spłacić swoje długi - wciąż mają tę samą kwotę nominalną, dopiero teraz mogą spłacić dług w dolarach wart mniej.

Czy tak się nie stanie z Bitcoinem?

Nie. Żaden cesarz, kanclerz ani przewodniczący Rezerwy Federalnej nie może arbitralnie decydować o zmniejszeniu wartości każdego Bitcoina w nadziei „stymulowania gospodarki" lub finansowanie wojny lub poszerzanie programów opieki społecznej. Maksymalna liczba Bitcoinów to 21 milionów w połowie 22 wieku. Ten limit jest zapiekany w matematyczne modele, które uruchamiają Bitcoin. W tej chwili nieco ponad 12 milionów monet zostało „wydobyte" i wprowadzone do użytku na świecie.

Cholera. Rząd będzie wtedy próbował to zamknąć, prawda?

Artykuł na stronie internetowej NBC News zauważył ostatnio, że Bitcoin zyskał w tym roku ponad 7600% wartości. „Wielu analityków i inwestorów określiło nieskrępowany wzrost bitcoinów bańką, jednak większa świadomość walut cyfrowych i zeszłotygodniowa aprobata senatu USA utorowała drogę do nowych zysków" - czytamy w artykule. Właśnie tak: przesłuchanie w Senacie USA było zaskakująco pozytywne i rozsądne. Dla kogoś, kto ostatnio był dość krytyczny wobec reakcyjnego podejścia Kongresu do technologii internetowych, byłem zadowolony - właściwie zdumiony! - że funkcjonariusze organów ścigania i wybrani członkowie przedstawili tak trzeźwe i rozsądne oceny tego, czym jest Bitcoin, a czego nie. To była największa chmura nad głową cyfrowej waluty: czy rząd USA wyceluje w Bitcoin i zamknie go? Odpowiedź brzmi, najwyraźniej, nie. Kolejne fantastyczne szczęście, które przeszło na drogę Bitcoina w listopadzie: BTC China przełączyło się na internet, giełdę Bitcoinów w Chinach kontynentalnych, a odpowiedź chińskich konsumentów była KUPUJ, KUPUJ, KUPUJ. Większość nowych zamówień Bitcoinów pochodzi z Chin, a nie z Zachodu. Chińczycy, podobnie jak my, mają dużą populację klasy średniej, chcącą się urozmaicić - chcą, aby ich ciężko zarobione pieniądze przetrwały wszelkie regionalne burze gospodarcze. Utrzymywanie wszystkich swoich pieniędzy w dolarach amerykańskich, chińskim juanie lub frankach szwajcarskich… to finansowy odpowiednik „wszystkich twoich jaj w jednym koszyku". Coś może pójść nie tak. Jest też cały problem z inflacją!

Kupno, sprzedaż, zabezpieczenie

Bitcoin składa się z adresu publicznego i odpowiedniego klucza prywatnego. Nowy adres i odpowiadający mu klucz prywatny można utworzyć za pomocą jednego kliknięcia, tyle razy, ile chcesz dla nowych transakcji. Pomyśl o adresie publicznym jako adresie pocztowym, jeśli ktoś wyśle ci czek pocztą. Adres publiczny jest tym, co chcesz dać każdemu, kto planuje wysłać ci pieniądze. I pomyśl o kluczu prywatnym jako kombinacji ze skrzynką pocztową, w której otrzymujesz czek. Nigdy nie udostępniaj nikomu swojego prywatnego klucza ani nie publikuj go.

Pozwólcie, że powtórzę, że: NIGDY NIE DZIEL SIĘ LUB POCZTAJ SWOJEGO PRYWATNEGO KLUCZA.

W rzeczywistości za każdym razem, gdy na komputerze przechowywane są klucze prywatne, komputer ten (najlepiej) nigdy nie powinien być online - a jeśli musi być w trybie online, te klucze prywatne powinny być przechowywane w folderze chronionym hasłem. I to hasło powinno być długie i słone. (tj. zamiast 21mydogsname, twoje hasło może być solone jako takie: mYd0gznAm3!).

Bezpieczeństwo portfela jest jednym z najważniejszych aspektów opanowywania Bitcoinów, a niepowodzenie w odrabianiu zadań domowych przed załadowaniem pieniędzy do portfela może doprowadzić do katastrofy - podobnie jak w przypadku wielu nowych użytkowników. To bolesne zobaczyć te historie o ruinach na forach Bitcoin. Prawie wszystkie z nich można było łatwo uniknąć. Przechowując Bitcoin, należy użyć klienta portfela na własnym komputerze - głównych internetowych portfelach Bitcoin, którym po prostu nie zaufałbym niczego ponad bardzo trywialną sumą pieniędzy. Firmy są zbyt nowe i malują cel na swoich plecach, mając tak wiele łącznego bogactwa w jednej usłudze. Największe hostowane usługi portfelowe bez wątpienia mają hakerów próbujących znaleźć lukę przez całą dobę, 365 dni w roku. A ta firma musi tylko dać upust swojej milisekundzie, aby stracić większość lub wszystkie zasoby swoich klientów. Podczas gdy klient portfela na twoim komputerze to tylko jeden cel, a hackerzy powinni być tego świadomi. Spośród wszystkich klientów portfela, których wypróbowałem, Electrum jest najlepszym - ładnym połączeniem łatwości użycia, prostoty i bezpieczeństwa. Przeczytaj dokumentację na temat Electrum na Electrum.org. Klientem jest bezpłatne oprogramowanie open-source, które można również pobrać z tej strony internetowej. W idealnej sytuacji należy odłączyć komputer od Internetu po pierwszym uruchomieniu Electrum. Przy pierwszym uruchomieniu Electrum zapewnia on zalążek portfela podczas procesu konfiguracji. Jest to fenomenalnie

ważne i zostanie wyjaśnione za chwilę, więc chcesz zrobić wszystko, co w twojej mocy, aby zapobiec naruszeniu tego zasobu portfela przez złośliwe oprogramowanie keyloggera lub złośliwe oprogramowanie, które robi zrzuty ekranu. Jeśli Twój komputer był używany do surfowania po Internecie przez jakiś czas, jest wysoce prawdopodobne, że komputer zawiera na nim złośliwe oprogramowanie. „Nie ja, chodzę tylko na bezpieczne strony internetowe!" Tak, ty, ja, prawie każdy. Oprogramowanie jest szalenie rozpowszechnione na komputerach osobistych. W niedawnej przeszłości takie złośliwe oprogramowanie było zwykle wykorzystywane do takich celów, jak spam, serwowanie niechcianych reklam itp. Jednak w miarę wzrostu wartości i akceptacji Bitcoinów, motywuje on twórców szkodliwego oprogramowania do sniffowania monet. Zasób, który można natychmiast skraść, jest kuszący dla ludzi, którzy projektują złośliwe oprogramowanie. Jeśli planujesz załadować znaczną ilość pieniędzy na swój portfel, powinieneś wyjść i kupić dedykowany nowy komputer, który nigdy nie dotyka Internetu. Możesz kupić przyzwoity laptop lub netbook w niższej cenie za mniej niż 400 USD już dziś. „Czas na mobilność!" jak powiedziałby Bane… Kiedy tworzysz portfel Bitcoin, który nigdy nie jest online, nazywa się to „zimnym portfelem". Zimny portfel, jeśli jest prawidłowo skonfigurowany, nie może stracić monet, ale może wygenerować nowe adresy publiczne, które będą rozdawać osobom, które chcą Ci wysłać pieniądze. Portfel podłączony do Internetu, który może wysyłać monety, a także generować adresy publiczne, nazywany jest „gorącym portfelem". Wszystko to jest dobrze wyjaśnione na stronie internetowej Electrum. Innym dobrym zasobem jest http://reddit.com/r/bitcoinbeginners. Jeśli zadasz pytanie, pamiętaj, że bez względu na to, co ktoś powie.

NIE PODWAJ ŻADNYCH swoich kluczy prywatnych i NIE DAJ IM ŻADNYCH nasion portfela.

Każdy, kto ma jedną z tych rzeczy, może wydać swoje monety - to tak, jakbyś dał im hasło do swojego konta bankowego. Drakońskie środki bezpieczeństwa nie są tak ważne w przypadku małych ilości bitcoinów - powiedzmy, wystarczy kupić używaną książkę lub telewizor na Craigslist. Ale kiedy kwoty są gromadzone w większych ilościach w nadziei, że uda ci się zapewnić twoim spadkobiercom lub sobie w przyszłości (co niektórzy robią; więcej o tym później) - musisz być „produktywnie paranoiczny". Pomyśl jako złodziej Bitcoinów: gdyby coś mogło zostać naruszone, będzie. Jeśli coś mogło zostać wystawione na działanie osoby trzeciej, załóżmy, że tak było i postępuj zgodnie z nimi. Przenieś swoje pieniądze na nowy adres publiczny, po upewnieniu się, że klucz prywatny został

odpowiednio zapisany. Utwórz kopię zapasową tego klucza prywatnego (lub zapamiętaj zalążek portfela macierzystego). I zabezpieczyć hasłem plik zawierający klucz prywatny.

Ponownie, ta sprawa brzmi trochę dziwnie, ale ponieważ kapitalizacja Bitcoinów wciąż rośnie, a każdy BTC staje się coraz bardziej cenny, zachęta dla twórców szkodliwego oprogramowania jest prawie nieograniczona. Stosunkowo łatwo jest opracować program, który sniffuje plik klucza prywatnego, a jeśli nie jest odpowiednio chroniony hasłem (lub w ogóle nie jest chroniony hasłem), aby połączyć te informacje. Bitcoin to gotówka na erę cyfrową. I tak jak nie umieściłbyś 100 000 dolarów w neonowym opakowaniu fantazyjnym i chodził po zatłoczonym rynku znanym z kradzieży kieszonkowych, tak nie powinieneś grać zbyt szybko i luźno z rutyną bezpieczeństwa Bitcoin. Tak jak w przypadku każdej rutyny, dobre nawyki ustanowione teraz doprowadzą do dobrych nawyków na zawsze. Jest też fascynująca kwestia uznania Bitcoinów; wielu spekulowało (do tej pory poprawnie), że sposób tworzenia Bitcoin prowadzi do presji deflacyjnej w czasie. Innymi słowy, ponieważ uważam, że jutro 1 BTC będzie wart więcej w dolarach amerykańskich (lub euro lub frankach) niż dzisiaj, dlaczego miałbym je dzisiaj wydawać? Poczekam do jutra. I ten sam problem pojawia się jutro. W związku z tym nawet niewielka ilość odłożonych dziś bitcoinów może być odpowiednikiem całorocznej pensji w nieodległej przyszłości. Poza tym wartość Bitcoinów korzysta ze zjawiska, które nazwałem „zgnilizną monet". Z czasem pewien odsetek użytkowników zapomina hasła, traci klucze prywatne lub dyski twarde komputera giną bez odpowiednich kopii zapasowych. Chociaż te pieniądze są nadal częścią ekosystemu Bitcoin w tym sensie, że przyczyniają się do całkowitej kapitalizacji rynkowej waluty, są one faktycznie nieważne: te pieniądze nigdy nie zostaną ponownie wykorzystane w transakcji. Jeśli więc strona chce przeprowadzić transakcję w Bitcoinie, prawdopodobnie kupuje nowsze monety, a nie monety z najwcześniejszych dni Bitcoinów. Mogliśmy dyskutować o intrygujących zaletach i wadach deflacyjnej waluty do końca czasu, ale ostatecznie presja ta ma minimalny wpływ na zdolność Bitcoin do bycia wybranym globalnym protokołem transakcji cyfrowych, ponieważ obie strony mogą wskoczyć i wyjść z Bitcoinów w ciągu kilku sekund dzięki płynności zapewnianej przez giełdy. Lubię myśleć o dolarze amerykańskim jako o „lokalnej walucie" w tym momencie, a Bitcoin jako o rozwijającej się międzynarodowej super walucie. Waluty lokalne nie znikną w najbliższym czasie, ponieważ zapewniają wygodę w regionie, ale w przypadku dużych i małych transakcji międzynarodowych oczywistym wyborem jest Bitcoin. Pomyśl o Bitcoin jako

chmurze dla naszego systemu finansowego i lokalnych walutach, takich jak dyski CD-ROM lub pendrive, które można wykorzystać do regionalnego transportu pieniędzy konsumenta.

Ok, rozumiem. Więc o czym wspomniałeś wcześniej o portfelu? Brzmi poważnie.

Dobre pytanie. Tak więc, wybierając klienta Bitcoin, polecam Electrum, ponieważ zapewnia on eleganckie rozwiązanie problemu śledzenie wszystkich adresów i kluczy prywatnych - przy pierwszym uruchomieniu generuje 12-wyrazowy mnemonik (coś, co zapamiętujesz) na podstawie 128-bitowej entropii (tj. bardzo wysoki stopień losowości komputera). Zapisz ten ciąg 12 słów .Sprawdź dokładnie, czy zapisałeś to poprawnie. Następnie sprawdź jeszcze raz. I innym razem. Jest to jeden z najważniejszych momentów w życiu Bitcoinów, więc warto być ostrożnym tutaj. Po prawidłowym zapisaniu 12 słów mnemonicznych, zapamiętaj je. Możesz zapamiętać to w ciągu kilku dni do tygodnia, wielokrotnie czytając je samemu. A jeszcze łatwiej jest zapamiętać, jeśli użyjesz 12 słów, aby stworzyć zabawną, wizualną historię w umyśle. Po zatwierdzeniu swojego unikalnego mnemonika w pamięci, umieść zapisaną kopię zapasową w bezpiecznym miejscu. Umieść drugą kopię w innym miejscu fizycznym, w torbie Zip-loc na wypadek uszkodzenia przez wodę. Piękną cechą tego portfela jest to, że nawet jeśli stracisz wszystko inne - wszystkie klucze prywatne, hasło, adresy ... lub nawet jeśli dysk twardy komputera ulegnie uszkodzeniu i przestanie działać lub zostanie zniszczony w wyniku pożaru lub trzęsienia ziemi ... możesz natychmiast odzyskać wszystko, wpisując ten portfel do Electrum za pomocą opcji Przywróć. Ziarno portfela jest jedyną informacją, którą musisz zachować, aby zachować kontrolę nad monetami. To intensywne. Jak to działa?

To jest intensywne! Nasiona portfela sprawią, że poczujesz się jak Bitcoinsling

James Bond. Szybko zrozumiesz, że te rzeczy są znacznie bardziej zaawansowane niż bankowość „tradycyjna". W lokalnym oddziale nie ma przyjaznej pani kasjerki, która pomoże ci odzyskać hasło. Zaletą tego jest oczywiście całkowita wolność i całkowity dostęp do własnych pieniędzy. Nasiona portfela działają, ponieważ Electrum tworzy portfel deterministyczny. Wszystkie adresy i klucze prywatne, które ci udostępniają, są generowane z tego materiału siewnego i można je odtworzyć, znając tylko nasiona. Pomyśl o tym jak o zakopanej mapie skarbów. Należy pamiętać, że klucze muszą być generowane natywnie w Electrum, aby mogły zostać zregenerowane przez twoje nasienie. Jeśli na przykład importujesz klucze prywatne z innego miejsca do Electrum, to

oczywiście nie będą one „przechowywane” przez nasienie portfela. Deterministyczne portfele to stosunkowo nowa innowacja w świecie Bitcoin. Oto jak opisuje je Bitcoin Magazine: „W przeciwieństwie do portfeli bitcoin w starym stylu, które generują losowo nowe adresy Bitcoin i klucze prywatne w razie potrzeby, w deterministycznym portfelu wszystkie dane są generowane przy użyciu konkretny algorytm z pojedynczego materiału siewnego. Oznacza to, że jeśli zapiszesz materiał siewny do swojego deterministycznego portfela, a po sześciu miesiącach Twój dysk twardy ulegnie uszkodzeniu, a portfel nieodwracalny, możesz po prostu utworzyć nowy portfel przy użyciu tego samego materiału siewnego a wszystkie adresy i klucze prywatne z twojego starego portfela powrócą dokładnie tak, jak były wcześniej. Ten trend w rozwoju portfela zyskał niemal powszechne uznanie, a prawie każdy klient Bitcoin, który zamierza obsługiwać wiele adresów, albo już ma deterministyczny portfel wdrożony lub planuje go utworzyć. ”

To nie jest ostatnie słowo na temat tworzenia portfela lub zabezpieczenia portfela. Powinieneś poświęcić trochę czasu na czytanie w Internecie na Electrum, a następnie grać tylko w niewielkich ilościach Bitcoinów w portfelu, dopóki nie będziesz pewny jego funkcji i nie spróbujesz zregenerować adresów i wyważyć z nasion przynajmniej raz. W przyszłości mogą pojawić się lepsi klienci portfeli. (Armory to kolejny klient, który został bardzo dobrze przyjęty przez społeczność Bitcoin, ale jest to bardziej złożony klient oferujący absolutnie najwyższy poziom bezpieczeństwa. Dla większości użytkowników prawdopodobnie nie jest to konieczne, ale możesz preferować ten. Fajnie, zacznę eksperymentować z klientami portfela.

Gdzie mogę kupić moje monety ?!

Oto zabawna część. Giełdy Bitcoin pozwalają kupować i sprzedawać monety po cenie rynkowej w czasie rzeczywistym plus opłata za wymianę. Miałem mieszane doświadczenia z wymianami - niektóre z nich rosną po prostu zbyt szybko, aby zapewnić niezawodne, profesjonalne usługi. Jedyną doskonałą, z której korzystałem do tej pory, czyli niezawodnie niezawodną, jest Coinbase. Mają siedzibę w Stanach Zjednoczonych, stosują się do wszystkich przepisów i wytycznych dotyczących zgodności finansowej, są wspierani przez ponad 6 milionów dolarów w finansowaniu technologicznym ... Krótko mówiąc, są dokładnie tym, czego chcielibyście u renomowanego sprzedawcy monet. Chociaż Coinbase podejmuje godne podziwu kroki w celu ochrony funduszy swoich klientów, w tym przechowywanie około 90% wszystkich zasobów Bitcoin w

portfelu papierowym offline (drukowane klucze prywatne) w skarbcu bankowym, nadal nie jest rozsądnie trzymać tam swoje monety przez długi okres czasu. Wysyłaj tam monety tylko wtedy, gdy planujesz je sprzedać, a kupione tam monety należy jak najszybciej wysłać do klienta portfela. Nie ma nic złego w ich praktykach biznesowych, to tylko czysta matematyka: wymiany są ogromnym celem dla hakerów, jak wspomniałem wcześniej. A giełdy, z powodu nieoczekiwanej zmienności i wynikającego z tego wzrostu kapitału wymaganego do zaspokojenia potrzeb klientów, mogą całkowicie zamrozić się lub przejść. Powtarzam: Kupuj tam swoje monety. Sprzedaj je tam. Ale trzymaj monety długoterminowe gdzie indziej. Kliknij ten link, aby zarejestrować się w Coinbase, a otrzymasz 5$ darmowego Bitcoina dodanego do Twojego konta, o ile zakup dotyczy przynajmniej jednej pełnej monety: http://bit.ly/1iysEi9

Jestem właścicielem małej firmy i jestem bardziej zainteresowany otrzymywaniem monet niż kupowaniem ich na giełdzie. Jak mam to zrobić?

Bardzo prosta odpowiedź: skonfiguruj klienta portfela, takiego jak Electrum, wygeneruj nowy adres publiczny i podaj ten adres klientom kiedy nadejdzie czas, aby zapłacić - uwzględnij go na fakturach itp. Mniej więcej ten sam proces przyjmowania darowizn, jeśli jesteś zainteresowany lub niezależny twórca treści: opublikuj swój publiczny adres i grzecznie zachęcaj fanów i przyjaciół do wysyłania tam Bitcoinów. Istnieją oczywiście bardziej zaawansowane implementacje. Na przykład w przypadku fizycznego sklepu możesz chcieć, aby komputer w twoim sklepie posiadał Electrum działający z głównego klucza publicznego, a nie z twojego portfela. Instrukcje dotyczące tego są włączone. Sekcja dokumentacji witryny Electrum. Dzięki temu Twój pracownik może wygenerować nowe adresy publiczne zgodnie z potrzebami, aby indywidualni klienci mogli rozliczyć swoje salda, ale nie ma zagrożenia bezpieczeństwa, ponieważ pracownik ma tylko „obserwację" dostępu do monet - ponieważ nie został przywrócony z rzeczywistego materiału siewnego , on lub ona nie może przenieść monet z twojego posiadania. Mogą generować tylko nowe adresy publiczne. Całkiem fajna funkcja!

Skąd się to bierze ... gdybyś musiał zgadywać?

Teraz jest chyba dobry moment, aby rzucić jakieś legalne: Nic w tej broszurze nie jest przeznaczone dla doradztwa inwestycyjnego, podejmowanie własnych

decyzji dopiero po konsultacji z profesjonalistą finansowym, nie ponoszę żadnej odpowiedzialności, Bitcoin jest ryzykowny i może stracić wartość itp. Zasadniczo: jeśli jesteś prawnikiem, bo zrobiłeś coś głupiego i straciłeś wszystkie swoje monety, będę bardzo zdenerwowany! Dorośli powinni wziąć odpowiedzialność za własną wolną od działań wolę jest całkiem słodka. Mając to wszystko, osobiście posiadam Bitcoiny ponieważ głęboko wierzę w technologię i myślę, że jesteśmy w tym na początku tej transformacji.

Pozytywne przesłanie Senatu USA było OGROMNE.

Chińska eksplozja zainteresowania była równie OGROMNA.

Bitcoin nie został wynaleziony wczoraj: istnieje już od 2009 roku. Mimo skalistej drogi wymiana i usługi są dziś bardziej profesjonalne i stabilne niż kiedykolwiek wcześniej. Więcej kupców akceptuje Bitcoin niż kiedykolwiek wcześniej. A zainteresowanie publiczne tą technologią jest większe niż kiedykolwiek. Bitcoin urzeka wyobraźnią, intryguje technika i uwodzi ludzi biznesu. Im więcej kontroli mamy nad własnymi pieniędzmi, tym szybsze mogą być transakcje, tym mniej płacimy za opłaty - to wszystko ekscytujące zmiany. W ciągu pięciu lat firmy i osoby, które wcześnie zaakceptowały Bitcoin, mogą znajdować się w godnej pozazdroszczenia pozycji. Do diabła, jesteśmy już w godnej pozazdroszczenia pozycji, ponieważ jest to zabawne i wydajniejsze niż starsze systemy płatności, które zostały opracowane dekady przed pierwszą stroną internetową.

Czysta (poinformowana) spekulacja

Teraz, gdy masz już wszystkie podstawy, bawmy się dobrze. Życie jest krótkie, a życie bez wyobraźni nie jest ekscytujące.

Biorąc pod uwagę fakt, że przeważająca większość sklepów nadal nie akceptuje Bitcoinów, a wielu ludzi nawet nie słyszało o Bitcoinie, po prostu nie zgadzam się z ludźmi, którzy uważają Bitcoin za „bańkę, która ma pęknąć". Czy e-mail w 1995 r. stał się bańką? Czy Google w 2002 r. był modą? Były to z pozoru wiarygodne pytania, ale biorąc pod uwagę to, co wiemy teraz, są komicznie krótkowzroczne. Pieniądze są na najbardziej podstawowym poziomie porozumieniem między ludźmi. Wcześniej poruszyliśmy koncepcję, że nic nie ma prawdziwej „wewnętrznej" wartości; cała wartość dla naszego gatunku jest względna i pochodzi. Z pewnością, gdyby cokolwiek miało wartość wewnętrzną, prawdopodobnie byłoby to coś w rodzaju puszki zupy lub noża szwajcarskiej armii lub seksu. Ale nie mamy systemu finansowego opartego na nożach szwajcarskiej armii i zupie Campbella jako jednostce transakcyjnej (na szczęście).

Zamiast tego mamy instrumenty takie jak dolar, złoto i - nieuchronnie - Bitcoin. Dolar i inne walutowe obligacje rządowe są umową między ludźmi wymuszonymi na nas. „Musisz zgodzić się na wykorzystanie tego jako pieniędzy". Jasne jest, że był czas, w którym takie mandaty miały sens. Jednak Internet zmienia ten krajobraz w sposób, którego rządy nie mogą po prostu cofnąć. Pieniądze dzisiaj mogą być porozumieniem między ludźmi, dobrowolnie. „Tak, zgadzamy się używać Bitcoinów jako pieniędzy, ponieważ Bitcoin to pieniądze". I oczywiście zgadzam się z tobą, że jest to okrągły argument. To samonapędzająca się pętla sprzężenia zwrotnego. Jest sławna, ponieważ jest sławna, co powoduje, że staje się bardziej sławna. To coś, co widziałem z pierwszej ręki w LA.

Waluta nie różni się więc tak bardzo od sławy. Coś może przejść od niczego do czegoś, a kiedy już osiągnie stabilność lub gwałtowny wzrost jest znacznie bardziej prawdopodobny niż nocna ruina. Bitcoin to coś, w co wierzysz bardziej, gdy go badasz.

Podstawowa matematyka jest zasadniczo czysta i rzeczywiście piękna. Że możesz wydać publiczny adres, nie ujawniając w żaden sposób klucza prywatnego, że prawie nieskończona liczba nowych adresów publicznych może zostać stworzona do woli, że cała umowa społeczna Bitcoina istnieje przez cały czas na Blockchain… co jest zasadniczo globalna zdecentralizowana chmura dla umów finansowych. Jest w nim piękno, które pod każdym względem przewyższa istniejącą sieć finansową zakładu. Czy to nowe zamówienie wyprzedzi bankowość tradycyjną? Absolutnie.

Przewidywanie czegokolwiek innego byłoby absurdalne, prawie kryminalne, krótkowzroczne. Tradycyjna bankowość jest daleko w tyle za Bitcoinem; jedyną rzeczą, jaką Twoja okolica jest zbyt duża, by zaoferować Ci - inne niż miesięczne opłaty za usługi i anemiczne oprocentowanie - to wygoda. Komfort, że naprawdę nie możesz stracić pieniędzy, ponieważ można je odwrócić. Komfort zapewniany przez kasjerkę bankową pytającą, jak wyglądał twój dzień i komentowanie pogody. Taki sam komfort zapewniały biura podróży. Nikt nie korzysta już z biur podróży, ponieważ Travelocity i inne strony internetowe do rezerwacji podróży sprawiły, że przemysł stał się łatwiejszy, szybszy i bardziej konkurencyjny. W taki sam sposób, w jaki biura podróży są teraz doświadczeniem butikowym dla bardzo zamożnych, bardzo niekompetentnych, a nietypowe - oddziały banków będą dokładnie takie same. Z Bitcoinem jesteś swoim własnym bankiem, a zbiorowa halucynacja waluty rozgrywa się w sposób bardziej sprawiedliwy i przejrzysty niż w jakimkolwiek innym momencie w historii. Czy Bitcoin stanie się

technologią wartą bilion dolarów? Nie wiem Może. Jest wystarczająco dużo powodów, by zasugerować tak: silną przewagę na pierwszym miejscu, pułap rynkowy i wolumen transakcji znacznie wyższy niż którykolwiek z konkurencyjnych walut „ja też”, które pojawiły się wkrótce po tym. Albo Bitcoin może się posypać. Krytyczne wady mogą zostać ujawnione. Coś bardziej wyrafinowanego, dopracowanego w sposób, którego jeszcze nie zdajemy sobie sprawy, że chcemy, może się pojawić. Ale pewne jest to, że matematyka kryptowaluty, na której jest zbudowana, w jakiejś formie, pozostanie tutaj. To na zawsze zmieniło sposób myślenia o walucie. W większości bezużyteczne numery seryjne i dziwaczne popiersia martwych prezydentów w naszej papierowej walucie wydają się pozytywnie prehistoryczne w porównaniu z niezniszczalną, bezsensowną naturą Bitcoinów. Jeśli Bitcoin stanie się tak skuteczny, jak sądzę, za kilka lat myślenie o bogactwie Bitcoinów w kategoriach dolarów również będzie przestarzałe. Podobnie jak nie porównalibyśmy pieniędzy na naszych kontach bankowych do równoważnej liczby skór zwierzęcych lub jednostek waluty muszli rdzennych Amerykanów. Do zobaczenia na Księżycu. (Lub w domu wariatów)