# Transkrypcja gawędy o Bitcoinie

To jest transkrypcja pierwszego odcinka gawędy o kryptowalutach.
Prelekcję prowadzi Tomasz Zieliński, autor bloga www.informatykzakladowy.pl

Uwaga! Tekst jest zapisem dwugodzinnego monologu. Aby lepiej się go czytało, dokonano pewnych zmian i modyfikacji - dotyczy to głównie powtórzeń, drobnych omyłek i doboru słów, ale także zwięzłości wywodu. Pominięto też fragmenty mające sens jedynie dla widzów słuchających gawędy na żywo.

Linki w tytułach rozdziałów prowadzą do odpowiednich fragmentów nagrania wideo, dostępnego pod adresem https://youtu.be/IVEug1rk0rU

TO JEST WERSJA BEZ ILUSTRACJI – niektóre fragmenty mogą być niezrozumiałe.



## 00:00:00 Wprowadzenie i spis treści

Dzień dobry, dzień dobry! Nazywam się Tomek Zieliński, jestem autorem bloga informatykzakladowy.pl, a to jest pierwszy live! Nie lubię tego słowa, więc: to jest pierwsza gawęda, którą prowadzę online, na żywo, i jestem troszkę zdumiony, że w tej chwili ogląda ją ponad 90 osób. Postaram się nie zmarnować waszego czasu. Dzisiaj opowiem o kryptowalucie Bitcoin. Wiele można o tej kryptowalucie przeczytać i zazwyczaj są to jakieś takie teksty w stylu, że nowy paradygmat, zupełnie nowe podejście do finansów itd. Być może - można tak uważać można tak nie uważać.

Ja chciałbym dzisiaj skupić się na technicznym aspekcie Bitcoina, to znaczy wytłumaczyć dokładnie co to jest, jak działa, jakie mechanizmy za tym stoją, i zostawić was po tej gawędzie z poczuciem że wiecie - mniej więcej - jak działa ta jedna konkretna kryptowaluta. Ethereum (druga najpopularniejsza) działa w inny sposób i realizowane przez nie działania są troszkę inne. Bitcoin jest pierwszą, najbardziej znaną i o niej dzisiaj będziemy mówić.

Bardzo, bardzo ważna sprawa - to wszystko, co będę dzisiaj mówił, to będzie mniej więcej prawda. To będzie taka prawda, którą da się zmieścić w ciągu godziny lub półtorej, co oznacza, że będzie tu masa, ale to naprawdę masa uproszczeń. Jeśli chodzi o samą mechanikę, matematykę, algorytmy itd. nie będę daleki od prawdy, i to co będę mówił, będzie opowiadało o rzeczywiście istniejących mechanizmach stojących za bitcoinem, natomiast tej wiedzy będzie za mało - tak po prostu.

Przy zabawie prawdziwymi bitcoinami trzeba wiedzieć więcej, trzeba znać więcej pojęć i po prostu sobie poćwiczyć. Więc jeśli ktoś będzie chciał próbować zabawy z bitcoinami, będzie chciał sobie coś kupić, zobaczyć jak wygląda oprogramowanie, jak działają serwisy on-line'owe zajmujące się tematyką BTC - musicie się doedukować. Wiedza z tej gawędy nie wystarczy. Będzie jedno szczególnie niebezpieczne miejsce, w którym powiem, że to jest właśnie to miejsce. Tam dodatkowa wiedza będzie najbardziej potrzebna - składają się na nią szczegóły techniczne, które należy znać, żeby się nie naciąć. Natomiast co do zasad działania, to tam nie dzieje się wiele.

To są zagadnienia, które będę chciał dzisiaj przedstawić. Te pogrubione, które widzimy na ekranie, są kluczowe, i one tak naprawdę składają się na mechanikę kryptowaluty Bitcoin. Natomiast aby je zrozumieć, trzeba wprowadzić trochę dodatkowych pojęć.

## 00:05:57 Funkcja skrótu

Pierwszą rzeczą, o jakiej opowiem, jest funkcja skrótu, inaczej zwana funkcją haszującą (hash function). To jest taka funkcja, jaką znamy w matematyce - algorytm, który dostaje jakieś argumenty na wejściu, w jakiś sposób te argumenty przetwarza, i zwraca jakieś dane wyjściowe. W przypadku funkcji haszujących (funkcji skrótu), na wejściu przekazywana jest dowolna ilość bajtów a w środku dokonują się bardzo takie złożone transformacje bitowe. Są one jednokierunkowe, tzn. nie potrafimy ich policzyć w drugą stronę, natomiast charakterystyczne dla funkcji haszującej jest to, że dane wyjściowe są zawsze tej samej długości. Niezależnie od tego, jakiej duże będą dane wejściowe, to wartość końcowa będzie stała, np. 32 bajty. I taki przykład widzimy tutaj:

Ten brązowy napis to jest przykładowy hash, czyli przykładowy skrót jakiegoś napisu. I teraz, gdy mamy do czynienia z porządną funkcją skrótu (spełniającą kryteria stawiane przy zastosowaniach kryptograficznych), to nie ma żadnego sposobu żeby w szybki sposób sprawdzić jaki napis wygenerował taki skrót, jaki tu widzimy. Jedyna możliwość jest taka, że bierzemy pusty ciąg i patrzymy czy pasuje. Pewnie nie. Potem bierzemy wszystkie 256 wariantów ciągu jednobajtowego i sprawdzamy dla każdego z nich, czy dostajemy pożądany skrót. Jeśli nie, sprawdzamy wszystkie ciągi dwubajtowe, trzybajtowe itd. Nie znamy żadnej szybszej metody aby się tego dowiedzieć.

Oprócz tego bardzo ważne jest to, aby funkcja, której użyjemy, nie pozwalała na generowanie tak zwanych „kolizji". Kolizja pojawi się, gdy znajdziemy dwa różne napisy wejściowe, które będą miały taki sam hash, albo gdy - patrząc na napis i jego hash - skonstruujemy inny napis z takim samym hashem.

Łatwo się przekonać, że kolizje muszą istnieć, bo gdy mamy 32-bajtowy skrót, to na pewno istnieje jakaś para napisów dłuższych od 32 bajtów, których skróty będą takie same. Liczba możliwych skrótów jest wielka, ale skończona, zaś napisów możemy generować nieskończenie wiele. Nie potrafimy jednak w ogóle znajdować takich kolizji dla dobrych funkcji skrótu. W przypadku bitcoina, używaną funkcją skrótu jest SHA256, tutaj mamy dwa przykłady:

Jeśli na wejściu podamy ciąg „Litwo, ojczyzno moja", to skrót w zapisie szesnastkowym się zaczyna od 5D825… itd. Natomiast demonstracją tego, że wejście może być dowolnej długości, może być na przykład cały tekst „Pana Tadeusza" i to planuję w tej chwili pokazać.

Weźmy cały tekst poematu w formacie txt ze strony wolnelektury.pl

Następnie otwieramy stronę (narzędzie) o nazwie Cyber Chef, znajdziemy funkcję SHA z rodziny 2, rozmiar 256, i skopiujemy do ramki z danymi wejściowymi cały tekst Pana Tadeusza.

I widzimy skrót B7D2998AD349EB... , czyli dokładnie ten podany na górze. Przyznacie, że dość trudne jest wygenerowanie całego „Pana Tadeusza" losowo, aby odnaleźć ten napis. Więc to był przykład, że długość napisu na wejściu może być dowolna, a skrót będzie zawsze takich samych rozmiarów. Ważne własności kryptograficzne które ta funkcja musi zachowywać są takie, aby dla dwóch różnych napisów średnio połowa bitów skrótu się różniła. Jeśli więc w napisie wejściowym zmienimy jeden bit, czyli np. w całym „Panu Tadeuszu" zamienimy jeden raz literkę „b" na „c", wtedy również wartość skrótu tak się przemiesza, że zmieni się średnio połowa tych bitów które składają się na 32 bajty skrótu.

Słowo wyjaśnienia, do czego te funkcje skrótu się przydają. Sporo się o nich słyszy gdy mowa o wyciekach danych. Zapisywanie w systemie informatycznym hasła użytkownika w jakiejś bazie danych albo w jakimś rejestrze, to jest bardzo poważny grzech przeciwko bezpieczeństwu systemów. Powinniśmy zapisywać jedynie hash - tak aby nie dało się dowiedzieć który użytkownik ma jakie hasło. Przy próbie logowania użytkownik wpisze swoją nazwę, swoje hasło, my to otrzymane hasło zahaszujemy tą samą funkcją i porównamy z wartością zapisaną w bazie. Jeśli się zgadza, to użytkownik faktycznie podał to samo hasło.

Natomiast kiedy ktoś włamie się i ukradnie tę naszą bazę danych z hashami, to są sposoby na to, aby on musiał zużyć bardzo bardzo dużo czasu i pieniędzy, by złamać choćby niewielką część tych hashy (czyli by odtworzyć hasła użytkowników).

Funkcji skrótu można używać do tego aby udowodnić, że jakiś dokument istniał w jakimś określonym czasie, np. mamy potrzebę udowodnić komuś, że napisaliśmy książkę dzisiaj, choć chcemy się nią pochwalić światu za 10 lat. Bierzemy sobie plik z książką, obliczamy skrót, publikujemy tę wartość na Twitterze albo Facebooku, lub dowolnym innym serwisie który - jak przewidujemy - będzie istniał za 10 lat. Gdy w przyszłości ujawnimy swoje dzieło, no to będziemy mogli pokazać że ten dokładnie ten plik istniał 10 lat wcześniej, i dowodem na to jest to obliczony i opublikowany wówczas skrót.

W bitcoinie używa się funkcji SHA w drugiej wersji (wariant SHA-256). Dawniej w użyciu były inne funkcje, np. MD5 lub SHA-1, ale albo odnaleziono w nich słabości, które np. pozwalały na wygenerowanie kolizji, albo ich bezpieczeństwo zostało podważone w inny sposób i wiem, że nie należy ich już używać. Zapamiętujemy z tego rozdziału, że funkcja skrótu bierze jakiś napis i zwraca skrót; oraz że nie da się zgadnąć, jaka wartość była na wejściu, jeśli mamy tylko skrót.

# 00:13:55 Blockchain

*Uwaga do transkrypcji - ten fragment jest bardziej zrozumiały w wersji wideo*

Zgodnie z obietnicą, Blockchaina wygenerujemy za chwilę na żywo. W tej chwili wrócimy do Cyber Chefa. Skasuję to, co tu było, włączę sobie notepada. Piszę tam:

I to będzie pierwszy blok, który sobie zapisuje w notatniku. Zapisuję też, jaka jest wartość skrótu tego napisu. Akurat tak się składa że napis jest krótki, więc skrót jest od niego dłuższy.
Potem zaczynamy drugi blok i ja sobie przeczytam na czacie, że np. Hubert P. napisał „mikrofon za daleko", kopiuję ten napis i doklejam do niego skrót poprzedniego bloku. I taki połączony napis wrzucam sobie do przehashowania - i mam jakąś inną wartość skrótu. Biorę tę wartość, i to będzie wklejone tutaj

Potem bierzemy sobie jakiś kolejny blok,  w którym będzie napisane "DestinationVoid na czacie" i dołączamy wartość poprzedniego hasha. Połączony napis wklejamy do przehaszowania.

Dostajemy jakąś wartość skrótu. Myślę, że już wiecie o co chodzi. Każdy z kolejnych napisów w kolejnych blokach, zawiera skrót poprzedniego bloku. Zróbmy to może jeszcze jeden ostatni raz.

I będziemy mieli kolejny blok blockchaina. W ten sposób powstaje nam taka struktura, do której dopisujemy kolejne rekordy, ale nie będziemy w stanie zmodyfikować tego co już było. Zwróćcie uwagę - jeśli spróbowalibyśmy cofnąć się do któregoś z tych wcześniejszych bloków, i zmodyfikować choćby jedną literę, to hash tego bloku się zmieni. W związku z tym, nie będzie już zgodne z hashem wklejonym do następnego bloku blockchaina, i w ten sposób wykryjemy jakąś modyfikację.

Blockchain to jest tak naprawdę rejestr, do którego coś możemy dopisywać. Jeśli coś do niego dopisujemy, ten rejestr rośnie. On może tylko rosnąć a nikt na świecie nie będzie w stanie zmodyfikować w sposób niezauważony jakiegokolwiek elementu, który nie jest tym nowo doklejanym. Wynika z tego, że aby móc zweryfikować integralność blockchaina, no to trzeba mieć dostęp do wszystkiego co tam się znajduje, do całego kompletu danych.

Tutaj przeskakujemy na chwilę do Bitcoina - na początku 2021 roku ma on już 660 tysięcy bloków i 311 GB danych, czyli troszkę urósł. Zwracam uwagę, że sam blockchain to nie jest jeszcze rejestr rozproszony. Gdy się przełączę na notepada, to widzę, że ten mój blockchain istnieje tylko w jednej kopii w notepadzie a mimo tego, sam sobie związałem ręce, tzn. nie jestem w stanie zmodyfikować żadnego z wcześniejszych bloków bez modyfikacji wszystkich wartości skrótu aż do samego końca.

# 00:19:00 Sieci Peer-to-Peer (P2P)

… czyli takie sieci, które nie wyróżniają żadnej roli, żadnego koordynatora, i pozwalają każdemu węzłowi dołączać na tych samych prawach. Nie ma zbyt wielu powszechnie znanych zastosowań sieci P2P. Jednym z bardziej popularnych jest Bittorrent, czyli protokół wymiany plików. Nie muszą to być od razu jakieś filmy, mogą to być np. pliki z dystrybucjami Linuksa, które często są rozpowszechniane w ten sposób. Pliki są przechowywane na wielu węzłach a protokół jest organizowany tak, by te węzły mogły łączyć się między sobą i wymieniać między różnymi fragmentami pliku.

Na animacji widzimy, że ta większa maszyna u dołu, żeby udostępnić pozostałym 7 komputerom plik, który ma, dzieli go na kilka części, które wysyła odbiorcom tylko jeden raz. Pozostałe węzły, które odebrały po jednym kawałku, zaczynają wymieniać się brakującymi częściami i w ten sposób w dość krótkim czasie, znacznie krótszym niż gdyby wszyscy ciągnęli dane z jednego komputera, każdy z węzłów będzie miał pełną kopię pliku.

Jak mówiłem, usług działających w tej architekturze nie spotyka się wiele. Bitcoin jest jednym z przykładów sieci w której nie ma jakiegoś centralnego serwera, który by zarządzał innymi węzłami, przydzielał im role, albo coś takiego. Gdy dołączamy się (oczywiście z wystarczająco szybkim komputerem z wystarczająco szybką siecią) do innych komputerów przetwarzających bitcoinowego blockchaina, to będziemy mieli, można tak powiedzieć, takie same prawa i obowiązki jak wszyscy inni uczestnicy sieci.

# 00:22:43 Rozproszony rejestr

Tutaj będzie trochę opowiadania i machania rękami. Gdy chcemy pomyśleć o rozproszonym rejestrze, to najpierw spojrzymy na jakiś rejestr scentralizowany. No i bardzo dobrym przykładem nawiązującym do finansów są np. banki. Bank, jako instytucja zaufania publicznego, prowadzi sobie taki właśnie rejestr, w którym odnotowuje wszystkie operacje, jakie mają miejsce związane z finansami jego klientów, np. że ktoś przyszedł i wpłacił jakąś kwotę na lokatę, ktoś inny przyszedł i zaciągnął kredyt (temu pierwszemu wypłacimy jakiejś odsetki od tej lokaty a drugiego z pewnością obciążymy kosztami kredytu).

Tak powstaje księga, rejestr - to się w banku nazywa księga główna, która zawiera wszystkie operacje, i ona jest tak naprawdę źródłem prawdy. Klient może zapomnieć ile ma pieniędzy, ale gdy pójdzie do banku i spyta - to się dowie. To jest informacja, z którą on może niewiele zrobić, tzn. jeśli uważa że coś powinno wyglądać inaczej, to może co najwyżej pójść do sądu i sąd rozstrzygnie jego ewentualne roszczenia. To może faktycznie zmienić zapisek w tym rejestrze scentralizowanym, ale cały czas naszym punktem odniesienia jest to, co wie bank.

Natomiast, w przypadku Bitcoina - kryptowaluty - chcielibyśmy skonstuować mechanizm, który będzie całkowicie niezależny od jakichkolwiek rejestrów scentralizowanych, aby wszystko mogło dziać się bez żadnej instytucji, którą dałoby się zbombardować, wyłączyć albo skutecznie zakazać jej działalności. Twórca Bitcoina chciał, aby ta właśnie kryptowaluta była odporna na właśnie tego typu wydarzenia.

Wymyślmy sobie taką przykładową sytuację. Niech będą sobie jacyś panowie A, B, C, D, E i F. Załóżmy że są to anarchiści, którzy na pewno nigdy nie pójdą do banku, nie będą klientami banku. Jak każdy, czasem potrzebują więcej pieniędzy niż mają (każdy z nich trochę ma, ale nie za dużo, jak to anarchiści), i czasem chcieliby móc trochę od kogoś pożyczyć. I sytuacja wygląda tak, że oni żyją sobie w jakimś squacie, i wiedzą, że są na siebie skazani, samotny anarchista sobie w życiu nie poradzi, musi mieć dookoła siebie kolegów. I oni właśnie stanowią taką grupę i nie wszyscy się lubią, są jakieś sympatie, antypatie. Wiedzą, że z jednej strony, jak kogoś nie lubią to być może chcieliby go oszukać. A z drugiej strony, wiedzą, że potrzebują siebie nawzajem. Ta grupa jest dla nich sporą wartością.

I tutaj rozwiązanie, które można im zaproponować, to jest właśnie rejestr rozproszony, a konkretnie rejestr pożyczek. Ci anarchiści spotykają się wieczorem na kolacji, któryś potrzebuje pieniędzy, sobie tam rozmawiają, i w którymś momencie pan A mówi głośno “Pożyczam panu D 10 pieniędzy”. I teraz wszyscy wyciągają swoje notatniki, i zapisują sobie tą informację, kto komu ile przekazał.

Jakiś czas później ma miejsce inna sytuacja, ileś pieniędzy wędruje od pada D do pana E, i wszyscy notują sobie tą informację. Takie sytuacje powtarzają się ileś razy, aż kartki im się skończą. Wszystkim skończą się jednocześnie, bo wszyscy zapisują w taki sam sposób, takimi samymi symbolami, na kartkach takich samych rozmiarów - i co oni robią teraz?

Teraz obliczają skrót napisów, które były na kartce. Następnie biorą sobie nową kartkę (każdy swoją) i piszą ten skrót na samej górze nowej kartki. A potem idzie znowu od początku, tzn. ktoś komuś pożycza, wstaje, głośno mówi, wszyscy to zapisują. I tak się to dzieje, aż kolejna kartka się zapełni, wtedy znowu wszyscy wyliczają hash, wychodzi im dokładnie to samo, i ten hash zapisują sobie na kolejną kartkę, itd.

W ten sposób powstaje blockchain, czyli łańcuch bloków, w którym każdy blok jest zależny od poprzedniego. Tutaj wewnątrz każdego bloku mamy - oprócz hasha poprzedniego bloku - również transakcje, czyli jakieś informacje o przepływach finansowych, które miały miejsce i które są dla nas faktem. Jak już zauważyliśmy, nie da się sfałszować niczego w środku blockchaina, więc blockchain chroni nam historię tych transakcji.

Teraz chcielibyśmy omówić sytuację, gdy przychodzi jakiś nowy człowiek, np. siódmy anarchista, który chce dołączyć do tej grupy. Chciałby on dołączyć też do tego systemu pożyczek z rozproszonym rejestrem. Co ten nowy robi? Nie może pójść np. do pana A i przepisać od niego całego rejestru, bo jeśli A ma kosę z B, to wygumkuje z rejestru wszystkie swoje zobowiązania wobec B, policzy na nowo wszystkie hashe, i przedstawi nowemu sfałszowany rejestr.

Nowy anarchista, aby móc poznać prawdziwą zawartość rejestru rozproszonego, każdą stronę weźmie od kogo innego, od losowych domowników. A gdy już będzie miał komplet stron, przepisanych czy przekserowanych, to on wtedy usiądzie i sam sprawdzi po kolei wszystkie hashe. Zweryfikuje, czy cały blockchain trzyma się kupy, czy tam nie było żadnego fałszerstwa. Jeśli nie było, to nowy ma pewność, że dysponuje taką samą kopią co wszyscy inni.

Jeśli coś jest po drodze nie tak, jeśli nowy anarchista gdzieś natrafi na jakieś fałszerstwo, to zacznie wypytywać wszystkich innych o ten blok który przestał pasować. I teraz, dopóki co najmniej połowa odpowiada uczciwie, czyli rzeczywiście powie jak te kartki wyglądają, no to ten nowy po prostu uwierzy większości, i pójdzie dalej. Jeśli więcej niż połowa kłamie, lub realizuje swoje własne cele, to wtedy cały blockchain się załamuje i w takiej sytuacji Bitcoin też nie miałby już racji bytu. Założenie jest jednak takie, że ci anarchiści wiedzą, że grupa jest dla nich wartością, więc nawet jeśli ktoś się nie lubi, to żaden członek grupy nie jest w stanie samodzielnie okłamać wszystkich innych i nie leży w ich interesie zrobienie takiej kliki w środku, która byłaby w stanie okłamać nowego.

To była jednak mała grupa anarchistów, sześć czy siedem osób, które spotykają się na kolacji, żyją obok siebie. Odrębny problem pojawia się, gdy chętnych do utworzenia sieci jest np. 10 milionów, i oni wszyscy chcieliby korzystać z rejestru rozproszonego. Skalowanie zapewni nam wspominana niedawno sieć peer-to-peer (P2P). Troszkę tracimy, troszkę zyskujemy. Oczywiście, zyskujemy znacznie większy potencjał dystrybucji informacji, bo ile osób możemy obsłużyć tym starym modelem z anarchistami przy kolacji? Pięćdziesiąt? Raczej nie więcej.

Natomiast przy sieciach P2P mogą to być miliony osób / komputerów / systemów, bo każdy z nich przekazuje odbierane informacje tym sąsiadującym węzłom, które tej informacji jeszcze nie mają. W ten sposób informacja w sieci P2P będzie w stanie podróżować bardzo szybko. Co tracimy? Nie mamy gwarancji, że informacja dojdzie do wszystkich w tej samej kolejności, bo jeśli np. ja jestem w Polsce, nadam jakiś komunikat, to ktoś w Czechach zazwyczaj odbierze go szybciej, niż jakiś węzeł w Australii. Z kolei gdy ktoś w Australii nada

jakąś informację do rozpowszechnienia  w rozproszonej sieci P2P, no to Nowa Zelandia dowie się o tym wcześniej niż Berlin lub Polska. Więc nie będzie możliwości upewnienia się, ani że wszyscy w każdej chwili wiedzą to samo, ani że odebrali te informacje w dokładnie tej samej kolejności.

W modelu z anarchistami mieliśmy jeden rozgłaszany komunikat typu „nowa transakcja” czyli ogłoszenie, że przekazuję komuś jakieś środki. W sieci P2P niemożliwe jest jednak synchroniczne notowanie ich na kartce ani sytuacje, że kartki z transakcjami notowanymi na całym świecie będą miały jednakową zawartość i skończą się wszystkim na raz.

Musimy wprowadzić drugi typ komunikatu, w którym ktoś będzie w stanie powiedzieć „oto pełna zawartość kolejnej kartki” (bloku). Gdy ktoś rozgłosi zestaw wcześniej ogłoszonych transakcji, i poda skrót zestawu, to wszyscy sobie dopiszą do swoich kopii rejestru tą samą kartkę (blok) - bo uwierzą w ten komunikat. Powiemy niebawem, dzięki jakim mechanizmom wszyscy zgodzą się w to uwierzyć.

Jesteśmy już niedaleko mechaniki Bitcoina. Mamy sieć P2P, której innym przykładem był Bittorrent. Wiemy, że każdy węzeł musi weryfikować prawidłowość operacji, więc musi przechowywać kompletną kopię blockchaina. Wiemy też, że nie da się w żaden sposób sfałszować czegoś co było w środku łańcucha bloków a ktoś, kto chciałby otrzymać od nas historię transakcji, będzie w stanie wykryć, że próbujemy go oszukać. Na razie mamy tylko intuicję, czym rzeczywiście będą transakcje.

# 00:34:53 Kryptografia klucza publicznego

W tym rozdziale będzie najmniej matematycznej prawdy. Będzie machanie rękami i proszę żebyście uwierzyli na słowo we wszystko, co powiem. To są oczywiście fakty, matematycznie do udowodnienia, natomiast te zagadnienia są bardzo trudne i skomplikowane. Na studiach informatycznych kurs kryptografii trwa semestr lub dwa, więc na pewno nie zmieścimy tego w paru minutach. Powiem rzeczy w które trzeba uwierzyć i pójdziemy dalej.

Kryptografia klucza publicznego charakteryzuje się tym, że potrafimy zaszyfrować dane jednym hasłem, a rozszyfrować innym hasłem. I to jest możliwe, są mechanizmy, które na to pozwalają. Gdy korzystamy z Worda i nakładamy jakieś hasło na dokument albo tworzymy archiwum plików chronione hasłem - wówczas to samo hasło służy nam do zaszyfrowania i odszyfrowania. Matematyka pozwala nam na zastosowanie takiego matematycznego wynalazku, w którym te klucze się różnią. Jeden jest do szyfrowania, inny do odszyfrowania. Powiedziałem „klucze”, gdyż w kryptografii mówimy o kluczach, nie hasłach, ale w praktyce te słowa będą oznaczały mniej więcej to samo.

Klucze kryptograficzne to liczby. Ilustracją tego, że te liczby są bardzo duże, może być następujący eksperyment myślowy. On nawiązuje trochę do tych mechanizmów w rzeczywistych systemach kryptografii asymetrycznej, natomiast to jest ten moment, że będzie dużo machania rękami. Żeby wygenerować jakiś klucz, którego nikt nie odgadnie, potrzebujemy jakiś losowy ciąg 0 i 1 które się na to złożą. Możemy sobie wziąć na przykład kostkę sześcienną, przypisać zero do parzystych, jeden do nieparzystych, rzucić 256 razy po kolei i zapisać sobie wyniki. Ten zapisany ciąg zer i jedynek to będzie w reprezentacji dwójkowej jakaś bardzo duża liczba. Jeśli sobie przełożymy tę liczbę na zapis dziesiętny to będzie jakaś liczba z przedziału od zera do… tej liczby na obrazku. Ta liczba jest gigantyczna, mózg ludzki nie jest przyzwyczajony do operowania na tak wielu rzędach wielkości.

Losowa liczba składająca się z 256 bitów jest niewiele mniejsza, od szacowanej liczby wszystkich atomów we wszechświecie. Więc to jest nieprawdopodobnie wielka liczba, i odgadnięcie liczby, jaką sobie wylosował ktoś inny, albo sprawdzenie wszystkich możliwych kombinacji - to jest po prostu niemożliwe. Przy ludzkich możliwościach czy ograniczeniach techniki czy matematyki, ta liczba jest po prostu nieskończona. Oczywiście nie jest. Ale w praktyce jest.

Gdy sobie wylosujemy taką wielką liczbę, to do tej liczby dobierzemy sobie w szczególny sposób inną dużą liczbę, i to będą właśnie te dwa hasła, dwa klucze, o których mówiliśmy wcześniej. Pierwsza z nich, to będzie klucz prywatny, i dla założeń kryptografii asymetrycznej to jest bardzo ważne żeby to była ścisła tajemnica, aby znał ją tylko posiadacz klucza. Natomiast drugi z kluczy będzie kluczem publicznym, on może być znany każdemu. Można go wydrukować w prasie, można go wrzucać na Facebooka, można opublikować na swojej stronie internetowej, można stanąć na rynku i wykrzykiwać bity swojego klucza publicznego (co spotka się na pewno z dużym zdziwieniem), w każdym razie to nie jest żadna tajemnica. Klucz publiczny, jak sama nazwa wskazuje, to jest coś, o czym będziemy mówić głośno, że to jest właśnie ten nasz klucz.

Na co nam to pozwoli? Kryptografia asymetryczna sprawia, że kluczem prywatnym możemy coś zaszyfrować, oczywiście po zaszyfrowaniu to jest zbiór bitów nieodróżnialnych od losowych. Natomiast kluczem publicznym możemy to sobie odszyfrować czyli: jeśli my zaszyfrujemy prywatnym, to każdy, kto dostał od nas klucz publiczny, może użyć go do odszyfrowania, wtedy dostanie jakiś tam sensowny dokument, sensowną zawartość. Ten ktoś wtedy przekona się, że faktycznie to ten czerwony ludzik zaszyfrował plik, bo nikt inny nie byłby w stanie tego zrobić, nikt inny nie ma powiązanego klucza prywatnego.

Możemy też zrobić inną ciekawą rzecz. Skoro znamy już trik z szyfrowaniem / odszyfrowaniem dwoma różnymi kluczami, to możemy sobie jakiś tekst (docelowo - tekst transakcji bitcoinowej) pozostawić zapisany otwartym tekstem, ale oprócz tego wyliczyć jego skrót i zaszyfrować ten skrót. Wtedy ktoś, kto odbierze taką wiadomość, samodzielnie obliczy skrót a potem odszyfruje podpis i sprawdzi zgodność wyników obu operacji. Ma wówczas potwierdzenie, że rzeczywistym autorem podpisu był posiadacz klucza prywatnego.

Podsumowując - jeśli popatrzymy sobie na jakiś tekst, podpis cyfrowy i klucz publiczny, to potrafimy sprawdzić, czy faktycznie podpis cyfrowy pod tekstem złożył posiadacz klucza prywatnego powiązanego z tym kluczem publicznym.

Jesteśmy o krok od zrobienia prawdziwego Bitcoina!

To jest ten moment, który jest najbardziej niebezpieczny. Jeśli będziecie chcieli sobie kupować własne kawałki bitcoinów, to musicie koniecznie się dokształcić. Dysponując tylko wiedzą, którą przekażę, możecie stracić swoje bitcoiny, tzn. dokonać operacji wskutek której przepadną i nikt nigdy nie będzie ich w stanie odzyskać.

To klucz publiczny będzie naszym „numerem konta” w sieci bitcoinowej. Ponownie - to nie jest taka całkiem prawda, ale w prawdziwym życiu to właśnie z klucza publicznego generuje się dowolnie wiele tych rzeczywistych „numerów kont”. W tym kontekście będziemy używać terminu „adres” albo „adres portfela”. Tak, jak w zwykłych bankach mamy IBAN, z numerem banku i rachunku sklejonymi w ciąg znaków o znanej strukturze, to tu również będziemy mieli ciąg znaków o określonej strukturze.

Pamiętacie zapewne ten obrazek W którym osoby A, B, C, D przekazywały sobie środki? Nie myślimy już tutaj o osobach. A, B, C, D - to są adresy. W sieci bitcoinowej środki będą przemieszczane między różnymi adresami. To, że z A do D przepłynie jakaś wartość

pieniężna, nie niesie już żadnej informacji, czy to są rzeczywiste osoby, czy też użytkownik posiadający wiele adresów sam robi sobie jakieś przelewy. Ważna rzecz: każdy może sobie wygenerować dowolną liczbę adresów w sieci Bitcoin, tak samo jak i dowolną liczbę kluczy prywatnych. Tysiąc, milion czy miliard adresów na własne potrzeby? Bez problemu. Nie powtórzą się, nie będzie kolizji, liczba możliwości jest w praktyce nieskończona. Nie potrzeba do tego żadnych komputerów, nie potrzeba komunikacji z innymi węzłami. Pamiętajcie - jeśli wygenerujemy sobie adres i przelejemy na niego środku ale zgubimy klucz prywatny, to będziemy mieli poważny problem (o którym za chwilę).

Transakcja w sieci bitcoinowej to jest przekazanie jakichś środków z jednego adresu na inny. Oczywiście taka transakcja będzie legalna tylko wtedy, gdy stan posiadania adresu źródłowego (można o tym myśleć jak o bieżącym saldzie), pozwala na wykonanie tej transakcji. Jedynie dysponent klucza prywatnego może takie transakcje wykonać - czyli rozgłaszać, że chce przekazać środki zgromadzone na jednym adresie pod jakiś inny adres. To o takim podpisie mówiliśmy wcześniej: jest tekst transakcji, wyliczamy skrót, skrót jest szyfrowany kluczem prywatnym. Każdy może spojrzeć na klucz publiczny (przypomnijmy - jest to adres źródłowy, zapisany w tekście transakcji), sprawdzić podpis i upewnić, się, że to rzeczywiście posiadacz klucza prywatnego autoryzował tę transakcję. O adresacie nie musimy wiedzieć niczego oprócz adresu jego portfela.

Dwa szczegóły techniczne - wspomniałem że nie trzeba mieć całego bitcoina, można mieć ułamek bitcoina. Jedna transakcja może rozbić środki z jednego adresu na wiele innych lub odwrotnie - może skonsolidować środki z wielu różnych adresów na jednym. W tym drugim przypadku działa to w ten sposób, że jedna transakcja jest podpisywana wielokrotnie, abyśmy byli w stanie zweryfikować zgodne życzenie posiadaczy kluczy prywatnych.

Co wiemy do tej pory - ano wiemy, że mamy bloki, a w nich transakcje. Nie wiemy jeszcze jak te bloki się generują, ale jesteśmy coraz bliżej.

Gdy bank przysyła nam wyciąg z konta, widzimy tam pozycję „saldo” z informacją ile mamy w tym banku pieniędzy. W blockchainie bitcoinowym, nie ma takiego czegoś, jak saldo, które byłoby gdziekolwiek ogłaszane. Jedyna wiedza, ile środków jest na którym adresie, to jest przejście całego blockchaina od początku do końca i notowanie. Jeżeli na adres A wpadł jeden bitcoin, to notujemy że jest jeden. Potem znajdziemy transakcję w której na ten adres przekazano 2 bitcoiny, to wiemy że mamy już 3 bitcoiny, ale musimy sami to notować, blockchain zagregowanej informacji nie trzyma. Potem idziemy dalej, znajdujemy miejsce gdzie z tego adresu schodzi 2,5 bitcoina na inny adres, więc odnotowujemy sobie na kartce albo w pamięci komputera, że zostało nam pół bitcoina pod adresem A. Mamy też pewność, że to saldo nigdy nie zejdzie poniżej zera, bo taka transakcja byłaby nielegalna, więc blok zawierający ją także byłby nielegalny więc nie zostanie dołączony do łańcucha bloków, bo naruszałoby to protokół Bitcoina. Użytych dotąd w blockchainie adresów są już grube miliony.

Na poprzednich slajdach pojawiało się słowo “bitcoin” z dużej i małej litery. Gdy mówimy o dużej literze, Bitcoin przez duże „be”, to jest ogólna nazwa kryptowaluty i systemu płatności z blockchainem działającym w sieci P2P, podpisywaniem transakcji itd. Natomiast bitcoin z małej litery to jest jednostka monetarna. Tak, jak walutą jest złotówka i mamy monetę jednozłotową, tak tutaj myślimy o bitcoinach jako monetach, czy też sztukach monetarnych tej kryptowaluty. Wcześniej mówiliśmy, że można przekazywać w transakcjach ułamki bitcointa, ale ten podział nie jest nieskończony. Każdy bitcoin składa się ze 100 milionów satoshi, czyli takich niepodzielnych „groszy”. To jest najmniejsza jednostka jaka jest zdefiniowana. Można sobie wyobrazić że ktoś przekazuje między dwoma adresami jednego satoshi, ale nie mniej. Czyli: jeśli mamy jednego bitcoina i mamy mieszkańców Europy, to nie da się go podzielić tak, aby każdy mieszkaniec dostał własny kawałek.

**Pytania z czata:**

*Czy jeśli pobieram aplikację przechowującą btc, to pobieram ponad 300 gb danych?*

Nie, nie pobierasz. Tak naprawdę bitcoiny możesz przelać sobie na adres, do którego klucz prywatny masz spisany na kartce, więc oprogramowanie na dobrą sprawę nie jest Ci koniecznie potrzebne. Możesz kupić bitcoina i powiedzieć giełdzie: „to co kupuję proszę przekazać na taki a taki adres" i mieć kartkę papieru, na której będzie klucz prywatny kontrolujący ów adres.

Owe 300 GB całego blockchaina muszą mieć węzły, które przetwarzają nowe transakcje i próbują generować nowe bloki. Żaden węzeł nie może ufać innym, wszystko musi sprawdzić sam, więc węzeł biorący udział w tzw. kopaniu, o czym będzie za chwilę, on faktycznie musi mieć pobrane 300 GB. Nie są one potrzebne do wygenerowania nowej transakcji.

*Czy przestrzeń kluczy publicznych jest plus minus tak duża, jak prywatnych. Jeśli tak, to czy mogę przypadkiem wygenerować klucz prywatny do portfela innej osoby.*

Można zrobić ćwiczenie matematyczne i obliczyć prawdopodobieństwo takiego zdarzenia, ale ono jest kosmicznie małe. Jeśli ktoś ma świra matematycznego to dla niego odpowiedź brzmi „tak", natomiast w prawdziwym życiu odpowiedź brzmi „nie". Nie jest to możliwe.

*Czy 256 bitowy klucz w postaci 00….001 to nadal klucz 256 bitowy? A klucz 0000…000010? Czy jest gdzieś granica?*

Jeśli cyferek było 256, to tak. Gdy klucz ma jedyną jedynkę na ostatniej lub przedostatniej pozycji - tak. Z definicji klucz o rozmiarze n bitów ma 2^n wariantów czyli taka jest właśnie liczba możliwych kombinacji zer i jedynek jakie można obrać i użyć jako klucza w algorytmie szyfrowania. Niezależnie od tego, czy wartość taką zapiszemy w postaci dwójkowej, dziesiętnej czy szesnastkowej.

# 00:56:24 Generowanie jednostek kryptowaluty

Wcześniej po cichu prześlignęliśmy się nad problemem, że chcielibyśmy przelewać środki z jednego adresu na drugi, ale nie bardzo wiemy skąd one się tam wzięły. Więc teraz będzie właśnie o generowaniu jednostek kryptowaluty. Odpowiemy na pytanie „skąd się biorą nowe bitcoiny". Prosta odpowiedź - każdy blok pozwala autorowi bloku na wygenerowanie z powietrza 6 i ćwierć bitcoina (po cenach z poranka 16.01.2021 to około 900 tysięcy złotych).

Uczestnicy sieci bitcoinowej będą konkurować o możliwość wykonania nowego bloku i ogłoszenia go właśnie dlatego, że mogą w tym bloku zawrzeć transakcję, która bierze bitcoiny z adresu „zero", czyli nieistniejącego. Taka transakcja i takie bitcoiny są legalnym elementem każdego bloku, i to jest właśnie źródło nowych bitcoinów. Nietrudno zgadnąć, że każdy górnik kopiący bloki ustawi swój portfel jako adres docelowy dla nowych bitcoinów. Kim jest górnik? O tym za chwilę.

Bardzo chytrym wynalazkiem twórcy Bitcoina było wbudowanie w całą kryptowalutę mechanizmu zapobiegającego inflacji. Niebezpieczeństwo było takie: jeśli dziś w obiegu jest X bitcoinów a za ileś lat będzie ich w obiegu 2*X, to mogą one tracić na wartości. Istnieje mechanizm zapobiegający temu - bitcoinów przybywa coraz mniej. Na początku istnienia sieci każdy blok mógł wygenerować 50 nowych Bitcoinów. Ta wartość dzieli się na pół mniej więcej co 4 lata, przeszliśmy przez 25, 12.5 i teraz mamy 6 i ¼ nowego bitcointa w każdym bloku. Można wybiec w przyszłość i policzyć w którym momencie tych nowych bitcoinów już nie będzie. Łącznie zamierzeniem twórcy protokołu było to, aby zaistniało 21 milionów

bitcoinów, i aktualnie około 88% tej liczby już jest wygenerowane. Dzięki temu, że przybywa ich coraz mniej, a coraz więcej ludzi chciałoby je posiadać, ich cena rośnie.

Nie wiadomo ile bitcoinów przepadło, czyli nastąpiła sytuacja, w której posiadacz środków stracił klucz prywatny. Wszyscy wiedzą, że los taki spotkał pewien procent portfeli, zaś środków z odnośnych adresów już nikt nigdy nie będzie w stanie ich w jakikolwiek sposób ruszyć. Nie odtworzymy klucza prywatnego tak, jak nie odtworzymy napisu ze skrótu. I to jest smutne, no bo znane są historie ludzi, którzy mieli laptopa, mieli jakieś bitcoiny na tym laptopie które były warte kilka centów w chwili wykopania, i komuś się ten laptop zepsuł, został wyrzucony, a po latach okazuje się ile warte byłyby te środki do których klucz prywatny był na zepsutym laptopie. Właściciel takiego laptopa rozważał przeoranie całego wysypiska śmieci aby go znaleźć, zreanimować dysk twardy i w ten sposób sobie te klucze prywatne odzyskać. Wiele smutnych historii. Tak samo twórca Bitcoina - szacuje się że on wygenerował grubo ponad milion bitcoinów samodzielnie, jak sobie zajrzymy do najstarszych bloków, to sobie zobaczymy że one sobie tam leżą po prostu i nikt ich nie dotyka, mimo że byłyby warte niewyobrażalną fortunę. Nie wiadomo tak naprawdę czy twórca ma do tych adresów klucze prywatne, czy nie ma, czy dbał o to lub nie dbał - jeszcze do tego wrócimy.

Zachęta nr 2 do kopania. Ona jest potrzebna, bo gdyby kopiący dostawali tylko premie, to nie mieliby żadnej zachęty, by dołączyć do tych bloków bloków jakiekolwiek inne transakcje oprócz tej generującej nowe środki. Mogliby stworzyć tylko tę transakcję która tworzy nowe bitcoiny, nie dołączać niczego więcej, i tyle. Dlatego właśnie drugą zachętą dla tworzących nowe bloki, jest mechanizm prowizji. Do każdej transakcji, która jest zgłaszana przez użytkowników, jako coś co chcą wykonać, do każdej z nich jest dołączona deklaracja, jaką część przekazywanych środków tworzący blok może dla siebie wziąć. Ta wartość jest niezależna od kwoty, jaka jest przelewana, ją się definiuje jako satoshi za jeden bajt. No bo jeśli mamy zlecenie transakcji między wieloma adresami (łączenie lub rozdzielanie), zapis będzie dłuższy a jeśli między dwoma adresami, to będzie mniej więcej 200 bajtów. Deklarujemy, jaką prowizję jesteśmy gotowi zapłacić dla osoby generującej blok, za to że ona uwzględni naszą transakcję w swoim bloku. Ponieważ transakcji na przetworzenie czeka o wiele wiele więcej niż mieści się w jednym bloku, to im większą prowizję zadeklarujemy, tym większe prawdopodobieństwo, że osoba generująca blok dobierze sobie akurat naszą transakcję do swojego bloku. Tutaj widzimy szacowane opóźnienie, czas zawarcia transakcji w bloku, w zależności od tego, jaką prowizję zdefiniujemy.

I tutaj takie prowizje, jak 200, 300 czy 400 satoshi za jeden bajt, to one są niskie, to znaczy ten screenshot był zrobiony we względnie spokojnych czasach, gdy jest jakaś bańka bitcoinowa, i wszyscy chcą jednocześnie przetwarzać transakcje, to prowizje bywają o wiele, wiele większe, no bo jak ktoś przewala między adresami bitcoiny warte dziesiątki milionów, to stać go, żeby zapłacić tysiące. I w związku z tym, że w jednym bloku mieści się jakieś 1,5 do 2,5 tysiąca transakcji, to z takich transakcji tworzący blok uciuła sobie jeszcze około 1 bitcoina. I w miarę, jak liczba generowanych monet będzie maleć, to głównym zarobkiem dla generujących mają być właśnie prowizje.

Całość tej sieci, opiera się więc tak naprawdę na chciwości. Aby cała sieć działa, ktoś musi formować nowe bloki a w nich umieszczać przetwarzane transakcje. Poznaliśmy zachętę i do jednego, i do drugiego. W efekcie mamy nowe bloki z transakcjami.

Krótkie podsumowanie:

- wiemy już mniej więcej, jak działają przelewy - gdy tworzymy nową transakcję, podajemy adres źródłowy, adres docelowy, przekazywaną kwotę i prowizję, jaką jesteśmy gotowi zapłacić, i to wszystko podpisujemy kluczem prywatnym (stowarzyszonym z adresem źródłowym)

- wysyłamy tę transakcję (ciąg bajtów) do sieci P2P, czyli do węzłów bitcoina, i ona trafia do puli. W puli jest bardzo dużo transakcji, tworzący bloki mogą sobie swobodnie dobierać transakcje do umieszczenia w bloku, ale w ich najlepszym interesie jest dobierać te, które płacą największą prowizję w przeliczeniu na bajt
- górnicy (ci którzy „kopią") próbują próbują sformować bloki z transakcji
- gdy blok zostanie sformowany i dołączony do blockchaina, to wtedy teoretycznie nasza transakcja jest już zrealizowana i ktoś, kto przejdzie sobie od początku do końca po wszystkich blokach, to w tym ostatnim bloku ją dostrzeże i będzie wiedział, skąd dokąd które środki przekazaliśmy.

Ale nie na pewno! O tym później.

# 01:08:15 Regulacja trudności

…czyli w jaki sposób powstrzymać tych wszystkich ludzi przed generowaniem bloku i zarabianiem 900 tysięcy zł tak często jakby chcieli. Więc - wygenerowanie nowego bloku musi być trudne, bo chętnych na prowizję jest wielu. Założeniem projektowym całego protokołu Bitcoina jest to że nowy blok ma się pojawiać średnio co 10 minut, czyli te 2500 nowych transakcji ma być z sukcesem uformowane w jeden nowy blok co mniej więcej taki okres czasu. I to będzie czasem minuta, czasem 20 minut. Nie będzie jakiejś strasznej regularności, ale oczywiście krzywa Gaussa będzie taka, że najczęstszy odstęp będzie faktycznie w okolicach tych 10 minut.

Potrzebujemy jakiegoś sposobu na to żeby każdy chętny miał równe szanse ale to nie znaczy że to będą sprawiedliwe szanse. One będą równe w tym sensie, że każdy jest w stanie dołączyć i wykonać czynności dzięki którym jakąś tam swoją szansę zdobędzie. I ten mechanizm musi być autonomiczny, to znaczy on nie może zależeć od żadnego człowieka, od jakiegoś losowania, od czegoś co przyjdzie z zewnątrz. To sama sieć, sam algorytm musi wiedzieć, w jaki sposób tę trudność realizować.

Odpada pomysł polegający na tym, że gromadzimy wszystkich ludzi którzy chcą być operatorami węzłów sieci i losujemy spośród nich autora bloku. Trzeba by ufać losującemu, że on faktycznie będzie losował a nie wybierał swoich kumpli. Nie może to być taki mechanizm, że będziemy ślepo losować numer telefonu, no bo wtedy by się okazało, że jacyś bogaci gracze albo założą nowy telekom albo kupią istniejący i wtedy będą mieli sto milionów numerów telefonów a taki zwykły człowiek będzie miał jeden, dwa, albo trzy numery.

Wymyślono więc troszkę inną rzecz czyli Proof of Work - dowód, że wykonało się jakąś pracę, czyli jakiś konkretny wysiłek ze strony węzła wszedł w formowanie transakcji w bloki. I tutaj wracamy do funkcji skrótu. Pamiętacie być może skrót napisu „Litwo Ojczyzno moja" złożony z 64 znaków szesnastkowych. Liczby szesnastkowe mają cyfry od 0 do 9 i od a do f (zakres cyfr zależy tak naprawdę od podstawy systemu liczbowego). Przypomnimy sobie, że zawartość hasha jest de facto losowa, nie potrafimy jej przewidzieć ani odgadnąć, jaka cyfra będzie np. na pierwszym miejscu skrótu.

Zauważmy, że w jednym przypadku na szesnaście na początku pojawi się zero. W jednym skrócie na 256 na początku będą dwa zera. W jednym skrócie na 4096 na początku będą trzy zera i tak dalej. Pamiętacie, że nie da się w żaden sposób przewidzieć jak będzie wyglądał hash, każda zmiana czy kolejna litera na wejściu całkowicie miesza wartością skrótu. Więc nie jesteśmy w stanie założyć sobie, że wygenerujemy jakiś skrót który będzie miał na początku pięć zer, albo siedem. Jedyna opcja to policzyć i sprawdzić, co wyszło.

W związku z tym jest to dobry sposób na to żeby regulować trudność. To znaczy mówimy w jakimś momencie że na przykład od tej chwili legalne są tylko te bloki których skrót ma na początku trzy zera. No i wtedy wszyscy próbują sobie te transakcje które dobrali poustawiać w różnej kolejności i próbować różne warianty przemieszane, żeby na końcu dostać blok ze skrótem spełniającym jakieś tam tego typu kryterium. Jeśli 4 tysiące ludzi wykona po jednej próbie wygenerowania bloku, to średnio jednemu się uda. I to będzie właśnie ten szczęściarz, który dostaje premię za wygenerowanie jednego bloku. On wtedy mówi wszystkim: słuchajcie udało mi się znaleźć taki blok, wysyła tę informację do sieci P2P.

Wtedy wszyscy sprawdzają czy faktycznie hash jest ok, tzn. czy spełnia wymaganą trudność. Sprawdzają też oczywiście czy wszystkie transakcje z bloku są legalne, czyli nie próbują przelać więcej środków niż jest na danym adresie, czy transakcja generująca nowe bitcoiny nie próbuje wygenerować ich więcej niż jest dozwolone itd. Jeśli wszystko się zgodzi no to wszystkie węzły dołączają sobie taki blok do blockchaina i zaczynają od nowa próbę generowania kolejnego bloku, z następnymi transakcjami.

Jak sobie popatrzymy na obecne bloki to tam jest obecnie aż 19 zer na początku i obecnie taka trudność to jest jeden legalny hash na 75 tryliardów możliwości. Czyli średnio tyle prób są w stanie przerobić co 10 minut wszyscy, którzy chcą generować nowe bloki, aby znaleźć jeden pasujący. Sama trudność jest regulowana automatycznie. W protokole Bitcoina co mniej więcej dwa tygodnie następuje sprawdzenie jak często generowane byłyby bloki w tym minionym okresie. Jeśli zbyt często, bo przybyło nowej mocy obliczeniowej, to trudność jest zwiększana, aby zachować mniej więcej 10 minut odstępu między każdymi między kolejnymi blokami. Dwutygodniowy odstęp służy do tego aby jakieś krótkotrwałe zaburzenia nie wpływały na trudność. Jeśli moc obliczeniowa sieci spadnie to dzięki odpowiedniej adiustacji trudność też spadnie.

# 01:16:25 Konsensus

Co się stanie gdy jednocześnie powstaną dwa różne legalne bloki i pół sieci usłyszy o jednym, a pół sieci usłyszy o drugim? To nie jest łatwy problem i na tym wiele kryptowalut przed Bitcoinem się wykładało, tzn. nie wchodziło do użycia właśnie przez to, że ten problem nie był rozwiązywany w sposób w który by działał samodzielnie i niezależnie, bez żadnego zewnętrznego arbitra.

Popatrzmy sobie na mapę kabli podmorskich, które obsługują internet na całym świecie. Ich jest dużo, są nadmiarowe, widać że dookoła niektórych kontynentów to są całe pęczki, ale jest jeden taki myk, są takie miejsca jak na przykład Australia, gdzie wystarczą dwie celnie rzucone kotwice, albo terroryści którzy podłożą dwie bomby, żeby cały kontynent odciąć od internetu. Dobra te slajdy się lepiej sprawdzały kilka lat temu, gdy nie było jeszcze internetu od Elona Muska, ale z tego co wiem to StarLink chyba w tej chwili obsługuje tylko północną półkulę, no więc roboczo zakładamy, że Australia może być relatywnie łatwo odcięta od całego internetu.

W Australii też będą wtedy kopiący bitcoiny, co się w takiej sytuacji wydarzy? Weźmy sobie stan rzeczy, w którym cała sieć działa jak należy, bloki pojawiają się systematycznie, co 10 minut pojawia się nowy blok i w tym momencie odcina Australię od internetu. I teraz Australia, użytkownicy czy węzły bitcoina w Australii słyszą tylko siebie, a cała reszta świata komunikuje się nadal bez zmian, ale Australii nie słyszy. Przyjmujemy roboczo, że Australia miała 10% całej mocy obliczeniowej, a reszta świata miała 90%, co się wydarzy?

Najprawdopodobniej reszta świata wygeneruje kolejny blok wcześniej, ale może się zdarzyć - tego nigdy nie wiadomo - że w Australii też uda się wygenerować nowy blok. Więc następuje rozdwojenie, to znaczy mamy blockchaina, który nie jest spójny, i co dalej?

Reszta świata raczej będzie szybsza, ale ponownie jest jakieś niezerowe prawdopodobieństwo że Australia dotrzyma tempa i że również w jakimś czasie wygeneruje sobie również drugi blok z tych rozdwojonych.

Niemniej matematyki nie oszukamy, statystyka gwarantuje, że reszta świata będzie jednak do przodu czyli te 90% sieci, 90% mocy obliczeniowej będzie generować bloki szybciej, a jak w Australii zostało 10% mocy, no to tam blok się będzie pojawiać nie co 10 minut tylko co 100 minut. Wszyscy w Australii zauważą oczywiście, że kontynent że nie ma komunikacji z resztą świata zaś kopanie idzie dużo wolniej. Tak samo reszta świata zobaczy brak Australii i dużo mniej znaczący spadek prędkości generowania bloku czyli średnio 11 minut, a nie 10.

Awaria zostaje naprawiona i znowu wszyscy mogą się komunikować. Co się dzieje w takiej sytuacji? Protokół jest brutalny. Dłuższy łańcuch wygrywa. Bloki stanowiące krótszy łańcuch były przez pewien czas widoczne tylko w Australii, tam stan był spójny, to była jedyna wiedza jaką tam mieli. Gdy łączność zostaje przywrócona i te węzły w Australii dowiadują się że istnieje dłuższy łańcuch, no to one po prostu zapominają o tym krótszym, swoim własnym, i od tej chwili wszyscy znowu operują na tym dłuższym blockchainie i do tego ostatniego bloku po prawej stronie będą próbować dopisać nowy.

To jest problem który jest znany jako double spend attack (podwójne wydawanie środków). Polega na tym, że jeśli w tym szarym bloku po prawej stronie ktoś zapłaciłby bitcoinami za Teslę na przykład, to tam byłaby transakcja przekazująca należność z adresu kupującego na adres salonu samochodowego, blok z nią został wydobyty i wszyscy zainteresowani patrzą że ojejku jak fajnie, transakcja się udała, bardzo proszę oto są kluczyki do Tesli. Klient sobie odjeżdża Teslą, a po godzinie albo po dobie sprzedawca dowiaduje się że tak naprawdę jednak ten transakcji nie ma, bo ona w tych blokach na górze obrazka nigdy nie została uwzględniona, bo ta górna reszta świata nie słyszała rozgłoszonej transakcji zakupu Tesli. Wówczas sprzedawca zostaje bez bitcoinów i bez Tesli.

Dlatego właśnie bitcoin nie nadaje się do tego, żeby pójść do sklepu i nim płacić, bo dopiero przykrycie bloku w którym jest nasza transakcja innymi blokami, dopiero to daje nam rosnącą gwarancję, że historia się nie cofnie, że nie będzie jakiejś zmiany, która by unieważniła blok z tą naszą transakcją. Z tego co wiem to przyjmuje się że z 4 czy 5 bloków na tym naszym to jest wystarczające zabezpieczenie.

Ale wyobraźmy sobie że mamy Bitcoina - sieć która ma jakąś określoną moc obliczeniową - i nagle ktoś dołącza z dwa razy większą mocą obliczeniową do tej sieci. Ten ktoś będzie w stanie generować bloki dwa razy szybciej czyli on będzie w stanie wykonać taką sekwencję działań: wydać swoje bitcoiny, otrzymać jakieś dobra, a potem cofnąć się do bloku sprzed swoich transakcji, wygenerować więcej bloków ale bez uwzględniania tych swoich transakcji i potem ogłosić taki dłuższy łańcuch. Wówczas miałby zarówno bitcoiny jak i dobra, które za nie kupił.

W przypadku Bitcoina jest to niemożliwe, bo wszystko jest po prostu zbyt ustabilizowane, natomiast jest wiele innych malutkich kryptowalut, w stosunku do których taki atak był skutecznie przeprowadzany, tzn. ktoś wynajmował sobie jakąś farmę serwerów na AWS, dołączał tyle mocy obliczeniowej że to stanowiło ponad połowę istniejącej, i w ten sposób był w stanie fałszować historię, przepisywać ją, dwa razy wydawać te same środki.

Przepustowość sieci bitcoin to jest około 5 transakcji na sekundę, można to obliczyć dzieląc ok. 2000 transakcji w bloku przez 600 sekund na jeden blok. To jest niewiele, np. Visa chwali się, że jest w stanie przetworzyć w ciągu sekundy jakieś 4000 transakcji. Dysproporcja jest spora, ale od jakiegoś czasu w użyciu jest tak zwana Lightning Network. Lightning to jest taki wynalazek że można głównym łańcuchu zablokować jakieś środki, i w obrębie mniejszej grupy wymieniać się transakcjami które prawie nic nie kosztują. Trwają też

bardzo szybko, bo są na takim jakby miniblockchainiku, tak to można o tym pomyśleć i dopóki stan rzeczy na tym małym nie zostanie zamrożony (co skutkuje rozejściem się finalnego stanu na główny blockchain), to tam działa szybko.

Ogólny problem jest jednak taki, że jak robi się gorąco, bo nie wiem, bitcoin wczoraj kosztował 40k a dziś kosztuje 70k, i wiele ludzi chce sprzedać a wielu chce kupić, to oni są wszyscy zblokowani tą przepustowością, i wtedy te marże czyli prowizje strzelają w kosmos. Gdy damy dużą prowizję, no to ktoś dobierze tę naszą transakcję do kopanego bloku chętniej, a ci oferujący mniejszą prowizję się nie załapią i muszą czekać na następny blok i następny i następny, i ta ich transakcja może tak naprawdę nigdy nie zostać zrealizowana, jeśli prowizja nie będzie wystarczająco duża i zawsze będą na końcu kolejki.

# 01:28:08 Co to jest kopalnia i czym się kopie bitcoiny

Na samym początku istnienia bitcoina, gdy cały ten koncept był dyskutowany w bardzo wąskim gronie ludzi interesujących się kryptografią, jedyną opcją kopania nowych bitcoinów było używanie procesorów. Możemy sobie poszukać bloków z tamtych czasów, otwórzmy serwis Blockchain Explorer. Można tam podglądać zawartość bloków, np. widać że nowy był minutę temu, 3 minuty temu, 4 minuty temu, no jakoś tak często się generowały ostatnio, ale my chcemy spojrzeć na te starsze.

Cofniemy się w czasie do roku 2010 i widzimy że tutaj są bloki o numerach stanowiących 10% obecnych, czyli tak naprawdę blockchain miał wtedy 1/10 historii, przy okazji możemy zobaczyć że pojawiają się bloki które mają po 216 bajtów i gdy blok jest tak mały, to wiadomo, że w nim się znajduje tylko jedna  transakcja z wygenerowaniem nowych środków i tu właśnie ten przykład którym mówiłem, że tutaj ten zielony glob to on informuje że ten adres przechowuje niewydane bitcoiny od 2010 aż do teraz, i tego jest cała masa i nie wiadomo czy ktoś ma klucze prywatne do tego czy nie.

W każdym razie, jak sobie popatrzymy na listę tych ówczesnych bloków sprzed 10 lat, to zobaczymy że na początku hasha jest 9 zer, więc 16 do potęgi 9 dzielone przez 600 sekund - to wymagało sprawdzenia około 120 mln hashy i to oznacza że cała ówczesna moc obliczeniowa sieci bitcoin to było mniej więcej sześć topowych procesorów Intela. Dość niewiele.

Oczywiście gdy cały koncept zyskał na popularności no to ludzie się zorientowali że używanie wielu komputerów naraz dużo kosztuje i odkryto czy też zorientowało się że obliczenia można wykonywać na karcie graficznej, bo chip GPU, to jest taka naprawdę od kilkuset do kilku tysięcy malutkich procesorów. Każdy z nich ma ograniczony zestaw instrukcji, dostęp do małej ilości pamięci, są różne inne ograniczenia, ale ich jest dużo i one liczbą jednostek obliczeniowych nadrabiają niewielką wydajność każdej z nich.

Topowy Radeon z lat 2011/12 był w stanie zastąpić kilkadziesiąt procesorów, a jak włożyliśmy trzy takie karty do jednego komputera to mogliśmy zastąpić nim sto procesorów. Wyścig zbrojeń rozpoczął się od kart graficznych, tylko że to również nie wystarczyło, bo ludzie myśleli: po co brać jakieś chipy ogólnego przeznaczenia, takie jak procesor albo chipy które służą do czegoś zupełnie innego, do generowania grafiki. A może zamiast tego zrobić kawałek krzemu którego jedynym zadaniem będzie łojenie tych hashy SHA-256?

Tak właśnie zrobiono i to jest przykładowy - pierwszy chyba jaki zaistniał moduł w formie gwizdka USB - Block Erupter. Tak nazywał się produkt, który służył wyłącznie do kopania

bitcoinów. Tak naprawdę poza jakimiś tam małym układem pamięci, układem komunikacyjnym, to jedyne co on potrafi robić to liczyć hashe SHA-256, tylko to. Za to robi to diablo szybko, 300 mln hashy na sekundę, czyli tyle co 10 ówczesnych procesorów intela. To jest wprawdzie mniej niż dobra karta graficzna, ale gdy weźmiemy hub USB, i włożymy tych gwizdków dużo, no to mamy już odpowiednik 20 kart graficznych, czyli ten wyścig zbrojeń przeszedł na nowy etap.

Tutaj jest taki przykładowy gwiazdeczek, czyli Block Erupter, którego kupiłem jakiś czas temu jako przedmiot kolekcjonerski. Te jego 300 milionów hashy na sekundę to już wtedy było nic. Przy ówczesnej wartości bitcoina i ówczesnej łącznej wydajności sieci, ta zabawka byłaby w stanie zarobić 1 grosz w ciągu 100 lat. To nie jest dużo.

Chciałbym pominąć troszkę historii. Zwróćcie uwagę, że robimy dość fundamentalny przeskok. Przed chwilą było 14 Ghps, tutaj mamy prawie 14 tysięcy Ghps czyli terahashe na sekundę. To jest urządzenie o mocy żelazka, nadal służy tylko do obliczania SHA-256 ale to z prędkością zwiększoną do nieprzytomności. Chciałem zwizualizować jakoś moc obliczeniową tego Antminera. Widzimy tu kilka tysięcy kropek a każda z nich symbolizuje jedną kartę graficzną zastępowaną przez tego jednego Antminera. Co więcej - to nie jest najnowsza konstrukcja, ona ma już parę lat. Antminer T19 wchodzi na 95Thps, takie żelazko ma wydajność siedmiu poprzednich, i kosztuje jakieś 5k dolarów.

Jest jedna rzecz, na którą warto zwrócić uwagę, to znaczy wydajność w przeliczeniu na pobieraną moc. Otwórzmy sobie jakiś kalkulator kosztów, i popatrzmy sobie czego możemy się spodziewać. Gdy sobie weźmiemy 13Thps, czyli ten poprzedni Antminer T9, który ciągnie jakieś 1500W, koszt prądu w stanach to jest 10 centów, czyli 40 groszy za kWh u nas, no to widzimy że na tym poprzednim Antminerze T9 (wydajność 13Thps), to my nie zarabiamy, bo wydamy na prąd więcej niż warte będą wykopane przez niego bitcoiny.

Policzymy wariant droższy - urządzenie za 5k dolarów, wydajność 95Thps. On zużywa 3300W, no to widzimy że zyski są dość skromne, to znaczy on w ciągu roku to nawet nie zarobi na połowę swojej ceny, bo musimy pamiętać że ta moc obliczeniowa to ona rośnie, i więcej ludzi będzie sobie kupować te Antminery T19 albo i kolejny model i ten nasz to musimy dobrze sobie skalkulować.

Dlatego właśnie w naszej strefie klimatycznej nie da się kopać bitcoinów, bo my oprócz tego że potrzebujemy prądu do zasilenia koparek, to potrzebujemy go też do chłodzenia. Gdy ktoś siedzi na Islandii albo na Syberii, to ma zimno gratis. Więc ci którzy mają zimne rejony no to oni są uprzywilejowani, dodatkowo, jak jesteśmy w krajach o niższej kulturze społecznej i możemy ukraść prąd, albo możemy przekupić właściciela czy tam operatora jakiejś elektrowni wodnej na przykład, żeby odpalał nam część tego prądu na lewo, czyli żeby ten prąd był darmowy, no to wtedy te zyski one się już robią konkretne. Nie płacimy za prąd, nie musimy niczego chłodzić, ewentualnie w grę wchodzi jakaś Islandia z energetyką geotermalną i to już wtedy kosztowo wygląda zupełnie inaczej.

Tu mam obrazek, którzy mnie zaszokował, gdy go zobaczyłem po raz pierwszy. Oto kopalnia kryptowalut. Każdy taki mały pojedynczy regał, on ma sprzętu za lekko licząc 100 tysięcy dolarów, czyli jeden taki rząd to będą grube miliony, a no te rzędy one się ciągną w nieskończoność. To jest prawdziwe zdjęcie z kopalni gdzieś w Rosji. No i teraz widzimy, że jeśli ktoś planował wziąć kredyt, by kupić Antminera i konkurować z takimi zawodnikami, to może nie być najlepszy pomysł na inwestowanie pieniędzy i czasu.

Oczywiście kopalnie mogą wyglądać też trochę inaczej. Wspomniałem parę razy słowo kopalnia. No oprócz tego że to jest jakieś tam zgromadzenie górników w jednym miejscu, to w świecie kryptowalut kopalnia oznacza spółdzielnię której członkowie kopią na wspólny rachunek. Jeśli mamy jedną koparkę, i konkurujemy z całym światem, to gdy już uda nam

się wykopać blok, dostaniemy BTC warte 900k złotych i będzie super. Niestety - możemy się nigdy nie doczekać, dlatego górnicy łączą się w kopalnie, dołączają do jakby wspólnej puli, gdzie moc obliczeniowa jest sumowana i jeśli takiej kopalni czy takiej spółdzielni uda się wykopać blok, to uczestnicy dzielą się zyskiem proporcjonalnie do włożonej mocy obliczeniowej. Sposobów na rozliczanie jest wiele, każdy może się podłączać do kopalni, która najbardziej mu odpowiada. To dobry sposób na to, aby coś jednak zarobić. Bo samodzielnie to można nigdy nie wykopać ani jednego bloku, nawet gdy włoży się furę siana w sprzęt.

Ilość energii zużywanej na kopanie bitcoina jest nieprzytomnie wielka. Gdy pierwszy raz opowiadałem tą historię 3 lata temu, wówczas zużycie prądu było na poziomie 27 TWh rocznie czyli troszkę więcej, niż produkuje elektrownia Bełchatów. W tej chwili kopanie bitcoina pochłania tyle co trzy elektrownie Bełchatów. I jak sobie tą makabryczna ilość energii podzielimy na sztuki transakcji, to się okazuje że na przetworzenie pojedynczego przelewu z adresu A do B poświęcamy (cudzy, niekiedy ukradziony) prąd wart 360 złotych. Oczywiście gdy mówimy o efektywności systemów płatniczych takich jak Visa czy Mastercard, to u nich przetworzenie jednej transakcji kartowej to są maluteńkie ułamki jednego grosza, więc to jest totalnie nieporównywalne. Gdyby Bitcoin był krajem, to byłby tam na 30-którymś miejscu jeśli chodzi o zużycie energii elektrycznej.

## 01:43:54 Jak przechowywać klucze prywatne

Rozdział bonusowy którego wcześniej nie zapowiadałem. Bardzo dużo się słyszy, że gdzieś komuś ukradziono bitcoiny, albo ktoś w ten czy inny sposób stracił bitcoiny itd. Zastanowimy się, jak przechowywać klucze prywatne, bo w świecie Bitcoina to jest najcenniejsza rzecz jaką mamy. Jeśli ktoś pozna ten klucz i sobie wytransferuje nasze środki, to żaden sąd na świecie, żadna instancja jakiegokolwiek prawodawstwa nie przywróci nam tego. Po prostu - transakcja wykonana, klepnięta, przykryta blokami, nic się nie da zrobić.

Musimy kluczy prywatnych strzec jak oka w głowie. Jest opcja, aby trzymać swoje środki, swoje bitcoiny, w giełdzie kryptowalut, to są w zasadzie dwie różne opcje. Albo będziemy trzymać środki na adresie giełdy (a ona będzie pamiętać że jakaś część tamtejszych bitcoinów jest nasza), albo możemy załadować swój klucz prywatny do giełdy (a ona wtedy będzie nim zarządzała, w naszym imieniu wydając dyspozycje transakcji). Dlaczego jest to ryzykowne? Bardzo duża ilość giełd została zhakowana i okradziona. Właściciele innych uznawali, że oni chcieliby wziąć wszystkie środki należące do swoich klientów i zniknąć. Klienci, których środki kontrolowała giełda, kończyli wówczas z niczym.

Druga opcja - możemy zainstalować sobie jakiś portfel bitcoinowy w telefonie, albo na PC. Będzie dobrze, dopóki ktoś się nie włamie do naszego komputera i nie wyszarpie z dysku albo z pamięci klucza prywatnego. Trzeba pamiętać, że zwłaszcza telefony łatwo jest zgubić albo zepsuć albo wrzucić do WC, albo utopić w jeziorze. Komputer też da się zepsuć na różne sposoby, może on na przykład spłonąć. Jeśli macie działające backupy, no to okej, ale kiedy ostatni raz sprawdzaliście, czy wasze backupy rzeczywiście działają?

Można wygenerować sobie adres i klucz prywatny całkowicie na papierze, mieć to wydrukowane, i trzymać sobie w tajemnym miejscu, oczywiście papier też płonie wyjątkowo łatwo, więc też warto się zastanowić ile jakich kopii gdzie będziemy trzymać. Kiedyś napisałem na blogu artykuł o rozdawaniu bitcoinów - pół milibitcoina trzymałem w papierowym portfelu i na potrzeby tego artykułu otworzyłem ten papierowy portfel. Klucz, który tu widzicie żadnych środków już nie kontroluje. Unikalną cechą papierowego portfela jest to, że jeśli nie przelejemy wszystkiego na raz na jakiś inny adres, tylko spróbujemy podzielić i trochę zostawić to stracimy wszystko co próbowaliśmy tam zostawić, więc to jest też ten element którego należy się nauczyć.

Zanim ktoś zacznie się bawić bitcoinami, niech przeznaczy ze 200-300 zł na straty, na koszty nauki. Lepiej stracić małe kwoty, niż potem bezpowrotnie stracić duże kwoty z powodu braku praktyki.

Dobrze, możemy trzymać nasze klucze w bezpiecznym urządzeniu, które kupiliśmy od producenta bezpiecznych urządzeń. Tu historia sprzed tygodnia czy dwóch - gdy ktoś shackuje tego producenta i wyciągnie emaile, adresy i telefony wszystkich klientów, no to będzie tych klientów szantażował, i wysyłał e-maile w rodzaju „obetniemy ci głowę jeśli nie zapłacisz nam okupu w bitcoinach, tu jest nasz adres". Więc smutno jest być użytkownikiem bezpiecznego urządzenia, gdy taka sytuacja się zdarza.

Są też oczywiście przypadki, w których ktoś pozyskał bitcoiny, zabezpieczył klucz prywatny w sprzętowym portfelu, zapomniał hasła, no i się okazuje - też news z poprzedniego tygodnia - że ten ktoś ma 7 tysięcy bitcoinów, 10 prób odgadnięcia, po których urządzenie się zresetuje, i już 8 wypróbował i co teraz. I to jest sytuacja w której albo się będzie miało 250 milionów dolarów albo nie. Taka alternatywa chyba nie daje spokojnie zasnąć.

# 01:50:17 Do czego komu Bitcoin i kto to w ogóle wymyślił

Zbliżamy się pomału do końca. Protokół Bitcoina zaprojektował w roku 2008 niejaki Satoshi Nakamoto, przedstawił on na liście dyskusyjnej jako swój pomysł na rozwiązanie problemu zdecentralizowanego elektronicznego pieniądza. Bo wiele osób wcześniej tego próbowało i zawsze czegoś brakowało. Albo występowała inflacja, albo mieliśmy problem podwójnego wydawania, albo konieczny był zaufany arbiter albo coś jeszcze innego. Wiele było różnych pomysłów na cyfrowy pieniądz, ale żadne rozwiązanie nie była kompletne.

Inaczej było z Bitcoinem. To była pierwsza kompletna wizja, która rzeczywiście mogła zadziałać, to trafiło do geeków, matematycznych nerdów którzy od dawna o tej idei dyskutowali. Zawiązała się grupa, która ulepszała pierwotne oprogramowanie Satoshiego, wymieniali się pomysłami na grupie dyskusyjnej. Sam Satoshi Nakamoto wykopał sam około miliona Bitcoinów w czasach gdy kopał tylko on i potem mała grupka ludzi na kilku komputerach. Te Bitcoiny leżą nieruszone. Tak sobie leżą na tych adresach, co wiemy, bo każdy może sobie popatrzeć w stare bloki. Gdyby tam się jakieś środki ruszyły któregoś dnia - uuuuuu, to by się zrobiło trzęsienie ziemi. Ale na razie się nie zrobiło.

Jest jeden problem - nie wiadomo, kto to jest Satoshi Nakamoto. Zadbał on zawczasu o swoją pełną anonimowość. Wiadomo, że zna angielski, że to prawdopodobnie nie był jego ojczysty język. Satoshi nie odezwał się od 2011 roku, wówczas po raz ostatni napisał coś na wspomnianej liście dyskusyjnej i nigdy więcej nikt już nic od niego nie usłyszał.

Było wiele podejrzeń, parę osób było podejrzewanych o bycie Satoshim. Z drugiej strony - kilka osób bardzo by chciało uchodzić za Satoshiego, ale im akurat nikt nie wierzył. Temat wraca co jakiś czas, ale coraz rzadziej. Parę miesięcy temu czytałem w Wired następującą analizę - ktoś wziął sobie wszystkie znane maile Satoshiego, na osi czasu pogrupował według godzin i spróbował to dopasować do Tokio, Nowego Yorku, Londynu, według domniemanego cyklu dobowego - np. zakładając, że zwykły człowiek śpi o 4 rano. Konkluzją artykułu było że… niczego nie wiadomo.

Nie wiadomo kto wymyślił Bitcoina. To człowiek któremu udało się utrzymać anonimowość.

## Do czego można zastosować Bitcoina?

Trzy konkurencyjne zastosowania. Po pierwsze: opłacanie okupu za odzyskanie danych po udanej infekcji ransomware. Bitcoin jest tu lubiany. Przez przestępców. Po drugie: Zakup nielegalnych usług, bo o towary dużo trudniej. Lewe hostingi w darkwebie, numery kart kredytowych - są często opłacane kryptowalutami. Po trzecie - inwestycja, spekulacja, albo taki skrót który nazywa się HODL czyli Hold On for Dear Life - „trzymaj póki Ci życie miłe". Z założeniem że zawsze wartość kryptowalut będzie rosła.

Pamiętajcie - nie wydawajcie na kryptowaluty więcej, niż bylibyście w stanie podrzeć, wyrzucić i spalić. W każdej sekundzie może się okazać, z jakiejś przyczyny wartość wszystkich bitcoinów zostanie na zawsze wyzerowana, więc nie wydawajcie więcej pieniędzy niż jesteście w stanie przeznaczyć na inwestycje stuprocentowno ryzykowne.

Co do zastosowań - wiele osób próbuje argumentować, że Bitcoina można używać do normalnego obrotu pieniężnego. Nie można. Po pierwsze mała przepustowość, po drugie mała płynność, po trzecie dzikie wahania kursów. Nie da się oprzeć gospodarki na pieniądzu, którego kurs wymiany może skakać o kilkadziesiąt procent jednego dnia. Ubieramy się, jemy, kupujemy mieszkania, samochody a koszty wytworzenia tych wszystkich dóbr są z grubsza niezmienne. Gdybyśmy zarabiali w Bitcoinie i nie wiedzieli czy za miesiąc nasz wypłata będzie warta pięćset złotych czy pięć tysięcy czy pięćdziesiąt tysięcy - nie dałoby się tak żyć i planować przyszłości. Bitcoin nie jest równoważnikiem zwykłego pieniądza stabilizowanego z lepszym czy gorszym skutkiem, ale jednak dającego pewne gwarancje, że bez nadzwyczajnych wydarzeń jego wartość będzie się deprecjonowała w przewidywalnym tempie.

## Zastosowanie blockchaina

To jest wyjątkowo słodkie. Jestem programistą, pracowałem w software house czyli firmie realizującej oprogramowanie dla klientów, którzy potrzebowali czegoś napisanego na zamówienie pod ich potrzeby. Jakieś trzy-cztery lata temu u wielu potencjalnych klientów pojawiło się jakieś takie nagłe przekonanie, że o rany, blockchain będzie przyszłością wszystkiego i że od tej chwili praktycznie każdy soft będzie z blockchainem i czy my mamy ludzi, którzy to znają, bo trzeba na szybko robić nowe kryptowaluty i wdrażać jakieś nowe tokeny i tak dalej.

Było wtedy jakieś takie dziwne wzmożenie: że służba zdrowia (czyli pewnie jakieś zapisy medyczne), że księgi wieczyste, że jakieś systemy uwierzytelniania czy systemy logistyczne - to wszystko nagle będzie na blockchainie bo on będzie taki wspaniały i niefałszowalny. I wiecie? To wszystko bzdura, ale taka piramidalna, bo w prawdziwym życiu ludzie się mylą i zapisy trzeba móc poprawić. A w wielu miejscach potrzebne jest zachowanie tajemnicy, np. w przypadku wyników badań lekarskich, chorób itp. Nie możemy tego wrzucić w blockchaina i mówić że od tej chwili będzie super. Chyba, że na blockchainie będziemy składować dane zaszyfrowane co rodzi oczywiście całą nową klasę problemów. Skracając opowieść - blockchain zasadniczo nie ma żadnych zastosowań oprócz kryptowalut. Porada: jeśli widzicie jakiś produkt który ma w nazwie IoT oraz blockchain to uciekajcie! To jasny sygnał, że ktoś chce zrobić kasę na buzzwordach ale raczej nie dostarczy czegoś, co działa.

# 01:58:43 Dlaczego Bitcoin jest tyle warty?

Dotarliśmy do finalnego pytania - dlaczego bitcoin jest wart XXXXX dolarów (16.01.2021 - 35 tysięcy USD). To jest bardzo dobre pytanie, na które nie znam odpowiedzi, ale wydaje mi

się, że przyczyną jest ludzka chciwość - wielu chciałoby się nie narobić, a zarobić. Cena bitcoina, która wystartowała od centów, potem przez dolary i setki doszła do dziesiątek tysięcy dolarów, inspiruje wielu ludzi. Myślą oni: „może się spóźniłem na ten moment gdy BTC był po dziesięć, sto lub tysiąc dolarów, ale jak dziś kupię za 10 000, to może kiedyś będzie kosztował milion i dużo zarobię?". No i kupują.

Ja osobiście swój niewielki ułamek bitcoina kupiłem kilka lat temu tylko po to, żeby poczuć jakiekolwiek emocje związane z obserwowania kursu. Włożyłem w to pieniądze, które mam już mentalnie pożegnane. Co więcej - jestem przekonany, że gdy zdecyduję się je sprzedać, to albo coś pomylę i je stracę, albo zostanę oszukany i je stracę, albo zrobię coś innego, zawinionego lub nie, ale żadnych zysków nie zobaczę. Z tym nastawieniem żyje mi się normalnie, mogę obserwować wahania Bitcoina, patrzeć na te swoje wirtualne złotówki w które w ogóle nie wierzę, ale daje mi to przyjemność, takie podejście jest chyba wystarczająco zdrowe.

Dojechaliśmy do końca. Ponownie bardzo was proszę, abyście nie kupowali bitcoinów dziś wieczorem. Jeśli ktoś ma ochotę pobawić się albo wierzy że to jest przyszłość i chce zainwestować - proszę się dokształcić. Wydać stówę albo dwie stówy na te kryptowaluty, które człowiek być może straci ale za to otrzaska się nieco z oprogramowaniem, zanim dokupi więcej za większe kwoty. Nie polecam żadnych giełd ani żadnych takich linków, bo nie jestem na bieżąco i też nie mam wiedzy, która by pozwalała na dawanie rekomendacji. Ale np. blog zrozumiecbitcoina.pl jest sensowny. Tam można rzeczywiście zdobyć wiedzę, jest pisany bardzo fajną, płynną polszczyzną, podobał mi się. Gdyby ktoś szukał informacji, które giełdy mają jakie prowizje albo jak się te prowizje realizują, to właśnie tam można przeczytać recenzje kilku polskich giełd kryptowalutowych.

**Pytania z czata:**

*Kto zostanie uczestnikami sieci, kiedy kopanie będzie już prawie nieopłacalne?*

Założenie jest takie, że gdy wartość kryptowaluty będzie rosła, to prowizje będą tym, co będzie napędzało chciwość kopiących. Więc choć nie będzie już nowych bitcoinów, to prowizje od nowych transakcji powinny wystarczyć.

*Z jakiego powodu papierowe portfele są jednorazowe?*

Nie należy używać dwa razy tych samych adresów - wbrew temu, co mówiłem podczas całej prezentacji. Każdy adres powinien być użyty tylko raz. Software'owe portfele potrafią to robić automatycznie, papierowy jest wydrukowany raz na zawsze. Papierowy portfel można zasilać ile razy się chce, ale wszystkie środki należy z niego wyprowadzić jedną transakcją. W przeciwnym razie reszta środków może przepaść, automatycznie przeniesie się na adres do którego nie będziemy mieli klucza prywatnego.

*Co z komputerami kwantowymi i ich możliwościami obliczeniowymi w kontekście prób złamania BTC?*

Nie jestem specjalistą, natomiast kryptografia asymetryczna w Bitcoinie jest oparta na krzywych eliptycznych i z tego, co wiem, komputery kwantowe nie są w stanie ugryźć tego problemu albo przynajmniej na razie nie wiemy jak. Jeśli się mylę, proszę o sygnał.

*Co z zastosowaniami blockchaina jako trwałym nośnikiem.*

Jeśli ktoś nam pokaże cały blockchain - wtedy OK. Ale wszystkie „trwałe nośniki" oparte na blockchainie, których doświadczałem jako klient, w najlepszym razie pokazywały mi hash czegoś. Jeśli to był hash PDF-a z regulaminem, wtedy OK, mogę żyć z takim trwałym

nośnikiem, w którym patrzę na dokument i widzę, że się nie zmienił. Do tego nie potrzeba blockchaina, wystarczy funkcja skrótu albo podpis cyfrowy. A gdy ktoś mi pisze „kliknij tutaj aby pobrać regulamin który trzymamy na blockchainie czyli trwałym nośniku” no to to jest śmiech na sali.

*Czy twoim zdaniem realne jest przejście z systemu opartego na nagrodach za bloki dla górników do systemu opartego o opłaty za poszczególne transakcje?*

To już się dzieje, kiedyś było 50 btc w bloku, teraz jest 6.25. Za 3 lata będą 3.125 BTC a prowizje będą stanowić ćwiartkę zysku górnika. To będzie rosło.

*Czy można kupić bitcoiny za prawdziwe pieniądze? Jeśli tak to w jaki sposób?*

Giełdy bitcoinowe. Przelewasz swoje własne złotówki na konto giełdy, giełda odsyła na wskazany adres równowartość w btc, oczywiście po potrąceniu prowizji giełdy i kosztów transakcji (obciążenie na rzecz pośrednika i na rzecz sieci).

# 02:10:57 Zakończenie

Jest 22:15 i ciągle setka obserwujących. Jak na pierwszą gawędę, sukces jest po prostu spektakularny - udało mi się utrzymać waszą uwagę przez tak długo. Normalnie godzina wykładu to już jest coś, ze swojej strony bardzo dziękuję za udział.

Jeśli mielibyście jakieś uwagi, proszę dać znać mailem. Nie wiem, czy mogę się uznać za prawdziwego youtubera, jeśli nie będę apelował o klikanie subów, kciuków, dzwoneczków - ale mam na to wyrąbane. Będę i tak informował wszystkimi kanałami - newsletterem, blogiem i socialami - gdy zaplanuję kolejną gawędę. Kto mnie czytuje, ten nie przeoczy. Jeśli ktoś mnie ogląda tylko na Youtube to ja nie wierzę, że są takie osoby, bo to przecież wszyscy są tu dziś pierwszy raz.

Jeśli mogę wybrać, to bardziej by mi zależało, abyście zasubskrybowali newsletter - na końcu każdego artykułu na blogu jest formularz i na tym mi zależy bardziej, niż na jakichś subach na Youtube. Łaska Google’a na pstrym jeździ koniu a e-mail to e-mail.

Dobrze, stream zajął strasznie długo, jesteście kochani i w ogóle. Trzymajcie się i do następnego razu. Na razie, pa.