Transkrypcja gawędy o tokenach, ICO, NFT i nie tylko - bez ilustracji

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

Uwaga! Tekst jest zapisem półtoragodzinnego monologu. Aby lepiej się go czytało, dokonałem pewnych zmian i modyfikacji - dotyczy to głównie powtórzeń, drobnych omyłek i doboru słów, ale także zwięzłości wywodu. Pominąłem 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/swqnXjG6J_I

[00:00:00] Rozpoczęcie

Dzień dobry dzień dobry! Witam wszystkich na trzeciej gawędzie o kryptowalutach. Nazywam się Tomek Zieliński, jestem autorem bloga informatykzakladowy.pl, dzisiaj będę kontynuował tematy, o których mówiłem wcześniej w dwóch pierwszych odcinkach.

W pierwszej gawędzie zaczęliśmy od kryptowaluty Bitcoin. W drugiej przeszliśmy do Ethereum - ale wtedy nie udało się opowiedzieć wszystkiego. Dziś będziemy mówić o tokenach, ICO, NFT i innych zjawiskach opartych o kryptowalutę Ethereum, będzie to więc głównie kontynuacja części drugiej.

Proszę pamiętać, że temat jest skomplikowany i nie należy inwestować w żadne kryptowaluty tylko na podstawie informacji, które zdobyliście z tego krótkiego cyklu. Jeśli ktoś jest zainteresowany tematem i zamierza zająć się inwestowaniem (czy też hazardem) kryptowalutowym - czytajcie, uczcie się, zdobywajcie jak najwięcej informacji z jak największej liczby źródeł. Zaczynajcie od małych kwot, żeby wypróbować narzędzia i zrozumieć ich działanie, wszystko wyćwiczyć, zrozumieć co jak działa. Dopiero wtedy inwestujcie pieniądze, ale tylko te, które możecie stracić. Ważne, żeby nie wkładać w kryptowaluty gotówki, która będzie konieczna do przeżycia, albo może być szybko potrzebna do pokrycia awaryjnych wydatków. W tej branży po prostu bardzo łatwo jest stracić wszystko.

Aby nie być gołosłownym: jakiś miesiąc temu na Reddicie pojawił się smutny wpis. Pewien człowiek dopytywał, czy on dobrze rozumie swoją sytuację, że właśnie stracił kryptowaluty warte 500 tysięcy dolarów. Bo zrobił na blockchainie operację, której do końca nie ogarniał, a która spowodowała utratę za jednym zamachem wszystkich posiadanych środków. I ludzie mu potwierdzili, że owszem, stracił wszystko. W świecie kryptowalut nie ma drugiej szansy, takiej operacji nikt nie może cofnąć. Na obrazku widać numer tej transakcji - można sobie podejrzeć, co dokładnie się stało i nauczyć się rozpoznawać takie sytuacje, czy też tę klasę zagrożeń. Po prostu uważajcie i nie wkładajcie w kryptowaluty więcej pieniędzy niż możecie stracić i przeboleć tę stratę.

To jest ostatnia część gawędy o kryptowalutach. Tym razem będę się musiał szczególnie pilnować, żeby nie wydostawały się ze mnie cynizm czy niesmak, bo szczególnie w ostatnim czasie mogliśmy zobaczyć, że z kryptowalut ani NFT naprawdę nie wynika nic dobrego. Wydaje się, że wystarczająco dużo czasu już minęło, żeby pojawiło się jakieś sensowne zastosowanie niezwiązane z wyłudzeniami czy przestępstwami - a jakoś uparcie, kurcze, nie chce.

To jest oczywiście moja opinia, każdy może mieć swoją. Postaram się, żeby ta gawęda była możliwie techniczna i żebyście po jej wysłuchaniu wiedzieli jak te rzeczy działają.

[00:04:43] Krótkie przypomnienie części 1 i 2

Poprzednio dowiedzieliśmy się, że aby powstał Bitcoin, potrzebne było połączenie paru różnych koncepcji. Pierwsza z nich to rozproszony rejestr. Rozproszony - czyli taki, którego kopie przechowywane są na wielu komputerach u wielu ludzi. Tak naprawdę każdy, kto staje się pełnoprawnym węzłem sieci Bitcoin, ma u siebie w komputerze kopię całego rejestru wszystkich transakcji, jakie kiedykolwiek zostały wykonane. Dowiedzieliśmy się, w jaki sposób synchronizowane są te dane.

Oprócz tego mieliśmy też blockchain, czyli strukturę danych zapisywaną w rozproszonym rejestrze. Blockchain przechowuje dane o transakcjach, podzielone na tak zwane bloki. Każdy kolejny blok to kilkaset lub kilka tysięcy transakcji. Poznaliśmy mechanizm tworzenia niezaprzeczalnych podpisów cyfrowych pod każdym blokiem i umieszczania takiego podpisu z poprzedniego bloku w bloku aktualnym. Dzięki temu nikt nie jest w stanie zmodyfikować w sposób niezauważony żadnego elementu takiego łańcucha - wówczas podpisy przestałyby się zgadzać.

Sieć Bitcoin to również generowanie jednostek kryptowaluty. Jest określony protokół definiujący, kto i kiedy dostanie ile nowych bitcoinów, wygenerowanych zupełnie z powietrza. Oczywiście każdy chciałby dostawać bitcoiny, ludzie rywalizują o to przeprowadzając tak zwane kopanie. Bitcoinów z czasem przybywa coraz mniej. Omawialiśmy takie koncepcje jak regulacja trudności czy kryptografia klucza publicznego. O tym wszystkim było w części pierwszej.

W części drugiej opowiadaliśmy o drugiej najpopularniejszej kryptowalucie, czyli Ethereum. Na jednostki tej kryptowaluty będę mówił „eter”. Nowością w tej kryptowalucie jest to, że w rejestrze jesteśmy w stanie zapisać nie tylko transakcje, ale i dowolne dane. Czyli liczby, napisy, proste struktury danych. Oprócz tego w blockchainie można także zapisywać smart kontrakty.

Smart kontrakt w sieci Ethereum to program, którego kod (czyli zestaw instrukcji) zostaje zapisany w blockchainie, zaś uruchomienie takiego programu następuje poprzez przekazanie środków (zrobienie przelewu) na adres tego kontraktu. Nowość - swoje adresy mają nie tylko portfele zakładane przez ludzi, ale także smart kontrakty i właśnie przelanie czegoś na adres smart kontraktu jest formą aktywacji funkcji, która w nim siedzi.

Program może dostać jakieś dane wejściowe, może wykonać pewne operacje, a wynik tych operacji może zapisać w blockchainie - tak naprawdę powstaje więc rozproszony komputer. To więcej, niż znany z Bitcoina rejestr przypominający księgi bankowe, ze stanami kont i historią przelewów. Tutaj mamy też programy, które siedzą w blockchainie i które możemy wywoływać, oczywiście opłacając przywilej ich uruchomienia. Każdy węzeł sieci Ethereum, który stara się wykopać nowy blok, będzie musiał wykonać obliczenia ze smart kontraktów aktywowanych w ramach przetwarzanych transakcji.

Instrukcje takiego specyficznego rozproszonego komputera są wykonywane na każdym węźle sieci Ethereum. Obliczenia są deterministyczne, bo nie zależą od niczego innego jak tylko od historii blockchaina (historii wszystkich transakcji) i tych danych, które przychodzą w transakcji aktywującej dane obliczenie. Potem wyniki są zapisywane w blockchainie lub nie są - i tyle.

Część trzecia

- Dwa słowa o wydajności Ethereum
- Co to są tokeny
- Co to jest ICO
- Co to jest NFT
- Co to jest Proof of Stake (oraz Space)
- Inne częste pytania

I to było mniej więcej treścią części drugiej. Teraz mamy część trzecią, w której powiem parę słów o wydajności Ethereum a potem przejdziemy do tematów związanych z zastosowaniami tej kryptowaluty - czyli do tokenów, ICO, czy NFT. Pomówimy też o nowej koncepcji ustalania konsensusu, która jakoś nie może wejść w życie, czyli o Proof of Stake. Na końcu odpowiemy na pytania, które często padają w kontekście kryptowalut.

[00:12:25] Wydajność maszyny wirtualnej Ethereum

Jak wydajny jest ten rozproszony komputer realizowany przez maszynę wirtualną Ethereum? Możemy to w miarę dokładnie obliczyć. Oczywiście, że będzie on dużo wolniejszy od typowego procesora w typowym pececie - instrukcje są wykonywane i powielone na tysiącach komputerów na całym świecie. Znamy maksymalny limit paliwa spalanego w jednym bloku, nowy blok pojawia się w Ethereum co 15 sekund. Średnio ta maszyna wirtualna będzie mogła wykonać instrukcje warte mniej więcej 2 miliony jednostek paliwa na sekundę. Dużo, mało? Najprostsza elementarna operacja matematyczna, czyli dodanie dwóch liczb, to koszt trzech jednostek paliwa. Maszyna wirtualna Ethereum będzie w stanie wykonać mniej więcej 600.000 dodawań na sekundę

Zwróćmy uwagę, że to nie do końca przekłada się na współczesne 64-bitowe procesory, bo w Ethereum liczby przechowywane są w zmiennych mających 256-bitów. Nie ma fizycznych procesorów o takiej charakterystyce. Z drugiej strony jednak, 600.000 operacji to jest niedużo, nawet biorąc poprawkę na rozmiar tych liczb.

Wydajność maszyny wirtualnej Ethereum (EVM) to jest mniej więcej 20 komputerów Commodore 64, czyli ośmiobitowców sprzed 40 lat. Jeśli spojrzymy na Raspberry Pi, czyli jednoukładowy komputerek kosztujący 300 zł, to taki Raspberry Pi sprzed 4 lat jest w stanie przeprowadzać obliczenia mniej więcej 5000 razy szybciej od EVM. Dlatego właśnie smart kontrakty nie mogą przeprowadzać żadnych skomplikowanych obliczeń - byłoby to zbyt wolne i zbyt kosztowne.

Teraz przejdziemy do tematu tokenów.

[00:15:30] Tokeny ERC-20

O tokenach zrobiło się głośno mniej więcej w roku 2017 roku, może trochę wcześniej. Aby opowiedzieć, czym są tokeny, zaczniemy od małej dygresji.

Wyobraźmy sobie, że gdzieś na ulicy stoi automat z autografami. Tak jak są automaty z napojami, tak tutaj będziemy mieli automat z autografami supergwiazdy. Gdy wrzucimy do tego automatu dwie stuzłotówki i wciśniemy guzik, to automat wypluje jedną stuzłotówkę, ale z odręcznym autografem gwiazdy. Łatwo policzyć, że skoro wrzuciliśmy 200 zł i dostajemy 100 zł z powrotem, to taki autograf jest wart (brakujące) 100 zł.

Co się teraz dzieje? Supergwiazda umiera. Okazuje się, że podpisała tylko 100 banknotów i umarła. Siłą rzeczy więcej takich autografów już nie będzie. No więc nagle się okazuje, że wszyscy fani na świecie rzucają się do tego automatu. Pierwszy wykupuje wszystkie autografy, wystawia na Ebay'u albo jakimś innym Allegro. Wszyscy kolekcjonerzy wiedząc, że już więcej nigdy żadnego autografu ta martwa supergwiazda nie podpisze, zaczynają się licytować. I okazuje się, że na przykład, że taki autograf po krótkiej chwili jest warty 100.000 zł. Autograf złożony na stuzłotówce! Nominalna wartość banknotu rozjeżdża się z kwotą, jaką ktoś chciałby za niego zapłacić.

Teraz sobie popatrzymy - fani nadal handlują pamiątkami po Elvisie Presleyu, który umarł bardzo dawno temu. Sporo pamiątek osiąga na kolejnych aukcjach coraz wyższe ceny. No to się okazuje, że taki autograf z automatu może być wart już nie 100.000, tylko milion albo i więcej. Co więcej - taki autograf sam staje się walutą. Kolekcjoner może nie sprzedać go za żadne pieniądze, ale będzie gotów wymienić się np. na gitarę, z którą supergwiazda występowała na jakimś koncercie.

I tutaj widzimy ciekawą rzecz. Wartość nominalna tego kawałka papieru przestaje mieć znaczenie. To, ile ten papier jest wart dla kolekcjonerów, całkowicie odrywa się od tego, że to jest banknot. Tutaj mamy po pierwsze o wiele większą wartość, a po drugie możliwość użycia jako waluty, której ten oryginalny nośnik w ogóle nie reprezentuje.

Wróćmy teraz do tematu Ethereum. Przypomnijmy dwa fakty. Pierwszy - kontrakty w sieci Ethereum mogą zapisywać dane w blockchainie. Drugi - kontrakt wie z jakiego adresu został aktywowany. Teraz piszemy i publikujemy smart kontrakt, który będzie robił następującą rzecz: będzie odnotowywał, ile dostał eterów z różnych adresów, ale nie ile sztuk, tylko ile dziesiątek sztuk. Czyli: jeśli wyślę ze swojego adresu na adres tego kontraktu 10 eterów to ten smart kontrakt popatrzy sobie i odnotuje: „dostałem 10 eterów z tego adresu, no to temu adresowi przypisuję jedyneczkę i zapiszę to sobie”. Ta jedyneczka to jakaś nowa jednostka i możemy się umówić, że będzie się ona nazywała TomekToken. Można dostać jednego TomekTokena za 10 eterów przekazanych smart kontraktowi.

I jeśli teraz zrobię drugą wpłatę, na przykład na 20 eterów, no to ten smart kontrakt odnotuje: „o, przyszło 20 eterów z tego adresu, z którego już kiedyś przyszło 10 eterów, wtedy odnotowałem jedynkę, teraz mam do dopisania dwie nowe sztuki TomekTokenów”. Więc ta jedynka zostaje zastąpiona trójką i taka informacja będzie zapisana ponownie w blockchainie.

Dzięki temu każdy będzie mógł zobaczyć, że smart kontrakt odpowiedzialny za TomekTokeny przypisał mojemu adresowi już 3 jednostki. I teraz gdy zechciałbym podarować komuś te moje trzy TomekTokeny, to eterów nie dostanę z powrotem, dostał je kontrakt i są już jego. Byłoby jednak fajnie, gdyby smart kontrakt miał jeszcze jedną funkcję, służącą do przelewania TomekTokenów czyli przekazywania ich komu innemu.

Oczywiście aktywowanie takiej funkcji wymagałoby już tylko opłacenia kosztów uruchomienia smart kontraktu, to są relatywnie małe kwoty. Ja - nadal z tego swojego adresu - mógłbym aktywować funkcję przelewania, a ta funkcja potrzebowałaby dwóch argumentów. Po pierwsze - adresu docelowego, po drugie - liczby TomekTokenów. Gdybym na przykład podał adres swojego kolegi, któremu chcę podarować dwa TomekTokeny, wówczas kontrakt powinien sprawdzić:

1. czy mam co najmniej tyle tokenów, ile chcę przelać
2. czy adres docelowy jest prawidłowym adresem w sieci Ethereum.

Jeśli wszystko gra, to kontrakt przeprowadza operację dopisania tokenów do nowego adresu i zredukowania liczby tokenów przynależnych do mojego adresu, zmiany zapisując w blockchainie.

Łatwo zauważyć, że to już prawie Bitcoin! Mamy sposób na kreowanie tokenów, bo wpłata każdych 10 eterów na konto smart kontraktu to wytworzenie jednego TomekTokena. Są przelewy między portfelami. To w zasadzie wszystko, co potrzebne.

Spojrzymy teraz na przykład troszeczkę uproszczony. Aby nie zajmować się kosztami generowania TomekTokenów wyrażonymi w eterach, spójrzmy na kod, który omija ten problem. To przykład z dokumentacji Ethereum, smart kontrakt o nazwie MyBitcoin. Tych tokenów nie trzeba generować po jednym, bo one wszystkie powstają w momencie zakładania smart kontraktu. Twórca definiuje, ile sztuk będzie istniało od początku, no i w przypadku takich tokenów będziemy potrzebować tylko funkcji do wykonywania przelewów.

Spostrzeżenie pierwsze - takich tokenów nigdy nie przybędzie, bo nie ma żadnego mechanizmu do ich generowania. Spostrzeżenie drugie - nigdy nie ubędzie tokenów, ale gdyby ktoś chciał sprawić, że żeby efektywnie było ich mniej, to może dokonać przelewu na losowy adres, o nieznanym kluczu prywatnym. Te tokeny zostają „spalone”, wychodzą z obiegu, już na zawsze będą leżeć w jakimś osamotnionym sejfie, do którego nikt nie ma dostępu.

Kontrakt MyBitcoin, o którym mówiłem, jest bardzo krótki. Mamy w nim jedną zmienną i dwie funkcje. Napis który zaczyna się od „mapping”, to zmienna pamiętająca, który adres ma ile środków czyli przypisanie liczników do adresów.

Pierwsza funkcja to jest konstruktor. W nim określamy ile tokenów dostanie założyciel tego smart kontraktu. Funkcja ta wykonana będzie jeden raz, przy tworzeniu smart kontraktu. To jest moment w którym następuje kreacja a wszystkie środki zostają przypisane do adresu twórcy tokena/kontraktu.

Druga funkcja, którą tu mamy, to funkcja transferu środków. Nadawcą jest zawsze ten, kto uruchamia funkcję, trzeba jeszcze przekazać w parametrach adres odbiorcy i kwotę tokenów. Następują sprawdzenia, zmiana liczników - i tyle.

Przy zakładaniu smart kontraktu, kontrakt ten dostaje automatycznie swój losowy, unikalny adres. Uwaga - jeśli ktoś sobie stworzy własną kopię danego smart kontraktu, z taką samą czy inną ilością tokenów, to będą to już zupełnie inne tokeny, bo inny będzie adres smart kontraktu, więc z punktu widzenia sieci to będzie coś zupełnie innego. Nazwy takie, jak TomekToken czy MyBitcoin, to tylko nazwy pomocne dla ludzi. Ethereum operuje na adresach.

Teraz przypomnijmy sobie przykład z automatem sprzedającym autografy na banknotach. Pamiętamy, że prawdziwa wartość takiego autografu nie ma związku z nominałem banknotu. Analogicznie - tu papierem jest Ethereum i blockchain, które tak naprawdę służą nam jako sposób na zapisanie, kto ma ile tokenów. Nie jest powiedziane, że wartość tych tokenów będzie w jakikolwiek sposób związana z wartością eteru. OK, w pierwszym przykładzie była, bo TomekTokeny były generowane po jednej sztuce za każde 10 eterów. Ale MyBitcoin nie ma żadnego związku z wartością Ethereum jako „papieru” - niezależnie od tego, czy tokenów wygenerujemy milion, miliard czy dowolną inną liczbę.

Tokeny zostały opisane w dokumencie ERC-20. Określa on uniwersalny standard tokenów po to, aby nie było potrzeby wymyślania wszystkiego za każdym razem od nowa. Gdyby ktoś miał TomekTokeny a kto inny miał MyBitcoiny generowane w odmienny sposób i z różnym zestawem funkcji - trudniej byłoby robić operacje łączące oba te tokeny.

Standard ERC-20 powstał relatywnie wcześnie, dzięki temu wiele tokenów ma wzajemnie zgodne schematy tworzenia i podobne kontrakty generujące te tokeny. Gdy ktoś się dowie, że smart kontrakt XYZ jest zgodny z ERC-20, to od razu zna jego najważniejsze cechy. Historia wywołań funkcji kontraktu XYZ może być też sprawdzana uniwersalnymi narzędziami operującymi na standardowych tokenach. Standard ERC-20 i maszyna wirtualna Ethereum sprawdziły się na tyle dobrze, że na ich bazie powstały także inne kryptowaluty i tokeny na innych blockchainach - przykładem może być Binance Smart Chain.

Pytania od publiczności:

Jak wygląda sprawa opłat za gas (czyli paliwo) kiedy tu kupujemy TomekTokeny za ethery? Czy kontrakt odejmie odpowiednią kwotę od przychodzącej transakcji?

Nie, kontrakt dostanie taką kwotę, jaka jest w transakcji. Natomiast oprócz kwoty transakcji trzeba przy wywołaniu funkcji wnieść osobną opłatę za paliwo. W przypadku kupowania TomekTokenów byłoby to 10 etherów plus jakiś malutki ułamek jedenastego na koszty wykonania. Jeśli będziemy chcieli robić przelewy TomekTokenów - wówczas wystarczy ta malutka kwota opłaty za paliwo do odpalenia funkcji przelewu.

Czy wiadomo, ile procesorów ma ta wirtualna maszyna Etherum i jak wygląda podział zadań? Czy różne smart kontrakty są obsługiwane jednocześnie?

Wykonanie jest w pełni sekwencyjne i jednowątkowe, nie ma podziału zadań. Zestaw instrukcji Ethereum VM przypomina specyficzny asembler; nie ma w nim żadnego wsparcia obliczeń równoległych. Jeśli mamy blok z transakcjami w sieci Ethereum, to on będzie legalny tylko wtedy, kiedy wszystkie transakcje z tego bloku też będą legalne, wykonywane od pierwszej do ostatniej.

To nie znaczy, że wszystkie wywołania smart kontraktów zawsze się skończą prawidłowo, że nigdy nie zabraknie paliwa na dokończenie obliczeń - taka sytuacja jest dopuszczalna i prawidłowa. Błąd walidacji skutkujący odrzuceniem bloku wywołałaby np. próba przelewania środków, których na adresie źródłowym nie ma, albo hash bloku który nie spełnia warunku trudności.

[00:37:35] ICO

Kolejny temat to ICO, czyli Initial Coin Offering. Ten skrót nie jest już na topie. Najwięcej szumu związanego z ICO mieliśmy 4-5 lat temu - podobnie, jak teraz jest z NFT.

O czym mowa? ICO wiąże się bezpośrednio z tokenami, o których mówiliśmy przed momentem, pierwotnie miał to być sposób na finansowanie startupów. Oczywiście szybko wynaturzyło się to w różne pokraczne formy, ale pierwotna idea była następująca: startup miał dostawać od inwestorów etery, w zamian tworząc i przekazując inwestorom tokeny. I dzięki temu, ci którzy wpłacili jakieś pieniądze, mieli osadzone w blockchainie potwierdzenie, że ich środki faktycznie zostały przekazane.

Potem miało się stać coś, co nie zostało do końca zdefiniowane, a na końcu miał pojawić się popyt na tokeny, aby inwestorzy mogli je odsprzedać z zyskiem. No i wtedy wiadomo - jest rynek, jest popyt, są wzrosty, wszyscy kupują i sprzedają, będzie coraz więcej pieniędzy i wszyscy będą zadowoleni. Niestety - nie do końca było wiadomo, co ma się wydarzyć tam w środku, w tym trzecim punkcie na obrazku.

Pomysły były różnorakie, że na przykład firma usługowa będzie przyjmować zapłatę w kryptowalutach, a te wyemitowane w pierwszej fazie finansowania tokeny będą jakoś uprzywilejowane, np. wyceniane wyżej. Były także koncepcje, że token reprezentuje akcje albo udziały. Problem - te pojęcia istnieją od bardzo dawna a emisja akcji lub obligacji jest ściśle uregulowana. Świat kryptowalut nie ma związku z giełdą papierów wartościowych albo zgromadzeniem akcjonariuszy albo zarządem czy radą nadzorczą. Ktoś mógł powiedzieć „kupujcie nasze tokeny, to będziecie tutaj naszymi akcjonariuszami" - ale za tym nie idą ani żadne zobowiązania, ani nie stoi za tym prawodawstwo jakiegokolwiek państwa.

Gdy więc nabywca tokena był przekonany, że będzie dostawał jakieś na przykład dywidendy od zysków startupu, to potem dowiadywał się ze zdziwieniem, że jednak nie pojawiła się żadna relacja prawna zobowiązująca do tego startup. To było dla sporej części ludzi zaskoczeniem.

Oczywiście smart kontrakty, które wydawały inwestorom tokeny w zamian za ethery, w znakomitej większości przypadków dawały założycielom kontraktu możliwość wyciągnięcia środków. Założyciele dawali tokeny, dostawali ethery i mogli z tymi etherami robić co zechcą. W wariancie A startup przez lata pozorował jakąś działalność. Albo i nie pozorował, tylko próbował coś rzeczywiście osiągnąć, co się z reguły nie udawało. Startup najpierw przejadał te ethery a potem znikał.

Był też wariant B, którym startup znikał od razu, twórcy też znikali i etery też znikały. Efekt końcowy taki sam, tylko osiągany znacznie szybciej. To się działo często, w 2017 tych ICO były dosłownie setki. Każdego dnia pompowano w nie miliony dolarów, bo każdy, kto miał nadwyżkę gotówki, a był wkręcony w kryptowaluty, nie chciał przegapić drugiego Bitcoina albo trzeciego Etherum, więc… były setki ICO ze świetlanymi obietnicami a wśród nich setki intencjonalnych przewałów.

Parę miesięcy później Google, Twitter i Facebook wprowadziły całkowity ban na reklamę ICO, spowodowany olbrzymią ilością oszustw. Rok czy dwa lata później zakaz został złagodzony - głównie dlatego, że gorączka złota się skończyła.

Mamy rok 2022, nie słyszy się o sukcesach firm, których początkowa faza działalności byłoby finansowana z ICO. Nie robiłem tu jakiegoś wielkiego researchu, ale na pewno taki niecodzienny fakt byłoby eksploatowany marketingowo, gdyby rzeczywiście jakaś poważna firma powstała i wyrosła w ten sposób.

W tamtym czasie pracowałem w firmie tworzącej oprogramowanie na zamówienie. W roku 2017 mieliśmy wielką ilość zapytań ofertowych, czy mamy ludzi, którzy jakkolwiek, na choćby podstawowym poziomie, znają się na kryptowalutach. Charakterystyczne, że tacy niedoszli zleceniodawcy często chcieli płacić swoimi tokenami, nie dolarami czy euro. Cóż, takich zleceń nie braliśmy.

Jeszcze jedna ciekawostka - założyciele ICO zawsze mieli wielką pulę tokenów gratis, przypisaną z automatu sobie. Gdyby się okazało, że jednak coś w biznesie zażre, byliby od razu bogaczami. Podobnie - kumplom czy innymi insiderom odpalali pewną działkę za ułamek wartości, by ci pompowali hype, żeby było głośno, żeby dużo się o tym mówiło i żeby zwabić więcej naiwnych, którzy oczywiście płacili pełną cenę.

Co więcej - gdy takie ICO startowało, założyciele mogli na giełdzie, na której token był notowany, po cichutku podbijać jego cenę, skupując część wyemitowanych wcześniej tokenów. No a skoro mieli swoją wielką darmową pulę, to mogli w pewnej chwili zrobić klasyczny pump and dump, czyli podbić cenę a potem nagle sprzedać swoje tokeny. No i koniec pieśni - założyciele oddalali się w losowym kierunku dzierżąc eter, a ludzie zostawali z tokenami bezpowrotnie tracącymi całą wartość.

[00:47:10] NFT

Co to jest NFT, czyli Non-Fungible Token? Pamiętacie, że w smart kontrakcie mieliśmy liczniki tokenów przynależnych do wskazanych adresów? Opowiadałem, że jeśli kupiłem jednego TomekTokena, potem dokupiłem dwa, to razem miałem trzy. Gdybym potem komuś jednego przelał, to nie jest w ogóle określone, „którego" TomekTokena przelewam. Jedyne, co znamy, to wartość liczbowa przypisana do określonego adresu. Gdy kupujemy wodę, to też nie kupujemy ponumerowanych molekuł H2O o znanej historii, tylko po prostu pewną objętość płynu.

Natomiast Non-Fungible Token, czyli NFT - to są ponumerowane tokeny, opisane przez dokument ERC-721. Ponumerowane, bo śledzimy losy każdego z nich osobno. Gdy ktoś kupił token nr 1 i potem komuś sprzedał a tamten też komuś odsprzedał, to cały czas jesteśmy w stanie prześledzić dokładne informacje o losach tokena nr 1. I to jest jedyna istotna różnica względem „zwykłych" tokenów ERC-20.

Umówmy się, że kupowanie cyferek czy symboli nie porwie tłumów, więc w roli NFT zaczęto osadzać obrazki. I te obrazki albo miały jakiś numer i można je było sobie zawczasu obejrzeć albo były w jakiś software'owy sposób generowane losowo podczas tworzenia. Dzięki temu na przykład, gdy ktoś tworzył (wykopywał) jakiegoś NFT, to nie wiedział zawczasu, co mu wyjdzie. Cechy obrazka zależały od przypadku - dodatkowo nie wszystkie pojawiały się z jednakowym prawdopodobieństwem.

Dodajmy, że relatywnie rzadko w dzisiejszych czasach mamy do czynienia z NFT, które od początku istnieją w blockchainie. Pojawiły się platformy takie jak OpenSea, które obsługują zarówno platformę aukcyjną, na której można sobie kupować albo sprzedawać NFT, jak i „generator" tworzący NFT w blockchainie dopiero po transakcji. W OpenSea „kupuje się" (w cudzysłowiu!) jakiś obrazek, ale nie jest on nawet wysyłany do tej platformy, tylko „kupuje się" URL-a określającego lokalizację obrazka. No i w związku z tym możliwe są takie dowcipy jak zrobił twórca Signala. Wystawił on na sprzedaż swoje dzieło, ale zależnie od tego, kto odpytywał jego serwer o obrazek, wyniki były odmienne. Jeśli zapytanie przychodziło z platformy OpenSea, no to był to obrazek z koncentrycznymi kreseczkami. Ten sam obrazek został wystawiony na platformie Rarible, tam wyglądał jak te takie niby kółeczka.

Natomiast gdy ktoś już kupił owego NFT i oglądał obrazek w swoim własnym portfelu, no to wtedy widział emoji z kupą. Nie była to więc sytuacja typu „widziały gały co brały", kupujący byli wprowadzani w błąd w sposób dość przewrotny.

Cofnijmy się do roku 2017, kiedy sporo osób miało etery i nie wiedziało co z nimi robić. Wtedy ludzie z firmy Larva Labs wymyślili, że wygenerują programatycznie Crypto Punki. Było to zestaw 10 tysięcy obrazków z ludzikami, generowanymi w sposób algorytmiczny. Crypto Punki to był pierwszy taki NFT, zanim jeszcze ta nazwa powstała. Ludzie mogli sobie zacząć tymi obrazkami handlować na giełdzie - każdy mógł wystawić posiadane ludziki, każdy mógł licytować te wystawione.

Crypto Punki były pierwszą rzeczą, którą można było kupić ze ether i chwalić się jej „posiadaniem” - nawet, jeśli mało kto byłby w stanie zweryfikować, czy faktycznie portfel chwalącego się ma przypisanego Crypto Punka o danym numerze.

Spójrzmy na statystyki czy też zapisy kryptopunkowych transakcji. To, że one tutaj idą w jakiejś dzikie miliony dolarów - to nie znaczy wiele! Całkiem niedawno mieliśmy sytuację, gdy ktoś kupił Crypto Punka za ponad 500 milionów dolarów. I co? Szybko okazało się, że to nie była rzeczywista transakcja, bo ktoś w obrębie tego samego bloku Ethereum pożyczał wielką ilość kryptowaluty, kupował za to Crypto Punka, a z adresu rzekomego sprzedawcy spłacał tę pożyczkę. No więc było widać, że to jest albo jakieś sztuczne pompowanie wartości, albo forma prania pieniędzy. Tak czy owak to na pewno nie była prawdziwa transakcja, w której ktoś za obrazeczek z łebkiem aliena zapłaciłby tak koszmarnie wielkie prawdziwe pieniądze.

Gdyby ktoś chciał kupić sobie NFT z Mona Lisą - ostrzeżenie. Sprzedawcą na pewno nie będzie rząd Francji, bo rząd Francji nie zamierza pozbywać się Mona Lisy. Jeśli kupisz NFT z takim obrazkiem, to ani sam obraz nie staje się twoją wartością, ani nie nabywasz żadnych praw majątkowych, ani nie nabywasz żadnych praw autorskich. Na platformach do handlu NFT nie ma żadnej gwarancji unikalności ani gwarancji, że wystawcą jest ktoś mający jakiekolwiek prawa do wystawionego dzieła. W przypadku NFT z Moną Lisą mamy wręcz pewność, że jest odwrotnie.

No i teraz pytanie - czy można kupić Monę Lisę jako NFT? Jeśli popatrzymy sobie na OpenSea, to widać że można. Mamy obraz Mona Lisa z kolekcji Cryptomasterpieces, ale jest też „The very first Mona Lisa NFT Untouched”, czyli bez retuszu. To nie są jedyne oferty. Jeśli ktoś chce, to może sobie kupić Monę Lisę przepuszczoną przez jakieś dziwaczny filtr graficzny i jeśli wydawałoby się, że to już jest najgłupsze, co może być, to się okazuje, że nie, bo na OpenSea można znaleźć także NFT ze screenshota z komórki, na której ktoś w Google Images wyszukuje Mona Lisę. Jeśli istnieje coś głupszego, to ja sobie tego nie potrafię wyobrazić.

Ostatnio popularne zrobiło się również to, że NFT sprzedają artyści. Doda na przykład sprzedawała swoje ciało jako NFT, udając, że wartość tegoż, no nie wiem - ciała czy NFT - będzie rosła wraz wraz z jej popularnością. Założenie cokolwiek ryzykowne. Pamiętajcie o koszcie energetycznym kryptowalut? Może by tak nie kupować od artystów NFT, tylko jakieś pamiątki albo płytę czy książkę, albo może pójść na koncert, czy wpłacić kasę na jakąś fundację?

Spędziłem 10 minut starając się znaleźć giełdę czy też tokeny, które miały reprezentować kawałki ciała Dody. Nie udało mi się. Znalazłem masę artykułów prasowych, że Doda to zrobi, że to robi, że to zrobiła - ale żeby ktoś podlinkował giełdę? Cisza. To zresztą oznacza, że pochwalenie się cyfrowym kawałkiem Dody może nie być takie całkiem łatwe.

Skąd popularność NFT? Jest całkiem prawdopodobne, że za promocją i pompowaniem tematu stoją ci, którzy kopią kryptowaluty, a chcieliby mieć dolary. Aby kupić NFT, trzeba przecież najpierw kupić eter albo jakieś tokeny - we wszystkich tych opcjach pierwotny posiadacz eteru ma na końcu dolary.

Obserwacja zupełnie bez związku z NFT - sprzedawcy koparek kryptowalut nie przyjmują kryptowalut jako zapłaty. Oni chcą prawdziwe pieniądze. Może to mieć związek z tym, że za kryptowaluty da się kupić niewiele rzeczy legalnych i użytecznych.

[01:01:24] Proof of Stake

Co to jest Proof of Stake (PoS), czyli dowód uczestnictwa? W pierwszej części gawędy opowiedziałem o mechanizmie Proof of Work (PoW), w którym górnicy rywalizują o możliwość dołączenia do blockchaina kolejnego bloku. Robią to poprzez ciągłe zestawianie oczekujących transakcji w nowy blok - by losowo natrafić na taką kombinację, której cyfrowy skrót (hash) spełni warunek trudności.

Miliony urządzeń na całym świecie dokonują milionów lub miliardów prób na sekundę, aż w końcu komuś się uda - mniej więcej raz na 10 minut powstaje nowy blok Bitcoina. Zużywana jest na to straszliwa ilość energii. Wiemy, mniej więcej, jaka jest łączna moc obliczeniowa tych urządzeń, które to robią i ile LINK dżuli trzeba włożyć w policzenie jednego hasza.

Z obliczeń wynika, że współcześnie jest to trochę ponad 200 terawatów energii elektrycznej rocznie. Dla porównania - elektrownia Bełchatów, największa w Polsce, produkuje rocznie 28 terawatów. Potrzebujemy wielu takich elektrowni, by rzeczywiście napędzić czy też zasilić koparki energią idącą w całości na zmarnowanie.

Wpływ kryptowalut na ekologię jest bezdyskusyjny. Kilka miesięcy temu jacyś ludzie w Stanach Zjednoczonych przywrócili do życia zamkniętą elektrownię węglową, ale nie podłączyli jej do sieci dystrybucyjnej. Zamiast tego, całą wyprodukowaną energię włożyli w kopanie kryptowalut. Jest oczywiste, że przyroda doznaje uszczerbku i to na pewno nie robi dobrej prasy kryptowalutom.

Od dawna trwają więc prace nad koncepcją alternatywną względem Proof of Work, która nie będzie przepalać tak strasznych ilości energii elektrycznej - jest to Proof of Stake. Koncepcja polega na tym, że uczestnicy rynku, którzy chcą zarabiać na tworzeniu bloków, muszą zamrozić część swoich środków. Nie takich zresztą małych. W sieci Ethereum w przymiarkach do przejścia na Proof of Stake wymaga się, by zamrozić 32 etery - w dzisiejszych cenach jest to około 100.000 USD. Lub wielokrotność, jeśli ktoś chce mieć więcej stawek.

Zamrożone środki sprawiają, że ich właściciel dostaje status walidatora, który będzie - potencjalnie - brał udział w tworzeniu bloku. Ma to działać w taki sposób, że co 15 sekund w sposób losowy sieć ma wybrać walidatora, który utworzy kolejny blok. A gdy ten walidator to zrobi, czyli złoży blok z zestawu transakcji wybranych z puli, to wtedy inni losowo wyznaczeni walidatorzy sprawdzą poprawność bloku. Czyli zweryfikują na przykład, czy nie następuje próba przelewu na większą kwotę niż zawiera konto źródłowe. Kto kantuje, ten traci stawkę - część albo całość tych 32 zablokowanych eterów. Karane jest tak oszustwo przy tworzeniu, jak i przy walidowaniu bloku. Ten, kto tworzy prawidłowy blok, dostaje zwyczajową nagrodę za utworzenie.

Kiedy Proof of Stake wejdzie w życie? Otwórzmy witrynę Ethereum i sprawdźmy. Na obrazku widzimy zaktualizowany 3 tygodnie artykuł głoszący, że Ethereum od zawsze miał plan przejścia z PoW na PoS. Gdy składałem te slajdy, to się trochę roześmiałem, bo pierwszy raz robiłem wykład o kryptowalutach w roku 2017 i już wtedy Proof of Stake miał wejść w życie za kilka miesięcy. Co poszło źle? Przez 5 lat no to naprawdę da się wyklepać potrzebny kod więc musiało być tu coś innego. Jaki jest prawdziwy powód takiego opóźnienia?

Zwróćmy uwagę, że Proof of Work dzieje się w „prawdziwym świecie”. Mamy prawdziwą elektryczność i prawdziwe urządzenia, które muszą te hashe policzyć. I to jest niezależne od tego, co dzieje się w świecie transakcji, bloków i tego wszystkiego. Natomiast Proof of Stake to jest coś co działa „w środku kryptowaluty”. O losach nowego bloku, czyli o losach nowych transakcji, będą decydować osoby wybrane spośród tych, którzy już dysponują znacznymi środkami.

Informacja, który w całości wynika z blockchaina i siedzi w blockchainie, ma decydować o przyszłości blockchaina. To coś jakościowo innego niż kopanie bloków urządzeniami istniejącymi „naprawdę”. Rejestr transakcji mówi nam, kto ma środki, potem zgodnie z koncepcjami PoS dzieje się jakieś mambo dżambo, ale na końcu to ludzie mający środki w blockchainie decydują o kolejnych transakcjach. A ich motywacje niekoniecznie muszą być tożsame z interesami pozostałych uczestników sieci Ethereum.

Zwróćmy uwagę na interesujący fakt. W Proof of Stake bogaci stają się jeszcze bogatsi. Jeśli ktoś ma 1/4 wszystkich eterów, i wszystkie zamrozi jako stawki w PoS, to on na pewno dostanie 1/4 wszystkich nowych eterów, nigdy nie przestanie być procentowo mniej bogaty niż jest. Byłoby jego decyzją, czy kiedykolwiek taki stan rzeczy się zmieni.

Zupełnie inaczej działa to w przypadku Bitcoina. Gdyby Warren Buffet albo Bill Gates zapragnęli zostać bitcoinowymi potentatami, to za swoje miliardy dolarów mogliby wykupić wszystkie dostępne urządzenia. Przepłacając - mogliby zdobyć znaczny udział łącznej mocy obliczeniowej w sieci Bitcoin. Nie zależałoby to od woli ani zgody aktualnych posiadaczy bitcoinów. W Proof of Work procentowy udział w wykopanych monetach nie jest dany raz na zawsze.

A co w przypadku hard forka? Mieliśmy ich wiele, jak Ethereum Classic czy Bitcoin Gold. W klasycznym Proof of Work to górnicy decydowali, która gałąź forka będzie tą „główną” - poprzez podłączenie swojej mocy obliczeniowej do konkretnego wariantu. Warianty poboczne były marginalizowane a ich wartość w dolarach jest rzędy wielkości mniejsza.

Gdyby fork miał miejsce w modelu Proof of Stake, bogaci pozostają bogaczami w obu wariantach i nadal będą w takim samym procencie kontrolować oba warianty forka. Co więcej - nie będzie żadnego „zewnętrznego” sposobu na określenie wariantu lepszego, dominującego. Gdyby nagle pojawiło się sto hard forków i setka konkurencyjnych sieci Ethereum z PoS, to… skąd chętni do zakupu kryptowaluty będą wiedzieli, co wybrać? Gdyby chcieli kupić Crypto Punka, to w której sieci? A może próbować kolejno w każdej? Ryzyko wzrośnie, oczekiwany zwrot ze spekulacji spadnie. Łączna wartość podzielonych kryptowalutek byłaby mniejsza, niż pierwowzoru.

Czy istnieją jakieś poważne alternatywy dla Proof of Work i Proof of Space? Jedynie Proof of Work jest powszechnie stosowanym mechanizmem konsensusu. Proof of Stake to na razie koncepcja, która nie została wypróbowana na poważną skalę w praktyce.

Pytanie od publiczności:

Jak technicznie wygląda zamrożenie 32 etherów w Proof of Stake?

Robimy to poprzez przelanie ich na konto specjalnego smart kontraktu. 32 ethery dają jeden udział w losowaniu prawa do wykopania bloku. Jeśli zechcesz się wycofać, to dostaniesz z powrotem te etery (przynajmniej docelowo będzie się dało - nie sprawdzałem, jak jest teraz). Wycofanie środków sprawia oczywiście, że przestaniesz brać udział w losowaniu.

[01:12:17] Proof of Space

Rok temu pojawił się jeszcze pomysł na konsensus - mechanizm Proof of Space. To już nie marnotrawienie energii elektrycznej na liczenie hashy, tylko marnowanie pojemności dyskowej jako dowód, że „zamroziliśmy” stawkę poprzez kupno dysków twardych.

Na obrazku jest bardzo znany youtuber Linus Sebastian. Ma on na stole dyski twarde o łącznej pojemności około 3 petabajtów. Tak, on byłby w stanie wejść w kryptowalutę Chia, która - jak to bywa w takich sytuacjach - na kilka tygodni rozregulowała handel dyskami twardymi. Zaczęło ich brakować na całym świecie. Jakbyśmy mieli mało problemów!

Kryptowaluta Chia opiera mechanizm konsensusu nie na mocy obliczeniowej, lecz na powiązaniu szansy na wykopanie bloku z rozmiarem powierzchni dyskowej przeznaczonej na zmarnowanie. Jest oczywiście matematyka stojąca za tym, żeby nie dało się oszukiwać i żeby faktycznie trzeba było zablokować ileś tam setek gigabajtów, by uczestniczyć w tej sieci.

Szczęśliwie dla nas wszystkich, wartość tej kryptowaluty szybko poleciała w dół, więc nie stała się ona popularna, więc nie mamy problemu z dostępnością dysków twardych. Bo wiecie, problem z wykupywaniem kart graficznych jest bardzo duży, zawdzięczamy to górnikom kopiącym Ethereum. Cóż, przynajmniej dyski twarde na razie się uchowały.

[01:17:23] Inne częste pytania

Czy kryptowaluty dają anonimowość? Niektóre większą, inne mniejszą. W Bitcoinie i Ethereum łatwiej śledzić przepływy, łączyć źródła i cele, przypisywać transakcje do osób lub organizacji. Inne kryptowaluty, na przykład Monero, były tworzone z intencją utrudnienia takiego śledzenia. Jest ono nadal do pewnego stopnia możliwe, jednak staje się bardziej niepewne - prawdopodobieństwo prawidłowego określenia stron transakcji jest np. rzędu 60%.

Trzeba też pamiętać, że gdy raz uda się połączyć portfel z człowiekiem, to w jednej sekundzie dowiemy się wielu rzeczy z przeszłości - skąd brał środki, na co je przeznaczał, z kim się wymieniał i tak dalej. Pod tym względem anonimowość będzie zależała od tego, kto zacznie drążyć. Jeśli FBI albo CIA - ich możliwości rozpytania operatorów giełd będą dużo większe niż przypadkowego człowieka z Europy.

Trzeba pamiętać o tym, że na końcu przestępcy chcą dostać dolary. W związku z tym najłatwiej i najprościej będzie pilnować początku i końca łańcucha. Władze i regulatorzy mogą zmuszać operatorów giełd do tego, żeby stosowali przepisy Anti Money Laundering i Know Your Customer - dotyczące zapobiegania praniu brudnych pieniędzy i obowiązku weryfikacji tożsamości osoby przystępującej do transakcji. Mogą też określić limity wartości transakcji. Niewykluczone, że władze państwowe potrafiłyby zmusić operatorów giełd do usunięcia notowań i zaprzestania handlu kryptowalutami w rodzaju Monero - a wtedy ci, którzy tam mają jakieś środki pochodzące z wyłudzeń czy kradzieży, będą musieli przepuszczać je przez giełdy w dzikich krajach, ryzykując ich utratę.

Miksery (tumblery) to mechanizmy „mieszające” kryptowaluty, utrudniające śledzenie ich przepływów. Chętni wpłacają środki na jeden adres zaś automat robi serię przekierowań, rozsyła środki w wielu kawałkach na różne świeże portfele, łącząc i dzieląc wartości, by na końcu przekazać je wpłacającym na inne adresy, w różnych odstępach czasu, niewielkimi kwotami.

To będzie do pewnego stopnia działać, dopóki nie zechcemy wyprać jakiejś wielkiej ilości kryptowalut. Gdybyśmy mieli 1000 osób wpłacających po 1 bitcoinie, a jedna wpłaci milion bitcoinów, to miksowanie niczego nie da. Cały czas będzie wiadomo, że 99,99% środków należy do jednej osoby, która na dobrą sprawę niczego nie wypierze. Polecam LINK artykuł w serwisie Ars Technica sprzed tygodnia - w ręce policji trafiła para kontrolująca portfel, na którym leżało 120 tysięcy Bitcoinów ukradzionych z giełdy Bitfinex w 2016 roku. Wtedy było to kilkadziesiąt milionów dolarów, teraz jest równoważnikiem ponad 3.6 miliardów dolarów. Gdy takie pieniądze są w grze, pościg się nigdy nie skończy.

Jeśli chodzi o pranie brudnych pieniędzy, to pamiętacie być może taką scenę z Breaking Bad, amerykańskiego serialu, w którym główny bohater zajmował się narkobiznesem. Jego żona miała prać pieniądze, które zarabiał, poprzez ich legalizację w myjni samochodowej. Szybko się okazało, że tych pieniędzy jest za dużo, by dało się w myjni wygenerować taki sztuczny obrót. Na obrazku scena, gdy bohater dowiaduje się, ile pieniędzy jest niewypranych.

Czemu o tym piszę? Ano, po włamaniu do Poly Network - ukradziono kilkadziesiąt milionów dolarów w eterze - operatorom tego serwisu udało się przekonać kopalnie (50 procent mocy kopania Ethereum to raptem 3 albo 4 kopalnie), aby adresy, na które przelano wykradzione środki, trafiły na czarną listę. Kopalnie w ogóle nie dopuszczały do puli zleceń transakcji z tych adresów. Okazało się że złodzieje nie byli w stanie nic zrobić z ukradzionymi środkami, bo w sieci nikt nie przyjmował ani nie przetwarzał transakcji z przelewami z tych adresów.

Gdy mowa o puli transakcji oczekujących na dołączenie do bloku, to miała miejsce inna ciekawa sytuacja. Błąd w pewnym smart kontrakcie dostrzeżono, zanim ktoś go wykorzystał. Na szczęście istniała możliwość poprawienia usterki poprzez wywołanie funkcji kontraktu. Jeśli jednak transakcja z takim wywołaniem trafiłaby do publicznie dostępnej puli, to złodziej mógłby zapoznać się z nią, zrozumieć jej znaczenie i próbować wyprzedzić poprawkę własną transakcją. Potrzebna była współpraca kopalni, która taką transakcję z bugfixem wstawiła do bloku bez uprzedniego ujawniania w publicznej puli. Dwa powyższe przykłady pokazują, że w krypto-świecie są równi i równiejsi.

Jak działa wymiana między różnymi kryptowalutami? No tutaj nie ma niestety żadnej magii. Gdy mamy do czynienia z różnymi blockchainami, czyli np. Binance kontra Ethereum - musimy mieć jakiegoś pośrednika, który przyjmie środki jednego typu i wyda lub wygeneruje środki drugiego typu. Czy da się zhackować takiego pośrednika? Na obrazku artykuł z lutego opisujący włamanie do Wormhole, wykradziono środki warte 323 miliony dolarów. Złodziejom udało się przekonać oprogramowanie po jednej stronie „łącznika”, że środki na wymianę wpłynęły, co w rzeczywistości nie miało miejsca. Ich równowartość dało się jednak wypłacić po drugiej stronie. Czynność była powtarzana, dopóki Wormhole nie stracił płynności.

Co to jest wrapped BTC czyli „owinięty” BTC? Jest to reprezentacja środków z jednego blockchaina w innym blockchainie. Jak w poprzednim przypadku, potrzebujemy pośrednika który przyjmuje środki po jednej stronie, a wyda po drugiej. Przykład: „owinięte” bitcoiny rejestrowane jako tokeny w sieci Ethereum. Będzie to token jak każdy inny, ale bitcoiny pozostaną tak naprawdę w dyspozycji pośrednika. Musimy mu zaufać, że w każdej chwili będziemy mogli wycofać token i dostać z powrotem bitcoina. Jeśli pośrednik zostanie okradziony albo sam gdzieś zniknie, to pozostaniemy z bezwartościowym tokenem który nie ma już pokrycia w niczym.

Co to jest „stablecoin”? Jest to kryptowaluta albo token powiązane z prawdziwymi pieniędzmi, czyli na przykład jeden do jednego z dolarem. Także i tym razem musimy zaufać emitentowi, że nie wytworzy więcej monet, niż przyjął depozytów. Stablecoiny są popularne, bo zwiększają płynność giełd kryptowalutowych. Jeśli ktoś chciałby sprzedać swoje etery albo bitcoiny, by dostać dolary, no to giełda musiałaby mu te dolary przelać i wtedy miałaby ich mniej. Jeśli ktoś zechce przyjąć tokeny powiązane z dolarem, wtedy może np. uniknąć opodatkowania zysków ze sprzedaży, bo de facto wymienia jedną kryptowalutę na drugą.

Co to jest „shitcoin”? Jest to kryptowaluta o niskiej płynności / popularności / wartości. Innymi słowy ta, o której jeszcze nie napisał Elon Musk. Bo jak Elon napisał o bezdyskusyjnym wówczas shitcoinie Dogecoin, to kurs Doge’a gwałtownie wzrósł.

Co to jest „DAO”? Zdecentralizowana Autonomiczna Organizacja, pojęcie bardzo niejasne. Czy to miałby być smart kontrakt? No to po co inna nazwa na to samo? Chyba, że to jakaś forma spółki czy spółdzielni, ale wracamy do wiedzy poprzedniego odcinka - rzeczy, które robimy w blockchainie, nie mają związku z prawdziwymi operacjami na rynkach finansowych. Ani niczym podobnym.

Kolejne pytanie co to jest DeFi, czyli Decentralized Finance? Słownikowa definicja: „systemy, aplikacje oparte o blockchain oferujące usługi finansowe nie regulowane w przepisach prawa i nie objęte właściwym nadzorem odpowiednich organów”. To oznacza, że sporo DeFi skupi się na unikaniu opodatkowania albo praniu brudnych pieniędzy.

Jak się czyta o DeFi, to można trafić na następujące wynurzenia: „opierająca się na zyskach pośredników klasyczna bankowość jest zazwyczaj niedostępna w regionach charakteryzujących się niskimi dochodami. Dzięki temu, że koszty DeFi są stosunkowo niewielkie, opłacalne staje się udostępnianie zdecentralizowanych aplikacji finansowych osobom o mniejszych zarobkach”. No kurde! Trzeba być bogatym białym człowiekiem z Doliny Krzemowej, żeby pisać takie bzdury. Jeśli gdzieś rzeczywiście nie ma klasycznej bankowości, to albo jesteśmy w górach Nepalu i nie docierają tam internety ani kable telefoniczne, albo mamy do czynienia z ludźmi, którzy nie mają absolutnie żadnej wiarygodności finansowej.

Autorzy piszący takie głodne kawałki nigdy nie słyszeli o spółdzielniach, o kasach chorych, o kasach zapomogowo-pożyczkowych. Takie rzeczy istnieją od 200 lat. Nie potrzeba do tego żadnych kryptowalut, tym bardziej, że kompetencje techniczne wymagane, by skorzystać ze zdecentralizowanych finansów jako tokenów w smart kontrakcie na blockchainie - są dość wysokie. I gdy mamy jakiegoś rolnika z Nepalu, to on, choć ma komórkę, raczej nie poradzi sobie z obsługą kryptowalut na tejże komórce. A już na pewno nie będzie gotów na ryzyka z nimi związane.

Czy zdecentralizowane finanse są bezpieczne? To bardzo skomplikowane smart kontrakty, więc są narażone jak dowolne inne skomplikowane smart kontrakty. Każdy może sobie obejrzeć kod każdego smart kontraktu, który siedzi w blockchainie. Na obrazku mamy opis tego, jak można było wysiorbać środki z takiego DeFi o nazwie Cream. Włamanie miało miejsce, kroki rozpisane na obrazku to analiza post factum. Badacz opisał sekwencję 23 działań, dzięki którym Cream został opróżniony.

Jeśli ktoś chciałby być na bieżąco, bardzo polecam stronę Web Three Is Going Great. Prawie każdego dnia pojawiają się tam opisy kolejnych włamań, kradzieży i nadużyć. Gdy przewiniemy pozycje na linii czasu, to licznik pokazuje, ile łącznie warte były opisane kradzieże, drenaże itp. Gdy sprawdziłem to dzisiaj - od pierwszego stycznia było to 559 milionów dolarów.

Kinomaniacy, pamiętający znakomitą komedię „Żywot Briana", przypomną sobie scenę, w której członkowie Judejskiego Frontu Wyzwolenia uczestniczą w zebraniu rewolucjonistów a ich lider pyta retorycznie „co takiego dali nam ci Rzymianie!". Monolog trochę się wykoleja, bo nagle okazuje się, że mieszkańcy okupowanych terenów doceniają opiekę zdrowotną, porządne drogi, akwedukty, wino i tak dalej.

Jeśli chodzi o kryptowaluty, nie sposób dostrzec analogicznych korzyści. Gdy się zastanowić, po stronie plusów nie ma prawie niczego. Przykłady minusów? Karty graficzne wykupywane na pniu przez górników. Zdjęcie sprzed paru dni z x-kom - dostępne modele są prawie dwa razy droższe od sugerowanej ceny producenta, zazwyczaj zawyżonej. Usługi online bez darmowych wersji „na wypróbowanie", bo amatorzy darmowej mocy obliczeniowej wszędzie, gdzie to możliwe, odpalali koparki kryptowalut.

Pytania od czytelników

Czy kryptowalutę Monero można uznać za stablecoin lub shitcoin?

Stablecoin to nie jest, bo tam nie ma przełożenia na jakąkolwiek klasyczną walutę FIAT. Shitcoin - do dyskusji. Niby nazwa znana, ale w rankingu kapitalizacji Monero jest dopiero w trzeciej dziesiątce kryptowalut.

Czym Monero wyróżnia się na tle innych kryptowalut?

Mechanizmami działania zmierzającymi do tego, by trudno było śledzić przekazy i wartości tych przekazów.

Czy miksery są skuteczne?

Do pewnego stopnia. Zależy od determinacji śledzącego oraz ilości środków - im więcej, tym trudniej je skutecznie przemiksować.

Czy można poznać, że osoba stosowała mikser?

Historia blockchaina zawiera adresy, nie osoby. Można sprawdzić, czy środki obecne na jakimś adresie przeszły przez jakiś znany mikser, ale nie jest powiedziane, kto był ich właścicielem. Są firmy, które zajmują się tylko tym, świadczą swego rodzaju usługi detektywistyczne - ale jedynie niewielką część adresów da się łatwo powiązać z osobami.

Czy miksowanie krypto jest równe praniu pieniędzy?

Nie bezpośrednio, niemniej miksowanie to usługa płatna. Tego typu wydatek ponosi się z reguły właśnie po to, by utrudnić śledzenie źródeł pochodzenia środków.

Czy można powiedzieć, że Monero ma w sobie wbudowany mikser / pralnię?

W pewnym sensie tak i to tworzy negatywny PR tej kryptowaluty. Mało kto chce używać czegoś, o czym wiadomo, że jest preferowaną przez przestępców metodą opłacania haraczy.

W jaki sposób zapewnia się stabilność stablecoina. Z tego, co powiedziałeś, wynika, że jego wartość opiera się na zaufaniu.

Tak właśnie jest. Jeśli jakiś emitent stablecoina regularnie co wtorek emituje milion tokenów reprezentujących dolary to można mieć uzasadnione wątpliwości, czy on rzeczywiście dostaje w depozyt równo milion dolarów co wtorek. Mieliśmy już w historii stablecoiny bez pokrycia. Gdy wieść się roznosiła, wartość takiej kryptowaluty odklejała się od dolara i leciała w dół - wszyscy chcieli odzyskać choć ułamek wartości.

Czemu zdobycie kryptowalut wymaga Know Your Customer i jest trudniejsze niż założenie konta bankowego.

No właśnie dlatego, że regulatorzy starają się ograniczyć możliwość prania brudnych pieniędzy. Chcą mieć możliwość określenia kto i kiedy włożył prawdziwe pieniądze w kryptowaluty albo je wyciągnął. Jest to też utrudnieniem w unikaniu opodatkowania.

Czy można powiedzieć, że bitcoin bitcoinowi nierówny? Jeśli jakiś BTC jest częścią przestępstwa, to wszystko jest blockchainie i jest brudny?

Niestety tak. Ślad zostaje i nawet jeśli kupujemy w dobrej wierze, może się zdarzyć, że środki będą pochodziły z adresu o podejrzanej przeszłości. Giełdy kryptowalut mogą nie przyjąć takich środków i nie pozwolą nimi handlować. Sporo jest zresztą historii, w których ktoś ma legalne bitcoiny sprzed wielu lat, wówczas kupił je anonimowo, dziś chce sprzedać i pojawiają się trudności. Wymienialność bitcoina względem klasycznych walut nie jest gwarantowana, lepiej zgłębić temat, zanim się utopi pieniądze.

Czy krypto w aktualnym wydaniu to twoim zdaniem zło?

Miałem spore nadzieje na pojawienie się interesujących, użytecznych zastosowań blockchaina i kryptowalut. Nie widać jednak, by cokolwiek szło w dobrą stronę. Gdy patrzymy na ilość oszustw czy wyłudzeń, zwłaszcza ostatnio w NFT, to im dalej w las tym gorzej.

[01:38:10] Zakończenie

Zamiast zakończenia, dwa cytaty. Pierwszy jest widoczny na obrazku - „kryptowaluty dziedziczą wszystko co najgorsze z systemu kapitalistycznego, czyli korupcję, oszustwa, nierówność. Dodatkowo dodają do tego techniczne sposoby na unikanie interwencji organów czy regulatorów”. Napisał to twórca Dogecoina, który od dawna wycofał się z branży kryptowalut, zniesmaczony i zasmucony tym w jaką stronę to wszystko poszło.

Drugi cytat to odpowiedź na argument, że kryptowaluty są wciąż nowością, więc poczekajmy i zobaczmy, co z nich wyniknie. Riposta - Bitcoin ma 14 lat! Gdy w takim wieku była sieć WWW, mieliśmy już Google, Wordpressa, Firefoxa, było bardzo dużo fajnych rzeczy, po których od razu było widać, że są dobre. Owe 14 lat Bitcoina to już nie jest wczesne stadium. Gdyby miało powstać na tej bazie coś rzeczywiście fajnego i dobrego, już byśmy to widzieli.

I to tyle.

Jeśli chodzi o standardowe dla youtuberów wezwania do tego, żeby kliknąć kciuka, dzwoneczek i tak dalej - no możecie, jeśli chcecie. Ten dzwoneczek to wam zadzwoni raz na kwartał, za to będzie mi bardzo miło gdy wejdziecie na stronę LINK informatykzakladowy.pl/newsletter i zasubskrybujecie newsletter. Dzięki temu będę mógł informować was nie tylko o przyszłych gawędach, ale też o różnych innych ciekawych rzeczach, które zdarza mi się robić. Nie spamuję, nikomu nie przekazuję tych adresów. Subskrybentów jest już prawie 3000, ludzie się zapisują, bardzo rzadko się wypisują. Zapraszam wszystkich. Nie będę spamował. Będą ciekawe informacje o kolejnych artykułach i nie tylko.

I to wszystko! Bardzo dziękuję za udział w gawędzie. Słyszymy się następnym razem! Nie deklaruję kiedy, bo już mam długą historię wielomiesięcznych obsuw z takimi obietnicami. Następnym razem będziemy mówić o jakimś zupełnie innym temacie, a dzisiaj się żegnam. Dzięki i do usłyszenia. Hej!