Bitcoin i ścieżka do stania się suwerenną jednostką

Przed powstaniem sieci bitcoin ścieżka do stania się suwerenną jednostką była bardzo trudna i stroma. Trzeba było uczyć się kryptografii i wewnętrznych schematów działania systemów komputerowych. Trzeba było zostać praktycznie krypto hakerem (cokolwiek to znaczy, gdyż nie ma to dokładnego odpowiednika w języku polskim).

Przez ogrom pracy jaką trzeba było włożyć w poznanie tak specjalistycznej wiedzy, nie pozostawało zbyt wiele czasu na kontakty społeczne. Ludzie tym się zajmujący musieli posiadać silną motywację do zgłębiania sposobów uniezależniania się od zaufanych trzecich stron. Najczęstszą motywacją była po prostu paranoja, brak zaufania do jakichkolwiek instytucji społecznych i głęboko zakorzeniona w osobowości nieufność. Cechą przeciętną takich osób była więc aspołeczność oraz brak zrozumienia, że ludzkość odnosi największe sukcesy właśnie współpracując.

Z powodu upowszechniania się łatwiejszej w obsłudze technologii pojawiła się najpierw możliwość dużo lepszego zabezpieczenia własnych systemów komputerowych przed ingerencją z zewnątrz m.in. za pośrednictwem antywirusów oraz zapór ogniowych (firewalli). Potem standardem stało się szyfrowanie komputerowych dysków (tak, że już nie jest tak łatwo przeglądać czyjeś dane).

Część przeciętnych ludzi już dziś woli podpisy elektroniczne dokumentów od podpisów ręcznych, ponieważ taki podpis zawiera w sobie sumę kontrolną podpisywanego kontraktu czy umowy. Ma więc taki podpis przewagę nad podpisem ręcznym, bo nie można zmienić nawet przecinka w już podpisanej umowie bez zniszczenia samego podpisu. Natomiast przy ręcznie podpisywanych umowach na papierze jest możliwość zmiany treści już podpisanego dokumentu i próby wymuszenia na podpisującym dodatkowych warunków na które się nie zgodził.

Ludzie używający tych technologii nie koniecznie muszą znać się na szczegółach tego jak działają. Aby wykorzystać wynikające z nich funkcjonalności, wystarczy tylko wiedzieć jak je uruchomić.

Podobnie łatwa w obsłudze staje się wymiana owoców własnej pracy pomiędzy użytkownikami sieci. Powstają coraz prostsze i intuicyjne systemy mające za zadanie to umożliwić. Bez posiadania wiedzy technicznej, z wykorzystaniem sieci bitcoin można wykonywać transfery pieniężne bez konieczności ufania bankom i innym instytucjom finansowym.

Aby takie działania były bezpieczne i nie narażone na kradzieże ze strony crackerów potrzebna jest silna kryptografia i paradoksalnie współpraca wielu podmiotów dążących do uczynienia takiej sieci odporną na zakłócenia. Podmioty te współpracują bez centralnego systemu koordynacji, bo każdemu z nich (jeśli dba o swoje przyszłe dochody) zależy na uczynieniu sieci bitcoin bardziej bezpieczną. To od poziomu bezpieczeństwa zależy napływ nowych użytkowników i zwiększenie zaangażowania finansowego tych, którzy już tej sieci używają.

Podmiotami o których mówię są górnicy bitcoina, czyli tzw. minerzy (ang. miners). Ludzie, a głównie przedsiębiorstwa, których działalność zabezpiecza siec bitcoin przed atakami z zewnątrz. W zamian za to górnicy otrzymują świeżo dodrukowanego bitcoina.

Z powodu tego dodruku cyfrowa waluta bitcoin (gdyby nie napływ nowych użytkowników) podlegała by inflacji. Jednak poziom tej inflacji jest obecnie w granicach 1,7% (jeden przecinek siedem) i jest niższy niż inflacja złota (około 2%). Z wykorzystaniem górnictwa przemysłowego na całym świecie wydobywa się bardzo dużo nowego złota w porównaniu z tempem wydobywania nowego złota w poprzednich wiekach. Co ciekawe około 7 kwietnia przyszłego 2024 roku inflacja na bitcoinie spowodowana tworzeniem nowego bitcoina z powietrza zmniejszy się o połowę. Stanie się on więc dwa razy lepszy w

utrzymywaniu wartości niż złoto (co wcale nie oznacza, że będzie rósł dwa razy szybciej jak złoto, gdyż złoto może w tym czasie przyciągnąć więcej nowych kupujących niż bitcoin).

Górnikami „wydobywającymi" nowy bitcoin mogą zostać dowolni użytkownicy sieci bitcoin, a nawet dowolni użytkownicy sieci Internet. Jednak ze względu na dużą konkurencję zwykle przeciętnym użytkownikom Internetu zostanie górnikiem się po prostu nie opłaca (zwłaszcza po ostatnich podwyżkach cen energii). Droga ku opłacalnemu górnictwu wiedzie poprzez dostęp do taniej energii lub poprzez dostęp do najwydajniejszych koparek najnowszej generacji (ang. *ASICs*). Są to specjalne procesory przystosowane tylko do jednego rodzaju aktywności, którą jest zabezpieczanie sieci bitcoina.

Zanim zastosowano do tego dedykowane procesory ASIC kopanie bitcoin przebyło długą drogę. Najpierw kopano z wykorzystaniem najzwyczajniejszych domowych komputerów. Potem za pomocą profesjonalnych serwerów. Potem budowano specjalne serwery z wykorzystaniem kart graficznych. Obecnie kart graficznych się do kopania bitcoina już praktycznie nie używa (przez to, że są one dużo mniej wydajne). Jednak ceny kart graficznych są nadal wysokie przez masowe wykorzystywanie ich do trenowania sieci neuronowych w tym tych najsłynniejszych: Golemów (czyli *Generative Large Language Multi-Modal Models* w skrócie: *GLLMMMs*, takich jak ChatGPT).

To dzięki pracy górników zabezpieczanie transferów bitcoina jest względnie łatwe bez szczegółowej znajomości technologii kryptograficznych. Wystarczy umieć odróżnić dobre narzędzia od złych zamiast robić wszystko samemu. Tak samo jak szyfrujemy zawartości naszych dysków, zabezpieczamy przed wirusami, czy chronimy przed hakerami – nie samodzielnie, lecz specjalnymi programami.

W każdej z tych sytuacji wiedzą jaką trzeba posiadać jest umiejętność znalezienia dobrego i sprawdzonego programu, który polecany jest przez wielu doświadczonych użytkowników i sprawdzony przez specjalistów, a nie ufać reklamom.

Transfer bitcoina odbywa się pomiędzy portfelami. Aby otrzymać i posiadać jakikolwiek bitcoin trzeba mieć taki portfel, na którym będzie on przechowywany. Jest to program albo fizyczne urządzenie. Co kluczowe trzeba znaleźć portfel, na którym będzie on mógł być bezpiecznie przechowywany. Chociaż ktoś mógłby powiedzieć, że nie potrzebujemy portfela aby posiadać bitcoin – wystarczy, że wiemy gdzie się on znajduje. Mogą to być programy zainstalowane na naszej komórce, czy na komputerze stacjonarnym, czy laptopie. Są one darmowe. Różnią się poziomem łatwości konfiguracji oraz bezpieczeństwem.

Jeśli nie chcemy uczyć się jak obsługiwać swój własny portfel możemy też zrezygnować z kontroli nad swoimi środkami i zaufać trzeciej stronie. Tego nie polecam, bo jak to nie twoje klucze to nie twój bitcoin (ang. *not your keys not your bitcoin*). W praktyce oznacza to, że ktoś inny będzie miał zainstalowany taki portfel i będziemy bitcoiny u niego trzymać. Jak pod jego materacem, a nie jak w banku, bo bez żadnych gwarancji bankowych. Paradoksalnie można więc otrzymać bitcoin na taki portfel i go nie posiadać (jeśli nasze środki nie znajdują się na naszym prywatnym portfelu).

To dlatego pierwszą rzeczą, którą polecam przed zakupem bitcoina, to zapoznać się z możliwościami instalacji i konfiguracji prywatnego portfela – najlepiej sprzętowego (ang. *hardware wallet*). Tak, aby nie musieć ufać nikomu w zakresie bezpieczeństwa naszych pieniędzy przechowywanych w bitcoinie i móc zachować finansową suwerenność. Jest ona w sieci bitcoin szczególnie łatwa do osiągnięcia, bo konfiguracja prywatnych portfeli nie jest szczególnie trudna (autorzy tych programów z roku na rok czynią je coraz prostszymi w obsłudze).

dr Zbigniew Galar

P.S.

Autor nie zachęca do zakupu bitcoina, nie odradza zakupu bitcoina, zachęca natomiast do edukacji na temat bitcoina oraz zdecydowanie odradza zakup jakiejkolwiek innej niezdecentralizowanej kryptograficznej waluty.