Jak zbudować własną kryptowalutę

Chyba ciężko dzisiaj unikać tego słowa – kryptowaluta. Wraz ze wzrostem popularności tej technologii niemal każdy z czytelników ma z nią mniejszą czy większą styczność. Okazuje się bowiem, że blockchain – technologia stojąca za kryptowalutami – może stanowić rozwiązanie wielu biznesowych problemów, nie tylko tych ze świata fintech. A zatem jak dołączyć do tego globalnego trendu i zbudować własne rozwiązanie oparte na technologii blockchain?

W tym artykule nie chcę omawiać tego, jak zbudowany jest blockchain i jak samemu zaimplementować uproszczone wersje jego mechanizmów w 300 liniach kodu. Nie będzie też prostej instrukcji odpowiadającej na pytanie tytułowe, bo taka nie istnieje. Zamiast tego opowiem o tym, jak zbudować w pełni działające rozwiązanie. Tak jak się to robi na poważnie.

TROCHĘ HISTORII (TYLKO TROCHĘ)

Koncept cyfrowych pieniędzy (z ang. *Ecash*) został przedstawiony już w 1983 roku przez amerykańskiego kryptologa Davida Chauma [0]. W 1995 roku pojawiła się pierwsza implementacja tego pomysłu, znana jako DigiCash. Rozwój tej gałęzi technologii mocno przyśpieszył; 3 lata później Wei Dai zaprezentował b-money jako „anonimowy, rozproszony pieniądz elektroniczny" [1]. B-money implementował *proof-of-work* i to na nim w dużej części została oparta najpopularniejsza dzisiaj kryptowaluta Bitcoin. Zbudowana w 2009 roku przez kogoś/coś/grupę ludzi pod pseudonimem Satoshi Nakamoto. Pewnie każdy słyszał wiele historii o rzekomym ujawnieniu się autora Bitcoina, jednak nikt do tej pory nie był w stanie udowodnić posiadania kluczy prywatnych kontrolujących te najwcześniej wykopane Bitcoiny. Co ciekawe, środki te (seria adresów po 50BTC każdy [2]) nie były transferowane nigdy w całej, już ponad 10-letniej historii Bitcoina. Całkiem niedawno nawet ktoś tłumaczył, że nie posiada dostępu do tych kluczy, bo – uwaga – w serwisie, do którego oddał swojego uszkodzonego laptopa, wyczyszczono mu dysk [3]. Autora najpopularniejszej aktualnie kryptowaluty nie znamy zatem do dziś.

Wkrótce po powstaniu Bitcoina na jego podstawie zaczęto pracować nad projektami pierwszych altcoinów (z ang. *alternative to Bitcoin*). Namecoin chwalił się wprowadzeniem odpornej na cenzurę domeny .bit, niezależnej od ICANN. Litecoin z kolei istotnie zmienia konfigurację sieci, m.in. zmniejszono czas bloku (z 10 min. do 2.5 min.) i zmieniono algorytm hashujący używany w *proof-of-work* (z SHA-256 na scrypt). Wszystko po to, żeby przyśpieszyć działanie sieci i ułatwić jej adaptację na szeroką skalę. Pierwsza udana implementacja nowego algorytmu konsensusu *proof-of-stake* to rok 2012 i Peercoin (PPCoin), a od kilku lat właściwie co tydzień powstaje nowy altcoin. Obecnie najpopularniejsze to wspomniany Litecoin, Ripple i – co jasne – Ethereum.

Ethereum, czyli druga najpopularniejsza kryptowaluta, została zaproponowana w 2013 roku przez rosyjskiego programistę Vitalika Buterina. Platforma ta, dzięki wprowadzeniu konceptu Smart Contractów (czyli niemal dowolnych kawałków kodu, które możemy odpalić na zdecentralizowanej maszynie wirtualnej EVM) została okrzyknięta blockchainem 2.0 i sporym krokiem naprzód w rozwoju tej technologii. Sam pomysł programowania zdecentralizowanych aplikacji przyjął się bardzo szeroko i zaczęły powstawać kolejne platformy oferujące podobną funkcjonalność. NEO, EOS czy Lisk to tylko przykłady.

CZY NA PEWNO TEGO POTRZEBUJESZ?

Blockchain to buzzword. Trend. Chyba podobnie jak AI, IoT i Big Data. Może ktoś słyszał historię małej, brytyjskiej firmy On-line Plc, której akcje wzrosły o 394% tylko po tym, jak dodali do swojej nazwy jedno słowo – Blockchain [4]. Teraz w samych Chinach jest ponad 33 tys. przedsiębiorstw zajmujących się tą technologią. To znaczy w jakiś sposób tłumaczących, że się zajmują [5]. Chyba nikogo nie zaskoczy stwierdzenie, że wszyscy chcą w jakiś sposób skorzystać na tej technologicznej bańce. Faktem jest jednak, że blockchain – jak przecież każda inna technologia – to tylko narzędzie. Użyte w nieodpowiednim projekcie lub w niewłaściwy sposób będzie tylko niewyczerpywalnym źródłem problemów. A zatem – kiedy prawie na pewno nie potrzebujesz tej blockchaina?

Brak potrzeby przechowywania danych to przypadek oczywisty – blockchain to przecież przede wszystkim baza danych. Jeśli zatem projekt nie przewiduje persystencji danych (lub te dane mają być trywialnie małe), blockchain raczej nie będzie pomocny.

Drugą skrajnością jest konieczność przechowywania ogromnych ilości danych. Przez „ogromne" rozumiem takie, które ciężko może być transferować na bieżąco pomiędzy wszystkimi użytkownikami sieci. Typowa transakcja BTC to 250 bajtów [6], więc szybko może się okazać, że nasze dane będą rzędy wielkości większe. Prostym przykładem może być biblioteka multimediów. Użycie do tego blockchaina jest niemal absurdalnym pomysłem.

Jeśli system ma być używany i kontrolowany przez jedną organizację, a jego użytkownicy nie mają uprawnień do modyfikacji przechowywanych danych, prawdopodobnie również potrzebuje zwykłej, scentralizowanej bazy danych. To rozwiązanie znacznie łatwiejsze, nie wprowadzające do projektu takiej złożoności, jaką wprowadza blockchain, a prawdopodobnie wystarczające do rozwiązania problemu biznesowego. Blockchain to też technologia, na której od podstaw, już na etapie projektowania, należy oprzeć system. Jego wprowadzenie na znacznym etapie zaawansowania projektu może się okazać zupełnie