https://wyborcza.pl/magazyn/7,124059,28656931,bitcoin-jest-dla-leszczy-poznajcie-ether-cos-wiecej-niz-kryptowalute.html

Wojciech Cellary 2022-07-09

Inteligentne kontrakty

W „Wolnej sobocie" z 21 maja opisałem sposób działania bitcoina – pierwszej kryptowaluty świata – i technologii łańcucha bloków (ang. Blockchain). Oprogramowanie bitcoina opracował i udostępnił w sieci jego kod źródłowy tajemniczy Satoshi Nakamoto w 2009 roku. Przy całej innowacyjności, bitcoin jest walutą i tylko walutą. Pomijając tworzenie bitcoinów, można je tylko kupić, mieć i sprzedać.

Pięć lat później objawił się kolejny innowator, który miał bardziej ambitny plan – zastosowanie łańcucha bloków do zbudowania światowego, rozproszonego, dobrze zabezpieczonego komputera, zdolnego do wykonywania dowolnie złożonych programów. Był nim Vitalik Buterin, urodzony w Rosji w 1994 r., który wyemigrował z rodzicami do Kanady w wieku 6 lat. W 2014 roku razem z kilkoma kolegami utworzył platformę *Ethereum* z nową kryptowalutą *ether*.

W systemie Bitcoin, w blokach są zapisywane transakcje płatności bitcoinami. Łańcuch bloków jest więc bazą danych, która przechowuje aktualny stan posiadania bitcoinów przez wszystkich ich właścicieli i całą historię płatności. Ethereum zapisuje w łańcuchu bloków dowolne dane, o różnym przeznaczeniu, i całą historię korzystania z nich.

Do wprowadzania danych do łańcucha bloków i operowania na nich służą *inteligentne kontrakty* (ang. smart contracts), nazywane w skrócie *i-kontraktami*. Są one podobne do kontraktów prawnych, ale są napisane w języku programowania i dlatego mogą być wykonane przez komputer. Kontrakty prawne mogą być niejednoznaczne w zależności od użytych wyrażeń, natomiast i-kontrakty są zawsze jednoznacznie interpretowane, co jednak nie oznacza, że zawsze w pełni oddają intencję kontraktora. I-kontrakty mogą obejść się bez prawników, sądów i komorników – jeśli warunki i-kontraktu są spełnione, to na pewno będzie on zrealizowany, a jeśli nie – to automatycznie będą zrealizowane zapisane w nim konsekwencje ich niespełnienia, które mogą obejmować wypłatę odszkodowania.

Wyobraźmy sobie i-kontrakt między dłużnikiem a wierzycielem. Zabezpieczeniem długu w etherach może być na przykład własność samochodu dłużnika. Jeżeli przed wyznaczonym terminem nie wpłynie do i-kontraktu kwota długu (tak, do i-kontraktu, a nie bezpośrednio do wierzyciela), to przeniesie on własność samochodu na wierzyciela. Jeśli kwota długu wpłynie do i-kontraktu, to przekaże on ethery wierzycielowi, a dłużnik pozostanie właścicielem samochodu. Jeśli w terminie wpłynie część długu, to można w i-kontrakcie zapisać dowolne warunki, jak wówczas postąpić – np. przedłużyć termin spłaty, ale naliczyć kary umowne.

I-kontrakty są pisane w specjalistycznych językach programowania, takich jak Solidity, a wykonywane przez *wirtualną maszyną Ethereum*. Jest to oprogramowanie, które dostosowuje dowolny komputer do platformy Ethereum. Aktualnie działają 23 tysiące węzłów Ethereum rozsianych po całym świecie.

Ethereum korzysta z łańcucha bloków, który jest replikowany w węzłach, w zasadniczo taki sam sposób jak w systemie Bitcoin. Też mamy do czynienia z wykopywaniem bloków przez konkurujących ze sobą kopaczy, którzy mozolnie poszukują dowodu pracy. W łańcuchu bloków Ethereum jest przechowywany kod i-kontraktów i ich trwała pamięć, więc nie można ich zmienić.

W Bitcoinie użytkownicy nie mają kont. Na podstawie transakcji zapisanych w łańcuchu bloków można jedynie obliczyć, ile każdy użytkownik ma bitcoinów. W Ethereum są dwa rodzaje kont: konta zewnętrzne przypisane do użytkowników i kontrolowane za pomocą ich kluczy prywatnych oraz konta i-kontraktowe kontrolowane przez kod i-kontraktu. Konto zewnętrzne nie zawiera kodu programowego; jego właściciel może natomiast wysyłać z niego wiadomości tworząc i podpisując transakcje swoim kluczem prywatnym. Za każdym razem, gdy konto i-kontraktowe dostanie wiadomość, uaktywnia swój kod, co umożliwia odczytanie pamięci, przetworzenie danych i zapisanie ich w pamięci, wysyłanie innych wiadomości, a nawet tworzenie innych i-kontraktów. Na koncie zewnętrznym są przechowywane ethery danego użytkownika, które mogą być przelewane na inne konta. Ethery można kupić na giełdach kryptowalut. Aktualnie jeden ether kosztuje około 1100 dolarów, ale w szczycie kosztował 4800 dolarów. Zasadniczym przeznaczeniem etheru nie jest zastąpienie walut narodowych, tylko opłacanie funkcjonowania światowego komputera. Koszt nie jest mały. Wykonanie transakcji kosztuje przy aktualnych cenach 1,16 dolara (w szczycie kosztowało ponad 11 dolarów), a zapisanie 1 MB pamięci do łańcucha bloków (2000 stron w Wordzie, czyli 4 ryzy papieru do drukarki) – aktualnie 35 tys. dolarów, a w szczycie 350 tys. dolarów (te koszty zależą nie tylko od kursu ETH/USD). Jeśli zamiast dokumentów zapisze się w łańcuchu bloków tylko ich kryptograficzne skróty, to obniży się koszty, ale skrót pozwoli tylko potwierdzić, że dokument jest autentyczny. Jeśli zostanie sfałszowany, lub skasowany, to ze skrótu nie odtworzy się oryginału.

Platforma Ethereum nie działa w tle, to znaczy niczego nie robi z własnej inicjatywy, a jedynie pod wpływem transakcji – tylko one mogą zmienić stan platformy i spowodować wykonanie i-kontraktu przez wirtualną maszynę Ethereum przekazując mu ethery i/lub niezbędne parametry. Jeśli jednak transakcja zostanie wysłana do nieistniejącego konta, to „spali" przekazywane ethery, które będą nie do odzyskania.

Najczęstszym zastosowaniem platformy Ethereum są tokeny, które mogą reprezentować:

- prywatną walutę – o wartości ustalonej w drodze handlu;
- zasób – np. pamięć, którą można współdzielić przez internet;
- aktywo – prawo własności np. do złota, nieruchomości, energii;

- prawo dostępu – do cyfrowej lub fizycznej własności, np. forum dyskusyjnego, strony internetowej, wynajętego samochodu;
- udział – np. w kapitale organizacji cyfrowej lub prawnej;
- prawo głosowania – w systemie cyfrowym lub prawnym;
- obiekt kolekcjonerski (NFT) – por. mój felieton w „Wyborczej" z 15 stycznia;
- tożsamość – cyfrową (np. awatara w wirtualnej rzeczywistości) lub prawną (np. PESEL);
- zaświadczenie – wydane przez formalny organ lub zdecentralizowany system reputacji (np. akt urodzenia, dyplom ukończenia studiów itp.).

Jak widać, tokeny są bardzo elastyczne i mogą znaleźć zastosowanie do różnych celów.

Drugim zasadniczym zastosowaniem platformy Ethereum jest tworzenie na niej rozproszonych aplikacji. Nie mają one centralnych serwerów ani administratorów, którzy ją kontrolują, a ich użytkownicy łączą się bezpośrednio. Po wystartowaniu, rozproszoną aplikację kontroluje większość jej użytkowników, a nie jej twórca. Takie aplikacje są odporne na sfałszowanie, co zapewnia łańcuch bloków, nie grozi im wyłączenie w powodu awarii centralnego serwera, bo nie ma centralnego serwera, nie można też w praktyce takiej aplikacji zablokować (ocenzurować), bo jej kopie działają na 23 tysiącach węzłów.

Wreszcie trzecim zasadniczym zastosowaniem platformy Ethereum są Rozproszone Autonomiczne Organizacje, które działają w podobny sposób jak przedsiębiorstwa, ale wszystkie decyzje są w nich podejmowane przez głosowanie ich właścicieli.

Podsumowując, Ethereum jest potężnym narzędziem realizacji umów między stronami bez pośredników za pomocą i-kontraktów, które są uniwersalnymi narzędziami umożliwiającymi tworzenie nowych form organizacyjnych i nowych wartości cyfrowych w formie specjalizowanych tokenów o różnym przeznaczeniu.

Zagrożenia w zastosowaniu Ethereum obejmują takie same, jak w przypadku Bitcoina, i dodatkowe. Takie same, to ryzyko zgubienia lub kradzieży kluczy prywatnych, co uniemożliwia dostęp do pieniędzy i i-kontraktów oraz wysokie koszty energii elektrycznej i obciążenie ekologiczne. Nowe – to wysoki koszt realizowania i-kontraktów, ryzyko niewykonania i-kontraktu ze względu na brak pieniędzy na koncie, błędy programistyczne w kodzie i-kontraktu i ryzyko wprowadzenia do łańcucha bloków sfałszowanych danych z zewnątrz, od których zależy przebieg i-kontraktu.

Korzystanie z Ethereum wymaga wysokich kompetencji, bo jest to narzędzie skomplikowane, a niewybaczające błędów. Jeśli w kodzie i-kontraktu będzie błąd wynikający z niekompetencji lub celowego oszustwa, to wykona się on z tym błędem, a jego skutki będą nieodwracalne. Korzystanie z Ethereum przez osoby niekompetentne i naiwne wystawia je na łatwy łup oszustów, bez możliwości dochodzenia sprawiedliwości.

Twórcom Ethereum zapewne marzył się świat bez prawników i pośredników – dwie umawiające się strony spisują i-kontrakt, który będzie bezwzględnie wykonany bez żadnych

opóźnień, zatorów płatniczych, konfliktów interpretacyjnych itp. To jednak oznacza oddanie się w ręce programistów. O ile bowiem wykształcony człowiek jest w stanie zrozumieć tekst napisany przez prawnika, nawet jeśli jest to prawnicza nowomowa, to bez zaawansowanej znajomości informatyki nikt nie zrozumie zapisu w Solidity. Jaki stąd wniosek? – Uczmy dzieci programować od szkoły podstawowej, aby przeżyły w cyfrowym świecie.