KRYPTOWALUTY

– ukryte, ale wszechobecne

by Kath Lockett

fot. © grandeduc / Adobe Stock

Każdy słyszał o bitcoinie. To była pierwsza kryptowaluta, która znalazła się w głównym nurcie. Są też inne, które z dnia na dzień zyskują na popularności. Teraz może już istnieć nawet ponad 1800 różnych rodzajów kryptowalut, a każdego dnia powstają nowe. Jak więc sprawić, aby waluty cyfrowe były bezpieczne?

Wyobraź sobie, że siedzisz w holu głównym ISO i czekasz na spotkanie. Obok ciebie siedzą jeszcze dwaj panowie, którzy też czekają na spotkanie. Witasz się z nimi i pytasz, co tu robią, a oni – Edward i Ryan – odpowiadają: „należymy do zespołu Komitetu Technicznego ISO/TC 68, który ma opracować Normy Międzynarodowe dotyczące aspektów bezpieczeństwa walut cyfrowych".

Jak większość ludzi najprawdopodobniej kiwniesz tylko uprzejmie głową, czując, że za mało wiesz, aby pytać dalej. Jest to trochę jak krok w nieznane, bo czym właściwie jest waluta cyfrowa? E-pieniądzem, b-pieniądzem, i-pieniądzem, e-walutą, walutą wirtualną? A definicja podaje tylko, że waluta cyfrowa to rodzaj pieniądza dostępnego tylko w formie cyfrowej, w przeciwieństwie do fizycznego, który znamy jako banknoty i monety.

Waluty cyfrowej, tak samo jak fizycznej, można używać do kupowania towarów i usług, choć w społecznościach graczy online sprawa może być nieco bardziej skomplikowana. W przeciwieństwie do prawdziwej waluty, waluta cyfrowa nie musi być wyemitowana przez rząd czy bank, a za to wykorzystuje kryptografię, aby online w sieci łączyć i datować transfery. Najlepszy znany przykład to bitcoin, który jest zdecentralizowany, ewentualnie nieregulowany, a także kontrolowany przez jego twórców i użytkowników w społecznościach internetowych.

Krypto rośnie w siłę

ISO ma już normę dla fizycznych walut – ISO 4217. Jest w użyciu od 1978 r. i zawiera listę kodów walut zweryfikowanych przez Bank Światowy. Te kody są trójliterowe, np. EUR dla euro, czy USD dla amerykańskiego dolara. Używają ich banki na całym świecie podczas transakcji finansowych.

Jednak rozwój walut cyfrowych jest tak szybki, że kody za nim nie nadążają. Norma ISO 4217 jest w stanie przydzielić ok. 500 trójliterowych kodów, podczas gdy waluty cyfrowe są tworzone i używane w Internecie w tysiącach odrębnych wersji. W 2018 r. oszacowano, że już wtedy istniało ponad 1800 możliwych walut cyfrowych.

W lipcu 2019 r. Międzynarodowy Fundusz Walutowy opublikował artykuł *The Rise of Digital Money*, w którym stwierdza się, że wzrost popularności waluty cyfrowej wynika z wygody, łatwości jej stosowania wraz z aplikacjami internetowymi oraz bardzo niskich kosztów dla użytkowników. Znaczenie ma również zaufanie, zwłaszcza w krajach takich jak Kenia, gdzie walutę cyfrową uważa się za bardziej godną zaufania niż banki czy firmy telekomunikacyjne.

W 2016 r., czyli mniej więcej w średniowieczu, jeśli chodzi o waluty cyfrowe, Grupa Studyjna ds. podstawowych usług bankowych Podkomitetu SC 7 Komitetu Technicznego ISO/TC 68 (obecnie rozwiązana) zwróciła uwagę, że waluty cyfrowe mogą zastąpić prawdziwy pieniądz w wielu dziedzinach, co wywołało obawy dotyczące stosowanych rozwiązań informatycznych, kryptografii oraz zaleceń bankowych, które miały zapewnić właściwą definicję waluty cyfrowej oraz bezpieczeństwo jej użycia. Już wtedy szacowano, że każdego dnia może dochodzić nawet do stu tysięcy transakcji przy użyciu kryptowalut.


fot. © dusanpetkovic1 / Adobe Stock

fot. © gmanedue / Adobe Stock

Ochrona walorów cyfrowych

Powróćmy do Edwarda i Rayana, a konkretniej do Edwarda Scheidt'a – przewodniczącego ISO/TC 68/SC 2/WG 17 *Security aspects of digital currencies* oraz Ryana Pierce'a – współprzewodniczącego grupy roboczej 17. Ich strona internetowa zawiera właściwie tylko tę niejasną nazwę. Czym więc zajmuje się ich grupa robocza?

Jako przewodniczący tej grupy Edward Scheidt współpracuje z krajową jednostką normalizacyjną USA (ANSI) i jest wiceprzewodniczącym tzw. ANSI x9 Global Security Standards (normy bankowe pod egidą ANSI); współpracuje również z Komitetem Waluty Cyfrowej Fiata i ITU (Międzynarodowa Unia Telekomunikacyjna). „Koncentrujemy się na sprawdzaniu potencjalnego bezpieczeństwa walut cyfrowych, żeby w przyszłości opracować normę ISO. Spotykamy się co miesiąc, a grupa liczy 21 członków reprezentujących różne stowarzyszone organy krajowe".

Technologia rozwija się w ogromnym tempie, a to stwarza problem wpływu na stabilność ekonomiczną waluty (niecyfrowej); oraz na to: jakie komercyjne oddziaływania na sektor prywatny może spowodować waluta cyfrowa; jakie pojawią się nowe kwestie polityczne i regionalne i jak połączyć te elementy w solidną strukturę, z której mogą korzystać wszyscy.

Edward Scheidt wyjaśnia, że pieniądze fizyczne mają mocne wsparcie ze strony zasad politycznych, prawa i reguł, które prowadzą do przepisów bankowych. Mimo że wygoda wydaje się być wielką przewagą pieniędzy w formacie cyfrowym, to do rozwiązania pozostają trzy kwestie dotyczące bezpieczeństwa:

1. Zaufanie, aby międzynarodowy ekosystem finansowy mógł gwarantować płatności i transakcje finansowe.
2. Wiążąca odpowiedzialność, aby inwestycje wspierające ekosystem finansowy nie miały negatywnych następstw prawnych.
3. Prywatność, aby indywidualny użytkownik dzięki wspierającej go infrastrukturze finansowej miał pewność, że informacje pozostaną prywatne, kiedy nie ma potrzeby ich ujawniania.

Wielkie plany

Kluczowe jest zbieranie informacji od członków ISO i ekspertów finansowych. Należy rozważyć szereg kwestii z punktu widzenia polityki, prawa, władz centralnych oraz bezpieczeństwa technicznego.

„Komitet Techniczny pracuje na linii styku między technologią bezpieczeństwa, jakiej wymagają te normy, a sposobem ich zastosowania w realnym biznesie. Potencjalnie przyglądamy się zbiorom pojęć i wskazówkom od władz krajowych, aby stworzyć ramy bezpieczeństwa, do których będą pasowały wszystkie formaty cyfrowe".

„Musimy obecne normy zaktualizować tak, aby zapewnić ich interoperacyjność między uznawanymi w różnych krajach systemami walut cyfrowych. To będzie pierwszy krok w kierunku powszechnego uznania. Zaufanie jest najważniejsze: bez niego cała technologia świata nie dostarczy rozwiązania".

Obaj panowie podkreślają, że trzeba również zauważyć, iż waluta cyfrowa to nie tylko zmartwienie dla krajów i ich agencji rządowych: przedsiębiorstwa i firmy komercyjne też działają w tym obszarze, który tradycyjnie pozostawiono rządom. Te normy mogą, przy ostrożnych szacunkach, oddziaływać na transakcje cyfrowe o wartości do jednego biliona dolarów dziennie, więc bezpieczeństwo jest arcyważne.

Rozproszone zaufanie

Ryan Pierce, wiceprzewodniczący Digital Asset Working Group w FIX Trading Community i jednocześnie członek i ekspert Komitetu Technicznego ISO/TC 68/SC 8/WG 3, idzie dalej. „Badamy tworzenie identyfikatorów dla tokenów cyfrowych. To jest w tej chwili przeszkoda dla nas wszystkich, ponieważ cały czas powstaje mnóstwo nowych typów zasobów cyfrowych, a my musimy być w stanie je zidentyfikować, aby wyeliminować wszelkie niejednoznaczności między firmą nadawcą i firmą odbiorcą".

Wyjaśnia, że chociaż bitcoin był pierwszą walutą cyfrową, to od jego powstania stworzono już tysiące innych kryptowalut, które są w użyciu. Te jednostki monetarne reprezentują handel wymienny, akcje, papiery wartościowe i usługi, a wszystkie wykroczyły poza pierwotną funkcję bitcoina. Spełniają funkcję podobną do walut, ponieważ mogą być używane jako środek wymiany, ale mogą wyjść poza tę definicję, jeśli są również tokenami powiązanymi ze specyficznymi użytecznościami lub usługami, jak np. pozwolenie na przechowywanie danych we wspólnej chmurze, otrzymywanie dodatkowych tokenów w zamian za oglądanie reklam albo dostarczanie innych usług.

„Kiedy po raz pierwszy wprowadzono bitcoina, pomógł on rozwiązać problem rozproszonego zaufania. Jeśli ktoś chciał w przeszłości handlować walorami cyfrowymi, musiał wybrać zaufaną stronę, aby prowadziła księgę rachunkową oraz rejestr tego, kto był właścicielem czego. Na przykład, większość z nas ufa bankom. Wiemy, że możemy użyć naszych kart kredytowych, żeby zapłacić za obiad; ufamy, że zostaniemy obciążeni właściwą sumą i tylko raz".

W przypadku bitcoina, jak mówi, nikt nie jest w stanie nadzorować ani modyfikować transakcji, a to nie wymaga już zaufania do jednego podmiotu. Technologia umożliwia stworzenie księgi rachunkowej, która jest niezależna od banku. Działa dzięki temu, że wystarczająca liczba osób używa tego samego oprogramowania komputerowego w celu osiągnięcia jednomyślności w sprawie stanu księgi rachunkowej; zmiana albo usuwanie dawnych transakcji staje się więc nieopłacalne.

Cyfrowy dowód tożsamości

Ryan Pierce podaje dobry przykład, jak właściwie należałoby identyfikować kryptowalutę. „Jeżeli chcesz zrobić mi przelew na sto dolarów USA, to automatycznie użyjesz normy ISO 4217 z kodami walut, która identyfikuje dolara amerykańskiego jako USD. Wszystkie banki świetnie wiedzą, co to znaczy i nie ma tu żadnych wątpliwości. Istnieją również numery ISIN (Międzynarodowy Numer Identyfikacji Papierów Wartościowych), też określone przez ISO, które definiują inne rodzaje papierów wartościowych, takich jak akcje, obligacje i instrumenty pochodne. Sprawia to, że wszystkie transakcje są zrozumiałe i jednoznaczne dla wszystkich banków na całym świecie".

„Waluta cyfrowa nie ma jednak oficjalnych identyfikatorów, nazw ani kodów walutowych. Twój bank odróżnia dolara amerykańskiego od euro, ale jak ma określić różnicę między bitcoinem a bitcoinem cash?". Oto problem, przed którym stoi ISO. Nigdzie na świecie nie ma żadnego urzędu,

który odpowiadałby za kryptowaluty, nie ma więc również oficjalnego sposobu na zdefiniowanie bitcoina czy jakiejkolwiek innej waluty cyfrowej; nie ma też żadnego uznanego powszechnie identyfikatora w tej materii".

„W 2016 r. ustalono, że walutom cyfrowym, takim jak bitcoin, które nie zostały wyemitowane przez władze monetarne, nie można przypisać kodów walutowych wg ISO 4217 (takich jak USD czy EUR). My zaś uważamy, że potrzebna jest odrębna lista kodów do identyfikacji – identyfikatory tokenów cyfrowych. Takie kody wyeliminują niepewność i umożliwią bankom i innym instytucjom finansowym transfery tokenów cyfrowych. Dzięki łatwej identyfikacji unikniemy nieporozumień" – tłumaczy Ryan.

Tak jak w przypadku wszystkich norm ISO, są to jedynie wytyczne najlepszych praktyk, a nie obowiązkowe regulacje. „Nie będziemy wydawać żadnych opinii w sprawie niezawodności tokenów cyfrowych, którym miałyby zostać wydane identyfikatory, ponieważ nie możemy dokonywać ocen. Jeżeli istnieje waluta cyfrowa albo token, to kwalifikuje się do posiadania identyfikatora. Co wcale nie oznacza, że wszystkie kryptowaluty, które mają identyfikatory są godne zaufania i mają wartość. To tak jak z aktem urodzenia, który określa, że ktoś się urodził i oficjalnie istnieje, ale nie można na podstawie tylko tego dokumentu dokonywać innych ocen (np. tego, czy ktoś jest wiarygodny albo czy ma zdolność kredytową)".

Zwalczając oszustwa

Pojawia się niepokojący model biznesowy, w którym firmy planują stworzyć platformę cyfrową w celu świadczenia usługi, a następnie sprzedają tokeny, którymi można płacić za tę konkretną usługę. Inwestorzy kupują tokeny, licząc na wzrost ich wartości po uruchomieniu serwisu. Ale na porządku dziennym są „firmy-wydmuszki", które biorą pieniądze, a potem znikają. W takiej sytuacji identyfikator tokena cyfrowego (DTI) nadal możne zostać wydany dla takiego tokena.

Ryan Pierce wyjaśnia znaczenie wprowadzenia identyfikatorów tokenów cyfrowych (DTI) przy ograniczeniu oszustw. „W regulowanych branżach organy regulacyjne często pytają o zapisy transakcji. Banki potrafią wykryć podejrzaną aktywność finansową i złożyć raporty, jeżeli np. na twoim koncie nieoczekiwanie pojawi się sto tysięcy dolarów amerykańskich. Ale czy organy regulacyjne mogą pytać o zapisy podejrzanych działań finansowych dokonanych walutą cyfrową? Bez oficjalnego identyfikatora tokena cyfrowego regulatorom trudno by było zrozumieć takie dane".

„Nie chodzi tylko o organy regulacyjne. Przeciętny użytkownik ma korzyść z dostępu do DTI oraz możliwość ich użycia, żeby wiedzieć dokładnie, co wysyła czy otrzymuje. Mogę sprzedać ci mój samochód za pięć tokenów bitcoina, ale kiedy dokonujemy faktycznej transakcji, możesz mi wysłać coś zupełnie innego. Bez oficjalnej definicji bitcoina czy rozpoznawalnego kodu identyfikacyjnego jest tu za dużo niepewności. Cyfrowe identyfikatory tokenów wyeliminują niepewność (albo celowe oszustwo); będzie to obiektywny sposób identyfikacji określonej waluty cyfrowej lub tokenu".

Warto obserwować postępy prac ISO/TC 68/SC 2/WG 17 *Security aspects of digital currencies*. Wygląda na to, że będzie się działo.

Źródło: www.iso.org
Oprac. P. M.

Z ISO/TC 68/SC 2 współpracuje krajowy PKN/KT 271 ds. Bankowości i Bankowych Usług Finansowych