Analizy finansowe blockchain

Marek Kołtun

Security
in practice

ISSN: 2719-9282

Analizy finansowe blockchain

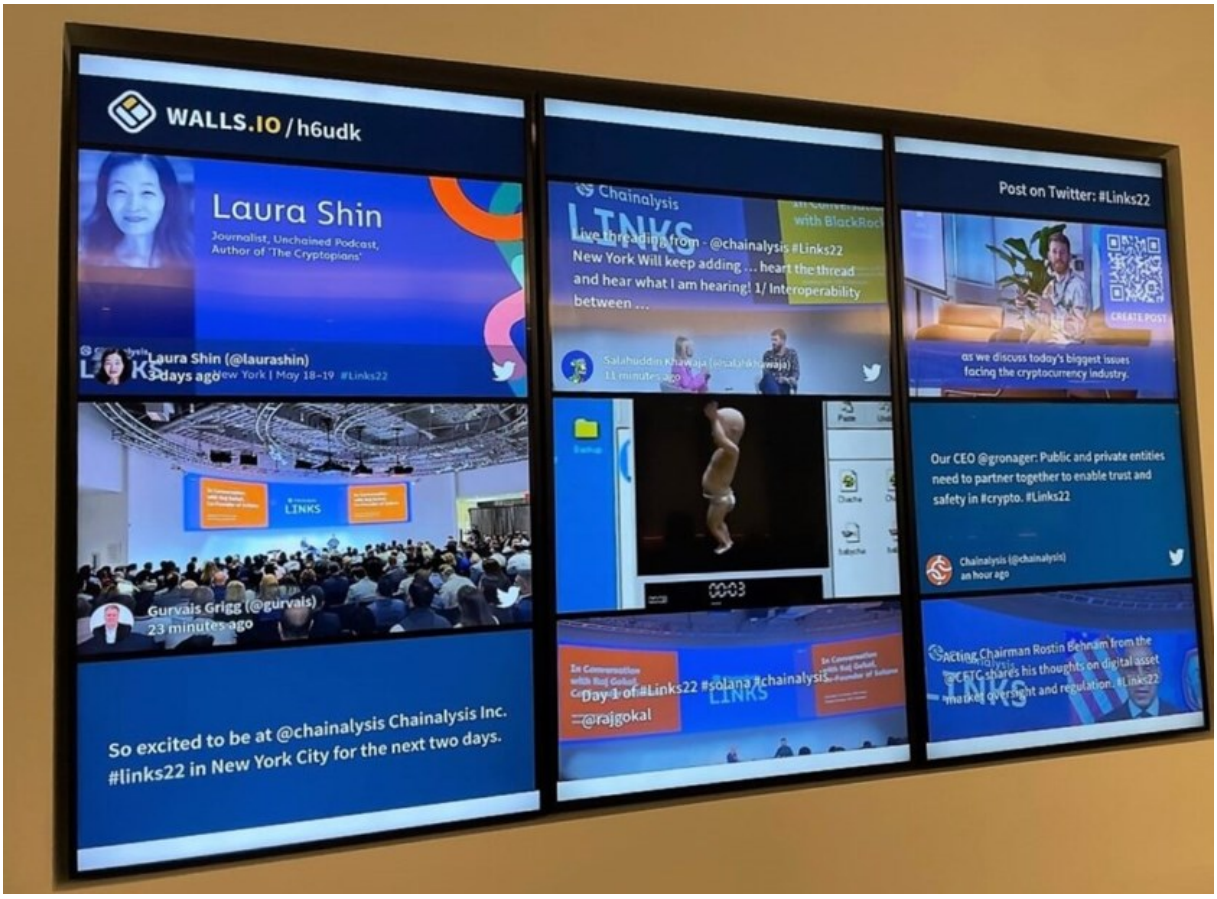
Opracował: Marek Kołtun, 12.09.2022 r.

W dniach 18–19 maja 2022 r. w Nowym Jorku odbyła się konferencja pt. „Chainalysis Links", w której uczestniczył Marek Kołtun – biegły sądowy, a także analityk firmy Security in Practice. Był on jedynym reprezentantem Polski na elitarnej nowojorskiej konferencji. Organizatorem uroczystości był globalny podmiot specjalizujący się w analizie blockchain – Chainalysis, który współpracuje na co dzień z Federalnym Biurem Śledczym Stanów Zjednoczonych (FBI) czy Narodową Agencjąnds. Przestępczości (NCA), Specjaliści z Chainalysis podejmują współpracę także z innymi podmiotami o profilu działania podobnym do FBI czy NCA, na całym świecie.

Głównym celem konferencji była wymiana doświadczeń ekspertów i liderów z całego świata, którzy zajmują się analizą ekosystemu kryptograficznego. Wydarzenie było zorganizowane na dwóch poziomach - dla początkujących i zaawansowanych w obszarach związanych z m.in. DeFi po NFT, DEX, czy Web3, a także zorganizowaną przestępczością kryptograficzną, compliance, zarządzaniem ryzykiem i śledztw. Wśród zaproszonych gości znalazły się takie osoby, jak burmistrz Nowego Jorku, dziennikarka Laura Shin, przedstawiciele administracji Stanów Zjednoczonych, a także osoby funkcyjne największych instytucji inwestycyjnych zajmujących się cyfrowymi finansami.

Drugim istotnym celem opisywanej konferencji było wskazanie występującego ryzyka przeciwdziałania praniu brudnych pieniędzy oraz finansowania terroryzmu, które powstają podczas wyzwań technologicznych, zachodzących przy opracowywaniu zgodności funkcjonowania kryptowalut [od tradycyjnych programów zgodności. Równie istotne było przytoczenie funkcji należytej staranności oraz regulacji bankowych (ang. KYC, czyli „poznaj swojego klienta") przy opracowywaniu kryptograficznych analiz finansowych. W trakcie prezentacji pojawiały się zagadnienia związane z Web3, czyli terminem, którego autorem jest Gavin Wood, współzałożyciel kryptowaluty Ethereum. Przewodnią funkcją Web3 – Internetu przyszłości jest

maksymalna decentralizacja, co oznacza, że opisywana sieć będzie we władaniu jej twórców, a nie globalnych koncernów.



Kolejnym istotnym obszarem w funkcjonowaniu kryptoaktywów są zdecentralizowane giełdy zwane DEX, które pozwalają kupującym lub sprzedającym kryptowaluty na ich wymianę bez obowiązku przekazywania nadzoru nad swoimi wartościami któremukolwiek pośrednikowi.

Do najpopularniejszych kryptogiełd należą Binance, Huobi, Bitfinex. Oprócz DEX prelegenci przedstawili prezentację dotyczącą funkcjonowania finansów zdecentralizowanych zwanymi DeFi. Termin ten odnosi się do aplikacji, która działa w oparciu o technologię blockchain. Zachodzą tam różnego rodzaju transakcje rachunkowe, które wcześniej nadzorowały banki lub inne instytucje finansowe. Dla kryptograficznych aplikacji DeFi pośrednicy są zbędni, a znaczna część kontroli należy do właścicieli kryptoaktywów. Niesie to za sobą przeprowadzanie szybszych transakcji, a także mniejsze koszty.

Warta uwagi była prezentacja połączonych trzech organów ścigania: US Secret Service, administracji podatkowej USA i funkcjonariuszy policji w Calgary w Kanadzie, którzy na podstawie prowadzonego postępowania przygotowawczego, własnych spostrzeżeń

i wyciągniętych wniosków pokazali sposoby ujęcia sprawców czynów zabronionych w obszarze blockchain.

Przedstawiciele Chainalysis podczas wystąpienia dla gości specjalnych zaprezentowali praktyczną prezentację przy wykorzystaniu swojej aplikacji analitycznej blockchain na przykładzie ujawnienia cybersprawców z Korei Północnej. W 2021 r. Grupa Lazarus powiązana z Koreą Północną, zwana także jako ATP38 (kierowana przez wojskową agencję wywiadowczą), dokonała co najmniej siedem ataków na platformy kryptowalutowe, podmioty inwestycyjne i scentralizowane giełdy. Przynętami były wiadomości phishingowe, expoity, złośliwe oprogramowanie, a także zaawansowana socjotechnika do wprowadzania wartości finansowych z „gorących" portfeli kryptograficznych wymienionych podmiotów, które posiadały stały dostęp do sieci online. Po kradzieży tych instrumentów finansowych Korea Północna rozpoczęła proces przeprowadzania cyfrowych instrumentów przez cztery etapy prania brudnych pieniędzy, aby w końcowym rezultacie zintegrować i wypłacić pieniądze. Zatem możemy określić ten przypadek jako klasyczny przykład wykorzystania kryptoaktywów do procederu prania brudnych pieniędzy.

Różnorodność skradzionych kryptoaktywów przez wywiad wojskowy Korei Północnej pozwoliła na określenie różnych metod wprowadzania do obiegu „wypranych" wartości finansowych:

1. Tokeny i altcoiny ERC-20 są zamieniane na kryptowalutę Ethereum za pośrednictwem wymiany zdecentralizowanych kryptogiełd.
2. Kryptowaluta Ethereum jest mieszana transakcjami wpłat i wypłat, a następnie wymieniana na kryptowalutę Bitcoin.
3. Transakcje kryptowaluty Bitcoin zostają zmiksowane i wysyłane do nowo utworzonych portfeli na adresy depozytowe, które znajdują się na kryptogiełdach usytuowanych w Azji – są to potencjalne punkty wypłaty.

Na uwagę zasługuje także nowa forma przestępczości kryptograficznej, czyli ransomware, która polega na blokowaniu dostępności do systemów elektronicznych. Federalne Biuro Śledcze Stanów Zjednoczonych poinformowało, że według stanu na luty 2022 r. zidentyfikowali płatności, jakie były pobierane za udostępnienie oprogramowania ransomware o wartości ponad 720 mln USD. FBI przedstawiło także praktyczne zastosowanie zaawansowanej aplikacji analiz finansowych, która pozwala na powiązanie schematami śladów, jakie zostały pozostawione w sieci online. Następnie aplikacja segreguje w schematy

graficzne, by w przejrzysty sposób można było wyciągnąć wnioski i dalsze zamierzenia w kierunku ujęcia sprawcy lub sprawców.

W dalszym ciągu rośnie ogromny postęp technologiczny w dziedzinie cyfrowych instrumentów finansowych. Wraz ze wzrostem pojawiają się nowe ryzyka zagrożeń, które bywają trudne do zidentyfikowania. Aby temu zapobiec, należy najpierw wejść w posiadanie odpowiedniej wiedzy specjalistycznej, dzięki której staniemy się ostrożniejsi i świadomi zagrożeń.