ZASTOSOWANIE TECHNOLOGII BLOCKCHAIN W OBSZARZE CYBERBEZPIECZEŃSTWA NA PRZYKŁADZIE CRYPTOJACKINGU

Łukasz Pietraszek
Wydział Elektroniki i Technik Informacyjnych
Politechnika Warszawska
Warszawa, Polska
lukasz.pietraszek@protonmail.com

***Abstrakt* — Technologia Blockchain przyniosła wiele nowych rozwiązań w obszarze cyberbezpieczeństwa. Niestety wraz z nią pojawiły się nowe rodzaje ataków. Cryptojacking to rodzaj ataku mającego na celu przejęcie zasobów ofiary w celu uzyskania zysków. Generuje to znaczne zużycie mocy obliczeniowej, zmniejszając wydajność komputera ofiary. Atak ten jest powszechny od 2017 roku i staje się coraz większym zagrożeniem dla bezpieczeństwa sieci. Artykuł ma charakter przeglądowy, przedstawiono podstawy funkcjonowania technologii Blockchain, a celem pracy jest przybliżenie rosnącego problemu, jakim jest cryptojacking w sieci.**

Słowa kluczowe – blockchain; cryptojacking; kryptowaluty; cyberbezpieczeństwo; złośliwe oprogramowanie

I. WPROWADZENIE

Współczesne realia technologiczne sprawiają, że bezpieczeństwo systemów staje się coraz bardziej kluczowym aspektem każdej dziedziny życia. Powszechna cyfryzacja powoduje przeniesienie sporej części życia publicznego do sieci. Obecnie kończy się era Internetu 2.0, który wniósł względem poprzedniej generacji możliwość interakcji ze stronami internetowymi. W miejsce sieci drugiej generacji wchodzi Internet 3.0, który wprowadza rozwiązania Internetu Rzeczy, sztucznej inteligencji, uczenia maszynowego, czy technologii Blockchain [1].

Powoduje to nasilenie ataków hackerskich oraz wzmożoną aktywność systemów odpowiedzialnych za bezpieczeństwo w sieci, ze względu na funkcjonowanie coraz większych i bardziej skomplikowanych systemów informatycznych. Jednym z przykładów jest rozwój kryptowalut, który sprawił, że atakujący mogą w łatwy sposób wykorzystać osobisty sprzęt ofiary bez jej wiedzy [2].

Aby dobrze zrozumieć problem najpierw zostanie opisana technologia Blockchain, jak działa i dlaczego jej zdecentralizowana budowa stwarza wiele możliwości zarówno dla użytkowników, ale również dla hackerów.

II. TECHNOLOGIA BLOCKCHAIN

Blockchain, czyli tłumacząc dosłownie „łańcuch bloków", to rozproszona baza danych, która zawiera wciąż rosnącą ilość informacji [3][4][5]. Charakterystycznymi cechami, którymi wyróżnia się ta technologia są decentralizacja i zastosowanie techniki peer-to-peer (P2P). Oznacza to, że takie systemy nie posiadają centralnego ośrodka sterującego, a zamiast tego korzystają z sieci rozproszonej, którą stanowią użytkownicy sieci. Stworzona w ten sposób infrastruktura sprawia, że taki model jest bardzo bezpieczną formą przechowywania danych [3][4][6].

Liczba zastosowań Blockchain rośnie z biegiem lat, przez co technologia ta staje się coraz bardziej popularnym rozwiązaniem w wielu aspektach tworzenia i wykorzystywania oprogramowania [7]. Od początku jej istnienia w 2009 roku kojarzona jest przede wszystkim z umożliwianiem wykonywania szybkich i bezpiecznych transakcji bez względu na odległość. W tym celu powstały kryptowaluty (*ang. cryptocurrency*). Rozwój technologiczny, a także stale rosnące zainteresowanie możliwościami, jakie daje Blockchain sprawiło, że obecnie liczba giełd kryptowalutowych, a także samych kryptowalut, znacznie wzrosła [3][7].

Dynamiczny rozwój rynku spowodowany jest łatwością, z jaką każdy może stworzyć własną kryptowalutę i wprowadzić ją na rynek. Zastosowana technika klucza publicznego i prywatnego (*ang. public-private key*) sprawia, że dobrze zabezpieczone dane mogą być przesyłane łatwo i niskim kosztem. Wykorzystanie tego rozwiązania oprócz zapewnienia bezpieczeństwa transakcji pozwala rozwiązać problem weryfikacji prawidłowości danych, co daje wiele możliwości w sektorze administracji [8].

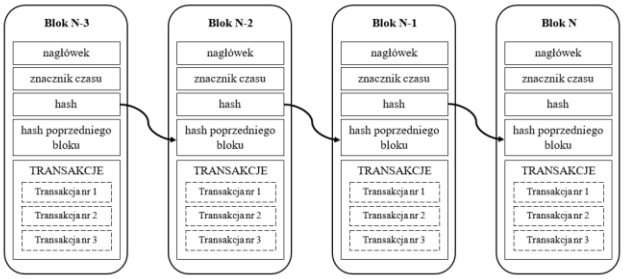
A. Konstrukcja i działanie bloków

Informacje przetwarzane wewnątrz systemu zapisywane są w blokach. Każdy blok składa się z kilku stałych elementów:

- nagłówek;
- czas jego utworzenia;
- unikalny odnośnik (*ang. hash*), który pozwala go zidentyfikować;
- odnośnik do poprzedniego bloku;
- transakcje, czyli dane zapisane w bloku.

Cechą charakterystyczną dla takiego systemu jest nierozerwalny łańcuch bloków, wynikający z połączenia między tymi blokami. Dzięki temu próba manipulacji

informacjami w bloku, który znajduje się już w sieci, wiązałaby się z koniecznością modyfikacji wszystkich innych bloków w łańcuchu, co nie jest możliwie. W przypadku błędu informacje zapisywane są jako nowa transakcja, zamiast nadpisywania poprzedniej [3][5]. Dodatkowo dzięki P2P każdy ma dostęp do rozproszonego rejestru, a każda transakcja rejestrowana jest tylko raz, co pozwala uniknąć dublowania informacji [6].



SCHEMAT I. SCHEMAT KONSTRUKCJI BLOKÓW

B. *Proces wydobycia i protokoły konsensusu*

Wydobycie (*ang. mining*) to proces, w ramach którego strony biorące udział w sieci opartej na technologii Blockchain zgadzają się na przeprowadzenie transakcji zatwierdzanej przez wszystkich uczestników tej sieci [9][10].

W celu zatwierdzenia bloku w łańcuchu używane są różne metody, ale wśród nich wyróżnia się dwie podstawowe:

1) Dowód pracy (ang. proof-of-work, PoW): oryginalny protokół konsensusu w sieci Blockchain, który umożliwia potwierdzanie transakcji w sieci, w którym czynnikiem determinującym udział w wydobyciu jest moc obliczeniowa jaką dysponują procesory graficzne górnika (*ang. miner*).

2) Dowód stawki (ang. proof-of-stake, PoS): protokół, w którym stan posiadania bieżących środków na portfelu (*ang. wallet*) decyduje o szansie zatwierdzenia poszczególnych bloków. W przeciwieństwie do PoW nie wymaga dysponowania dużą mocą obliczeniową, a jedynie blokady depozytu środków w specjalnym portfelu. Algorytm zaprojektowany jest w taki sposób, aby zapobiec monopolowi na wydobycie w obszarze konkretnego łańcucha [3][10].

Istnieje wiele innych, nowszych protokołów, jednakże wszystkie w większym lub mniejszym stopniu bazują na PoW lub PoS [10].

C. *Rozwiązania programistyczne oparte o Blockchain*

Aplikacje oparte na Blockchain są określane mianem aplikacji zdecentralizowanych (dApp) [11] i można utworzyć je przy pomocy większości współczesnych języków programowania. Realizacja transakcji jest możliwa dzięki inteligentnym kontraktom (*ang. smart contracts*) zawieranym pomiędzy użytkownikami w sieci. Polega to na cyfrowej realizacji transakcji z gwarancją obustronnej korzyści. Charakterystyczną cechą takich aplikacji jest konieczność dokładnego testowania i unikania błędów w inteligentnych kontraktach [12], ponieważ po wydaniu ostatecznej wersji i stworzeniu łańcucha, modyfikowanie jego zawartości będzie niemożliwe, a zatem błędów nie będzie można skorygować.

Obecnie jednymi z bardziej popularnych języków programowania, służącymi do implementacji rozwiązań opartych na Blockchain są JavaScript i TypeScript, a szczególnie warta wyszczególnienia jest obszerna biblioteka web3.js [13]. Rozwiązanie to jest najbardziej popularne wśród deweloperów, dzięki czemu można znaleźć bardzo wiele dokładnych objaśnień specyfikacji. Ponadto specyfika tych języków sprawia, że kod interpretowany jest po stronie klienta, co jest kluczowe dla bezpieczeństwa transakcji zapisywanych w łańcuchu bloków [3].

D. *Blockchain w zakresie cyberbezpieczeństwa*

Każdą technologię można wykorzystać w dobrym lub złym celu. Doskonałym przykładem rozwiązania problemu cyberprzestępczości w życiu publicznym jest wprowadzony w Estonii projekt administracji publicznej E-stonia. Wiosną 2007 roku Estońska Partia Reform po wygranych wyborach, chcąc podkreślić swoją autonomię od dawnego ZSRR, wydała decyzję o przeniesieniu pomnika tzw. Brązowego Żołnierza [14]. W wyniku tego rosyjscy cyberprzestępcy na kilkanaście dni zablokowali wszystkie strony bankowe, informacyjne, a także rządowe w Estonii, co spowodowało całkowity paraliż państwa. Wówczas władze tego nadbałtyckiego państwa postanowiły wdrożyć do infrastruktury publicznej system X-road, który zabezpieczony został przy pomocy technologii Blockchain. Serwis udostępniał takie usługi jak e-Voting (głosowanie online), e-Tax Board (rozliczanie podatków), e-Ticket (bilety), e-Banking (bankowość elektroniczna) i wiele innych [15]. System prężnie rozwijał się przez ostatnie 15 lat, jednak obecnie po zmianie władzy w kraju zauważalny jest trend odchodzenia od rozwiązań zdecentralizowanych [16].

Negatywnym wpływem rozwoju technologii łańcucha bloków jest cryptojacking, który staje się coraz bardziej popularnym rodzajem cyberataku.

III. CRYPTOJACKING

Cryptojacking to metoda ataku, wykorzystująca urządzenia w sieci, aby bez zgody i wiedzy ich właścicieli potajemnie wydobywać waluty cyfrowe na koszt ofiary. Zamiast wykorzystywać własne komputery do wydobywania, hakerzy wykorzystują cryptojacking do kradzieży zasobów obliczeniowych urządzeń swoich ofiar. Po zsumowaniu wszystkich kradzionych zasobów, hakerzy są w stanie konkurować z zaawansowanym sprzętem do wydobywania kryptowalut bez ponoszenia wysokich kosztów ogólnych [17][18].

A. *Rodzaje cryptojackingu*

1) Cryptojacking oparty na plikach: wykorzystuje złośliwe wiadomości e-mail w celu uzyskania dostępu do infrastruktury komputera. Technika ta bazuje

na nieuwadze użytkowników, którzy są przekonani, że przeglądają kolejny mail od zaufanego podmiotu (np. banku, operatora sieci) i nieświadomie pobierają na swój komputer pliki wykonywalne w formie załączników. Po pobraniu skrypty działają w tle, niezauważalnie wydobywając kryptowalutę bez wiedzy wiedzy użytkownika [19].

2) Cryptojacking oparty o przeglądarkę: dotyczy popularnych przeglądarek, takich jak Google Chrome, Mozilla, Safari. Atakujący tworzą skrypt do wydobywania kryptowalut. Osadzają go bezpośrednio w witrynach, do których uzyskuje się dostęp z zainfekowanej przeglądarki, ale także przy pomocy przestarzałych wtyczek czy reklam.

3) Cryptojacking wykorzystujący chmurę: osoby atakujące przeszukują kod lub pliki organizacji w nadziei na znalezienie kluczy API umożliwiających dostęp do usługi w chmurze. Następnie mogą wykorzystywać zasoby procesora do wydobywania kryptowalut, co prowadzi do ogromnego wzrostu poziomu energii elektrycznej i wykorzystanej mocy komputera. Przejęcie usług w chmurze jest bardziej skomplikowane, ale mimo to chmury mogą być celem ataku [19][20].

B. Obrona przed cryptojackingiem

Wydobywanie kryptowalut może odbywać się lokalnie w systemie lub w przeglądarce. Znajomość różnicy może pomóc w rozwiązaniu problemu, ponieważ obie metody wymagają różnych form ochrony. Rozwiązania są prawie tak znane jak problem, ale żeby się bronić trzeba być świadomym ataku [21]. Kluczową kwestią jest trudność wykrycia po zainfekowaniu w systemie, ponieważ procesy potrafią ukrywać się udając zadania systemowe. Wśród klasycznych objawów ataku typu cryptojacking wyróżnia się m.in.: przegrzany procesor, wyższe wykorzystanie CPU i GPU, drastyczne zwolnienie systemu operacyjnego, nietypowe działanie systemu. W przypadku przeglądarki istnieją wtyczki blokujące kod JavaScript, wśród których najpopularniejsze to *NoCoin* i *MinerBlock* [22].

C. Cryptojacking – realne zagrożenie

Według raportu analityków, w 2022 roku wśród wszystkich rodzajów cyberataków nadal najpopularniejszy jest ransomware oraz cryptojacking. Sytuacja ta utrzymuje się od 2017 roku, a w obie te techniki zaangażowane są kryptowaluty. Cyberprzestępcy będą coraz szybciej wykorzystywać luki w urządzeniach i systemach do instalowania złośliwego oprogramowania. Na znaczeniu zyskają też techniki umożliwiające generowanie fałszywych obrazów i dźwięku, które będą wykorzystywane m. in. w atakach phishingowych czy kampaniach dezinformacyjnych [23].

W badaniu najgroźniejszych zagrożeń w chmurze respondenci najczęściej wskazują wyciek danych, co jest zrozumiałe. Wycieki zdarzają się stosunkowo rzadko, a gdy już się wydarzą to często informacje o nich są publikowane. Należy jednak zwrócić uwagę na fakt, że respondenci wyraźnie oddzielili złośliwe oprogramowanie i cyberataki od cryptojackingu. Świadczy to o tym, że tego typu atak staje się coraz bardziej powszechnym, a co za tym idzie pojawia się w świadomości respondentów jako potencjalne zagrożenie [24][25].

IV. Złośliwe oprogramowanie

Cryptojacking oparty na plikach charakteryzuje się wykorzystaniem procesów podszywających się pod zadania systemowe. Wykorzystuje się do tego celu bezplikowe złośliwe oprogramowanie, czyli odmianę złośliwego kodu, który wpływa na system ofiary bez zostawiania żadnego pliku. Tego typu oprogramowanie jest zapisywane bezpośrednio w pamięci RAM komputera, a jego kod jest wstrzykiwany do działających procesów, takich jak iexplore.exe (główny plik wykonywalny przeglądarki Internet Explorer) [26].

A. COINHIVE

Coinhive był na rynku od 2017 roku, wykorzystywał biblioteki JavaScript, które można było instalować na stronach internetowych, aby wykorzystywać moc obliczeniową odwiedzających do legalnego wydobywania kryptowaluty Monero. Po jego zamknięciu liczba ataków związanych z cryptojackingiem wykorzystującym witryny internetowe spadła w drugiej połowie 2019 r o 78%. Według ENISA w wyniku tego spadku cyberprzestępcy zaczęli koncentrować się na celach o większej wartości, takich jak potężne serwery i infrastruktury chmurowe. Miejsce Coinhive w czołówce zajęły od tego czasu Jsecoin 22%, XMRig 21%, i Cryptoloot 21% [27].

B. XMRIG

XMRig to wysokowydajne otwarte oprogramowanie wykorzystujące procesor CPU/GPU i test porównawczy RandomX. Oficjalne pliki binarne są dostępne dla systemów Windows, Linux, macOS i FreeBSD. Domyślnym sposobem konfiguracji koparki jest plik konfiguracyjny JSON. Interfejs wiersza poleceń nie obejmuje wszystkich funkcji, takich jak profile wyszukiwania dla różnych algorytmów. Ważne opcje można zmienić w czasie wykonywania bez ponownego uruchamiania procesu górnika, edytując plik konfiguracyjny lub wykonując wywołania API [28][29].

C. JSECOIN

Jsecoin to usługa służąca do wydobywania kryptowalut za pośrednictwem przeglądarki internetowej. Osiąga się to poprzez wstrzyknięcie kodu napisanego w JavaScript do docelowej strony internetowej, a wydobywaną walutą cyfrową jest znane ze swej anonimowości Monero. Jsecoin nie jest przełomowym oprogramowaniem, w zasadzie działania jest bardzo podobny do CoinHive Cryptojacker. Oprogramowanie zostało pierwotnie wstrzyknięte do stron internetowych popularnych w Stanach Zjednoczonych, Indiach, Kanadzie i Nigerii, obecnie występuje powszechnie na całym świecie [30].

D. *Kryptowaluta dla cryptojackerów*

Unit 42, globalny zespół ds. analizy zagrożeń w Palo Alto Networks, który przeprowadził i opublikował badania w ramach większego „Raportu o zagrożeniach w chmurze", po raz pierwszy zaczął śledzić cryptojacking w 2018 roku. Autorzy twierdzą, że raport koncentruje się w szczególności na nielegalnym wydobywaniu kryptowaluty Monero (XMR), biorąc pod uwagę jej popularność wśród hakerów. Badania prowadzono od września 2020 do lutego 2021. XMR od lat jest jednym z najpopularniejszych tokenów do wydobywania w chmurze, Unit 42 przyjrzał się również połączeniom sieciowym dla ETH, BTC, LTC i DASH. W każdym przypadku połączenia wydobywcze XMR znacznie przewyższały inne operacje kopania walut cyfrowych [27][31].

Monero to kryptowaluta, którą zaprojektowano w celu zapewnienia pełnej anonimowości transakcji dokonywanych z jej udziałem. Zapewniają to techniki sygnatur pierścieniowych i ukrytych adresów. Nie ma możliwości wyśledzenia historii konkretnego tokena, dlatego cyberprzestępcy tak chętnie z niej korzystają, a XMR uważane jest za najbardziej anonimową kryptowalutę na rynku. Dodatkowo jest to pierwsza waluta cyfrowa, w której wdrożono technologię „bulletproofs", pozwalającą na poprawę wydajność transakcji [27].

V. OPROGRAMOWANIE ANTYWIRUSOWE

Poniżej przedstawiono zastosowania technologii Blockhain w sektorze cyberbezpieczeństwa:

- *MythX* to usługa analizy bezpieczeństwa, która potrafi znajdować luki w zabezpieczeniach w kodzie inteligentnych kontraktów Solidity podczas cyklu życia oprogramowania.
- *Harvey* – system oparty o algorytm *greybox fuzzing* do inteligentnych kontraktów Ethereum. Integruje różne innowacyjne techniki w celu szybszego i bardziej niezawodnego wyszukiwania błędów.
- *Legions* – zestaw narzędzi dla testerów bezpieczeństwa wyszukujących luk w węzłach i kontraktach Ethereum, posiada przyjazny interfejs wiersza poleceń, z poleceniami autouzupełniania i historią.
- *Karl* – monitor inteligentnych kontraktów, który sprawdza luki w zabezpieczeniach za pomocą silnika wykrywania *Mythril*. Może być używany do monitorowania w czasie rzeczywistym łańcucha bloków Ethereum pod kątem nowo wdrożonych podatnych na ataki inteligentnych kontraktów [32].

PODSUMOWANIE I WNIOSKI

Pomimo bogatej i dostępnej literatury oraz stale rozwijającej się technologii w zakresie cyberbezpieczeństwa należy zwrócić uwagę na fakt, że od 2017 roku cryptojacking wciąż się rozwija. W wielu badaniach w literaturze zaproponowano metody wykrywania złośliwego oprogramowania tego typu przy użyciu różnych systemów antywirusowych, jednakże autor nie dostrzega jednoznacznego kierunku rozwoju. Niemniej jednak ciągły rozwój tego typu ataku wskazuje, że technologia Blockchain coraz częściej jest wykorzystywana przez hakerów.

Poziom skomplikowania ochrony przed atakami typu cryptojacking wynika z trudności zidentyfikowania infekcji, dlatego trzeba być świadomym zagrożenia i starać się podejmować działania zapobiegawcze. Aktualne wtyczki w przeglądarce, rozważne przeglądanie Internetu, czy odpowiednie zabezpieczenie chmury to podstawa skutecznej ochrony. Ponieważ zagrożenia stale się zmieniają, ochrona przed najnowszymi atakami, takimi jak cryptojacking jest bardzo pracochłonna, dlatego warto regularnie aktualizować swoją wiedzę na temat trendów wśród cyberprzestępców.

BIBLIOGRAFIA

[1] Web 3.0 vs Web 2.0: w czym tkwi różnica? (2022, August 17). BeInCrypto Polska. https://pl.beincrypto.com/learn/web-3-0-vs-web-2-0/

[2] O. Vorobyova, J. Polyakova, & O. Borzenkova, (2020, May). Leading Opportunities for Fighting Cyberterrorism Using Blockchain Technology. In 6th International Conference on Social, economic, and academic leadership (ICSEAL-6-2019) (pp. 523-528). Atlantis Press.

[3] L. Lantz, & D. Cawrey, (2020). Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications (1st ed.). O'Reilly Media.

[4] Czym jest Blockchain? (n.d.). Oracle Polska. https://www.oracle.com/pl/blockchain/what-is-blockchain/

[5] Kriptomat. (n.d.). Czym Jest Technologia Blockchain i Jak To Działa? [2022]. https://kriptomat.io/pl/blockchain/co-to-blockchain-technologia/

[6] The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007)

[7] N. Kshetri, (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications policy, 41(10), 1027-1038.

[8] S. Demirkan, I. Demirkan, & A. McKee, (2020). Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics, 7(2), 189-208.

[9] cryptomining.com.pl. (2021, June 4). Crypto Mining, kopalnie kryptowalut. Metody wydobywania PoW, PoS i Masternode ». CryptoMining.com.pl. https://www.cryptomining.com.pl/

[10] Cryptomining. (n.d.). https://www.ibm.com/docs/en/qradar-common?topic=extensions-cryptomining

[11] Ethereum. (n.d.). Wprowadzenie do zdecentralizowanych aplikacji. ethereum.org. https://ethereum.org/pl/developers/docs/dapps/

[12] What are smart contracts on blockchain? | IBM. (n.d.). https://www.ibm.com/topics/smart-contracts

[13] web3.js - Ethereum JavaScript API — web3.js 1.0.0 documentation. (n.d.). https://web3js.readthedocs.io/en/v1.8.1/

[14] J. Walewski, Blockchain Revolution: Estonia, pub. Helion, Warszawa 2018

[15] G. Anthes, (2015). Estonia: a model for e-government. Communications of the ACM, 58(6), 18-20.

[16] What is the Estonian X-Road all about? – how a digitalized nation is making life easier for citizens. – Thompson&Stein. (n.d.). https://www.thompsonstein.com/en/what-is-the-estonian-x-road-all-about-how-a-digitalized-nation-is-making-life-easier-for-citizens/

[17] Malwarebytes. (2019, January 7). Cryptojacking — co to jest i jak działa? https://pl.malwarebytes.com/cryptojacking/

[18] ENISA. (2020). Crypto-jacking. In Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). (Original work published 2019)

[19] E. A. Antonyan, N. A. Grishko, (2020, March). New Technologies in Cyber Terrorism Countering. In XVII International Research-to-Practice Conference dedicated to the memory of MI Kovalyov (ICK 2020) (pp. 28-31). Atlantis Press.

[20] J. Rauchberger, S. Schrittwieser, T. Dam, R. Luh, D. Buhov, G. Potzelsberger, & H. Kim, (2018, August). The other side of the coin: A framework for detecting and analyzing web-based cryptocurrency mining campaigns. In Proceedings of the 13th International Conference on Availability, Reliability and Security (pp. 1-10).

[21] N. Etemadi, Y. G. Borbon, & F. Strozzi, (2020). Blockchain technology for cybersecurity applications in the food supply chain: A systematic literature review. Proceedings of the XXIV Summer School "Francesco Turco"—Industrial Systems Engineering, Bergamo, Italy, 9-11.

[22] F. Dai, Y. Shi, N. Meng, L. Wei, & Z. Ye, (2017, November). From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues. In 2017 4th International Conference on Systems and Informatics (ICSAI) (pp. 975-979). IEEE.

[23] Check Point Software Technologies. (May 5, 2021). Most prevalent cryptomining malware worldwide in 2020, by type [Graph]. In Statista. Retrieved December 21, 2022, from http://www.statista.com/statistics/1238946/top-cryptomining-malware-worldwide/

[24] Xopero. (November 2, 2021). What cloud threats are you most concerned about? [Graph]. In Statista. Retrieved December 21, 2022, from https://www.statista.com/statistics/1273730/poland-cloud-threats-most-feared/

[25] ISC2. (May 27, 2022). What do you see as the biggest security threats in public clouds? [Graph]. In Statista. Retrieved December 21, 2022, from https://www.statista.com/statistics/1172307/biggest-security-threats-in-public-clouds/

[26] V. Khushali, (2020). A Review on Fileless Malware Analysis Techniques. vol, 9, 46-49.

[27] Y. Sovbetov, (2018). Factors influencing cryptocurrency prices: Evidence from bitcoin, ethereum, dash, litcoin, and monero. Journal of Economics and Financial Analysis, 2(2), 1-27.

[28] XMRig. (n.d.). https://xmrig.com/docs/miner

[29] Github, [2022]. https://github.com/xmrig/xmrig

[30] Jsecoin (2020, June). Remove Spyware & Malware with SpyHunter - EnigmaSoft Ltd. https://www.enigmasoftware.com/jsecoin-removal/

[31] H. Hasanova, U. J. Baek, M.G. Shin, K. Cho, & M. S. Kim, (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. International Journal of Network Management, 29(2), e2060.

[32] F. Naseem, A. Aris, L. Babun, E. Tekiner, & S. Uluagac, (2021, February). MINOS: A lightweight real-time cryptojacking detection system. In 28th Annual Network and Distributed System Security Symposium, NDSS.