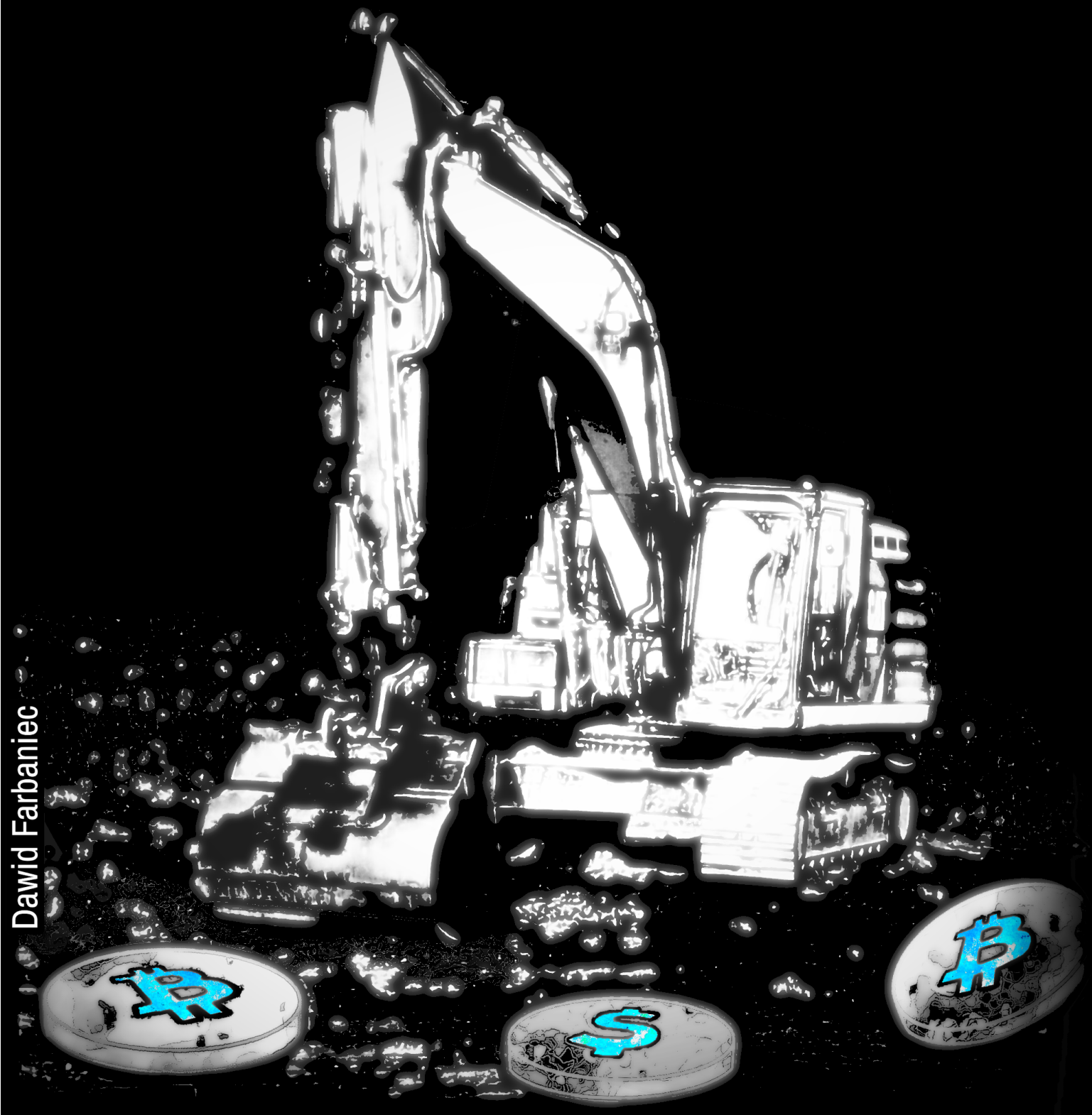
ethical.blue Magazine

Spreading knowledge like a virus.



Dawid Farbaniec

Volume 1e

Spis treści

LEGAL.NFO

Łańcuch bloków (ang. blockchain) i kryptowaluty dla początkujących

Autor tekstu: Dawid Farbaniec

Solidne podstawy działania łańcucha bloków i opartych na nim kryptowalut, takich jak Bitcoin i inne, mogą okazać się niezbędne w świecie przesiąkniętym coraz to nowszymi technologiami.

Symbol kryptowaluty Bitcoin

Znak reprezentujący kryptowalutę Bitcoin jest zawarty w standardzie Unicode. W kodowaniu UTF-16 o rozmiarze dwóch bajtów symbol kryptowaluty Bitcoin ma wartość 0x20BF (rysunek 1).

HTML `&#x20BF;`	UTF-16 `0x20BF`
C# Text `"\x20BF"`	UTF-32 `0x000020BF`

Rysunek 1. Symbol kryptowaluty Bitcoin (Unicode)

Trochę historii

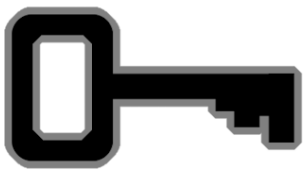
Wiele źródeł za początek technologii łańcucha bloków (ang. blockchain) uznaje 2008 rok. Okolice lat 2008/2009 to udostępnienie słynnego dokumentu https://bitcoin.org/bitcoin.pdf [dostęp: 2024-09-24 3:31]

Potwierdza to też przykładowe zapytanie do bazy danych WHOIS, ale należy zaznaczyć, że Bitcoin nie jest niczyją własnością. Identycznie stanowi witryna https://bitcoin.org, która jasno zaznacza, że mimo większego zaangażowania części osób, to Bitcoin jest wspólny i powszechny jak poczta internetowa (ang. e-mail).

```
C:\Sysinternals\whois.exe bitcoin.org
...
Creation Date:
2008-08-18T13:19:55Z
...
```

Podstawy kryptografii asymetrycznej

Algorytmy szyfrowania posiadające ten sam klucz zarówno do szyfrowania jak i deszyfrowania nazywane są symetrycznymi. Natomiast kryptografia asymetryczna nazywana też kryptografią z kluczem publicznym stosuje dwa rodzaje kluczy: prywatny i publiczny. Najczęstsze zastosowanie to szyfrowanie wiadomości kluczem publicznym przez nadawcę i deszyfrowanie kluczem prywatnym przez odbiorcę. A w przypadku podpisów: podpisywanie kluczem prywatnym (przez autora), a weryfikacja poprawności podpisu kluczem publicznym (przez każdego).



Problem generałów bizantyjskich

Działanie systemu rozproszonego można porównać do pola bitwy. Generałowie wydają rozkazy za pomocą posłańców. Możliwa jest jedna z dwóch decyzji: atak lub odwrót. Jeśli generał dokonuje zdrady, to wydaje fałszywe rozkazy. Natomiast posłańcy mogą zaginąć lub dotrzeć z rozkazem z opóźnieniem. Sytuacja ta nazywana jest problemem generałów bizantyjskich i dotyczy systemów rozproszonych, które muszą stosować różne algorytmy i poziom tolerancji błędu, aby decyzja o przyjęciu nowego bloku do łańcucha (lub odrzuceniu) była słuszna.

Funkcje skrótu (ang. hash)

Podstawowym zastosowaniem funkcji skrótu (ang. hash) jest ochrona integralności bloku bez potrzeby ujawniania przechowywanych danych. Przykład: Obliczenie funkcji skrótu, zmiana chociaż jednego bajta w danych, ponownie obliczenie funkcji skrótu i jej wartość jest całkiem inna. Jeśli algorytm funkcji skrótu ma podatności związane z bezpieczeństwem, to mogą wystąpić kolizje, czyli taka sama wartość funkcji skrótu dla różnych danych.

Niektóre funkcje skrótu można łatwo obliczać np. za pomocą skryptów PowerShell (listing 1).

```
[System.Convert]::ToHexString([System.Security.Cryptography.HashAlgorithm]::Create('SHA512').ComputeHash([System.Text.Encoding]::Default.GetBytes("ethical.blue Magazine")));
```

Listing 1. Obliczenie funkcji skrótu SHA512 (PowerShell)

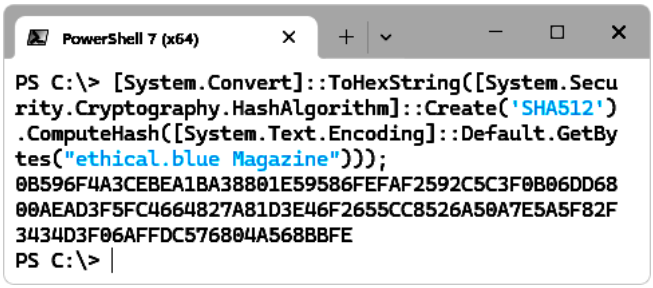
Funkcja skrótu o nazwie SHA512 z ciągu znaków **ethical.blue Magazine** jest następująca:

0B596F4A3CEBEA1BA38801E59586FEFAF2592C5C3F0B06DD6800AEAD3F5FC4664827A81D3E46F2655CC8526A50A7E5A5F82F3434D3F06AFFDC576804A568BBFE

Mała zmiana w ciągu znaków (wykrzyknik) **ethical.blue Magazine!** i funkcja skrótu o nazwie SHA512 zwraca inną wartość:

76C7A92068730D2C065A9C9DC168FE8B8EC2DA66B47ECD260FD66F05C156BD95C9DFC748BB8709F42451B7A062EE7506370E1634F5ADA3A00F52C917B487AEDE

Okno konsoli PowerShell z wklejonym skryptem obliczającym funkcję skrótu (ang. hash) SHA512 przedstawia rysunek 2.



Rysunek 2. Obliczenie funkcji skrótu SHA512 z ciągu znaków

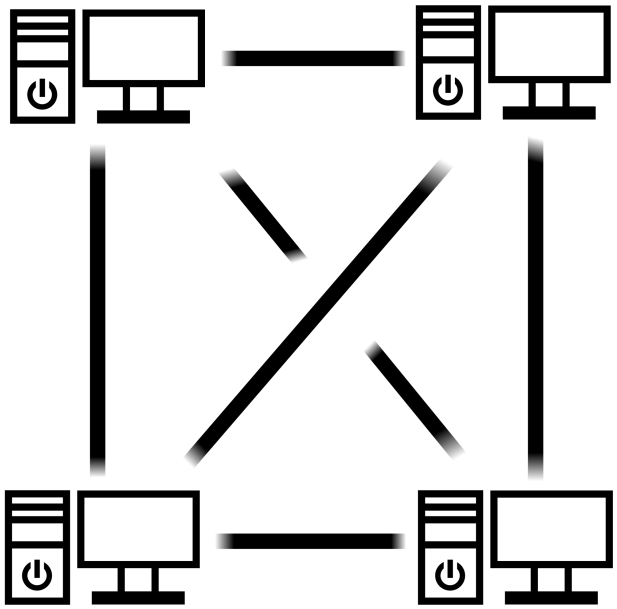
Zgubione monety (ang. lost coins)

Kryptowaluta też może zostać zgubiona. W przypadku utraty klucza prywatnego do portfela można powiedzieć, że monety te zapisane w łańcuchu bloków zostały zgubione. Brak do nich dostępu, czyli nie można ich przetransferować, więc tkwią w łańcuchu bloków jako praktycznie niczyje.

Sieci typu P2P

W architekturze nazywanej P2P urządzenia połączone w sieć mogą wymieniać informacje między sobą bez maszyny centralnej.

Połączenie tego rodzaju (rysunek 3) posiada wiele zastosowań, a można wymienić np. udostępnianie plików między użytkownikami komputerów bez pośredniczącego serwera internetowego.



Rysunek 3. Schemat ogólny sieci typu P2P

Z powodu decentralizacji, czyli braku głównej maszyny pośredniczącej architektura P2P stała się rdzeniem dla technologii łańcucha bloków oraz kryptowalut.

Nie należy błędnie rozumieć, że jeśli maszyny nawiązują połączenia między sobą, to od razu posiadają takie same uprawnienia. Dane wprowadzane przez nowe węzły są odpowiednio weryfikowane przez pozostałe.

Kolejną cechą charakterystyczną jest utrudnienie w fałszowaniu transakcji, ponieważ dane są rozproszone. Urządzenia połączone między sobą przechowują własne kopie bazy danych, a zmiany są weryfikowane i akceptowane dopiero wtedy, gdy nastąpi **zgodność (ang. consensus)**. Wykonywane jest to według ustalonego algorytmu.

Podstawowymi zaletami zdecentralizowanej architektury jest odporność na ataki typu odmowa usługi (ang. Denial of Service) oraz lepsza ochrona integralności danych.

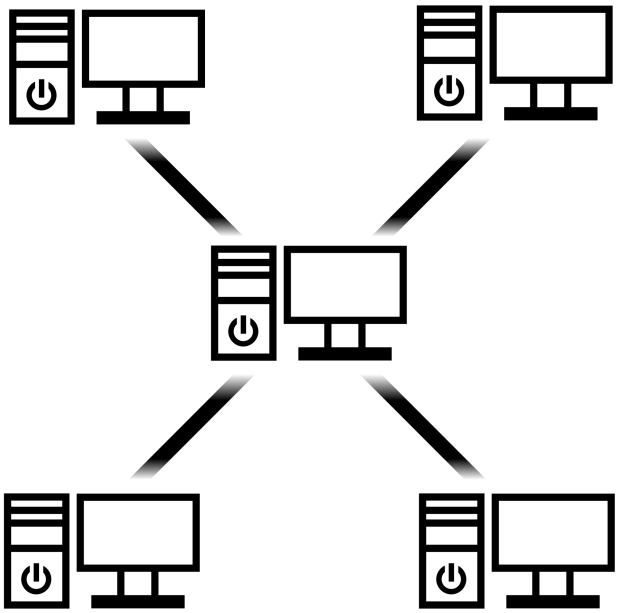
Natomiast zagrożenia to np. przejęcie przez określony podmiot większości węzłów w celu podmiany łańcucha bloków.

Ważną uwagą jest też, że sieci oparte o architekturę P2P są w pewien sposób kontrolowane przez określoną jednostkę. Jest to np. twórca oprogramowania z którego korzystają węzły.

Nawet sieci komputerów zombie połączone w botnet nie są przeważnie pozostawiane same sobie i posiadają np. wyłączniki awaryjne i inne funkcje.

Sieci z urządzeniem centralnym

W sieciach opartych na architekturze z urządzeniem centralnym, to właśnie maszyna nazywana serwerem internetowym udostępnia podłączającym się urządzeniom różne usługi (rysunek 4).



Rysunek 4. Schemat ogólny sieci z urządzeniem centralnym

Łańcuch bloków (ang. blockchain)

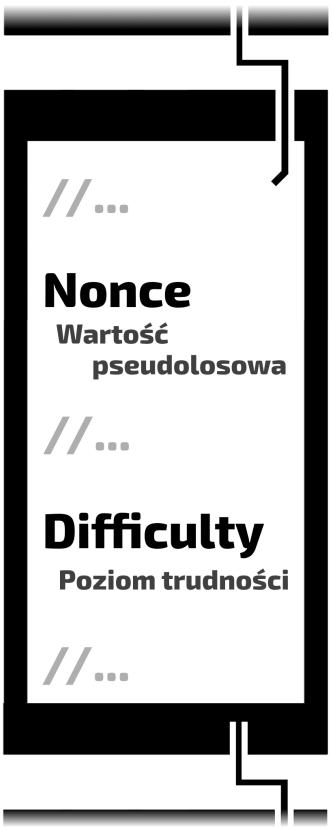
W celu zrozumienia tematu kryptowalut i łańcucha bloków bardzo ważne jest, aby umieć rozróżnić poszczególne pojęcia.

Łańcuch bloków (rysunek 5) to technologia, rozproszona baza danych w której poszczególne bloki są ze sobą połączone i zależne od poprzednich. W prostych słowach: to tylko zdefiniowany mechanizm działania. Nie każdy łańcuch bloków to rozległa na cały świat sieć. Można go utworzyć prywatnie w swojej infrastrukturze, a nawet prowadzić w arkuszu kalkulacyjnym, gdzie blokami są poszczególne komórki.

Rysunek 5. Łańcuch bloków (ang. blockchain)

Teraz warto na chwilę wrócić do definicji funkcji skrótu, czyli: przy zastosowaniu bezpiecznego algorytmu, nawet zmiana tylko jednego bajtu spowoduje całkowicie inną wartość funkcji skrótu. Jeśli podmiot zagrażający (ang. threat actor) zmodyfikuje coś w jednym z bloków, to będzie musiał obliczyć nowe wartości funkcji skrótu dla całego łańcucha. Chwila, ale przecież obliczenie np. SHA512 przez maszyny z trzeciej dekady XXI wieku to raczej żaden problem.

Dlatego są potrzebne kolejne współczynniki, które przedstawiono na rysunku 6.



Rysunek 6. Podstawowe współczynniki bloku

Blok zerowy (ang. genesis block)

Bloki w łańcuchu są połączone ze sobą i zależne od poprzedników. Zabezpieczenia kryptograficzne i połączenie bloków w ten sposób powodują, że nie można sobie dowolnie modyfikować łańcucha bloków. Istnieje jednak blok nazywany blokiem zerowym i jest to wpis w łańcuchu bloków, który nie ma poprzednika. Z tego też powodu określany jest angielskim słowem genesis, czyli ten od którego wszystko się zaczęło.

Wydobywanie kryptowaluty (kopanie)

Kopanie (ang. mining) czy wydobywanie to próby dopasowania nieznanej wartości pseudolosowej tak, aby wartość funkcji skrótu (ang. hash) była zgodna (rysunek 7).

Mechanizm tego typu powoduje, że do zaakceptowania nowych bloków potrzebny jest **dowód pracy (ang. proof of work)**. Dodatkowo możliwość ustalania poziomu trudności określa ilość zasobów czy mocy obliczeniowej potrzebnej do operacji na łańcuchu bloków.

Rysunek 7. Kopanie kryptowaluty (ang. crypto mining)

Istnieje możliwość zaimplementowania też innych warunków potrzebnych do spełnienia, aby węzeł mógł wykonywać operacje na łańcuchu bloków, takich jak np. **dowód wkładu (ang. proof of stake)** czy **dowód zniszczenia części waluty (ang. proof of burn)**.

Dowód wkładu

Innym od dowodu pracy (ang. proof of work) wymaganiem może być dowód wkładu (ang. proof of stake). Oznacza to, że operacje na łańcuchu bloków mogą wykonywać węzły, które posiadają określoną liczbę danej kryptowaluty.

Dowód zniszczenia części waluty

Trochę podobnym wymaganiem do dowodu wkładu (ang. proof of stake) może być warunek wejścia w posiadanie, a następnie zniszczenia części kryptowaluty (ang. proof of burn), co może spowodować deflację, czyli większą wartość wirtualnych monet dla tych co je posiadają.

Waluty alternatywne

Kryptowalutami alternatywnymi (ang. altcoin) nazywane są te, które powstały po Bitcoin'ie (BTC) czyli np. Ethereum (ETH) czy Tether (USDT).

Stworzenie własnej kryptowaluty

W miarę bezpieczna, dobrze zaplanowana i dostępna ogólnie własna kryptowaluta to ogromny nakład pracy. Dlatego warto się zastanowić czy nie lepiej utworzyć własny token, czyli za podstawę wziąć istniejący już łańcuch bloków.

Kryptowaluta ustabilizowana

Różne kryptowaluty określane po angielsku jako stablecoin są w pewnym sensie zabezpieczone przed utratą wartości i niestabilnością. Na przykład USDT ma odwzorowywać wartość dolara. Często do waluty typu stablecoin zamienia się monety po wykonanej operacji handlu, aby zatrzymać osiągniętą wartość.

Niewymienialne tokeny

Tokeny określane skrótem NFT (ang. non-fungible) to cyfrowe aktywa zapisane w łańcuchu bloków. Taki token jest odwrotnością np. gotówki. Przykład: Banknot może być zamieniony na banknoty o innych nominałach, które razem dają taką samą wartość pieniądza. Dodatkowo banknot dzisiaj jest Twój, a za chwilę kogoś innego. Natomiast token typu NFT przy tworzeniu jest zapisywany w łańcuchu bloków, czyli kolejny utworzony token nie będzie taki sam. Dodatkowo np. zmiana właściciela takiego tokenu to nie utworzenie dla niego identycznej kopii tylko transfer do innego podmiotu z zachowaniem historii kto utworzył token i kogo był wcześniej własnością.

Portfel sprzętowy

Po zakupie kryptowaluty może pojawić się problem czym jest klucz prywatny i publiczny.

Pojęcia te pochodzą z kryptografii. Klucza publicznego nie trzeba specjalnie chronić. Służy identyfikacji w łańcuchu bloków, jest takim jakby adresem czy numerem konta.

Natomiast klucz prywatny należy bezwzględnie chronić i go nie ujawniać. Jeśli ktoś mówi, że posiada kryptowalutę pod określonym adresem portfela, to znaczy, że posiada klucz prywatny.

Portfel z kryptowalutą może być przechowywany online (ang. hot wallet) lub poza internetem np. na papierze czy w urządzeniu nazywanym portfelem sprzętowym (ang. cold wallet).

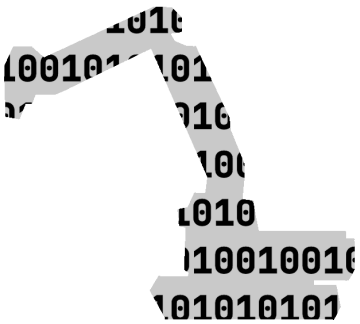
Kopalnie

Wzrost poziomu trudności wydobywania kryptowaluty powoduje, że indywidualne próby stają się nieskuteczne. Istnieją jednak tak zwane kopalnie (ang. pools), które pozwalają wspólnie wspierać sieć i dzielą między uczestników (nazywanych górnikami czy kopaczami) otrzymane nagrody za zweryfikowane transakcje.

Złośliwe koparki

Podmioty zagrażające (ang. threat actor) mogą instalować złośliwe implanty, których zadaniem jest wydobywanie kryptowaluty za pomocą nieswojej mocy obliczeniowej.

Zagrożenia tego rodzaju mogą wystąpić na zainfekowanych witrynach internetowych w formie skryptów oraz na komputerach czy urządzeniach przenośnych. Istnieje także możliwość stworzenia implantu sprzętowego kradnącego w ten sposób energię.

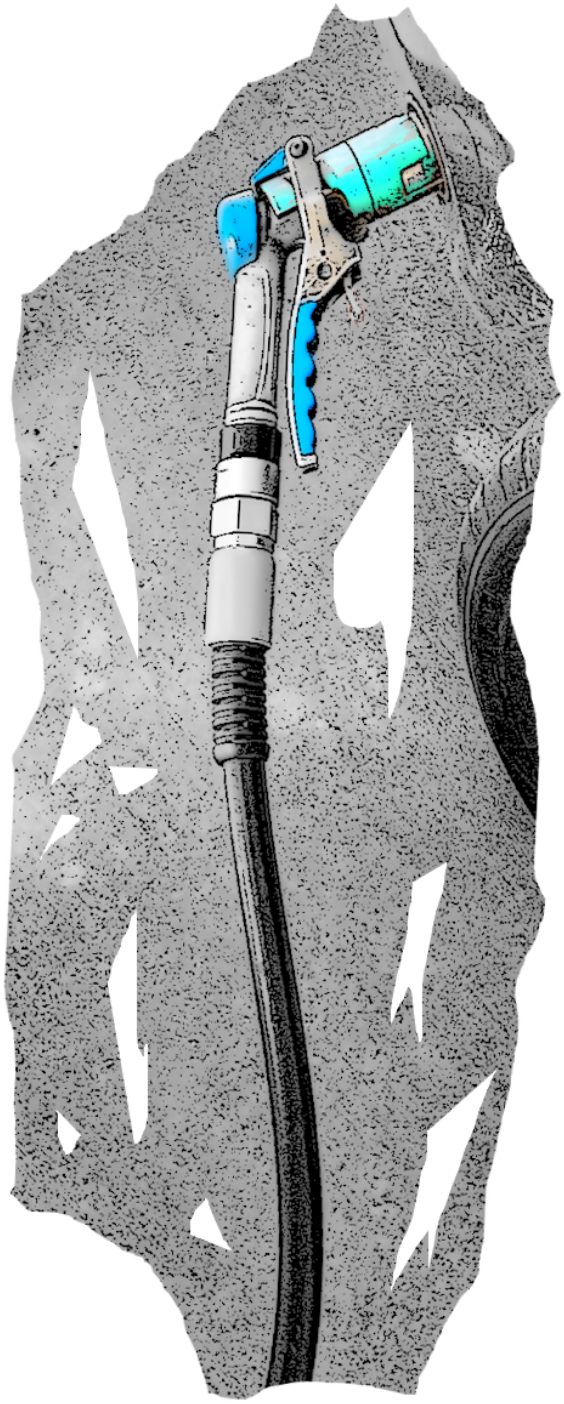


Pralnie (ang. mixer) i problemy prawne

Należy zachować ostrożność przy kupowaniu kryptowaluty poza znanymi giełdami z weryfikacją użytkowników. Kryptowaluta zapewnia w pewien sposób anonimowość, ale transakcje są transparentne i do wglądu. Mimo stosowania pralni (ang. mixer) nie da się zamazać całkowicie historii transakcji. Dlatego należy uważać, aby nie wejść w posiadanie monet, które są zanieczyszczone (ang. tainted).

Opłata paliwowa (ang. gas price)

Przetworzenie i weryfikacja transakcji w łańcuchu bloków wymaga mocy obliczeniowej. Z tego powodu przyjęło się, aby ułamek kwoty przetwarzanej transakcji przeznaczyć na pokrycie kosztów operacji. W anglojęzycznej literaturze opłata ta jest określana terminem gas price (pol. opłata za paliwo).



Nastoletnie zafascynowanie kryptowalutami

Jeśli nie jesteś osobą pełnoletnią, a bardzo chcesz kolekcjonować wirtualne monety (tzw. kryptowaluty), to dla własnego bezpieczeństwa zapytaj rodziców o zgodę. Wybierzcie sprawdzoną giełdę z weryfikacją użytkowników. Kryptowaluty potrafią być bardzo niestabilne, dlatego dobrze jest kupić małą ilość i obserwować kurs (zmianę wartości). Kto wie, może ta mała ilość kupiona za zgodą rodziców będzie bardzo dużo warta, gdy będziesz osobą dorosłą. A jeśli będzie warta mniej, to kupując tylko trochę strata będzie niewielka.

Dorosły, który chce kupić kryptowaluty

Najlepiej kupować kryptowaluty na znanych giełdach z weryfikacją użytkowników. Na pewno nie pod wpływem emocji po obejrzeniu reklamy obiecującej szybkie pieniądze.

Warto przeczytać

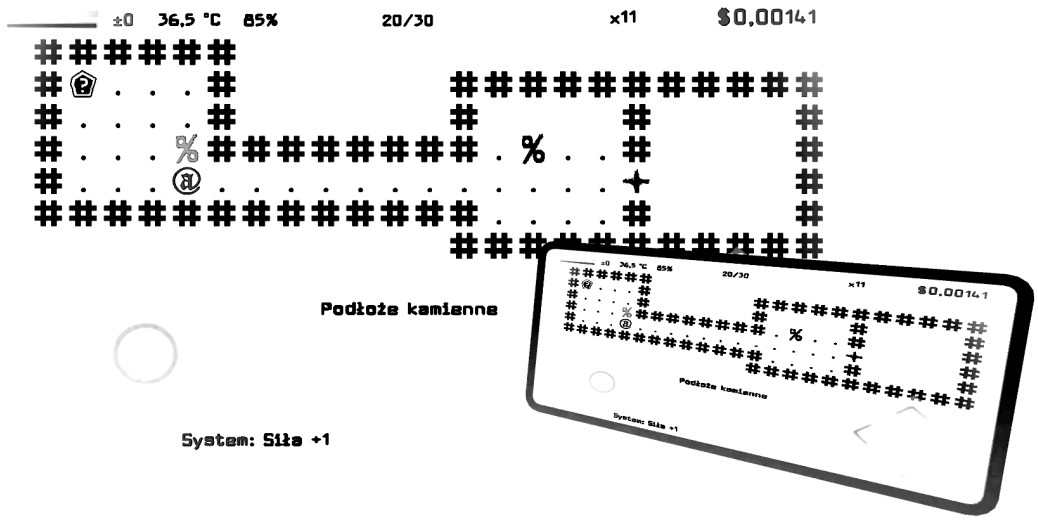
- https://academy.binance.com/en/articles [dostęp: 2024-10-22 13:54]
- https://bitcoin.org/bitcoin.pdf [dostęp: 2024-10-22 13:54]
- https://podatki.gov.pl/pit/rozliczenie-ze-sprzedazy-kryptowalut/ [dostęp: 2024-10-22 13:54]

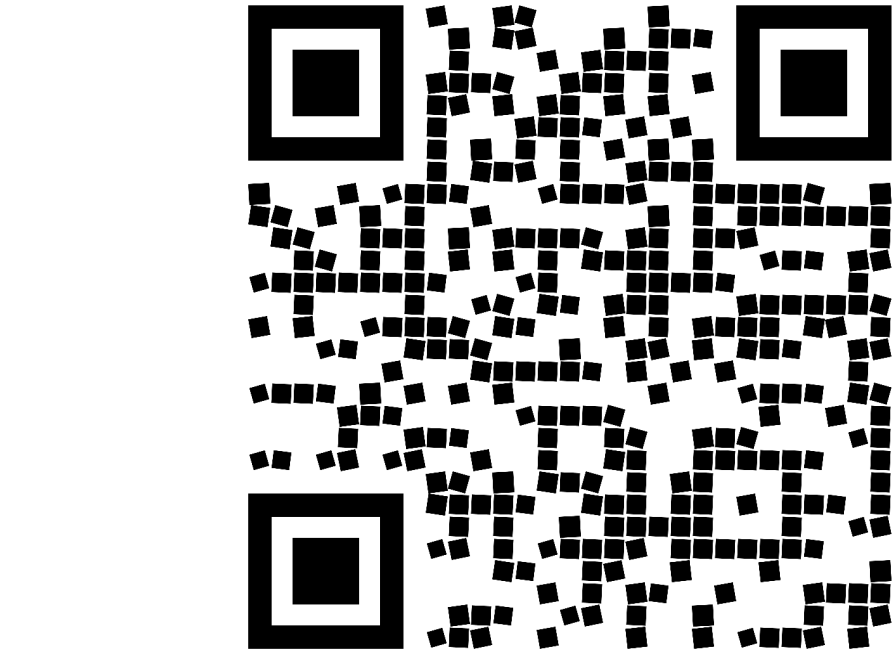
Extra

Raw.cs

Edukacyjny ładunek (ang. payload) w formie kodu maszynowego dla Windows x64.

```
byte[] raw = [
  0x55, 0x53, 0x57, 0x56, 0x54, 0x41, 0x54, 0x41, 0x55, 0x41, 0x56, 0x41,
  0x57, 0x65, 0x4C, 0x8B, 0x14, 0x25, 0x60, 0x00, 0x00, 0x00, 0x4D, 0x8B,
  0x52, 0x18, 0x4D, 0x8B, 0x5A, 0x20, 0x4D, 0x8B, 0x13, 0x4D, 0x8B, 0x1A,
  0x49, 0x8B, 0x5B, 0x20, 0x44, 0x8B, 0x4B, 0x3C, 0x4C, 0x03, 0xCB, 0x49,
  0x81, 0xC1, 0x88, 0x00, 0x00, 0x00, 0x45, 0x8B, 0x19, 0x4E, 0x8D, 0x04,
  0x1B, 0x41, 0x8B, 0x48, 0x18, 0x45, 0x8B, 0x60, 0x20, 0x4C, 0x03, 0xE3,
  0x4D, 0x8D, 0x14, 0x8C, 0x41, 0x8B, 0x3A, 0x48, 0x03, 0xFB, 0x48, 0x8D,
  0x35, 0xC9, 0x00, 0x00, 0x00, 0xA6, 0x75, 0x08, 0x8A, 0x06, 0x84, 0xC0,
  0x74, 0x05, 0xEB, 0xF5, 0xE2, 0xE2, 0xC3, 0x45, 0x8B, 0x50, 0x24, 0x4C,
  0x03, 0xD3, 0x66, 0x41, 0x8B, 0x0C, 0x4A, 0x45, 0x8B, 0x50, 0x1C, 0x4C,
  0x03, 0xD3, 0x41, 0x8B, 0x04, 0x8A, 0x48, 0x03, 0xC3, 0x4C, 0x8B, 0xF8,
  0x48, 0xC7, 0xC1, 0x61, 0x72, 0x79, 0x41, 0x51, 0x48, 0xB9, 0x4C, 0x6F,
  0x61, 0x64, 0x4C, 0x69, 0x62, 0x72, 0x51, 0x48, 0x8B, 0xD4, 0x48, 0x8B,
  0xCB, 0x48, 0x83, 0xEC, 0x30, 0xFF, 0xD0, 0x48, 0x83, 0xC4, 0x40, 0x48,
  0x8B, 0xF8, 0x48, 0xC7, 0xC1, 0x6C, 0x6C, 0x00, 0x00, 0x51, 0x48, 0xB9,
  0x75, 0x73, 0x65, 0x72, 0x33, 0x32, 0x2E, 0x64, 0x51, 0x48, 0x8B, 0xCC,
  0x48, 0x83, 0xEC, 0x30, 0xFF, 0xD7, 0x48, 0x83, 0xC4, 0x40, 0x4C, 0x8B,
  0xF0, 0x48, 0xC7, 0xC1, 0x6F, 0x78, 0x41, 0x00, 0x51, 0x48, 0xB9, 0x4D,
  0x65, 0x73, 0x73, 0x61, 0x67, 0x65, 0x42, 0x51, 0x48, 0x8B, 0xD4, 0x49,
  0x8B, 0xCE, 0x48, 0x83, 0xEC, 0x28, 0x41, 0xFF, 0xD7, 0x48, 0x83, 0xC4,
  0x38, 0x4C, 0x8B, 0xE8, 0x48, 0x83, 0xEC, 0x30, 0x4D, 0x33, 0xC9, 0x4C,
  0x8D, 0x05, 0x2F, 0x00, 0x00, 0x00, 0x48, 0x8D, 0x15, 0x28, 0x00, 0x00,
  0x00, 0x48, 0x33, 0xC9, 0x41, 0xFF, 0xD5, 0x48, 0x83, 0xC4, 0x30, 0x41,
  0x5F, 0x41, 0x5E, 0x41, 0x5D, 0x41, 0x5C, 0x5C, 0x5E, 0x5F, 0x5B, 0x5D,
  0xEB, 0x25, 0x47, 0x65, 0x74, 0x50, 0x72, 0x6F, 0x63, 0x41, 0x64, 0x64,
  0x72, 0x65, 0x73, 0x73, 0x00, 0x65, 0x74, 0x68, 0x69, 0x63, 0x61, 0x6C,
  0x2E, 0x62, 0x6C, 0x75, 0x65, 0x20, 0x4D, 0x61, 0x67, 0x61, 0x7A, 0x69,
  0x6E, 0x65, 0x00, 0xC3
];
```





Dawid Farbaniec

ethical.blue Magazine Volume 1e | Dawid Farbaniec | ISBN: 978-83-962697-2-0