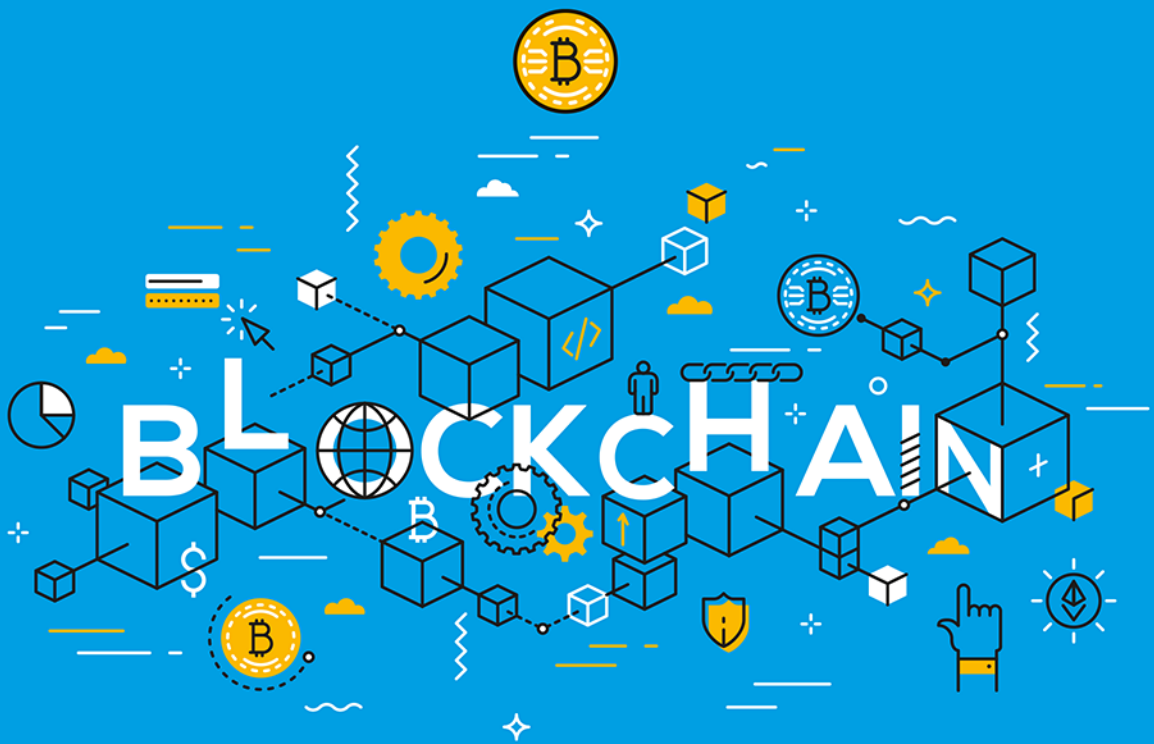
Mateusz Mach

ŚWIAT KRYPTOMILIONERÓW

Znajdź swoją szansę w świecie BLOCKCHAINA



onepress
EXCLUSIVE

Redaktor prowadzący: Barbara Gancarz-Wójcicka
Projekt okładki: Jan Paluch

Materiały graficzne na okładce zostały wykorzystane za zgodą Shutterstock.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *onepress@onepress.pl*
WWW: *http://onepress.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://onepress.pl/user/opinie?swikry
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-8776-8

Printed in Poland.

Spis treści

Rozdział 4.

Gorączka Bitcoina, czyli cyfrowe eldorado

4.1. MILIONOWY BIZNES Z CIEKAWOSTKI PROGRAMISTYCZNEJ

Społeczność Bitcoina wywodziła się z ruchu Cypherpunk. Zrzeszał on setki osób, które pracowały zupełnie dla idei. Chodziło o to, aby wykorzystać osiągnięcia techniki do szerzenia wolnościowej wizji społeczeństwa, niezależności jednostki, anonimowości i równego dostępu do usług cyfrowych. Cypherpunkom zależało, żeby być tak samo daleko od rządów, jak i korporacji. To wszystko w sferze ideałów; skąd jednak brać pieniądze na swoją działalność? Gdy więc pojawił się Bitcoin i przestał być jedynie ciekawostką technologiczną, pierwszymi, którzy cieszyli się z sukcesów i majątku zbudowanego na usługach blockchainowych, były osoby z niekwestionowanym zmysłem biznesowym.

Pierwsze kwartały działalności Bitcoina potwierdzają tę zależność, którą opisuję. Wokół liderów środowiska deweloperskiego w Bitcoinie ludzie zmieniali się według następującego schematu. Zaczynało się od niepraktycznych nerdów. Aktywiści tacy jak Wei Dai, którzy podobno jako pierwsi korespondowali z Satoshim Nakamoto, żyli zupełnie w swoim świecie. Byli odklejeni od rzeczywistości; na forach internetowych pisali o swojej „fascynacji technologiczną kryptoanarchią”[1]. Zupełnie nierozumiani przez mainstreamowe otoczenie, ograniczali swoją działalność do najbardziej niszowych list mailingowych, na których wzajemnie przesyłali sobie newslettery i artykuły. Pewnie dla samych siebie byli cyfrową kontrkulturą, ale dla reszty społeczeństwa — dziwakami. Potem przyszedł czas na takich ludzi jak Gavin Andresen. Ze względu na doświadczenie

[1] *https://news.bitcoin.com/satoshi-revolution-chapter-2-satoshi-libertarian-anarchist-part-4/*

w pracy w sektorze IT nadal mieli w sobie rys programisty introwertyka, ale o wiele większe obycie w środowisku biznesowym. Andresen pracował w Dolinie Krzemowej, zarządzał projektami, prowadził start-upy. Jeszcze wyżej w hierarchii obycia był Mike Hearn, przystojny, dobrze zbudowany, z dobrą umiejętnością prezentacji, były pracownik oddziału Google w Zurychu. Zostawił prestiżową karierę, by pracować dla niszowej technologii bez jakiegokolwiek zastosowania biznesowego; na początku robił to w ramach wolontariatu. Dużo zaryzykował, ale poniósł porażkę. Nie udało mu się zrealizować swojej wizji poprawy mechanizmu Bitcoina i jego globalnej promocji.

W tej całej dynamice zdarzeń, wreszcie pojawił się Craig Wright — albo oszust, albo geniusz. Można zarzucić mu bardzo wiele, ale należy przyznać, że ma talent biznesowy. Wbrew (a może dzięki) zamieszaniu wokół jego osoby był w stanie zbudować imperium technologiczne i finansowe. A z drugiej strony najnowsze doniesienia i procesy sądowe sugerują, że historia Craiga jest jeszcze bardziej skomplikowana i fascynująca, niż mogliśmy początkowo myśleć. Sam Craig Wright — mimo miliardowych pozwów, w których musi się bronić — jest stroną oskarżającą głównych deweloperów Bitcoina o zawłaszczenie jego praw intelektualnych do pomysłu na Bitcoina. Swoje straty, sformułowane w pozwie z maja 2021 r., wycenia na 5,7 miliarda dolarów[2]. Ma częściowe szanse na wygraną, bo — wbrew równoległym wyrokom z innych krajów — sąd w Wielkiej Brytanii przyznał, że do Wrighta należą prawa autorskie do white papera Bitcoina, opublikowanego pod pseudonimem Satoshi Nakamoto[3]. Obok tego faktu łatwo przejść obojętnie, bo w sprawie nie zasądzono żadnej rekompensaty finansowej (poza pokryciem kosztów sądowych). Jednak spójrzcie: poważny sąd w rozwiniętym kraju z wielkimi tradycjami prawniczymi poświadczył, kto jest autorem najważniejszej publikacji w środowisku Blockchaina, która rozpoczęła historię kryptowalut — sektora wycenianego na 2 biliony dolarów („dwójka" z 12 zerami), czyli ⅒ wielkości amerykańskiej gospodarki. Przyznanie Wrightowi praw autorskich do white papera Bitcoina może być przełomem w sprawie ustalenia tożsamości Nakamoto (lub w uwierzeniu w nią).

Zatem kto ma tu rację? Nie wiadomo. Można jednak odnieść silne wrażenie, że konflikty powstałe na samym początku w środowisku pierwszych „bitcoinowców" ciągną się za nimi do dzisiaj. Tajemnice, które sięgają korzeni Bitcoina w 2009 r., od ponad 12 lat czekają na rozwiązanie. Po latach eksperymentów osobowych

[2] *https://www.reuters.com/article/us-britain-bitcoin-lawsuit-idCAKBN2CT1VZ.*

[3] Sprawa ta dotyczyła postępowania przed Sądem Najwyższym w Londynie, w którym operator strony Bitcoin.org, występujący pod pseudonimem Cobra, został zmuszony do zaprzestania hostingu white papera Bitcoina — *https://www.coindesk.com/markets/2021/06/29/uk-court-orders-bitcoinorg-to-remove-white-paper-following-craig-wright-lawsuit/*

i skandali w raczkującym ekosystemie kryptowalut przyszła wreszcie pora na doświadczonych menedżerów i przedsiębiorców; osoby, które zarówno miały wiedzę teoretyczną, jak i spędziły lata w biznesie. Zamiast jednak polegać na skonfliktowanym środowisku aktywistów i programistów Bitcoina, kreatywni przedsiębiorcy i użytkownicy Internetu sami zaczęli organizować własne przedsięwzięcia. W większości opierały się one na Blockchainie i ułatwiały posługiwanie się portfelami kryptowalutowymi, ale nie uczestniczyły bezpośrednio w projekcie Bitcoina. Korzystały z jego atutów, bez angażowania się w rozwiązywanie wrodzonych (i pewnie nieuleczalnych) wad środowiska pierwszych deweloperów kryptowalut.

4.1.1. Cyfrowi górnicy

Z czasów wielkich odkryć geograficznych i podróży do dopiero co odkrytej Ameryki najbardziej podoba mi się historia El Dorado. W XVI w. to słowo rozpalało wyobraźnię hiszpańskich podróżników, którzy podejmowali ogromne ryzyko, płynąc w poszukiwaniu bogactwa ku terenom dzisiejszej Kolumbii. Za sprawą odkrycia Ameryki do Europy zaczęły napływać nie tylko potwierdzone informacje o nieznanych wcześniej kulturach, ale również niesprawdzone legendy. Wśród nich była opowieść o majątku indiańskich plemion, które miały budować złote posągi swoich bożków — po hiszpańsku *El Hombre Dorado*, czyli „człowiek ze złota"[4]. Stąd wzięło się określenie *eldorado* — kraina złota.

W znacznej mierze legendy o bogactwie Indian okazały się nieprawdziwe. To jednak nie zmieniało faktu, że marzenia o złocie i majątku nadal musiały jakoś się urzeczywistnić. Pragnienie posiadania jest głęboko wpisane w ludzką psychikę, dlatego niezależnie od czasów i okoliczności ludzie przez wieki nie przestawali szukać swojej szansy na wzbogacenie się. Po poszukiwaniach eldorado powstało nowe określenie: gorączka złota. W połowie XIX w. było to dążenie do osiedlania się w niezamieszkałych wcześniej miejscach, głównie na Zachodnim Wybrzeżu USA. Puste prerie i regiony bez dostępu do infrastruktury przyciągały ludzi, którzy liczyli na możliwość wydobywania złota i innych rzadkich metali. Przecież o to chodzi w tzw. kalifornijskim śnie; była to nadzieja, że każdy mógł niemal natychmiast stać się bardzo bogaty[5].

Nawiązanie do górnictwa i marzenia o powszechnym bogactwie wróciły 150 lat później, podczas narodzin kryptowalut. Satoshi Nakamoto zaprojektował system, w którym wydobywanie bitcoinów (*mining*) to podstawowy proces niezbędny

[4] J. Ocampo López (2007), *Grandes culturas indígenas de América*, Plaza & Janes Editores Colombia S.A.

[5] K. Starr (1985), *Inventing the Dream*, Oxford University Press.

do tego, aby nowe jednostki BTC mogły zostać wprowadzane do obiegu. Jednocześnie mining pozwala na potwierdzenie transakcji i dodanie ich do rejestru Blockchaina. „Wydobywanie" odbywa się przy użyciu zaawansowanego sprzętu, który rozwiązuje niezwykle skomplikowany problem matematyczny — zagadkę kryptograficzną w ramach algorytmu *Proof-of-Work*. Pierwszy komputer, który znajdzie rozwiązanie problemu, otrzymuje kolejny blok bitcoinów i proces rozpoczyna się od nowa. Osoby, które wydobywają Bitcoina, nazywa się „minerami" (górnikami)[6].

4.2. JAK POWSTAJE CYFROWY PIENIĄDZ?

System potwierdzania transakcji w zamian za nagrodę w postaci bitcoinów przyznawanych minerom był zupełną rewolucją w świecie finansów. Dotychczasowe systemy pieniężne opierały się na banku centralnym, który reguluje produkcję nowego pieniądza. Mówiąc językiem ekonomicznym, ma monopol na emisję pieniądza — czyli nikt inny nie może drukować pieniędzy, tylko sam bank centralny, np. Narodowy Bank Polski albo, w USA, Rezerwa Federalna (w skrócie „Fed"). Aby utrzymać ten monopol i kontrolę władzy centralnej nad pieniądzem, policja i sądy ścigają oszustów podrabiających banknoty. Jest to ciężkie przestępstwo, regulowane przez Kodeks karny. Czasem oszustwa polegające na drukowaniu pieniędzy są karane surowiej niż kradzieże, gwałty, a nawet zabójstwa. W Polsce za podrabianie pieniędzy grozi od 5 do 25 lat więzienia, a za wprowadzanie ich do obiegu — do 10 lat[7]. Do więzienia można pójść nawet za przygotowywanie materiałów do drukowania pieniędzy, za co grozi od 3 miesięcy do 5 lat więzienia[8].

Można powiedzieć, że rząd wymusza na wszystkich używanie jednego, powszechnego systemu pieniężnego, ale z drugiej strony daje za to pewną „nagrodę". Chodzi o to, że przymuszenie wszystkich do korzystania z jednej waluty uruchamia następujący mechanizm. Otóż wszystkie podmioty w społeczeństwie „zgadzają się" co do dwóch kwestii. Po pierwsze, że kawałek papieru z napisem „100 dollars" i „Federal Reserve Note" jest cokolwiek wart. Po drugie, że jest on na tyle zrozumiały i powszechny, aby każdy znał jego znaczenie i wartość; by każdy mógł oszacować, co za ten 100-dolarowy banknot może kupić. Żeby zbudować zaufanie do tradycyjnej waluty, jej emitent, czyli bank centralny, używa

[6] *https://www.investopedia.com/terms/b/bitcoin-mining.asp*

[7] *https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-18/63904,Falszowanie-pieniedzy-i-papierow-wartosciowych-art-310.html*

[8] Ibid., art. 310 §4 k.k.

licznych zabiegów zabezpieczających pieniądz przed fałszerstwem albo zmianami. Z jednej strony grafika banknotów dolarowych nie zmieniła się od 1963 r. — prawie od 60 lat. Z drugiej — Rezerwa Federalna używa skomplikowanych zabiegów, aby zapewnić społeczeństwo, że posługuje się ono banknotami wyprodukowanymi przez jedynego uprawnionego, centralnego emitenta. W przypadku „papierowego" dolara banknoty produkuje się ze specjalnej mieszanki lnu i bawełny[9]. Używa się też tajnej kombinacji różnych atramentów, aby dolary miały zielony kolor — ze względów bezpieczeństwa skład tej mieszanki jest jedną z najściślej strzeżonych tajemnic USA. A dlaczego nikt tego autorytetu Stanów Zjednoczonych nie podważa? Bo są światowym mocarstwem, którego terytorium lądowe nie zostało zaatakowane przez jakąkolwiek armię od ponad 170 lat.

Nawet płatności cyfrowe są wspierane przez władze centralne. Przykładowo Mastercard czy Visa przetwarzają wszystkie transakcje, gdy dokonujecie zakupu online przy użyciu karty płatniczej albo płacicie kartą kredytową w sklepie. Oprócz rejestrowania historii transakcji firmy te sprawdzają, czy transakcje nie są fałszywe, co jest jednym z powodów, dla których Twoja karta debetowa lub kredytowa może zostać zawieszona podczas podróży. Cały ten system opiera się na zaufaniu do scentralizowanego systemu — od centralnie emitowanych pieniędzy (przez bank centralny) po globalne marki o wypracowanej nienagannej reputacji w sektorze technologii i finansów (czyli banki komercyjne i operatorów kart).

Dlaczego więc w świecie, który tak bardzo polega na zaufaniu, ktoś uznał, że stworzy anonimowy system transakcji, do którego wejść może każdy człowiek — bez względu na tożsamość, przeszłość prawną, wiek czy wiarygodność? Może się to wydawać paradoksalne, ale tak właśnie było. Satoshi Nakamoto stworzył kompletny i spójny system, który nie wymaga centralnej regulacji. Zamiast tego Bitcoin jest wspierany przez miliony komputerów na całym świecie zwanych węzłami (*nodes*). Ta sieć komputerów pełni tę samą funkcję co Rezerwa Federalna, Visa i Mastercard, ale z kilkoma kluczowymi różnicami.

W sieci Bitcoina węzły przechowują informacje o wcześniejszych transakcjach i pomagają zweryfikować ich autentyczność. Jednak w przeciwieństwie do tych władz centralnych, węzły Bitcoina są rozsiane po całym świecie i rejestrują dane transakcji na publicznej liście, do której każdy może uzyskać dostęp[10].

---

9 *https://bestlifeonline.com/20-crazy-af-facts-dollar-bills/*

10 *https://cryptonews.com/news/this-is-how-satoshi-nakamoto-defended-bitcoin-mining-convert-9640.htm*

W lipcu 2021 r. padł rekord w liczbie aktywnych węzłów sieci; było ich ponad 14 tysięcy — jako centrów zintegrowanych „koparek" i punktów dostępowych obsługujących sieć[11]. Logika kryptowalut działa więc w ten sposób, że zamiast ufać jednemu centralnemu podmiotowi, który wymusza zaufanie do siebie, lepiej jest polegać na setkach tysięcy użytkowników, którzy nie znają swojej tożsamości, ale dostają nagrodę w postaci ciągle umacniającego się Bitcoina. Anonimowi operatorzy sieci w tradycyjnej gospodarce pewnie nie mieliby do siebie zaufania, ale w tak dobrze zaprojektowanym systemie, jakim są kryptowaluty, utrzymują oni funkcjonowanie sieci przez dążenie do zysku. Udostępniają swoje komputery, lub nawet inwestują w specjalne maszyny obliczeniowe, bo na potwierdzaniu kolejnych transakcji zarabiają duże pieniądze. Tak zaprojektowanej sieci praktycznie nie da się zatrzymać ani wyłączyć — lub po prostu się to nie opłaca.

To właśnie było głównym założeniem modelu opracowanego przez Satoshiego Nakamoto: że wyłączenie sieci Bitcoina wymagałoby skoordynowanego ataku na przynajmniej 51% węzłów (*nodes*). Żeby przeprowadzić taką akcję, trzeba mieć do dyspozycji ogromną moc obliczeniową, którą bardziej opłacałoby się zaprząc do kopania BTC i zarabiania pieniędzy. To samo dotyczy prób zgadywania kluczy prywatnych, które są niezbędne do logowania się na portfel bitcoinowy przez użytkownika. Wiecie, ile jest możliwych kombinacji takich kluczy dostępowych, zgodnie z obecnie panującym standardem przydzielania? Dwa do potęgi sto sześćdziesiątej (2^{160}), czyli dokładnie:

1 461 501 637 330 902 918 203 684 832 716 283 019 655 932 542 976.

Na co dzień nie operujemy takimi wartościami, więc nawet nie ma sensu tego rozpisywać. Dla przykładu pomyślcie tylko, że na świecie istnieje ok. 2^{63} ziarenek piasku. Czyli o dobre 100 rzędów wielkości mniej, niż wynosi liczba dostępnych kombinacji bitcoinowych kluczy[12]. Porównajcie tylko długość zapisu obu tych liczb:

9 223 372 036 854 775 808.

O ile więc nie dojdzie do błędu zabezpieczeń i ataku na oprogramowanie portfela lub giełdy kryptowalut, Bitcoin oraz alternatywne opcje są raczej bezpiecznym systemem do monitorowania przepływów pieniądza.

[11] *https://cointelegraph.com/news/bitcoin-network-node-count-sets-new-all-time-high*

[12] *https://privacypros.io/btc-faq/how-many-btc-addresses*

Czy sprawiło to docenienie działania Bitcoina i chęć zarobku, czy wytworzony hype — dość szybko przybywało osób, które dołączały do tej blockchainowej gry. Każda kryptowaluta — a Bitcoin jako pierwszy przykład tej klasy narzędzi technologiczno-finansowych — to zupełnie nowy system ekonomiczny, nowa rzeczywistość, nowe relacje między nadawcą a odbiorcą środków. Wszystkie zagadnienia dotyczące rozwiązań ekonomicznych danej kryptowaluty określa się mianem *token economics* — czyli ekonomii tokenowej. W przypadku Bitcoina rozkład tokenów działa w ten sposób, że jego maksymalna wielkość zakodowana w systemie wynosi 21 milionów jednostek. Obecnie w obiegu znajduje się niecałe 19 milionów bitcoinów. Ludzie wiedzą, że czas ucieka, a w pewnym momencie najpopularniejsza kryptowaluta okaże się towarem luksusowym, którego już nie przybędzie. Wszystkim zależy więc na tym, żeby znaleźć swoją szansę i posiąść Bitcoina, póki jego cena nie jest aż tak wysoka. Każdego dnia dodaje się do sieci ok. 900 nowych bitcoinów[13], ale pewnego dnia wartość ta spadnie do zera. Póki to możliwe, każdy próbuje skorzystać z możliwości zarabiania na „produkcji" bitcoinów, choć szanse na to coraz szybciej maleją. Według obecnych szacunków ostatni bitcoin, czyli jednostka BTC o numerze 21 000 000, zostanie wydobyty w 2140 r.[14]

Powstanie sieci Bitcoina sprawiło, że narodziła się nowa szansa na zarabianie pieniędzy w roli górnika kryptowalut. Stawiając się w tej roli, wiele osób poczuło szanse na duży zarobek. W przeciwieństwie do pierwszych miesięcy działania Bitcoina, teraz zainteresowanie kryptowalutami jest o wiele większe niż faktyczna możliwość ich obsługi przez komputery aktywnych użytkowników. Liczba górników jest ograniczona, ponieważ ciągle rośnie zapotrzebowanie na moc obliczeniową komputerów i koparek do kryptowalut. Patrząc na dane z całego świata z 2020 r., samo utrzymanie mechanizmu Bitcoina i dodawanie nowych transakcji do sieci dały minerom przychód ponad 8 milionów dolarów... dziennie[15].

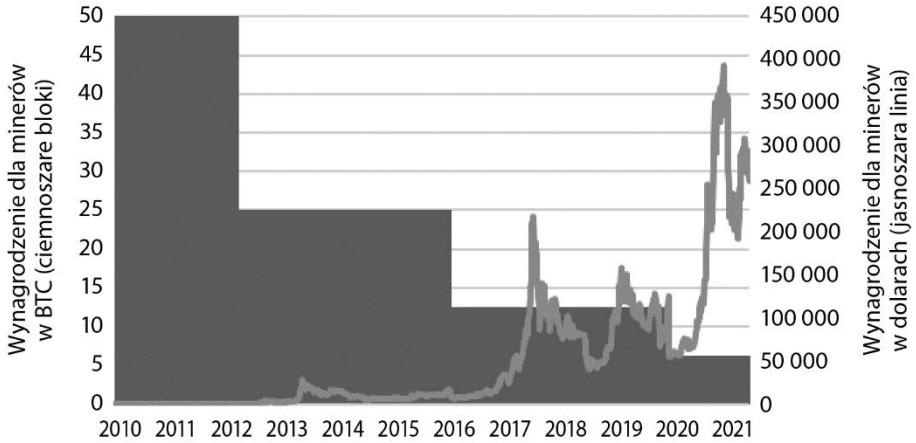
Aby dokładnie zrozumieć mechanizm wynagrodzenia, jaki otrzymują minerzy za utrzymywanie sieci, musimy wrócić do korzeni Bitcoina. Gdy Satoshi Nakamoto udostępniał pierwszą wersję oprogramowania do obsługi sieci BTC, każdy miner dostawał 50 jednostek kryptowaluty w zamian za udostępnienie swojego komputera do rozwiązania zagadki programistycznej i potwierdzenia zapisu o nowej transakcji. Takie potwierdzenie odbywa się w formie pakowania informacji o transakcjach w bloki (stąd nazwa *Blockchain* — łańcuch bloków).

[13] *https://www.buybitcoinworldwide.com/how-many-bitcoins-are-there/*

[14] *https://finance.yahoo.com/news/90-bitcoin-total-supply-mined-112422242.html*

[15] *https://www.buybitcoinworldwide.com/mining/profitability/*

Liczba nowych bitcoinów uwalnianych z każdym wydobytym blokiem jest nazywana nagrodą za blok. Nagroda za blok zmniejsza się o połowę co 210 tysięcy bloków (lub mniej więcej co 4 lata). W 2009 r. było to 50, potem 25, następnie 12,5, a w maju 2020 r. tę liczbę zmniejszono o połowę, do 6,25. Kolejny *halving* — czyli obcięcie wielkości nagrody o połowę — jest przewidziany na 2024 r. Halvingi zmniejszają tempo tworzenia nowych monet, a tym samym zmniejszają dostępną podaż. Skoro więc bitcoinów w sieci przybywa coraz wolniej, a zainteresowanie nimi rośnie, to na biznesie kopania wciąż można dużo zarobić. Widać to na wykresie pokazanym na **rysunku 4.1**; mimo że wynagrodzenie minerów maleje co 4 lata, to ostatecznie jego wartość w dolarach rośnie. Minerzy, którzy otrzymują kryptowalutę jako wynagrodzenie za swoją pracę, mogą ją sprzedać na giełdach kryptowalut i wymienić — albo na inne tokeny cyfrowe, albo na tradycyjną walutę — i w ten sposób zrealizować swój zysk.



Rysunek 4.1. Nagrody dla minerów za utrzymywanie sieci BTC

Aby potwierdzać nowe transakcje na Blockchainie, minerzy korzystają ze specjalnego sprzętu — koparek do kryptowalut. Ich schemat technologiczny przypomina karty graficzne (GPU), jednak moc obliczeniowa koparek przewyższa wszystko, o czym mógłby marzyć użytkownik nawet najlepszej jednostki GPU. Podczas gdy na początku Bitcoina kopać mógł każdy posiadacz zwykłego komputera, teraz jest to praktycznie niemożliwe. Zmieniło się to w 2013 r., gdy sieć Bitcoina była już na tyle duża, że wymagała wyspecjalizowanego sprzętu[16]. Do potwierdzania transakcji na Blockchainie potrzeba zapasu pamięci komputera na bardzo wymagające obliczenia. Jak bardzo jest to trudne? Na to pytanie odpowiada

[16] *https://spectrum.ieee.org/bitcoin-mining*

rachunek prawdopodobieństwa. Szansa, że sprzęt kopiący Bitcoina poprawnie rozwiąże zagadkę matematyczną w ramach systemu *Proof-of-Work* i zweryfikuje nową transakcję w sieci, wynoszą 1 do 16 bilionów (szesnaście z 12 zerami)[17]. Z tego powodu do obsługi sieci i zarabiania na samych operacjach kryptowalutowych zaczęto produkować specjalne urządzenia: koparki kryptowalut. Gigantem w produkcji takiego sprzętu jest Bitmain. Nawet 70% koparek używanych na świecie może pochodzić właśnie od tego chińskiego producenta[18].

4.3. HAŁAS, ZUŻYCIE PRĄDU I WŁASNY DOCHÓD PASYWNY

Obecnie koparki kryptowalut są drogimi narzędziami, których ceny wynoszą średnio 5 – 6 tysięcy dolarów, chociaż najlepszy sprzęt kosztuje nawet 10 tysięcy. W ostateczności można pokusić się o zakup najtańszych koparek, takich za kilkaset dolarów, ale ich parametry nie będą równie dobre. Koparki to wyspecjalizowane komputery, stworzone wyłącznie w celu wydobywania bitcoinów oraz pozostałych typów kryptowalut. Za wykonywanie skomplikowanych obliczeń do potwierdzenia bitcoinowych transakcji osoby wydobywające Bitcoina otrzymują nagrodę w postaci nowych bitcoinów; obecnie wynosi ona 6,25 BTC. System dystrybuuje taką „nagrodę" mniej więcej co 10 minut, aby zachęcić minerów do utrzymywania sieci oraz przetwarzania nowych transakcji.

Aby wydobyć nowe jednostki BTC, rzesza minerów rozproszona po całym świecie wykorzystuje swoją moc obliczeniową do uruchomienia algorytmu Bitcoina. Taki mechanizm łączy w sobie współpracę (utrzymanie globalnej sieci) oraz rywalizację. Minerzy konkurują ze sobą, aby zobaczyć, kto może jako pierwszy odblokować każdą partię nowych bitcoinów. Trwa więc obliczeniowy wyścig zbrojeń, w którym osoby i organizacje o największej mocy obliczeniowej (*hash rate*) będą w stanie wydobyć najwięcej bitcoinów. Nawet dziś w tym wyścigu wciąż jest miejsce na historie nowych kryptomilionerów.

Jeśli rozważacie kupno koparki, to musicie wziąć pod uwagę trzy podstawowe parametry, które określają przydatność koparek i ich sens inwestycyjny:

- ***Hash rate*** — To najważniejszy parametr, czyli moc obliczeniowa: ile hashów (paczek informacji o transakcjach) na sekundę może wykonać koparka bitcoinów? Hash rate pokazuje moc obliczeniową koparki w dodawaniu

[17] *Network Difficulty*, Blockchain.com, dostęp: 16 sierpnia 2020.

[18] *https://spectrum.ieee.org/bitcoin-mining*.

do sieci BTC nowych hashów. Im więcej mocy obliczeniowej ma koparka, tym więcej rozwiązań może znaleźć miner[19].

- ***Wydajność*** — Chodzi tu o to, ile energii elektrycznej zużywa koparka. Ponieważ minerzy zużywają duże ilości energii, najlepszy sprzęt to ten, który produkuje jak najwięcej bitcoinów przy jak najmniejszym zapotrzebowaniu na prąd[20]. Wydajność mierzy się stosunkiem hash rate'u do mocy koparki. Hash rate powinien być jak najwyższy przy możliwie małej liczbie watów (wat to jednostka mocy sprzętu elektrycznego).
- ***Cena*** — Ile kosztuje koparka bitcoinów? Tani sprzęt będzie wydobywał mniej bitcoinów, dlatego ważna jest wydajność i zużycie energii elektrycznej. Oczywiście najszybsze i najwydajniejsze koparki kosztują więcej, ale być może taka inwestycja się zwróci, bo jako miner otrzymacie więcej bitcoinów lub mniej zapłacicie w rachunkach za prąd[21].

Sugeruje się, żeby koparek nie wybierać tylko na podstawie ceny ani tylko wysokiego hash rate'u. Należy celować w wartość, czyli optymalizację wszystkich parametrów koparki. Jak ją zmierzyć? W Internecie dostępne są kalkulatory, które pozwalają oszacować wydajność i rentowność sprzętu. Trzeba jednak pamiętać, że ze względu na postęp techniczny na rynku pojawia się coraz więcej minerów z lepszymi i mocniejszymi koparkami. Przez to w szacunkach trzeba wziąć pod uwagę rosnącą konkurencję. Dobry kalkulator powinien zakładać dzienny wzrost hash rate'u w całej sieci o mniej więcej 0,5% — o tyle wzrastała ta wartość w pierwszej połowie 2021 r.

Biorąc pod uwagę te wszystkie czynniki, możemy pokusić się o pewne założenia i eksperymenty. Załóżmy, że chcecie zostać minerem Bitcoina. Wybieracie sprzęt ze średniej półki, przykładowo model Whatsminer M30S+. Jest on stosunkowo świeży, bo na rynek wszedł mniej więcej rok temu. Nowy kosztuje ok. 2,5 tysiąca dolarów, ale używany znajdziecie nawet za kilkaset[22]. Kupując konkretną koparkę, dwa parametry musicie założyć jako stałe: pobór energii oraz moc obliczeniową (hash rate). W przypadku omawianego Whatsminera te wartości wynoszą, odpowiednio, 3400 W oraz 100 Th/s[23]. Wreszcie, musicie sprawdzić u swojego dostawcy energii elektrycznej, za ile ją dostarcza, bo to od jej ceny — a jest coraz droższa — będzie zależał końcowy zysk. Jeśli koparki mają pracować

[19] *https://www.buybitcoinworldwide.com/mining/hardware/*

[20] Ibid.

[21] Ibid.

[22] *https://www.buybitcoinworldwide.com/mining/hardware/*

[23] *https://www.asicminervalue.com/miners/microbt/whatsminer-m30s-1*

na większą skalę, warto rozważyć wynegocjowanie z elektrownią przejścia na taryfę przemysłową.

W tych wszystkich założeniach wychodzi więc na to, że do uwzględnienia mamy szereg parametrów, przedstawionych w **tabeli 4.1**.

Tabela 4.1. Parametry wpływające na rentowność koparek do kryptowalut

Parametry stałe (model Whatsminer M30S+)	**Parametry zmienne**
Cena koparki = 2500 $ (~10 000 zł) Maksymalny hash rate = 100 Th/s Moc przy maksymalnej wydajności koparki = 3400 W Zużycie energii w ciągu dnia (założenie pracy 24 godz. na dobę) = 81,6 kW	Koszt energii [zł/kWh] — zależny od rynku energii Kurs BTC/PLN — zależny od rynku kryptowalut

Przy takich parametrach warto oszacować opłacalność kopania w kilku scenariuszach i rozpisać je w formie tabeli. Żaden miner nie jest w stanie przewidzieć faktycznego kursu kryptowalut, dlatego trzeba przygotować się na duże wahania zysku. Przykładowo we wrześniu 2021 r. kurs BTC wahał się w granicach 40 – 52 tysięcy dolarów — czyli ok. 157 – 205 tysięcy złotych. Z takimi wahaniami trzeba się po prostu liczyć; tak działa rynek kryptowalut. Jednocześnie rosną ceny energii. Przykładowo, gdyby doszło do krachu w kryptowalutach, np. kurs BTC spadłby w okolice 100 tysięcy złotych (ok. 25 tysięcy dolarów), a ceny prądu poszybowały do poziomów takich jak w Europie Zachodniej, to biznes koparkowy mógłby przynosić straty. Jest to jednak scenariusz raczej nieprawdopodobny; kryptowaluty pną się w górę, więc rosnąca wartość Bitcoina obecnie rekompensuje podwyżki cen prądu.

Wszystkie scenariusze związane z cenami prądu i kursem Bitcoina rozpisuje się w specjalnej tabeli, która nazywa się tabelą sensytywności. Pokazuje, jak czuły jest dzienny zysk wypracowany przez koparkę na zmiany podstawowych parametrów — tutaj są to ceny energii oraz kurs kryptowaluty. W polu tabeli widać wartości, które wskazują, ile pieniędzy zarabia koparka w ciągu dnia. Walutą jest tu oczywiście złotówka (**tabela 4.2**).

Tabela 4.2. Scenariusze dziennej rentowności koparek przy poszczególnych parametrach kursu BTC/PLN oraz ceny za kilowatogodzinę energii elektrycznej

		Cena za 1 kWh energii elektrycznej						
		0,40 zł	0,50 zł	0,60 zł	0,70 zł	0,80 zł	0,90 zł	1,00 zł
Kurs BTC do PLN	100 000 zł	40	31	24	16	8	-1	-8
	150 000 zł	78	67	61	51	44	35	28
	200 000 zł	113	103	97	87	81	73	65
	250 000 zł	149	139	133	123	117	107	101
	300 000 zł	185	176	169	160	153	144	137
	350 000 zł	222	212	206	196	189	180	173

Przy założeniu parametrów, które tutaj omawiam, widzimy, jaka rozpiętość scenariuszy codziennie czeka bitcoinowego górnika. Przykładowo w Warszawie w 2021 r. taryfa za prąd dla osób prywatnych wynosiła ok. 70 groszy za 1 kWh. Oznacza to, że we wrześniu tego roku zysk z pracy jednej koparki mógł wynosić od 51 do 87 zł dziennie. Jeśli uśrednimy te wartości, to spodziewany zysk w ciągu miesiąca wynosi 2070 zł. Zatem taka koparka spłaciłaby się w ciągu 5 miesięcy. Dlatego częstą taktyką jest zaczynanie z kilkoma koparkami, a następnie rozszerzanie działalności na większą skalę — w miarę spłacania pierwszych maszyn i budowania bitcoinowego majątku. Co istotne, wraz z rozwojem takiego biznesu można budować własne zaplecze różnych typów koparek, aby produkować inne kryptowaluty, takie jak Litecoin czy Ethereum. Dzięki temu można dywersyfikować inwestycje i źródła dochodu, aby ograniczać ryzyko strat, gdy spada kurs konkretnej kryptowaluty.

W założeniach i obliczeniach dotyczących koparek kryptowalut trzeba być jednak bardzo ostrożnym. Skoro coraz więcej górników wydobywa bitcoiny i liczy na nagrodę, to z każdym miesiącem rosną bariery wejścia do tej gry. Spada więc rentowność inwestycji w koparki kryptowalut. Dzieje się tak, ponieważ sieć BTC zużywa coraz więcej prądu; nawet najlepiej zoptymalizowane koparki pobierają go więcej, przez co ich faktyczny zysk maleje. W 2021 r. średni zysk jednej koparki wynosił ok. 8 dolarów dziennie[24]; to dlatego minerom zależy, żeby mieć ich tak wiele. Trwa więc obliczeniowy wyścig zbrojeń, w którym osoby i organizacje dysponujące największą mocą obliczeniową (hash rate) będą w stanie wydobyć najwięcej bitcoinów. Jednak jak pokazują założenia, nawet dziś, powtórzę, jest w tym wyścigu miejsce na historie nowych kryptomilionerów.

[24] *https://www.buybitcoinworldwide.com/mining/profitability/*

Blockchain. Klucz do świata kryptowalut. Słowo, które brzmi jak obietnica bogactwa. Tylko... czym właściwie jest Blockchain? Niestety, w większości książek, artykułów, dyskusji w mediach tradycyjnych i internecie mówi się o nim albo niezrozumiale, albo w mocnych uproszczeniach i z niepotrzebnym bagażem emocji. Albo technicznie, albo ideologicznie. Albo pokłada się w Blockchainie nadzieję na uratowanie społeczeństwa przed pazernymi bankierami, albo pokazuje się go jako narzędzie do budowania znienawidzonych przez banki centralne kryptowalut. Który obraz ma więcej wspólnego z rzeczywistością?

Mateusz Mach związał z Blockchainem swoją działalność biznesową. W książce przedstawia sposób, w jaki ta technologia — na początku funkcjonująca w formie ciekawostki kryptograficznej — wpisuje się w szerszy kontekst społeczny, ekonomiczny i historyczny. Opowieść o Blockchainie, to nie tylko opowieść o matematycznych eksperymentach. To przede wszystkim historia odwiecznej próby zapisania działalności człowieka, a także płynącej z niej wartości. Tym razem jednak ma to być zapis dostępny dla wszystkich, na równych zasadach. Czy również dla Ciebie? Odpowiedzi szukaj w książce.

Patron medialny:

nextrope

onepress

Księgarnia internetowa:
http://onepress.pl

HELION SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
onepress@onepress.pl

książkiklasybusiness

ebook dostępny na:
ebookpoint

ISBN 978-83-283-8776-8

Cena: 69,00 zł