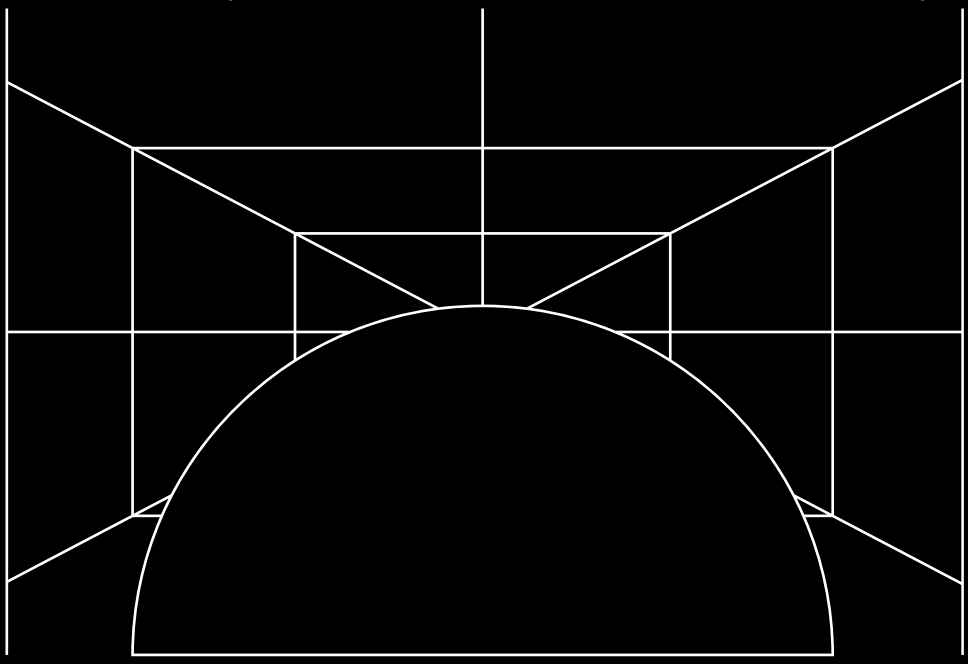
KRYPTOWALUTY

Michał Grzybkowski
Szczepan Bentyn



Dlaczego jeden bitcoin wart będzie milion dolarów?

I co zrobić, żeby zrozumieć rewolucję większą niż powstanie internetu, nie będąc informatykiem?

ED 2.0

01001101 01101001 01100011 01101000 01100001 01101100
00100000 01000111 01110010 01111010 01111001 01100010
01101011 01101111 01110111 01110011 01101011 01101001
00100000 01010011 01111010 01100011 01111010 01100101
01110000 01100001 01101110 00100000 01000010
01100101 01101110 01110100 01111001 01101110 00100000
01001011 01110010 01111001 01110000 01110100 01101111
01110111 01100001 01101100 01110101 01110100 01111001

Michał Grzybkowski

KRYPTOWALUTY

Szczepan Bentyn

Projekt okładki: Krzysztof Domaradzki
Skład: Olga Beyga
Korekta językowa: Anna Adamowicz
Konsultacja merytoryczna wydania drugiego: Janusz Zieliński

Bezpośrednia dystrybucja wysyłkowa przez internet: www.kryptowaluty.edu.pl
Dostępne są także egzemplarze z autografami autorów (do wyczerpania zapasów).

Fotografie autorów na okładce:
Michał Grzybkowski – fot. Szymon Brodziak
Szczepan Bentyn – fot. Fotostube.pl

Wydawnictwo: Crypto—logic Sp. z o. o.

ISBN: 978-83-950222-1-0
Cena: 59 zł

Wydanie drugie, zaktualizowane i uzupełnione
Poznań, listopad 2021 r.

ISBN 978-83-950222-1-0

#BibliaKryptowalut

Od autorów, zaproszenie do przeczytania ebooka na YouTube

Naszym Przyjaciołom

#BibliaKryptowalut

Wstęp

O1OO11O1 O11O1OO1 O11OOO11 O11O1OOO O11OOOO1 O11O11OO
OO1OOOOO O1OOO111 O1110O1O O1111O1O O1111OO1 O11OOO1O
O11O1O11 O11O1111 O1110111 O1110O11 O11O1O11 O11O1OO1
OO1OOOOO O1O1OO11 O1111O1O O11OOO11 O1111O1O O11OO1O1
O1110OOO O11OOOO1 O11O111O OO1OOOOO O1OOOO1O
O11OO1O1 O11O111O O1110100 O1111OO1 O11O111O OO1OOOOO
O1OO1O11 O1110O1O O1111OO1 O1110OOO O1110100 O11O1111
O1110111 O11OOOO1 O11O11OO O1110101 O1110100 O1111OO1

Najdroższa pizza świata, czyli dla kogo jest ta książka?

Michał Grzybkowski

Pierwsze bitcoiny zostały użyte do transakcji handlowej 22 maja 2010 roku przez Laszlo Hanyecza, który za ok. 10 tys. BTC kupił od znajomego z internetowego forum dyskusyjnego – Jeremiego „Jercosa" Sturdivanta – dwie pizze. Gdyby Laszlo postanowił tego dnia zapłacić gotówką, a swoje bitcoiny pozostawić w cyfrowym portfelu, ich wartość 22 października 2021 roku wyniosłaby nieco ponad 650 milionów dolarów[1]. Biorąc pod uwagę technologie, które wspierają integralność kryptowalut, dynamikę zmian ich wartości oraz podstawowe prawa ekonomii, nie jest wykluczonym, że pizza, którą zjadło kilka lat temu dwóch entuzjastów technologii, na zawsze zapisze się jako najdroższy posiłek w historii świata[2].

Dwanaście lat później, w roku 2021, miały miejsce następujące wydarzenia:

- Paypal, lider światowych płatności cyfrowych, posiadający 346 milionów użytkowników, zapowiedział pełną obsługę kryptowalut, zarówno w obszarze inwestycji jak i możliwości wykorzystania ich w celu realizacji zakupów w milionach sklepów internetowych które obsługuje[3];
- Salwador, jako pierwszy kraj na świecie, 9 czerwca 2021 roku uchwalił prawo stanowiące bitcoina (BTC) legalnym środkiem płatniczym[4] i rozpoczął aktywne zwiększanie swoich rezerw finansowych w tej kryptowalucie[5];
- CircleK, operator stacji benzynowych oraz sklepów typu convenience, zapowiedział uruchomienie w swoich lokalizacjach tysięcy bitcoinowych bankomatów[6];
- notowana na nowojorskiej giełdzie Tesla zainwestowała w bitcoiny półtora miliarda dolarów, a inni inwestorzy instytucjonalni rozpoczęli aktywne inwestycje zarówno w kryptowaluty, jak i w oparte na nich pochodne instrumenty finansowe;
- obalono wiele mitów, w tym ten dotyczący ekologii „kopania" kryptowalut (poświęcamy temu kilka rozdziałów). Udowodniono, że w skali planety,

[1] Zagregowana wycena kryptowaluty bitcoin (BTC), będąca średnią danych transakcyjnych z głównych giełd wymiany kryptowalut, dane z coinpaprika.com (dostęp: 14 kwietnia 2021 r.).

[2] Na pamiątkę tego wydarzenia obchodzimy Bitcoin Pizza Day.

[3] https://www.reuters.com/article/paypal-cryptocurrency/paypal-to-allow-cryptocurrency-buying-sellin-and-shopping-on-its-network-idUSL1N2HB14U

[4] https://www.reuters.com/world/americas/el-salvador-approves-first-law-bitcoin-legal-tender-2021-06-09/

[5] https://www.cnbc.com/2021/09/07/el-salvador-buys-400-bitcoin-ahead-of-law-making-it-legal-currency.html?&qsearchterm=salvador%20buy%20400%20bitcoin

[6] https://www.coindesk.com/business/2021/07/22/bitcoin-atms-to-invade-circle-k-convenience-stores/

w porównaniu do tradycyjnych systemów bankowych, sieć bitcoina zużywa o ponad połowę mniej prądu[7];

• wartość (kapitalizacja) bitcoina w marcu 2021 roku była wyższa niż firm Visa i Mastercard razem wziętych[8];

• Twitter umożliwił przekazywanie napiwków w bitcoinie dla twórców treści umieszczanych na swojej platformie[9];

• w 2021 roku połowa wszystkich użytkowników kryptowalut mieszkała w Azji;

• mieszkańcy krajów rozwijających się, w szczególności tych o niestabilnych systemach monetarnych, jak Nigeria, Brazylia, Kenia, Wietnam czy Wenezuela wzięli sprawy w swoje ręce i aktywnie przeszli na codzienne rozliczenia w kryptowalutach[10], stanowiących realną alternatywę dla tradycyjnych systemów finansowych, o czym rozpisywał się we wrześniu 2021 roku Financial Times;

• 5 października 2021 roku, pierwszy amerykański bank, US Bank, zapowiedział uruchomienie usługi przechowywania depozytów kryptowalutowych dla klientów instytucjonalnych[11].

Warto także wspomnieć o jeszcze jednej przełomowej zmianie – od roku 2017 kapitalizacja rynku kryptowalutowego zaczęła dynamicznie przybierać na masie, a we wrześniu 2021 roku kapitalizacja najważniejszych, w pełni wymienialnych na pieniądze fiducjarne kryptowalut wyniosła prawie dwa i pół biliona dolarów.

Wydarzenia przełomu dekady cechują się jednak czymś nowym – JF Kennedy lubił powtarzać, że „przypływ unosi wszystkie łodzie" – kryptowaluty przestały ze sobą rywalizować o względy dolarów, euro czy funtów. W ekosystemach takich jak bitcoin, ethereum i inne, pojawiły się pierwsze większe pieniądze. Ludzkość stanęła przed faktem dokonanym: nie czekając na rządy, banki czy regulatorów rozpoczęła się masowa popularyzacja. Kryptowaluty trafiły pod strzechy, zaś technologia stojąca za tą rewolucją, czyli tzw. „rejestr rozproszony", w szczególnej wersji jaką jest *blockchain*, swoją potęgą przyćmił wszystko, co do tej pory widziała ludzkość, z wynalezieniem internetu włącznie. I o tym właśnie przeczytasz w tej książce.

---

[7] https://www.nasdaq.com/articles/research%3A-bitcoin-consumes-less-than-half-the-energy-of-the-baking-or-gold-industries

[8] https://www.investing.com/news/cryptocurrency-news/bitcoin-is-now-worth-more-than-visa-and-mastercard-combined-2448375

[9] https://www.cnbc.com/2021/09/23/you-can-now-get-paid-in-bitcoin-to-use-twitter.html

[10] https://www.ft.com/content/1ea829ed-5dde-4f6e-be11-99392bdc0788 (dostęp: 4 września 2021).

[11] https://ir.usbank.com/news-releases/news-release-details/us-bank-announces-new-cryptocurrency-custody-services

Jeżeli zewsząd słyszysz o inwestycjach w kryptowaluty, chcesz poznać i przede wszystkim zrozumieć nowe medium, w którym niebawem wyceniane będą wszelkie dobra materialne, od porannej kawy po nieruchomości, a zarazem potrafisz samodzielnie korzystać chociażby z bankowości internetowej, ta książka jest dla Ciebie. Chcielibyśmy w niej pokazać, jak w praktyce kupić za przysłowiowego dolara coś z koszyka kryptowalut, zarówno jako inwestor, użytkowniczka codziennych mikropłatności, kolekcjonerka cyfrowej sztuki czy przedsiębiorca planujący wprowadzić obsługę płatności w takiej formie w swoim sklepie internetowym.

Przede wszystkim chcielibyśmy podzielić się z Tobą wiedzą, która pozwoli zrozumieć nadciągającą rewolucję oraz poznać sposoby poruszania się w nowych obszarach zagadnień w sposób bezpieczny, wskaże, na co uważać i gdzie szukać pomocy, jeśli coś pójdzie nie tak.

Jeżeli zaś frazy takie jak „zabendowany kernel" czy „deployowanie farmy serwerów przez API" są dla Ciebie chlebem powszednim, to szczegóły techniczne zawarte w tej publikacji mogą się Tobie wydać nudne i jesteśmy przekonani, że jesteś co najmniej geekiem, o ile nie nerdem i o bitcoinie słyszałeś już nieco wcześniej. Nie szkodzi.

Jeżeli natomiast jesteś bankierem, pracujesz w branży finansowej w tradycyjnym rozumieniu tego słowa lub jesteś politykiem odpowiedzialnym za finanse państwa to warto, abyś przeczytał tę książkę już teraz, aby zrozumieć rewolucyjną skalę zmian, jaką niesie technologia blockchain oraz zbudowane na niej kryptowaluty, bo może się okazać, że już niedługo zostaniesz bez pracy.

Postaramy się udowodnić, że stojąca za nowymi pieniędzmi matematyka jest bezwzględnym i apolitycznym strażnikiem, którego można wykorzystać do zabezpieczenia części swoich oszczędności, wygodnych rozliczeń ze znajomymi czy też zaprzęgnięcia technologii stojących za kryptowalutami do autoryzacji i weryfikacji zdarzeń w nieskończenie skomplikowanych ekosystemach gospodarczych i politycznych.

Odpowiadając na pytanie otwierające słowo wstępu – to nie jest książka dla informatyków, choć liczymy, że i oni znajdą w niej coś dla siebie.

W naszym mniemaniu, w publikacji tej udało się zebrać zarys wiedzy związanej z kryptowalutami, która może stać się kompendium dla osób ciekawych nowych technologii, porządkującym w przystępny sposób dostępne źródła i zachęcającym do dalszych poszukiwań.

To książka dla osób, dla których współczesne technologie są bardziej środkiem, a mniej celem samym w sobie.

Organizacja książki „Kryptowaluty”

Michał Grzybkowski

Ze względu na skalę i różnorodność zagadnień, które przybliża ta publikacja, postanowiliśmy podzielić omawiane kwestie na trzy główne grupy tematyczne.

Technologia – w pierwszych rozdziałach omawiamy w przystępny sposób działanie stojącej za bitcoinem technologii rejestru rozproszonego, czyli blockchain bitcoina. Przybliżamy także zagadnienia związane z mechaniką stojącą za działaniem kryptowalut i ich bezpieczeństwem oraz wyjaśniamy, skąd w ogóle biorą się bitcoiny i waluty alternatywne. W dalszej części omawiamy kwestie związane z funkcjami pieniądza tradycyjnego w kontekście kryptowalut. Przygotowaliśmy usystematyzowaną klasyfikację cyfrowych pieniędzy ze względu na ich cechy i funkcje, a także omówiliśmy najpopularniejsze w tej chwili instrumenty kryptowalutowe w uporządkowanej formie, co jest pionierskim działaniem na rynku wydawniczym związanym z tym tematem.

Przyszłość – w tej części książki mierzymy się z potencjalnymi konsekwencjami, jakie niesie za sobą powszechna adaptacja technologii rejestrów rozproszonych w szeregu gałęzi gospodarki. Omawiamy kolosalne znaczenie blockchaina, który bez wątpienia jest fundamentem rewolucji o skali i znaczeniu większym niż powstanie internetu! Przechodzimy od rankingu zawodów i branż, które przestaną niebawem istnieć, po rewolucje w poszczególnych sektorach gospodarki, od logistyki, poprzez finanse, aż po dzieła sztuki. Mierzymy się także z zagadnieniami trudnymi, takimi jak wpływ kryptowalut na światowe finanse, bezpieczeństwo czy państwowość. Liczymy na to, że rozdziały zgrupowane w sekcji „Narodziny Nowego Porządku Świata” będą szczególnie interesujące zarówno dla entuzjastów nowych technologii, jak ekonomistów, inwestorów kapitałowych czy polityków i filozofów.

Praktyczny poradnik – w ostatnich rozdziałach postaramy się poprowadzić Czytelnika za rękę i przygotować do bezpiecznego wejścia w świat kryptowalut, wyjaśniając po drodze wszystkie istotne kwestie związane z bezpiecznym zakupem pierwszego bitcoina (lub jego części). Część tę powinno się traktować jako praktyczny poradnik dla osób, które nigdy nie miały do czynienia z kryptowalutami. Omawiamy w nim także wszelkie ryzyko związane z globalnym światem krypowalut, począwszy od przechowywania cyfrowych wartości, przez transakcje kryptowalutowe, po analizę prawną kryptowalut i związane z nią regulacje prawno-skarbowe w naszym kraju.

Dodatkowo, ze względu na fakt, że książka „Kryptowaluty" pisana jest wspólnie przez dwóch autorów – Michała Grzybkowskiego (autora głównego) oraz Szczepana Bentyna – przy każdym rozdziale oznaczyliśmy osobno autorstwo poszczególnych części. Wyjątkowym rozdziałem jest ten traktujący o regulacjach prawno–skarbowych w świetle polskiego prawa, napisany przez mecenasa Adama Rajewskiego, specjalistę od podatków, opracowany przy współpracy z Kancelarią Adwokacką Grzybkowski–Guzek.

Książkę kończymy częścią poświęconą twórcy bitcoina i technologii blockchain – Satoshiemu Nakamoto, który jak nikt w tej branży zasługuje na odrębny rozdział.

Zdając sobie sprawę z ilości faktów, na które się powołujemy, właściwe na każdej stronie umieszczaliśmy przypisy, których jest w tej publikacji ponad czterysta, wskazując źródła, na których się opieraliśmy.

Przedmowa do drugiego wydania

Michał Grzybkowski

Trzymasz w rękach drugie wydanie książki „Kryptowaluty – Dlaczego jeden bitcoin wart będzie milion dolarów?". Pierwsza edycja była debiutem wydanym przez nas własnym sumptem i trafiła drukarni po prawie roku wytężonej pracy, dokładnie wieczorem, 17 lutego 2018 roku i miała białą okładkę. Jest nam bardzo miło, że książka zebrała wysokie oceny i jako pierwsza publikacja tego typu została uznana w wielu kręgach za biblię polskiego świata kryptowalut. Wydanie książki w ramach samopublikowania było dla autorów wielką przygodą, ale największą nagrodą jest fakt, że praktycznie bez wydania złotówki na marketing, wyprzedaliśmy cały papierowy nakład. Nie zastanawiając się długo, podjęliśmy decyzję o tym, że nie zrobimy zwykłego dodruku, ale znów wypijemy szalone ilości kawy i zarwiemy kilkadziesiąt nocy, aby przygotować wersję zaktualizowaną, w kilku miejscach poprawioną i uzupełnioną o najważniejsze wydarzenia ponad tysiąca dni, jakie dzielą oba papierowe wydania. A wydarzyło się więcej niż mogłoby się nam przyśnić. A jako, że papier jest cierpliwy, to pokusimy się o podsumowanie tego, co udało nam się przewidzieć, gdzie nasze prognozy zawiodły i co nas zaskoczyło.

Wybrane trafne przewidywania i prognozy zawarte w pierwszej wersji książki:

- wielkim wydarzeniem opisanym we wstępie pierwszej edycji było to, że w kwietniu 2017 r. Japonia jako pierwszy kraj na świecie zalegalizowała bitcoina,

traktując go jak normalny środek płatniczy. Patrząc z perspektywy czasu, w 2021 roku bitcoin jest prawnie uregulowany w większości krajów na świecie, w tym w Stanach Zjednoczonych i Unii Europejskiej, z wyjątkiem garstki krajów, które go nadal zakazują[12]. Legislacja umożliwia nie tylko legalny obrót i posiadanie kryptowalut, ale także, co najważniejsze, możliwość legalnego rozliczania się przed urzędem skarbowym. Nasze wyobrażenia natomiast przerósł fakt, że w połowie 2021 roku pierwszy kraj, jakim był Salwador uznał bitcoina (BTC) za obowiązujący na swoim terenie środek płatniczy. I jesteśmy przekonani, że w jego ślady pójdą kolejne państwa;

• prognozowaliśmy wzrost popularności bitcoina i innych kryptowalut, a także wzrost akceptacji ich jako środka płatniczego. Ale nie spodziewaliśmy się, że przez trzy lata bitcoin przebije się do świadomości społecznej i zacznie funkcjonować w wiadomościach gospodarczych czy ekonomicznych na równi z informacjami z giełd surowców czy kursów walut tradycyjnych, a także tego, że najbogatsi ludzie na trzeciej planecie od Słońca, jak chociażby Elon Musk, będą otwarcie informować o swoich inwestycjach w krypto. Bitcoin przebił się do mainstreamu i nic nie wskazuje na to, żeby miało się to zmienić;

• po cichu liczyliśmy, że kiedyś, w odległej przyszłości, do grupy inwestorów indywidualnych będą mogły dołączyć także fundusze inwestycyjne i szeroko rozumiani inwestorzy instytucjonalni. Jak grom z jasnego nieba spadła na nas informacja, że będące rdzeniem Unii Europejskiej Niemcy, kraj słynący z konserwatywnego spojrzenia na politykę finansową, w 2021 roku uchwalił prawo dopuszczające możliwość inwestycji pieniędzy z funduszy w aktywa kryptowalutowe. W USA zaś fundusze takie jak Rotschild, Microstrategy, Ark Invest, czy Tesla inwestują w kryptowaluty miliardy dolarów;

• trafnie przewidzieliśmy zbliżającą się rewolucję czekającą obszar praw autorskich. Wybuch popularności sztuki (a także innych dóbr kolekcjonerskich) opartej na unikatowych tokenach NFT, w okresie poprzedzającym drugie wydanie zasłużył na nowy, osobny i dość obszerny rozdział;

• przewidzieliśmy także wykorzystanie technologii rejestrów rozproszonych w obsłudze danych medycznych, czego najlepszym przykładem są certyfikaty szczepienia na Covid-19, zrealizowane na blockchainie, chociażby w Estonii;

• przewidzieliśmy także skokowy wzrost ilości użytkowników kryptowalut oraz rozwój całego ekosystemu fin-techów;

• przewidzieliśmy również krok Facebooka związany z emisją wewnętrznej kryptowaluty Libra (obecnie nazywanej Diem);

• przewidzieliśmy wzrost ceny bitcoina, stawiając kilka prognoz w rozdziale

[12] https://www.investopedia.com/articles/forex/041515/countries-where-bitcoin-legal-illegal.asp

dotyczącym wartości, starając się oszacować, kiedy dokładnie może być on wart tytułowe milion dolarów za sztukę. Można powiedzieć, że do tej pory przynajmniej dwie długoterminowe prognozy ceny wykazały się wysokim poziomem trafności, gdzie szczególną uwagę należy zwrócić na analizę ceny na podstawie fal Eliota oraz związek między ilością użytkowników a ceną na podstawie Prawa Metcalfe'a;
• kompletnie zaś nie sprawdził się skrajnie agresywny model oparty na danych z 2017 roku, zakładający, że bitcoin nigdy już nie potanieje, będzie rósł wykładniczo i osiągnie cenę miliona dolarów pod koniec 2020 roku. Co do wyceny "cyfrowego złota", w 2020 pomyliło się także kilku ekspertów branży finansowej, takich jak Michael Novogratz (inwestor, miliarder, były partner w Goldman Sachs), który twierdził, że 1 bitcoin (BTC) będzie można kupić za 40.000 USD do końca 2018 roku[13], nieżyjący już John McAfee (programista, twórca oprogramowania antywirusowego McAfee), czy James Altucher (autor, przedsiębiorca oraz *hedgefund manager*, redaktor The Financial Times oraz TechCrunch), przewidujący koszt 1 bitcoina (BTC) na 1 mln USD do końca 2020 roku[14], na których powoływaliśmy się, zbierając prognozy metodą delficką. Kilka innych prognoz pozostało w mocy.

Bezsprzecznym jest natomiast to, że od czasu publikacji pierwszej edycji „Kryptowalut" bitcoin zyskał na wartości. Co ciekawe, gdy zaczynaliśmy pisać naszą książkę w 2017 roku, bitcoin kosztował „tylko" jeden tysiąc dolarów[15]. Mimo znacznych ruchów cenowych (co jest specyfiką tego rynku), w połowie kwietnia 2021 roku wyceniany był już sześćdziesiąt pięć razy tyle! Można dowcipnie zaznaczyć, że po tym jak podrożał już 65 razy, to aby osiągnąć milion dolarów wystarczyłoby, aby podrożał jeszcze „tylko" 15.3 raza.

Co nas zaskoczyło:
• to, że bitcoin potrafił być droższy od kilograma złota w 2021 r.;
• to, jak szybko tradycyjna branża finansowa, zamiast walczyć z kryptowalutami,

[13] CNBC, 7 listopada 2017 roku, https://www.cnbc.com/2017/11/27/bitcoin-could-easily-reach-40000-by--the-end-of-2018-novogratz.html

[14] http://cointelegraph.com/news/john-mcafee-doubles-down-predicts-1-mln-btc-bets-his-dk-on-it
John McAfee skorygował swoją prognozę ceny bitcoina do poziomu 1 mln USD za 1 BTC do końca 2020 i jeżeli by się tak nie stało poprzysiągł...zjeść swoje przyrodzenie w programie transmitowanym na żywo w publicznej telewizji (twitter: @officialmcafee).

[15] Gdyby w dniu wydania pierwszej edycji książki 17 lutego 2018 roku przeznaczyć całe jednomiesięczne świadczenie 500+ na zakup bitcoina, można byłoby przy cenie 34.6 tys. zł za 1 BTC kupić dokładnie 0,0144 bitcoina, który trzy lata później, w kwietniu 2021 roku wart był 3.3 tys. zł. Gdyby zaś kupić za 500 zł bitcoiny dwa lata wcześniej, czyli 1 kwietnia 2016, w momencie gdy świadczenie 500+ zostało wypłacone po raz pierwszy, można było nabyć aż 0.3135 bitcoina, co w szczycie ceny, 14 kwietnia 2021 roku, wyceniałoby tę jednomiesięczną inwestycję na prawie 81 tys. złotych! Historyczne dane o cenie BTC: http://www.coinpaprika.com

zaangażowała się w rozwój rynku, czego kulminacją był debiut giełdy Coinbase na nowojorskiej giełdzie w kwietniu 2021 r.;
• pojawienie się w roku 2017 i wzrost na znaczeniu giełdy Binance, będącej dziś liderem handlu kryptowalutami;
• pojawienie się kosmicznej, w dosłownym tego słowa znaczeniu, technologii Starlink, zapewniającej bezprzewodowy dostęp do internetu w skali całej planety, mimo że w wydaniu z 2017 prognozowaliśmy, że może się to odbyć dzięki projektom Google lub Facebooka;
• niesłychanie trafny, działający od marca 2019 r. model prognozy ceny bitcoina zwany *stock-to-flow* (któremu również poświęciliśmy osobny rozdział), dla którego rok 2022 będzie największym testem.

Co przeżyliśmy:
• pandemię choroby Covid-19, a także opracowanie szczepionki na nią w niespotykanym dotąd tempie;
• kolejny, trzeci już dla nas *halving* bitcoina;
• kolejną, jak fraktal powracającą co kilka lat, bańkę inwestycyjną w świecie kryptowalut w roku 2017. Jako osoby mające kontakt z kryptowalutami od roku 2013, widzieliśmy niejedno szaleństwo cenowe i prawdę mówiąc, znów nie bardzo nas ona zaskoczyła, w przeciwieństwie do milionów nowych osób, które chciały szybko zarobić. Temu tematowi także poświęciliśmy osobny rozdział;
• upadek wielu startupów blockchainowych, o których pisaliśmy w roku 2017, ale także pojawienie się nowej generacji przedsiębiorstw, opartych o solidne ekonomiczne fundamenty, co jest naturalną koleją rzeczy. Część z nich przekształciła się w firmy o nieco innym profilu, wykorzystując kompetencje i doświadczenie zebrane w pierwszych latach pracy nad rozwiązaniami blockchain.

W skali planety przybyło zaś 300 milionów ludzi, a ilość osób przyłączonych do internetu wzrosła z 3.8 miliarda do 4.6 miliarda użytkowników. Po drodze zaś wszystko zamarło przez pandemię Covid-19, która pochłonęła wiele istnień, ale także była katalizatorem digitalizacji świata.

W mikroskali, my, Autorzy tej książki, zebraliśmy wiele, także trudnych i pouczających doświadczeń. Spotkaliśmy przez ten okres na naszej drodze wspaniałych ludzi, którzy są teraz naszymi wspólnikami w odnoszących globalną popularność przedsięwzięciach związanych z technologią blockchain – *Coinpaprika.com* i *Gamerhash.com* (Michał) oraz *Sapiency.io* (Szczepan).

Michał Grzybkowski i Szczepan Bentyn

Kryptowaluty: bitcoin, litecoin, ethereum, monero... i inne. Z jednej strony ostrzegawcze sygnały – bańka spekulacyjna (uważajcie!), z drugiej zaś, rozgrzani do białości, ortodoksyjni ewangeliści, którzy z pianą na ustach wieszczą rychły kataklizm, a zaraz po nim – Nowy Porządek Świata, lub w wersji zachowawczej – co najmniej trzecią wojnę światową. W tle zaś – banki, regulatorzy rynku kapitałowego i operatorzy płatności, którzy obserwują miliardowe przelewy na kontach klientów mających styczność z nowym rodzajem giełd, oferujących w pełni legalną wymianę dolarów, jenów czy euro na bitcoiny i inne kryptowaluty. A na dodatek jeszcze państwa i rządy zmagające się w obszarze legislacji z nowym wyzwaniem.

Nowy, globalny i oparty na internecie i zaufaniu do kryptografii system finansowo-rozliczeniowy, do zastanego stanu prawnego pasuje jak pięść do nosa. W rezultacie jedne kraje legalizują bitcoiny, inne bezradnie ścigają posiadaczy[16], kolejne udają, że tematu nie ma, skutecznie go ignorując, a ostatnia grupa – na wszelki wypadek, bez wnikania w istotę materii – opodatkowuje zyski z obrotu kryptowalutami. A na końcu (lub może właśnie tym razem na początku), kraje globalnego Południa[17], przez wielkie światowe gospodarki traktowane do tej pory po macoszemu, nagle pomijają zupełnie cały dorobek współczesnej finansjery i zaczynają rozliczać się cyfrowymi odpowiednikami walut przenoszącymi wartość. Po co czekać, skoro nie ma na co? Po co płacić wysokie prowizje, skoro można ich uniknąć?

A teraz zbierzmy fakty. Wyobraźmy sobie globalny, w pełni zdecentralizowany, odporny na awarie i niemożliwy do zablokowania czy kontrolowania system rozliczeniowy. System oparty na zaufaniu do praw matematyki, a nie praw stworzonych przez ludzi. Oparty na bezwzględnych prawach algorytmów kryptograficznych potężnej matematyki, będącej jego jedynym gwarantem i strażnikiem.

Niech system ten będzie w całości przejrzysty, do tego stopnia, aby każda pojedyncza transakcja w jego obrębie i w całej historii była jawna i na dodatek możliwa do zweryfikowania pod względem poprawności przez chętnych do takiej pracy. Dodajmy do tego całkowitą odporność na inflację[18] (brak możliwości

[16] https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory

[17] https://cryptocoinsnews.com/africa-ripped-bitcoin/

[18] Dotyczy bitcoina, w dalszej części książki omawiamy kryptowaluty nieinflacyjne.

„dodruku" pieniądza), wynikającą z ustalonego od początku twardego ograniczenia liczby „cyfrowych monet" wyemitowanych w jego obrębie.

Sprawność działania? Proszę bardzo – „przelewy", które odbywają się w ciągu sekund i realizowane są w sposób bezpośredni między portfelami jego uczestników, bez potrzeby i udziału żadnej centralnej instytucji typu bank. Zasięg działania – na razie nasza planeta, a właściwie, uwzględniając przyłączoną do internetu międzynarodową stację kosmiczną ISS, już nawet mały fragment kosmosu. System transgraniczny i działający ponad ograniczeniami wynikającymi ze stref czasowych, bariery odległości czy regulacji prawnych. Łatwy w obsłudze – przekazanie środków jest równie „skomplikowane" jak wysłanie e-maila. Lub postawienie kropki na końcu tego zdania. System, który od początku swego istnienia nie miał ani sekundy awarii.

Dodajmy także brak technicznej możliwości zablokowania czy wycofania raz złożonego zlecenia przez jakąkolwiek instytucję czy zewnętrzną siłę. Dotyczy to także bezpieczeństwa „rachunków" rozliczeniowych, które raz uruchomione stają się trwałą częścią systemu i nie mogą nigdy zostać „zamknięte" czy też „zamrożone". System jest w pełni zautomatyzowany. Oczywistym jest zatem, że działa nieprzerwanie całą dobę, 365 dni w roku. Prowadzenie „rachunku" jest bezpłatne i nie ma przeciwwskazań, aby w razie potrzeby uruchomić praktycznie nieskończoną ilość zabezpieczonych jedynie hasłami dostępu kont.

Pewność? Proszę bardzo – może przekonają Cię stojące za integralnością i niewypieralnością transakcji cyfrowe podpisy największego superkomputera świata o mocy obliczeniowej większej o kilka rzędów wielkości tysięcy największych superkomputerów świata razem wziętych. Jest to moc kryptograficzna, o której nawet najbogatszy kraj, wojsko czy centrum badawczo-naukowe może jedynie pomarzyć. W tle silna kryptografia oparta na zaufaniu wynikającym z realizacji swojego działania w oparciu o technologię *open source*[19]. Odporność na ataki hakerów czy błędy w oprogramowaniu praktycznie wyeliminowane dzięki temu, że system został zweryfikowany przez setki, o ile nie tysiące specjalistów, a najlepszym dowodem jest to, że działa nieprzerwanie już od ponad dwunastu lat![20]

Aby dodać odrobiny pikanterii, wspomnijmy o kosztach, a właściwie ich braku i co za tym idzie, zniwelowaniu jakiejkolwiek bariery wejścia. Aby przyłączyć się do systemu i przyjąć pierwszą płatność, niewymagane są żadne nakłady finansowe, a sam czas przystąpienia trwa dosłownie tyle, ile zarejestrowanie się na stronie internetowej lub zainstalowanie odpowiedniej aplikacji w smartfonie[21].

---

[19] Open source – oprogramowanie, którego kod źródłowy jest jawny – otwarty i przejrzysty, a także dostępny publicznie. Każdy na świecie może zobaczyć dokładnie, jak działa każdy element tego oprogramowania.

[20] Pierwszy blok transakcyjny bitcoin został wykopany 3 stycznia 2009 r.

[21] Przykłady w dalszej części książki, w rozdziale „Praktyczny poradnik".

A na koniec dodajmy dość unikatową cechę. Niektóre z kryptowalut pozwalają zapewnić daleko idącą lub absolutnie pełną anonimowość[22]. Stwarza to wiele nowych możliwości, którymi zajmiemy się w dalszych częściach tej książki.

Drogi Czytelniku, droga Czytelniczko, zapraszamy Cię do zapoznania się z fundamentami rewolucji większej niż wszystko, co do tej pory wymyśliła ludzkość. Rewolucji, która pochłonie i bezpowrotnie wymaże z kart historii całe grupy zawodów w tempie szybszym i bardziej brutalnym niż zrobiła to Wielka Rewolucja Przemysłowa czy upowszechnienie się internetu.

Serdecznie witamy w świecie kryptowalut – instrumentów finansowych XXI wieku!

Michał Grzybkowski & Szczepan Bentyn

[22] Dotyczy kryptowaluty monero.

Internet skomunikował świat, blockchain go rozliczy

TECHNOLOGIA

Zrozumieć blockchain

O1OO11O1 O11O1OO1 O11OOO11 O11O1OOO O11OOOO1 O11O11OO
OO1OOOOO O1OOO111 O111OO1O O1111O1O O1111OO1 O11OOO1O
O11O1O11 O11O1111 O1110111 O1110O11 O11O1O11 O11O1OO1
OO1OOOOO O1O1OO11 O1111O1O O11OOO11 O1111O1O O11OO1O1
O1110OOO O11OOOO1 O11O1110 OO1OOOOO O1OOOO1O
O11OO1O1 O11O1110 O1110100 O1111OO1 O11O1110 OO1OOOOO
O1OO1O11 O1110O1O O1111OO1 O1110OOO O1110100 O11O1111
O1110111 O11OOOO1 O11O11OO O1110101 O1110100 O1111OO1

Michał Grzybkowski i Szczepan Bentyn

Ekscytująca przyszłość znajduje się dosłownie o krok przed nami.

Wyobraźmy sobie, że pewnego dnia prawie cała infrastruktura finansowa budowana będzie na otwartym i niepodważalnym oprogramowaniu(...)

Stanie się nieuniknionym, że gospodarka będzie bardziej efektywna, uczciwa, produktywna i sprawiedliwa w stopniu wynikającym z oparcia jej na prawach oprogramowania i matematyki, zamiast na prawach stanowionych przez ludzi. (...)

Finanse staną się proste i sprawiedliwe – nie przez dekrety polityków, ale przez gwarantowane bezpieczeństwo i innowacje dostarczoną przez uwolniony rynek. (...)

Społeczeństwo nie zasługuje na nic innego!

Fragment wypowiedzi Erika Vorheesa[23], założyciela i prezesa firmy ShapeShift.

[23] *Some day, we imagine, nearly all financial infrastructure will be built upon open, objective, non-discretionary code. The ability of a human to decide not to fulfill a transactional obligation (either by mistake or malice), will seem quaint. Inevitably, an economy is more efficient, honest, productive and fair to the extent it is built upon the laws of code and mathematics, instead of the laws of men. Pre-blockchain, that was impossible. Upon products like Prism (itself built upon the pioneering work of blockchain protocol engineers), it is our hope that some day it won't merely be possible, but indeed the expectation, that finance itself becomes provably fair; not by the decree of politicians, but by the demanded security and supplied innovation of a marketplace set free. Society deserves nothing less.* – Erik Vorhees – tłum. autor.

Blockchain, czyli narodziny rejestrów rozproszonych

Michał Grzybkowski

Słowo „rewolucja" wywodzi się z łacińskiego – *revolutio* – i w dosłownym tłumaczeniu oznacza „przewrót" lub przynajmniej znaczącą zmianę, która zachodzi w stosunkowo krótkim czasie. Bardzo lubię tę definicję, bo oddaje dokładne znaczenie i wagę momentu, w którym następuje wielka zmiana biegu wydarzeń. Bez wątpienia takim momentem dla ludzkości było zupełnie nieoczekiwane pojawienie się tak zwanego *distributed ledger*, czyli w rozumieniu finansowym – „rozproszonej księgi głównej" lub po prostu w wolnym tłumaczeniu – technologii „rejestru rozproszonego". Pomimo swej mało porywającej nazwy, wynalazek ten w pełni wyczerpuje znamiona *disruptive technology*, czyli wydarzenia zmieniającego dotychczasowe prawa funkcjonowania świata, będąc nie tylko fundamentem działania całego ekosystemu kryptowalut, ale także (niebawem) większości gałęzi gospodarki.

Różnego rodzaju rejestry prowadzono od czasów zamierzchłych i regulowano w nich szereg aktywności, takich jak chociażby prawa do nieruchomości czy różnorakich rozliczeń finansowych. Pierwotnie zapisy prowadzono na zwojach papirusów, później korzystano z papierowych ksiąg, natomiast w sposób naturalny pełen rozkwit zastosowań nastąpił w erze cyfryzacji, kiedy to komputery przejęły na siebie ciężar przetwarzania coraz większych partii danych.

W roku 2008 rejestr rozproszony pojawił się na świecie dość niespodziewanie, choć wcześniej w świecie IT istniały różnorakie listy i rejestry. Jednak dopiero połączenie ich z zabezpieczeniem kryptograficznym przy użyciu funkcji *hash*, o której kilka słów więcej powiemy w rozdziałach późniejszych, dało początek pierwszej, skutecznie działającej implementacji technologii pod nazwą *blockchain* stojącej za technologią kryptowaluty bitcoin.

Rejestr rozproszony bitcoina jest zdecentralizowaną, rozproszoną w wielu kopiach, współdzieloną, nieustannie przyrastającą listą następujących po sobie kolejno zapisów. Warto przypomnieć słowa Janusza Zielińskiego[24], który w tym miejscu podkreśliłby chętnie, że blockchain nie jest rozproszony. Jeżeli zgra się go na dysk i schowa do szuflady, to zostanie tylko tam. Gdy w 2009 roku Satoshi Nakamoto sam kopał pierwsze bitcoiny, nie było decentralizacji, a był blockchain. Dokument ten funkcjonuje na równych prawach pomiędzy wszystkimi uczestnikami danego systemu (osobami, przedsiębiorstwami, krajami i instytucjami) i nie podlega centralnemu nadzorowi i kontroli. Jest to technologia zaprojektowana pod środowisko zdecentralizowane.

[24] Janusz Zieliński, ekspert kryptowalut i blockchaina, http://januszzielinski.com

Nośnikiem wymiany danych jest sieć internetowa, która zapewnia łączność pomiędzy węzłami systemu opartego o zasadę równorzędności uczestników (sieć *peer-2-peer*). Naturalną zaś cechą każdego rejestru rozproszonego są zaawansowane mechanizmy sprawdzające integralność zawartych w nim danych, oparte o silną kryptografię. Zdarza się, że pojęcia *blockchain* i rejestr rozproszony używane są zamiennie i jest to błąd logiczny. Nie każdy rejestr rozproszony może być nazywany blockchainem (czyli np. infrastrukturą kryptowaluty bitcoin), natomiast bitcoinowy blockchain jest szczególnym, a zarazem pierwszym w historii wdrożeniem koncepcji rejestru rozproszonego.

Zdajemy sobie sprawę, że nieuchronnie przybliżamy Czytelników do zmierzenia się z odpowiedzią na pytanie „jak działa rejestr rozproszony i czym tak naprawdę jest blockchain?"

Możliwość wytłumaczenia i zbudowania świadomości konstrukcji tej technologii jest, naszym zdaniem, kluczowa dla uzyskania zaufania do większości zagadnień poruszanych w tej publikacji. Mamy jednak świadomość, że zmierzenie się z zagadnieniami kryptografii czy matematyki nieco wyższego poziomu niż znany nam ze szkoły średniej, może nie być tym, co „tygrysy lubią najbardziej" – jak mawiał bohater bajki o Kubusiu Puchatku.

Dlatego przygotowaliśmy aż trzy równorzędne rozdziały, opisujące z grubsza potęgę rejestru rozproszonego.

Humanistów i humanistki zapraszamy do przeczytania „Bajki o blockchainie" w dwóch wersjach – dla przedszkolaków i dla nastolatków.

Inżynierów i inżynierki zaś zachęcamy do pogłębienia wiedzy i lektury kolejnego rozdziału, traktującego o „największym superkomputerze ludzkości", w którym wpuścimy Was już na nieco głębszą wodę. Postaramy się Was przekonać, że nie ma większej gwarancji dla ochrony wartości niż matematyka i kryptografia.

Bajki o blockchainie

Szczepan Bentyn

Od pewnego czasu słowo *blockchain*, czyli w dosłownym tłumaczeniu „łańcuch bloków" jest odmieniany przez wszystkie możliwe przypadki i formy, będąc często używanym zamienne ze słowem bitcoin. Należy w tym miejscu rozróżnić dwa pojęcia: bitcoin rozumiany jako system (np.blockchain) oraz bitcoin jako waluta.

Jak już wspomnieliśmy, jest to daleko idące uproszczenie. Bitcoin nie może istnieć bez technologii systemu blockchainowego, natomiast, jak się zapewne szybko przekonamy, systemy oparte na łańcuchach bloków zdominują szereg,

o ile nie większość znanych nam w tej chwili gałęzi gospodarki. Blockchain, dzięki swoim genialnym właściwościom, zrewolucjonizuje branże takie jak: logistyka, bankowość, finanse, prawa autorskie i dzieła sztuki (NFT), notariat i wszelkiego rodzaju prywatne oraz państwowe rejestry, o czym piszemy nieco dalej. Postaramy się teraz wytłumaczyć, w czym rzecz i nieco rozbudzić Waszą wyobraźnię. Przygotowaliśmy dwie wersje bajki o blockchainie.

Bajka o Rozproszonym Banku Krasnoludków

(wersja dla przedszkolaków) Szczepan Bentyn

Dawno, dawno temu, za górami, za lasami, w krainie mlekiem i miodem płynącej, żyły sobie Krasnoludki. Gospodarka kwitła i każdy Krasnal mógł cieszyć się słońcem i górskimi widokami. Król Krasnoludków, w centrum miasta, zbudował wielki Bank, w którym wszyscy mieszkańcy trzymali swoje pieniądze. Bank dawał każdemu magiczną kartę płatniczą, tak, by nie trzeba było nosić przy sobie gotówki. W Banku pracował kochający papier i zapach atramentu Krasnal Papierek, który mozolnie zapisywał w głównej księdze banku wszystkie transakcje, których dokonywały swoimi kartami krasnoludki.

Jednak pewnego dnia wszystko się zmieniło. Miasto napadła banda wstrętnych gnomów, które niszczyły i plądrowały wszystko co napotkały na swej drodze. Gnomy zabiły króla i spaliły wielki bank krasnoludków. Wraz z nim spłonęły wszystkie pieniądze i mozolne zapiski Krasnala Papierka.

Gdy gospodarka krasnali miała się już zapaść, pewien anonimowy Krasnal opisał pomysł na nowy Rozproszony Bank Krasnoludków, którego gnomy nigdy nie będą w stanie zniszczyć. Swój pomysł opisał na dużej kartce i pod osłoną nocy przybił do ściany Banku Krasnoludków, która jako jedyna ostała się z pożaru.

W dokumencie przeczytać można było:

Drogie Krasnale i Krasnalki.

Nadszedł czas odrodzić pieniądz, bo bez niego nasz piękny świat przepadnie. Ale nie pieniądz z góry nam narzucony, ale przez nas wszystkich wybrany. Niech każdy z nas będzie swoim Bankiem, wtedy żadne gnomy nie będą w stanie nam zaszkodzić.

Spytacie zapewne: „Po co nam Bank?! Skoro nie ma już pieniędzy...".

Stworzymy je na nowo! I nie będzie ich rozdawał król, ale nowe pieniądze będą powstawać w sprawiedliwej codziennej loterii, w której każdy Krasnolud będzie mógł wziąć udział.

Wieść o genialnym pomyśle szybko rozeszła się po królestwie i każdy Krasnal chciał wziąć udział w loterii. Losowania odbywały się codziennie o zachodzie słońca na głównym placu. Jednak, aby móc wziąć udział w losowaniu, należało przynieść spisane na kartce transakcje, których dokonało się w ciągu dnia, bądź których było się świadkiem. Na dole kartki należało podsumować wszystkie transakcje, tak aby otrzymać sumę kontrolną i to ona dawała szansę na zwycięstwo.

Następnie odbywało się coś w rodzaju gry w bingo. Krasnal ochotnik losował liczby, wyciągając je z kapelusza. Jeśli w czyjejś sumie kontrolnej znalazła się wylosowana liczba, zaznaczał ją kółeczkiem.

Pierwszy Krasnal, któremu udało się zaznaczyć wszystkie cyferki, wygrywał. Jego kartka trafiała na stos „zatwierdzonych transakcji" i mógł on dopisać sobie do konta 50 nowych talentów. Pozostałe Krasnale przepisywały zwycięską kartkę i sprawdzały czy na pewno wszystko się zgadza. Przepisaną kartkę zanosiły do domu i kładły na swoim stosie. W ten sposób każdy miał swoją kopię wszystkich transakcji, których dokonały Krasnale. Nazajutrz na szczycie nowej kartki, każdy zapisywał sumę kontrolną zwycięzcy poprzedniego losowania.

I od tej pory Krasnale mogły spać spokojnie, nie bojąc się już gnomów, bo wystarczyło, że przetrwa chociaż jeden stos „zatwierdzonych transakcji", by móc odtworzyć całą gospodarkę Krasnali.

Koniec.

Bajka o Rozproszonym Banku Krasnoludków

(wersja dla nastolatków) Michał Grzybkowski i Szczepan Bentyn

Dawno, dawno temu...

...za górami, za lasami, była sobie kraina Krasnoludów. Ich kraina dawała im do życia wszystko, czego potrzebowali. Gospodarka kwitła i każdy Krasnolud mógł cieszyć się słońcem i górskimi widokami. Król Krasnoludów zbudował wielki Bank, w którym wszyscy mieszkańcy trzymali swoje pieniądze. Bank dawał każdemu kartę płatniczą, tak, aby nie trzeba było nosić przy sobie złota. W Banku pracował kochający papiery i zapach atramentu Krasnal Papierek, który mozolnie zapisywał każdą operację zmiany stanu konta leniwych Krasnoludów. Krasnoludy używały swoich kart w każdej sytuacji i wykonywały wiele operacji mikropłatności dziennie – co przysparzało trochę pracy Cierpliwemu Księgowemu, który zapisywał wszystko skrupulatnie, linijka po linijce, na kolejnych kartkach.

Jednak dobrobyt i bezpieczeństwo szybko zniknęły... Złe gnomy zaatakowały pewnej nocy Bank Krasnoludów, podkładając ogień i wszystkie zapisy Krasnala Papierka oraz Cierpliwego Księgowego spłonęły... Król Krasnali kazał odbudować Bank, jednak kiedy udało się wykonać jego rozkaz, gnomy spaliły go ponownie. Gospodarka krainy Krasnali legła w gruzach, kiedy po kolejnej odbudowie Gnomy spaliły już trzeci ich Bank...

Gdy krasnoludzka gospodarka zaczęła popadać w tarapaty, anonimowy Krasnolud opisał pomysł na nowy Zdecentralizowany Krasnoludzki System Transakcyjny, którego gnomy nie będą już w stanie zniszczyć. Królowi Krasnoludów tak bardzo spodobał się nowy system, że postanowił natychmiast go wdrożyć. Powołał nowy, wolny zawód, którego rolą było odnotowywanie transakcji. Postanowił nazwać go zawodem górnika, gdyż praca ta była bardzo mozolna. Każdy Krasnal, dokonując transakcji, musiał ją zgłosić i podpisać u najbliższego górnika, który odnotowywał ją w swoim notesie. Górnicy chodzili po wsiach, miasteczkach i miastach i jako świadkowie zbierali i wymieniali się informacjami o transakcjach i o wszystkich obywatelach, którzy chcieli transakcji dokonać. Zapis w rejestrze podzielony był na pojedyncze strony i odbywał się po uiszczeniu niewielkiej opłaty księgowej. Co godzinę górnicy spotykali się w wyznaczonym miejscu pod dębem na rozstaju dróg, przynosząc ze sobą wszystkie zebrane przez siebie transakcje, żeby ustalić jak wyglądała ostatnia godzina historii transakcyjnej. Jednak każdy z nich posiadał inny zestaw propozycji transakcji do zapisania na nowej karcie, należało więc ustalić, które z nich powinny zostać uznane za obowiązujące na kolejnej kartce Krasnoludzkiego Rejestru. Rozwiązanie okazało się proste. Krasnale górnicy zdecydowali, że będą do swojego rejestru dodawać w pierwszej kolejności zapisy Krasnoludów, którym na tym najbardziej zależało, czyli te, które w formie licytacji za miejsce na kartce opłacały Krasnoludki – klienci. Zachętą do wykonywania tej pracy dla Krasnali – górników była opłata składająca się z dwóch części: sumy prowizji za zapis na danej kartce od najbardziej hojnych klientów oraz małej loterii.

O tym, który zestaw transakcji zostanie tym razem uznany przez wszystkie Krasnale, decydowała rozgrywana co godzinę gra w kości. Każdy z górników rzucał dziesięcioma kośćmi do gry. Górnik, który jako pierwszy wylosował 5 z 10 kostek z takim samym numerem, wygrywał. Jego zestaw transakcji zostawał sprawdzony, zatwierdzony i przepisany przez wszystkich innych górników do tak zwanego „Zdecentralizowanego Łańcucha Bloków Transakcyjnych". Na końcu zestawu transakcji zapisywany był wylosowany zestaw liczb. W ten sposób, każdy z górników posiadał dokładnie identyczny zapis historyczny wszystkich krasnoludowych transakcji. Te, które znalazły się w zwycięskim zestawie, otrzymywały miano „zatwierdzonych". Krasnal-górnik, któremu udało

się wygrać w danej godzinie, mógł dopisać sobie do konta wynagrodzenie w postaci nowych 50 krasnalcoinów (czyli waluty obowiązującej w świecie Krasnoludów) oraz wartość wszystkich opłat za zapisy transakcji, które znalazły się na danej kartce. Po zakończonym losowaniu (które w tym bajkowym przykładzie jest metaforą zabezpieczenia rejestru przed dodawaniem przez Krasnoludki swoich własnych, nieautoryzowanych transakcji, jako że nie wszyscy rachmistrzowie się znali i nie mogli mieć do siebie pełnego zaufania), górnicy zapisywali wynik poprzedniego losowania na początku nowej kartki z transakcjami i komponowali nowy „blok transakcyjny", czyli zapis zestawu transakcji. Ci, którym nie udało się wygrać, a posiadali jeszcze niezatwierdzone transakcje, mogli je zapisać w swoim nowym zestawie i próbować je „zatwierdzić" w kolejnym losowaniu za godzinę.

I w taki sposób, co godzinę, Krasnale uzgadniały nowy stan ich księgi rozrachunkowej, która istniała w wielu kopiach oraz była dostępna i transparentna dla każdego, a gnomy musiały palić swoje ogniska gdzie indziej.

Koniec.

A teraz wyobraźmy sobie, że w blockchainowym świecie:

- bloki to arkusze z zapisami transakcji Krasnali;
- górnicy to właściciele serwerów wykonujących obliczenia i potwierdzających historie stanów kont za pracę, otrzymujący wynagrodzenie w formie krasnalcoinów;
- wylosowany zestaw liczb na końcu listy transakcji to wynik funkcji hashującej, przeplatający się przez cały łańcuch kart z zapisami, gwarantujący jego integralność;
- zestaw wszystkich arkuszy z zapisami transakcji Krasnali (bloków) to kompletny rejestr rozproszony – blockchain.

Drogi Czytelniku, droga Czytelniczko – należą się Tobie gratulacje – właśnie zrozumiałeś/łaś, jak w uproszczeniu działa technologia blockchain.

Blockchain jest po prostu rozproszoną, w pełni zdecentralizowaną i nieustannie przyrastającą listą zapisów, które są sprawdzane, weryfikowane, a następnie grupowane w bloki. Każdy z takich bloków zawiera: znacznik czasu, wyliczoną kryptograficznie sumę kontrolną i sumę kontrolną poprzedniego bloku. Oznacza to, że w takim łańcuchu przechowywana jest cała historia przepływu danej monety – czy to stanu konta walutowego, czy np. lokacji produktu w magazynach na świecie. Dzięki tej konstrukcji blockchain bitcoina jest idealnie przejrzysty, co jeszcze bardziej zwiększa wiarygodność zawartych w nim zapisów. Można prześledzić kompletną historię każdego bitcoina lub jego części, od momentu stworzenia systemu aż do dziś. Zupełnie inaczej, niż w przypadku gotówki.

Być może jako dzieci zastanawialiście się kiedyś, ile osób miało w ręce dany banknot (w USA istnieje nawet bardzo popularna gra „Gdzie jest George", polegająca na zgłaszaniu na stronie internetowej www.wheresgeorge.com jednodolarówek ze swojego portfela i przy dużej dozie szczęścia – odkrywaniu, gdzie były poprzednio). Gdyby amerykańskie dolary były pieniądzem opartym na blockchainie, możliwe byłoby prześledzenie pełnej drogi każdego egzemplarza banknotu od momentu wydruku w mennicy, aż do chwili, w której znalazł się on w Twoim portfelu.

Mając już wyobrażenie o tej technologii warto zaznaczyć, że prace teoretyków kryptografów pojawiały się wraz z hipotezami dotyczącymi możliwych obszarów zastosowań już w 1991 roku. Pierwsza praktyczna implementacja koncepcji została wykonana właśnie jako mechanizm systemu waluty zdecentralizowanej przez Satoshiego Nakamoto[25], któremu świat zawdzięcza bitcoina, a samemu tajemniczemu autorowi (lub grupie autorów) postanowiliśmy poświęcić ostatni rozdział tej książki.

Największy superkomputer ludzkości i model emisji bitcoinów

Michał Grzybkowski

Nie sposób porównać siły stojącego za bitcoinem rejestru rozproszonego do czegokolwiek innego. Wielkość tego osiągnięcia sytuuje się poza skalą wszystkiego, co stworzyła do tej pory ludzkość. Zaznaczamy od razu, że jest to bez wątpienia najbardziej „uciążliwa" dla osób nie przepadających za matematyką część książki, dlatego pozwoliliśmy sobie najbardziej techniczne szczegóły pozamykać w ramkach, z wyraźnym ostrzeżeniem, że jest tam zapisana wiedza dla geeków. Jesteście gotowi? Zapraszamy Was w fascynującą podróż po świecie kryptowalut!

Jak już wiemy, liczba bitcoinów została od początku określona w algorytmie i nigdy nie będzie ich więcej niż 21 milionów sztuk[26]. Wiemy też, że każdy bitcoin składa się ze stu milionów „centów" zwanych potocznie satoshi. Oznacza to, że emisja bitcoinów trwa nadal, zgodnie z pewnym „planem" i przy udziale bitcoinowej społeczności – co postaramy się w tym rozdziale wytłumaczyć.

Informacja o tym, kiedy pojawi się w obiegu ostatni bitcoin, ma szczególne znaczenie dla rozumienia potencjalnej wartości BTC, który w przeciwieństwie do typowych walut odporny jest technologicznie na możliwości jej rozwodnienia

[25] https://en.bitcoin.it/wiki/Controlled_supply

[26] ibidem

i „dodrukowywania" pieniądza[27].

Żeby precyzyjnie udzielić odpowiedzi na pytanie dotyczące rozłożenia w czasie emisji bitcoinów, należy wyjaśnić model jego „pojawiania się" i to, skąd w ogóle bierze się w obiegu ta kryptowaluta, choć, jak wiemy, nie istnieje żadna instytucja odpowiedzialna za jej emisję.

Po pierwsze, jak już wspomniałem wcześniej, oprogramowanie odpowiedzialne za blockchain bitcoina zostało napisane w modelu open source. Oznacza to, że kody źródłowe całości projektu są publicznie dostępne i każdy zainteresowany sposobem działania tego systemu może dowolnie analizować zarówno każdy fragment kodu, jak i całość programu. Można założyć, że przez ponad dekadę działania systemu, tysiące, o ile nie dziesiątki tysięcy programistów[28] wypatrzyły i naprawiły wszelkie niedociągnięcia i błędy, czego dowodem jest fakt, że blockchain BTC działa nieprzerwanie przez cały ten czas i jest odporny na szereg typowych dla internetu ataków[29]. Taka publiczna weryfikacja jakości oraz ilość czasu, jaki upłynął od momentu uruchomienia tego otwartego systemu, jest najlepszą gwarancją stabilności i ciągłości działania.

Po drugie, sieć bitcoin jest infrastrukturą w pełni zdecentralizowaną, opartą o model sieci P2P (*peer-to-peer* to rozwinięcie angielskiego skrótu P2P, oznaczającego równy z równym). Jest to model wymiany informacji pomiędzy węzłami sieci, oparty o równorzędność uczestników. Dzięki temu, rejestr rozproszony bitcoina znajduje się w tysiącach pełnych kopii na świecie, a w razie jednoczesnej awarii wielu jego części – odbuduje się z ostatniej dostępnej kopii. Pełen węzeł transakcyjny jest tak naprawdę małym, ale kompletnym fragmentem idealnie rozproszonego „bitcoinowego banku".

W tradycyjnym systemie finansowym, w każdym państwie świata to bank emisyjny (obecnie rolę banków emisyjnych pełnią banki centralne) zajmuje się emisją pieniądza. Za emisję bitcoinowej waluty odpowiada natomiast publicznie znany algorytm, który „wypłaca" co pewien czas „wynagrodzenie" komputerom utrzymującym tę rozproszoną infrastrukturę[30].

---

[27] Dodrukowywanie pieniędzy przez rządy jest nazywane „podatkiem inflacyjnym" – podatek inflacyjny jest jednym ze źródeł pozyskiwania renty emisyjnej. Jest to dochód, jaki rząd otrzymuje z inflacji, przy założeniu, że dochód realny oraz produkcja są stałe. Jest to przyczyną powstania takiej sytuacji, w której dochody gospodarstw domowych i przedsiębiorstw się zmniejszają, natomiast podatki liczone od wartości nominalnej pozostają takie same. Przyczyną takiego zjawiska jest próba finansowania przez państwo deficytu budżetowego poprzez dodrukowanie pieniędzy. Gdy dochód realny jest stały, wzrost nominalnej podaży pieniądza powoduje wzrost cen – inflację. Jednak w tej sytuacji jest ona dla państwa niewątpliwie korzystna, gdyż zmniejsza się wartość gotówki, czyli realna wartość nieoprocentowanej części długu. Stopa inflacji staje się zatem stopą podatkową, a realna wartość gotówki jest podstawą opodatkowania.

[28] Rozwój oprogramowania bitcoina można śledzić na Github – https://github.com/bitcoin/bitcoin

[29] Ataki przeciążeniowe typu DDoS na węzły sieci, ataki spamerskie, ataki polegające na wyłączaniu części sieci bitcoin etc.

[30] https://en.wikipedia.org/wiki/Bitcoin

Komputery będące jej składowymi, połączone są siecią internetową i używają identycznego oprogramowania do rozwiązywania problemów matematycznych, w zamian otrzymując pewną liczbę cyfrowych monet za wykonaną pracę. Ponieważ obliczenia te są wyjątkowo mozolne i ze względu na ich ilość, niewyobrażalnie pracochłonne[31], przyjęło się nazywać osoby udostępniające swoją moc obliczeniową na cele tego projektu „górnikami", urządzenia (domowe komputery, serwery czy specjalistyczne maszyny) „koparkami", w serwerowniach zwanych „kopalniami", a federacje „górników", którzy, aby zwiększyć skalę działania, rozwiązują te matematyczne zadania łącząc siły – „pulami górniczymi".

Algorytm sieci zapewnia bardzo atrakcyjny dla uczestników sposób emisji „pieniądza" (bitcoinów), a zarazem zachęca coraz więcej osób do „kopania" i w ten sposób umacniania trwałości i skali systemu. Jest to także przykład ekonomicznej funkcji produkcji[32] w czystej postaci – wszyscy górnicy mają szansę otrzymać wynagrodzenie za pracę na rzecz systemu adekwatną do udostępnianej mocy obliczeniowej. Mają oni także żywotny interes w otrzymywaniu wynagrodzenia w bitcoinach za wykonane obliczenia. Im więcej odprowadzanej przez górników mocy obliczeniowej, tym bezpieczniejsza i stabilniejsza sieć.

A mówimy o skali, która jest ciężka do wyobrażenia nawet dla informatyków. Już na koniec roku 2013 Forbes wykazał, że moc obliczeniowa sieci bitcoinowego blockchaina przewyższa 256-krotnie (!) sumę mocy obliczeniowej wszyskich komputerów ze światowej listy TOP 500, wyrażonej we FLOPSach[33] (*Floating Point Operations Per Second*), listy największych superkomputerów świata, zwanej Top 500. Moc bitcoinowego blockchaina wynosiła wtedy 1 exaFLOPS (10^18), czyli mniej więcej tysiąc petaFLOPSów[34].

W maju 2021 roku moc sieci obliczeniowej bitcoina wynosiła prawie dwieście milionów exahashy (10^18)[35]. Żeby wyobrazić sobie tę skalę, przytoczę słowa Erika P. DeBenedictisa[36] z amerykańskiego laboratorium *Sandia National*

---

[31] Ken Shirriff, w swoim filmiku zamieszczonym na Youtube 28 września 2014 roku pokazał, że bitcoiny można „kopać" nawet używając papieru i ołówka! – jest to oczywiście możliwe, ale skrajnie niepraktyczne: https://www.youtube.com/watch?v=y3dqhixzGVo

[32] Funkcja produkcji: ekonomiczna zależność między nakładami czynników produkcji: pracy (L) i kapitału (K) a wielkością produkcji (Q), z reguły rozważana w odniesieniu do przedsiębiorstwa. Najczęściej funkcja produkcji ma postać: Q = f(K, L), gdzie: Q — skala produkcji, K — nakłady kapitału, L — zatrudnienie. (zródło: https://encyklopedia.pwn.pl/haslo/funkcja-produkcji;3903282.html)

[33] Floating Point Operations Per Second – liczba operacji zmiennoprzecinkowych na sekundę. Jest jednostką mocy obliczeniowej komputerów, używaną szczególnie w zastosowaniach naukowych. Jest bardziej uniwersalna od wcześniej używanej jednostki MIPS, oznaczającej liczbę instrukcji procesora wykonanych na sekundę.

[34] https://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/?sh=24d9b4ce6e5e

[35] https://blockchain.info/charts/hash-rate

[36] Erik DeBenedictis jest pracownikiem Sandia National Laboratories, specjalistą od budowy superkomputerów. Pracował między innymi przy projekcie superkomputera ASCI Red Storm.