

KRYPTOWALUTY

Michał Grzybowski

Szczepan Bentyn

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

<i>Wstęp</i>	11
Najdroższa pizza świata, czyli dla kogo jest ta książka?	13
Organizacja książki „Kryptowaluty”	16
Nowy Początek	17

TECHNOLOGIA

<i>Finansowe tsunami</i>	23
Blockchain, czyli narodziny rejestrów rozproszonych	24
Bajka o blockchainie	25
Największy superkomputer ludzkości i model emisji bitcoinów	28
<i>Petahashe</i> , czyli dowód pracy górnika	34
Transakcje w sieci bitcoin	40
Z wizytą w kopalni bitcoinów.	42
Krypto-mining, czyli rachunek rentowności górnictwa	49
Wspomnienia okradzionego górnika	53

<i>Funkcje i role kryptowalut</i>	56
Kryptowaluty wymienne	56
Waluty inflacyjne i o stałej ilości monet	58
Waluty anonimowe	59
Inteligentne kontrakty i organizacje zdecentralizowane	62
Tokeny, czyli jednostki rozliczeniowe	63
ICO, czyli Initial Coin Offering	65
The DAO, czyli <i>Zdecentralizowana Autonomiczna Organizacja</i>	66
Tokeny personalne, czyli stokenizuj się!	68
Lightning network	73
Altcoiny	75
Shitcoiny, jokecoiny, spamcoiny oraz martwe monety	76
Klasyfikacja kryptowalut ze względu na budowę rejestrów rozproszonych	81
Piramidy finansowe podszywające się pod kryptowaluty	82

<i>Zagrożenia i wyzwania</i>	84
Własność	84
Technologia	85
Ataki ekonomiczne, czyli stare sztuczki rekinów finansowych	90
Ryzyka regulacyjne	91
Upadki i możliwe manipulacje giełd kryptowalutowych	92
Ekologia i energetyka	94

<i>Czym jest pieniądz fiducjarny?</i>	96
---	----

PRZYSZŁOŚĆ

<i>Narodziny Nowego Porządku Świata</i>	105
Logistyka	106
Organizacje charytatywne i świadczenia społeczne	108
Venture Capital	109
Demokracja i polityka	112
Systemy rządowe i administracja publiczna	118
Multimedia i prawa autorskie	121
Gospodarka rolna	124
Medycyna	125
Turystyka	129
Cyberbezpieczeństwo oraz <i>Internet Rzeczy</i>	130
Energetyka	137
Umierające zawody	138
Konsekwencje ekonomiczne w gospodarce światowej	146
Upadek państwowości	149
Wpływ na geografę	155
Rynki predykcyjne	159

<i>Ile wart będzie bitcoin?</i>	163
Słowo do inwestorów	165
Wartość bitcoina w kontekście reszty rynku finansowego	166
Ujęcie adopcyjne	167
Analiza statystyczna	173
Silne korelacje	173
Trendy i modele statystyczne	180
Analiza techniczna	184
Prawo Metcalfe'a	188
Metoda delficka	190
Ujęcie fundamentalne	191

PRAKTYCZNY PORADNIK 195

<i>Kupujemy pierwszego bitcoina</i>	197
Być bardziej bankowym niż bank, czyli podstawy podstaw	198
Rodzaje portfeli	199
Bezpieczeństwo zaczyna się u podstaw	202

<i>Transakcje kryptowalutowe</i>	210
Giełdy krypto-FIAT	210
Giełdy krypto-krypto	213
Kantory online	214
<i>Shapeshift</i>	214
Giełdy sąsiedzkie	215
Giełdy zdecentralizowane	215
Atomic swap	216
Zewnętrzne i wewnętrzne koszty transakcji	216
Portfele na kryptowaluty w wersji online	217
Portfele sprzętowe	218
Portfele aplikacyjne	219
Portfele „papierowe”	220

Siedem przykazań głównych	221
Gdzie można płacić kryptowalutami?	222

<i>Przegląd wybranych kryptowalut</i>	224
Bitcoin	224
Litecoin	226
Ethereum	228
Bitcoin Cash	230
Monero	232
Dash	234
TOP 50 kryptowalut w jednym zdaniu	236

<i>Kryptowaluty w świetle prawa</i>	238
Kryptowaluta w polskim prawie	240
Kryptowaluta, a podatki	242

<i>Kim NIE jest Satoshi Nakamoto?</i>	253
---------------------------------------	-----

<i>Zakończenie</i>	263
Jak powstała ta książka?	265
Podziękowania	270

<i>Tokeny personalne autorów</i>	274
----------------------------------	-----

<i>Słowniczek</i>	276
-------------------	-----

<i>Indeks</i>	279
---------------	-----

<i>Patronaty i partnerzy</i>	285
------------------------------	-----

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

Najdroższa pizza świata, czyli dla kogo jest ta książka?

13

Wstęp

Pierwsze bitcoiny zostały użyte do transakcji handlowej 22 maja 2010 roku przez Laszlo Hanyecz'a, który za ok. 10 tys. BTC¹ kupił od znajomego z internetowego forum dyskusyjnego² – Jeremiego „Jercosa” Sturdivanta – dwie pizze. Gdyby Laszlo postanowił tego dnia zapłacić gotówką, a swoje bitcoiny pozostawić w cyfrowym portfelu, ich wartość pod koniec 2017 roku wyniosłaby prawie 132 miliony dolarów³. Biorąc pod uwagę dynamikę zmian wartości, technologie, które wspierają integralność kryptowalut oraz zwykłe prawa mikroekonomii, nie jest wykluczone, że pizza, którą zjadło kilka lat temu dwóch entuzjastów technologii, na zawsze zapisze się jako najdroższy posiłek w historii świata.

Niecałe siedem lat później, w drugiej połowie 2017 r., miały miejsce następujące wydarzenia:

- w kwietniu 2017 r. Japonia zalegalizowała bitcoina traktując go jak normalny środek płatniczy, tworząc tym samym potężny popyt na tę kryptowalutę. W pierwszym tygodniu zaczęło rozliczać się nią 260 tys. punktów handlowych;
- Australia ogłosiła, że od 1 lipca 2017 r. zacznie traktować bitcoina jak każdą inną walutę, legalizując faktyczny obrót;
- SEC czyli *US Securities and Exchange Commission* – amerykańska komisja nadzoru finansowego, po wcześniejszym odrzuceniu propozycji braci Winklevoss⁴ związanych z projektem uruchomienia funduszu inwestycyjnego opartego na bitcoinach, ogłosiła możliwość ponownego przeanalizowania swojej decyzji⁵;
- największy rosyjski sklep internetowy⁶ – *Ulmart* zadeklarował, że jest gotów przyjmować płatności w kryptowalutach po tym, jak Rosja ogłosiła plany dotyczące legalizacji bitcoina;

¹ BTC to powszechnie używany skrót dla kryptowaluty bitcoin

² www.bitcointalk.org

³ Zagregowana wycena kryptowaluty bitcoin, będąca średnią głównych giełd wymiany kryptowalut z coinmarketcap.com, dostęp z dnia 31 grudnia 2017

⁴ Założyciele facebooka (wraz z Markiem Zuckerbergiem)

⁵ www.cnbc.com/2017/04/26/bitcoin-price-sec-winklevoss-etf-review.html

⁶ www.newsBTC.com/2017/05/11/russias-largest-online-retailer-ulmart-plans-accept-bitcoin-september-2017/

- największy japoński bank⁷ ogłosił, że przystępuje do konsorcjum *Ripple* (XRP) – międzynarodowego i międzybankowego systemu rozliczeń opartego o technologię „blockchain”, będącą fundamentem budowy i działania kryptowalut;
- kapitalizacja najważniejszych, w pełni wymieniających na tradycyjne pieniądze kryptowalut, będących w obiegu, w grudniu 2017 r. przekroczyła wartość 600 miliardów dolarów⁸, a strona internetowa coinmarketcap.com będąca źródłem informacji o cenach kryptowalut była najczęściej odwiedzaną na świecie w kategorii witryn z kategorii finanse i inwestycje⁹.

Ale wcześniej stała się też rzecz, bez której nie byłoby możliwe nadanie tej książce tak odważnego tytułu – 23 marca 2017 roku, na konferencji *Consensus 2017*, odbywającej się w Nowym Jorku, ponad 55 firm i organizacji z 22 krajów, reprezentujących ponad 83% mocy obliczeniowej stojącej za infrastrukturą bitcoina, wypracowało porozumienie techniczne dotyczące zmiany protokołu jego działania, zwiększającego pojemność transakcyjną systemu i przyszłą łatwą integrację mikropłatności¹⁰.

Warto także wspomnieć o jeszcze jednej przełomowej zmianie – w całym 2017 roku kapitalizacja rynku kryptowalutowego zaczęła dynamicznie przybierać na masie.

Wydarzenia przełomu 2017 r. cechują się jednak czymś nowym – JF Kennedy lubił powtarzać, że „przyływ unosi wszystkie łodzie”¹¹ – kryptowaluty przestały ze sobą rywalizować o względy dolarów, euro czy funtów. W ekosystemach takich jak bitcoin, ethereum, monero, dash czy inne, pojawiły się pierwsze większe pieniądze. Ludzkość stanęła przed faktem dokonanym – nie czekając na rządy, banki czy regulatorów – rozpoczęła się masowa adopcja. Kryptowaluty trafiły pod strzechy, zaś technologia stojąca za tą rewolucją, czyli tzw. „rejestr rozproszony”, z angielskiego – blockchain, swoją potęgą przyćmił wszystko, co do tej pory widziała ludzkość, z wynalezieniem internetu łącznie. I o tym właśnie przeczytasz w tej książce.

Jeżeli zewsząd słyszysz o inwestycjach w kryptowaluty, chcesz poznać i przede wszystkim zrozumieć nowe medium, w którym niebawem wyceniane

⁷ finance.yahoo.com/news/75-banks-now-ripples-blockchain-network-162939601.html

⁸ coinmarketcap.com

⁹ www.similarweb.com/top-websites/category/finance/investing

¹⁰ Porozumienie zwane *New York Bitcoin Scaling Agreement* zostało zrealizowane potowicznie, ale w części najistotniejszej dla rozwoju bitcoina, czyli implementacji protokołu *SegWit*, która nastąpiła 24 sierpnia 2017 en.wikipedia.org/wiki/SegWit

¹¹ Ang.: „A rising tide lifts all boats”

będą wszelkie dobra materialne, od porannej kawy po nieruchomości, a razem potrafiś samodzielnie korzystać chociażby z bankowości internetowej, ta książka jest dla Ciebie. Chcielibyśmy w niej Tobie pokazać, jak w praktyce kupić za przysłowiowego dolara coś z koszyka kryptowalut, zarówno jako inwestor, użytkownik codziennych mikropłatności, czy przedsiębiorca planujący wprowadzić obsługę płatności w takiej formie w swoim sklepie internetowym. Przede wszystkim natomiast chcielibyśmy podzielić się z Tobą wiedzą, która pozwoli zrozumieć nadciągającą rewolucję oraz poznać sposoby poruszania się w nowych obszarach zagadnień w sposób bezpieczny, na co uważać i gdzie szukać pomocy, jeśli coś pójdzie nie tak.

Jeżeli zaś pojęcia takie jak „zabendowany kernel” czy „deployowanie farmy serwerów przez API” są dla Ciebie chlebem powszednim, to szczegóły techniczne zawarte w tej publikacji będą dla Ciebie prawdopodobnie nudne i jesteśmy przekonani, że jesteś co najmniej geekiem, o ile nie nerdem i o bitcoinie słyszałeś 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 bezwzględnie 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 zachęcającą do dalszych poszukiwań.

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

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

Technologia – w pierwszych rozdziałach omawiamy w przystępny sposób działania stojącej za bitcoinem technologii rejestru rozproszonego czyli „blockchain”. 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 omawiamy 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 implikacjami, jakie niesie za sobą powszechna adaptacja technologii rejestrów rozproszonych w szeregu gałęzi gospodarki. Omawiamy kolosalne znaczenie blockchain’a, 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 rewolucję w poszczególnych sektorach gospodarki, od logistyki po finanse. Mierzmy 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.

Praktyczny poradnik – w ostatnich rozdziałach postaramy się poprowadzić czytelnika/czkę 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 kryptowalut, począwszy od przechowywania cyfrowych wartości, przez transakcje kryptowalutowe, po analizę prawną kryptowalut i związane z nią regulacje prawno-skarbowe w naszym kraju (dodatek do wydania polskiego).

Dodatkowo, ze względu na fakt, że książka „Kryptowaluty” pisana jest wspólnie przez dwóch autorów – Michała Grzybrowskiego i Szczepana Benty – w końcowym podsumowaniu rozdziałów 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 Grzybowski–Guzek.

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

Nowy Początek

Kryptowaluty, bitcoin, litecoin, ethereum, monero... i inne. Z jednej strony ostrzegawcze sygnały – bańka spekulacyjna (uważajcie!), z drugiej zaś strony rozgrzani do białości, ortodoksyjni ewangeliciści, którzy z pianą na ustach wieszczą rychły kataklizm, 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 bitcoiny¹², inne bezradnie ścigają posiadaczy¹³, kolejne udają, że tematu nie ma, skutecznie go ignorując, a ostania 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 tzw. Trzeciego Świata,¹⁴ traktowane do tej pory po macoszemu przez wielkie światowe gospodarki, 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?

¹² money.cnn.com/interactive/technology/where-is-bitcoin-legal/

¹³ en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory

¹⁴ www.cryptocoinsnews.com/africa-ripped-bitcoin/

A teraz zbierzmy fakty. Wyobraźmy sobie globalny, w pełni zdecentralizowany, odporny na awarie i niemożliwy do zablokowania czy kontrolowania system rozliczeniowy. 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 inflację¹⁵ (brak możliwości „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 wystanie e-maila. Lub postawienie kropki na końcu tego zdania.

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. Oczywiście 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 takich 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 niż pół tysiąca 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*¹⁶. Odporność na ataki hakerów, czy błędy w oprogramowaniu praktycznie wyeliminowane dzięki temu, że system został zweryfikowany przez setki, o ile nie

¹⁵ Dotyczy bitcoina, w dalszej części książki omawiamy kryptowaluty nieinflacyjne.

¹⁶ *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.

tysiące specjalistów, a najlepszym dowodem jest to, że działa nieprzerwanie już od ponad dziewięciu lat¹⁷!

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 smartfonie¹⁸. A na koniec dodajmy dość unikatową cechę. Niektóre z kryptowalut pozwalają zapewnić daleko idącą lub absolutnie pełną anonimowość¹⁹. 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 wymaze 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 XXI finansowego wieku!

Michał Grzybkowski & Szczepan Bentyn

¹⁷ Pierwszy blok transakcyjny bitcoin został wykopany 3 stycznia 2009 r.

¹⁸ Przykłady w dalszej części książki, w rozdziale „Praktyczny poradnik”.

¹⁹ Dotyczy kryptowaluty monero.

Internet skomunikował świat, blockchain go rozliczy

TECHNOLOGIA

Zrozumieć blockchain

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

Finansowe tsunami

23

Cała 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. (...)

Spółeczeństwo nie zasługuje na nic innego!

Fragment wypowiedzi Erika Vorheesa²⁰,
założyciela i prezesa firmy ShapeShift.

²⁰ 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

Słowo „rewolucja” wywodzi się z łacińskiego – *revolutio* – i w dosłownym tłumaczeniu oznacza „przewrót” lub przynajmniej znaczącą zmianę, która zachodzi w stosunkowo krótkim czasie²¹. Bardzo lubię tę definicję, bo oddaje dokładne znaczenie i wagę momentu, w którym następuje wielka zmiana biegu wydarzeń. Bez wątplenia takim momentem dla ludzkości było zupełnie nieoczekiwane pojawienie się tak zwanego *distributed ledger*²², 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 zamierzczłych i regulowano w nich szereg aktywności, jak chociażby prawa do nieruchomości czy różnorakie rozliczenia finansowe. Pierwotnie zapisy prowadzono na zwójach 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 „rejestru rozproszonego” pojawił się na świecie zupełnie niespodziewanie, niejako przez przypadek, w formie pierwszej skutecznie działającej implementacji technologii pod nazwą „blockchain” stojącej za technologią kryptowaluty bitcoin.

Rejestr rozproszony jest zdecentralizowaną, rozproszoną w wielu kopiach, współdzieloną bazą danych. Dokument ten funkcjonuje na równych prawach pomiędzy wszystkimi uczestnikami danego systemu (osobami, przedsiębiorstwami, krajami czy instytucjami) i nie podlega centralnemu nadzorowi czy kontroli. 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 danych w nim zawartych, oparte o silną kryptografię. Zdarza się, że pojęcia „blockchain” i „rejestru rozproszonego” używane są zamiennie i jest to błąd logiczny. Nie każdy rejestr rozproszony może być nazywany blockchainem (czyli np. infrastrukturą kryptowaluty

²¹ Def. rewolucji – pl.wikipedia

²² Ang.: „rejestru rozproszony”

bitcoin), natomiast bitcoinowy blockchain jest szczególnym, a zarazem pierwszym w historii wdrożeniem koncepcji rejestru rozproszonego.

Zdajemy sobie sprawę, że nieuchronnie przybliżamy Czytelnika/czkę 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 zmierzanie 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 też przygotowaliśmy dwa równorzędne rozdziały opisujące z grubsza potęgę rejestru rozproszonego.

Humanistów i humanistki zapraszamy do przeczytania „bajki o blockchainie”.

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.

Bajka o blockchainie

Od pewnego czasu słowo „blockchain”, czyli w dosłownym tłumaczeniu „łańcuch bloków” jest odmieniany przez wszystkie możliwe przypadki i formy, będąc często używanym zamiennie ze słowem bitcoin. Jak już wspomnieliśmy, jest to daleko idące uproszczenie. Bitcoin nie może istnieć bez technologii blockchainowej, natomiast, jak się zapewne szybko przekonamy, systemy oparte na łańcuchach bloków zdominują szereg²³, o ile nie większość znanych nam w tej chwili gałęzi gospodarki. Blockchain, dzięki swoim genialnym właściwościom, zrewolucjonizuje branże takie jak: logistyka, bankowość, finanse, 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.

Dawno, dawno temu...

²³ Więcej o tym w rozdziale „Przyszłość”.