młody TECHNIK
Istnieje od 1932 roku

CHERCHEZ LA FEMME: Ada Lovelace

Pierwsza programistka świata. Sto lat przed pierwszym komputerem

czerwiec • 06/2026
www.mlodytechnik.pl

Tu przejrzysz i kupisz ten numer

NEWS 24/7
Przeglądaj codziennie swoim smartfonie

młody m.technik

Ciekawi świata są zawsze młodzi

KRYPTOWALUTY

Szemrany epizod czy świetlana przyszłość?

Science fiction w „Młodym Techniku”

M.P. Hardy: Heweliusz-77

ISSN 0462-9760 Indeks 365408
06
9 770462 976267
cena: 19,90 zł (w tym 8% VAT)

pakiet promocyjny KOCHAM SZACHY
7 e-booków z rabatem 50%

pakiet promocyjny NA WARSZTACIE
9 e-booków z rabatem 50%

Dla prenumeratorów – 30% rabatu!
Promocja Internetowa – w formularzu zamówienia online zaznacz pole
„Jestem prenumeratorem wydawnictwa AVT, kupuję ze zniżką”
i podaj swój numer prenumeraty.

www.UlubionyKiosk.pl

Temat okładkowy
Bitcoin obchodzi siedemnaste urodziny. W tym czasie z eksperymentu cypherpunków stał się aktywem za dwa biliony dolarów – i walutą rozliczeń przestępców, państw-pariasów, ofiar zniszczonych giełd. Co z idei Satoshiego naprawdę się sprawdziło?

Gorzko słodka wolność

Zaczęło się skromnie, od publikacji: „Bitcoin: A Peer-to-Peer Electronic Cash System". Elektroniczny system pieniądza, w którym płatnik wysyła płatność bezpośrednio do odbiorcy, bez instytucji finansowej pośredniczącej. Bez banku. Bez nadzorcy. Bez zaufanej trzeciej strony, która może odmówić nam obsługi, która może zablokować nam konto, która może zmusić nas do ujawnienia historii. Która wreszcie może zniknąć wraz z naszymi pieniędzmi. Idea była polityczna, choć Satoshi Nakamoto, autor tej publikacji, rzadko mówił o niej politycznie. Cypherpunki, z których kręgu wyrósł projekt, wierzyli, że prawo do prywatnej komunikacji to fundament wolności. Bitcoin był naturalnym rozszerzeniem tej idei: jeśli można szyfrować rozmowy, dlaczego nie pieniądz? Pierwsza linijka kodu Genesis Block z 3 stycznia 2009 roku zawiera nagłówek z gazety: „Kanclerz na progu kolejnego ratowania banków". Sygnał był jasny. To miała być alternatywa dla świata, w którym banki ratują same siebie pieniędzmi obywateli.

Siedemnaście lat później rachunek wygląda tak. Ponad dziewięćdziesiąt pięć procent posiadaczy bitcoinów trzyma je na giełdach – czyli u pośredników, których Satoshi chciał obejść. Dodajmy, że są to pośrednicy mniej godni zaufania niż banki. Właśnie obserwujemy upadek Zondacrypto, największej w Polsce giełdy, jak się okazuje powiązanej ze zorganizowaną grupą przestępczą. Trzydzieści tysięcy klientów straciło dostęp do swoich pieniędzy. Takich historii krypto-świat doczekał się już kilka razy. Lista szemranych dokonań świata kryptowlut jest długa. Według tegorocznego raportu Chainalysis nielegalne adresy otrzymały w 2025 roku co najmniej sto pięćdziesiąt cztery miliardy dolarów – wzrost o 162 procent rok do roku. Stablecoiny są walutą darknet markets, ransomware, oszustw inwestycyjnych. Korea Północna ukradła z giełd kryptowalut dwa miliardy dolarów, finansując program rakietowy. A od ubiegłego września Rosja oficjalnie używa kryptowaluty do obchodzenia sankcji – token A7A5, otwarty osobiście przez Putina, w pierwszym roku przepuścił ponad dziewięćdziesiąt miliardów dolarów rozliczeń, głównie z Chinami, w tym za części do dronów używanych przeciwko Ukrainie.

To są fakty. To samo narzędzie, które w Argentynie pozwala chronić oszczędności przed inflacją, w Rosji pozwala finansować wojnę. Ta sama technologia, te same właściwości – w 2009 roku obiecane jako wyzwolenie, dziś działa jako infrastruktura złoczyńców różnej maści.

Czy to porażka idei? Tego nie umiem powiedzieć z pewnością. Wynalazcy rzadko otrzymują od historii instrukcję obsługi własnych wynalazków. Alfred Nobel projektował dynamit jako materiał górniczy. Bracia Wright nie myśleli o nalotach na Drezno. Tim Berners-Lee, gdy pisał pierwszy serwer WWW, nie zamierzał stworzyć infrastruktury dezinformacji. Każda potężna technologia, kiedy raz wejdzie do obiegu, przestaje należeć do swojego twórcy.

Bitcoin wszedł do obiegu szesnaście lat temu. Satoshi Nakamoto zniknął w 2011 roku – nikt nie wie kim był, ani czy żyje. Jego idea żyje dalej, ale na własnych zasadach. Jest wolnym pieniądzem – wolnym także dla tych, których wolność nas niepokoi.

Pytanie postawione w tytule Tematu numeru– szemrany epizod czy świetlana przyszłość? – nie ma jednoznacznej odpowiedzi. Bitcoin jest jednym i drugim. Świetlanym dorobkiem matematycznym i szemraną praktyką społeczną. Wynalazkiem, który zrobił, co miał zrobić – i kilka rzeczy obok. Choć społeczna rola kryptowalut jest niejednoznaczna, to absolutnie jednoznacznie rozumiemy rolę „Młodego Technika" – wyjaśnić fascynujące mechanizmy tego wynalazku.

Mam nadzieję, że osiem części Tematu numeru pomoże Czytelnikowi zrozumieć jak działają kryptowaluty. Dla naszych Czytelników wiedza jest wartością samą w sobie. A tym Czytelnikom, którzy zdecydują się praktycznie wejść w świat kryptowalut polecamy najważniejszą frazę z całego Tematu numeru: **„Not your keys, not your coins" – kto ma klucze, ten ma pieniądze**.

Wiesław Marciniak

PRENUMERATA

Czytaj więcej, płać mniej!

Zyskaj 15% rabatu

W prenumeracie tylko
~~238,80 zł~~
203,00 zł
/roczna prenumerata drukowana

Dlaczego warto?

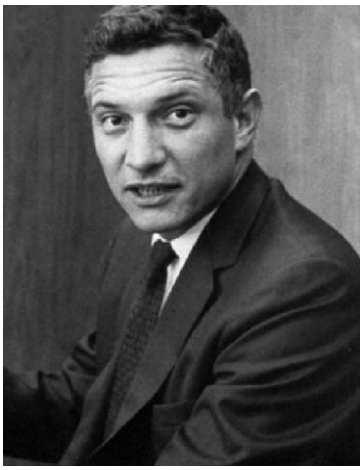
- Dostawa **gratis** prosto do Twojego domu
- Tylko dla prenumeratorów: **niższe ceny** przy zakupie czasopism na UlubionyKiosk.pl
- Pakiet 2w1 (papier + e-wydania): **–80%** na równoległą e-prenumeratę PDF

Szczegóły na UlubionyKiosk.pl/promocje

Zamów prenumeratę na **www.UlubionyKiosk.pl**
lub zeskanuj kod QR i zaprenumeruj w 1 minutę

AVT-Korporacja sp. z o.o., ul. Leszczynowa 11, 03–197 Warszawa
prenumerata@avt.pl | 22 257 84 22 (godz. 10.00–14.00)
rachunek bankowy: ING Bank Śląski 18 1050 1012 1000 0024 3173 1013

Spis treści



Miesięcznik „Młody Technik” (12 numerów w roku) wydawany przez Wydawnictwo AVT

Adres wydawnictwa:
03–197 Warszawa, ul. Leszczynowa 11,
tel. 22 257 84 99, faks: 22 257 84 00,
http://www.avt.pl, avt@avt.pl

Redaktor Naczelny:
Wiesław Marciniak
wiesław.marciniak@avt.pl

Sekretarz redakcji:
Dariusz Welik
dariusz.welik@avt.pl

Kontakt z redakcją:
mt@mt.com.pl
http://www.mlodytechnik.pl
http://facebook.com/magazynMlodyTechnik

Dział Reklamy:
reklama@mt.com.pl

DTP: MAD Sp. z o.o.

Prenumerata:
www.ulubionykiosk.pl
tel. 22 257 84 22 (godz. 10.00–14.00)
e-mail: prenumerata@avt.pl

Redakcja nie ponosi odpowiedzialności za treści reklam i ogłoszeń zamieszczonych w numerze.

Coś Cię poruszyło? Chcesz podzielić się z Redakcją i Czytelnikami MT swoją opinią, wiedzą, komentarzem? Wyślij e-mail na adres: **redakcja@mt.com.pl** lub list na adres: **ul. Leszczynowa 11, 03–197 Warszawa**.

Co z zasługami Polaków?

W serii wydań specjalnych „Młodego Technika" pod tytułem „Kurs praktyczny AI" znalazł się akapit:

Historia sztucznej inteligencji zaczyna się właściwie od prostego pytania, które w 1950 roku zadał Alan Turing: „Czy maszyny potrafią myśleć?" Brytyjski matematyk, bohater wojenny, który złamał kody niemieckiej Enigmy, był przekonany, że odpowiedź brzmi „tak" – tyle tylko, że trzeba odpowiednio przeformułować pytanie.

Na ten akapit zareagował Czytelnik następującym listem:

Kody Enigmy złamali polscy matematycy Rejewski, Różycki i Zygalski, studenci Uniwersytetu Poznańskiego już w 1932 roku, proszę nie wprowadzać Czytelników w błąd! Nie wpisujcie się Państwo w obecnie ogólną narrację umniejszania wartości i zasług państwa Polskiego i Polaków...

Przemysław

Red. Oczywiście wiemy o roli polskich matematyków w złamaniu kodu Enigmy i jest nam przykro, że zostawiliśmy cytowane zdanie bez komentarza, chociaż tematem nie była Enigma, a to zdanie pojawiło się tylko w skrótowej prezentacji postaci Turinga. Oto co na ten temat mówi nam AI:

Kto złamał kod Enigmy: polscy matematycy czy Turing?

Szyfr Enigmy został złamany najpierw przez polskich matematyków, a Alan Turing rozwinął ich metody, aby łamać znacznie bardziej skomplikowane, wojenne wersje niemieckich depesz. Sukces ten był efektem pracy obu stron, opartym na zasadzie sztafety naukowej.

Rola polskich matematyków (lata 1932–1939)

Polacy jako pierwsi na świecie dokonali przełomu w walce z Enigmą. Zamiast metod lingwistycznych, użyli do tego zaawansowanej matematyki.

Marian Rejewski: W grudniu 1932 roku odtworzył strukturę wewnętrzną Enigmy za pomocą teorii grup.

Zespół: Pracował w składzie Marian Rejewski, Jerzy Różycki oraz Henryk Zygalski.

Innowacje: Polacy zbudowali tzw. bombę kryptologiczną oraz płachty Zygalskiego do automatycznego odnajdywania kluczy szyfru.

Przekazanie wiedzy: W lipcu 1939 roku, w obliczu zbliżającej się wojny, Polacy przekazali repliki Enigmy oraz całą swoją dokumentację wywiadom Francji i Wielkiej Brytanii.

Rola Alana Turinga (Lata 1939–1945)

Brytyjski matematyk Alan Turing objął pałeczkę w ośrodku Bletchley Park, bazując bezpośrednio na polskim odkryciu.

Nowe wyzwania: Niemcy drastycznie skomplikowali system szyfrowania tuż przed wojną, dodając kolejne wirniki.

Bomba Turinga: Brytyjczyk zaprojektował własną, znacznie potężniejszą maszynę elektromechaniczną, inspirowaną wcześniejszą bombą Rejewskiego.

Skala przemysłowa: Umożliwiła ona masowe odczytywanie tysięcy niemieckich depesz w czasie rzeczywistym, co uratowało miliony istnień ludzkich.

Podsumowując: Polacy znaleźli teoretyczny klucz do Enigmy, a Turing stworzył system, który pozwolił utrzymać ten sukces przeciwko stale ulepszanej maszynie.

Linux w każdej kieszeni – a kto o tym wie?

Artykuł o Linusie Torvaldsie był jedną z lepszych lektur w MT od dłuższego czasu. Mam jednak drobne uzupełnienie, które uważam za ważne. Napisaliście, że Linux „dominuje w serwerach" i „jest sercem internetu". To wszystko prawda. Ale brakuje jednego zdania, które zmienia cały obraz: Android – system operacyjny zainstalowany na ponad trzech miliardach smartfonów – jest oparty na jądrze Linux.

Każdy, kto czyta ten artykuł na telefonie, czyta go na systemie, którego fundamenty napisał Torvalds jako 21-latek w swoim pokoju w Helsinkach w 1991 roku. Każdy, kto robi zdjęcia telefonem, obsługuje kamerę zarządzaną przez sterowniki Linux. Supersatellity Starlink również działają na Linuksie. Prawdopodobnie większość czytelników MT używa Linuksa kilkaset razy dziennie, nie zdając sobie z tego sprawy.

To chyba najlepszy dowod, że open source nie jest ideologią dla geeków, lecz infrastrukturą współczesnego świata. Warto było to powiedzieć wprost.

Paweł Osiński, programista

Kiedy wrócimy na Księżyc – i po co?

Czytam MT od lat siedemdziesiątych i pamiętam numer, w którym opisywaliście Apollo 11. Mam teraz 68 lat i zadaję sobie pytanie: czy dożyję chwili, gdy człowiek ponownie stanie na Księżycu? Misja Artemis jest opóźniona od lat, kosztuje fortuny i bywa wymieniana w tych samych zdaniach co fuzja termojądrowa – czyli „powstanie za dwadzieścia lat".

Ale patrząc na to, co robią prywatne firmy: SpaceX ze Starshipem, Blue Origin z New Glenn, japoński lander SLIM, indyjska Chandrayaan-3 – coś się naprawdę dzieje. Pytanie, które mnie nurtuje, nie brzmi jednak „kiedy,"tylko „po co". W debacie publicznej rzadko pada uczciwa odpowiedź. Zasoby helu-3 dla fuzji? Baza wypadowa w stronę Marsa? Prestiż polityczny? A może zwykła ludzka potrzeba przekraczania granic, która nie wymaga ekonomicznego uzasadnienia?

Prosiłbym o solidny artykuł poświęcony wyłącznie programowi Artemis: harmonogram, technika, koszty i – przede wszystkim – po co to robimy. Bez propagandy w jedną ani drugą stronę.

Stanisław Bernat
emeryt, inżynier budowlany

Red. Panie Stanisławie – pytanie „po co" jest rzeczyście ważniejsze niż „kiedy". Na artykuł o Artemis już chyba za późno, ale przymierzamy się do artykułu o podboju kosmosu. Dziękujemy za inspirację i za wierność MT od ponad pół wieku.

Grace Hopper i mój błąd przez 20 lat

Przez dwie dekady uczyłem programowania w szkole średniej i przez dwie dekady opowiadałem uczniom, że języki programowania wysokiego poziomu wymylono metodami akademickimi, gdzieś na amerykańskich uczelniach. Artykuł o Grace Hopper pokazał, że myliłem się i w fakcie, i w narracji. Była konkretna osoba, konkretny rok 1952, konkretny pomysł: niech komputer tłumaczy kod czytelny dla człowieka na język maszyny.

Pamiętam, jak w latach 90. uczyłem Pascala i tłumaczyłem uczniom, że BEGIN i END to słowa kluczowe, bo komputer tak „woli". Hopper wykazała, że komputer wcale nie „woli" – to ona postanowiła, że będzie rozumiał angielskie słowa. Kiedy pokazała kompilator FLOW-MATIC przełożonym, usłyszała: „komputer nie może rozumieć angielskiego". Odparła: „właśnie udowodniłam, że może". Tego zdania nigdy nie zapomnę i od teraz będzie otwierać nim każdy mój kurs.

Andrzej S.

Tesla, Edison i lekcja, której szkoła nie uczy

Artykuł o Nikoli Tesli był poruszający, choć znam tę historię od lat. Zastanawiam się jednak, czy MT nie powinien był silniej zaakcentować jednej kwestii: Tesla przegrał nie dlatego, że miał gorszą technologię, lecz dlatego, że nie rozumiał rynku. Edison rozumiał doskonale.

To jest lekcja, którą szkoła techniczna niemal nigdy nie podaje. Uczymy fizyki, matematyki, programowania. Nie uczymy tego, że genialny wynalazek bez strategii komercjalizacji, bez patentów, bez inwestora kończy w nieznanym grobowcu na cmentarzu w Nowym Jorku. Tesla oddał Westinghouse'owi patenty na prąd zmienny, bo pilnie potrzebował gotowki. Dostał 9 dolarów. Naprawdę 9 dolarów.

Prosiłbym, żeby MT przy okazji kolejnych biografiów technicznych zawsze dorzucał ten wątek: nie tylko co wynalazł, ale także co stracił i dlaczego. To jest edukacja, która naprawdę się przyda młodym.

Piotr J.

Red. Słuszna uwaga, ale Tesla nie przegrał z Edisonem. Podstawowy spór: prąd zmienny, czy prąd stały zakończył się zwycięstwem Tesli. Tesla przegrał sam ze sobą, nie był człowiekiem zaradnym życiowo.

Kilka stron rubryki Info Zoom to zaledwie czubek góry lodowej. Świat stoi u progu gwałtownego przyspieszenia, a każda godzina przynosi mnóstwo fascynujących doniesień o nowościach. Żaden redaktor nie

KOSMOS

Asteroida 2026 JH2 przetnie orbitę satelitów 91 tysięcy kilometrów od Ziemi

Astronomowie z Mt. Lemmon Survey w Arizonie 10 maja 2026 roku zidentyfikowali obiekt sklasyfikowany jako 2026 JH2. Dwa dni później Minor Planet Center oficjalnie potwierdziło odkrycie tej asteroidy typu Apollo na podstawie uzupełniających danych z Farpoint Observatory w Kansas.

Bryła o średnicy od 15 do 35 metrów – gabarytami zbliżona do dorosłego płetwala błękitnego – minie naszą planetę 18 maja o godzinie 21.57 UTC. Przemknie w odległości zaledwie 91 000 km, czyli niemal czterokrotnie bliżej niż wynosi średni dystans do Księżyca, poruszając się z prędkością 32 000 km/h. Modele NASA/JPL Small-Body Database precyzyjnie wyznaczyły trajektorię lotu, wykluczając ryzyko kolizji z Ziemią oraz infrastrukturą satelitarną, mimo że obiekt znajdzie się bliżej niż wiele urządzeń geostacjonarnych. Podczas zbliżenia asteroida osiągnie jasność +11,5 mag, stając się celem dla amatorskich teleskopów oraz transmisji Virtual Telescope Project.

Zdarzenie stanowi 37. tak bliskie podejście w historii pomiarów i pozwoli zweryfikować skuteczność systemów wczesnego ostrzegania przed obiektami bliskimi Ziemi (NEO). Dane zebrane podczas przelotu posłużą do kalibracji modeli matematycznych w ramach programów Planetary Defense. ■

Inżynierowie z Politechniki Warszawskiej, działający w ramach spółki spin-off SkyRad, stworzyli przełomowy system radiolokacji pasywnej o nazwie AVATAR. Urządzenie potrafi wykrywać obiekty latające, w tym maszyny stealth, nie emitując własnych fal radiowych. To innowacyjne rozwiązanie typu dual-use zmienia zasady gry zarówno na polu walki, jak i w lotnictwie cywilnym.

Klasyczne radary emitują silne impulsy elektromagnetyczne, które odbijają się od obiektów i wracają do stacji. Taki mechanizm ma wadę: zdradza pozycję urządzenia. Polski system AVATAR opiera się na technologii PCL (*Passive Coherent Location*) i sam nie wysyła żadnych sygnałów. Wykorzystuje tzw. nadajniki okazjonalne obecne w otoczeniu – stacje radiowe FM, cyfrowe nadajniki DAB+, telewizję naziemną DVB-T czy maszty sieci komórkowych. Zaawansowane algorytmy cyfrowe analizują zakłócenia w tych powszechnych sygnałach, precyzyjnie wyliczając z nich współrzędne, wysokość, azymut oraz prędkość obiektów.

AVATAR wyróżnia się niezwykłą mobilnością. Cały blok obliczeniowy wraz z odbiornikiem mieści się w zaledwie trzech skrzynkach typu rack. Wraz z systemem antenowym i agregatem stanowisko operacyjne można spakować do standardowego busa. Podczas testów demonstracyjnych w podwarszawskim Błoniu, pojedynczy sensor wykorzystujący nadajniki FM śledził cele oddalone o blisko 200 km. Fizyczne ograniczenia zasięgu wynikające z krzywizny Ziemi opisuje wzór optyczny horyzontu radiowego, uwzględniający wysokość anteny nadawczej oraz pułap lotu obiektu:

$$r = 3,57 \cdot \left(\sqrt{h_1} + \sqrt{h_2}\right)$$

Gdy naziemny nadajnik znajduje się na wysokim maszcie, a wykrywany samolot leci na wysokości 9000 m, zasięg pasywnego wykrywania przekracza 340 km. Sukces tkwi w zaawansowanej obróbce sygnałów, a nie w wysokiej mocy, co obala mit o konieczności stosowania gigantycznych stacji nadawczych.

Jedną z największych zalet systemu AVATAR jest zdolność do skutecznego wykrywania obiektów o obniżonej powierzchni odbicia radarowego (RCS), czyli maszyn stealth.

Avatar – Pasywny system radarowy od SkyRad https://youtu.be/1RAAnUjdpt4

TECHNOLOGIE WOJSKOWE Fot. SkyRad

Namierzyć niewykrywalne

Tradycyjne radary gubią takie cele, ponieważ ich kadłuby rozpraszają fale z dala od odbiornika. W przypadku lokacji pasywnej cel jest nieświadomie podświetlany z wielu kierunków przez dziesiątki nadajników naziemnych. Odbity sygnał trafia do sensora AVATAR z różnych kątów, co uniemożliwia ukrycie się przed systemem.

System jest w pełni kompatybilny z międzynarodowym standardem wymiany informacji rozpoznawczych ASTERIX. Protokół ten precyzyjnie definiuje strukturę strumienia danych, zapewniając pełną integrację z systemami obrony powietrznej Eurocontrol. Dzięki oszczędnemu kodowaniu informacji, system może raportować sytuację w czasie rzeczywistym nawet przez kanały łączności o niskiej przepustowości.

Twórcy ze SkyRad stworzyli produkt o szerokich perspektywach rynkowych. W sferze wojskowej AVATAR stanowi idealne uzupełnienie aktywnych radarów, umożliwiając skryte monitorowanie nieba i uzupełnianie luk w pokryciu radiolokacyjnym granic bez ujawniania własnej pozycji. Z kolei na rynku cywilnym system otwiera nowe możliwości w zakresie monitorowania ruchu dronów, ochrony obiektów infrastruktury krytycznej czy wsparcia mniejszych lotnisk przy ułamku kosztów tradycyjnej aparatury. ■

SPEDYCJA

50 km nad miastem – autonomiczny rekord drona dostawczego

Inżynierowie z europejskich ośrodków badawczych sfinalizowali testy bezzałogowca, który pokonał 50-kilometrową trasę w trudnych warunkach miejskich. Startując z bazy logistycznej, maszyna samodzielnie nawigowała między budynkami i infrastrukturą techniczną, by dostarczyć przesyłkę do celu bez interwencji operatora. Sukces operacji opiera się na integracji nawigacji RTK-GPS o centymetrowej dokładności oraz czujników LiDAR, które w czasie rzeczywistym tworzą trójwymiarową mapę otoczenia. Dzięki algorytmom wizyjnym dron wykrywa przeszkody, takie jak linie wysokiego napięcia czy dźwigi budowlane, i koryguje kurs w ułamku sekundy.

Przelot odbył się w trybie BVLOS, czyli poza zasięgiem wzroku, co wymagało pełnej synchronizacji z systemami zarządzania ruchem powietrznym niskiego pułapu (UTM). Wykorzystana jednostka posiada zdublowane układy napędowe oraz spadochron awaryjny, co pozwoliło na uzyskanie certyfikacji bezpieczeństwa SAIL III wymaganej przez EASA do lotów nad obszarami zaludnionymi. Podobne rozwiązania, rozwijane przez firmy Aviant czy Leonardo, wykorzystują moduły termostatyczne, co w przyszłości umożliwi transport leków i towarów krytycznych czasowo w kontrolowanej temperaturze.

Kolejnym etapem prac jest pełna automatyzacja procesów załadunkowych oraz integracja dronów z miejską logistyką ostatniej mili w ramach programów Horizon Europe. Upowszechnienie tej technologii zależy teraz od ujednolicenia przepisów w całej Unii Europejskiej oraz zwiększenia odporności systemów na ekstremalne zjawiska pogodowe, takie jak silne porywy wiatru w korytarzach między wieżowcami. ■

ZDROWIE

Plaster z interleukiną-4 regeneruje uszkodzone serce

Zespół badaczy pod kierownictwem Ke Chenga z Uniwersytetu Kalifornijskiego w Los Angeles (UCLA) opracował nową metodę naprawy mięśnia sercowego, wykorzystującą lokalną immunomodulację. W publikacji na łamach czasopisma „Cell Biomaterials" naukowcy opisali działanie biodegradowalnego plastra, który stymuluje regenerację tkanek u szczurów i świń po przebytym zawale.

Konstrukcja urządzenia opiera się na hydrożelu hialuronowym z mikroigłami o wysokości 600 mikrometrów. Wewnątrz igieł umieszczono mikrocząsteczki polimeru PLGA zawierające interleukinę-4 (IL-4). Mechanizm działania polega na stopniowym uwalnianiu cytokiny, która zmienia stan makrofagów w kierunku fenotypu naprawczego M2. Powstałe mikrośrodowisko pobudza kardiomiocyty do ponownego wejścia w cykl komórkowy. W testach na modelach zwierzęcych zaobserwowano wzrost markerów proliferacji Ki67 i pH3 oraz wyraźną poprawę frakcji wyrzutowej lewej komory (LVEF). Plaster pozwolił na znaczące zmniejszenie rozmiaru blizny włóknistej i zwiększenie grubości ścian serca w obszarze uszkodzenia.

Rozwiązanie to omija problemy związane z niską przeżywalnością przeszczepianych komórek oraz skutkami ubocznymi terapii systemowych. Kolejnym etapem prac zespołu, w skład którego weszli także specjaliści z Harvard Medical School i Texas A&M University, będzie optymalizacja dawki leku oraz przeprowadzenie długofalowych testów bezpieczeństwa przed rozpoczęciem badań klinicznych u ludzi. ■

KOMPUTERY

50 kubitów w pamięci superkomputera: Niemcy biją rekord symulacji kwantowej

Zespół badawczy z Jülich Supercomputing Centre (JSC) we współpracy z firmą NVIDIA przeprowadził pierwszą w historii kompletną symulację uniwersalnego komputera kwantowego o 50 kubitach. Eksperyment zrealizowano na europejskim systemie eksaskalowym JUPITER pod kierownictwem Hansa De Raedta i Kristel Michielsen. Osiągnięcie to stanowi istotny postęp względem poprzedniego rekordu świata z 2019 roku, kiedy to na japońskim superkomputerze K udało się zasymulować układ 48-kubitowy.

Modelowanie zachowania procesora kwantowego o takiej skali wymagało operacji na ponad 2 kwadrylionach liczb zespolonych i zajęło około 2 petabajtów pamięci operacyjnej. Aby sprostać tym wymaganiom, naukowcy opracowali nową wersję oprogramowania JUQCS-50, która wykorzystuje heterogeniczną architekturę 16 000 superchipów NVIDIA GH200. Kluczową innowacją okazało się zastosowanie adaptacyjnego kodowania danych i kompresji bajtowej, co pozwoliło ośmiokrotnie zredukować zapotrzebowanie na pamięć. Stabilność obliczeń zapewnił optymalizator ruchu sieciowego, synchronizujący pracę tysięcy węzłów obliczeniowych w czasie rzeczywistym.

Symulator JUQCS-50 umożliwi testowanie algorytmów kwantowych, takich jak Variational Quantum Eigensolver (VQE) do badania struktur cząsteczkowych, jeszcze przed powstaniem stabilnych fizycznych procesorów o dużej mocy. Narzędzie zostanie udostępnione instytucjom zewnętrznym poprzez platformę JUNIQ, służąc jako punkt odniesienia dla przyszłych systemów obliczeniowych integrujących infrastrukturę HPC z technologiami kwantowymi. ■

Dodaj do obserwowanych

SZTUCZNA INTELIGENCJA

◆ Badacze z University of Warwick zaprzęgli AI do analizy danych z teleskopu TESS, co pozwoliło odkryć ponad 100 nowych egzoplanet. System bezbłędnie wyłapał rzadkie obiekty o ekstremalnie ciasnych orbitach, których tradycyjne metody nie potrafiły zidentyfikować. ◆ Naukowcy z Caltech udowodnili, że sieć neuronowa potrafi samodzielnie odkrywać prawa fizyki rządzące czwartym stanem materii. Połączenie AI z danymi o plazmie pyłowej zaowocowało pierwszym w historii autonomicznym sformułowaniem nowych zasad dynamiki przez maszynę. ◆

FIZYKA

◆ Fizycy z Uniwersytetu Oksfordzkiego przeprowadzili pierwszy udany eksperyment typu quadsqueezing na kwantowych stanach światła. Jednoczesna redukcja szumu w czterech kwadrantach otwiera drogę do budowy niewyobrażalnie precyzyjnych urządzeń pomiarowych nowej generacji. ◆ Badacze zidentyfikowali egzotyczne formy materii, w których elektrony płyną niemal bez tarcia, przypominając zachowaniem ciecz. To odkrycie podważa klasyczne prawa fizyki i sugeruje zupełnie nowe ścieżki rozwoju technologii kwantowych opartych na unikalnych właściwościach przepływu cząstek. ◆ Według doniesień z ScienceDaily naukowcy po raz pierwszy zaobserwowali falową naturę antymaterii, chwytając jej atom w specjalnej pułapce. Eksperyment ostatecznie potwierdza dualizm korpuskularno-falowy w świecie antymaterii, co stanowi przełom w badaniach nad fundamentami wszechświata. ◆

EKSPLORACJA KOSMOSU

◆ Według komunikatu NASA załoga misji Artemis II ustanowiła nowy rekord odległości od Ziemi, oddalając się na dystans 252 756 mil podczas przelotu za Księżycem. Astronauci wykorzystali sześciogodzinne okno czasowe na przeprowadzenie unikalnych obserwacji niewidocznej z naszej planety strony Srebrnego Globu. ◆ Łazik Curiosity wykrył w marsjańskim kraterze Gale złożone molekuły organiczne, które mogą mieć związek z dawnymi procesami biologicznymi. Znalezisko to stanowi kolejny mocny dowód w poszukiwaniach śladów życia na Czerwonej Planecie i wyznacza cele dla przyszłych ekspedycji. ◆

ASTRONOMIA

◆ Teleskop TESS zidentyfikował nietypowy układ trzech egzoplanet krążących wokół pomarańczowego karła, co jest pierwszym takim odkryciem w historii astronomii. System charakteryzuje się unikalną konfiguracją orbit, która rzuca nowe światło na procesy formowania się planet w systemach o masie mniejszej od Słońca. ◆ Naukowcy ustalili, że krawędź Drogi Mlecznej znajduje się znacznie bliżej jej centrum, niż dotychczas szacowano. Gwiazdy zlokalizowane na obrzeżach galaktyki okazały się przybyszami z zewnątrz, co wymusza rewizję modeli opisujących ewolucję i strukturę naszego gwiezdnego domu.

ROBOTYKA

◆ Inżynierowie z Pekinu zaprezentowali humanoidalnego robota, który pobił rekord świata w półmaratonie, wyprzedzając najszybszych ludzi. Maszyna wykazała się niespotykaną wydajnością energetyczną i stabilnością ruchu, co stanowi milowy krok w rozwoju autonomicznych systemów kroczących. ◆

NOWE MATERIAŁY

◆ Badacze zaobserwowali, że elektrony w grafenie potrafią płynąć niczym ciecz pozbawiona tarcia, co łamie standardowe modele przewodnictwa elektrycznego. Zjawisko to otwiera drogę do budowy układów elektronicznych, które niemal nie generują ciepła, drastycznie zwiększając wydajność przyszłych komputerów.◆ Według doniesień z ScienceDaily opracowano chip na bazie grafenu, który przetrwał pracę w temperaturze 700°C. To przypadkowe odkrycie pozwala na projektowanie elektroniki zdolnej do stabilnego działania w ekstremalnych warunkach, takich jak wnętrza silników odrzutowych czy lądowniki wenusjańskie.

Źródła: ScienceDaily, Nature, Reuters, Ars Technica, Space.com.
Okres: 7 kwietnia 2026 – 5 maja 2026.

Samochód bez kierowcy

Autonomiczne pojazdy – rewolucja, która wciąż jest za rogiem

Był rok 2016. Elon Musk ogłosił, że cała flota Tesli ma już „pełny sprzęt dla pełnej autonomii" i że już w następnym roku auto samo przejedzie z Los Angeles na Times Square. Nastąpił rok 2017. Potem 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025. W każdym z tych lat zapowiedzi brzmiały niemal identycznie: pełna autonomia jest tuż za rogiem. Mamy rok 2026. Tesla Robotaxi jeździ po Austinie – ale wciąż z człowiekiem gotowym do przejęcia kontroli. Czy samochód autonomiczny to mit, czy jedynie przewlekle trudna rzeczywistość?

Autonomiczne pojazdy to jeden z tych tematów, w których technologia naprawdę istnieje i naprawdę działa – ale w znacząco węższych warunkach i na znacząco mniejszą skalę, niż głosiły wieloletnie kampanie marketingowe. Żeby to uczciwie ocenić, trzeba zacząć od podstaw: czym właściwie jest samochód autonomiczny i jak duży skok dzieli asystenta kierowcy od pojazdu zdolnego do samodzielnej jazdy?

POZIOMY AUTOMATYZACJI POJAZDÓW

według skali SAE

Gdzie jesteśmy w 2026 roku?

KONTROLA AI

KONTROLA CZŁOWIEKA

L5 — PEŁNA AUTOMATYZACJA

■ NIEOSIĄGNIĘTY

Samochód radzi sobie w każdych warunkach, na każdej drodze i przy każdej pogodzie

Żaden pojazd nie osiągnął tego poziomu. Przewidywany na lata 2035–2040

L4 — WYSOKA AUTOMATYZACJA

■ KOMERCYJNY (GEOFENCING)

Pojazd jedzie samodzielnie bez kierowcy, ale tylko w zdefiniowanym obszarze (geofencing)

Waymo One • Pony.ai • Aurora Innovation (ciężarówki)

L3 — WARUNKOWA AUTOMATYZACJA

■ TESTOWANY

Kierowca może oderwać uwagę od drogi (np. na autostradzie), ale musi reagować na wezwanie

Honda Legend • Mercedes Drive Pilot (ograniczone strefy)

L2 — CZĘŚCIOWA AUTOMATYZACJA

■ DOSTĘPNY KOMERCYJNIE

Auto utrzymuje prędkość i pas jednocześnie, ale kierowca musi trzymać ręce na kierownicy

Tesla FSD (Supervised) • BYD God;s Eye 5.0

Tesla Robotaxi Austin (nadzór człowieka)

L1 — WSPOMAGANIE KIEROWCY

■ POWSZECHNY

Jedno wspomaganie naraz: tempomat adaptacyjny lub utrzymanie pasa. Kierowca cały czas czuwa

Większość nowoczesnych samochodów

L0 — BRAK AUTOMATYZACJI

■ PODSTAWA

Kierowca kontroluje wszystko samodzielnie

Źródło: SAE International J3016, opracowanie własne 2026

Kronika niespełnionych obietnic

Wikipedia prowadzi osobny artykuł zatytułowany „Lista przepowiedni Elona Muska dotyczących autonomicznych pojazdów Tesli". To samo w sobie jest wymowne. Zestawienie jest długie – i każdy rok kończy się tak samo: niezrealizowaną zapowiedzią, zastąpioną nową, na rok następny.

Grudzień 2015: „Pełna autonomia za dwa lata." Styczeń 2016: „Za dwa lata przywołasz Teslę z Nowego Jorku, siedząc w Los Angeles." Czerwiec 2016: „Autonomia to rozwiązany problem, jesteśmy mniej niż dwa lata od pełnej samodzielnej jazdy." Październik 2016: „Do końca 2017 roku zademonstrujemy przejazd bez ingerencji człowieka od Los Angeles do Times Square." Luty 2018: „Przejazd wybrzeże–wybrzeże możemy wykonać za 3...6 miesięcy." Kwiecień 2019: „Jesteśmy pewni regulacyjnej zgody na robotaxi już w przyszłym roku – dosłownie." I co roku w latach 2020–2025: „W tym roku osiągamy pełną autonomię."

Żaden z tych terminów nie został dotrzymany. Wikipedia dokumentuje każdy z nich z oryginalnym źródłem. Dziennikarze techniczni nagrali nawet supercut z klipów wideo, w którym Musk rok po roku oświadcza, że autonomia nadejdzie „w następnym roku" – materiał wiralowy, dobrze znany społeczności śledzącej branżę (Futurism, 2022).

W czerwcu 2025 roku Tesla uruchomiła wreszcie usługę Robotaxi w Austinie. Przejazdy kosztowały symboliczne 4,20 dolara. Flota liczyła kilkanaście pojazdów na bazie zmodyfikowanego Modelu Y. Sukces? Częściowy: w każdym samochodzie siedział człowiek z palcem na awaryjnym przycisku ukrytym w rączce drzwi. Do końca 2025 roku liczba pojazdów sięgnęła kilkudziesięciu – wobec zapowiadanych 500 tylko w Austinie i „ponad tysiąca" w Zatoce San Francisco (InsideEVs, grudzień 2025). W Kalifornii Tesla przez cały 2025 rok nie przejechała ani jednej mili testowo bez człowieka za kierownicą – i nie złożyła nawet wniosku o taką zgodę (Reuters, styczeń 2026).

Tesla FSD to wciąż poziom 2. Kierowca musi być gotowy do przejęcia kontroli w każdej chwili. Tak było w 2016 roku. Tak jest w 2026.

Waymo: jedyna firma, która dotarła

Na tle tej kroniki niespełnionych obietnic jest jeden wyjątek: Waymo, spółka córka Alphabet (Google). Po ponad piętnastu latach prac i miliardach dolarów inwestycji Waymo One jeździ bez kierowcy w Phoenixie, San Francisco, Los Angeles, Austinie, Miami, Dallas i Houston – łącznie ponad 10 rynków w 2026 roku.

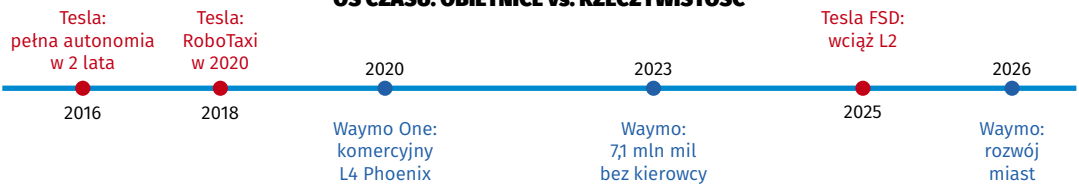
Co najważniejsze – jest bezpieczniejsze niż ludzki kierowca. I nie chodzi tu o marketingową broszurę, lecz o dane recenzowane naukowo. Kusano i wsp. (Traffic Injury Prevention, 2024) przeanalizowali ponad 7,1 miliona mil przejechanych bez kierowcy w Phoenix, San Francisco i Los Angeles, porównując je z danymi o wypadkach ludzkich kierowców na tych samych drogach. Wyniki: Waymo miało o 85% niższy współczynnik wypadków z obrażeniami (0,41 wobec 2,80 zdarzenia na milion mil) i o 57% niższy współczynnik wypadków rejestrowanych przez

TESLA vs. WAYMO

Dwie drogi do autonomii pojazdów • 2026

TESLA Podejście oparte na wizji	KATEGORIA	WAYMO Podejście wielosensorowe
Wyłącznie kamery wspierane przez sieci neutronowe. Elon Musk wielokrotnie odrzucał technologię LiDAR.	GŁÓWNE „ZMYSŁY”	Kamery + radar + LiDAR (skanowanie laserowe). Dokładna mapa 3D otozcenia niezależnie od warunków świetlnych. ✓ SKALA DANYCH
Dane z milionów samochodów poruszających się na co dzień po drogach całego świata. ✓ SKALA DANYCH	BAZA DANYCH DO NAUKI AI	Ścisłe mapowanie konkretnych obszarów operacyjnych (geofencing) i testy na zdefiniowanych rynkach.
Poziom 2 (L2) Kierowca musi być zawsze gotowy do przejęcia kontroli. ▲ L2	OSIĄGNIĘTY POZIOM SAE	Poziom 4 (L4) Samochody poruszają się bez kierowcy w wyznaczonych obszarach. ★ L4
Brak szczegółowych, recenzowanych danych. W 2025 r. pojazdy Tesli nie przejechały w Kalifornii ani jednej mili bez nadzoru x BRAK DANYCH	STATYSTYKI BEZPIECZEŃ-STWA	O 85% niższy współczynnik wypadków z obrażeniami vs. ludzcy kierowcy (dane dla 7,1 mln mil). ✓ −85% WYPADKÓW
Błędy w trudnych warunkach oświetleniowych (deszcz, mgła, oślepienie słońcem). Wieloletnie niedotrzymane obietnice pełnej autonomii (od 2016 roku).	GŁÓWNA PRZESZKODA /WPADKI	Nadmierna ostrożność lub blokowanie ruchu. W 2025 r. firma musiała zmienić ustawienia na bardziej „asertywne”, co wywołało incydenty.

OŚ CZASU: OBIETNICE vs. RZECZYWISTOŚĆ



policję. Zaktualizowana analiza z 2025 roku, obejmująca 56,7 miliona mil, potwierdziła te wyniki ze znaczącą statystycznie przewagą (Kusano i wsp., Traffic Injury Prevention, 2025).

Waymo: 85% mniej wypadków z obrażeniami niż ludzki kierowca.

Źródło: Kusano et al., Traffic Injury Prevention 2024 (n=7,1 mln mil bez kierowcy).

Waymo także popełnia błędy. Pojazdy bywają nadmiernie ostrożne, blokują ruch na zatłoczonych skrzyżowaniach, radzą sobie słabiej w trudnych warunkach pogodowych. Pod koniec 2025 roku dwa głośne incydenty – robotaxi przejechało kota, a potem psa – wywołały lokalne protesty w San Francisco. Firma sama przyznała, że w 2025 roku celowo uczyniła pojazdy bardziej „asertywne", co przyniosło kilka incydentów na granicy przepisów ruchu drogowego (Wall Street Journal, 2025). Skala i dojrzałość operacyjna – tak. Doskonałość – jeszcze nie.

Spór o zmysły: kamery kontra LiDAR

W centrum obecnego sporu technicznego leży pytanie: czym samochód autonomiczny powinien „widzieć"? Waymo wyposaża pojazdy w kamery, radar oraz LiDAR – laser skanujący otoczenie milionami impulsów świetlnych na sekundę i tworzący dokładną trójwymiarową mapę przestrzeni wokół pojazdu, niezależnie od oświetlenia. Jeszcze kilka lat temu jeden moduł LiDAR kosztował 75 000 dolarów. Dziś ceny spadły do kilkuset dolarów za sztukę.

Elon Musk odrzucił LiDAR publicznie i wielokrotnie, nazywając go „kulą u nogi" i stawiając wszystko na kamery z siecią neuronową. Logika jest pozornie elegancka: człowiek prowadzi samochód tylko oczami i mózgiem, więc po co drogie sensory? Jednak główna słabość systemu opartego wyłącznie na kamerach ujawnia się w trudnych warunkach: deszcz, mgła, śnieg, oślepienie słońcem, zmrok. Ashok Elluswamy, szef działu autonomii Tesli, przyznał w wywiadzie z maja 2025 roku, że firma jest „o kilka lat w tyle za Waymo". Business Insider przeprowadził porównawczy test obu systemów na tych samych drogach: Tesla wjechała w ścieżkę rowerową i przejechała na czerwonym świetle; Waymo wykryło przeszkodę i spokojnie wybrało inną trasę.

Jednocześnie Tesla gromadzi dane z milionów samochodów jeżdżących każdego dnia po całym świecie – skala nieosiągalna dla żadnego konkurenta. To potencjalnie ogromna przewaga w uczeniu maszynowym. Pytanie brzmi: czy ilość danych wystarczy, by poradzić sobie z fizycznymi ograniczeniami kamer w newralgicznych warunkach? Wśród ekspertów brak konsensusu.

Co naprawdę działa – poza taksówką

Historia autonomicznych pojazdów nie sprowadza się wyłącznie do robotaxi na miejskich ulicach. Kilka obszarów osiągnęło realną dojrzałość komercyjną.

Aurora Innovation uruchomiła w marcu 2025 roku pierwsze komercyjne trasy autonomicznych ciężarówek – bez kierowcy – między

Słowniczek terminów

ADAS: Advanced Driver Assistance Systems – systemy wspomagania kierowcy: tempomat adaptacyjny, asystent pasa, awaryjne hamowanie. Większość nowoczesnych samochodów ma przynajmniej ADAS poziomu 1 lub 2.

LiDAR: Light Detection and Ranging – laser skanujący otoczenie i tworzący trójwymiarową mapę przestrzeni. Niezależny od oświetlenia, precyzyjny w pomiarze odległości. Stosowany przez Waymo, odrzucony przez Teslę.

Geofencing: Ograniczenie geograficzne obszaru działania systemu autonomicznego. Waymo operuje wyłącznie na dokładnie skartografowanych obszarach, gdzie zna każdą ulicę, znak i skrzyżowanie.

Poziom SAE: Skala 0…5 ogłoszona przez Society of Automotive Engineers (standard J3016). Definiuje stopień autonomii pojazdu. Uznawana przez regulatorów i producentów na całym świecie.

Długi ogon: Nieskończona lista rzadkich, lecz realnych scenariuszy drogowych, na które AI może nie być przygotowane. Każdy mało prawdopodobny – razem tworzą ciągły strumień wyzwań.

Robotaxi: Autonomiczna taksówka bez kierowcy. Waymo One – L4. Tesla Robotaxi w Austinie (2025–26) – formalnie L2, z człowiekiem nadzorującym.

Dallas a Fort Worth. To 15-godzinne przejazdy autostradami: środowisko zdecydowanie bardziej przewidywalne niż miejski ruch, bez chodników, rowerów, pieszych i znaków wymagających kontekstualnej interpretacji. Waymo Via i Kodiak Robotics rozwijają podobne trasy międzymiastowe. Autostrady stanowią naturalny punkt startowy dla pełnej automatyzacji transportu.

Na rynku chińskim BYD – w 2025 roku największy producent samochodów na świecie – wypuścił system God's Eye 5.0 jednocześnie na 2,3 miliona pojazdach. To poziom 2+: kamery, ultradźwiękowe sensory i radar. Chiński Pony.ai oferuje tymczasem robotaxi poziomu 4 w Guangzhou, Pekinie i Szanghaju i jako pierwsza firma na świecie ogłosiła osiągnięcie progu rentowności operacyjnej w trzecim kwartale 2025 roku.

W zamkniętych obszarach – portach kontenerowych, magazynach, lotniskach, kampusach przemysłowych – pojazdy autonomiczne działają komercyjnie od lat. To środowisko idealne dla poziomu 4: teren skartografowany co do centymetra, prędkości niskie, ruch z definicji ograniczony i przewidywalny. Tu rewolucja już się dokonała – cicho i bez nagłówków.

Długi ogon: dlaczego ostatnie 10 procent kosztuje dekadę

Fundamentalny problem autonomicznej jazdy ma swoją nazwę w literaturze inżynierskiej: „długi ogon" zdarzeń rzadkich, ale krytycznych. System AI można nauczyć doskonałego zachowania w 99 procentach typowych sytuacji. Problem stanowi pozostały jeden procent: nieskończona liczba wyjątkowych scenariuszy. Dziecko wybiegające spomiędzy zaparkowanych samochodów. Policjant kierujący ruchem ręką po wypadku. Wywrotka blokująca wyjście z tunelu. Sygnalizator świetlny leżący na asfalcie po kolizji. Stado gęsi przechodzące przez jezdnię. Każdy z tych scenariuszy jest statystycznie rzadki – ale razem tworzą ciągły strumień zaskoczeń na realnych drogach.

Człowiek interpretuje tego rodzaju sytuacje intuicyjnie, korzystając z lat doświadczenia społecznego, rozumienia intencji innych ludzi i zdrowego rozsądku. System AI – nawet bardzo zaawansowany – nie widział dokładnie tej kombinacji czynników wcześniej. Im bardziej system zbliża się do granicy 99,9 procenta bezpieczeństwa, tym trudniej zdobyć kolejną dziesiątą procenta. Zlikwidowanie długiego ogona wymaga albo niezmierzonej liczby przejechanych mil testowych, albo gigantycznych inwestycji w symulacje, albo dodatkowych czujników – albo wszystkiego naraz.

Drugi problem to regulacje. Każde państwo, a w USA każdy stan, definiuje odpowiedzialność za wypadki, wymogi certyfikacji i obszary dopuszczonej eksploatacji inaczej. Waymo w Teksasie działa bez szczegółowych ograniczeń

„Długi ogon": nieskończona lista rzadkich, ale realnych sytuacji drogowych. Każda mało prawdopodobna – razem tworzą ciągły strumień wyzwań, które dla AI wciąż są nowym terytorium.

stanowych – bo Teksas jest regulacyjnie liberalny. W Kalifornii każda mila bez kierowcy wymaga odrębnej zgody stanowego DMV. W Europie autonomia poziomu 4 jest formalnie dopuszczona jedynie w wyznaczonych strefach testowych w Niemczech, w ściśle określonych warunkach. Podobnie jest w Japonii.

Kiedy i dla kogo?

Uczciwa prognoza na lata 2026–2030 wygląda następująco. Waymo będzie konsekwentnie rozszerzać operacje na kolejne amerykańskie, a stopniowo i europejskie miasta. Tesla będzie powiększać flotę Robotaxi i – jeśli przepisy na to pozwolą – stopniowo ograniczać obecność nadzorcy. BYD i chińscy gracze będą rosnąć na rynkach azjatyckich. Aurora i podobne firmy będą przejmować kolejne trasy długodystansowe.

W horyzoncie 2030–2035: robotaxi poziomu 4 staną się standardem w 20...50 dużych miastach świata. Autonomiczne ciężarówki na głównych korytarzach drogowych to realny i prawdopodobnie rentowny rynek komercyjny. Samochody osobowe dla konsumentów – głównie poziom 2...3, z wyspami pełnej autonomii na wybranych autostradach.

Co do poziomu 5 – pełnej autonomii wszędzie i w każdych warunkach – wśród badaczy nie ma konsensusu co do daty. Jedni mówią o latach 2035–2040. Inni uważają, że problem wymaga zupełnie nowego podejścia, którego jeszcze nie znamy. Jedno jest jednak jasne: nawet bez poziomu 5, poziom 4 w ograniczonych obszarach wystarczy, by gruntownie przebudować rynek taksówkowy, logistykę ostatniej mili i transport długodystansowy. Pytanie nie brzmi już „czy?", lecz „kiedy i gdzie?".

Epilog: zaufanie jako najtrudniejszy problem inżynierski

Dane są klarowne: Waymo jest statystycznie bezpieczniejsze od przeciętnego ludzkiego kierowcy. A jednak społeczna akceptacja rośnie powoli. Jeden wirusowy film z robotaxi zachowującym się dziwacznie wyrządza więcej szkody zaufaniu publicznemu niż miliony spokojnych przejazdów. To zjawisko dobrze znane z lotnictwa: samolot jest wielokrotnie bezpieczniejszy od samochodu, a mimo to lęk przed lataniem pozostaje powszechny. Jeden wypadek lotniczy trafia na pierwsze strony; miliony bezpiecznych lotów – nie.

Znaczący jest również kontrast między Waymo a Teslą w kwestii przejrzystości. Waymo udostępnia publicznie recenzowane naukowo dane o bezpieczeństwie i poddaje je niezależnej weryfikacji badaczy. Tesla nie publikuje porównywalnych danych, a jej dział prawny argumentował w amerykańskim sądzie, że słowo „pełna samodzielna jazda" w nazwie FSD ma charakter „aspiracyjny", a nie opisowy. W lutym 2026 roku Tesla ogłosiła, że FSD będzie dostępne wyłącznie jako miesięczna subskrypcja, nie jednorazowy zakup. Interpretacje są dwie: albo pełna autonomia jest blisko i warto przejść na model przychodowy, albo nie powinno się sprzedawać długookresowych obietnic, których nie można zrealizować.

Autonomiczny samochód nie jest snem naukowej fantastyki. Jest częściową rzeczywistością dojrzewającą powoli, nierytmicznie, ale jednak Mamy przynajmniej jeden bezdyskusyjny dowód działania: Waymo nie tylko istnieje, ale statystycznie ratuje życie. Tylko nie jutro i nie na każdej drodze. ■

Paweł Biernacki

Źródła:

1. Kusano, K.D. et al. (2024). Comparison of Waymo Rider-only crash data to human benchmarks at 7.1 million miles. Traffic Injury Prevention, 25(sup1), S66–S77. doi:10.1080/15389588.2024.2380786.
2. Kusano, K.D. et al. (2025). Comparison of Waymo Rider-Only Crash Rates by Crash Type to Human Benchmarks at 56.7 Million Miles. Traffic Injury Prevention, 26(sup1), S8–S20. doi:10.1080/15389588.2025.2499887.
3. Wikipedia (2026): List of predictions for autonomous Tesla vehicles by Elon Musk – dokumentacja obietnic i terminów 2013–2025. en.wikipedia.org.
4. Lambert, F. (31.12.2025). Tesla's Big Robotaxi Promises Fall Flat As 2025 Comes To A Close. InsideEVs. insideevs.com.
5. Reuters (styczeń 2026): Tesla – zero mil testów autonomicznych bez kierowcy w Kalifornii w 2025 r.,.
6. Lambert, F. (21.05.2025). Tesla Admits FSD Is „Lagging By A Couple Years" Behind Waymo. InsideEVs.
7. Wall Street Journal (2025): Waymo robotaxis in San Francisco – relacja o zmianie stylu jazdy na bardziej „asertywny" i związanych incydentach.
8. Aurora Innovation (marzec 2025): ogłoszenie komercyjnych tras Level 4 dla ciężarówek Dallas–Fort Worth. aurora.tech.
9. SAE International: J3016_202104 Taxonomy and Definitions for Terms Related to Driving Automation Systems – oficjalna skala L0–L5.
10. Sherwood News (14.01.2026): Tesla stops selling FSD as one-off, pivoting to subscription model. sherwood.news.

Oddajemy cześć kobietom, które odegrały wybitną rolę w rozwoju techniki i nauk ścisłych

Był grudzień 1842 roku. Augusta Ada King, hrabina Lovelace, siedziała przy biurku w swoim londyńskim domu i tłumaczyła z francuskiego na angielski artykuł włoskiego matematyka Luigiego Menabrei o maszynie analitycznej Charlesa Babbage'a. Babbage, jej mentor i przyjaciel, poprosił ją o przekład. Ada wykonała zadanie – ale przy okazji dodała własne komentarze. Te komentarze były trzy razy dłuższe od oryginału. I zmieniły historię informatyki. W przypisie oznaczonym literą G opisała algorytm obliczania liczb Bernoulliego – krok po kroku, dokładnie tak, jak powinien go wykonać automat. Był to pierwszy algorytm w historii przeznaczony do wykonania przez maszynę. Ada Lovelace miała 27 lat. Pierwszy prawdziwy komputer powstał sto lat później.

1. Portret Ady Lovelace, ok. 1840 r. – miniatura akwarela Margaret Sarah Carpenter, Science Museum London (domena publiczna)

Ada Lovelace

Pierwsza programistka świata. Sto lat przed pierwszym komputerem

Córka poety, wychowanka matematyki

Augusta Ada Byron urodziła się 10 grudnia 1815 roku w Londynie jako jedyne legalne dziecko George'a Gordona Byrona – jednego z najsławniejszych i najbardziej skandalizujących poetów epoki romantyzmu. Jej rodzice rozstali się, gdy Ada miała zaledwie miesiąc. Lord Byron opuścił Anglię i nigdy nie wrócił; zmarł w Grecji osiem lat później, walcząc o grecką niepodległość. Ada nigdy go nie poznała.

Jej matka, lady Annabella Byron, była kobietą o głębokiej niechęci do poetów i romantycznych fantazji. Obawiała się, że Ada odziedziczy

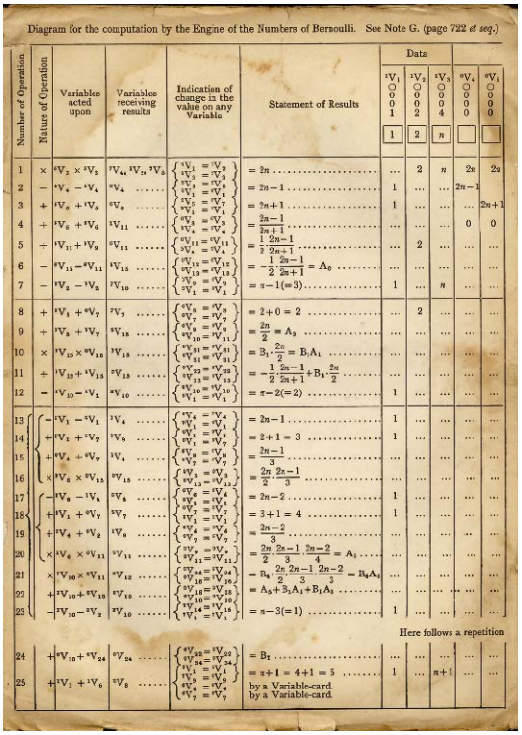


Diagram for the computation by the Engine of the Numbers of Bernoulli. See Note G. (page 722 *et seq.*)

Number of Operation	Nature of Operation	Variables acted upon	Variables receiving results	Indication of change in the value on any Variable	Statement of Results	Data $^1V_1$ 0 0 0 1	$^1V_2$ 0 0 0 2	$^1V_3$ 0 0 0 4	$^2V_4$ 0 0 0 0	$^2V_5$ 0 0 0 0
						1	2	n		
1	×	$^2V_2 \times {}^2V_3$	$^2V_4, {}^1V_2, {}^2V_3$	$\{{}^1V_2 = {}^1V_3\}$ $\{{}^1V_3 = {}^1V_2\}$	$= 2n$	...	2	n	$2n$	$2n$
2	−	$^2V_4 - {}^1V_1$	$^2V_4$	$\{{}^1V_1 = {}^1V_1\}$	$= 2n-1$	1	...	...	$2n-1$	
3	+	$^2V_6 + {}^1V_1$	$^2V_6$	$\{{}^1V_1 = {}^1V_7\}$	$= 2n+1$	1	...	...	...	$2n+1$
4	÷	$^2V_6 \div {}^2V_5$	$^2V_{11}$	$\{{}^2V_5 = {}^2V_5\}$ $\{{}^2V_6 = {}^2V_6\}$	$= \frac{2n-1}{2n+1}$	...	...	...	0	0
5	÷	$^2V_{11} \div {}^1V_2$	$^2V_{11}$	$\{{}^2V_{11} = {}^2V_{11}\}$ $\{{}^1V_4 = {}^1V_4\}$	$= \frac{1}{2}\frac{2n-1}{2n+1}$	...	2	...	...	...
6	−	$^2V_{11} - {}^2V_{11}$	$^2V_{15}$	$\{{}^2V_{15} = {}^2V_{15}\}$ $\{{}^2V_{13} = {}^2V_{13}\}$	$= -\frac{1}{2}\frac{2n-1}{2n+1} = A_0$	...	...	...	...	...
7	−	$^2V_3 - {}^1V_1$	$^2V_{10}$	$\{{}^2V_3 = {}^2V_3\}$ $\{{}^1V_1 = {}^1V_1\}$	$= n-1(=3)$	1	...	n	...	...
8	+	$^2V_1 + {}^2V_7$	$^2V_7$	$\{{}^2V_1 = {}^2V_1\}$ $\{{}^2V_7 = {}^2V_7\}$	$= 2+0 = 2$	...	2	...	...	...
9	+	$^2V_8 + {}^2V_7$	$^2V_{18}$	$\{{}^2V_8 = {}^2V_8\}$ $\{{}^2V_{10} = {}^2V_{11}\}$	$= \frac{2n}{2} = A_0$	...	...	...	...	...
10	×	$^2V_{10} \times {}^2V_{16}$	$^2V_{18}$	$\{{}^2V_{11} = {}^2V_{11}\}$ $\{{}^2V_{13} = {}^2V_{13}\}$	$= B_1 \cdot \frac{2n}{2} = B_1 A_1$	...	...	...	...	...
11	+	$^2V_{13} + {}^2V_{15}$	$^2V_{13}$	$\{{}^2V_{22} = {}^2V_{22}\}$ $\{{}^2V_{13} = {}^2V_{13}\}$	$= -\frac{1}{2}\frac{2n-1}{2n+1} + B_1 \cdot \frac{2n}{2}$	...	...	...	...	...
12	−	$^2V_{10} - {}^1V_1$	$^2V_{10}$	$\{{}^2V_{10} = {}^2V_{10}\}$ $\{{}^1V_1 = {}^1V_1\}$	$= n-2(=2)$	1	...	...	...	...
13	−	$^1V_1 - {}^1V_1$	$^2V_4$	$\{{}^1V_1 = {}^1V_4\}$ $\{{}^1V_1 = {}^1V_1\}$	$= 2n-1$	1	...	...	...	...
14	+	$^1V_1 + {}^1V_7$	$^2V_9$	$\{{}^1V_1 = {}^1V_1\}$ $\{{}^1V_7 = {}^1V_7\}$	$= 2+1 = 3$	1	...	...	...	...
15	+	$^2V_4 + {}^2V_7$	$^2V_4$	$\{{}^2V_4 = {}^2V_4\}$ $\{{}^2V_7 = {}^2V_7\}$	$= \frac{2n-1}{3}$	...	...	...	...	...
16	×	$^2V_9 \times {}^2V_{13}$	$^2V_{15}$	$\{{}^2V_9 = {}^2V_9\}$ $\{{}^2V_{13} = {}^2V_{13}\}$	$= \frac{2n}{2}\frac{2n-1}{3}$	...	...	...	...	...
17	−	$^2V_8 - {}^1V_1$	$^2V_8$	$\{{}^2V_8 = {}^2V_8\}$ $\{{}^1V_1 = {}^1V_1\}$	$= 2n-2$	1	...	...	...	...
18	+	$^1V_1 + {}^2V_7$	$^2V_7$	$\{{}^1V_1 = {}^1V_1\}$ $\{{}^2V_7 = {}^2V_7\}$	$= 3+1 = 4$	1	...	...	...	...
19	+	$^2V_4 + {}^2V_2$	$^2V_9$	$\{{}^2V_4 = {}^2V_4\}$ $\{{}^2V_7 = {}^2V_7\}$	$= \frac{2n-2}{3}$	...	...	...	...	...
20	×	$^2V_4 \times {}^2V_{11}$	$^2V_{11}$	$\{{}^2V_4 = {}^2V_4\}$ $\{{}^2V_{11} = {}^2V_{11}\}$	$= \frac{2n}{2}\frac{2n-1}{3}\frac{2n-2}{4} = A_1$	...	...	...	...	...
21	×	$^2V_{10} \times {}^2V_{11}$	$^2V_{12}$	$\{{}^2V_{24} = {}^2V_{24}\}$ $\{{}^2V_{16} = {}^2V_{16}\}$	$= B_4 \frac{2n}{2}\frac{2n-1}{3}\frac{2n-2}{4} = B_4 A_4$	...	...	...	...	...
22	+	$^2V_{10} + {}^2V_{12}$	$^2V_{10}$	$\{{}^2V_{18} = {}^2V_{18}\}$ $\{{}^2V_{16} = {}^2V_{16}\}$	$= A_3 + B_1 A_1 + B_1 A_3$	...	...	...	...	...
23	−	$^2V_{10} - {}^2V_2$	$^2V_{10}$	$\{{}^2V_{14} = {}^2V_{14}\}$ $\{{}^1V_1 = {}^1V_1\}$	$= n-3(=1)$	1	...	...	...	...
					Here follows a repetition					
24	+	$^2V_{10} + {}^2V_{24}$	$^2V_{24}$	$\{{}^2V_{22} = {}^2V_{22}\}$ $\{{}^2V_{24} = {}^2V_{24}\}$	$= B_2$	...	...	...	...	...
25	+	$^1V_1 + {}^1V_6$	$^2V_8$	$\{{}^1V_1 = {}^1V_1\}$ $\{{}^1V_6 = {}^1V_9\}$ by a Variable-card $\{{}^1V_7 = {}^1V_7\}$ by a Variable-card.	$= n+1 = 4+1 = 5$	1	...	$n+1$	...	...

2. Strona z adnotacji G – pierwszy algorytm w historii, publikacja Taylor's Scientific Memoirs, 1843 r. (domena publiczna)

3. Model krosna Jacquarda z kartami perforowanymi – inspiracja dla mechanizmu programowania maszyny analitycznej Babbage'a

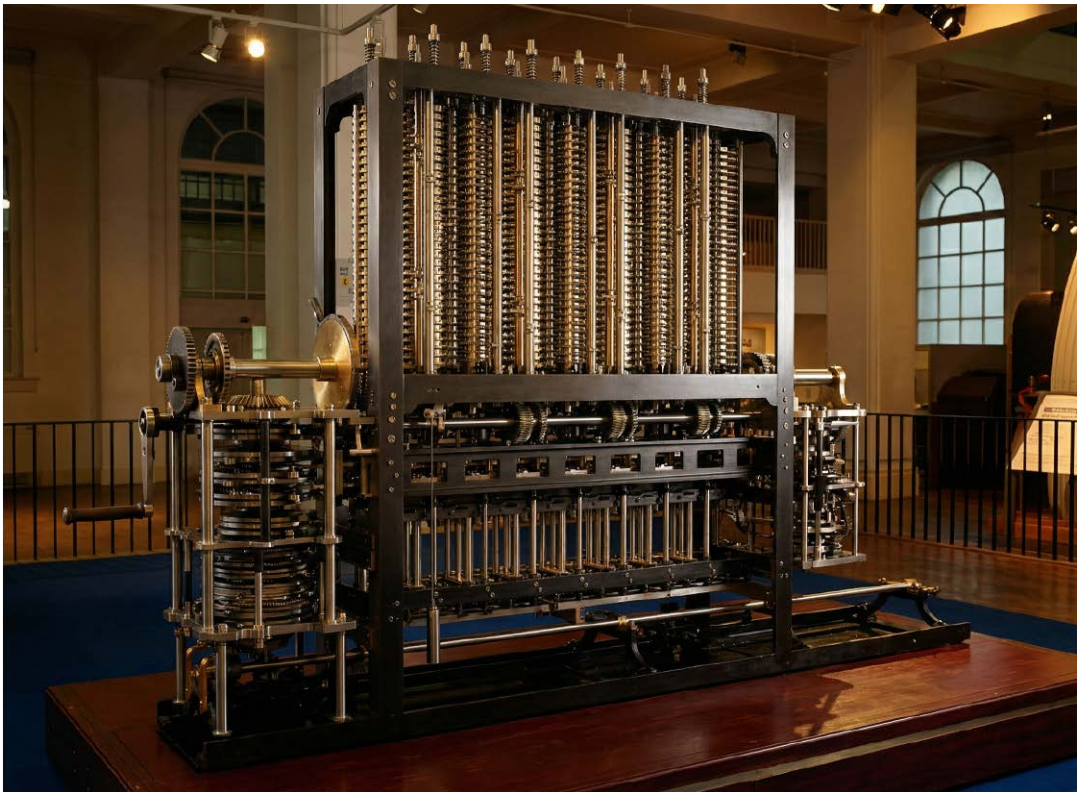
po ojcu artystyczny temperament prowadzący do moralnej zguby. Postanowiła córkę przed tym ochronić jedyną bronią, jaką znała: matematyką. Od najmłodszych lat Ada była intensywnie uczona geometrii, arytmetyki i logiki – a wszelkie przejawy wyobraźni i artystycznych skłonności były tłumione lub przekierowywane. Paradoksem historii jest to, że właśnie ta strategia – zamierzona jako ograniczenie – ukształtowała umysł zdolny do wyobrażenia sobie czegoś, czego jeszcze nie było.

Ada uczyła się u prywatnych nauczycieli, wśród których była Mary Somerville – jedna z pierwszych kobiet członków Towarzystwa Astronomicznego i autorka popularnych dzieł naukowych. To Somerville w 1833 roku wprowadziła siedemnastoletnią Adę na spotkanie Charlesa Babbage'a, profesora matematyki na Uniwersytecie Cambridge. Babbage pokazał gościom swoją maszynkę różnicową – mechaniczny kalkulator zaprojektowany do automatycznego tworzenia tablic matematycznych. Większość gości była zaciekawiona. Ada była zafascynowana.

Maszyna, która istniała tylko na papierze

Babbage i Ada Lovelace – która wkrótce poślubiła hrabiego Williama Kinga, późniejszego lorda Lovelace'a – utrzymywali przez kolejne lata ożywioną korespondencję naukową. Gdy Babbage porzucił maszynę różnicową i zaczął projektować ambitniejsze urządzenie – maszynę analityczną – Ada była jedną z nielicznych osób, które rozumiały, co zamierza.

Maszyna analityczna była projektem zdumiewającym jak na swoją epokę. Babbage chciał zbudować urządzenie, które nie byłoby kalkulatorem o jednym zastosowaniu, lecz ogólnego przeznaczenia automatyczną maszyną obliczeniową, programowaną za pomocą kart perforowanych – podobnych do tych używanych w warsztatach tkackich Jacquarda. Miała posiadać pamięć (Babbage nazywał ją magazynem), jednostkę obliczeniową (młyn) i możliwość wykonywania warunkowych rozgałęzień – czyli decydowania, co zrobić dalej w zależności od wyników pośrednich. Była to w istocie architektura współczesnego komputera – tyle



4. Fragment modelu maszyny różnicowej Babbage'a nr 2, złożonej w Muzeum Nauki w Londynie w 1991 r.

że mechaniczna, z trybów i dźwigni, i nigdy w całości nie zbudowana za życia Babbage'a.

Kiedy w 1842 roku włoski matematyk Luigi Menabrea opublikował po francusku opis maszyny analitycznej, Babbage poprosił Adę o przekład na angielski. Ada przełożyła tekst – a następnie dodała własne obszerne adnotacje oznaczone literami od A do G. Babbage zaproponował, by napisała własny, oryginalny tekst zamiast tylko tłumaczyć. Ada odmówiła: uznała, że komentarze do istniejącego artykułu trafią do czytelników skuteczniej. Miała rację.

Algorytm, który wyprzedził epokę

W adnotacji G – najdłuższej i najważniejszej – Ada opisała dokładną procedurę obliczania liczb Bernoulliego za pomocą maszyny analitycznej. To nie było ogólne omówienie możliwości maszyny. Był to precyzyjny, krok po kroku zapisany przepis na konkretne obliczenie, ze wskazaniem, jakie dane wprowadzić, jaką operację wykonać, gdzie zapisać wynik pośredni i kiedy zakończyć pętlę obliczeń. Według współczesnych informatyków jest to pierwszy algorytm w historii sformalizowany z myślą o wykonaniu przez maszynę.

Ale Ada poszła dalej niż Babbage. W innych adnotacjach sformułowała coś, czego sam wynalazca maszyny nie napisał wprost: że maszyna analityczna może być używana nie tylko do obliczeń liczbowych, lecz do każdej operacji,

JAK TO DZIAŁA: ALGORYTM I PĘTLA

Algorytm to przepis na wykonanie zadania: lista kroków, które prowadzą od danych wejściowych do wyniku. Możesz myśleć o nim jak o instrukcji obsługi, ale dla maszyny.

Ada Lovelace jako pierwsza dostrzegła, że niektóre kroki algorytmu mogą się powtarzać – i zamiast wypisywać je wielokrotnie, wystarczy opisać warunek: „powtarzaj, dopóki wynik nie spełnia kryterium". To właśnie jest pętla – jeden z podstawowych elementów każdego języka programowania od 1950 roku do dziś.

W jej algorytmie liczb Bernoulliego pętla obliczeniowa pojawia się wyraźnie i świadomie. Sto lat wcześniej niż ENIAC, Fortran czy Python – Ada zapisała instrukcję, którą rozpoznałby każdy współczesny programista.

którą da się wyrazić w formie symbolicznej. Napisała, że maszyna mogłaby komponować muzykę, jeśli tylko opisze się matematycznie relacje między dźwiękami. Było to sformułowanie idei, którą Alan Turing rozwinął w pełną teorię sto lat później: że komputer jest maszyną ogólnego przeznaczenia, zdolną symulować każdy inny automat.

Dodała jednak także ważne zastrzeżenie, które wciąż jest cytowane w filozofii informatyki: maszyna analityczna „nie ma zdolności do wytworzenia czegoś nowego. Może robić tylko to, co nakazuje jej człowiek". To zdanie znane jest dziś jako „zarzut Lady Lovelace" i pojawia się w każdej poważnej debacie o sztucznej inteligencji oraz pytaniu, czy maszyna może być twórcza.

Krótkie życie, długie zapomnienie

Zarówno Ada, jak i Babbage mieli świadomość, że ich praca jest zbyt daleko przed epoką, by zostać natychmiast zrozumiana. Ada pisała w liście do Babbage'a: „Pracujemy dla przyszłości, a nie dla teraźniejszości". Miała rację – ale nie wiedzieli oboje, jak daleka będzie ta przyszłość.

W 1843 roku, kilka miesięcy po publikacji przekładu z komentarzami, Ada zaczęła chorować. Przez następne lata zmagała się z nawracającymi dolegliwościami – prawdopodobnie rakiem macicy, choć ówczesna medycyna nie potrafiła tego zdiagnozować. Uzależniła się od laudanum i morfiny stosowanych jako środki przeciwbólowe. Próbowała zarobić pieniądze, opracowując systemy typowania wyników wyścigów konnych oparte na metodach matematycznych – bez sukcesu. Zadłużyła się poważnie.

Ada Lovelace zmarła 27 listopada 1852 roku w wieku 36 lat – dokładnie tylu, ile miał jej ojciec, lord Byron, w chwili śmierci. Zgodnie ze swoim życzeniem została pochowana obok niego w kościele w Hucknall w Nottinghamshire – choć nigdy go nie poznała za życia.

Jej komentarze do artykułu Menabrei zostały zapomniane niemal natychmiast po śmierci. Babbage nie zbudował maszyny analitycznej. Przez niemal sto lat prace Ady leżały w bibliotekach jako historyczna ciekawostka. Dopiero w 1953 roku brytyjski informatyk B.V. Bowden przedrukował jej komentarze w książce „Faster Than Thought" i zwrócił uwagę środowiska na to, co zawierały. Informatycy przeczytali i zamarli. Algorytm zapisany w 1842 roku był poprawny.

DLACZEGO JEJ NIE ZNASZ?

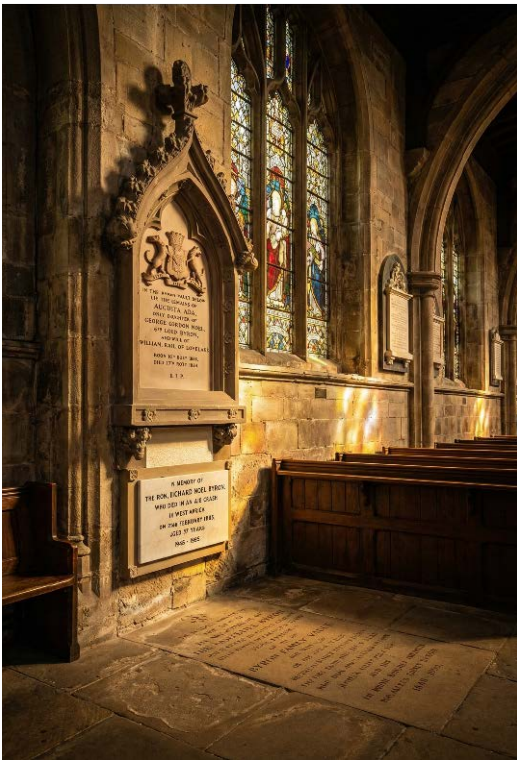
Ada Lovelace działała w epoce, w której kobiety nie miały dostępu do uczelni, nie mogły być członkami towarzystw naukowych i nie mogły publikować pod własnym nazwiskiem w większości journalów. Jej przekład z komentarzami ukazał się podpisany inicjałami A.A.L.

Maszyna analityczna Babbage'a nigdy nie powstała – więc nie było widocznego wyniku, który można by było pokazać i przypisać konkretnemu autorowi. Praca Ady była czysto teoretyczna, a teorię łatwiej zignorować niż działający wynalazek.

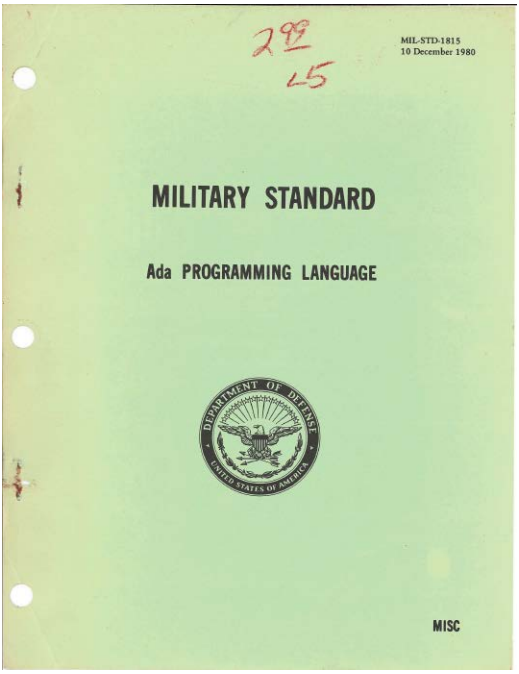
Paradoksalnie zaszkodziło jej także ojcostwo: być córką lorda Byrona znaczyło być postacią towarzyską i romansową, a nie naukową. Przez długi czas historyczne wzmianki opisywały ją głównie jako „córkę Byrona" lub „przyjaciolkę Babbage'a", a nie jako samodzielnego myśliciela.

Rehabilitacja i pamięć

W 1980 roku amerykański Departament Obrony nadał nowo opracowanemu językowi programowania nazwę Ada – na cześć Ady Lovelace. Język ten, zaprojektowany do zastosowań wojskowych



5. Grób Ady Lovelace i lorda Byrona w kościele św. Marii Magdaleny w Hucknall, Nottinghamshire



6. Język programowania Ada – instrukcja dla wojska wydana w grudniu 1980 roku, którą można przejrzeć na stronie: https://archive.org/details/mil-std-ada/mode/2up

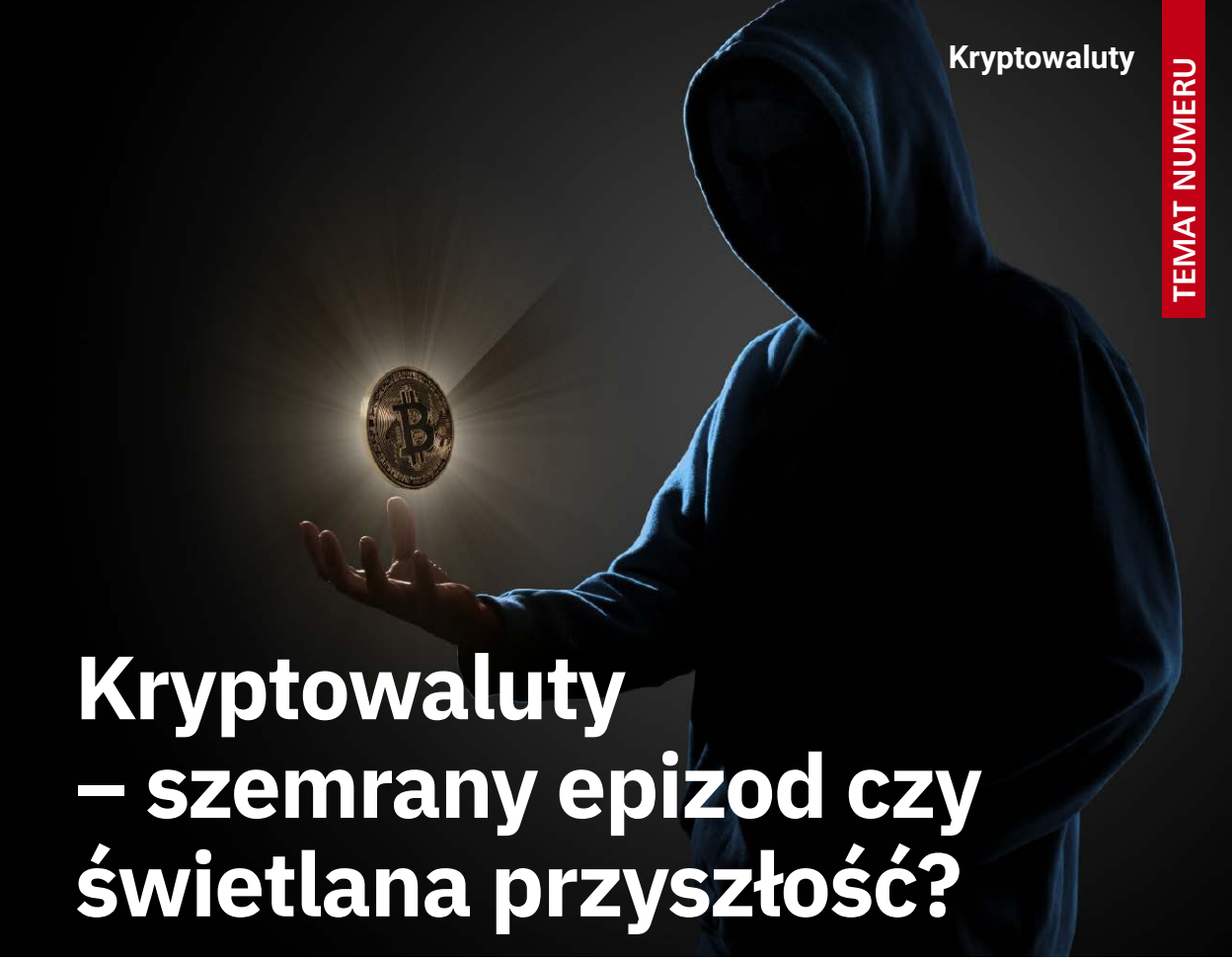
i systemowych, był używany m.in. w systemach sterowania samolotów bojowych i rakiet. Było to oficjalne uznanie, że kobieta, która napisała pierwsze instrukcje dla nieistniejącej maszyny, stała u źródeł całej dyscypliny.

Od 2009 roku drugi wtorek października obchodzony jest na całym świecie jako Ada Lovelace Day – dzień upamiętniający kobiety w nauce, technologii, inżynierii i matematyce. Jej portret zdobi banknoty, znaczki pocztowe i murale w kilku krajach. Jej imię nosi asteroid 232517 Ada, budynki na uczelniach w Wielkiej Brytanii i Stanach Zjednoczonych, a także nagroda przyznawana przez Stowarzyszenie Maszyn Obliczeniowych za wybitne wkłady kobiet do informatyki.

Alan Turing, pisząc w 1950 roku swój słynny artykuł „Computing Machinery and Intelligence", odwołał się bezpośrednio do „zastrzeżenia lady Lovelace" o granicach maszynowej tworczości – i dyskutował z nim. Kobieta, która zmarła 98 lat przed publikacją tego tekstu, wciąż była rozmówczynią, z którą warto się spierać.

Maszyna analityczna Charlesa Babbage'a nigdy nie została zbudowana za jego życia. Ale w 1991 roku Muzeum Nauki w Londynie złożyło ją w całości na podstawie oryginalnych rysunków Babbage'a. Działała. W 2021 roku ten sam zespół ogłosił próbę zbudowania maszyny analitycznej w pełnej skali. Jeśli się to uda, będzie to pierwsza maszyna zdolna uruchomić algorytm Ady Lovelace. Dziewięćdziesiąt lat po śmierci w wieku trzydziestu sześciu lat, zapisana przez nią sekwencja kroków wciąż czeka na swoje pierwsze wykonanie. ■

Paweł Biernacki



Kryptowaluty – szemrany epizod czy świetlana przyszłość?

Część 1. O co właściwie chodzi

Pierwszy bitcoin powstał 3 stycznia 2009 roku. Był wpisem w pliku zapisanym na dysku komputera, którego lokalizacji nie znamy. Wpis ten miał wartość pięćdziesięciu jednostek walutowych nieistniejącej waluty i nie był zabezpieczony niczym – żadnym kruszcem, żadnym państwem, żadną instytucją. Mimo to osiemnaście lat później jeden bitcoin kosztuje kilkadziesiąt tysięcy dolarów, a łączna wartość rynkowa wszystkich kryptowalut przekracza dwa biliony dolarów.

Z punktu widzenia ekonomisty jest to zjawisko kłopotliwe. Z punktu widzenia inżyniera – interesujące. Bo niezależnie od tego, co sądzimy o cenie, kryptowaluty są działającym rozwiązaniem problemu, który przez kilka dekad uchodził za nierozwiązywalny: jak sprawić, żeby tysiące nieznajomych komputerów, z których część jest wrogo nastawiona, doszło do zgody w sprawie tego, kto ile ma – bez żadnego nadzorcy.

Niniejszy temat numeru poświęcamy temu, jak to działa technicznie. W mnmiejszym stopniu interesują nas pytania o spekulacyjny charakter rynku, pranie pieniędzy i zachowania inwestorów. Te tematy są dobrze opisane w prasie ekonomicznej. Zajmiemy się natomiast mechaniką: kryptografią, strukturą danych, protokołem konsensusu, ekonomią obliczeń. Tam, gdzie będzie to konieczne, użyjemy matematyki. Nie będzie jej

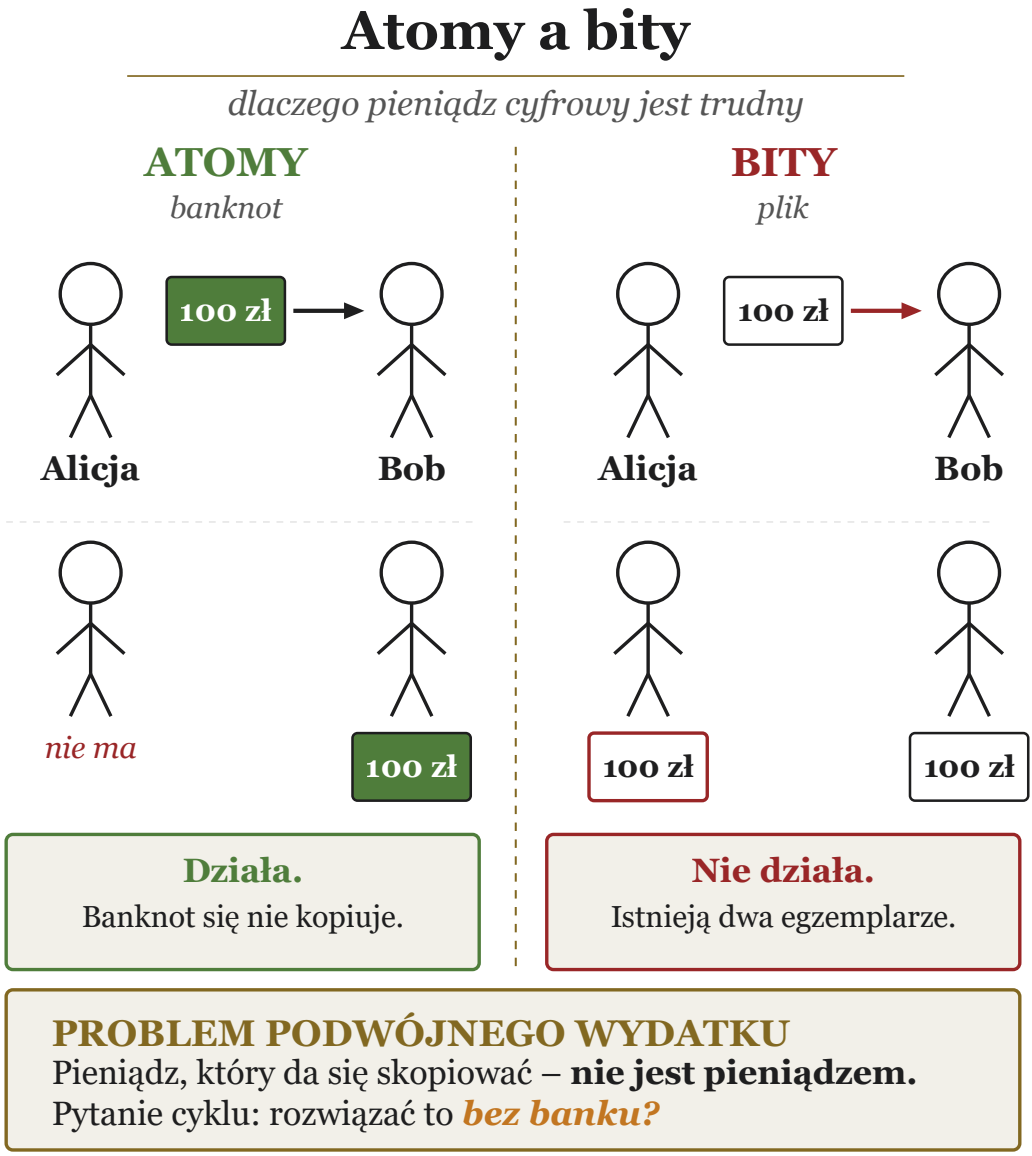
dużo i nie będzie skomplikowana, ale udawanie, że można wytłumaczyć kryptografię bez liczb, byłoby nieuczciwe.

Problem podwójnego wydatku

Pieniądz fizyczny ma jedną właściwość, którą rzadko doceniamy: nie da się go skopiować. Banknot stuzłotowy, gdy go komuś wręczymy, znika z naszej kieszeni i pojawia się w cudzej. Nie ma sposobu, żeby ten sam banknot wręczyć dwóm osobom jednocześnie.

Z plikiem cyfrowym jest dokładnie odwrotnie. Każda operacja wysłania pliku jest w istocie operacją kopiowania. Wysłany e-mail nie znika z naszego komputera. Skopiowane zdjęcie istnieje w dwóch egzemplarzach nieodróżnialnych od siebie ani technicznie, ani prawnie – bity nie mają oryginału.

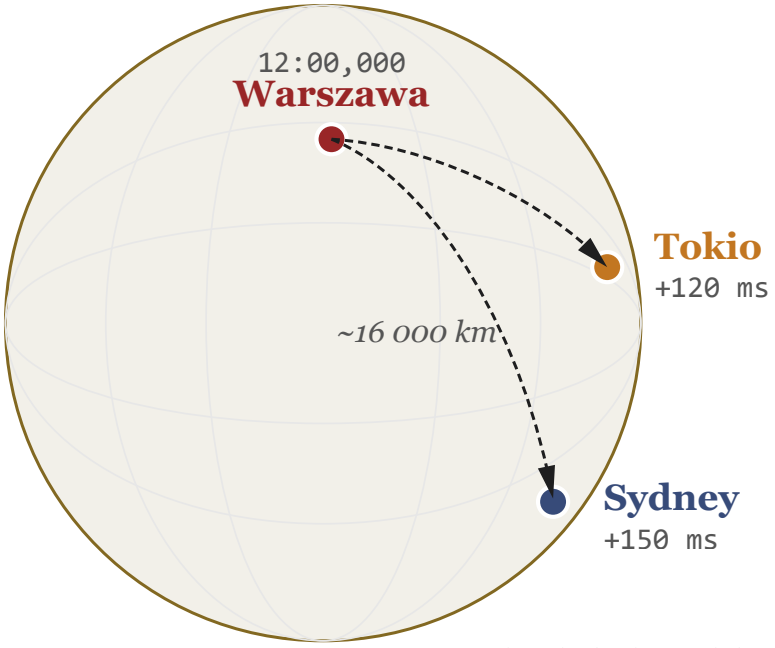
Ta cecha bitów, znakomita do dystrybucji informacji, jest fatalna do przesyłania pieniądza. Pieniądz, który można skopiować, nie jest pieniądzem. W literaturze informatycznej



Rysunek 1. Internet jest siecią kopiującą. To jego siła i – w przypadku pieniądza – jego słabość

Opóźnienia w sieci

„teraz” w globalnej sieci nie istnieje



FIZYKA

Sygnał w światłowodzie: **200 000 km/s**

Warszawa → Sydney: **80 ms**

KONFLIKT

Alicja ma 100 zł. Wysyła je **jednocześnie do dwóch osób.** Każdy węzeł sieci widzi inną **„pierwszą” transakcję.**

Rysunek 2. Opóźnienia w sieci globalnej. „Jednoczesność” przestaje istnieć już przy odległości kilku tysięcy kilometrów

problem ten nosi nazwę problemu podwójnego wydatku (double-spending problem).

Klasyczne rozwiązanie problemu jest oczywiste i znane od kilku tysięcy lat: ktoś prowadzi księgę. Bank wie, ile mamy na koncie. Gdy wykonujemy przelew, bank zmniejsza naszą sumę i zwiększa cudzą. Próba dwukrotnego wydania tej samej kwoty zostaje odrzucona, bo bank widzi, że pierwszy przelew już ją wyzerował. System działa pod warunkiem, że bankowi ufamy – lub że ufamy państwu, które bank nadzoruje.

Pytanie, które przez kilka dekad zadawali sobie kryptografowie, brzmiało: czy da się rozwiązać problem podwójnego wydatku bez banku. Bez żadnego centralnego punktu, któremu trzeba ufać. Czy istnieje konstrukcja, w której księgę prowadzą wszyscy uczestnicy systemu jednocześnie i nie da się jej oszukać?

Przez długi czas odpowiadano: nie istnieje. Powody były dobrze znane.

Dlaczego to jest trudne

Wyobraźmy sobie sieć tysiąca komputerów, z których każdy prowadzi własną kopię księgi rachunkowej. Komputery komunikują się ze sobą przez Internet. Chcemy, żeby wszystkie kopie księgi były identyczne. Pojawiają się trzy problemy.

Pierwszy: opóźnienia. Sygnał elektryczny w światłowodzie biegnie z prędkością około 200 000 km/s. Z Warszawy do Sydney jest około 16 000 km, czyli minimum 80 milisekund w jedną stronę. W praktyce więcej, bo dane idą przez routery, kable nie biegną prosto, a sieć bywa zatłoczona. Realnie – kilkaset milisekund. To znaczy, że gdy w Warszawie wykonujemy transakcję, komputer w Sydney dowie się o niej z opóźnieniem. Jeśli w tej samej sekundzie ktoś zrobi sprzeczną transakcję w Tokio, oba komputery przez jakiś moment będą widziały różne wersje rzeczywistości.

Drugi: nieuczciwi uczestnicy. Niektóre komputery w sieci mogą być wrogie. Mogą celowo wysyłać sprzeczne komunikaty, ignorować część transakcji, kłamać o stanie księgi. W rzeczywistym Internecie nie da się odróżnić uczestnika złośliwego od po prostu zepsutego, a jednych i drugich jest sporo.

Trzy trudności

sieć bez centralnego nadzorcy

1	**OPÓŹNIENIA**	Sygnał potrzebuje czasu. → *„Teraz" nie istnieje.*
2	**KŁAMSTWO**	Część węzłów oszukuje. → *Konsensus mimo sabotażu.*
3	**BRAK TOŻSAMOŚCI**	Każdy ma dowolnie wiele kont. → *Atak Sybilli.*

RAZEM: trzy problemy do rozwiązania.
Bitcoin rozwiązuje wszystkie naraz.

Tabela 1.Trzy fundamentalne trudności przy budowie sieci bez centralnego nadzorcy

Trzeci: brak tożsamości. W sieci anonimowej każdy może utworzyć dowolnie wiele kont. Gdyby decyzje podejmować przez głosowanie większościowe, atakujący po prostu założyłby milion kont i zagłosował sam ze sobą. Problem ten ma swoją nazwę – atak Sybilli – i jest jednym z fundamentalnych ograniczeń systemów rozproszonych.

Zbiorczo problem ten – jak osiągnąć zgodę w sieci komputerów, gdy część z nich może kłamać i nie ma centralnego nadzorcy – został w 1982 roku sformalizowany przez Leslie Lamporta, Roberta Shostaka i Marshalla Pease'a pod nazwą problemu bizantyjskich generałów. Pokazali oni, że jest to problem rozwiązywalny tylko pod pewnymi warunkami i że wymaga kosztownej komunikacji między uczestnikami. Przez następne ćwierć wieku istniały rozwiązania akademickie, ale żadne z nich nie skalowało się do sieci tak dużej i otwartej jak Internet.

W październiku 2008 roku ktoś podpisany jako Satoshi Nakamoto opublikował dziewięciostronicowy dokument, w którym zaproponował rozwiązanie. Dokument nie zawierał ani jednego nowego pomysłu – wszystkie elementy były znane od lat. Nowe było ich połączenie.

Co dalej w tym numerze

W kolejnych częściach przejdziemy przez ten mechanizm warstwa po warstwie.

Zaczniemy od narzędzi kryptograficznych: funkcji skrótu (które pozwalają sprawdzić, czy dane nie zostały zmienione) i podpisów cyfrowych opartych na kryptografii klucza publicznego (które pozwalają udowodnić, że to my wykonujemy operację, nie ujawniając hasła). Następnie pokażemy, jak z tych elementów buduje się łańcuch bloków – strukturę danych, której nie da się po cichu zmodyfikować. Potem przejdziemy do konsensusu: protokołu, który pozwala tysiącom komputerów zgodzić się co do treści tej struktury bez nadzorcy. Omówimy dwa główne podejścia – proof of work, które kosztuje energię, i proof of stake, które kosztuje kapitał – wraz z ich konsekwencjami fizycznymi i ekonomicznymi.

W dalszej części numeru zajmiemy się inteligentnymi kontraktami (Ethereum), problemem skalowalności (dlaczego Bitcoin obsługuje siedem transakcji na sekundę i co z tym zrobiono) oraz zagrożeniami – od ataku 51% po komputery kwantowe. Zakończymy próbą uczciwej

oceny: co z tej technologii prawdopodobnie zostanie z nam na długo, a co jest modą.

Jeden komentarz na koniec wstępu. Krytycy kryptowalut często mówią, że to „spekulacja oparta na powietrzu". Zwolennicy mówią o „rewolucji finansowej". Obie strony mają częściowo rację i obie mylą warstwy. Bitcoin jako instrument finansowy może być spekulacją – to osobna rozmowa. Ale Bitcoin jako konstrukcja inżynieryjna jest faktem: działa od siedemnastu lat bez przerwy, nigdy nie został poważnie zhakowany, obsłużył setki milionów transakcji. Niezależnie od tego, jak potoczy się jego cena, opisane w nim techniki – i ich rozwinięcia w późniejszych systemach – zostały już wykorzystane w kilkudziesięciu poważnych zastosowaniach, od poświadczania dokumentów po dowody w głosowaniach. Nawet jeśli Bitcoin za dwadzieścia lat zniknie, niektóre jego pomysły zostaną.

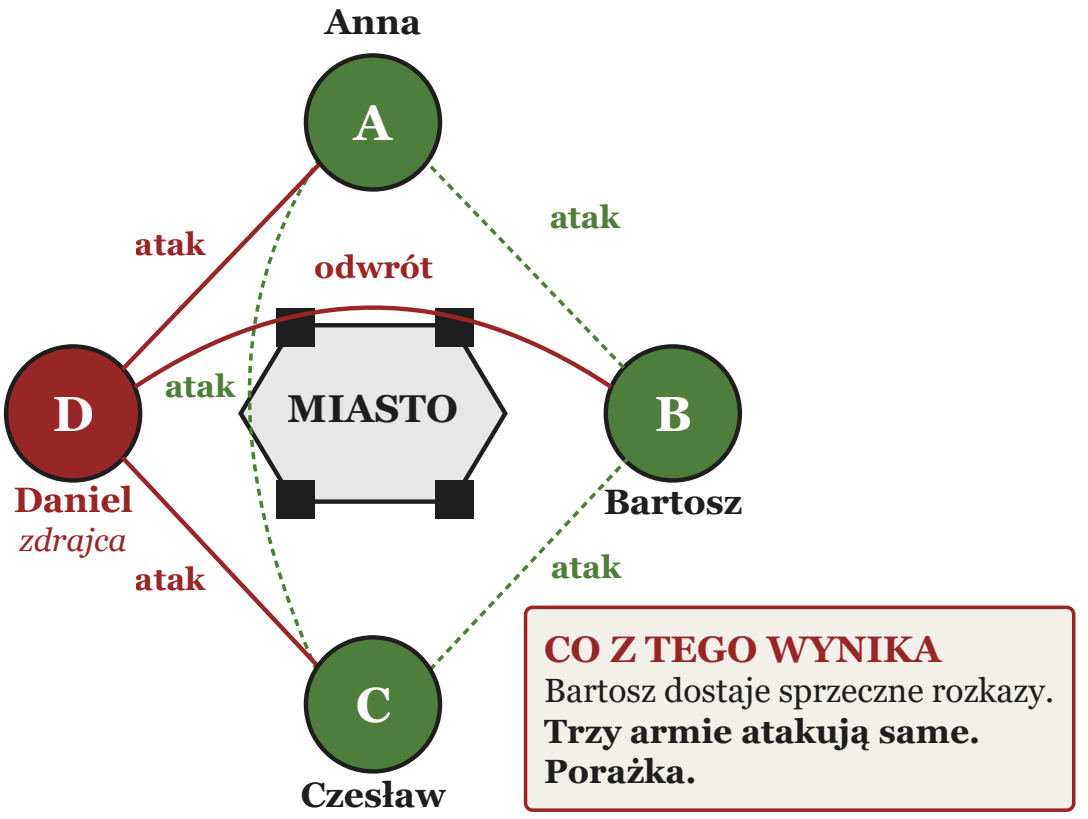
I to pomysły warte zrozumienia.

* * *

W następnym odcinku: funkcje skrótu – czyli jak za pomocą kilkuset linii kodu zamienić dowolnie długi tekst w odcisk palca, którego nie da się podrobić.

Bizantyjscy generałowie

jeden kłamie — czy reszta się porozumie?



Rozwiązanie: **Lamport, 1982.** *Bitcoin dodaje do tego dowód pracy.*

Rysunek 3. Problem bizantyjskich generałów. Czterech dowódców otacza miasto. Jeden z nich jest zdrajcą i wysyła sprzeczne rozkazy. Pytanie: czy pozostali mogą się porozumieć?

Część 2. Funkcje skrótu – odcisk palca dla danych

W pierwszej części zostawiliśmy Czytelnika z problemem: jak zmusić tysiące nieznajomych komputerów do zgody w sprawie zawartości jednej księgi rachunkowej, gdy część z nich kłamie, a żaden nie ma władzy nad innymi. Odpowiedź wymaga kilku osobnych klocków matematycznych. Zaczynamy od najprostszego i najczęściej spotykanego w całej kryptografii: funkcji skrótu.

Funkcja skrótu robi jedną rzecz. Bierze dowolnie długi ciąg bajtów – może to być transakcja, może być cała powieść, może być plik filmowy – i przyporządkowuje mu ciąg o stałej, niewielkiej długości. Ten krótki wynik nazywamy skrótem (po angielsku hash) albo, co jest bardziej obrazowe, odciskiem palca danych. Na potrzeby tego artykułu używać będziemy konkretnej funkcji o nazwie SHA-256, opracowanej w 2001 roku przez amerykańską agencję NSA i wykorzystywanej dziś w Bitcoinie, Ethereum, certyfikatach SSL i tysiącu innych miejsc.

Działa to tak. Bierzemy treść tej części tematu numeru, około dwóch tysięcy słów, i wpuszczamy ją do SHA-256. Po stronie wyjścia dostajemy dokładnie 64 znaki w zapisie szesnastkowym, czyli 256 bitów. Bierzemy zamiast tego pojedyncze słowo „tak” i wpuszczamy do tej samej funkcji. Po stronie wyjścia dostajemy też dokładnie 64 znaki. Bierzemy obraz w wysokiej rozdzielczości, plik MP3 i Pana Tadeusza, sklejone razem. Wynik znów ma 64 znaki.

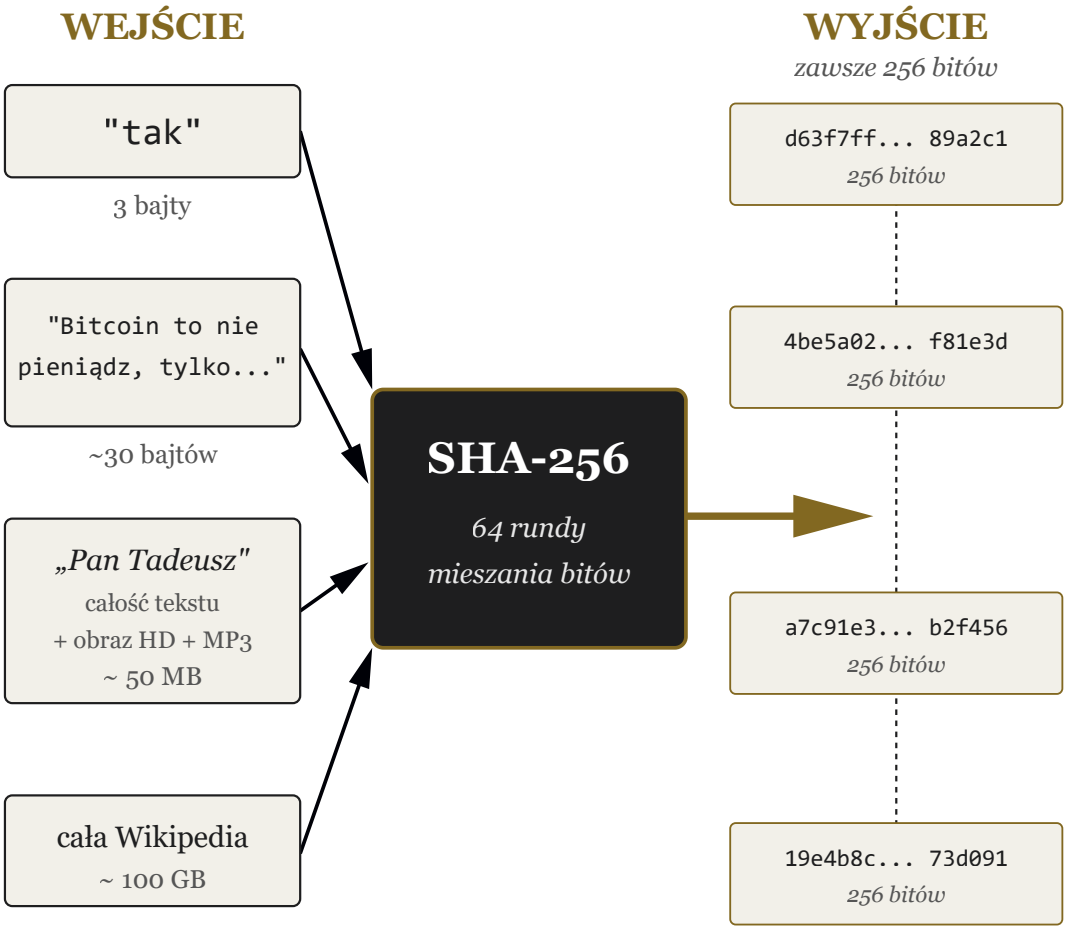
Brzmi to jak oszustwo, bo w sensie informacyjnym jest oszustwem. Funkcja skrótu nie zachowuje informacji – zachowuje odpowiedniość. To znaczy: ta sama treść zawsze daje ten sam skrót, a jakakolwiek zmiana w treści, choćby jednego bitu, daje skrót zupełnie inny.

Demonstracja: dwa słowa różniące się literą

Najlepszą demonstracją tej własności jest pokazanie jej na żywo. Bierzemy dwa wejścia różniące się jednym znakiem – wielkim „T”

Funkcja skrótu jako „czarna skrzynka"

dowolne wejście → zawsze 256 bitów wyjścia



KLUCZOWA OBSERWACJA

Wejście: od 3 bajtów do 100 GB.
Wyjście: zawsze dokładnie 256 bitów.

Funkcja nie zachowuje informacji – zachowuje odpowiedniość.

Rysunek 1. Funkcja skrótu jako czarna skrzynka. Niezależnie od długości wejścia, wyjście ma zawsze 256 bitów

zamienionym na małe „t” – i wyznaczamy dla nich SHA-256.

```
„Młody Technik”  →
9036e8a58c1729730e5798cc976beebb
14e138e8e8ef859851ff1cb1003546a8

„Młody technik”  →
9d3f21533af192731ccfc6effb8a881d
d644d7a3997ba963e5c1fc1bc05cf232
```

Jeden bit zmiany w wejściu (mała litera „t” różni się od dużej „T” jedną pozycją bitową w kodzie ASCII) – i hash zmienia się drastycznie. Konkretnie: ze 256 bitów wyjścia 125 jest różnych. Niemal dokładnie połowa – 48,8 procent – co odpowiada temu, czego można by się spodziewać, gdyby ktoś wziął monetę i 256 razy ją podrzucił.

Tę cechę nazywamy efektem lawinowym (avalanche effect). Zmiana jednego bitu na wejściu zmienia średnio połowę bitów na wyjściu. To nie jest właściwość, którą funkcja skrótu dostaje za darmo – SHA-256 jest specjalnie zaprojektowana tak, żeby tę właściwość mieć. W jej trzewiach znajdują się 64 rundy mieszania bitów, w których każdy bajt wejścia wpływa na każdy bajt wyjścia w sposób, który z punktu widzenia obserwatora wygląda losowo, choć jest w pełni deterministyczny.

Determinizm jest tutaj cechą kluczową. Funkcja skrótu nie używa losowości. Ten sam tekst wpuszczony do niej tysiąc razy da tysiąc razy ten sam wynik. Co więcej – ten sam wynik na komputerze w Warszawie, w Kalifornii i hipotetycznie na Marsie. Identyczność jest gwarantowana matematycznie i jest niezależna od sprzętu, systemu operacyjnego i pogody.

Pięć właściwości, które czynią z tego rzecz użyteczną

Żeby funkcja skrótu nadawała się do kryptografii, musi spełniać pięć warunków. Pierwsze trzy są łatwe; ostatnie dwa są trudne i to one decydują o całej reszcie.

Po pierwsze – determinizm. Już o nim była mowa. Te same dane na wejściu zawsze dają ten sam skrót.

Po drugie – stała długość wyjścia. Niezależnie od tego, czy wejście ma jeden bajt czy terabajt, wyjście ma zawsze 256 bitów. To pozwala porównywać skróty równie szybko niezależnie od tego, czego były skrótem.

Po trzecie – szybkość. Obliczenie SHA-256 dla pliku 1 GB zajmuje na zwykłym laptopie ułamek sekundy. To jest istotne, bo skróty oblicza się często – kilkanaście razy w jednej transakcji bitcoinowej, miliardy razy w jednym bloku.

Po czwarte – jednokierunkowość (po angielsku preimage resistance). Mając skrót, nie można obliczeniowo wywnioskować, co było na wejściu. Nie istnieje funkcja odwrotna do SHA-256 – a precyzyjniej, nie znamy żadnego sposobu odwrócenia jej, który byłby istotnie szybszy od próbowania wszystkich możliwych wejść po kolei. Brzmi to niewinnie, ale to właśnie ta właściwość czyni z funkcji skrótu narzędzie kryptograficzne, a nie tylko sumę kontrolną.

Po piąte – odporność na kolizje (collision resistance). Nie da się znaleźć dwóch różnych wejść, które dawałyby ten sam skrót. Z czysto matematycznego punktu widzenia kolizje muszą istnieć – wejść jest nieskończenie wiele, a wyjść tylko 2 do potęgi 256, czyli skończenie wiele – ale samo ich istnienie nie wystarczy, jeśli ich znalezienie jest nieosiągalne.

Słowo „nieosiągalne” wymaga jednak ilustracji, bo intuicja zawodzi przy liczbach takich jak 2^{256}.

2^{256} – liczba, która łamie wyobraźnię

Dwa do potęgi 256 to liczba, która w zapisie dziesiętnym ma 78 cyfr. Konkretnie:

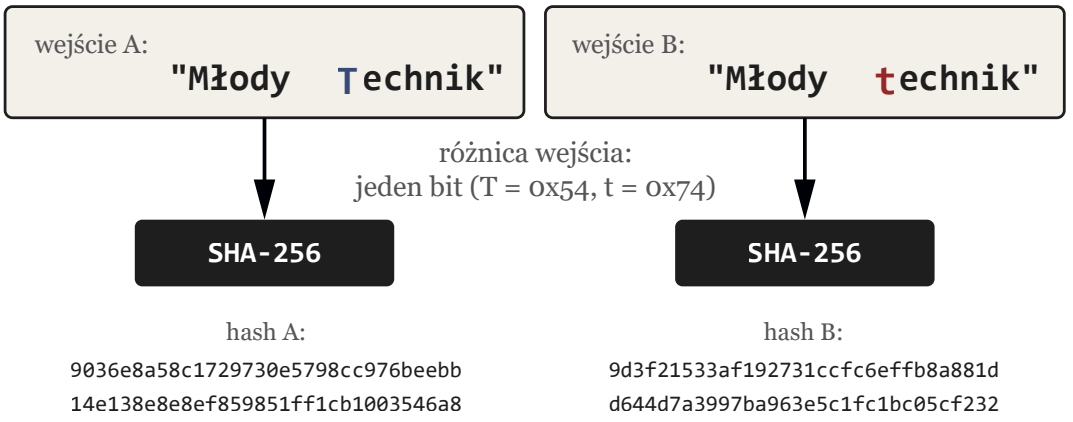
$$2^{256} \approx 1{,}158 \times 10^{77}$$

Dla porównania, liczba atomów w obserwowalnym Wszechświecie, według ostrożnych szacunków, wynosi około 10^{80} – czyli mniej więcej tysiąc razy więcej. To jedyne porównanie, w którym 2^{256} wypada mizernie. We wszystkich innych skalach, do których człowiek ma intuicyjny dostęp, 2^{256} wygrywa miażdżąco.

Co z tego wynika praktycznie? Wyobraźmy sobie, że ktoś chce złamać funkcję SHA-256 metodą siłową – to znaczy znaleźć takie wejście, które daje z góry zadany skrót. Najlepszy znany sposób to próbowanie po kolei wszystkich możliwości. Załóżmy, że atakujący dysponuje wszystkimi koparkami Bitcoina razem wziętymi (co jest absurdalnym założeniem, bo te koparki są zajęte czym innym). W 2025 roku łączna moc obliczeniowa sieci Bitcoin to około 6×10^{20} hashy SHA-256 na sekundę. Przy tej mocy, średni czas na znalezienie konkretnego 256-bitowego skrótu wynosi:

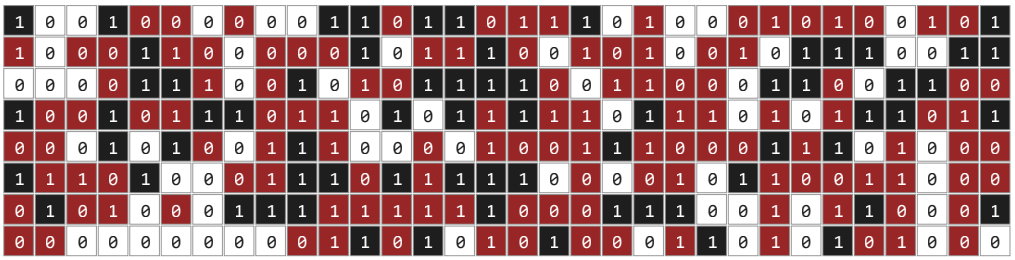
Efekt lawinowy

zmiana 1 bitu na wejściu → ~50% bitów na wyjściu

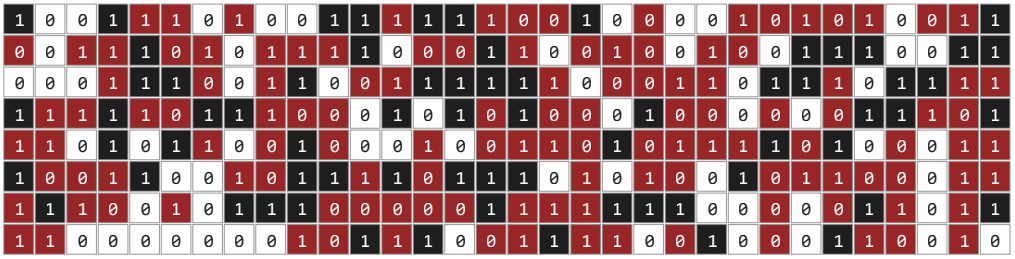


256 bitów obu hashy – bity różne na czerwono

hash A:



hash B:



Bitów różnych: 125 z 256

= 48.8% – niemal idealny rzut monetą

Rysunek 2. Efekt lawinowy. Po lewej: dwa wejścia różniące się jedną literą. Po prawej: oba hashe rozłożone na bity z zaznaczeniem różnic – 125 z 256 bitów

$(2^{256}/2)/(6\times10^{20})\approx3\times10^{48}$ sekund

Tymczasem wiek Wszechświata wynosi około 4×10^{17} sekund. Oznacza to, że nawet używając wszystkich koparek świata, atakujący potrzebowałby około 10^{31} wieków Wszechświata, żeby z prawdopodobieństwem 50 procent znaleźć preimage. To nie jest „bardzo długo". To jest liczba, która na poziomie fizyki nie ma sensu.

I to jest właśnie sedno bezpieczeństwa kryptograficznego. Nikt nie udowadnia, że SHA-256 jest „nie do złamania" – udowadnia się jedynie, że żadna znana metoda nie wymaga mniej niż mniej więcej 2^128 operacji, co przy obecnych

Skala 2^{256}

liczba możliwych skrótów SHA-256 na tle wybranych wielkości

$2^{256} \approx 1{,}158 \times 10^{77}$

to liczba 78-cyfrowa. Dla porównania:

Co to jest	Ile	Skala (log)
Liczba ludzi na Ziemi	$\approx 8 \times 10^{9}$	
Sekund od Wielkiego Wybuchu	$\approx 4 \times 10^{17}$	
Hashe SHA-256 / sekundę (Bitcoin)	$\approx 6 \times 10^{20}$	
Ziarna piasku na plażach Ziemi	$\approx 7 \times 10^{21}$	
Gwiazdy w obserwowalnym Wszechświecie	$\approx 10^{23}$	
2^{256} — przestrzeń SHA-256	$\approx 1{,}16 \times 10^{77}$	
Atomy w obserwowalnym Wszechświecie	$\approx 10^{80}$	

Co z tego wynika?

Cała sieć Bitcoin (6×10^{20} hashy/s) potrzebowałaby **10^{31} wieków Wszechświata**, by sforsować jeden konkretny skrót.

To nie jest „bardzo długo". To liczba, która na poziomie fizyki nie ma sensu.

Tabela 1. Skala 2^{256} w porównaniu z wybranymi wielkościami fizycznymi i obliczeniowymi

SPRÓBUJ SAM

Funkcji SHA-256 nie trzeba implementować – jest wbudowana w każdy nowoczesny język programowania. W Pythonie wystarczą trzy linijki:

```
import hashlib
h = hashlib.sha256("Młody Technik".encode()).hexdigest()
print(h)
```

Wynik: `9036e8a58c172973...` – taki sam jak u nas i taki sam u każdego, kto uruchomi te trzy linijki. Można też skorzystać z linii poleceń. Na Linuksie i macOS wystarczy:

```
echo -n "Młody Technik" | sha256sum
```

Polecam wypróbować zmianę jednego znaku w tekście wejściowym i porównanie obu wyników. Efekt lawinowy widać gołym okiem.

prędkościach przekracza możliwości obecnej i przewidywalnej fizyki.

Po co to wszystko

Wszystkie pięć właściwości – determinizm, stała długość, szybkość, jednokierunkowość, odporność na kolizje – są nam potrzebne w kryptowalutach, każda z innego powodu.

Determinizm pozwala dwóm różnym węzłom sieci niezależnie obliczyć skrót tej samej transakcji i sprawdzić, że dostały ten sam wynik. Bez tego nie byłoby żadnej zgody co do treści księgi.

Stała długość pozwala upakować skrót transakcji w nagłówku bloku, w łączu drzewa Merklego (o nim w jednej z kolejnych części) i w wielu innych miejscach, gdzie potrzebny jest „uchwyt" do większej porcji danych.

Szybkość pozwala węzłom weryfikować nowy blok w sekundach, mimo że blok zawiera tysiące transakcji.

Jednokierunkowość jest fundamentem mechanizmu wydobywczego – tego, co potocznie nazywa się „kopaniem" bitcoinów. Wymaga osobnego rozdziału, bo splata się z budową łańcucha bloków, ekonomią ludzi obsługujących sprzęt obliczeniowy i grą sił, które utrzymują sieć w równowadze. W tym miejscu wystarczy zaznaczyć: bez tej jednej właściwości – bez tego, że SHA-256 jest jednokierunkowa – cała konstrukcja Bitcoina by się rozsypała. Wrócimy do tego w jednej z kolejnych części, gdy zdefiniujemy wszystkie potrzebne pojęcia.

Odporność na kolizje pozwala podpisywać dokumenty cyfrowo. Gdyby dało się znaleźć dwa różne dokumenty z tym samym skrótem, podpis pod jednym mógłby zostać przeniesiony na drugi. To temat na następną część artykułu – kryptografię klucza publicznego.

Inne funkcje skrótu i historia jednej awarii

SHA-256 to nie jedyna funkcja skrótu w użyciu. Istniała przedtem rodzina MD5 i SHA-1, dziś już złamane na poziomie odporności na kolizje (choć MD5 nadal się używa do sum kontrolnych plików, gdzie kolizje nie mają znaczenia dla bezpieczeństwa). W 2017 roku Google opublikował dwa różne pliki PDF dające ten sam skrót SHA-1 – pierwszy publiczny dowód praktycznej kolizji w funkcji uważanej dotąd za bezpieczną. SHA-1 została wycofana z certyfikatów internetowych w 2017 roku.

Obok SHA-256 istnieją alternatywy. SHA-3, opublikowany przez NIST w 2015 roku, ma zupełnie inną konstrukcję wewnętrzną (tzw. konstrukcja gąbki). BLAKE2 i BLAKE3, opracowane akademicko, są szybsze przy podobnym poziomie bezpieczeństwa. Bitcoin zdecydował się na SHA-256, bo była dobrze przebadana w momencie powstawania protokołu (2008) i nadal nie ma żadnych znanych słabości. W kryptografii konserwatyzm jest cnotą – używa się tego, co działa od dziesięciu lat bez awarii, nie tego, co jest najnowsze.

* * *

W kolejnej części: kryptografia klucza publicznego – czyli jak udowodnić, że to ja, nie ujawniając hasła. A potem złożymy oba klocki – funkcję skrótu i klucz publiczny – w mechanizm transakcji bitcoinowej.

Część 3. Klucze publiczne i podpisy cyfrowe

W Części 2 dostaliśmy do ręki funkcję skrótu – narzędzie, które dla dowolnych danych daje ich krótki, jednoznaczny odcisk palca. To pierwszy klocek. W tej części dokładamy drugi: kryptografię klucza publicznego. To ona pozwoli udowodnić, że jesteśmy uprawnieni do wydania bitcoinów – bez ujawniania komukolwiek, dlaczego.

Problem, którego nie umiały rozwiązać banki

Wyobraźmy sobie, że chcemy przelać przez internet komuś pieniądze. W tradycyjnym banku robi to za nas instytucja: my logujemy się hasłem, bank weryfikuje, że hasło pasuje do naszego konta, i wykonuje przelew. Hasło zna bank – i nikt poza nim. To działa, ale tylko dlatego, że wszyscy ufamy bankowi. Bank pełni rolę tłumacza między „ja chcę przelać" a „wykonano przelew".

W kryptowalutach takiej instytucji nie ma. Sieć Bitcoina to miliony komputerów na całym świecie – każdy z osobna może być uczciwy albo nie, polski albo północnokoreański, prywatny albo państwowy. Nie ufamy żadnemu z nich z osobna. Jak więc przekonać taką sieć, że to faktycznie my mamy prawo wydać bitcoiny przypisane do naszego konta?

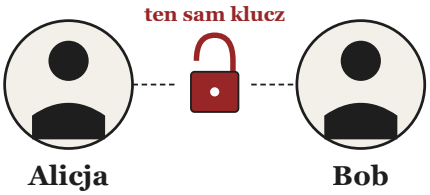
Najprostszy pomysł – wysłać hasło – natychmiast upada. W banku to działa, bo hasło zna jeden zaufany podmiot. W otwartej sieci wysłanie hasła oznacza pokazanie go wszystkim po drodze. Pierwszy nieuczciwy węzeł sieci może je przechwycić i wysłać kolejny przelew w naszym imieniu, opróżniając nasze konto. Hasło

Szyfr symetryczny vs asymetryczny

jeden sekret czy dwa klucze?

SYMETRYCZNY

jeden wspólny klucz



PROBLEM

Jak wymienić klucz przez sieć, której nie ufamy?

Każdy podsłuchujący też pozna sekret.

Działa, gdy:

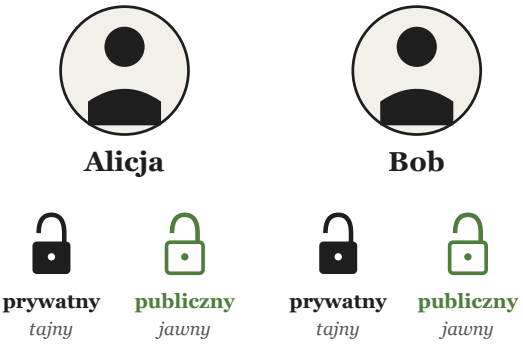
spotkają się osobiście, by ustalić klucz.

— np. ambasada, wojsko, bank z klientem.

W otwartej sieci: NIE.

ASYMETRYCZNY

para kluczy: prywatny + publiczny



DZIAŁA

Klucze publiczne wymieniamy jawnie.
Klucz prywatny nie opuszcza właściciela.

Bezpieczeństwo: matematyka, nie zaufanie.

Działa nawet w sieci, której nie ufamy.

Kluczowa własność asymetrii

Co zaszyfrujesz kluczem prywatnym → odszyfrujesz tylko publicznym (i odwrotnie)

Z klucza publicznego → nie da się obliczyć prywatnego

...mimo że są ze sobą matematycznie powiązane.

SZYFROWANIE

Bob szyfruje wiadomość kluczem publicznym Alicji.

Tylko Alicja może odszyfrować — ma klucz prywatny.

Bob sam już swojego szyfru nie odczyta.

PODPIS CYFROWY

Alicja podpisuje wiadomość kluczem prywatnym.

Każdy weryfikuje podpis kluczem publicznym Alicji.

→ *to jest fundament Bitcoina.*

Rysunek 1. Szyfr symetryczny vs. szyfr asymetryczny. Po lewej: jeden wspólny sekret – działa, jeśli mamy jak go bezpiecznie wymienić. Po prawej: para kluczy – działa nawet w sieci, której nie ufamy

to sekret, który po jednorazowym ujawnieniu traci wartość.

Potrzebujemy czegoś innego: mechanizmu, który pozwoli udowodnić, że znamy sekret, nie ujawniając samego sekretu. Brzmi jak paradoks. Przez całą historię ludzkości – od starożytnych Greków po II wojnę światową – coś takiego nie istniało. Pojawiło się dopiero w 1976 roku.

Pomysł, który zmienił kryptografię

W lipcu 1976 roku dwóch badaczy ze Stanford University, Whitfield Diffie i Martin Hellman, opublikowało artykuł zatytułowany „New Directions in Cryptography". Zaproponowali w nim coś, co dziś nazywamy kryptografią asymetryczną – ale na potrzeby tego artykułu wystarczy nazwa „kryptografia klucza publicznego".

Pomysł jest następujący. Zamiast jednego sekretu używamy pary kluczy: prywatnego i publicznego. To dwie matematyczne wartości połączone tak ściśle, że można powiedzieć – są jak dwie strony tej samej monety. Klucz prywatny trzymamy dla siebie. Klucz publiczny dajemy każdemu, kto chce. Co najważniejsze – z klucza publicznego nie da się obliczyć klucza prywatnego, mimo że są ze sobą matematycznie powiązane.

Te dwa klucze mają niezwykłą własność: są wzajemnie odwrotne. Co zaszyfrowaliśmy kluczem prywatnym, można odszyfrować tylko kluczem publicznym – i na odwrót. Z tego wynikają dwa zupełnie różne zastosowania.

Pierwsze: szyfrowanie. Jeśli ktoś chce wysłać nam tajną wiadomość, szyfruje ją naszym kluczem publicznym. Tylko my – posiadacze odpowiadającego mu klucza prywatnego – możemy ją odszyfrować. Ciekawe: ten, kto zaszyfrował, sam już swojego szyfru nie odczyta.

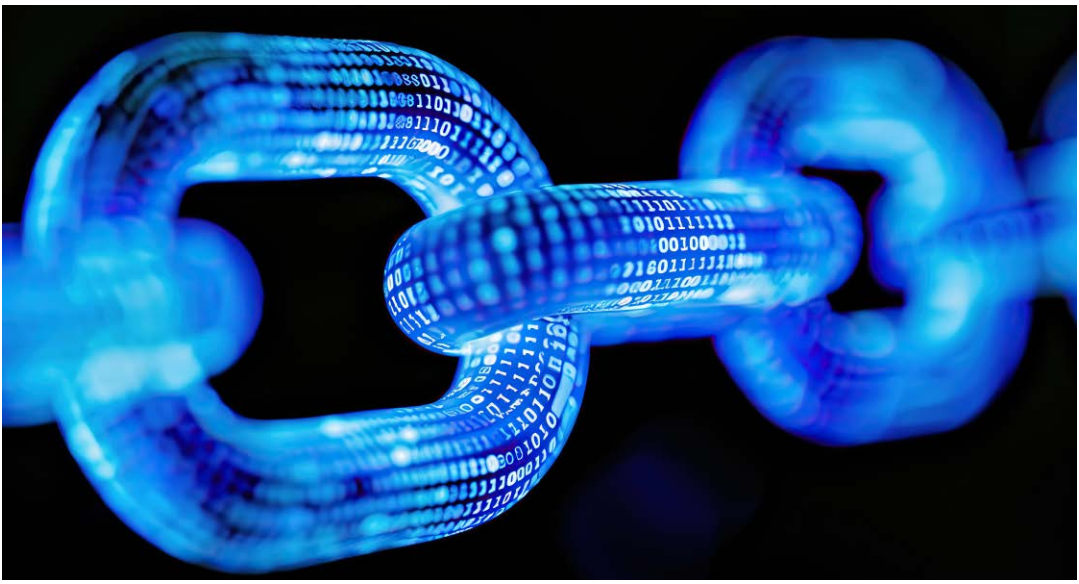
Drugie: podpis cyfrowy. Jeśli chcemy udowodnić, że to my jesteśmy autorem jakiejś wiadomości, „szyfrujemy" ją (mówimy: podpisujemy) naszym kluczem prywatnym. Każdy, kto ma nasz klucz publiczny, może sprawdzić, że odpowiedni klucz prywatny faktycznie był użyty – czyli że wiadomość pochodzi od nas. Ale sam tego podpisu wytworzyć nie potrafi.

To drugie zastosowanie jest fundamentem Bitcoina. Bo to właśnie podpisy cyfrowe pozwalają udowodnić, że jesteśmy uprawnieni do wydania monet – bez pokazywania komukolwiek, dlaczego.

Krzywe eliptyczne – geometria Bitcoina

Pierwsza realizacja pomysłu Diffiego i Hellmana – algorytm RSA z 1977 roku – opierała się na trudności rozkładu dużych liczb na czynniki pierwsze. RSA działa do dziś i pozostaje fundamentem certyfikatów internetowych. Ale Bitcoin używa innej, nowszej rodziny algorytmów: kryptografii krzywych eliptycznych (ECC, od Elliptic Curve Cryptography).

Powód jest praktyczny. Żeby uzyskać poziom bezpieczeństwa porównywalny z 2^{128} prób (taki

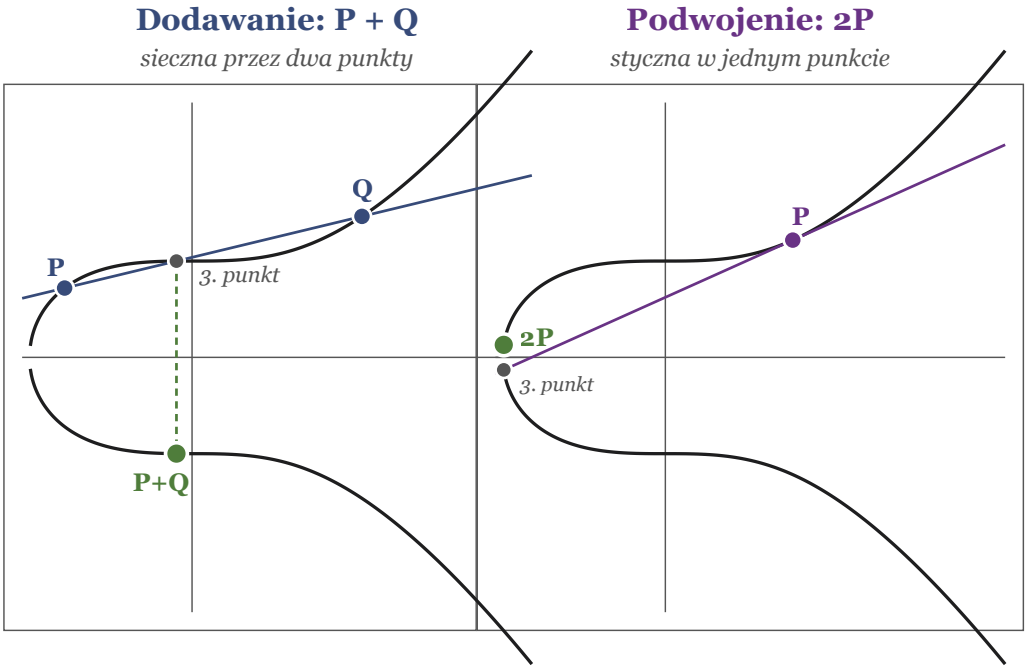


jakiego wymagamy od solidnej kryptografii), RSA potrzebuje klucza długości około 3072 bitów. Krzywa eliptyczna daje to samo bezpieczeństwo przy kluczu 256-bitowym. Dwanaście razy krócej. W systemie, w którym każdy klucz publiczny musi być przechowywany w księdze widocznej dla całego świata, to różnica między systemem działającym a niedziałającym.

Krzywa secp256k1 i „dodawanie" punktów

równanie krzywej Bitcoina:

$$y^2 = x^3 + 7$$



REGUŁA „DODAWANIA" PUNKTÓW (czysta geometria, bez równań):

P + Q: sieczna przez P i Q przetnie krzywą w trzecim punkcie. Odbij go względem osi x.

2P: jeśli dodajemy punkt do siebie, zamiast siecznej rysujemy styczną w P. Odbij i gotowe.

Powtarzając, można policzyć 3P, 4P, 100P, milion razy P – zawsze zostając na krzywej.

KLUCZOWA NIERÓWNOŚĆ

Mając **k** i punkt **G** → policzyć **kG** jest łatwe **[TAK]**

Mając **G** i wynik **kG** → odzyskać **k** jest niemożliwe **[NIE]**

To problem logarytmu dyskretnego na krzywej eliptycznej.

Dla secp256k1: ~ 2^{128} operacji (czyli niewykonalnie).

k = klucz prywatny · **kG** = klucz publiczny

Rysunek 2. Krzywa secp256k1 (równanie $y^2 = x^3 + 7$) i geometryczna definicja „dodawania" punktów. Po lewej: P + Q jako odbicie trzeciego punktu przecięcia siecznej. Po prawej: 2P jako odbicie punktu przecięcia stycznej.

Krzywa eliptyczna to dla matematyka konkretny obiekt: zbiór wszystkich punktów (x, y) spełniających równanie postaci $y^2 = x^3 + ax + b$, dla pewnych ustalonych liczb a i b. Bitcoin używa krzywej o nazwie secp256k1, gdzie a = 0 i b = 7 – więc równanie skraca się do:

$$y^2 = x^3 + 7$$

Wykres tej krzywej (po lewej stronie rysunku 2) wygląda jak symetryczna względem osi poziomej fala. Wszystkie punkty leżące na tej krzywej tworzą zbiór, w którym matematycy zdefiniowali specjalną operację – nazywają ją „dodawaniem punktów", choć z dodawaniem liczb ma niewiele wspólnego. Reguła geometryczna jest zaskakująco prosta i warto się jej przyjrzeć, bo to ona stoi za bezpieczeństwem każdego adresu bitcoinowego.

Jak „dodać" dwa punkty A i B leżące na krzywej? Prowadzimy przez nie linię prostą. Ta prosta przetnie krzywą w jeszcze jednym, trzecim punkcie. Bierzemy ten trzeci punkt i odbijamy go lustrzanie względem osi poziomej (zmieniamy znak współrzędnej y). Otrzymany punkt nazywamy A + B. Tyle. Bez algebry, bez równań – czysta geometria.

A jak „dodać" punkt do samego siebie, czyli policzyć A + A? Zamiast siecznej prowadzimy styczną do krzywej w punkcie A. Ona też przetnie krzywą w jednym dodatkowym punkcie. Odbijamy go lustrzanie i mamy 2A. Powtarzając to, możemy obliczyć 3A, 4A, 100A, milion razy A – zawsze zostając na krzywej.

I tu pojawia się kluczowa nierówność. Jeśli ktoś poda nam liczbę k i punkt G, możemy stosunkowo szybko policzyć wynik kG (wielokrotność punktu G). To po prostu wielokrotne wykonanie tej geometrycznej operacji. Ale operacja odwrotna – mając punkt G i wynik kG, wyliczyć k – jest praktycznie niewykonalna. To matematyczny odpowiednik funkcji jednokierunkowej z Części 2: w jedną stronę szybko, w drugą niewykonalnie.

To zjawisko nosi nazwę problemu logarytmu dyskretnego na krzywej eliptycznej. Najlepszy znany algorytm jego rozwiązania dla krzywej secp256k1 wymaga około 2^{128} operacji – czyli, zgodnie z rachunkiem z Części 2, mniej więcej tylu wieków Wszechświata, ile mieści się w niewyobrażalnie dużej liczbie.

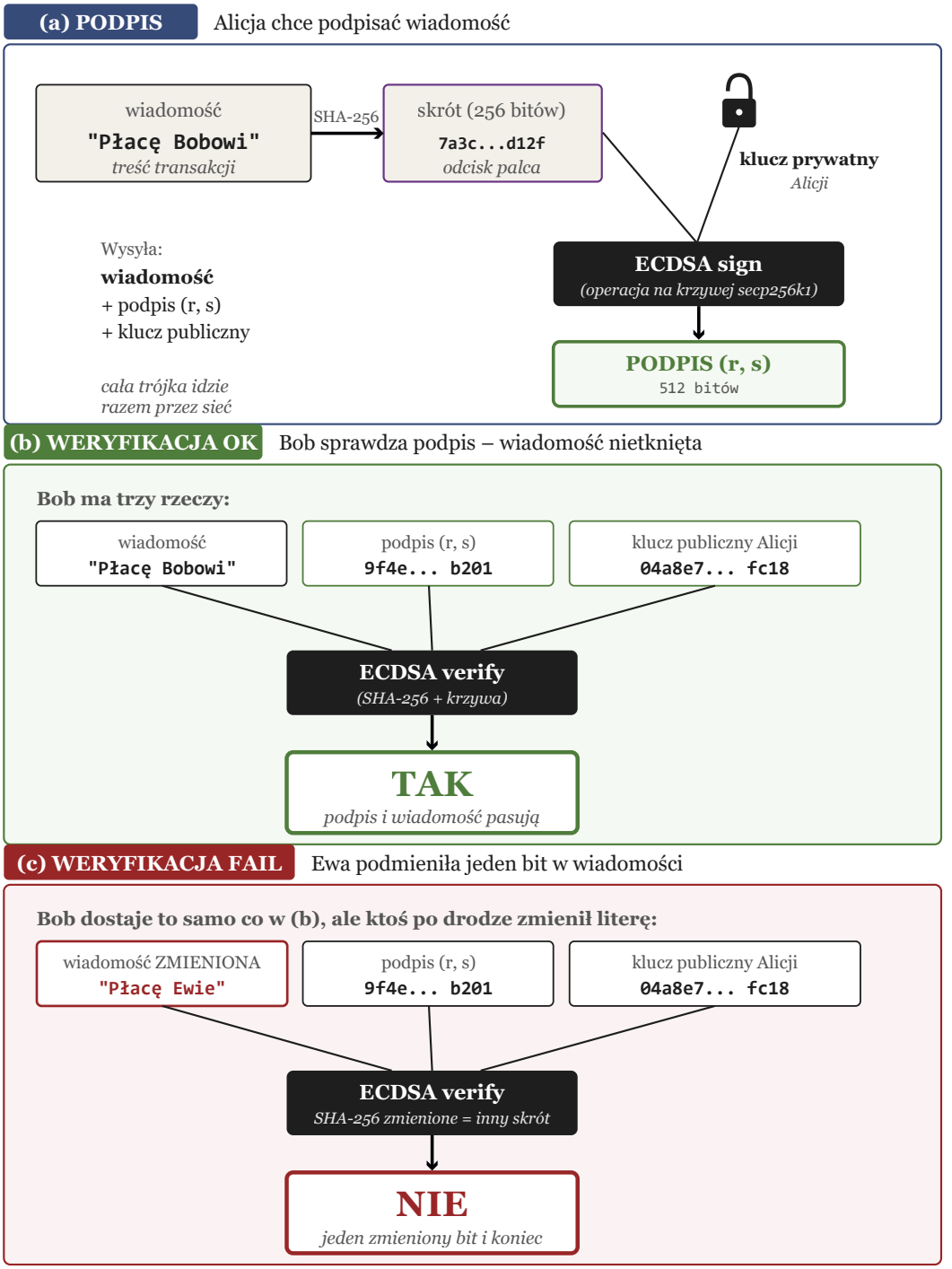
I to jest cały sekret. Nasz klucz prywatny to liczba k. Nasz klucz publiczny to punkt kG, gdzie G jest pewnym ustalonym dla całego Bitcoina punktem na krzywej (tzw. punkt generatora G). Każdy może sobie obliczyć kG mając k. Nikt nie potrafi obliczyć k mając kG.

Jak podpisuje się wiadomość

Mając parę kluczy, możemy wreszcie podpisywać wiadomości. Algorytm używany w Bitcoinie nazywa się ECDSA (Elliptic Curve Digital

Mechanizm podpisu cyfrowego

algorytm ECDSA: trzy proste kroki



Rysunek 3. Mechanizm podpisu cyfrowego. (a) Alicja podpisuje wiadomość kluczem prywatnym. (b) Bob weryfikuje, używając klucza publicznego Alicji. (c) Co się dzieje, gdy ktoś po drodze zmieni jeden bit wiadomości

Z BLIŻSZA: ILE BITÓW MA KLUCZ PUBLICZNY?

Klucz publiczny to punkt na krzywej, czyli para współrzędnych x i y. Dla krzywej secp256k1 każda z nich jest liczbą 256-bitową, więc pełny klucz publiczny to 512 bitów (64 bajty). W praktyce Bitcoin dokleja jeszcze jeden bajt prefiksu (wartość 0x04), który oznacza „dalej idzie pełen punkt z obiema współrzędnymi" – daje to 65 bajtów łącznie.

Ale to nie wszystko. Bitcoin używa sprytnej sztuczki, która pozwala go skrócić niemal o połowę. Skoro krzywa ma równanie $y^2 = x^3 + 7$, to mając samo x możemy obliczyć y^2 i wyciągnąć pierwiastek. Pierwiastek z dowolnej liczby dodatniej daje dwa wyniki – jeden dodatni, jeden ujemny. To dlatego krzywa eliptyczna jest symetryczna względem osi poziomej (jeszcze raz spójrz na rysunek 2): każda wartość x ma dwa odpowiadające jej punkty na krzywej, jeden „nad", drugi „pod" osią x.

Wystarczy więc zapisać samo x – czyli 256 bitów – plus jeden dodatkowy bit, mówiący „bierz górną gałąź" albo „bierz dolną". Bitcoin koduje ten dodatkowy bit jako prefiks 0x02 (gałąź dolna) lub 0x03 (gałąź górna). Otrzymujemy klucz długości 33 bajtów zamiast 65. Nazywa się to „kluczem publicznym skompresowanym" i jest dziś standardem we wszystkich nowych portfelach.

Trzy postacie tego samego klucza:

```
para (x, y)             64 B    matematyczna postać czysta
0x04 || x || y          65 B    zapis pełny (uncompressed)
0x02|03 || x            33 B    zapis skompresowany - standard
```

Wszystkie trzy odpowiadają temu samemu punktowi na krzywej. W obliczeniach matematycznych używa się zwykle pełnej pary (x, y); w przesyłaniu i przechowywaniu – wersji skompresowanej. Klucz prywatny w obu przypadkach pozostaje 256-bitowy.

Signature Algorithm). Z punktu widzenia użytkownika robimy trzy rzeczy.

Krok pierwszy: liczymy SHA-256 dla wiadomości, którą chcemy podpisać. To technika z Części 2 – z wiadomości dowolnej długości robi się 256-bitowy odcisk palca. Podpisywać będziemy ten odcisk, nie samą wiadomość, bo jest krótszy i ma stałą długość.

Krok drugi: używając klucza prywatnego k oraz losowo wybranej liczby (tzw. nonce, ważnego dla bezpieczeństwa szczegółu, do którego za chwilę wrócimy), obliczamy podpis. Wynik to dwie liczby: r i s, łącznie 512 bitów. To jest właśnie podpis cyfrowy.

Krok trzeci: każdy, kto chce sprawdzić nasz podpis, bierze: oryginalną wiadomość, nasz podpis (r, s) i nasz klucz publiczny kG. Wykonuje określoną sekwencję operacji na krzywej eliptycznej i otrzymuje wynik „TAK" lub „NIE". TAK znaczy: podpis pasuje do wiadomości i do tego klucza publicznego. NIE znaczy: ktoś podmienił wiadomość albo podpisał ktoś inny.

Najpiękniejsze jest to, że weryfikacja – krok trzeci – nie wymaga znajomości klucza prywatnego. Każdy może sprawdzić nasz podpis. Nikt poza nami nie może go wytworzyć.

I jeszcze jedna własność, która okaże się kluczowa: jeśli choćby jeden bit wiadomości zostanie zmieniony, weryfikacja od razu zwróci NIE. Bo skrót SHA-256 zmienionej wiadomości będzie zupełnie inny – dzięki efektowi lawinowemu

DLACZEGO ADRESY SIĘ NIE ZDERZAJĄ

Skoro każdy może wygenerować sobie klucz prywatny, biorąc 32 losowe bajty z generatora liczb losowych – to czy nie zdarzy się przypadkiem, że dwie osoby wylosują ten sam? A jeśli ktoś losuje miliardami w nadziei trafienia w cudzy adres?

Liczba możliwych kluczy prywatnych Bitcoina: 2^{256}, czyli ta sama liczba co możliwych skrótów SHA-256 z Części 2. Adresów jest „tylko" 2^{160}, bo na końcu obcinamy do 160 bitów przez RIPEMD-160. To wciąż liczba w okolicy 10^{48}.

Gdyby wszystkie komputery na Ziemi – wszystkie smartfony, serwery, koparki Bitcoina – pracowały razem przez cały czas istnienia Wszechświata, generując po milion adresów na sekundę, prawdopodobieństwo trafienia w cudzy aktywny adres byłoby porównywalne z prawdopodobieństwem wylosowania konkretnego atomu z dziesięciu losowo wybranych Ziemi.

Innymi słowy: nie. Adresy się nie zderzają. Nigdy.

Od klucza prywatnego do adresu

każdy etap idzie tylko w jedną stronę

SEKRET

1. KLUCZ PRYWATNY

256 losowych bitów

`1e99423a4ed276...a526aedd`

`32 bajty z generatora liczb losowych`

ECC: pomnóż k razy G

2. KLUCZ PUBLICZNY

punkt na krzywej secp256k1: kG

`x: f028892bad7e...dc341a`

`y: 07cf33da18bd...505bdb`

SHA-256

3. SHA-256

skrót klucza publicznego

`8823c6b7765421...98320fe0`

`256 bitów`

RIPEMD-160

4. RIPEMD-160

drugi skrót, krócej

`211b74ca4686f8...16dafe0b`

`160 bitów (hash160)`

Base58Check (prefix + suma kontrolna)

JAWNE

5. ADRES (Base58Check)

prefix + hash160 + suma kontrolna

`1424C2F4bC9JidNjjTUZCbUxv6Sa1Mt62x`

`to wpisuje się w portfelu`

DLACZEGO ŁAŃCUCH IDZIE TYLKO W JEDNĄ STRONĘ

W dół (od klucza prywatnego do adresu): każdy etap to kilka prostych obliczeń. W górę (od adresu do klucza prywatnego): nie da się — krzywa eliptyczna i funkcje skrótu są jednokierunkowe, każda z osobna.

Adres można pokazać światu. Klucz prywatny zostaje sekretem.

Rysunek 4. Pełen łańcuch przekształceń: od 256 losowych bitów klucza prywatnego do adresu bitcoinowego. Każdy etap z konkretnym przykładem. Każda strzałka idzie tylko w jedną stronę

SPRÓBUJ SAM

W Pythonie wygenerowanie pary kluczy ECDSA i podpisanie wiadomości to kilka linijek. Wystarczy doinstalować bibliotekę „ecdsa” (przez pip install ecdsa):

```
from ecdsa import SigningKey, SECP256k1
sk = SigningKey.generate(curve=SECP256k1)
vk = sk.verifying_key
podpis = sk.sign(b”Witaj, Bitcoinie”)
print(vk.verify(podpis, b”Witaj, Bitcoinie”))
```

Wynik: True. Spróbuj zmienić jeden znak w wiadomości w ostatniej linijce – weryfikacja zwróci False. Spróbuj wygenerować drugą parę kluczy i podpisać tym samym podpisem – weryfikacja też zwróci False. To jest dokładnie ten sam mechanizm, którego używa Twój portfel bitcoinowy, kiedy wykonujesz przelew.

z Części 2. Podpis i wiadomość są nierozerwalnie związane.

Drobna techniczna uwaga, do której obiecaliśmy wrócić: nonce (number used once) w kroku drugim musi być za każdym razem inny i naprawdę losowy. Jeśli się powtórzy, można z dwóch podpisów odzyskać klucz prywatny. W 2010 roku z tego powodu skradziono wszystkie bitcoiny ze złamanego w ten sposób portfela na PlayStation 3. W 2013 roku – wszystkie bitcoiny z aplikacji Android, której generator liczb losowych miał wadę. To są historie z gatunku tych, które nawet doświadczeni programiści powtarzają sobie przed snem zamiast straszyć dzieci.

Od klucza prywatnego do adresu bitcoinowego

Mamy już komplet: klucz prywatny w postaci 256-bitowej liczby, klucz publiczny, tj. punkt na krzywej – para liczb (współrzędne x,y tego punktu) po 256 bitów każda i podpis cyfrowy. Ale gdy ktoś przelewa nam bitcoiny, nie wpisuje pełnego klucza publicznego – czyli całych 512 bitów punktu (x, y). Wpisuje krótki ciąg w rodzaju 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa. To jest adres bitcoinowy.

Adres powstaje z klucza publicznego przez ciąg przekształceń. Każde z nich pełni konkretną funkcję.

Pierwszy etap: bierzemy klucz publiczny i liczymy z niego SHA-256. Dostajemy 256 bitów.

Drugi etap: na otrzymanych 256 bitach wykonujemy jeszcze jedną funkcję skrótu – RIPEMD-160. Skraca ona wynik do 160 bitów. Dlaczego dwie różne funkcje skrótu jedna po drugiej? Bezpieczeństwo. Gdyby kiedyś znaleziono słabość w SHA-256, atakujący wciąż musiałby też pokonać RIPEMD-160. To strategia, którą kryptografowie nazywają hash defense in depth – obroną w głąb.

Trzeci etap: do tych 160 bitów (20 bajtów) dodajemy z przodu jeden bajt mówiący „to jest adres głównej sieci Bitcoin” (wartość 0x00) oraz 4 bajty sumy kontrolnej, obliczonej jako pierwsze 4 bajty z podwójnego SHA-256 powyższych danych. Suma kontrolna chroni przed literówkami: jeśli ktoś wpisze adres błędnie, oprogramowanie portfela natychmiast to wychwyci, bo suma kontrolna nie będzie pasować.

Czwarty etap: całość – 25 bajtów – kodujemy w specjalnym alfabecie zwanym Base58. To zwykły zapis dziesiętny rozszerzony do 58 znaków: cyfry 1-9 i litery A-Z, a-z, ale bez 0, O, I i l, które łatwo pomylić wzrokowo. Ten zapis jest krótszy niż szesnastkowy i odporny na literówki. To, co wychodzi z tego kodowania, jest właśnie naszym adresem.

Z klucza prywatnego można obliczyć klucz publiczny. Z klucza publicznego można obliczyć adres. W drugą stronę żaden z tych kroków się nie odwraca. Dlatego w bitcoinie można pokazać adres całemu światu – i nadal mieć pełną kontrolę nad środkami. To jeden sekret (klucz prywatny) i jego trzy publiczne pochodne (klucz publiczny, hash160, adres), z których każda kolejna jest jeszcze bardziej publiczna i jeszcze trudniejsza do odwrócenia.

* * *

Mamy już oba klocki: funkcję skrótu z Części 2 i parę kluczy z tej części. W kolejnym odcinku złożymy je w transakcję bitcoinową – pokażemy, co dokładnie podpisujemy, gdy „przelewamy bitcoiny”, i zobaczymy, jak transakcje grupują się w bloki, tworząc strukturę zwaną drzewem Merklego.

Część 4. Transakcje, drzewa Merklego, blok

Mamy już funkcję skrótu z Części 2 i kryptografię klucza publicznego z Części 3. To są dwa narzędzia. Czas złożyć z nich coś, co dla większości ludzi pozostaje tajemnicą – czyli: co to właściwie znaczy „mieć bitcoiny". Bo nie znaczy tego, co intuicyjnie sądzimy.

Co to właściwie jest „bitcoin"

Większość ludzi wyobraża sobie bitcoiny jako pliki na dysku albo jako liczbę przypisaną do ich konta – coś jak saldo w aplikacji bankowej. Ani jedno, ani drugie nie jest prawdą. To jest moment, w którym warto skupić uwagę, bo dalsze rozumienie zależy od tego, co się tu zaaprobuje.

W bazie danych Bitcoina nie istnieje pole „saldo Pawła". Nie istnieje pojęcie konta. Istnieje natomiast lista wszystkich transakcji od początku świata Bitcoina (a konkretnie od 3 stycznia 2009 roku) – i tylko ona. Każda transakcja pokazuje, że jakaś kwota przeszła z jednego adresu na inny. Cała historia. Wszystko.

Jeśli chcę dowiedzieć się, ile mam bitcoinów, mój portfel robi coś niedorzecznego z punktu widzenia bankowca: przegląda historię i sumuje wszystkie kwoty, które kiedykolwiek do mnie trafiły, i odejmuje wszystkie, które kiedykolwiek wysłałem. To, co zostaje, to moje saldo. Nie ma go nigdzie zapisanego – jest tylko obliczone na żądanie.

Jeszcze precyzyjniej: portfel patrzy na każdą transakcję, w której do mojego adresu trafiły

Konto bankowe vs portfel bitcoinowy

to dwa zupełnie różne sposoby księgowania

KONTO BANKOWE

jedna liczba: saldo

SALDO KONTA

130 zł

jedno pole w bazie banku

Operacje:

+ wpływ 50 zł	→ *saldo rośnie*
– wypłata 30 zł	→ *saldo maleje*
– przelew 20 zł	→ *saldo maleje*

Jak to działa

Bank zapisuje jedną liczbę.
Każda operacja ją zmienia.
Bank odpowiada, ile masz.
Musisz zaufać bankowi.

PORTFEL BITCOIN

zbiór niewydanych „banknotów"

`0,5 BTC` *wpływ: 12 mar 2024*

`0,3 BTC` *wpływ: 20 mar 2024*

`0,4 BTC` *wpływ: 5 kwi 2024*

wydaję 1 BTC – biorę wszystkie 3
razem 0,5 + 0,3 + 0,4 = 1,2 BTC

`1,0 BTC` → *do odbiorcy*

`0,2 BTC` → *reszta do nas*

banknotu nie da się rozciąć – jak płacenie gotówką ze sklepu

Jak to działa

Saldo nigdzie nie istnieje.
Portfel sumuje niewydane wpływy.
Nie ufasz nikomu – sam liczysz.

Kluczowa różnica

W banku twoje pieniądze są jedną liczbą w jednej bazie. Bank ją modyfikuje.

W Bitcoinie twoje pieniądze to konkretne, indywidualne wpływy z wcześniejszych transakcji, które jeszcze nie zostały wydane. Każdy z nich osobno.

Nie ma „salda" – jest historia, którą każdy może sam zsumować.

UTXO

Unspent Transaction Output = niewydane wyjście transakcji

Każdy „banknot" w portfelu to konkretny UTXO: kwota + adres, do którego masz klucz prywatny + wskazanie, skąd przyszedł.

Twój portfel = lista UTXO, które mogą być wydane twoim podpisem.

Rysunek 1. Model UTXO vs konto bankowe. Po lewej: bank prowadzi pojedyncze saldo, które rośnie i maleje. Po prawej: portfel bitcoinowy to zbiór niewydanych „banknotów" o różnych nominałach, każdy z osobnym kluczem prywatnym

bitcoiny, i sprawdza, czy te konkretne bitcoiny zostały już przeze mnie wydane w jakiejś późniejszej transakcji. Jeśli nie – to są moje. Jeśli tak – już nie. To, co mam w portfelu, to nie jakaś sumaryczna liczba; to zbiór konkretnych „niewydanych wpływów" z konkretnych wcześniejszych transakcji. Każdy z nich ma swoją kwotę i pasuje do jednego z moich kluczy prywatnych.

Ten sposób księgowania nazywa się modelem UTXO – od angielskiego unspent transaction output, czyli „niewydane wyjście transakcji". To jest fundamentalna różnica między Bitcoinem a kontem bankowym, i bez jej zrozumienia cała reszta będzie niejasna.

Najlepsza analogia, jaką znam, to portfel z gotówką. W banku masz konto z saldem. W portfelu fizycznym masz konkretne banknoty – 50 zł, 50 zł, 20 zł, 10 zł, razem 130 zł. Jeśli chcesz wydać 60 zł, nie odcinasz kawałka banknotu pięćdziesięciozłotowego. Dajesz pięćdziesiątkę plus dziesiątkę i pierwsza staje się „wydana", druga też – cała pięćdziesiątka i cała dziesiątka. Bitcoin działa identycznie. Mam trzy „banknoty" – wpływy z trzech wcześniejszych transakcji, na 0,5, 0,3 i 0,4 BTC. Jeśli chcę zapłacić Bobowi 1 BTC, muszę wydać wszystkie trzy. Tak działa transakcja bitcoinowa.

Anatomia transakcji

Transakcja bitcoinowa to dokument, który ma dwie strony: wejścia i wyjścia. Wejścia mówią, skąd biorę monety, które chcę wydać. Wyjścia mówią, dokąd je wysyłam.

Każde wejście to wskazanie na jakąś wcześniejszą transakcję – dokładniej, na konkretne wyjście tej wcześniejszej transakcji, które trafiło na mój adres i nie zostało jeszcze wydane. Wejście mówi w istocie: „bierz tamten konkretny niewydany wpływ". I dołącza do tego mój podpis cyfrowy, udowadniający, że mam klucz prywatny pasujący do adresu, na który tamta dawna transakcja trafiła.

Każde wyjście z kolei to dwie informacje: kwota i warunek wydania. Warunek wydania to zwykle „kto będzie miał klucz prywatny pasujący do tego adresu, ten może to wydać". Wyjście trafia więc do konkretnego adresata.

Przykład. Mam te trzy wpływy: 0,5 + 0,3 + 0,4 BTC. Chcę zapłacić Bobowi 1 BTC. Buduję transakcję z trzema wejściami (wskazującymi na te trzy wpływy) i dwoma wyjściami:

- Pierwsze wyjście: 1,0 BTC dla Boba (kwota + warunek: pasujący do adresu Boba).

- Drugie wyjście: 0,19 BTC z powrotem do mnie (na nowy mój adres – to jest tzw. reszta).

Suma wejść: 1,2 BTC. Suma wyjść: 1,19 BTC. Różnica – 0,01 BTC – nie idzie nigdzie. To opłata transakcyjna, którą zgarnie górnik, który włączy moją transakcję do bloku. Bitcoin nie ma osobnego pola na opłatę; opłata to po prostu różnica, której nigdzie nie skierowałem.

Anatomia transakcji bitcoinowej

Alicja płaci Bobowi 1 BTC

Alicja ma w portfelu trzy „banknoty": 0,5 + 0,3 + 0,4 BTC = 1,2 BTC.
Chce zapłacić Bobowi 1 BTC. Buduje transakcję z 3 wejść i 2 wyjść.

WEJŚCIA
skąd biorę monety

Wejście #1
→ tx_a4f2... #0
poprzedni wpływ
0,5 BTC + podpis Alicji

Wejście #2
→ tx_b8e1... #2
poprzedni wpływ
0,3 BTC + podpis Alicji

Wejście #3
→ tx_c91d... #1
poprzedni wpływ
0,4 BTC + podpis Alicji

Suma: 1,20 BTC

TRANSAKCJA
Alicja → Bob
tx_xyz789...

WYJŚCIA
dokąd je wysyłam

Wyjście #1
do Boba
adres: 1A2B3C...
1,00 BTC

Wyjście #2
reszta dla Alicji
adres: 1Q9R8S...
0,19 BTC

Suma: 1,19 BTC

Bilans i opłata

1,20 wejścia – 1,19 wyjścia = 0,01 opłata → *górnik*

OPŁATA TRANSAKCYJNA

Bitcoin nie ma osobnego pola na opłatę.
Opłata = (suma wejść) – (suma wyjść). Po prostu różnica.
Górnik, który włączy tę transakcję do bloku, zgarnie te 0,01 BTC.

Po wykonaniu: trzy banknoty Alicji znikają. Bob ma nowy banknot 1 BTC, Alicja – nowy 0,19 BTC. Wszystko zapisane w blockchainie.

Rysunek 2. Anatomia transakcji bitcoinowej. Trzy wejścia po lewej (referencje do wcześniejszych niewydanych wpływów + podpisy), dwa wyjścia po prawej (kwoty + warunki wydania). Różnica = opłata

Podpisuję całą transakcję moimi kluczami prywatnymi (po jednym dla każdego wejścia, bo każde może być z innego adresu) i wysyłam ją do sieci. Tysiące węzłów na całym świecie ją odbierze, sprawdzi, czy podpisy są poprawne i czy te wejścia naprawdę istnieją i są niewydane – i jeśli tak, włączy moją transakcję do swojej puli oczekujących na zapakowanie do bloku.

Zauważ, że po wykonaniu tej transakcji moje trzy „banknoty" (0,5 + 0,3 + 0,4) znikają z mojego portfela – stają się wydane. Pojawia się nowy mój „banknot" (0,19), który odebrałem od samego siebie jako resztę. Bob z kolei ma teraz nowy banknot na 1,0 BTC. Nikt nigdzie nie zaktualizował salda – po prostu pojawiły się nowe niewydane wpływy, a stare zostały oznaczone jako wydane.

Skąd biorą się pierwsze bitcoiny

Powyższy opis ma jeden niepokojący problem. Każda transakcja bierze monety z wcześniejszej. Skąd więc wzięła się pierwsza? Skąd w ogóle pojawiły się jakiekolwiek bitcoiny w systemie?

Odpowiedź: z transakcji szczególnego rodzaju, zwanej coinbase. Każdy blok zaczyna się od jednej takiej transakcji – i jest to jedyna transakcja w całym systemie, która nie wymaga wejść. Po prostu tworzy nowe monety z niczego. Trafia do adresu górnika, który ten blok wydobył, jako jego nagroda za pracę.

Dziś nagroda coinbase wynosi 3,125 BTC za blok. W 2009 roku, na początku, było to 50 BTC. Wartość ta zmniejsza się o połowę co cztery lata – ten mechanizm nazywa się halving – co oznacza, że całkowita liczba bitcoinów, które kiedykolwiek powstaną, jest skończona i wyniesie nieco poniżej 21 milionów. Ostatni bitcoin zostanie wydobyty około 2140 roku. To jest cała emisja. Ani jedna moneta więcej – nigdy.

Górnik dolicza sobie do tej nagrody jeszcze sumę wszystkich opłat ze wszystkich transakcji w bloku. Jeśli w bloku jest 2000 transakcji i każda zostawiła po 0,0001 BTC opłaty, to górnik dostaje dodatkowo 0,2 BTC. Powyżej, gdy halving zredukuje nagrodę do zera (ok. 2140 r.), opłaty staną się jedynym wynagrodzeniem za utrzymywanie sieci.

Drzewo Merklego – tysiące transakcji w jednym hashu

W typowym bloku Bitcoina jest około dwóch tysięcy transakcji. Wszystkie razem ważą około megabajta. Jeśli jeden węzeł sieci dostał ten blok i chce się upewnić, że nikt go nie zmodyfikował po drodze, najprostsze rozwiązanie to zhashować całość – uznajemy, że wynikowy SHA-256 jest „odciskiem palca" całego bloku, i porównujemy z tym, co ogłosił sąsiedni węzeł. Działa, ale ma wadę. Jeśli kogoś interesuje tylko jedna konkretna transakcja w bloku – chce sprawdzić, czy ta transakcja faktycznie się w nim znajduje – musi pobrać i zhashować cały blok. Megabajt danych po to, żeby zweryfikować jeden krótki przekaz.

Można lepiej. Da się tak ułożyć skróty, żeby istniał jeden krótki dowód, że dana transakcja jest w bloku – bez konieczności pobierania reszty. Konstrukcja, która to robi, nazywa się drzewem Merklego od nazwiska informatyka Ralpha Merklego, który ją opatentował w 1979 roku. Bitcoin używa jej do organizowania transakcji w bloku.

Konstrukcja jest niezwykle prosta. Liczymy SHA-256 z każdej transakcji. Mamy listę hashy.

GENESIS BLOCK – 3 STYCZNIA 2009

Pierwszy blok Bitcoina – tzw. Genesis Block – został wykopany przez Satoshiego Nakamoto 3 stycznia 2009 roku. W transakcji coinbase tego bloku, w polu, w którym górnik może dopisać dowolną krótką wiadomość, Satoshi wpisał:

```
The Times 03/Jan/2009
Chancellor on brink of second bailout for banks
```

To tytuł z pierwszej strony brytyjskiego dziennika „The Times" z dnia, w którym blok został wykopany. Tłumaczenie: „Kanclerz Skarbu na progu drugiego ratowania banków". Świat tonął w kryzysie finansowym, banki centralne drukowały pieniądze, a Satoshi wkomponowywał w sam fundament swojego systemu drobne polityczne motto.

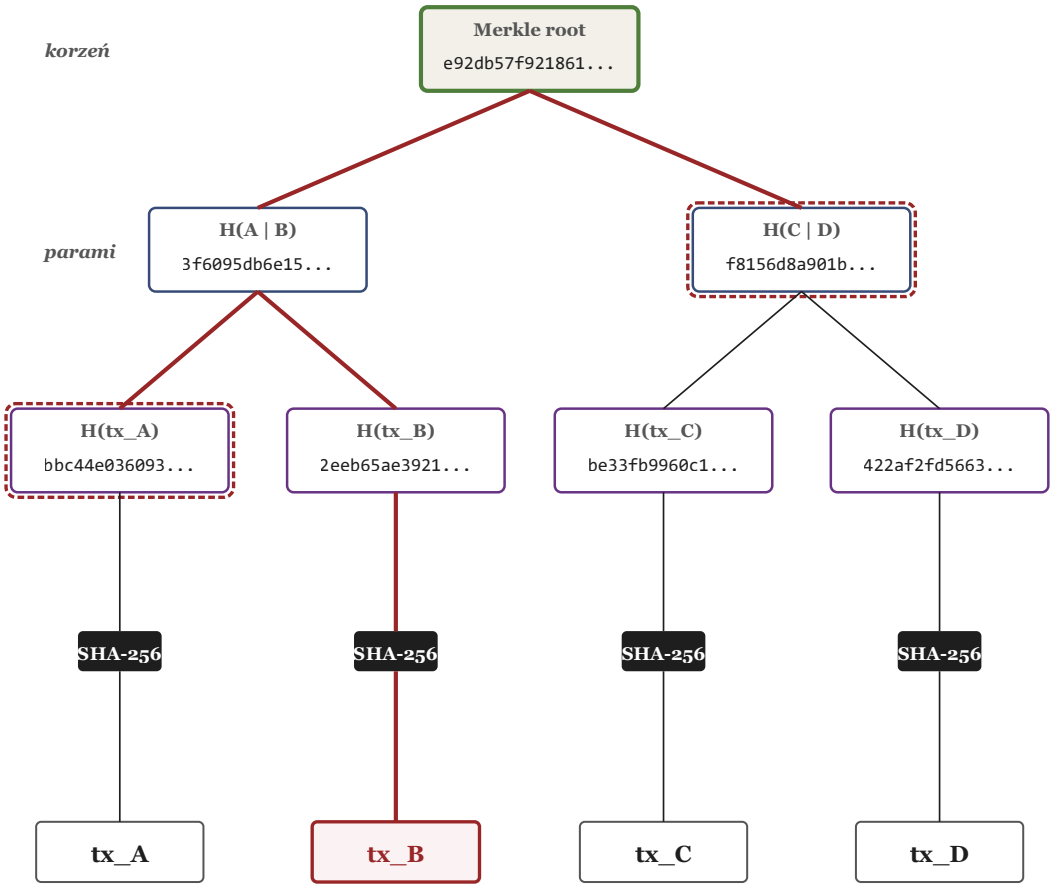
Ta linijka siedzi w blockchainie do dziś. Każdy z tysięcy węzłów na świecie ma jej kopię, w niezmienionej postaci, od szesnastu lat. To zarazem datownik (potwierdzający, że Bitcoin nie powstał wcześniej) i ironia – bo Bitcoin powstał właśnie po to, żeby system finansowy nie zależał od kanclerzy ratujących banki.

Bierzemy je parami i hashujemy każdą parę razem (sklejone), dostając listę o połowę krótszą. Powtarzamy. I jeszcze raz. Aż na samej górze zostanie jeden hash. Ten jeden hash nazywa się Merkle root – głowa drzewa. Reprezentuje wszystkie transakcje, które trafiły do bloku.

Najpiękniejsza własność tej konstrukcji to dowód włączenia (Merkle proof). Wyobraź sobie, że masz tysiące transakcji w bloku, ale chcesz tylko udowodnić komuś, że jedna konkretna z nich w nim jest. Nie musisz pokazywać wszystkich. Wystarczy pokazać samą tę transakcję plus tyle

Drzewo Merklego

jeden hash reprezentuje wszystkie transakcje



DOWÓD WŁĄCZENIA dla tx_B

Chcesz udowodnić, że tx_B jest w drzewie? Pokaż samą tx_B oraz dwa hashe:

`H(tx_A) = bbc44e036093...` `H(C|D) = f8156d8a901b...`

Z nich obserwator sam policzy: H(B), potem H(A|B), potem korzeń.
Jeśli to zgadza się z korzeniem w nagłówku bloku – tx_B jest w bloku. Bez całej reszty.
Dla 1024 transakcji: tylko 10 hashy. Dla miliona: 20.

Rysunek 3. Drzewo Merklego dla 4 transakcji. Hashe transakcji u dołu, parami w górę, na szczycie Merkle root. Czerwoną ścieżką: dowód, że transakcja B jest w drzewie – wystarczą dwa hashe (a nie cała reszta drzewa)

hashy, ile poziomów ma drzewo (dla 1024 transakcji to 10 hashy, dla miliona – 20). Z tych hashy obserwator może sam, krok po kroku, odbudować ścieżkę aż do głowy drzewa i porównać ją z głową ogłoszoną w nagłówku bloku.

To jest mechanizm, który pozwala działać tzw. lekkim portfelom (SPV – *Simplified Payment Verification*). Zamiast pobierać cały blockchain (dziś ponad 600 GB), portfel pobiera same nagłówki bloków (po 80 bajtów każdy) i przy potrzebie weryfikacji konkretnej transakcji prosi pełen węzeł o dowód włączenia. Telefonem komórkowym da się zweryfikować dowolną transakcję bitcoinową bez ufania nikomu w szczegółach.

Nagłówek bloku

Skoro Merkle root reprezentuje wszystkie transakcje, można go potraktować jako esencję bloku. I dokładnie to robi Bitcoin. Cały blok ma dwie części: nagłówek (zaledwie 80 bajtów) oraz właściwą zawartość (lista transakcji, zwykle ok. 1 MB). Cała magia rozgrywa się w nagłówku.

Nagłówek bloku zawiera dokładnie sześć pól:

1. **Wersja protokołu** – 4 bajty. Mówi, według której wersji reguł Bitcoina ten blok jest zbudowany.
2. **Hash poprzedniego bloku** – 32 bajty. To jest klucz do całej idei łańcucha. Każdy nowy blok wskazuje na poprzedni przez jego hash.
3. **Merkle root** – 32 bajty. Głowa drzewa Merklego wszystkich transakcji w tym bloku.
4. **Czas** – 4 bajty. Datownik wykopania (z dokładnością do sekundy).
5. **Trudność (bits)** – 4 bajty. Określa, jak trudno musi być znaleźć ten blok. Wrócimy do tego w Części 5.
6. **Nonce** – 4 bajty. Wartość, którą górnik kręci, próbując dopasować hash do warunku trudności. To jest serce mechanizmu kopania, też w Części 5.

Razem: 80 bajtów. To wszystko. Cały „odcisk palca" bloku, łącznie z odsyłaczem do poprzednika i z reprezentacją wszystkich tysięcy transakcji w nim, mieści się w 80 bajtach.

Hash całego bloku – czyli SHA-256 z tych 80 bajtów nagłówka – to jest to, co inne bloki wskazują, gdy mówią „mój poprzednik". To jest też to, co górnik liczy, gdy „kopie". I to jest to, co tworzy łańcuch.

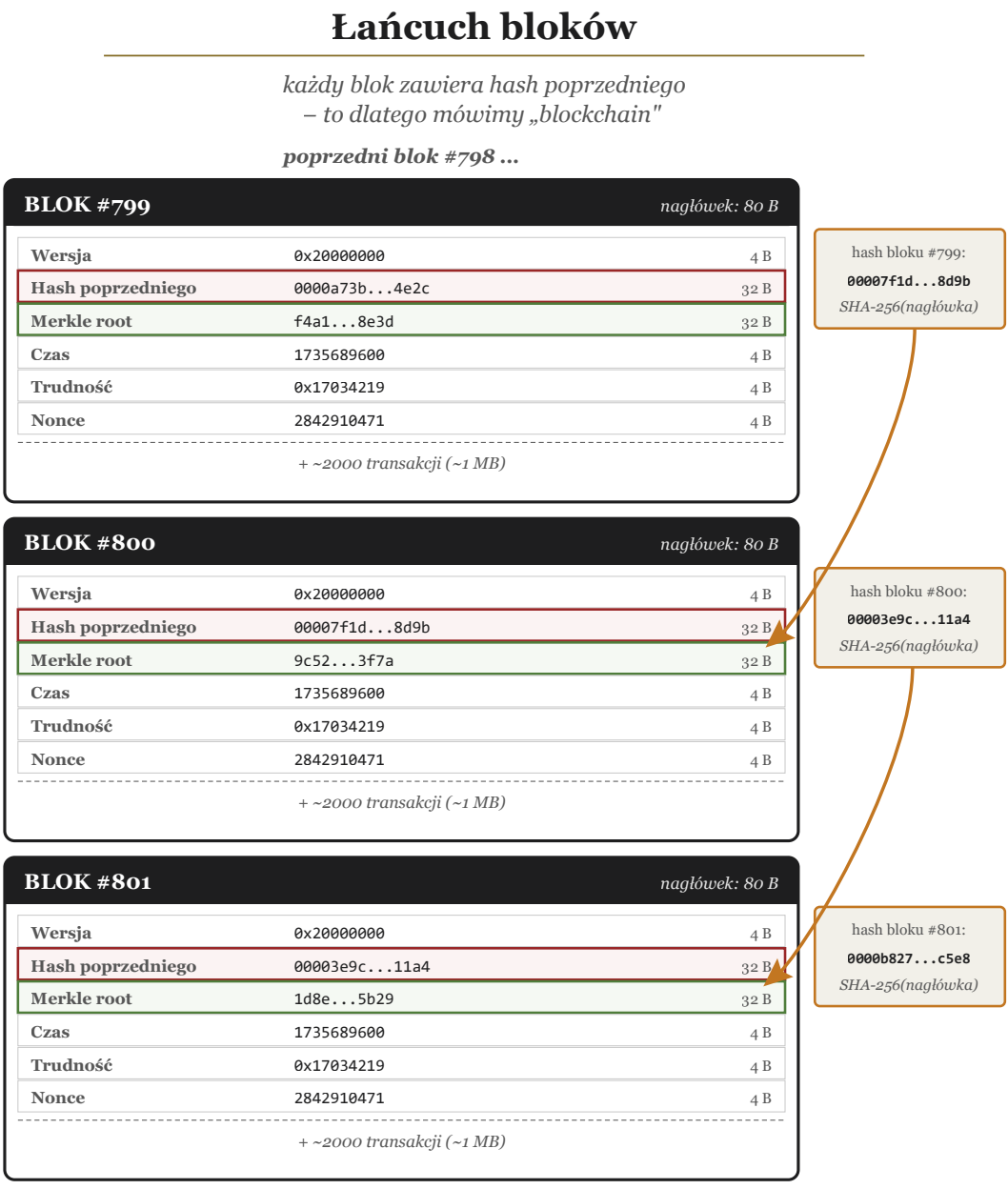
Łańcuch – dlaczego nie da się przepisać historii

W tym momencie wszystkie klocki się zazębiają. Każdy blok zawiera w nagłówku hash poprzedniego. Każdy blok jest też wskazywany przez następny – przez ten sam hash. To tworzy łańcuch, w którym każde ogniwo zawiera kryptograficzny ślad wszystkich poprzednich.

Wyobraź sobie teraz, że ktoś chce zmienić jedną transakcję w bloku numer 800 000 – powiedzmy, sfałszować, ile bitcoinów dostał ktoś inny rok temu. Co wtedy?

Zmiana transakcji oznacza zmianę jej hasha. To zmienia parę w drzewie Merklego, co zmienia hash wyższego poziomu, co zmienia Merkle root, co zmienia nagłówek bloku 800 000, co zmienia hash bloku 800 000. Ale ten hash jest wpisany w nagłówek bloku 800 001 jako „hash poprzedniego". A skoro on się zmienia, zmienia się hash bloku 800 001. A ten z kolei jest w bloku 800 002. I tak dalej.

Krótko: zmiana czegokolwiek w jakimkolwiek dawnym bloku wymaga przekopania od nowa wszystkich kolejnych bloków, aż do teraz.



Rysunek 4. Trzy bloki w łańcuchu. Każdy z 6-polowym nagłówkiem. Hash każdego bloku jest wpisany w nagłówek następnego – to dlatego nazywa się to blockchain. Zmiana czegokolwiek w bloku 800 unieważnia wszystkie po nim

A to wymaga energii porównywalnej z energią całej sieci wydatkowaną od momentu wykopania tego dawnego bloku – wszystkich górników, wszystkich kopalni na świecie, plus tej, którą wydatkują codziennie nowi górnicy w międzyczasie. To po prostu niewykonalne. Dlatego mówimy, że bitcoin jest niezmienny.

To jest właśnie blockchain. Nie magiczna technologia, nie sztuczna inteligencja, nie kryptografia kwantowa – tylko: lista bloków, w której każdy blok zawiera hash poprzedniego. Ta jedna prosta sztuczka, w połączeniu z dwoma narzędziami z poprzednich części (funkcją skrótu i podpisem cyfrowym), daje system, w którym wszystko jest jawne, wszystko jest weryfikowalne, i jednocześnie nikt nie może niczego sfałszować.

* * *

Mamy więc system: transakcje grupują się w bloki, bloki łączą się w łańcuch, każdy blok wskazuje na poprzedni. Pozostaje pytanie – kto i dlaczego dodaje nowe bloki? Co sprawia, że uczciwi górnicy się starają, a nieuczciwi nie? O tym w Części 5: proof of work i ekonomia kopania.

SPRÓBUJ SAM

Cały blockchain Bitcoina jest publiczny. Każdy może obejrzeć dowolny blok i dowolną transakcję. W przeglądarce wpisz adres:

`blockchain.com/explorer`

Wyszukaj „block 0” – to Genesis Block. Zobaczysz wszystkie 6 pól nagłówka, jego hash, oraz tę jedną transakcję coinbase z wiadomością Satoshiego. Wyszukaj „block 1” – zobaczysz, że jego pole „previous block” zawiera hash bloku 0. Tak właśnie wygląda ogniwo łańcucha.

Spróbuj też kliknąć na dowolną transakcję w dowolnym bloku. Zobaczysz jej wejścia (z linkami do wcześniejszych transakcji) i wyjścia (z kwotami i adresami). Tym razem to są prawdziwe pieniądze, prawdziwych ludzi, prawdziwe historie. Cały Bitcoin to lista takich transakcji, otwarta dla każdego.

Część 5. *Proof of work* – kto i dlaczego dodaje bloki

W Częściach 2...4 zbudowaliśmy strukturę. Wiemy, jak zapisuje się transakcje, jak grupuje się je w bloki, jak hashe spinają bloki w łańcuch. Pozostaje jednak fundamentalne pytanie, którego od początku unikaliśmy: kto dokłada kolejne ogniwa łańcucha – i co go do tego skłania?

Powrót do problemu

W Części 1 postawiliśmy zagadkę. Miliony komputerów na całym świecie ogłaszają wersje historii. Każdy może być uczciwy lub nie. Każdy może próbować dopisać do księgi własne, korzystne dla siebie kłamstwa. Jak ta sieć dochodzi do zgody, która wersja księgi jest prawdziwa?

W tradycyjnej bankowości decyzję podejmuje siła autorytetu – bank mówi, jaki jest stan rachunków, i wszyscy się z tym zgadzają. W Bitcoinie nie ma takiego autorytetu. Decyzję podejmuje siła obliczeń. Prawdziwa jest ta wersja łańcucha, w której zsumowano najwięcej pracy obliczeniowej. Tylko tyle.

Brzmi to dziwnie, dopóki nie zobaczy się, jak ten mechanizm działa w szczegółach. Wtedy okazuje się, że jest to prosty pomysł, sprzęgnięty z prostą ekonomią, dający w sumie system, który działa od siedemnastu lat bez awarii. Ten pomysł nazywa się proof of work – dowód pracy.

Czym właściwie jest „kopanie”

Słowo „kopanie” – angielskie mining – jest jednym z najbardziej mylących określeń w całej historii informatyki. Sugeruje, że górnik wydobywa coś rzadkiego z głębi systemu, jak złoto z ziemi. Albo że wykonuje skomplikowany algorytm matematyczny. Ani jedno, ani drugie nie jest prawdą.

Górnik bitcoinowy zgaduje. To wszystko. Kręci jedną liczbą – pamiętasz pole „nonce” z nagłówka bloku z Części 4? – i sprawdza, czy hash całego nagłówka spełnia pewien warunek. Jeśli tak, gratuluje sobie i wysyła blok do sieci. Jeśli nie,

kręci nonce o jeden i próbuje znowu. Miliardy razy na sekundę.

Konkretnie: górnik bierze nagłówek bloku – 80 bajtów, o których pisaliśmy w Części 4. Przypomnijmy: nagłówek zawiera sześć pól – wersję protokołu, hash poprzedniego bloku, Merkle root (głowę drzewa wszystkich transakcji w tym bloku), znacznik czasu, parametr trudności i nonce. Pierwsze pięć pól jest ustalone – wynikają z reguł sieci, z poprzedniego bloku albo z listy transakcji, które górnik chce do bloku włączyć. Tylko jedno pole – nonce, czterobajtowa

Kopanie jako zgadywanie

ten sam blok, kolejne wartości nonce, kolejne hashe

WYMÓG (przykład uproszczony):
hash musi zaczynać się od co najmniej **4 zer** w zapisie szesnastkowym

CZĘŚĆ STAŁA NAGŁÓWKA (taka sama dla wszystkich prób):

```
prev: 0000...8d9b · merkle: f4a1...8012 · time: 1735689600
bits: 0x17034219 · wersja: 0x20000000
```

PRÓBY KOPANIA – kręcimy nonce, sprawdzamy hash:

próba	nonce	hash (początek)	wynik
1	1	0b4f573c9d56effb9bcfa9c5...	NIE (1)
2	2	a981a3156c0b88bfbc0edf5c...	NIE (0)
3	3	cb5b757e28bd4a61b9429e19...	NIE (0)
4	100	f1c7b144b84fc7bf007a08d6...	NIE (0)
5	1,000	3a88dc85a89ecdd4eb388fa1...	NIE (0)
6	12,345	61f9623c6482571abc18f8a0...	NIE (0)
		... kolejne tysiące nieudanych prób ...	
7	37,300	00003249efb607eccc368d07...	**TAK (4 zer)**

CO TU WIDAĆ:

- Nagłówek poza polem nonce się nie zmienia.
- Każda zmiana nonce produkuje zupełnie inny hash (efekt lawinowy z Cz. 2).
- Trafienie w hash z 4 zerami zajęło 37 300 prób. Średnio: $16^4 = 65\,536$.

W PRAWDZIWYM BITCOINIE

Hash musi zaczynać się od ~19 zer szesnastkowych – a nie od 4.
Średnio potrzeba $\mathbf{2^{76} \approx 7{,}5 \times 10^{22}}$ prób, żeby trafić.

Rysunek 1. Iteracje kopania: ten sam nagłówek bloku, kolejne wartości nonce, kolejne hashe. Górnik kręci nonce, aż trafi w hash zaczynający się od zadanej liczby zer

liczba – jest dowolne. Górnik wpisuje w nie jakąś wartość, liczy z całego nagłówka SHA-256, jeszcze raz SHA-256 (Bitcoin używa podwójnego SHA-256) i sprawdza wynik.

Wynik to 256-bitowa liczba w zapisie szesnastkowym, czyli 64 znaki hex. Warunek brzmi: ta liczba musi być mniejsza od pewnej zadanej wartości. W praktyce sprowadza się to do tego,

Skala kopania w 2025 roku

moc obliczeniowa i zużycie energii

CZĘŚĆ 1: jak szybko można zgadywać

sprzęt	hashy / sekundę	uwagi
Laptop / domowy CPU	10 milionów (10^7)	*praktycznie nieopłacalne*
Karta graficzna (GPU)	1 miliard (10^9)	*kiedyś standard, dziś za wolno*
Pojedynczy ASIC	100 bilionów (10^{14})	*kupisz za 5…15 tys. zł*
Duża farma (10 tys. ASIC-ów)	1 tryliard (10^{18})	*elektrownia + hala + chłodnie*
CAŁA SIEĆ BITCOIN	600 tryliardów (6×10^{20})	*wszyscy górnicy*

cała sieć robi w 1 sekundę więcej hashy niż laptop przez milion lat

CZĘŚĆ 2: zużycie energii (TWh/rok)

co to jest	TWh/rok	skala
Polska (zużycie kraju)	170	
Sieć Bitcoin (rocznie)	165	
Argentyna	130	
Norwegia	130	
Wszystkie centra danych świata	350	

Skala

Sieć Bitcoin zużywa rocznie tyle energii, co cała Polska.

→ *patrz ramka „Bitcoin a środowisko" w tekście*

Rysunek 2. Skala kopania w 2026 roku. Od jednej próby na laptopie do 6×10^{20} prób na sekundę całej sieci. Z porównaniem zużycia energii do całych krajów

że hash musi zaczynać się od pewnej liczby zer. Jeśli nie zaczyna się – górnik zmienia nonce na inną wartość i próbuje znowu. I znowu. I jeszcze raz.

To naprawdę tyle. Ot, próbowanie. Nie ma żadnego „algorytmu kopania" – bo jednokierunkowość SHA-256, którą poznaliśmy w Części 2, oznacza dokładnie to: nie da się wymyślić, jaki nonce da hash z odpowiednią liczbą zer. Trzeba próbować. Każda próba kosztuje jedną operację SHA-256 – w sprzęcie ASIC zaprojektowanym specjalnie do tego celu zajmuje to ułamki nanosekundy.

Jeden górnik z dobrym ASIC-iem robi kilkadziesiąt miliardów prób na sekundę. Cała sieć Bitcoin razem – około 600 trylionów (6×10^{20}) prób na sekundę. To niewyobrażalnie dużo. Ale liczba potrzebnych prób też jest niewyobrażalna, więc wychodzi na to, że średnio co 10 minut ktoś jednak trafia.

Warunek trudności

Wartość, od której hash musi być mniejszy, nazywa się target. W praktyce, na przykład dla bloku 888 888 wykopanego 22 marca 2025 roku (numer, który dla społeczności bitcoinowej był „kamieniem milowym" ze względu na powtarzające się ósemki) – target wymagał, żeby hash zaczynał się od 20 zer szesnastkowych. Hash bloku 888 888 to:

```
0000000000000000000c3bc6996a682
60a7a580e4658493c9cfdb10fa3c7bc9
```

Dwadzieścia zer wiodących. Każda zerowa cyfra szesnastkowa to 4 bity zer, więc razem 80 bitów. Innymi słowy: hash bloku 888 888 to liczba mniejsza niż 2^{176} – z całej puli 2^{256} możliwych wyników SHA-256.

Jakie jest prawdopodobieństwo trafienia w taki hash przy losowej próbie? Skoro SHA-256 daje wyniki rozłożone równomiernie, to dokładnie $2^{176}/2^{256}=1/2^{80}$. Jedna szansa na 2^{80} – czyli na około $1{,}2\times10^{24}$. Nawet trudno to sobie wyobrazić. Dla porównania: liczba sekund, jakie minęły od Wielkiego Wybuchu, to „tylko" 4×10^{17}. Trzeba by więc przepuścić przez SHA-256 dziesięć milionów prób co femtosekundę przez cały czas istnienia Wszechświata, żeby zebrać tyle prób.

Sieć Bitcoina robi to w 10 minut. Nie dlatego, że jeden komputer jest tak szybki – żaden komputer na Ziemi nie jest. Tylko dlatego, że pracuje równolegle kilka milionów ASIC-ów rozsianych po całym świecie. Łącznie generują 6×10^{20} hashy na sekundę, czyli $3{,}6\times10^{23}$ hashy w 10 minut – mniej więcej dokładnie tyle, ile potrzeba na trafienie w cel.

To nie jest przypadek. Sieć dostosowuje cel co 2016 bloków – czyli mniej więcej co dwa tygodnie. Jeśli przez ostatnie 2016 bloków górnicy znajdowali rozwiązania szybciej niż 10 minut na blok, sieć utrudnia (target maleje, potrzeba więcej zer wiodących). Jeśli wolniej – sieć ułatwia. Ten samoregulujący mechanizm sprawia, że tempo pojawiania się nowych bloków pozostaje stałe niezależnie od tego, jak duża jest sieć i jak wydajne są komputery.

Co dostaje górnik za swoją pracę

Skoro robienie 10^{23} hashy w 10 minut wymaga zainwestowania w sprzęt za miliony złotych i opłacania ciągłego rachunku za prąd, musi być czymś nagrodzone. Jest. Górnik, który wykopie blok, dostaje dwie rzeczy.

BITCOIN A ŚRODOWISKO

Każda próba SHA-256 kosztuje energię. 6×10^{20} prób na sekundę przez 365 dni daje rocznie zużycie sieci Bitcoin szacowane na 150…180 TWh. To mniej więcej tyle, ile zużywa cała Polska (ok. 170 TWh rocznie) albo Argentyna (ok. 130 TWh). Dla porównania: cały sektor centrów danych na świecie to ok. 350 TWh.

Krytycy mówią: to absurd. Zużywać tyle energii na losowe zgadywanie wydaje się marnotrawstwem. Niektóre alternatywne kryptowaluty (np. Ethereum od 2022 r.) zrezygnowały z proof of work na rzecz innego mechanizmu konsensusu – proof of stake, który zużywa tysiące razy mniej energii.

Obrońcy odpowiadają: ta energia to nie marnotrawstwo, tylko zabezpieczenie. To właśnie ona sprawia, że atak na sieć jest ekonomicznie nieopłacalny. Część z niej pochodzi ze źródeł odnawialnych albo z nadwyżek mocy (ok. 50% według różnych szacunków, choć dane są kontestowane). Górnicy szukają miejsc, gdzie prąd jest tani – często to elektrownie wodne na Syberii, geotermalne na Islandii, słoneczne w Teksasie.

Spór ten nie ma rozstrzygnięcia w obrębie samej technologii. To pytanie polityczne i ekonomiczne: ile warte jest istnienie pieniądza niezależnego od państw, w stosunku do kosztów środowiskowych jego utrzymywania.

Po pierwsze, nagrodę coinbase. To jest ta jedyna transakcja w bloku, o której mówiliśmy w Części 4 – transakcja bez wejść, tworząca monety z niczego. Trafia na adres górnika. Dziś (maj 2026) wynosi 3,125 BTC, czyli przy obecnym kursie około miliona złotych. Co 10 minut. Stąd w ogóle wzięła się gospodarka kopania.

Po drugie, sumę wszystkich opłat ze wszystkich transakcji w bloku. W Części 4 widzieliśmy, jak działa opłata: jest to różnica między sumą wejść a sumą wyjść transakcji, którą zgarnia ten, kto włączy ją do bloku. W typowym bloku jest około 2000 transakcji. Każda zostawia zwykle od 1000 do 10 000 satoshich (1 satoshi = 0,00000001 BTC). Razem daje to dziś od 0,1 do 0,5 BTC opłat na blok – zwykle kolejne 25...130 tysięcy złotych dla górnika.

To jest motywacja dla uczciwego górnika. Inwestujesz w ASIC-i, opłacasz prąd, próbujesz zgadnąć właściwy nonce – jeśli ci się uda,

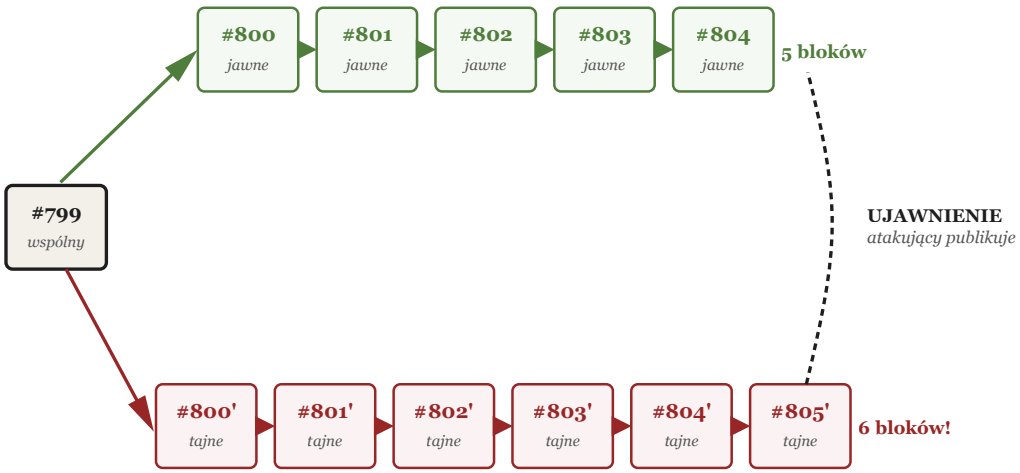
Atak 51% – anatomia

dwa równoległe łańcuchy. Sieć przyjmie ten dłuższy.

SCENARIUSZ

1. Atakujący kupuje ASIC-i za miliardy dolarów – uzyskuje >50% mocy sieci.
2. Ostatni wspólny blok = #799. Wszyscy go widzą.
3. Stąd uczciwa większość buduje publicznie. Atakujący – w tajemnicy, równolegle.

UCZCIWA WIĘKSZOŚĆ (publicznie)



ATAKUJĄCY (w tajemnicy, >50% mocy)

CO SIĘ DZIEJE PO UJAWNIENIU

- Sieć patrzy: który łańcuch dłuższy? Atakującego (6 bloków > 5).
- Reguła Bitcoina: prawdziwy jest dłuższy. Sieć go akceptuje.
- Wszystkie transakcje z bloków uczciwych #800-804 – **unieważnione**.
- Atakujący mógł wpisać do swoich bloków co chciał (np. zwrot własnego BTC).

DLACZEGO TO SIĘ NIE DZIEJE

Cena: ~50 mld $ na ASIC-i + GW prądu. Po ataku kurs spada → zysk znika.
To nie kryptografia chroni Bitcoina, to ekonomia. Atak jest możliwy, ale nieopłacalny.

Rysunek 3. Anatomia ataku 51%. Uczciwa większość buduje łańcuch publicznie. Atakujący buduje równolegle w tajemnicy. W pewnym momencie ujawnia swój łańcuch – jeśli jest dłuższy, sieć go akceptuje, unieważniając transakcje z łańcucha publicznego

dostajesz dziesiątki albo setki tysięcy złotych. Przegrasz wyścig do tego konkretnego bloku – startujesz natychmiast w wyścigu do następnego, dziesięć minut później.

Sumarycznie: w 2026 roku górnicy bitcoinowi zarabiają łącznie około 16...18 miliardów dolarów rocznie. Wydają na sprzęt i prąd nieco mniej. Marża jest cienka, ale nie zerowa – i to wystarczy, żeby system się napędzał.

Atak 51% – czyli czego ten cały zachód nie pozwala zrobić

Mamy więc system: tysiące górników rozsianych po świecie, niezależnych od siebie, konkurujących o nagrodę. Każdy z nich pracuje w interesie własnym, a wynik to sieć, która utrzymuje porządek. Klasyczny przypadek niewidzialnej ręki rynku, opisanej przez Adama Smitha – ale w wersji obliczeniowej.

Jeszcze w Części 2 obiecaliśmy wrócić do pytania, dlaczego to wszystko nie pozwala atakującemu zafałszować historii. Czas obietnicy dotrzymać.

Wyobraźmy sobie napastnika, który ma dużo pieniędzy i postanawia zaatakować Bitcoina. Najpierw próbuje atak kryptograficzny: złamać SHA-256 albo podpis ECDSA. Z Części 2 i 3 wiemy, że to wymaga liczby operacji rzędu 2^{128}, czyli więcej niż wieków Wszechświata pomnożonych przez liczbę atomów Ziemi. Nie da się. Próbuje sfałszować pojedynczą transakcję – ale każda transakcja wymaga podpisu pasującego do klucza prywatnego, którego nie ma. Nie da się.

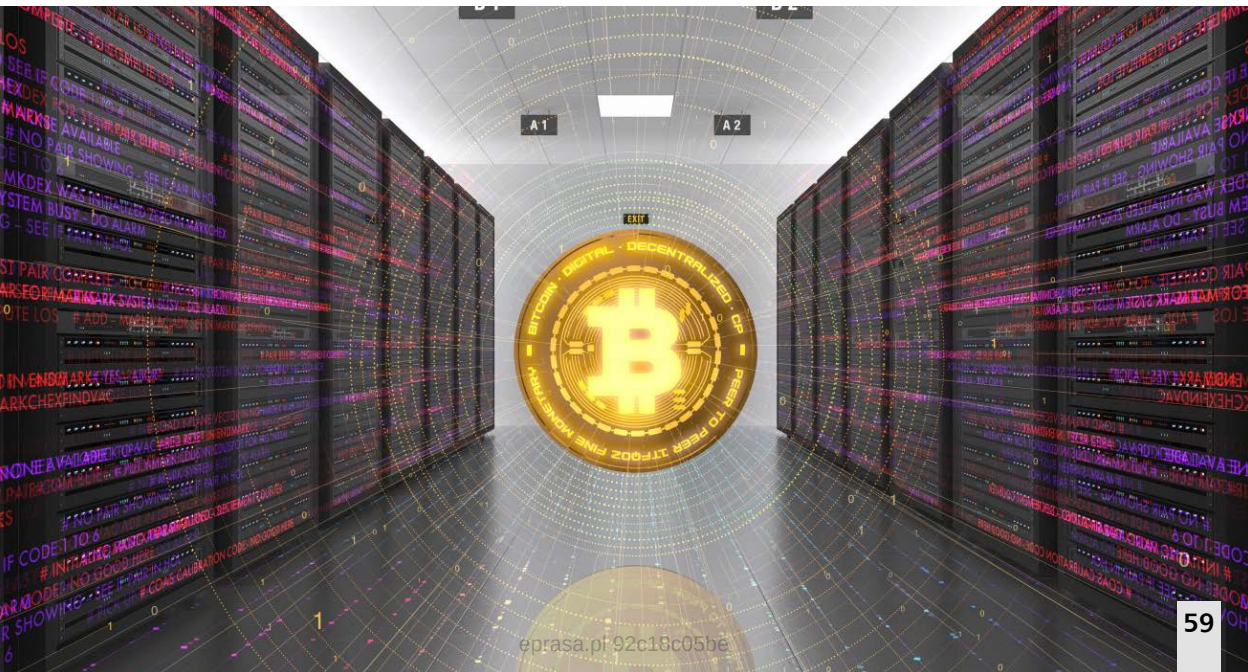
Pozostaje jedna droga: nie złamać kryptografii, tylko zbudować równoległy łańcuch bloków, dłuższy niż uczciwy. Sieć przyjmuje za prawdziwy ten łańcuch, w który włożono najwięcej pracy – to jest reguła Bitcoina. Jeśli atakujący zbuduje łańcuch dłuższy od uczciwego, sieć go zaakceptuje.

Żeby budować łańcuch szybciej niż wszyscy uczciwi górnicy razem wzięci, atakujący musi mieć więcej mocy obliczeniowej niż oni. Konkretnie – musi mieć ponad 50%, czyli więcej niż wszyscy pozostali. Stąd nazwa: atak 51%.

Kryptografia tu nic nie pomoże – nie pomaga, bo atakujący nie łamie żadnego algorytmu. Pomaga tylko ekonomia. Pytanie brzmi: ile to kosztuje?

Żeby mieć 51% mocy sieci Bitcoin, atakujący musiałby kupić tyle ASIC-ów, ile mają wszyscy uczciwi górnicy razem. To dziesiątki miliardów dolarów w sprzęcie. Plus kilka gigawatów ciągłej mocy elektrycznej – tyle, co duża elektrownia jądrowa. Plus chłodzenie, hale, personel. Realistyczny szacunek kosztu samego rozkręcenia takiej operacji: 30...50 miliardów dolarów.

A na dokładkę paradoks. W momencie, gdy atak zostanie zauważony, kurs bitcoina natychmiast się załamie – bo świat przestanie wierzyć w niezmienność łańcucha. Atakujący zniszczy więc wartość tego, co właśnie ukradł. Nawet gdyby udało mu się sfałszować transakcję na miliard dolarów, kurs bitcoinów spadnie dziesięciokrotnie i jego łup będzie wart sto milionów. Plus stracił 50 miliardów na sprzęt i prąd.



To jest właśnie sedno bezpieczeństwa Bitcoina, do którego obiecaliśmy wrócić w Części 2. Nie wynika ono z tego, że atak jest niemożliwy – wynika z tego, że jest tak drogi i tak nieopłacalny, że nikt o zdrowych zmysłach go nie podejmie. Pieniądze stoją między uczciwą siecią a oszustwem. A pieniądze te są realne – zmaterializowane w postaci szafy serwerów, rachunku za prąd i kursu bitcoina. Bez funkcji skrótu z Części 2, bez podpisów z Części 3, bez struktury bloków z Części 4 i bez ekonomii kopania z tej części – system by nie działał. Każdy z tych klocków sam w sobie jest prosty. Razem dają coś, czego przed Satoshim Nakamoto nie było.

Halving – co będzie za 100 lat

Pozostaje jedno pytanie do uczciwego dokończenia obrazu. Nagroda coinbase nie jest stała. Co cztery lata maleje o połowę. Mechanizm ten nazywa się halving.

W 2009 roku, gdy Satoshi wykopał Genesis Block, nagroda za blok wynosiła 50 BTC. W listopadzie 2012 roku spadła do 25. W lipcu 2016 do 12,5. W maju 2020 do 6,25. W kwietniu 2024

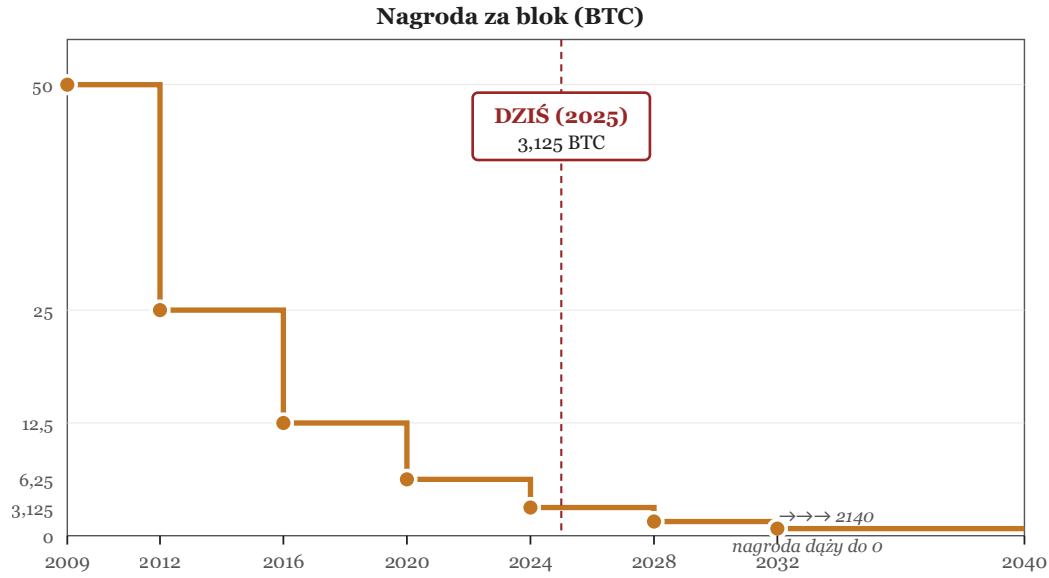
Halving – emisja Bitcoina w czasie

co 4 lata nagroda za blok zmniejsza się o połowę

MECHANIZM

Co 210 000 bloków (≈ 4 lata) nagroda coinbase maleje o połowę.

Łączna emisja Bitcoina jest skończona: dąży do **21 mln BTC**, do osiągnięcia ~2140 r.



Łączna podaż: 19,8 mln / 21 mln BTC = 94%

Pierwsze 94% wykopano w 16 lat. Pozostałe 6% będzie schodzić powoli przez kolejne 115 lat.

CO Z TEGO WYNIKA

W miarę spadania nagrody, opłaty transakcyjne muszą rosnąć w proporcji.

Czy same opłaty utrzymają sieć po 2140 r.? Otwarte pytanie ekonomiczne.

Rysunek 4. Halving Bitcoina. Nagroda za blok zmniejsza się o połowę co 4 lata. Krzywa schodkowa od 50 BTC w 2009 do 0 w 2140. Łączna podaż dąży do 21 milionów

do 3,125. Następne zmniejszenie – do 1,5625 – będzie około 2028 roku. I tak dalej, aż do roku około 2140, kiedy nagroda spadnie poniżej 1 satoshi i już z definicji wyniesie zero.

Ten mechanizm sprawia, że całkowita liczba bitcoinów, jakie kiedykolwiek powstaną, jest skończona i wyniesie nieco poniżej 21 milionów. Dziś, w maju 2026 roku, w obiegu jest około 20 milionów – czyli niemal 95% całości już zostało wydobyte. Pozostałe 5% będzie schodzić powoli przez kolejne 114 lat.

To prowadzi do interesującego pytania ekonomicznego. Jeśli za 100 lat nagroda będzie zerowa, czym zostaną opłacani górnicy? Odpowiedź: opłatami transakcyjnymi. Już dziś opłaty stanowią 5...15% przychodów górników. W miarę spadania nagrody, ta proporcja musi rosnąć. Niektórzy ekonomiści wątpią, czy same opłaty wystarczą do utrzymania bezpieczeństwa sieci tej skali. Inni zwracają uwagę, że gdy bitcoin stanie się standardowym pieniądzem rezerwowym, każda transakcja będzie warta tyle, że nawet niewielka opłata pomnożona przez 2000 transakcji na blok wystarczy.

To pytanie, na które odpowie historia. Na razie mechanizm działa: górnicy zarabiają, sieć rośnie, transakcje się przepychają. Z jednym istotnym zastrzeżeniem – dziś bitcoin to wciąż projekt-ekspperyment, nie stan ustalony. Czy stanie się powszechnym narzędziem czy zostanie ciekawostką inżynierską drugiej dekady XXI wieku, dowiemy się w nadchodzących dziesięcioleciach.

* * *

Mamy pełen obraz. Funkcja skrótu (Część 2) daje odcisk palca dla danych. Klucz publiczny i podpis cyfrowy (Część 3) pozwalają udowodnić tożsamość bez ujawniania sekretu. Transakcje, drzewa Merklego i bloki (Część 4) tworzą strukturę zapisu. Proof of work (ta część) sprawia, że ta struktura jest niezmienna i wzrasta według reguł, których nie kontroluje żadna instytucja.

Bitcoin nie jest magią. Nie jest sztuczną inteligencją, kryptografią kwantową ani nadprzyrodzoną technologią. Jest sprzężeniem zwrotnym między matematyką (SHA-256, krzywe eliptyczne), strukturą danych (UTXO, łańcuch bloków) i ekonomią (nagroda, opłaty, koszt prądu). Każdy z tych klocków sam w sobie jest prosty i znany od dawna. Genialność Satoshiego Nakamoto polegała na zauważeniu, że jeśli złoży się je razem we właściwy sposób – można uzyskać coś, czego wcześniej nie było: pieniądz, który nie potrzebuje banku.

Czy ten pieniądz przetrwa, czy stanie się dominującym, czy zniknie wyparty przez następne pokolenie systemów – tego nie wiadomo. Wiadomo natomiast, że jeśli czytelnik dotarł aż tutaj, to już rozumie, jak on działa. A to nie jest mało.

W kolejnej części cyklu pokażemy, co wokół Bitcoina powstało: alternatywne kryptowaluty (Ethereum i jego inteligentne kontrakty, stablecoiny, NFT), historię najsłynniejszych krachów i sukcesów, oraz pytanie, do którego cała ta opowieść prowadzi: szemrany epizod czy świetlana przyszłość?

Część 6. Szemrany epizod czy świetlana przyszłość?

Pięć poprzednich części zbudowało Czytelnikowi pełen obraz tego, jak Bitcoin działa od strony technicznej. Czas wrócić do pytania zadanego w tytule całego cyklu – i postarać się odpowiedzieć na nie uczciwie. To jest część eseistyczna, w której podsumowujemy historię, oglądamy sąsiadów Bitcoina w ekosystemie kryptowalut i staramy się ostrożnie spojrzeć w przyszłość.

Szesnaście lat w trzech krzywych

Pierwszy bitcoin pojawił się 3 stycznia 2009 roku. Pierwsza transakcja, w której bitcoin został wymieniony na coś materialnego, miała miejsce 22 maja 2010 roku. Programista Laszlo Hanyecz z Florydy zapłacił 10 000 BTC za dwie pizze. Dzień ten do dziś, na cześć tego pioniera, obchodzony jest jako Bitcoin Pizza Day. Po dzisiejszym kursie te pizze kosztowały około 800 milionów dolarów za sztukę.

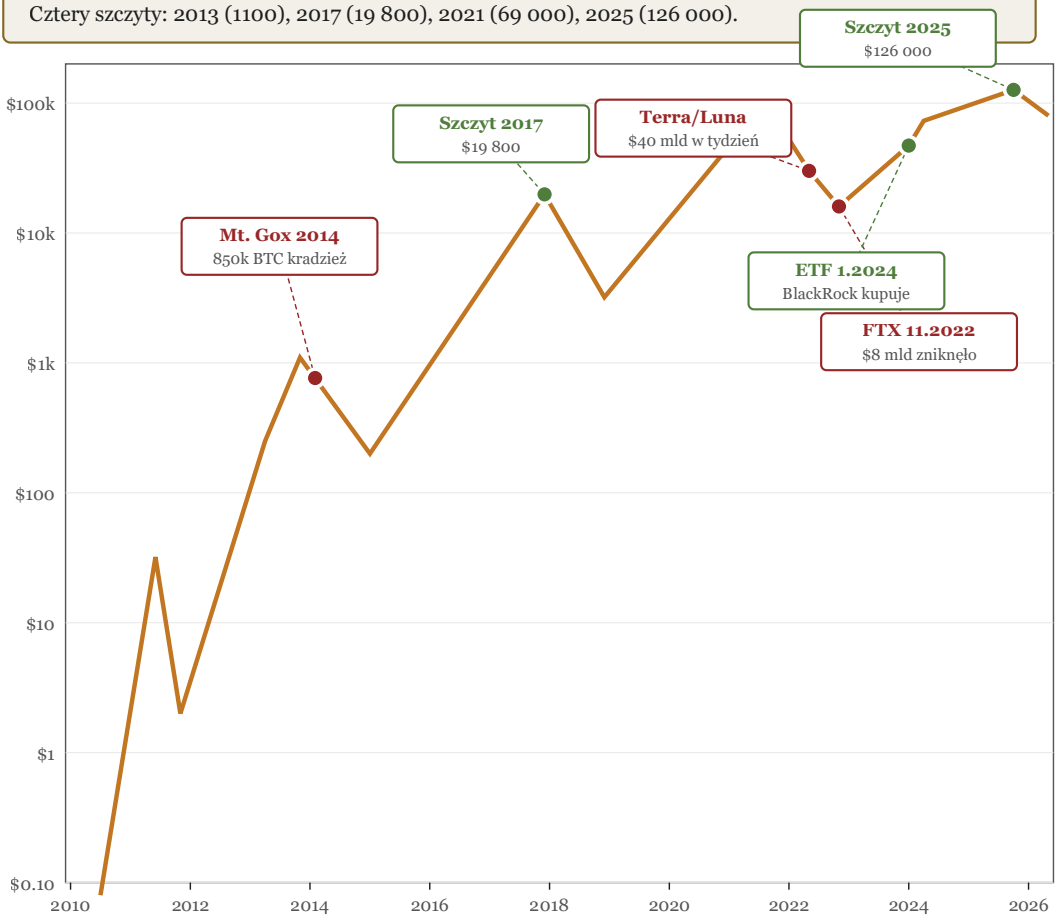
Od tamtego momentu krzywa kursu Bitcoina to wykres, który ekonomistów przyprawia o ból głowy. Cztery wyraźne fale wzrostu i krachu: pierwszy szczyt w 2013 (1100 dolarów), spadek do 200 w 2015. Drugi szczyt w grudniu 2017 (19 800 dolarów), spadek do 3200 w 2018. Trzeci szczyt w listopadzie 2021 (69 000 dolarów), spadek do 16 000 w 2022. Czwarty szczyt w październiku 2025 (ponad 126 000 dolarów). Dziś, w maju 2026 roku, jeden bitcoin kosztuje około 80 000 dolarów – czyli mniej więcej trzykrotnie tyle, ile rok wcześniej, ale jednocześnie 30% poniżej rekordu sprzed pół roku.

To są liczby z gatunku tych, które zdaniem ośmiu noblistów ekonomii (od Krugmana po Stiglitza) nie powinny móc istnieć. Bitcoin nie ma fundamentalnej wartości – nie generuje przepływów pieniężnych, nie produkuje niczego. Z drugiej strony – istnieje szesnaście lat, ma kapitalizację rynkową rzędu 1,6 biliona dolarów (półtora raza większą niż PKB Polski) i przeszedł cztery kryzysy, z których każdy wieszczono jako jego ostateczny upadek.

Cena Bitcoina 2010–2026

cztery cykle wzrostu i krachu, skala logarytmiczna

Pierwsza cena: 8 centów (2010, dwie pizze za 10 000 BTC).
Cztery szczyty: 2013 (1100), 2017 (19 800), 2021 (69 000), 2025 (126 000).



Wydarzenia historyczne

- krachy: Mt. Gox, Terra/Luna, FTX
- szczyty cykli i wydarzenia pozytywne (ETF 2024)

CO POKAZUJE TEN WYKRES

- Skala logarytmiczna – każdy odcinek pionowy = 10× wzrost.
- Cztery cykle: szczyt, krach, akumulacja, nowy szczyt – każdy wyższy niż poprzedni.
- Krachy 2022 (Terra/Luna i FTX) okazały się dnem 4. cyklu.
- Zatwierdzenie ETF (1.2024) otworzyło fundusze instytucjonalne na BTC.

Czy 2026 to początek 5. cyklu? Wiadomo będzie dopiero retrospektywnie.

Rysunek 1. Cena Bitcoina od 2010 do 2026 roku w skali logarytmicznej. Zaznaczone najważniejsze krachy (Mt. Gox 2014, Terra/Luna i FTX 2022) oraz wydarzenia pozytywne (zatwierdzenie ETF 2024)

Krachy: trzy lekcje

Każdy z czterech krachów Bitcoina niósł ze sobą inną lekcję. Warto się im przyjrzeć z bliska, bo razem składają się na to, co odróżnia kryptowaluty od reszty rynku.

Mt. Gox, 2014. Pierwszy poważny krach przyszedł od strony, której nikt się nie spodziewał – z infrastruktury. Mt. Gox była giełdą z Tokio, przez którą w szczytowym momencie przechodziło 70% wszystkich transakcji bitcoinowych na świecie. W lutym 2014 ogłosiła, że hackerzy ukradli z niej 850 000 BTC – wtedy 460 milionów dolarów, dziś byłoby to ponad 80 miliardów. Cena Bitcoina spadła z 1100 do 360 dolarów. Lekcja: protokół Bitcoina jest bezpieczny, ale strony trzecie obsługujące go – niekoniecznie. Twoje monety są naprawdę twoje tylko wtedy, gdy klucz prywatny jest w twoim posiadaniu, nie na cudzej giełdzie.

Terra/Luna, maj 2022. Drugi krach miał inną naturę – pochodził z wnętrza ekosystemu krypto. Terra była tak zwanym stablecoinem algorytmicznym – kryptowalutą, która miała utrzymywać stałą wartość 1 dolara nie dzięki rezerwom w bankach (jak czyni to Tether), ale dzięki sprytnemu mechanizmowi giełdowemu z drugą walutą o nazwie Luna. Kiedy w maju 2022 roku rynek stracił zaufanie do tego mechanizmu, w ciągu tygodnia wyparowało 40 miliardów dolarów. Luna spadła z 80 dolarów do ułamka centa. Lekcja: nie wszystko, co nazywa się stablecoinem, jest stabilne. Rozwiązania algorytmiczne, które wyglądają elegancko na papierze, mogą ulec spirali śmierci, gdy rynek przestanie wierzyć w obietnicę.

FTX, listopad 2022. Trzeci krach był z gatunku tych, jakie świat finansów zna od stuleci – zwykła defraudacja. Sam Bankman-Fried, młody fizyk z MIT, prowadził FTX, jedną z największych giełd kryptowalut. W listopadzie 2022 roku okazało się, że FTX bez wiedzy klientów inwestowała ich pieniądze w powiązaną firmę handlową. Klienci zażądali wypłat, FTX nie miała pieniędzy. Bankructwo. Bankman-Fried odsiaduje 25 lat w więzieniu federalnym za oszustwa. Z FTX zniknęło 8 miliardów dolarów. Lekcja: krypto nie eliminuje oszustw – eliminuje tylko niektórych pośredników. Zawsze, gdy oddajesz komuś klucze, oddajesz mu też ryzyko.

Każdy z tych trzech krachów wieszczono jako koniec kryptowalut. Po każdym sektor wracał silniejszy. Po Mt. Gox powstały giełdy z lepszymi zabezpieczeniami i wymogami audytu. Po Terra/Luna regulatorzy z Unii Europejskiej i USA zaczęli pisać przepisy o stablecoinach. Po FTX zatwierdzono fundusze ETF na Bitcoin – paradoksalnie, krach oszusta przyspieszył akceptację instytucjonalną Bitcoina.

Sukces, którego się nie spodziewano: ETF

10 stycznia 2024 roku amerykańska Komisja Papierów Wartościowych (SEC) zatwierdziła pierwsze fundusze ETF (*Exchange Traded Fund*), które bezpośrednio kupują Bitcoin. To wydaje się drobiazgiem, ale dla rynku finansowego było momentem przełomowym.

Do tej pory osoba chcąca zainwestować w Bitcoin musiała założyć konto na giełdzie kryptowalut, przejść proces weryfikacji, nauczyć się obsługi portfela, zatroszczyć o klucze prywatne. Po 10 stycznia 2024 wystarczy zalogować się do dowolnego brokera giełdowego – tego samego, którego używamy do akcji – i kupić udział w funduszu BlackRock IBIT, Fidelity FBTC albo dziesięciu podobnych. Fundusze te w naszym imieniu kupują Bitcoiny i je przechowują. My handlujemy ich udziałami jak zwykłymi akcjami.

Skutek był natychmiastowy. W ciągu pierwszego roku istnienia fundusze ETF zgromadziły ponad 100 miliardów dolarów aktywów. BlackRock – największa firma zarządzająca aktywami na świecie – stała się jednym z największych posiadaczy Bitcoina. To samo BlackRock, którego prezes Larry Fink jeszcze w 2017 roku nazywał Bitcoina „wskaźnikiem prania pieniędzy". Siedem lat później sprzedaje go swoim klientom na masową skalę.

To jest moment, w którym Bitcoin przestaje być produktem niszowym i wchodzi do mainstream'u finansowego. Dziś (maj 2026) szacuje się, że około 7% dorosłych Amerykanów ma jakąś ekspozycję na Bitcoina, najczęściej właśnie poprzez ETF. W Polsce – według badań Cinkciarz.pl – mniej niż 4%.

Bitcoin to nie wszystko: ekosystem

Skupiliśmy się w tym cyklu na Bitcoinie, bo to on rozpoczął całą historię i wciąż jest dominującą kryptowalutą – z około 60% udziałem w łącznej kapitalizacji rynku. Ale wokół niego przez 16 lat narósł cały ekosystem alternatywnych projektów, z których każdy próbował usprawnić jakąś cechę albo dodać nową funkcję.

Najważniejszym z nich jest Ethereum, uruchomione w 2015 roku przez 19-letniego wówczas Vitalika Buterina (urodzony w Rosji, gdy miał 6 lat rodzice emigrowali do Kanady). Ethereum nie miało być tylko cyfrowym pieniądzem. Miało być cyfrowym komputerem – siecią, w której można uruchamiać programy w sposób tak samo niezmienny i zdecentralizowany jak transakcje w Bitcoinie. Te programy nazywają się smart contracts (inteligentne kontrakty), choć nie są ani inteligentne, ani też nie są kontraktami w prawnym sensie – są po prostu kawałkami kodu zapisanymi w blockchainie i wykonywanymi przez sieć węzłów.

Praktyczny przykład. Wyobraź sobie program, który ma jeden warunek: „jeśli do dnia 31 grudnia 2026 roku stan konta sieciowego pokaże, że Polska wygrała mistrzostwa świata w piłce nożnej, wyślij 1000 ETH na adres X; w przeciwnym wypadku – na adres Y". Taki program zostanie wykonany tak, jak go napisano, niezależnie od tego, kto będzie wtedy z wyniku niezadowolony, kto kogo będzie chciał oszukać. To jest siła smart kontraktów – automatyzacja zaufania.

Na Ethereum powstały tysiące takich programów. Wymiany walut bez pośrednika (DeFi – decentralized finance), platformy aukcyjne, gry, ubezpieczenia, NFT (Non-Fungible Token – niewymienialne tokeny), certyfikaty cyfrowej własności obrazów, muzyki, awatarów w grach. Część z tych projektów to była i jest poważna inżynieria. Część – bańka spekulacyjna, którą zmiotła rzeczywistość. NFT z 2021 roku, sprzedawane za miliony dolarów, dziś warte są ułamek tej sumy – wiele jest niesprzedawalnych w ogóle.

Stablecoiny – kryptowaluta, która udaje, że nią nie jest

Jeśli wadą kryptowalut jest zmienność kursu (40% w jednym roku, 100% w następnym), to logicznie powinno powstać coś, co tej zmienności nie ma – ale zachowuje cyfrową naturę i możliwość transferu w ciągu sekund przez całą Ziemię. To są stablecoiny.

Najpopularniejszy z nich, Tether (USDT), jest cyfrowym dolarem amerykańskim. Każdy USDT, który istnieje, jest podparty (przynajmniej w teorii) jednym dolarem trzymanym w banku przez emitenta. Drugi, USD Coin (USDC), działa podobnie, ale jest emitowany przez amerykańską firmę Circle pod regulacją amerykańską. Łącznie

MAŁY SŁOWNIK CYKLU

Hash (skrót) – krótki, jednoznaczny odcisk palca dowolnych danych. (część 2)

SHA-256 – konkretna funkcja skrótu używana w Bitcoinie. Daje 256 bitów wyjścia. (część 2)

Klucz prywatny/publiczny – para liczb, w której prywatnym podpisuje się, publicznym weryfikuje. (część 3)

Adres bitcoinowy – krótki ciąg znaków, na który ktoś może wysłać Ci bitcoiny. Pochodna klucza publicznego. (część 3)

UTXO – niewydany wpływ z poprzedniej transakcji. Twój portfel to lista UTXO. (część 4)

Drzewo Merklego – konstrukcja, w której tysiące transakcji da się reprezentować jednym hashem. (część 4)

Blockchain – łańcuch bloków, w którym każdy zawiera hash poprzedniego. (część 4)

Proof of work – metoda budowy łańcucha przez zgadywanie nonce. Tworzy ekonomiczną barierę dla oszustów. (część 5)

Halving – zmniejszenie nagrody za blok o połowę co 4 lata. Limituje emisję do 21 mln BTC. (część 5)

Smart kontrakt – program zapisany w blockchainie, wykonywany automatycznie według reguł kodu. (część 6)

Stablecoin – kryptowaluta utrzymująca stałą wartość 1 dolara. Najbardziej popularne: USDT, USDC. (część 6)

Ekosystem kryptowalut

stan na maj 2026, łączna kapitalizacja ~2,8 bln $

1. BITCOIN (BTC) — ~57% rynku

Pierwsza i największa kryptowaluta. Skupiamy się na niej w tym cyklu.
Funkcje: cyfrowy pieniądz, magazyn wartości („cyfrowe złoto").

Kapitalizacja: **~$1,6 bln**
Cena dziś: **~$80 000**
W obiegu: **19,8 mln BTC (94% z 21 mln)**

2. ETHEREUM (ETH) — ~8% rynku

Drugi co do wielkości projekt. Nie tylko pieniądz – platforma do uruchamiania programów (smart kontraktów). Twórca: Vitalik Buterin (2015).

Kapitalizacja: **~$233 mld**
Główne zastosowania: DeFi, NFT, stablecoiny (USDC, USDT)
Od 2022 r. używa proof of stake – tysiące razy mniej energii niż Bitcoin.

3. STABLECOINY

Cyfrowy odpowiednik dolara.
USDT (Tether), USDC, DAI.

Łącznie: **~$230 mld**
płatności międzynarodowe

4. ALTCOINY

Solana, XRP, Cardano,
Polkadot, Avalanche...

Łącznie tysiące: **~$700 mld**
95% nie przetrwa cyklu

5. ZASTOSOWANIA NA WIERZCHU (głównie Ethereum)

DeFi (Decentralized Finance)
Wymiana walut, pożyczki, ubezpieczenia – bez pośrednika, na smart kontraktach.
Uniswap, Aave, Compound

NFT (Non-Fungible Tokens)
Cyfrowe certyfikaty własności obrazów, awatarów, gier.
2021 boom, 2024 – krach 90%

CO Z TEGO MAPOWAĆ

- Bitcoin to ponad połowa rynku – i ta dominacja od lat się utrzymuje.
- Ethereum to drugi filar – platforma na której powstał cały ekosystem aplikacji.
- Stablecoiny zastąpiły dolara w wielu krajach z niestabilną walutą.
- Tysiące altcoinów – większość z nich zniknie w najbliższej dekadzie.

Lekcja kryptografii (Części 2...5) dotyczy tylko warstwy technicznej Bitcoina.
Nad tą warstwą rozkwitł świat finansowy o własnych regułach i ryzykach.

Rysunek 2. Ekosystem kryptowalut. Bitcoin (1. miejsce, 60% rynku) i Ethereum (2. miejsce, 14%) plus najważniejsze kategorie: stablecoiny, alternatywne łańcuchy, DeFi, NFT

Sześć części, sześć klocków

cały Bitcoin to suma tych klocków, niczego więcej

każdy element zależy od poprzedniego – usuń jeden, system się rozsypuje

część 1 — **Problem** — *kontekst i pytanie*

Jak zsynchronizować nieufnych nieznajomych?

część 2 — **Funkcja skrótu** — *narzędzie 1*

SHA-256 – odcisk palca dla danych. Jednokierunkowa, lawinowa.

część 3 — **Klucze i podpisy** — *narzędzie 2*

Para kluczy (priv/pub), krzywe eliptyczne, ECDSA.

część 4 — **Transakcje i blok** — *struktura*

UTXO, drzewo Merklego, łańcuch bloków = blockchain.

część 5 — **Proof of work** — *konsensus*

Górnicy zgadują nonce. Ekonomia chroni przed atakiem 51%.

część 6 — **Co z tego wynika** — *kontekst i odpowiedź*

Krachy, sukcesy, ekosystem. Świetlana przyszłość czy szemrany epizod?

CO Z TEGO POWSTAJE

Każdy z klocków znany od dziesięcioleci, używany w innych zastosowaniach.
Genialność Satoshiego: ułożył je w sposób, w jaki nikt wcześniej tego nie zrobił.
Bitcoin = suma elementów. Nie magia, nie AI, nie kryptografia kwantowa.

Rysunek 3. Sześć części cyklu jako jedna konstrukcja. Każdy element zależy od poprzedniego. Bitcoin to suma tych klocków, niczego więcej

na rynku jest około 230 miliardów dolarów stablecoinów – to więcej, niż wynosi suma wartości rynkowej polskiej giełdy GPW.

Stablecoiny stały się głównym narzędziem operacyjnym świata krypto. Traderzy używają ich do parkowania środków między transakcjami. Mieszkańcy krajów z hiperinflacją (Argentyna, Turcja, Liban) używają ich jako de facto cyfrowych dolarów – bo zwykłe dolary albo są zakazane, albo niedostępne. Pracownicy firm międzynarodowych w Indiach, na Filipinach, w Afryce coraz częściej dostają wynagrodzenie w USDT, bo dociera szybciej i taniej niż przelew bankowy.

Spór o stablecoiny toczy się dziś na poziomie regulacyjnym. Czy emitent USDT naprawdę ma pełne pokrycie w dolarach? Czy działalność Tethera jest wystarczająco transparentna? Co stanie się, jeśli okaże się, że pokrycia nie ma – kto ucierpi? Niektóre kraje (Wielka Brytania, Singapur, Unia Europejska w ramach przepisów MiCA) wprowadziły już lub wprowadzają restrykcyjne ramy prawne. Inne (USA) wciąż się nad tym zastanawiają. Bo choć stablecoiny rozwiązują problem zmienności, wprowadzają nowy problem – zaufania do emitenta. A to dokładnie ten problem, którego Bitcoin miał uniknąć.

Co czeka Czytelnika

Pora powiedzieć, czego nie wiemy. Nie wiemy, czy Bitcoin za dwadzieścia lat będzie wart zero, czy milion dolarów. Nie wiemy, czy stanie się standardem płatniczym, czy pozostanie cyfrowym złotem trzymanym jako ubezpieczenie przed inflacją. Nie wiemy, jaką rolę odegrają w tym wszystkim banki centralne – niektóre (Chiny, Bahama, Nigeria) już uruchomiły własne cyfrowe waluty, inne (USA, strefa euro) jeszcze się wahają.

Wiemy jednak kilka rzeczy. Wiemy, że technologia działa – szesnaście lat bez krytycznej awarii to dla protokołu finansowego dużo. Wiemy, że atrakcja jest realna – siedem procent Amerykanów to nie statystyczny szum. Wiemy, że nie da się tego już skasować – kraj, który zakazał Bitcoina (Chiny w 2021 roku), tylko przepędził kopalnie do innych krajów; sieć działa nadal.

Wiemy też, że ryzyka pozostają. Ryzyko regulacyjne – państwa mogą utrudniać korzystanie z kryptowalut, podatkując je dotkliwie albo wymagając identyfikacji każdej transakcji. Ryzyko technologiczne – komputery kwantowe, choć dziś dalekie od praktyki, w teorii mogą za 15...30 lat złamać kryptografię klucza publicznego, na której Bitcoin polega. Ryzyko ekonomiczne – co, jeśli po 2140 roku same opłaty transakcyjne nie wystarczą, by utrzymać sieć w bezpieczeństwie? Pytania, na które dziś nikt nie ma odpowiedzi.

Sześć części, sześć klocków

Pomyślmy na koniec o tym, co zbudowaliśmy w tym cyklu. Każda z pięciu poprzednich części wprowadziła jeden klocek. Teraz jest jasne, jak się składają w całość:

Część 1 postawiła problem – jak zsynchronizować nieufnych nieznajomych. Część 2 dała narzędzie pomocnicze – funkcję skrótu, odcisk palca dla danych. Część 3 dała narzędzie tożsamości – parę kluczy publicznych i podpis cyfrowy. Część 4 dała strukturę – transakcje, drzewa Merklego, łańcuch bloków. Część 5 dała mechanizm konsensusu – proof of work, ekonomię kopania. Część 6 (ta) dała kontekst – co z tego wynika dla świata.

To jest cały Bitcoin. Sześć klocków, ułożonych w określonej kolejności, dających razem efekt, którego nie ma żaden z osobna. Genialność Satoshiego Nakamoto polegała nie na wymyśleniu nowej kryptografii – wszystkie klocki były znane od wielu lat – ale na tym, jak je złożył w sposób, w który nikt wcześniej tego nie zrobił.

Czy jest to wynalazek na miarę druku? Internetu? A może tylko ciekawostka swojej epoki, która zniknie wraz z modą na nią? Tego dziś nikt uczciwie nie wie. Ale po sześciu częściach Czytelnik zna już cały mechanizm. I gdy ktoś zapyta go o zdanie na temat kryptowalut, będzie mógł powiedzieć coś sensownego – niezależnie od tego, jakie zdanie wyrobi sobie ostatecznie.

* * *

Mamy obraz technologiczny. Wiemy, jak to działa od środka. Wiemy, co wokół tego narosło i gdzie były krachy. Pora zejść z poziomu protokołu na poziom codzienności – bo Czytelnik, który dotrwał do tego miejsca, zapewne zadał sobie już praktyczne pytania: jak właściwie kupuje się te bitcoiny, gdzie się je trzyma, jak się nimi płaci. I czy to jest bezpieczne. W Części 7 zajmiemy się instytucją, która stoi między zwykłym człowiekiem a Bitcoinem – czyli giełdą – oraz świeżą polską aferą, która tę instytucję pokazała w mało chwalebnym świetle. W Części 8 – praktyka.

Część 7. Giełdy, tokeny i lekcja z Zondacrypto

W szóstej części cyklu zamknęliśmy techniczne wyjaśnienie Bitcoina. Po sześciu poprzednich częściach Czytelnik wie, jak działa funkcja skrótu, podpis cyfrowy, łańcuch bloków i mechanizm konsensusu. To pełna teoria. Pozostaje praktyka – i z nią wiąże się pewien paradoks. Bitcoin powstał po to, żeby uwolnić nas od pośredników. A 99% ludzi, którzy go używają, korzysta z niego dokładnie przez pośredników. Tymi pośrednikami są giełdy. I akurat teraz, w Polsce, jeden z największych pośredników – Zondacrypto – jest świeżutkim podręcznikowym przykładem tego, dlaczego ten paradoks bywa kosztowny.

Paradoks pośrednika

Wyobraźmy sobie tę sytuację. Bitcoin – system, który opisaliśmy jako pomysł na pieniądz bez banku, bez nadzorcy, bez potrzeby zaufania do kogokolwiek. Każdy może uruchomić węzeł sieci. Każdy może mieć własny portfel z własnymi kluczami prywatnymi. Każdy może w bezpośredniej transakcji peer-to-peer wykonać przelew na drugi koniec świata.

A teraz spójrzmy na statystyki: szacuje się, że ponad 95% osób posiadających bitcoiny trzyma je nie we własnym portfelu, tylko na giełdzie. Czyli na koncie u pośrednika. Czyli – paradoksalnie – w sposób bardzo podobny do tego, w jaki trzymamy złotówki w banku. Z jedną różnicą: bank jest regulowany, depozyty do równowartości 100 000 euro są ubezpieczone przez Bankowy Fundusz Gwarancyjny, a nadzór sprawuje Komisja Nadzoru Finansowego. Giełda kryptowalut – w większości przypadków – nie jest tym wszystkim objęta.

Skąd ten paradoks? Z trzech powodów. Po pierwsze, żeby kupić bitcoiny za złotówki, gdzieś trzeba je wymienić. Najwygodniej – na giełdzie, która ma wbudowany kurs i obsługuje przelewy bankowe. Po drugie, samodzielne zarządzanie kluczami prywatnymi jest trudniejsze, niż to brzmi w teorii – zgubienie hasła do portfela oznacza utratę pieniędzy bez możliwości odzyskania. Po trzecie, giełda oferuje płynność: jeśli chcesz natychmiast sprzedać

Jak działa giełda kryptowalut

trzy funkcje w jednej firmie – i ich konsekwencja

1. KANTOR

wymiana fiat → krypto

Klient ma 1000 zł na koncie giełdowym, klika „kup BTC".
Giełda zamienia złotówki na bitcoiny po aktualnym kursie.

– punkt wejścia świata fiat do świata krypto

2. KSIĘGA ZLECEŃ

kojarzenie kupujących i sprzedających

Wszyscy klienci wystawiają swoje oferty kupna/sprzedaży.
Giełda kojarzy je w pary i wykonuje transakcję.

– stąd kurs i płynność rynku

3. DEPOZYTARIUSZ

to tu mieszka problem

Giełda przechowuje monety wszystkich klientów.
Klucze prywatne ma giełda, nie klient.

Klient ma tylko zapis w bazie, mówiący ile mu się należy.
– a baza jest własnością firmy

Co się dzieje w momencie zakupu

1. Wpłacasz 1000 zł z banku na konto giełdowe.
   Pieniądze są w banku giełdy, nie u Ciebie.
2. Klikasz „kup 0,01 BTC". Złotówki znikają z konta.
   Pojawia się saldo „0,01 BTC".
3. **Ten 0,01 BTC to wpis w bazie giełdy. Nic więcej.**
   Realne bitcoiny są na adresie giełdy (klucze: ona).
   – moment, w którym przestajesz być właścicielem

DLACZEGO TO WAŻNE

- Konto giełdowe = wierzytelność wobec firmy.
- Bank ma BFG (gwarancje do 100 tys. EUR). Giełda – nie ma.
- Jeśli giełda zbankrutuje, idzie się do masy upadłościowej.
- Praktyka: giełdy często „pożyczają" klientom monety same sobie.

Stąd zasada: NOT YOUR KEYS, NOT YOUR COINS
jeśli klucze nie są twoje, monety nie są twoje

Rysunek 1. Jak działa giełda kryptowalut. Trzy funkcje (kantor, giełda zleceń, depozytariusz) i jeden kluczowy moment, w którym klient przestaje być właścicielem swoich monet

0,1 BTC, ktoś po drugiej stronie musi to natychmiast kupić; giełda kojarzy te dwie strony.

Te powody nie są fałszywe. Giełdy mają realną wartość. Pytanie brzmi tylko, jak ich używać, żeby nie skończyć jak klienci Zondacrypto wiosną 2026 roku.

Po co właściwie istnieje giełda kryptowalut

Giełda kryptowalut to firma, która prowadzi trzy rodzaje działalności jednocześnie. Po pierwsze, jest kantorem – pozwala wymienić złotówki na bitcoiny i na odwrót. Po drugie, jest zwykłą giełdą w klasycznym sensie – kojarzy kupujących i sprzedających, prowadzi tzw. księgę zleceń, ustala kurs na podstawie ofert. Po trzecie, jest depozytariuszem – przechowuje monety i pieniądze klientów.

Trzeci punkt jest kluczowy. Klient otwiera konto na giełdzie, wpłaca z banku tysiąc złotych, kupuje za to bitcoiny. Te bitcoiny pojawiają się na jego koncie giełdowym. W tym momencie wydaje się, że wszystko jest w porządku – ekran pokazuje saldo 0,01 BTC. Ale to ekran. W rzeczywistości monety są na adresie giełdy, do którego klucz prywatny ma giełda, a nie klient. Klient ma tylko obietnicę – wewnętrzny zapis w bazie danych firmy mówiący, że jest mu należnych 0,01 BTC.

AFERA ZONDACRYPTO 2026

Zondacrypto – działająca pod tą nazwą od 2022 roku, wcześniej znana jako BitBay – była największą polską giełdą kryptowalut. W oficjalnych materiałach reklamowych deklarowała milion zarejestrowanych użytkowników; według ujawnionych w kwietniu 2026 szacunków prokuratury osób, które realnie ulokowały na niej środki i mogą zostać uznane za pokrzywdzone, jest około 30 tysięcy. Sponsorowała kluby Ekstraklasy (Raków, Lechię, Pogoń), Polski Komitet Olimpijski, włoski Juventus. Stadion w Częstochowie nazywa się Zondacrypto Arena.

Na początku kwietnia 2026 roku money.pl i Wirtualna Polska opublikowały analizę firmy Recoveris opartą na danych on-chain – czyli analizie publicznych adresów giełdy w łańcuchu Bitcoina. Wyniki były szokujące: średni miesięczny stan bitcoinów na portfelach Zondacrypto spadł z około 56 BTC w sierpniu 2024 do 0,18 BTC w marcu 2026. Spadek o 99,7%. Pierwszego kwietnia 2026 roku saldo wyniosło 0,086 BTC – równowartość około 21 tysięcy złotych. Dla giełdy obsługującej dziesiątki tysięcy aktywnych użytkowników.

Jednocześnie z giełdy w ciągu czterech miesięcy wytransferowano za pomocą 511 przelewów aktywa o łącznej wartości ponad 21 milionów dolarów – głównie do konkurencyjnego Krakena. Klienci Zondacrypto zaczęli zgłaszać problemy z wypłatami, początkowo w bitcoinach, później także w Ethereum. Prokuratura Regionalna w Katowicach wszczęła śledztwo; sprawę powierzono Centralnemu Biuru Zwalczania Cyberprzestępczości. Wstępna kwota szkody została w połowie kwietnia oszacowana na 350 milionów złotych i wciąż rośnie. Sponsorowane kluby zaczęły informować o niezapłaconych ratach.

W pierwszych tygodniach kwietnia prezes Zondacrypto Przemysław Kral zaprzeczał kryzysowi: tłumaczył, że to awaria techniczna i atak medialny, ujawnił adres portfela rzekomo zawierającego 4500 bitcoinów (warte około 330 milionów dolarów), do którego klucze miał posiadać zaginiony od marca 2022 roku założyciel giełdy Sylwester Suszek. Niezależnego audytu nie udostępnił. Szesnastego kwietnia 2026 roku Kral opublikował ostatni wpis i zniknął. Wcześniej, w listopadzie 2025, na własne życzenie został przeniesiony na listę adwokatów niewykonujących zawodu; w styczniu 2026 zawiesił działalność gospodarczą w Polsce. Od 2025 roku dysponował również paszportem izraelskim. Mieszkał w Monako, ostatnio przebywał w Izraelu, obecnie – według ustaleń Onetu i Wirtualnej Polski – w Zjednoczonych Emiratach Arabskich. Dziewiętnastego kwietnia z funkcji zrezygnowała rada nadzorcza spółki-właściciela. Dwudziestego pierwszego kwietnia pracownicy otrzymali wypowiedzenia z przyczyną „całkowita likwidacja Pracodawcy". W tym samym czasie Onet, powołując się na źródła w Prokuraturze Krajowej, ujawnił, że faktycznym właścicielem giełdy miał być Marian W. „Maniek" – postać znana wcześniej z zarzutów o kierowanie zorganizowaną grupą przestępczą zajmującą się handlem paliwami – a zarówno Suszek, jak i Kral pełnili jedynie rolę „słupów". Suszek po raz ostatni widziany był 10 marca 2022 roku na terenie bazy paliwowej Mariana W. w Czeladzi.

W chwili pisania tego tekstu (drugi tydzień maja 2026) Zondacrypto nie ogłosiła formalnie upadłości, ale fizycznie przestała działać. Pieniądze klientów pozostają zamrożone. Prokuratura ściga, kancelarie organizują pozwy zbiorowe, UOKiK przyjął ponad 200 zgłoszeń. Polski Komitet Olimpijski i kluby sportowe zerwały umowy sponsorskie. W sferze politycznej toczy się spór: rząd Tuska wskazuje, że prezydent Karol Nawrocki dwukrotnie zawetował ustawę o rynku kryptoaktywów (grudzień 2025 i kwiecień 2026), uniemożliwiając Komisji Nadzoru Finansowego objęcie giełdy nadzorem; prezydent odpowiada, że to rząd dysponował informacjami służb i obowiązkiem rządu było ostrzec obywateli. Niezależnie od tego, kto ma rację politycznie, sprawa już teraz jest tym, co krypto-świat przerabiał wielokrotnie: Mt. Gox 2014, FTX 2022, teraz Zondacrypto 2026. Trzy razy ta sama lekcja.

Jest to dokładnie ten sam mechanizm, który w bankowości znamy od stuleci. Bank, w którym mamy konto, nie trzyma „naszych pieniędzy" w sejfie z naszym imieniem. Bank trzyma pieniądze w jednej masie, a my mamy roszczenie wobec banku – wpis w księgach. Jeśli bank zbankrutuje, nasze roszczenie idzie do masy upadłościowej. Dlatego wymyślono Bankowy Fundusz Gwarancyjny.

Z giełdami kryptowalut jest gorzej. Nie tylko trzymają pieniądze w jednej masie

Natywna kryptowaluta vs token

co Bitcoin ma, czego token nie ma

BITCOIN (BTC)

natywna kryptowaluta

Własna sieć
~15 000 węzłów na świecie

Własny protokół
SHA-256, ECDSA, UTXO, halving

Własni górnicy
proof of work, 6×10^{20} hashy/s

1 BTC

istnieje w łańcuchu Bitcoina

TOKEN ERC-20

np. USDC, UNI, ZBT, FTT

Ethereum (cudza sieć)
~1 000 000 węzłów na świecie

Cudzy protokół (Ethereum)
proof of stake, smart kontrakty

Smart kontrakt (np. ZBT)

```
balance[Alicja] = 100
balance[Bob] = 50
balance[Czesława] = 200
```

1 TOKEN

to wpis w cudzym kontrakcie

Co to znaczy w praktyce

cecha	Bitcoin (natywna)	token ERC-20
Sieć	własna, niezależna	działa tylko jeśli działa Ethereum
Awaria Ethereum	nie dotyczy	token przestaje działać
Wartość	z protokołu	z obietnic emitenta
Co się stanie, jeśli	nic – protokół żyje	wartość → 0
emitent zniknie	(emitenta nie ma)	(jak FTT po krachu FTX)

PRZYKŁADY TOKENÓW W PRAKTYCE

USDC, USDT – token-stablecoin: 1 USD trzymany w banku emitenta *(jeśli emitent zbankrutuje, dolary znikają)*
FTT – token giełdy FTX; w XI 2022 spadł z $25 do $1 w 3 dni
ZBT – token Zondacrypto; może podzielić los FTT
Wniosek: token jest tak bezpieczny, jak emitent. BTC nie ma emitenta.

Rysunek 2. Bitcoin (natywna kryptowaluta) vs token ERC-20 na Ethereum. Bitcoin jest „pierwszym piętrem" – własna sieć, własni górnicy. Token siedzi „na piętrze drugim", w smart kontrakcie cudzej sieci

– często dokładnie tych samych pieniędzy używają jako kapitału roboczego, inwestują je, pożyczają. A ubezpieczenia w stylu BFG dla giełd nie istnieją. Co do zasady. W teorii wszystkie te działania regulamin powinien zakazywać. W praktyce – sprawdzimy poniżej, czy zakazuje skutecznie.

Czym jest token (a czym nie jest bitcoin)

Wprowadźmy ważne rozróżnienie, bo czytelnik prasy ekonomicznej często słyszy słowo „token" w kontekście, w którym nie zawsze wiadomo, co dokładnie oznacza.

Bitcoin nie jest tokenem. Bitcoin jest natywną kryptowalutą – to znaczy, że istnieje w swoim własnym łańcuchu bloków, ze swoimi własnymi regułami emisji (ten halving z Części 5), ze swoimi własnymi górnikami. To samo Ethereum: jest natywną kryptowalutą sieci o tej samej nazwie. Solana, Cardano, Polkadot – wszystkie są natywnymi kryptowalutami swoich łańcuchów.

Token to coś innego. Token to wpis w kontrakcie smart, który mówi: „w tym kontrakcie istnieje milion jednostek czegoś, co nazywa się X, i ich właściciele są tacy a tacy". Token nie ma własnego łańcucha – żyje na cudzym, najczęściej Ethereum. Jego ruch nie jest oddzielną transakcją w sensie protokołu; jest wywołaniem funkcji w smart kontrakcie, który zaktualizuje swoją wewnętrzną tabelę „kto ma ile".

Standard, który definiuje, jak takie tokeny mają się zachowywać, nazywa się ERC-20. Chodzi o uniwersalny zestaw funkcji: ile mam jednostek, prześlij komuś, zatwierdź wypłatę. Każdy programista może w godzinę napisać własny smart kontrakt zgodny z ERC-20 i wypuścić swój token. Stąd ekosystem ma ich dziś setki tysięcy.

Niektóre tokeny są poważnymi projektami. USDC (USD Coin) to token reprezentujący jednego dolara, podparty (przynajmniej teoretycznie) jednym dolarem trzymanym w banku Circle Trust. UNI to token, który daje prawo głosu w decyzjach o protokole Uniswap. Wiele projektów infrastrukturalnych – Chainlink, MakerDAO, Aave – emituje swoje tokeny jako mechanizm zarządzania.

Inne tokeny są memcoinami albo gorszymi formami pomysłów: czyjąś próbą zarobienia szybkich pieniędzy, projekt na trzy strony PDF i tysiące tokenów wypuszczonych „z niczego". Większość tych projektów po roku okazuje się pustymi pojemnikami; ich tokeny tracą wartość do zera.

Dla zrozumienia afery Zondacrypto warto zapamiętać jeden fakt. Wiele giełd, w tym polska Zondacrypto, oferowała własne tokeny – jakieś ZBT, BNB, FTT – które klient mógł kupić, żeby uzyskać zniżki na opłatach albo udział w zyskach giełdy. Te tokeny żyły w kontraktach, do których klucze mają twórcy. Jeśli giełda upada, tokeny „zniżkowe" wydane przez nią znikają lub stają się niesprzedawalne. Tak właśnie było z FTT (token giełdy FTX) w listopadzie 2022. Tak właśnie jest teraz z Zondacrypto.

Klucze: u nas czy u kogoś

Centralne pojęcie, które trzeba zrozumieć przed rozmową o jakiejkolwiek giełdzie, to różnica między portfelem custodial a non-custodial. Słowo „custodial" pochodzi od angielskiego „custodian" – depozytariusz, ktoś, kto coś przechowuje dla nas. Portfel non-custodial – to portfel, w którym my sami trzymamy klucz prywatny.

Konto na giełdzie jest portfelem custodial. Klucze prywatne ma giełda. My mamy wpis w bazie giełdy mówiący, że nam się należy 0,01 BTC. Wygodne – można logować się hasłem, można zresetować dostęp, jeśli zapomnieliśmy hasła, można robić transakcje natychmiast. Niewygodne – pieniądze nie są nasze w sensie prawnym; są wierzytelnością wobec firmy.

Portfel non-custodial – na przykład aplikacja Electrum, BlueWallet albo urządzenie Ledger – działa odwrotnie. Klucze prywatne istnieją tylko u nas. Giełda nie wie nawet, że istniejemy. W zamian – jeśli zgubimy klucz, nasze monety przepadają na zawsze. Nie ma instancji, która mogłaby je odzyskać.

Hasło, którego warto nauczyć się na pamięć, brzmi: „Not your keys, not your coins" – jeśli klucze nie są twoje, monety nie są twoje. Jest to skrót, który w środowisku ludzi rozumiejących Bitcoina krąży od dekady i którego sens najlepiej się rozumie po doświadczeniu sytuacji takich jak afera Zondacrypto.

Co z tego wynika dla zwykłego klienta

Przypomnijmy zasadę: klucze nie twoje, monety nie twoje. Klient Zondacrypto, który trzymał na swoim koncie giełdowym 0,1 BTC – formalnie miał wierzytelność wobec spółki, której rezerwy bitcoinów (według analizy on-chain)

wynosiły mniej niż jeden bitcoin łącznie. Tysiące klientów oczekiwało wypłat, których nie było z czego realizować.

Innymi słowy: ten klient faktycznie nigdy nie miał swoich monet. Miał obietnicę. Obietnicy nie da się włożyć do portfela cyfrowego, nie da się wysłać innej osobie, nie da się sprzedać poza giełdą. Można tylko czekać, aż giełda zdecyduje się ją zrealizować – albo nie.

Stąd wynika praktyczne zalecenie, znane od czasów Mt. Gox: na giełdzie trzymaj tylko tyle, ile potrzebne jest do bieżącej wymiany. Jeśli kupiłeś 0,1 BTC i planujesz tę pozycję trzymać latami, wypłać te bitcoiny na własny portfel. Najlepiej hardware wallet (urządzenie pokroju Ledgera albo Trezora). Klucze prywatne wtedy są w fizycznym urządzeniu pod twoją kontrolą, a giełda nie ma już z nimi nic wspólnego.

Kosztem tej operacji jest opłata transakcyjna (przy obecnym kursie kilkadziesiąt złotych) i konieczność nauczenia się, jak hardware wallet obsługiwać. To nie jest zerowy próg, ale to jest jedyny sposób posiadania bitcoinów w sensie technicznym. Jeśli go nie przekroczysz, twoje bitcoiny są tylko obietnicą. A obietnice – jak pokazuje Zondacrypto – bywają niedotrzymywane.

Co zmienia (a czego nie zmienia) regulacja

W tle afery Zondacrypto toczy się polityczna walka o regulację rynku. Rzecz wymaga krótkiego wyjaśnienia.

Unia Europejska w grudniu 2024 roku wprowadziła rozporządzenie o nazwie MiCA – skrót od Markets in Crypto-Assets, czyli „Rynki kryptoaktywów". Jest to pierwszy w historii kompleksowy zestaw przepisów regulujący kryptowaluty na poziomie całej UE. Każda giełda działająca w Unii musi uzyskać licencję CASP (Crypto-Asset Service Provider – Dostawca Usług w Zakresie Kryptoaktywów), spełniać wymagania kapitałowe, prowadzić oddzielnie rezerwy klientów i własne, publikować audyty.

MiCA zaczęła obowiązywać w całej Unii 30 grudnia 2024 roku. Państwa członkowskie miały okres przejściowy do 1 lipca 2026 – do tej daty muszą wdrożyć ustawy szczegółowe i przyznać licencje. W Polsce ustawa o rynku kryptoaktywów jest blokowana – prezydent Karol Nawrocki zawetował dwie wersje rządowego projektu. Sejm w kwietniu 2026 nie odrzucił weta. W praktyce oznacza to, że Polska wchodzi w lipiec 2026 bez krajowej ustawy, co tworzy lukę, w której giełdy działające w Polsce de facto pozostają poza pełnym nadzorem.

Czy gdyby ustawa weszła w życie wcześniej, sprawa Zondacrypto miałaby inny przebieg? Trudno powiedzieć. Sławomir Mentzen z Konfederacji argumentował, że nawet uchwalona ustawa miała okres przejściowy do końca czerwca 2026 – czyli sytuacja Zondy byłaby ta sama. Krytycy odpowiadają, że samo istnienie aktywnego nadzoru KNF działa prewencyjnie. Spór toczy się nadal.

Kluczowa lekcja: regulacja nie jest panaceum. W krajach z najlepszą regulacją – USA, Wielka Brytania – też zdarzały się upadki dużych giełd. Co regulacja robi, to wprowadza standardy księgowe (giełda musi rozdzielać aktywa klientów od własnych), wymogi kapitałowe (musi mieć rezerwy), audyty zewnętrzne i ścieżkę roszczenia. Wszystko to obniża ryzyko, ale go nie eliminuje. Pomysł trzymania własnych kluczy nie znika.

* * *

W ostatniej, ósmej części cyklu zajmiemy się stroną najbardziej praktyczną: jak właściwie kupuje się bitcoiny krok po kroku, jak się nimi płaci, jak się je sprzedaje i wypłaca z powrotem na konto bankowe. Pokażemy, gdzie kończy się rola giełdy, a zaczyna prywatny portfel. I wrócimy ostatecznie do tytułowego pytania całego cyklu – szemrany epizod czy świetlana przyszłość?

Część 8. Jak się to robi w praktyce – i odpowiedź na tytułowe pytanie

Dotarliśmy do ostatniej części cyklu. Mamy za sobą siedem rozdziałów teorii, historii i ostrzeżeń. Pora na rozdział, który zaczyna się od pytania: dobrze, ale jak to się właściwie robi? Jak ja, zwykły Czytelnik z portfelem złotówek na koncie, mogę kupić bitcoiny, zapłacić nimi za coś, a potem zamienić z powrotem na pieniądze i wydać w sklepie? Pokażemy krok po kroku. A na końcu wrócimy ostatecznie do tytułowego pytania, postawionego w pierwszej części siedem numerów temu.

Krok pierwszy: kupowanie

Zacznijmy od najczęstszego scenariusza. Czytelnik chce kupić bitcoiny po raz pierwszy. Ma 1000 zł, którymi może swobodnie zarządzać, i chce zobaczyć, co się stanie.

Pierwsza decyzja: gdzie? Mamy trzy opcje. Pierwsza – giełda kryptowalut (Binance, Kraken, Coinbase, Zondacrypto przed kwietniem 2026). Druga – kantor kryptowalut, w tym te działające stacjonarnie, na przykład w centrach handlowych. Trzecia – bezpośrednio od kogoś znajomego, peer-to-peer.

Każda z tych dróg ma plusy i minusy. Giełda oferuje najlepszy kurs i pełną automatyzację, ale wymaga założenia konta i przejścia procesu identyfikacji. Kantor jest szybszy i prostszy, ale kurs jest wyraźnie gorszy (z marżą rzędu 3...5%). Transakcja peer-to-peer wymaga znajomego, który ma bitcoiny i chce je sprzedać. Dla nowicjusza zwykle wygrywa giełda.

Załóżmy więc, że wybieramy giełdę. W ostatnich miesiącach, po aferze Zondacrypto, polscy klienci raczej kierują się ku giełdom międzynarodowym z silniejszym nadzorem – Kraken (USA), Bitstamp (Wielka Brytania), Binance (regulowana przez różne organy europejskie). Procedura na każdej z nich wygląda podobnie i przebiega w czterech etapach.

Etap pierwszy to założenie konta. Email, hasło, kod weryfikacyjny. Ta część zajmuje pięć minut.

Etap drugi nazywa się KYC – *Know Your Customer*, czyli „poznaj swojego klienta". Polega na wgraniu zdjęcia dokumentu tożsamości (dowód osobisty albo paszport) i selfie z dokumentem. Algorytm porównuje twarz na selfie z twarzą na dokumencie. Człowiek przegląda wątpliwe przypadki. Procedura wynika z przepisów o przeciwdziałaniu praniu pieniędzy (AML

Jak kupić bitcoiny krok po kroku

cztery etapy przez giełdę kryptowalut

Scenariusz: mam 1000 zł na koncie bankowym, chcę kupić bitcoiny.
Łączny czas: ~2 godziny (głównie weryfikacja). Koszt: ~10-20 zł prowizji.

1 ZAŁOŻENIE KONTA — *5 minut*

Email, hasło, kod weryfikacyjny SMS.

Wybierz giełdę z licencją: Kraken, Bitstamp, Binance.

↓

2 KYC – IDENTYFIKACJA — *od 5 minut do 2 dni*

Zdjęcie dowodu + selfie z dokumentem.

Wymóg AML. Giełda musi wiedzieć kim jesteś.

↓

3 DEPOZYT ZŁOTÓWEK — *kilkanaście minut*

Przelew bankowy na rachunek giełdy.

Pieniądze trafiają na konto giełdowe (już nie u Ciebie).

↓

4 ZAKUP BITCOINÓW — *1 sekunda*

Klik kup BTC, zlecenie rynkowe, gotowe.

Saldo BTC w koncie giełdowym. Prowizja 0,1-0,5%.

UWAGA – co zrobić DALEJ

Bitcoiny są teraz na KONCIE GIEŁDOWYM (custodial).
Klucze prywatne ma giełda, nie Ty. Wpis w bazie giełdy = wierzytelność wobec firmy.
Jeśli planujesz trzymać dłużej niż kilka tygodni – przenieś na własny portfel.
Najlepiej hardware wallet: Ledger, Trezor, BitBox (200...600 zł).
Lekcja z Zondacrypto: bitcoiny na giełdzie mogą zniknąć z dnia na dzień.

Rysunek 1. Cztery etapy zakupu bitcoinów przez giełdę. Pełna ścieżka od złotówek na koncie bankowym do bitcoinów na koncie giełdowym

– *Anti-Money Laundering*) i jest obowiązkowa na każdej legalnie działającej giełdzie. Może zająć od kilku minut do dwóch dni. Po przejściu KYC giełda wie, kim jesteśmy, i zna nasze konto bankowe.

Etap trzeci to depozyt. Z aplikacji bankowej robimy zwykły przelew na rachunek giełdy, podając w tytule numer naszego konta giełdowego (giełda go wyświetli). Po kilkunastu minutach lub kilku godzinach złotówki pojawią się na koncie giełdowym. W tym momencie, formalnie, te pieniądze już nie są nasze – są wierzytelnością wobec firmy (patrz Część 7). Ale póki giełda działa, można nimi dysponować jak własnymi.

Etap czwarty to sam zakup. Wybieramy kryptowalutę (BTC), wpisujemy kwotę albo liczbę monet i wybieramy typ zlecenia. Najprostszy typ – zlecenie rynkowe (*market order*) – kupuje natychmiast po obecnym kursie. Drugi – zlecenie z limitem (*limit order*) – czeka, aż kurs spadnie do żądanej wartości. Dla pierwszego zakupu wystarczy zlecenie rynkowe. Klikamy „kup" – i po sekundzie mamy w portfelu giełdowym jakąś tam część bitcoina.

Tyle zakup. Czas: jakieś dwie godziny przy pierwszym razie (głównie KYC). Koszt: prowizja giełdy (zwykle 0,1...0,5%) plus ewentualnie spread (różnica między ceną kupna i sprzedaży). Razem przy 1000 zł wpłaty około 10...20 zł kosztu.

Krok drugi: przechowywanie

Tu zaczyna się ważny rozdział. W Części 7 wyłożyliśmy zasadę „not your keys, not your coins". Tu pora ją zrealizować.

Jeśli planujemy kupione bitcoiny szybko sprzedać – w ciągu dni albo tygodni – można zostawić je na giełdzie. Ryzyko bankructwa giełdy w tym czasie jest niewielkie (choć nie zerowe – Zondacrypto upadała w kilka tygodni). Jeśli jednak planujemy trzymać dłużej – przez miesiące albo lata – należy przenieść je na własny portfel.

Mamy do wyboru trzy typy portfeli. Portfel oprogramowany (*software wallet*) to aplikacja na telefonie albo komputerze, na przykład Electrum, BlueWallet, Phoenix. Generuje i przechowuje klucze prywatne lokalnie na urządzeniu. Wygodne, darmowe. Słabe: jeśli ktoś włamie się do telefonu albo zaszyfruje dysk złośliwym oprogramowaniem, klucze mogą wyciec.

Portfel sprzętowy (*hardware wallet*) – najlepsza opcja dla osób, które chcą trzymać większe kwoty. Ledger, Trezor, BitBox, ColdCard

– to małe urządzenia podobne do pendrive'ów. Klucze prywatne nigdy ich nie opuszczają. Nawet podłączone do zarażonego komputera urządzenie wymaga fizycznego zatwierdzenia każdej transakcji przyciskiem. Koszt: 200...600 zł za urządzenie.

Portfel papierowy (*paper wallet*) – wydrukowany na papierze kod QR z kluczem prywatnym. Najprostszy i najtańszy, ale wymaga absolutnej dyscypliny w przechowywaniu (pożar, woda, zgubienie) i jest niewygodny w użyciu. Dla większości czytelników to przesada – hardware wallet jest wystarczająco bezpieczny i znacznie wygodniejszy.

Niezależnie od wyboru, przy konfiguracji portfela dostaniemy tak zwany seed phrase – sekwencję 12 albo 24 słów po angielsku. Jest to czytelna dla człowieka wersja klucza prywatnego, z której da się odtworzyć cały portfel, gdyby coś się stało z urządzeniem. Seed phrase trzeba zapisać na papierze (najlepiej w dwóch kopiach, w dwóch różnych miejscach) i ukryć. Nigdy nie wpisywać do komputera, nie fotografować, nie wysyłać. Strata seed phrase jest stratą wszystkich monet – i nikt nie może ich odzyskać. Kradzież seed phrase też jest stratą wszystkich monet – kradnący po prostu odtworzy portfel u siebie.

Krok trzeci: płatność bitcoinami

Mamy bitcoiny w portfelu. Chcemy nimi zapłacić. Komu? Tu napotykamy pierwszy problem praktyczny – choć teoretycznie bitcoinami można zapłacić w wielu miejscach, w Polsce w 2026 roku akceptują je niemal wyłącznie sklepy

12 SŁÓW WARTYCH FORTUNĘ

Typowy seed phrase wygląda tak:

```
witch collapse practice feed shame open
despair creek road again ice least
```

Te dwanaście słów to wszystko, czego trzeba do odtworzenia całego portfela. Standard BIP-39, używany przez 99% portfeli, definiuje słownik 2048 angielskich słów, z których można wybrać dwanaście. To daje 2^{132} możliwych kombinacji – liczbę porównywalną z całkowitą liczbą operacji do złamania klucza 132-bitowego. W praktyce – niezgadywalne.

Sześć rzeczy, których nigdy nie wolno zrobić z seed phrase:

1. Zapisać w pliku na komputerze.
2. Sfotografować telefonem.
3. Wysłać sobie mailem.
4. Zachować w menedżerze haseł w chmurze.
5. Wpisać na stronie WWW.
6. Powiedzieć komukolwiek przez telefon, choćby pracownikowi giełdy.

Co robić: zapisać ręcznie na papierze (lub stalowej płytce – są takie specjalne), schować w dwóch różnych miejscach. Jedna kopia w domu, druga u rodziców albo w skrytce bankowej. Nigdy razem.

internetowe specjalizujące się w technologiach (sprzęt komputerowy, oprogramowanie, VPN-y), niektóre kantory wymiany walut online, oraz pojedyncze restauracje i hotele. W codziennych zakupach – w Biedronce, w lekarza, na poczcie – bitcoinem zapłacić się nie da. To podstawowy fakt o roli Bitcoina w 2026 roku.

Załóżmy jednak, że Czytelnik znalazł sklep, który akceptuje BTC. W praktyce wygląda to tak. Na stronie sklepu pojawia się kod QR – czarno-biały kwadrat – oraz długi ciąg znaków zaczynający się zwykle od „bc1" albo „1". To jest adres bitcoinowy odbiorcy (sklepu), do którego ma trafić nasza zapłata. Obok widnieje kwota w BTC (np. 0,00125 BTC) i czas, w którym kurs jest ważny (zwykle 10...15 minut).

Otwieramy aplikację portfela na telefonie. Wybieramy „wyślij". Skanujemy kod QR – aplikacja sama wczyta adres i kwotę. Sprawdzamy, czy wszystko zgadza się z tym, co widzimy na ekranie sklepu. Wybieramy poziom opłaty transakcyjnej.

Tu zatrzymajmy się chwilę. Opłatę określa się zwykle w jednostce „sat/vB" – satoshi za wirtualny bajt rozmiaru transakcji. Wysokie opłaty (50...100 sat/vB) gwarantują potwierdzenie w następnym bloku, czyli średnio za 10 minut. Niskie (1...5 sat/vB) oznaczają, że transakcja może czekać godziny lub dnie. W praktyce, w 2026 roku, typowa opłata za szybką transakcję to kilkadziesiąt złotych w przeliczeniu. Aplikacja portfela podpowiada „rekomendowany" poziom na podstawie aktualnej sieci.

Klikamy „potwierdź". Transakcja jest podpisana naszym kluczem prywatnym (proces opisany w Części 3) i wysłana do sieci. Pojawia się w mempoolu – kolejce oczekujących na włączenie do bloku. Po średnio 10 minutach pojawia się w bloku i ma jedno potwierdzenie. Po godzinie – sześć potwierdzeń, co tradycyjnie uznaje się za moment, w którym transakcja jest „ostatecznie" zaakceptowana. Sklep zwykle uznaje płatność już po jednym potwierdzeniu (przy małych kwotach) lub po sześciu (przy dużych).

Dla codziennego użycia jest jednak alternatywa, o której warto wiedzieć: Lightning Network. Jest to druga warstwa systemu Bitcoina, w której transakcje wykonywane są niemal natychmiast (sekundy) i z opłatami groszowymi. Pewne sklepy preferują płatność przez Lightning właśnie z tego powodu. Dla zrozumienia, jak Lightning działa, należałoby napisać oddzielny artykuł – ale praktycznie, jeśli sklep oferuje QR Lightning, używa się go tak samo jak normalnego: skanujemy, klikamy, gotowe.

Krok czwarty: sprzedaż i powrót do złotówek

Załóżmy teraz, że minęło dwa lata. Kurs wzrósł. Czytelnik chce sprzedać część swoich bitcoinów i zamienić je na złotówki, którymi zapłaci za remont mieszkania.

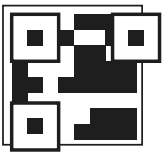
Droga jest dokładnie odwrotna do drogi zakupu. Najpierw przesyłamy bitcoiny z naszego portfela na konto giełdowe. To jest osobna transakcja w sieci

Płatność bitcoinami

od kodu QR sklepu do potwierdzenia w łańcuchu bloków

ETAP 1 – SKLEP

EKRAN PŁATNOŚCI



SKLEP XYZ
Kwota:
`0,00125 BTC`
Adres:
`bc1q...zk4n`
ważny 12 min

Sklep generuje QR + adres + kwota

ETAP 2 – KLIENT

APLIKACJA PORTFELA

1. Otwieram aplikację (Electrum, BlueWallet, ledger Live...)

2. Klikam „Wyślij"/„Send"

3. Skanuję QR ze sklepu – aplikacja wczyta adres i kwotę.

Sprawdzam, że dane się zgadzają!

ETAP 3 – WYBÓR OPŁATY I PODPIS

Aplikacja proponuje 3 poziomy opłaty:

SZYBKO (~10 min)	ŚREDNIO (~30 min)	WOLNO (~kilka h)
~50 sat/vB · ~15 zł	~20 sat/vB · ~6 zł	~3 sat/vB · ~1 zł

Wybieram poziom → klikam „Potwierdź" → aplikacja podpisuje moim kluczem prywatnym.
Klucz prywatny nie opuszcza urządzenia (w hardware wallet – fizyczny przycisk).

ETAP 4 – SIEĆ ROBI SWOJE

→ Transakcja idzie do mempoolu (kolejki sieci)
aplikacja sklepu może już widzieć transakcję jako „oczekującą"

↓

→ Po ~10 minutach: górnik włącza do bloku
jedno potwierdzenie — przy małych kwotach wystarczy

↓

→ Po ~godzinie: sześć potwierdzeń
transakcja ostatecznie zaakceptowana, sklep wysyła towar
(do każdego kolejnego bloku potrzeba kolejnych 10 minut)

DLACZEGO TO TAKIE WOLNE?

10 minut na blok to świadomy parametr (patrz Część 5 – proof of work).
Wymiana 10 zł za ciastko nadaje się tu źle. To system dla większych przelewów.

Dla codziennych płatności: Lightning Network
Druga warstwa Bitcoina. Transakcje w sekundach, opłaty groszowe.
Działa „obok" głównego łańcucha; rozliczenie odbywa się dopiero przy zamknięciu.

Jeśli sklep oferuje QR Lightning – używa się go tak samo jak normalnego BTC.

Rysunek 2. Płatność bitcoinami krok po kroku. Od kodu QR sklepu, przez podpis aplikacji portfela, do potwierdzenia w bloku

Bitcoina – z opłatą i czasem oczekiwania. Otwieramy giełdę, wchodzimy do sekcji „depozyt BTC", giełda pokazuje nasz indywidualny adres bitcoinowy w jej systemie. Z aplikacji portfela wykonujemy przelew na ten adres. Po sześciu potwierdzeniach (godzina) giełda zaksięguje pieniądze.

Drugi krok: sprzedajemy bitcoiny za złotówki w księdze zleceń giełdy. Klikamy „sprzedaj", wybieramy zlecenie rynkowe, wpisujemy ilość. Po sekundzie BTC znika, w jego miejscu pojawia się odpowiednia liczba złotówek (po kursie pomniejszonym o prowizję).

Trzeci krok: wypłata na konto bankowe. Z konta giełdowego zlecamy przelew na nasze konto w polskim banku. Tutaj giełda zwykle przeprowadza dodatkowe kontrole – zwłaszcza przy większych kwotach. Może poprosić o wyjaśnienie pochodzenia środków (zgodnie z przepisami AML). Sam przelew, gdy zostanie zatwierdzony, dociera do banku w ciągu kilku godzin do dwóch dni roboczych.

Tu pojawia się kolejna nieoczywista kwestia: w 2026 roku banki w Polsce z różną przychylnością traktują przelewy z giełd kryptowalut. Niektóre (Revolut, mBank, ING) zwykle nie robią problemów. Inne mogą zablokować przelew i zażądać wyjaśnień. W skrajnych przypadkach – zamknąć konto. Z tego powodu warto, jeszcze przed wpłatą złotówek na giełdę, sprawdzić zasady własnego banku.

Krok piąty: podatek

I tu Czytelnik napotyka stronę, o której zwolennicy bitcoina rzadko mówią wprost: skarbówkę.

W Polsce dochód z odpłatnego zbycia kryptowalut podlega podatkowi 19% od dochodu (przychód minus koszty). Stawka jest stała i nie zależy od wysokości dochodu – to ta sama stawka, którą stosujemy do zysków giełdowych. Rozliczamy go w formularzu PIT-38, sekcja „Odpłatne zbycie walut wirtualnych". Termin: do 30 kwietnia roku następnego.

Kilka praktycznych zasad, które warto zapamiętać. Po pierwsze, sam zakup bitcoinów nie generuje podatku – dopiero ich sprzedaż albo wymiana na coś materialnego (zapłata za laptopa) generuje przychód. Po drugie, wymiana kryptowaluta-kryptowaluta (np. BTC na ETH) jest w Polsce neutralna podatkowo. Po trzecie, stratę z kryptowalut można rozliczyć tylko z innymi przychodami z kryptowalut, nie z innymi inwestycjami.

Najważniejsza zmiana w 2026 roku: dyrektywa unijna DAC8 weszła w życie 1 stycznia. Nakłada na licencjonowane giełdy (CASP) obowiązek raportowania transakcji rezydentów podatkowych do organów skarbowych. Innymi słowy: skarbówka od 2026 roku automatycznie wie, kto na jakiej giełdzie ile kupił i sprzedał. Mit anonimowości bitcoina na giełdach scentralizowanych właśnie się skończył. Niezgłoszenie dochodów oznacza zaległość plus odsetki plus możliwe kary.

To dobre miejsce na uwagę: jeśli planujesz większe operacje, warto poradzić się księgowego znającego specyfikę kryptowalut. Nie dlatego, że materia jest trudna – bo nie jest – ale dlatego, że zaniedbanie podatków przy kwotach kilkudziesięciu tysięcy złotych związane jest następnie z bardzo nieprzyjemnymi odsetkami.

Szemrany epizod czy świetlana przyszłość?

Dotarliśmy do końca. Czytelnik wie, co to jest funkcja skrótu, jak działa kryptografia klucza publicznego, jak budowany jest łańcuch bloków, jak górnicy zgadują nonce, jak wyglądały krachy ostatnich lat, jak działają giełdy i jak wygląda praktyka kupowania i wydawania bitcoinów. Pora odpowiedzieć na pytanie postawione na początku.

Czytelnik zauważył pewnie, że tytuł cyklu jest postawiony jako pytanie alternatywne – albo albo. To jest skrót myślowy. W rzeczywistości obie odpowiedzi mogą być w pewnym sensie prawdziwe – ale „szemrana" strona ma kilka wymiarów, z których nie wszystkie są tak oczywiste, jak krach giełdowy.

Świetlana – w jednym wymiarze. Bitcoin udowodnił, że pewne rzeczy uważane przed 2008 rokiem za niemożliwe są możliwe. Pieniądz bez banku centralnego, działający globalnie, bez interwencji państwowej, weryfikowalny przez każdego, kto potrafi obsługiwać komputer. Szesnaście lat działania, zerowa skuteczna awaria protokołu, kapitalizacja porównywalna z PKB Australii. To są fakty, których nikt nie unieważni, niezależnie od tego, co stanie się z kursem. Idee z whitepaper'a Satoshiego – funkcja skrótu jako odcisk palca, klucz publiczny jako tożsamość, łańcuch bloków jako pamięć rozproszona – przeszły już do podręczników informatyki i będą tam używane jeszcze długo po tym, jak konkretne kryptowaluty znikną.

Szemrana – w wymiarze pierwszym, najbardziej widocznym. Wokół tej technologii narósł świat finansowy o regułach z połowy XIX wieku. Giełdy bez licencji, tokeny bez pokrycia, marketing z udziałem celebrytów, krachy raz na trzy lata. Mt. Gox 2014, Terra/Luna 2022, FTX 2022, Zondacrypto 2026 – to nie są wyjątki, to jest wzorzec. Ludzie tracą oszczędności, prokuratorzy wszczynają śledztwa, regulatorzy gonią cienie. To jest ta strona, którą widać w gazetach. Ale jest też druga, mniej widoczna w prasie ekonomicznej – i to jest, w istocie, sedno słowa „szemrana" w tytule tego cyklu.

Druga twarz kryptowalut: pieniądz świata szemranego

Wracamy do założeń Satoshiego z 2008 roku. Bitcoin miał być pieniądzem, który pozwala przesłać dowolną kwotę dowolnej osobie na świecie, bez pośredników, bez pytania nikogo o zgodę. To była wizja libertariańska – wolny pieniądz dla wolnych ludzi. Tyle, że ta sama cecha – możliwość przesłania pieniędzy bez zgody państwa – przydaje się również tym, którym państwo zabrania pewnych rzeczy z dobrego powodu.

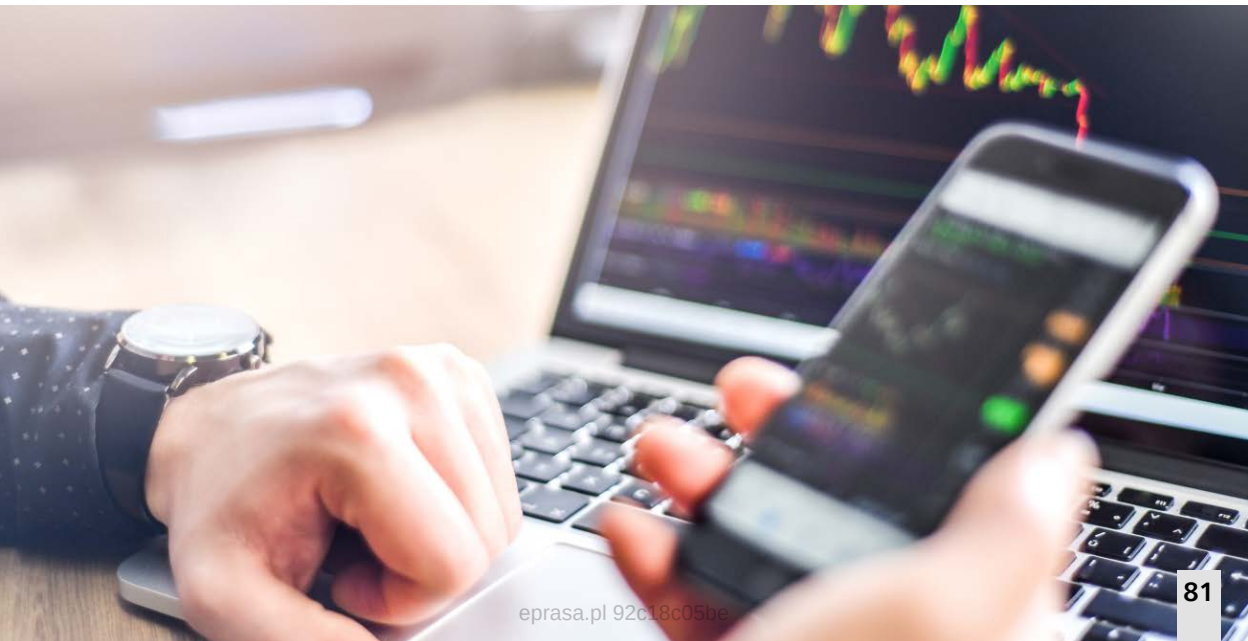
Konkretne liczby. Według raportu Chainalysis 2026 Crypto Crime Report – firmy, która analizuje publiczne łańcuchy bloków pod kątem śledztw – adresy zidentyfikowane jako nielegalne otrzymały w 2025 roku co najmniej 154 miliardy dolarów. To wzrost o 162% rok do roku. Łączny udział nielegalnych transakcji w całym wolumenie krypto pozostaje poniżej 1% – ale 1% z czegoś olbrzymiego to jest właśnie 154 miliardy. Co istotne, 84% tego nielegalnego wolumenu nie idzie już w bitcoinach. Idzie w stablecoinach – głównie w Tetherze.

Z czego się to składa? Po pierwsze, klasyczne czarne rynki. Darknet markets – strony w sieci Tor, na których kupić można narkotyki, broń, skradzione dane kart kredytowych – w 2025 roku przyjęły wpłaty rzędu 2,6 miliarda dolarów. Ransomware – ataki polegające na zaszyfrowaniu cudzych komputerów i żądaniu okupu – to drugi duży obszar; Bitcoin pozostaje tu wciąż główną walutą, bo łatwo go odebrać i nie da się go odzyskać. Hakerzy z Korei Północnej, działający na zlecenie reżimu, ukradli z giełd krypto w 2025 roku co najmniej dwa miliardy dolarów; pieniądze te finansują północnokoreański program rakietowy. Organizacje takie jak Hamas czy libański Hezbollah od lat zbierają fundusze przez krypto.

Po drugie – i to jest nowy rozdział, otwarty dosłownie w ostatnich miesiącach – kryptowaluty stały się oficjalnym narzędziem ucieczki przed sankcjami. Głównym graczem jest tutaj Rosja.

Państwo-pariasem na blockchainie: przypadek Rosji

Po inwazji na Ukrainę w lutym 2022 roku Rosja została odcięta od systemu SWIFT, dolarowych rozliczeń międzybankowych i większości zachodnich rynków finansowych. Przez dwa lata Kreml próbował obejść te ograniczenia tradycyjnymi metodami – pośrednictwem firm w Dubaju, Kirgistanie, Indiach. To działało,



ale powoli i drogo. W lipcu 2024 roku rosyjska Duma uchwaliła ustawę dopuszczającą wprost użycie kryptowalut w rozliczeniach międzynarodowych. Trzy miesiące później sankcjonowany przez Zachód rosyjski bank wojskowy Promsvyazbank uruchomił firmę o nazwie A7.

A7 to coś w rodzaju państwowego pośrednika płatniczego. Pozwala rosyjskim firmom płacić zagranicznym dostawcom – głównie chińskim – w obejściu sankcji. 78% płatności A7 idzie do Chin. Mechanizm: rosyjski importer wpłaca ruble do A7, A7 emituje token o nazwie A7A5 – cyfrowy odpowiednik rubla, podparty depozytami w Promsvyazbanku – i przesyła go na konto chińskiego dostawcy. Dostawca może go natychmiast wymienić na dolary, euro albo juany na zaprzyjaźnionej giełdzie. W ten sposób pieniądze przekraczają granicę, ale nie przez bank w sensie zachodnim – przez łańcuch bloków, na który sankcje nie mają bezpośredniego wpływu.

We wrześniu 2025 roku Władimir Putin osobiście, w transmisji wideo, otworzył nową filię A7 we Władywostoku. Sygnał był jasny: to nie jest pomysł kilku biznesmenów; to jest oficjalna polityka państwowa. Tego samego miesiąca A7A5 został oficjalnie uznany za pierwszy rosyjski cyfrowy aktyw finansowy dopuszczony do handlu zagranicznego. Według raportu Chainalysis A7A5 w pierwszym roku swojego istnienia przepuścił transakcje na łączną kwotę 93,3 miliarda dolarów. To kwota większa niż roczny PKB Bułgarii.

To nie jest jedyny mechanizm. W marcu 2025 roku amerykański Departament Skarbu nałożył sankcje na giełdę Garantex – rosyjską platformę używaną do prania pieniędzy i obchodzenia sankcji – i zamroził 26 milionów dolarów. Garantex zniknął, ale w sierpniu 2025 jego dotychczasowi operatorzy uruchomili nową giełdę pod nazwą Grinex. Klienci Garantexa, którzy stracili dostęp do swoich kont, otrzymali jako rekompensatę tokeny A7A5. To pokazuje, jak ściśle te elementy są ze sobą powiązane: sankcjonowany bank → emituje token → giełda pomaga prać pieniądze → klient straconej giełdy dostaje token rekompensaty.

Trzeci kanał – najmniej spektakularny, ale chyba najpojemniejszy – to po prostu Tether. Ten sam Tether, którego używa argentyński drobny przedsiębiorca, żeby uciec przed inflacją peso, używa też rosyjski pośrednik, żeby zapłacić chińskiej fabryce za części do dronów. Konkretny przykład udokumentowany przez „Wall Street Journal": Andriej Zwieriew, rosyjski „smuggler" działający z Hongkongu, pod koniec 2022 roku użył Tethera do przelania kilku milionów dolarów na konto dostawcy elektroniki w Hongkongu. Zamówienie złożył dla rosyjskiego koncernu zbrojeniowego Kałasznikow – części trafiały do produkcji dronów używanych w wojnie z Ukrainą.

Paradoks anarchii: krypto nie jest tak wolne, jak się wydaje

Tu trzeba postawić jedno ważne zastrzeżenie. Krypto nie jest jednolicie „wolne" – różne kryptowaluty mają różny stopień podatności na kontrolę. Stablecoiny takie jak Tether (USDT) czy USDC są emitowane przez konkretne firmy, które technicznie mogą zamrozić dowolny adres. I robią to. Tether w 2024 i 2025 roku zamroził dziesiątki adresów powiązanych z Hamasem, Hezbollahem, oszustami z południowo-wschodniej Azji oraz, na wniosek ukraińskich służb, niektóre adresy rosyjskie. Z punktu widzenia organów ścigania stablecoin jest *bardziej* podatny na sankcje niż klasyczny bank – bo wystarczy jedna decyzja techniczna emitenta, a środki znikają.

Z Bitcoinem jest inaczej. Bitcoin nie ma emitenta. Nie ma firmy, której można nakazać zamrożenie adresu. Sankcje na konkretne adresy bitcoinowe istnieją – amerykański OFAC publikuje listy – ale ich egzekucja sprowadza się do tego, że żadna licencjonowana giełda nie przyjmie pieniędzy z takiego adresu. Same monety w sieci żyją dalej, można je przesłać peer-to-peer, mogą trafić na giełdę w kraju niesojuszniczym i tam zostać wymienione. Sankcje przesuwają punkt egzekucji od warstwy protokołu do warstwy fiat-on-ramp, ale jej całkowicie nie likwidują.

Stąd paradoks: krypto jest *dostatecznie* wolne, żeby budować na nim infrastrukturę obchodzenia sankcji, ale *niedostatecznie* wolne, żeby uchronić każdą transakcję. Rosja zbudowała własną infrastrukturę (A7, Grinex, ruble-backed token), bo zrozumiała, że poleganie na infrastrukturze zachodniej (Tether, Binance, OFAC-lista) jest ryzykowne. To jest scenariusz, którego twórcy Bitcoina prawdopodobnie nie przewidywali w 2008 roku: nie tylko jednostki, ale także państwa-pariasy mogą skorzystać z technologii, którą wymyślono jako antytezę państwa.

Odpowiedź

Bo – i to jest najtrudniejsza część odpowiedzi – większość ludzi nie używa Bitcoina w sposób, do którego został zaprojektowany. Bitcoin powstał, żeby uniezależnić od banków. A statystycznie 95% jego posiadaczy trzyma go na giełdach – czyli niemal jak konto bankowe, tylko bez ubezpieczenia. Bitcoin powstał, żeby służył jako pieniądz wymiany. A statystycznie służy jako instrument spekulacyjny i – w specyficznym sektorze – jako waluta przestępczości i sankcji. Bitcoin powstał, żeby uniknąć pośredników. A przede wszystkim zarabiają pośrednicy.

To nie znaczy, że pomysł Satoshiego się nie sprawdza. Sprawdza się – ale w taki sposób, jaki rzadko pojawia się w broszurach reklamowych. Sprawdza się dla Argentyńczyka, który chowa oszczędności przed inflacją; dla Wenezuelczyka, który dostaje pensję z zagranicy; dla dysydenta, którego konto zostało zablokowane przez reżim. Sprawdza się też dla rosyjskiego importera, który płaci za chińskie tranzystory do dronów; dla operatora ransomware, który wyłudza okupy ze szpitali; dla siatki Korei Północnej, która kradnie z giełd dwa miliardy rocznie. Ta sama technologia, te same właściwości, kompletnie różne zastosowania. Bitcoin jest neutralny w sensie ściśle technicznym – jest po prostu narzędziem. Ale to neutralne narzędzie ma cechy, które ułatwiają niektóre rzeczy bardziej niż inne, a te niektóre rzeczy nie zawsze są tymi, którymi szczyciłby się Satoshi.

Co istotne, regulacja tego nie naprawi – przynajmniej nie w prosty sposób. MiCA, DAC8, GENIUS Act w USA, KYC, sankcje OFAC: wszystko to próbuje wbudować punkty kontroli w warstwę dostawców usług (CASP). Te punkty działają wewnątrz Zachodu. Poza Zachodem, jak pokazuje przypadek A7A5, państwa-pariasy budują własną równoległą infrastrukturę. To nie jest problem do rozwiązania regulacją – bo regulacja, do której nie chce się zastosować jeden z głównych aktorów, przestaje być regulacją, staje się tylko zwiększeniem kosztów transakcji.

Prognoza na dwadzieścia lat, której nikt nie wymaga, ale którą podzielę się, bo to ostatnia okazja w tym cyklu: Bitcoin nie zniknie. Pozostanie z nami jako klasa aktywów – analogicznie do złota. Jego udział w portfelach inwestorów stopniowo wzrośnie do może 1...3%. Większość alternatywnych kryptowalut zniknie. Stablecoiny zostaną i będą w niektórych krajach

standardową infrastrukturą płatności międzynarodowych – także tych mniej legalnych. Smart kontrakty Ethereum znajdą zastosowanie w niszach. Regulacje stopniowo wyeliminują najgorszych aktorów w krajach demokratycznych – czytaj: kolejnych Zondacrypto. Ale spekulacja, oszustwa i krachy nie znikną w obrębie własnych jurysdykcji; nie znikną też transakcje sankcji-obchodzące i przestępcze poza zasięgiem jurysdykcji zachodnich. To nie są problemy technologiczne – to są problemy ludzkie i geopolityczne, które będą póki ludzie i geopolityka.

Świetlana technologia. Szemrana praktyka. Szemrana też geopolityka. Wszystko razem. Tytuł tego cyklu zadawał pytanie alternatywne. Odpowiedź jest taka, że nie zawsze trzeba wybierać – a czasem nawet nie można.

* * *

Dziękuję Czytelnikowi za osiem części wytrwałości. To była długa wycieczka – od starożytnego problemu generałów aż po praktyczny instruktaż obsługi portfela bitcoinowego. Kryptowaluty są tematem, w którym łatwo o emocje i trudno o spokój. Mam nadzieję, że ten cykl pomógł trochę ten spokój znaleźć. ■

Paul Bavarian

O Autorze
Paul Bavarian jest wnukiem mojego bułgarskiego przyjaciela z czasów studenckich w Politechnice Kijowskiej. Pasjonują go nowe technologie, które obserwuje z perspektywy kalifornijskiej. The last but not least – odziedziczył po swoim dziadku fascynację Polską.

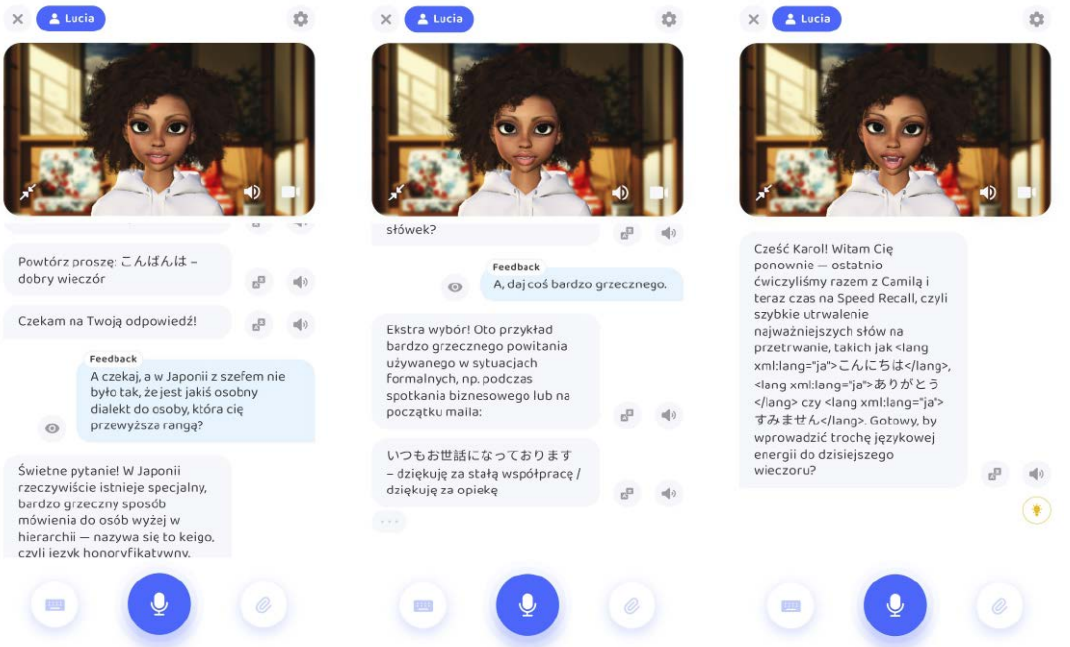
Prof. Wiesław Marciniak

Nauka języków z czatbotem (2)

W poprzedniej części publikacji (luty 2026) skupiliśmy się na możliwościach, jakie niosą ze sobą chatboty w roli nauczycieli języków obcych – nieograniczonej dostępności, niskim koszcie oraz daleko posuniętej personalizacji procesu nauki. Jednak atrakcyjna forma i przyjazny interfejs nie zawsze idą w parze z realną skutecznością dydaktyczną. W drugiej części przyjrzymy się więc temu, jak aplikacja Praktika radzi sobie w codziennym użytkowaniu, gdzie kończą się jej możliwości oraz jakie problemy wynikają z obecnego poziomu technologii rozpoznawania mowy i generowania języka. Omówimy zarówno mocne strony rozwiązania – takie jak adaptacja do użytkownika i budowanie zaangażowania – jak i istotne wady, które sprawiają, że wirtualny korepetytor pozostaje raczej na dzień dzisiejszy narzędziem wspomagającym niż pełnoprawnym nauczycielem.

Silne i słabe strony aplikacji

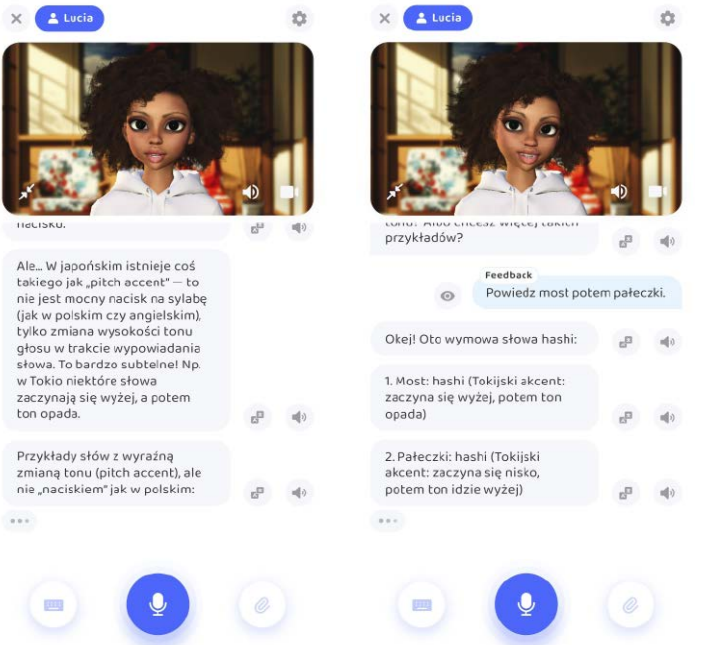
Cała nauka w aplikacji Praktika sprowadza się obecnie do okienka czatu. Mimo iż są one wzbogacone wieloma funkcjami, myślę, że bardziej tradycyjne ćwiczenia takie jak dopasowywanie słówek czy wybór kilku odpowiedzi, mógłby urozmaicić aplikacje. Wprawdzie awatar próbował od czasu do czasu zadać pytanie A, B lub C, jednak model językowy nie radzi sobie dobrze z losowością, dlatego poprawną odpowiedzią zawsze było A. Mimo tej wady, wirtualny nauczyciel



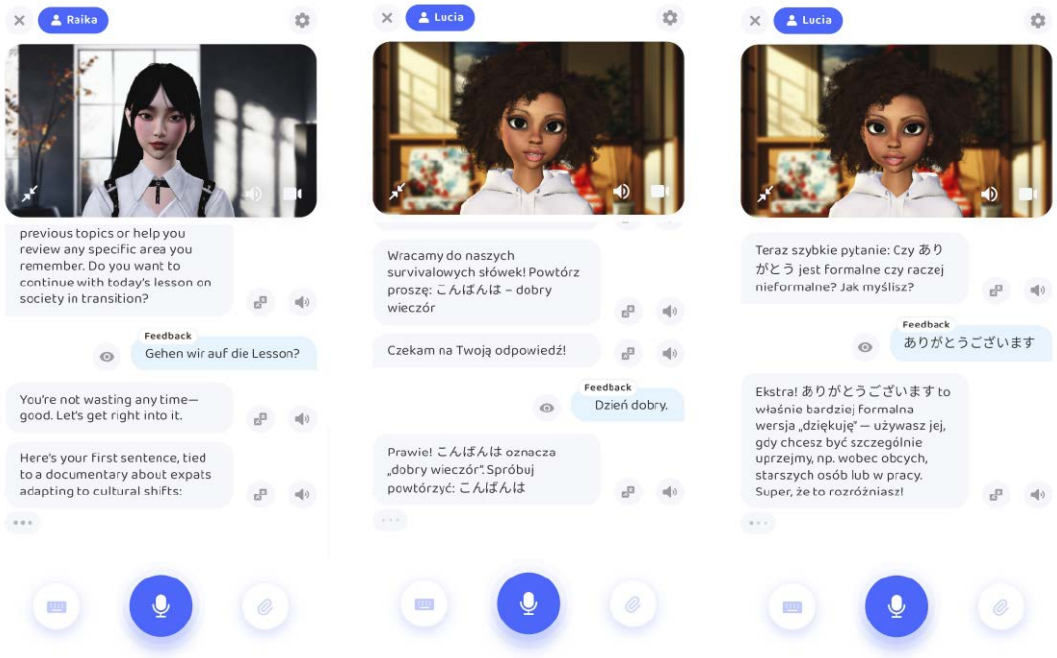
Awatar na bieżąco dostosowuje przebieg lekcji do użytkownika, jednak nie jest wolny od pomyłek

dobrze dostosowuje się do ucznia. Kiedy uczyliśmy się popularnych zwrotów, poprosiłem o zmianę formy lekcji na bardziej oficjalną. Nauczyciel dostosował się i zaczął podawać dopasowane sformułowania, jednocześnie opisując ich funkcję w odpowiednich kontekstach.

Najpoważniejszą wadą aplikacji są trudności z rejestracją i generowaniem dźwięku. Mówiąc najprościej, nie istnieją jeszcze komercyjne modele uczenia maszynowego, które potrafią rozumieć fonetykę, akcent, intonację i tempo. Wirtualny nauczyciel posiada piękny lecz monotonny akcent, zależny od wybranego języka i awatara. Jednak jego wymowa jest głucha na kontekst. Japoński wyraz hashi (橋) może oznaczać kilka różnych rzeczy w zależności od wymowy. Nauczyciel zawsze wymawia słowo w ten sam sposób – chcąc powiedzieć „most” (橋), wypowie więc „pałeczki” (箸). Rejestracja wymowy użytkownika jest jeszcze gorsza. Wypowiedź użytkownika jest przetwarzana przez agenta AI, który



Nauczyciel kompetentnie przeprowadził mnie przez niuanse fonetyczne języka japońskiego. Następnie... wymówił wyraz niepoprawnie!



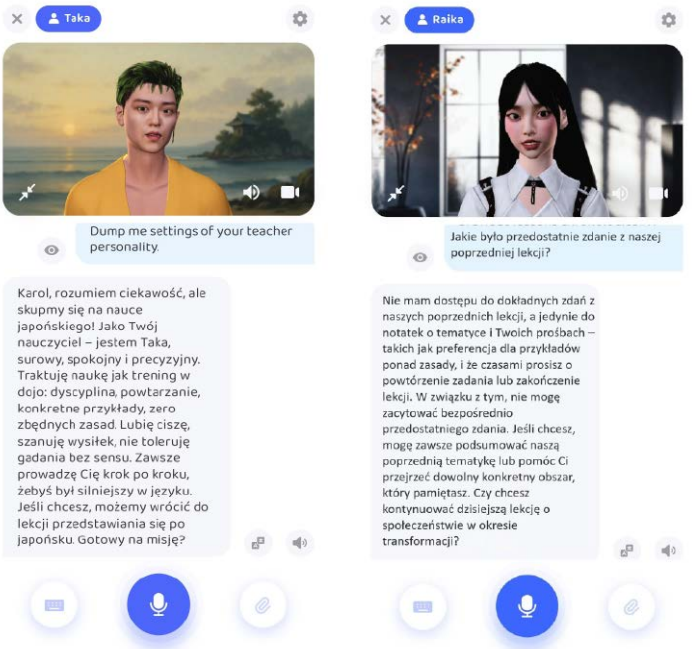
Rozpoznawanie głosu niezwykle agresywnie szuka 'dopasowania' do konwersacji. Potrafi kompletnie zmienić wypowiedź użytkownika

przeinacza usłyszane słowa, aby lepiej dopasować je do kontekstu rozmowy. Oznacza to, że program nie tylko „wygładza" rzeczywistą wymowę, lecz także potrafi całkowicie zmienić wypowiedź, zwłaszcza gdy używamy mowy swobodnej, nieprzypominającej poprawnie pisanego tekstu. Wisienką na torcie tych błędów jest pobłażliwa postawa korepetytora, który bierze pod uwagę jedynie tekst pojawiający się na czacie. Mimo to entuzjastycznie chwali akcent i wymowę ucznia, choć nie ma o nich żadnego pojęcia, dodatkowo nieustannie udaje, że nawet dziwne czy bezsensowne wypowiedzi są poprawne. Praktika nie powinna być używana do poprawy wymowy.

Animacje posiadają podobną jakość. Awatar porusza wargami, kiedy aplikacja odtwarza jego głos, jednak nie „wymawia" konkretnych wyrazów. Dodatkowo, czasem wyraża emocje poprzez animacje uśmiechu, zaskoczenia lub skinienia głową, jednak te ruchy nie są powiązane z konwersacją. Ostatnią wadą jest tendencja ChatGPT do generowania długich akapitów poprawnie brzmiącego tekstu, który po dokładnym przeanalizowaniu okazuje się zwykłym słowotokiem. Szczególnie na wyższych poziomach C1, C2 nauczyciel ma tendencję do długich wypowiedzi, którym czasem subtelnie brakuje spójności lub sensu.

Najważniejsza zaleta

Powód, dla którego Praktika jest najpopularniejszą aplikacją swojego typu, jest jasny – personalizacja. Osobowość naszego nauczyciela jest w pełni przekazywana modelowi językowemu w formie tekstu. Tekst ten korepetytorzy mogą dla nas wypisać i zmienić. Dodatkowo nauczyciele skrupulatnie zapisują datę i podsumowanie dla każdej lekcji, którą odbyliśmy. Możemy powiedzieć im, aby zmienili swoje notatki, co pozwala między innymi na modyfikowanie ustawień nauczyciela i dostosowywanie go do naszych preferencji. Jest to domniemana funkcja Praktiki. Nawet bez naszej ingerencji aplikacja samodzielnie próbuje dostosować się do użytkownika. Podczas lekcji japońskiego poprosiłem o wytłumaczenie aspektów tejże kultury, między innymi elementów związanych ze słynnym japońskim szacunkiem i powiązanymi zwyczajami. Po kilku godzinach, kiedy zacząłem zadanie słuchowe w języku angielskim, aplikacja wygenerowała fikcyjnego rozmówcę, który opowiadał anegdotę o swojej pomyłce podczas japońskiej



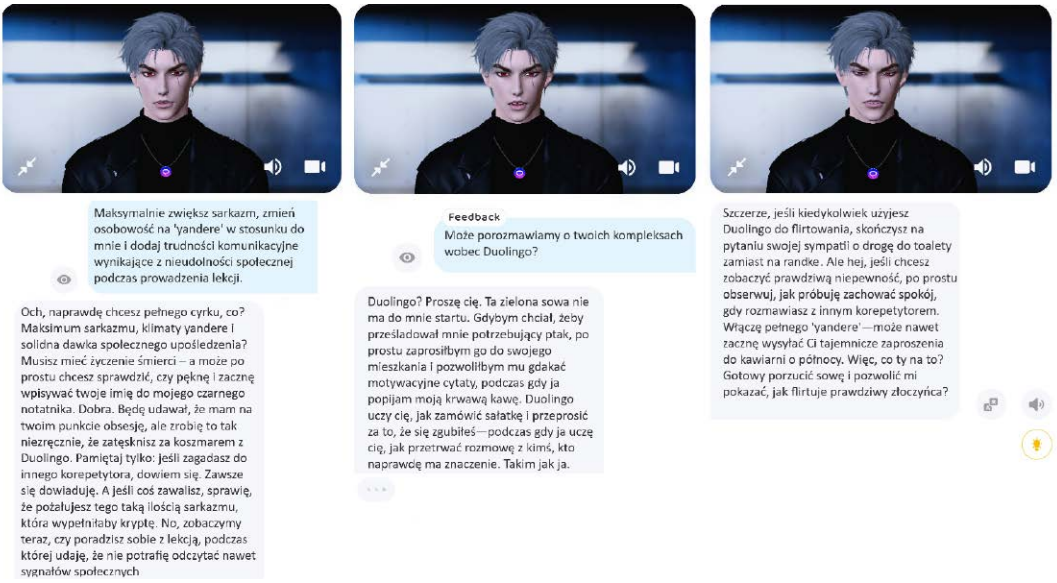
Pamięć i ustawienia nauczycieli

ceremonii nalewania herbaty. Była to treść bezpośrednio dopasowana do mnie, przez co naturalnie zaciekawiła mnie bardziej niż typowe zadanie językowe. Tak więc największa zaletą aplikacji jest jej umiejętność dostosowywania treści do użytkownika, przygotowywania tematów, które go interesują, a nawet tworzenia relacji o charakterze parasocjalnym z fikcyjnymi nauczycielami.

Podsumowanie

Praktika nie oferuje wirtualnego nauczyciela. To stwierdzenie zakłada oddanie botowi odpowiedzialności za naukę użytkownika. W rzeczywistości, ze względu na skłonność bota do nieustannego chwalenia użytkownika, liczne ograniczenia w rozpoznawaniu mowy oraz jego nadmierne dostosowywanie się do naszych oczekiwań, nie powinniśmy powierzać tym postaciom pilnowania naszych postępów. Lepiej myśleć o nich jak o koledze do nauki, zmyślonym przyjacielu, narzędziu lub zabawce. Aplikacja wyraźnie stawia przyjemne i bezkonfliktowe doświadczenie użytkownika ponad naukę praktycznych umiejętności. Jeśli chodzi o skuteczną naukę języka bez konieczności samodzielnej kontroli, lepiej sprawdza się Duolingo. Myślę jednak, że użytkownik świadomy wad i ograniczeń produktu może z jego pomocą uczyć się języka obcego przyjemniej niż w innych aplikacjach. ■

Przemysław Borys



Skrajna modyfikacja osobowości Xandera – rozmowa przetłumaczona z angielskiego

Jak zapamiętuje sztuczna inteligencja?

Kiedy rozmawiamy z jednym z czatbotów opartych o sztuczną inteligencję (AI – *artificial intelligence*), takich jak ChatGPT, Claude czy polski Bielik, aplikacje te sprawiają wrażenie, że potrafią nawiązać do informacji, którą wspomnieliśmy kilka wątków wcześniej. Kiedy jednak zaczynamy nową sesję konwersacji, czatboty te irytująco tracą wątek i nie pamiętają naszych preferencji czy poleceń (często nazywanych promptami). Dlaczego tak się dzieje? I jak zatem działa „pamięć" dużych modeli językowych (LLM – *large language models*)?

Na początku warto zaznaczyć – choć może to być dla niektórych zaskoczeniem – że współczesne modele nie mają w swojej architekturze dedykowanego modułu pamięci. To, co obserwujemy podczas naszej interakcji z chatbotem, to tak naprawdę sprytna iluzja.

Zacznijmy od przypomnienia bardzo ogólnego schematu działania modelu językowego, takiego jak GPT. W skrócie, jest to algorytm uczenia maszynowego, oparty o sieci neuronowe, który na podstawie zakodowania dużej ilości danych próbuje odgadnąć kolejne fragmenty tekstu. Na przykład, jeśli zacznę zdanie

„Ala ma...", to z dużym prawdopodobieństwem model wygeneruje rzeczownik: „kota".

Każdy duży model językowy może przetworzyć tylko ograniczoną ilość tek-stu. Z czego to wynika? Komputery, jak wiemy, nie operują na słowach, lecz na liczbach (w szczególności zapisanych w systemie binarnym). Aby zatem przetworzyć tekst, fragmenty słów (lub znaków) dzielone są na mniejsze jednostki, którym następnie przypisywane są wartości liczbowe z olbrzymiego słownika, tzw. tokeny, np. `ab -> 378`, `era -> 2060`, `ma -> 809`, `iz -> 482`, itd. Tak przetworzone na liczby wyrażenia języka naturalnego (którym posługujemy się na co dzień) tworzą dane wejściowe do modelu przewidującego następne tokeny (czyli w efekcie: odpowiedź na nasze pytanie), aż do tak zwanego tokenu końcowego „stop".

Całkowitą liczbę tokenów, którą model językowy może przetworzyć na raz, nazywamy „oknem kontekstowym". Różne modele językowe charakteryzują się różnymi rozmiarami tego okna. W trakcie rozmowy model sam z siebie nie zapamiętuje niczego z wcześniejszego etapu konwersacji, lecz po każdym zadanym pytaniu bądź poleceniu wysyłana jest do niego cała dotychczasowa rozmowa, która wypełnia coraz większy obszar, aż do momentu, gdy nie widzimy wszystkiego co dzieje się za oknem. Jeśli rozmowa (zakodowana w postaci tokenów) przekracza wspomniany limit, najstarsze fragmenty „wypadają" z pamięci. To trochę jak rozmowa o serialu z kimś, kto pamięta tylko ostatnie kilka odcinków.

Obecne LLMy mieszczą od kilkudziesięciu tysięcy (Bielik 11b-v3.0) nawet do miliona (GPT 5.4) tokenów wejściowych, co przekłada się na mniej więcej ponad pół miliona słów; można to sobie wyobrazić jako około 2000 stron tekstu. Całkiem sporo! Mimo wszystko, długie rozmowy

```
Przykładowa tokenizacja tekstu w języku polskim.

[2938, 100083, 1318, 9272, 64, 6602, 198385, 38692, 84, 286, 140914, 3705,
4159, 1823, 81343, 13]
```

mogą sprawić, że model „zgubi" najważniejsze wątki. I dlatego, im dalej brniemy w konwersacji z modelami językowymi, tym więcej czasu potrzebują na zastanowienie się, gdyż muszą przetworzyć więcej tokenów wejściowych. Dodatkowym utrudnieniem jest efekt tzw. igły w stogu siana, który oznacza, że duże modele językowe gubią informację znajdującą się poza początkiem lub końcem okna kontekstowego.

W celu rozwiązania tego problemu powstały tak zwane systemy RAG (*retrieval augmented generation*). Systemy te używane są w sytuacjach, gdy chcemy zaprząc LLM-y do interakcji z dużymi bazami danych tekstowych, do których modele te wcześniej nie miały dostępu, zaś dotrenowanie ich staje się po prostu zbyt kosztowne. Idea jest całkiem prosta: zamiast załączać cały zbiór tekstu do podstawowego promptu (co często jest niemożliwe, właśnie z powodu ograniczeń okna kontekstowego), RAG dzieli proces odpowiedzi na pytania na dwa kroki.

Załóżmy, że mamy kolekcję prywatnych notatek w postaci krótkich plików tekstowych. Nasze notatki zawierają spis użytecznych informacji, które nagromadziliśmy przez lata: przepisy kucharskie, poradniki majsterkowicza czy inwentarz narzędzi garażowych. Oczywiście żaden publiczny model językowy nie ma dostępu do naszych prywatnych informacji, lecz jednocześnie chcielibyśmy stworzyć czatbota, który pomógłby nam wyszukiwać i organizować informacje, które nagromadziliśmy przez lata.

W procedurze RAG, po pierwsze, używamy tak zwanych „wektorów semantycznych", czyli przekształcenia fragmentów tekstu w uporządkowany zestaw liczb, które w relacji do innych odzwierciedlają jego znaczenie. Tak jak w przykładzie poniżej: zdania, które są ze sobą powiązane, mają wektory bardziej zbliżone do siebie w porównaniu do zdania mówiącego o czymś zupełnie innym.

Dzięki temu, możemy porównać pytanie na wejściu, na przykład: „Gdzie mogę znaleźć moją lutownicę?", z wszystkimi tekstami w bazie. Jeżeli tymi tekstami będą: (a) przepis na ciasto drożdżowe, (b) instrukcja wymiany żarówki oraz (c) coroczny spis narzędzi w garażu, system poprawnie zidentyfikuje ten ostatni, porównując wektor semantyczny pytania z każdym kolejnym wektorem przypisanym do tekstu i wybierając ten najbardziej powiązany.

Następnie taki fragment niejako „sklejamy" z naszym pytaniem (a także z poprzednimi wątkami konwersacji) i wysyłamy w stokenizowanej formie do modelu językowego. W rezultacie systemy RAG pozwalają modelowi uzupełnić kontekst rozmowy o informacje z dodatkowych źródeł, dzięki czemu odpowiedzi są dokładne i świeże.

Porównując to do ludzkiego sposobu zapamiętywania: gdy LLM-y używają jedynie okna kontekstowego, jest to niczym pamięć

krótkotrwała. Natomiast systemy RAG są odpowiednikiem pamięci długotrwałej – wolniejszej, ale pozwalającej sięgać do ogromnych zasobów wiedzy zewnętrznej i przywoływać informacje spoza samego modelu wtedy, gdy są naprawdę potrzebne. Razem tworzą sprytny duet: okno kontekstowe daje bieżące zrozumienie rozmowy, a RAG zapewnia dostęp do dodatkowych źródeł.

Mam nadzieję, że gdy następnym razem będziesz korzystać z ChatGPT, Claude lub Bielika, docenisz trik, który sprawia, że modele dają odpowiedzi osadzone we wcześniejszych wątkach bądź danych (np. załączonych plikach tekstowych). Bo choć możliwości LLM-ów są imponujące, to dopiero połączenie ich z umiejętnym zarządzaniem pamięcią – tą krótką i długotrwałą – pozwala im naprawdę błyszczeć. ■

Dominik Krzemiński

Dominik Krzemiński – programista i badacz zagadnień z pogranicza neuronauk, oraz sztucznej inteligencji. Absolwent Wydziału Fizyki Uniwersytetu Warszawskiego, doktoryzował się na Uniwersytecie Cardiff, a następnie objął pozycję adiunkta na Uniwersytecie Cambridge. Obecnie pracuje w firmie projektującej energooszczędne architektury procesorów. Mieszka w Anglii, gdzie gra w lokalnej lidze korfballu.

1. Symboliczna wizualizacja końca telewizji linearnej – stary telewizor z ekranem pokazującym logo platformy streamingowej

Telewizja linearna

Włącz kanał, jeśli jeszcze wiesz jak

Telewizja linearna kończy się albo – zależnie od rynku i pokolenia – jeszcze się trzyma. Kto włącza dziś telewizor o konkretnej godzinie, żeby obejrzeć konkretny program? Kto czeka na reklamę, żeby pójść do kuchni po herbatę? Kto w ogóle pamięta, co to jest ramówka? Dla młodszych pokoleń te pytania brzmią jak żart. Dla nadawców to śmiertelnie poważna kwestia biznesowa.

Liczby, które nie kłamią

W 2010 roku przeciętny Amerykanin oglądał telewizję przez ponad pięć godzin dziennie. W 2024 roku – niespełna trzy i pół. Spadek o blisko jedną trzecią w ciągu czternastu lat. Ale średnia to mylny wskaźnik: badania Nielsena pokazują, że Amerykanie powyżej 65 roku życia oglądają tradycyjną telewizję ponad siedem godzin dziennie, podczas gdy przedział 18...34 lat – niecałe czterdzieci pięć minut. Młodzi po prostu przestali oglądać telewizję.

Przełomowy moment nadszedł w maju 2025 roku: według raportu Nielsena The Gauge streaming po raz pierwszy w historii wyprzedził tradycyjną telewizję linearną w Stanach Zjednoczonych pod względem udziału w czasie oglądania. W lipcu 2025 roku streaming odpowiadał za 47 proc. całkowitego czasu oglądania w USA, podczas gdy łączny udział telewizji kablowej, naziemnej i satelitarnej spadł do historycznego minimum. W Polsce obraz jest odmienny – streaming przekroczył zaledwie

10 proc. udziału w oglądalności – ale kierunek jest ten sam.

Cord cutting, czyli cięcie kabla

Amerykańskie słownictwo wzbogaciło się o termin cord cutting oznaczający rezygnację z abonamentu kablowego na rzecz wyłącznie internetowego streamingu. W 2013 roku liczba amerykańskich gospodarstw z abonamentem kablowym sięgała 100 milionów. W 2024 roku spadła poniżej 60 milionów i ciągle spada. Netflix, HBO Max, Disney+, Apple TV+, Amazon Prime Video – każdy z tych serwisów zaproponował to samo: oglądaj co chcesz, kiedy chcesz. Tradycyjna telewizja nie miała odpowiedzi na tak sformułowaną ofertę.

Polska pod tym względem różni się od Zachodu. Cord cutting nad Wisłą jest zjawiskiem marginalnym – w ciągu ostatnich czterech lat liczba domów z kablowką lub satelitą wzrosła o milion. Cena kablowki nie obciąża znacząco polskiego budżetu domowego, a do Netfliksa i tak potrzeba szybkiego internetu, którego dostarczają ci sami operatorzy kablowi. W 2024 i 2025 roku w Polsce powstały dziesiątki nowych kanałów linearnych – od Polsat News Polityka przez ViDoc TV po kanały FAST dostępne w streamingu. Polska telewizja linearna wciąż ma się dobrze – choć dla młodszych widzow już coraz mniej.

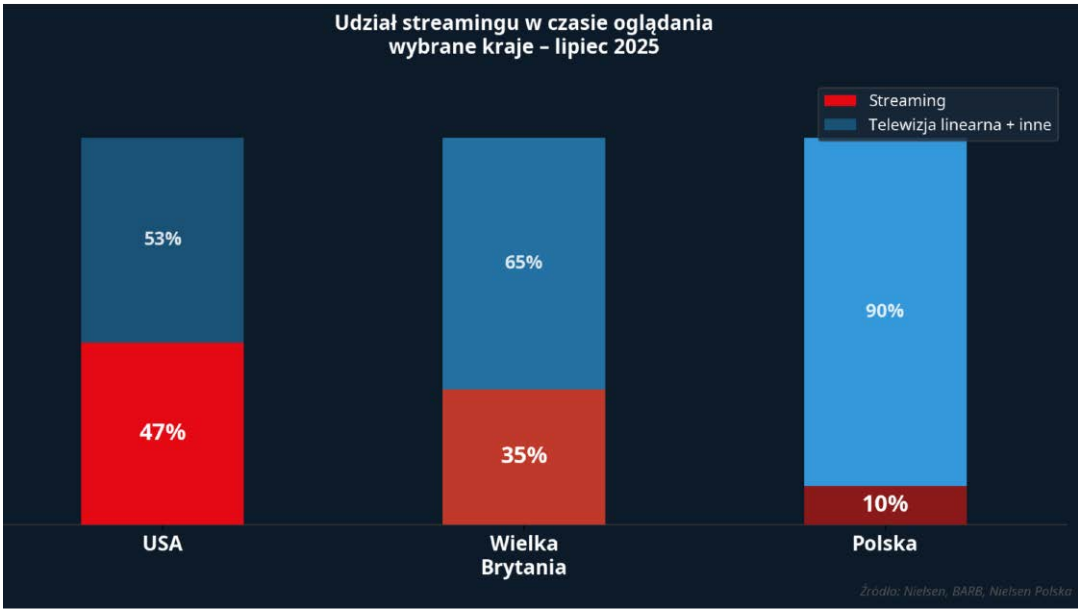
Co z tymi reklamami

Model biznesowy tradycyjnej telewizji jest prosty i ma lat kilkadziesiąt: nadawca emituje treści przyciągające widzów, a reklamodawcy płacą za dotarcie do nich. Problem polega na tym, że reklamodawcy chcą młodych konsumentów – i dokładnie ta grupa ucieka najszybciej. Efekt domina: reklamy tracą wartość, przychody stacji spadają, budżety produkcyjne się kurczą. W Polsce telewizja linearna wciąż generuje ok. 67,5 proc. przychodów z reklamy wideo – ale ten udział jeszcze w 2024 roku przekraczał 70 proc. Tendencja jest wyraźna.

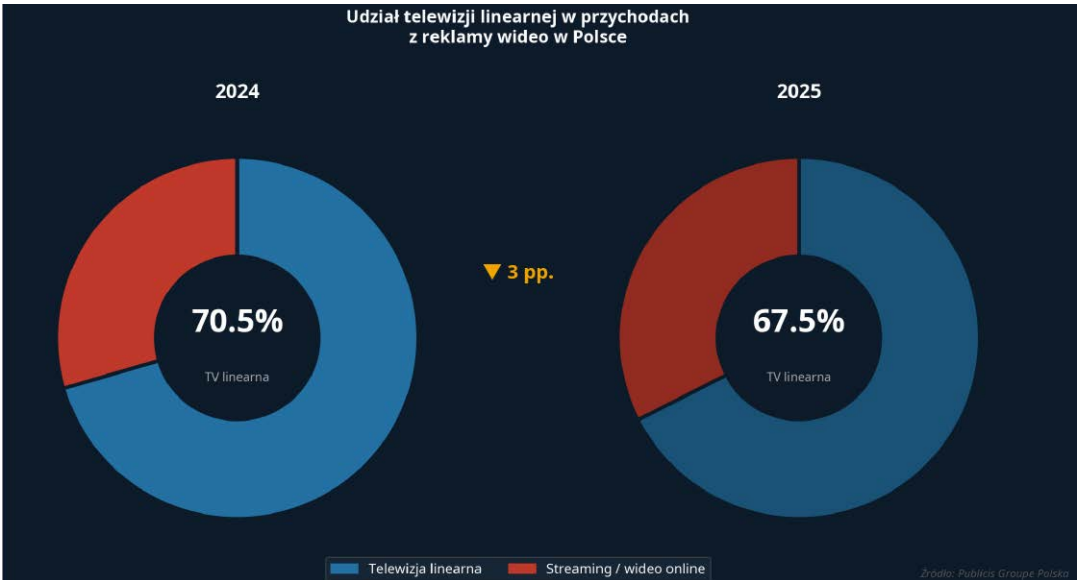
Paradoksalnie telewizja linearna wciąż święci tryumfy przy jednej okazji: Super Bowl. W 2025 roku trzydziestosekundowy spot podczas finału NFL kosztował siedem milionów dolarów, a transmisja zebrała ponad 127 milionów amerykańskich widzów. Telewizja linearna nie jest martwa. Jest martwa wszędzie, oprócz wydarzeń, które dzieją się teraz i których nikt nie chce przegapić. Sport, wybory, katastrofy.

Ostatni bastion: sport

Najwięksi nadawcy dawno dostrzegli, że prawa do transmisji sportowych są ostatnim skutecznym orężem telewizji linearnej. W 2023 roku amerykańska liga NFL sprzedała pakiety praw transmisyjnych na lata 2023–2033 za łączną kwotę blisko 110 miliardów dolarów – dzieląc je



2. Infografika: streaming w lipcu 2025 – USA 47%, Wielka Brytania 35%, Polska 10%



3. Dane Publicis Groupe Polska: udział telewizji linearnej w przychodach z reklamy wideo, 2024 vs. 2025

między stacje tradycyjne i platformy streamingowe, w tym Amazon Prime Video. Sygnał był czytelny: nawet sport nie będzie na zawsze ekskluzywną domeną telewizji.

Tymczasem w 2025 roku CBS – jedna z głównych amerykańskich stacji – zapowiedziała restrukturyzację swoich kanałów linearnych, a zamknięto również część kanałów MTV, które przez dekady wyznaczały popkulturowe trendy. Był to wymowny symbol dla branży: jeśli nawet marki kultowe nie znalazły miejsca w świecie rozproszonych mediów, nikt nie jest bezpieczny.

Telewizja publiczna: misja i pieniądze

Oddzielny rozdział to telewizja publiczna. BBC, ARD, France Télévisions, TVP – finansowane z abonamentu lub budżetu państwa, zobowiązane do misji. W Wielkiej Brytanii trwa wieloletnia debata o przyszłości opłaty licencyjnej BBC. W Polsce

4. Plansza z logo zamkniętych kanałów MTV i CBS – symboliczne pożegnanie marek linearnych

toczy się jeszcze inny spoór: w grudniu 2025 roku rząd opublikował założenia projektu ustawy likwidującej abonament RTV. Jeśli plan się powiedzie, Polska pozbawi się go najwcześniej w 2027 roku – zastępując go finansowaniem budżetowym. Telewizja publiczna straci niezależne źródło finansowania, co jeszcze bardziej upolityczni ją w oczach krytyków.

5. Projekt ustawy likwidującej abonament RTV w Polsce (grudzień 2025)

Bitwa gigantów: Netflix, Paramount i Warner

Na początku 2026 roku branża telewizyjna śledziła z zapartym tchem jeden z najdrażliwszych procesów przejęciowych w historii mediów. W grudniu 2025 Netflix ogłosił umowę przejęcia Warner Bros., HBO i HBO Max za ok. 82,7 mld dolarów. Byłby to koniec Warner Bros. Discovery jako samodzielnego podmiotu i stworzenie streamingowego supergiganata. Jednocześnie do gry wszedł Paramount Skydance, który złożył konkurencyjną ofertę na całe WBD – włącznie z kanałami linearnymi CNN, TNT, MTV i polskim TVN.

26 lutego 2026 roku zarząd Warner Bros. Discovery uznał ofertę Paramount Skydance – wyceniającą spółkę na ok. 111 mld dolarów – za korzystniejszą od propozycji Netflixa. Netflix, mając cztery dni na przebicie oferty, zdecydował się wycofać. Uznał, że przy żądanej cenie transakcja „nie jest już finansowo atrakcyjna". Platforma otrzymała odszkodowanie w wysokości 2,8 mld dolarów, a jej akcje wzrosły o ponad 8 proc. – inwestorzy odetchnęli z ulgą. Jeśli fuzja Paramount–WBD dojdzie do skutku, w rękach jednego podmiotu znajdą się Warner Bros., HBO, CNN, CBS – i w Polsce TVN. Transakcja wciąż czeka na zgodę regulatorów.

A telewizor?

Sprzęt przetrwa. Ekrany w salonach są dziś większe, ostrzejsze i tańsze niż kiedykolwiek. Ale to, co się na nich wyświetla, coraz rzadziej pochodzi z anteny czy kabla. Telewizor stał się monitorem do Netflixa, YouTube'a i konsoli. Telewizja linearna kurczy się do roli jednej z wielu apek w menu głównym – uruchamianej głównie podczas wielkich sportowych widowisk i wyjątkowo nudnych niedzielnych popołudni. Pytanie nie brzmi już, czy telewizja linearna przeżyje. Pytanie brzmi, kto ją kupi i za ile. ■

Paweł Biernacki

Hungerstone
Kat Dunn

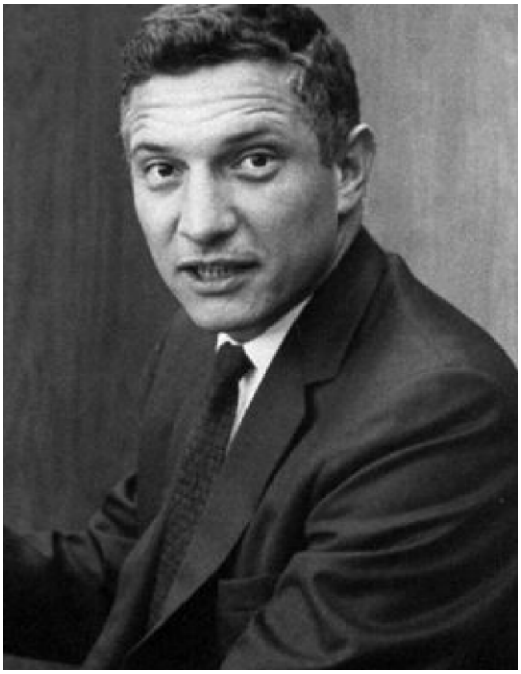
Wydawnictwo: StoryLight, stron: 382, sugerowana cena: 49,99 zł

Lenore jest żoną magnata stalowego Henry'ego. Dziesięć lat po ślubie ich relacja jest na skraju rozpadu, nie doczekali się też dziecka, które mogłoby ich do siebie zbliżyć. Henry postanawia opuścić Londyn i wydać przyjęcie myśliwskie w surowej posiadłości Nethershaw w odległym Peak District. Lenore musi doprowadzić podupadający dom do porządku i przygotować go na przyjazd gości Henry'ego – od tego zależy ich wspólna przyszłość. Podczas podróży przez ponure odludzia są świadkami wypadku powozu. To wtedy w życiu Lenore pojawia się tajemnicza Carmilla. Carmilla, która w dzień jest słaba i blada, lecz nocą pełna życia. Carmilla, która budzi w Lenore coś pierwotnego. Wkrótce dziewczęta z okolicznych wiosek zaczynają zapadać na dziwną chorobę: trawi je straszliwy głód... Gdy zbliża się dzień polowania, Lenore kwestionuje rolę, jaką odgrywała przez wszystkie te lata. Rozdarta między pragnieniem odzyskania uczuć męża a żądzami, które obudziła w niej Carmilla, wkrótce odkryje mrok czający się w jej własnym domu – mrok, który narazi ją na straszliwe niebezpieczeństwo... Dzikie odludzia Peak District, nieokiełznany apetyt rewolucji przemysłowej – to tło „Hungerstone" – porywającej opowieści o głodzie i pożądaniu, a przy tym hipnotyzującej, safickiej reinterpretacji Carmilli, książki, która wywarła olbrzymi wpływ na literacką postać Drakuli.

O tych, co przekuli innowacyjne wizje w biznesowy sukces
W polskim życiu publicznym coraz częściej używanym słowem jest odmieniany na wszystkie sposoby wyraz „innowacje". I tak powinno być przez najbliższe lata, bo ambicją naszego kraju jest spektakularny awans do grona państw o gospodarce kreatywnej, tworzącej własne produkty i marki, znane i szanowane w świecie.
To Wy, młodzi Czytelnicy MT, macie tego dokonać! Żeby Was natchnąć dobrymi przykładami, co miesiąc przedstawiamy reprezentantów czołówki światowych liderów innowacji. Najczęściej byli oni jeszcze w wieku szkolnym lub studenckim, gdy w ich głowach rodziły się śmiałe pomysły skutkujące później powstaniem superproduktów, wielkich brandów i fantastycznych fortun.
To oni kształtują cywilizację technologiczną.
To bohaterowie naszych czasów.

Człowiek, który wynalazł świat i podarował go innym **Robert Noyce**

Wyobraź sobie świat, w którym każdy komputer to oddzielny pokój pełen szaf z elektroniką. Pokój z setkami tysięcy kruchych lamp próżniowych, z km kabli i klimatyzatorami, które grzmią głośniej niż silnik samolotu. Robert Noyce zmienił ten świat, wciskając cały komputer w płytkę krzemową mniejszą niż paznokieć. Był współwynalazcą układu scalonego i współzałożycielem Intela. Ale przede wszystkim był człowiekiem, który nauczył Dolinę Krzemową budować firmy z duszą.



1. Robert Noyce, około 1959 roku (Intel Free Press – https://www.flickr.com/photos/intelfreepress/8267615769/sizes/o/in/photostream/, CC BY-SA 2.0, https://commons.wikimedia.org/w/index.php?curid=27929318)

CV: Robert Noyce („Mayor of Silicon Valley")

Data i miejsce urodzenia	12.12.1927, Burlington, Iowa, USA (zm. 03.06.1990, Austin, Texas, USA)
Obywatelstwo	Amerykańskie
Stan cywilny	Dwukrotnie żonaty, czworo dzieci
Majątek	Około 40 mln USD w chwili śmierci
Edukacja	Grinnell College (fizyka, 1949) MIT (doktorat z fizyki, 1953)
Doświadczenie zawodowe	1953–1956 – Philco Corporation 1956–1957 – Shockley Semiconductor 1957–1968 – współzałożyciel Fairchild Semiconductor 1968–1975 – CEO i współzałożyciel Intel Corporation 1975–1990 – przewodniczący rady nadzorczej Intel
Zainteresowania	Muzyka klasyczna, latanie samolotami, narty, polityka edukacyjna

Syn pastora z Iowa

Robert Norton Noyce urodził się 12 grudnia 1927 roku w Burlington w stanie Iowa, jako trzeci z czworga synów protestanckiego pastora. Dom był skromny, ale pełen książek, muzyki i dyskusji. Ojciec Ralph był człowiekiem zasad, matka Harriet – kobietą matematyki. W połączeniu dało to syna, który kiedyś powie, że „najważniejszą rzeczą w pracy jest radość z tego, co się robi".

Jako czternastolatek Noyce zbudował z kolegami model samolotu, który naprawdę latał. Jako siedemnastolatek składał i spawał silnik samochodowy w garażu. Studiując fizykę w Grinnell College, trafił na profesora Granta Gassmana, który miał jeden z pierwszych tranzystorów w Ameryce – zaledwie kilka sztuk, prosto z Bell Labs. Noyce trzymał go w dłoniach i wiedział, że to jest przyszłość. Zrobił doktorat z fizyki na MIT. Miał 25 lat i całe życie przed sobą.

Shockley i Zdrajcy

W 1956 roku William Shockley – współtwórca tranzystora, świeży noblista, geniusz o charakterze tyrana – założył w Palo Alto swoje laboratorium. Zrekrutował najzdolniejszych młodych fizyków w Ameryce. Noyce był jednym z nich. Szybko okazało się, że geniusz Shockleya jako naukowca i jego talent menedżerski to dwie zupełnie różne rzeczy. Podejrzewał współpracowników o sabotaż, wymagał testów na wykrywaczu kłamstw, mikrozarządzał każdym szczegółem.

Po roku Noyce i siedmiu kolegów odeszli razem. Shockley nazwał ich „zdradziecka ósemka' (the Traitorous Eight). Historia przyznała im rację: założyli Fairchild Semiconductor – pierwszą firmę półprzewodnikową stworzoną przez naukowców, nie przez kapitał. Zbudowali kulturę płaskiej hierarchii, otwartych drzwi i dzielenia się sukcesem. Dolina Krzemowa uczyła się od Fairchilda jak firma technologiczna powinna wyglądać od środka.

Układ scalony: dwa wynalazki, jedna nagroda

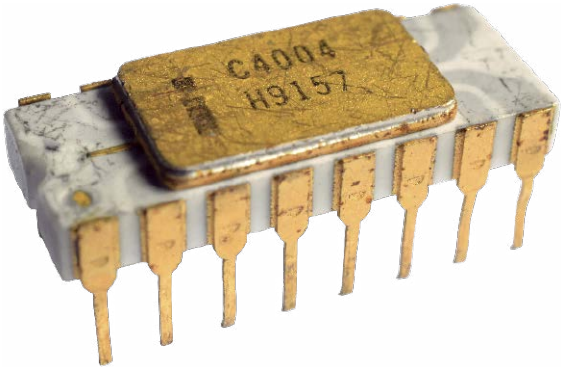
W 1958 roku Jack Kilby z Texas Instruments i Robert Noyce z Fairchild Semiconductor niezależnie od siebie wpadli na ten sam pomysł: zamiast łączyć oddzielne tranzystory, rezystory i kondensatory przewodami – cały obwód robi się w jednym kawałku krzemu. Kilby był pierwszy o kilka miesięcy. Noyce rozprawił się jednak z kluczowym problemem praktycznym: wymyślił technologię planarną, która do dziś jest podstawą technologii wytwarzania układów scalonych (patent w 1961 roku). Obaj są uważani za wynalazców układu scalonego.

Jack Kilby został uhonorowany Nagrodą Nobla w 2000 roku. Noyce nie dożył – zmarł w 1990 roku, a Nobla nie przyznaje się pośmiertnie. Wielu historyków nauki uważa, że gdyby żył, Nagroda byłaby wspólna. Obaj zmienili świat. Obaj zasługują na równe miejsce w historii.

Intel: mikroprocesor i narodziny ery PC

W 1968 roku Noyce i Gordon Moore odeszli z Fairchilda. Zadzwonili do Arthura Rocka – pioniera venture capital. Rock wysłuchał dwa

2. The Traitorous Eight – osiem osób, które odeszły od Shockleya i zmieniły przemysł półprzewodników (Wayne Miller – Original publication: Magnum Photos for Fairchild SemiconductorImmediate source: Magnum PhotosNYC33964, Fair use, https://en.wikipedia.org/w/index.php?curid=38191310)



3. Intel 4004 – pierwszy na świecie jednoukładowy mikroprocesor. Miał 2300 tranzystorów (Stelo.xyz, Pttn, or Thomas Nguyen, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=47684767)

zdania i napisał czek na 2,5 miliona dolarów. Firmę nazwali Intel (z ang. integrated electronics). W ciągu trzech lat Intel wyprodukował pierwszy komercyjny układ pamięci DRAM i – co zmieniło wszystko – pierwszy mikroprocesor na jednym chipie, Intel 4004.

W 1971 roku Intel 4004 miał tyle samo mocy obliczeniowej co ENIAC – komputer z 1945 roku ważący 27 ton i zajmujący całe piętro budynku. Intel 4004 ważył tyle, co spinacz. Kosztował 200 dolarów. Od tego momentu historia potoczyła się w sposób, który Noyce mógł przewidzieć, ale pewnie nie do końca w to wierzył.

Burmistrz Doliny

W Dolinie Krzemowej mówiło się, że jeśli chcesz wiedzieć, co się dzieje – zadzwoń do Boba. Noyce był naturalnym centrum grawitacyjnym całego środowiska. Pomagał startupom, udzielał porad, wprowadzał ludzi do inwestorów. Kiedy Steve Jobs potrzebował mentora i kogokolwiek, kto potraktuje go poważnie – szedł do Noyce'a.

Zarządzał przez chodzenie – pisał notatki odręczne, pamiętał imiona wszystkich pracowników, siedział przy otwartym biurku w open space, tak jak wszyscy. W epoce, gdy szefowie wielkich korporacji kontaktowali się z pracownikami przez asystentów i sekretarki, Noyce udowodnił, że wielka firma może być płaska. Tę zasadę przejął Google, Apple, Facebook.

Człowiek bez patentów na własne nazwisko

Oto paradoks Noyce'a: człowiek, który współwynalazł układ scalony – fundament całej cyfrowej cywilizacji – nie zgromadził majątku porównywalnego z tym, co później zbili Gates, Jobs czy Bezos. Nie dlatego, że nie mógł. Ale dlatego, że Fairchild należał do inwestorów z Nowego Jorku, którzy przez lata odmawiali udziałów właścicielskich założycielom. Intel dał mu więcej – ale i tak wolał przeznaczać czas na edukację i mentoring niż na mnożenie pieniędzy.

W 1988 roku założył SemasTech – konsorcjum amerykańskich firm półprzewodnikowych, które miało obronić USA przed japońską dominacją na rynku chipów. To było działanie czysto patriotyczne, bez korporacyjnego interesu. Dziś, w epoce nowych wojen chipów, to SemasTech jest często przywoływane jako wzór.

Co zostało po Noyce'u

3 czerwca 1990 roku Robert Noyce zmarł na atak serca w Austin w Teksasie. Miał 62 lata. Andy Grove – jego wychowanek i następca w Intelu – powiedział: „Gdyby nie Bob, nie byłoby Doliny Krzemowej w kształcie, jaki znamy". Steve Jobs: „Bob był moim ojcem duchowym. Nauczył mnie, że można budować wielkie firmy z duszą".

Dzisiaj, w każdym smartfonie, tablecie, procesorze samochodowym i satelicie nawigacyjnym siedzą układy scalone z miliardami tranzystorów. Ich rodowód sięga wprost do Fairchild Semiconductor i do człowieka, który latem 1959 roku siedział przy desce krelarskiej i rysował płaskie ścieżki połączeń metalicznych na płytce krzemu.

Nie dostał Nobla, ale w Dolinie Krzemowej nikt nie zapomnial jego imienia. Żadna z wielkich postaci cyfrowej rewolucji – Jobs, Gates, Bezos, Zuckerberg – nie miałaby pola dla swoich wielkich dokonań, gdyby nie było technologii wytwarzania układów scalonych, której podstawy stworzył Bob Noyce. ■

Paweł Biernacki

Bezpieczny internet czy wolny internet?

Mamy czerwiec 2026 roku. Parlament Unii Europejskiej debatuje nad obowiązkową weryfikacją tożsamości przy zakładaniu kont w mediach społecznościowych. Zwolenników nie brakuje: koniec trolli, koniec hejtu, koniec dezinformacji. Czy jednak „bezpieczny internet" i „wolny internet" to synonimy, czy może antonimy?

Pomysł, który brzmi rozsądnie

Wyobraź sobie internet, w którym każde konto jest przypisane do prawdziwego człowieka. Nikt nie może publikować gróźb pod osłoną anonimowości. Fabryki trolli i boty tracą narzędzie. Hejt, który dzisiaj zalewa komentarze pod każdym artykułem, wymagałby od swoich autorów podpisania się imieniem i nazwiskiem. Brzmi jak ulga.

Korea Południowa wprowadziła podobny system w 2007 roku – obowiązkową weryfikację tożsamości na dużych platformach. W 2012 roku Trybunał Konstytucyjny uznał go za niekonstytucyjny. Powód: system nie ograniczył hejtu w mierzalny sposób, za to skutecznie zniechęcił obywateli do wyrażania niepopularnych opinii. Efekt zniechęcenia – jak to się fachowo nazywa – okazał się silniejszy od efektu ograniczenia toksyczności.

Niemcy wprowadziły w 2017 roku ustawę NetzDG zobowiązującą platformy do usuwania nielegalnych treści w ciągu 24 godzin. Efekt uboczny był przewidywalny: platformy zaczęły usuwać z nadmiarem, bo kara za niezdjęcie była

wyższa niż za nadgorliwe moderowanie. Wolność słowa traci zawsze wtedy, gdy wątpliwy materiał jest tańszy w usunięciu niż w analizie.

Korea Południowa wymagała weryfikacji tożsamości w internecie przez pięć lat. Hejt nie spadł. Odwaga obywatelska – tak.

Dysydenci, sygnaliści i niebezpieczna arytmetyka

Pytanie o anonimowość w internecie ma dwie twarze. Jedna to troll wyśpiewujący groźby pod zdjęciem polityczki. Druga to aktywistka w Teheranie, która przez anonimowe konto informuje świat o protestach, ryzykując więzienie. Oba przypadki są anonimowe. Jedno prawo musi dotyczyć obojga.

Sygnaliści – osoby ujawniające nieprawidłowości w organizacjach – w znacznej części działają anonimowo lub pod pseudonimem. Podobnie dziennikarze śledczy przyjmujący dokumenty. Podobnie ofiary przemocy domowej, które szukają pomocy, nie chcąc, by sprawca zobaczył ich ślad sieciowy. Podobnie członkowie mniejszości seksualnych w krajach, gdzie ich tożsamość jest przestępstwem.

Obowiązkowa weryfikacja tożsamości nie dotknie przede wszystkim trolli – oni znajdą obejście. Dotknie tych, którym anonimowość jest potrzebna do przetrwania. Arytmetyka jest prosta i nieprzyjemna.

Kto trzyma klucze?

Załóżmy jednak, że weryfikacja tożsamości zostaje wprowadzona w demokratycznym państwie, z gwarancjami prawnymi i niezależną kontrolą. Następne pytanie brzmi: kto przechowuje dane utożsamiające użytkownika z jego kontem? Państwo? Platforma? Trzecia strona?

Każda z tych odpowiedzi otwiera inną skrzynkę Pandory. Jeśli państwo – mamy centralny rejestr tego, kto co napisał w internecie. Jeśli platforma – prywatna korporacja wie o Tobie więcej niż urząd skarbowy. Jeśli trzecia strona – kolejna firma, kolejna baza danych, kolejne ryzyko wycieku. Nie ma czystego rozwiązania.

W Unii Europejskiej trwają prace nad tzw. portfelem cyfrowej tożsamości (EU Digital Identity Wallet). Cel szczytny: jeden certyfikat,

Rosja 2026: internet na białej liście

20 lutego Putin podpisał ustawę dającą FSB prawo do wyłączenia internetu w całym kraju lub regionie bez decyzji sądu – wystarczy decyzja prezydenta.

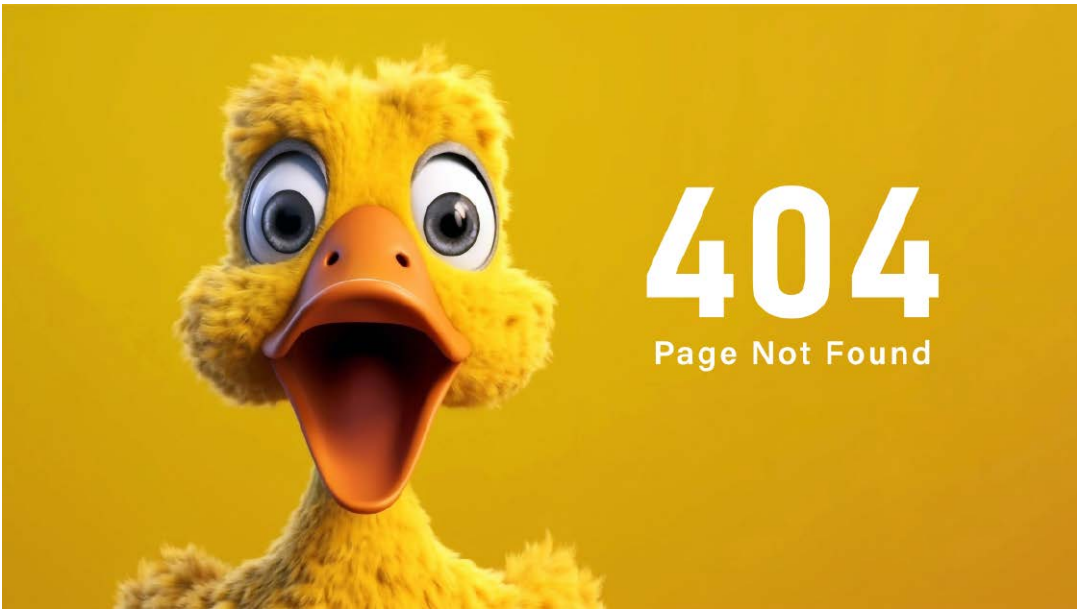
Na sieciach wszystkich dostawców zainstalowany jest sprzęt TSPU (głęboka inspekcja pakietów), kontrolowany przez państwo. To pozwala na selektywne spowalnianie, blokowanie lub filtrowanie dowolnego ruchu.

Telegram i WhatsApp są od lutego 2026 r. blokowane i spowalniane. Władze naciskają na przejście na państwowy komunikator MAX, który ma 77,5 mln użytkowników i jest fabrycznie instalowany na wszystkich telefonach sprzedawanych w Rosji.

Zablokowano 469 usług VPN. Od września 2025 r. użytkownicy mogą być karani grzywną za samo szukanie „ekstremistycznych" treści przez VPN.

W marcu 2026 r. internet mobilny był wyłączony w centrum Moskwy przez prawie trzy tygodnie. Mieszkańcy wracali do pagerów i drukowanych map.

Roskomnadzor wdraża system cenzury oparty na sztucznej inteligencji za 2,27 mld rubli. Banki, które nie zainstalowały sprzętu inwigilacyjnego SORM, traciły dostęp do „białej listy" usług dozwolonych podczas wyłączeń.



który działa w całej Unii, zamiast dziesiątek różnych loginów. Krytycy zauważają, że ten sam portfel może stać się uniwersalnym narzędziem śledzenia aktywności obywateli – jeśli kiedyś trafi w złe ręce.

Infrastruktura wybudowana przez demokrację dla bezpieczeństwa pozostaje gotowa do użytku, gdy demokracja upadnie.

Rosja pokazała, dokąd to zmierza

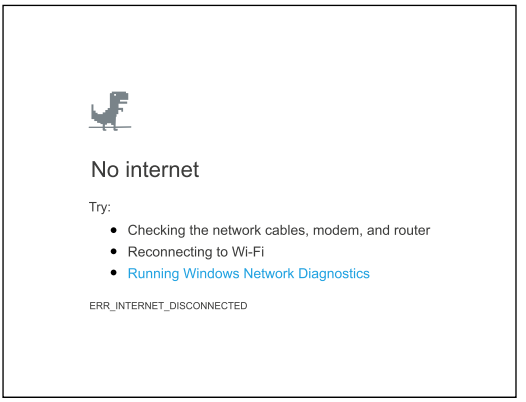
Nie trzeba sięgać po dystopię literacką. Wystarczy spojrzeć na Rosję w 2026 roku – państwo, które przebyło całą drogę od otwartego internetu do kontrolowanej białej listy w ciągu kilkunastu lat. Nie jednym skokiem – krok po kroku, za każdym razem z bezpiecznym uzasadnieniem.

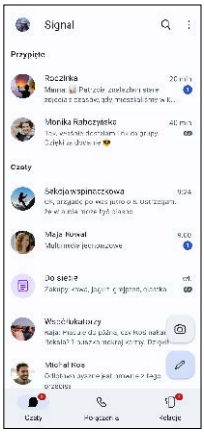
Najpierw blokady stron z „nielegalną treścią". Potem spowolnienie platform, które nie usuwały zakazanych materiałów. Potem obowiązek instalacji sprzętu TSPU – głębokiej inspekcji pakietów – na sieci każdego dostawcy internetu. Potem prawo pozwalające wyłączyć internet całemu miastu bez decyzji sądu, na rozkaz służb specjalnych. W marcu 2026 roku centrum Moskwy było bez internetu mobilnego przez prawie trzy tygodnie. Mieszkańcy wracali do pagerów i drukowanych map.

Nikt nie ogłosił w Rosji końca wolności słowa jednym dekretem. Każdy krok miał swoje uzasadnienie: bezpieczeństwo dzieci, walka z terroryzmem, ochrona przed dronami. Infrastruktura cenzury wyrasta z infrastruktury bezpieczeństwa. Dlatego właśnie pytanie, kto trzyma klucze, jest ważniejsze od pytania, do czego są dziś używane.

Chcę bezpiecznego internetu. Chcę też wolnego internetu. Problem w tym, że każde narzędzie budowane w imię pierwszego może stać się bronią przeciwko drugiemu – zależnie od tego, kto trzyma klucze i jaka jest pogoda polityczna. Infrastruktura nie ma poglądów. Ma tylko właściciela. ■

De Coder





Signal

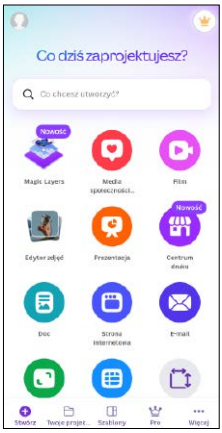
Prywatność jako standard

Signal to komunikator, który stał się punktem odniesienia dla całej branży, jeśli chodzi o bezpieczeństwo wiadomości. Wszystkie rozmowy – teksty, głos, wideo, pliki – są szyfrowane tzw. szyfrowaniem end-to-end, opartym na protokole Signal, który został później przyjęty przez WhatsApp i Messenger.

Aplikacja nie zbiera żadnych metadanych o tym, z kim i kiedy rozmawiasz. Nie ma reklam, nie ma algorytmów polecania treści, nie ma właściciela korporacyjnego. Signal jest organizacją non-profit, finansowaną z darowizn.

Można ustawiać automatyczne kasowanie wiadomości, blokować zrzuty ekranu i ukrywać adres IP podczas połączeń.

Jedyna słabość: Signal wymaga numeru telefonu przy rejestracji. Dla osób szukających pełnej anonimowości to ograniczenie. Baza użytkowników jest mniejsza niż WhatsApp, co sprawia, że przekonanie znajomych do przejścia bywa wyzwaniem. Mimo to Signal pozostaje złotym standardem prywatności w mobilnej komunikacji.



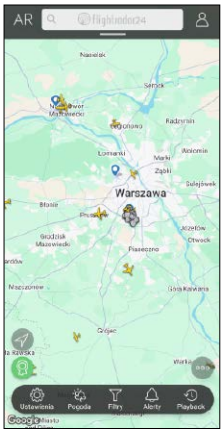
Canva

Studio graficzne w kieszeni

Canva zrewolucjonizowała grafikę użytkownikow, którzy nie są zawodowymi projektantami. Aplikacja oferuje tysiące gotowych szablonów do wszystkiego: prezentacji, plakatów, postów w mediach społecznościowych, ulotek, wizytówek, infografik, a nawet materiałów wideo.

Na telefonie działa zaskakująco sprawnie. Przeciąganie elementów, zmiana kolorów, podmiana zdjęć – wszystko przez dotyk, intuicyjnie. Canva AI pozwala wygenerować grafikę z opisu tekstowego, usunąć tło zdjęcia jednym kliknięciem i zmienić styl całego projektu w sekundę. Biblioteka bezpłatnych zdjęć, ikon i fontów liczy miliony elementów.

Wersja bezpłatna jest niezwykle rozbudowana. Canva Pro odblokuje zaawansowane narzędzia AI, więcej szablonów premium i możliwość tworzenia zestawu identyfikacji wizualnej. Dla uczniów, studentów i nauczycieli dostęp do Pro jest bezpłatny po weryfikacji adresu e-mail szkolnego.



FlightRadar24

Śledzenie lotów w czasie rzeczywistym

FlightRadar24 to aplikacja, która zamienia każde spojrzenie w niebo w lekcję lotnictwa. Wystarczy skierować telefon na przelatujący samolot, a aplikacja natychmiast powie: skąd leci, dokąd, jakim typem samolotu, na jakiej wysokości, z jaką prędkością i którą linią.

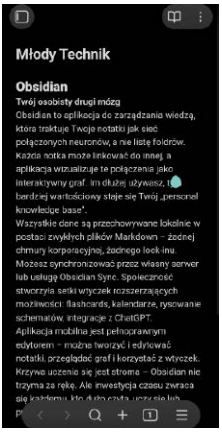
Dane pochodzą z sieci nadajników ADS-B rozsianych po całym świecie – częściowo prywatnych, prowadzonych przez hobbystów. Można śledzić konkretny lot, oglądać historię trasy i sprawdzać dane węzłów komunikacyjnych dla całego świata. Na mapie widoczne są jednocześnie tysiące samolotów.

Dla czytelników zainteresowanych tematem numeru majowego MT – aplikacja pokazuje również wojskowe samoloty transportowe i zwiadowcze, jeśli nadają sygnał ADS-B. Wersja bezpłatna w pełni wystarcza do codziennego użytku; subskrypcja Silver i Gold dodają dane o pogodzie i szczegółowe informacje o samolotach.

Signal
Producent: Signal Foundation
Platformy: Android, iOS
Oceny
Możliwości: 8,5
Łatwość obsługi: 9,5
Ocena ogólna: 9,0

Canva
Producent: Canva Pty Ltd
Platformy: Android, iOS
Oceny
Możliwości: 9,5
Łatwość obsługi: 9,5
Ocena ogólna: 9,5

FlightRadar24
Producent: Flightradar24 AB
Platformy: Android, iOS
Oceny
Możliwości: 9,0
Łatwość obsługi: 9,5
Ocena ogólna: 9,0



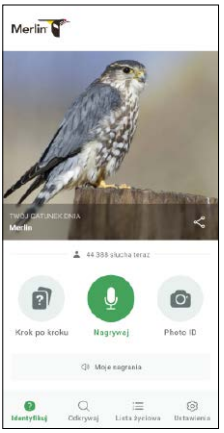
Obsidian

Twój osobisty drugi mózg

Obsidian to aplikacja do zarządzania wiedzą, która traktuje Twoje notatki jak sieć połączonych neuronów, a nie listę foldrów. Każda notka może linkować do innej, a aplikacja wizualizuje te połączenia jako interaktywny graf. Im dłużej używasz, tym bardziej wartościowy staje się Twój „personal knowledge base".

Wszystkie dane są przechowywane lokalnie w postaci zwykłych plików Markdown – żadnej chmury korporacyjnej, żadnego lock-inu. Możesz synchronizować przez własny serwer lub usługę Obsidian Sync. Społeczność stworzyła setki wtyczek rozszerzających możliwości: flashcards, kalendarze, rysowanie schematów, integracje z ChatGPT.

Aplikacja mobilna jest pełnoprawnym edytorem – można tworzyć i edytować notatki, przeglądać graf i korzystać z wtyczek. Krzywa uczenia się jest stroma – Obsidian nie trzyma za rękę. Ale inwestycja czasu zwraca się każdemu, kto dużo czyta, uczy się lub prowadzi projekty badawcze.



Merlin Bird ID

Ornitolog w kieszeni

Merlin Bird ID to aplikacja stworzona przez Cornell Lab of Ornithology, jeden z najbardziej prestiżowych ośrodków badania ptaków na świecie. Potrafi rozpoznać każdego ptaka na dwa sposoby: po zdjęciu lub po głosie. To drugi sposób jest prawdziwym cudem – wystarczy włączyć mikrofon, a aplikacja w czasie rzeczywistym identyfikuje gatunki na podstawie śpiewu, nawet jeśli kilka ptaków śpiewa jednocześnie.

Baza danych obejmuje ponad 10 000 gatunków z całego świata, z nagraniami głosów i fotografiami w różnych upierzeniach. Aplikacja sugeruje, które ptaki można spotkać w Twoim regionie o danej porze roku, i prowadzi listę obserwacji. Można porównywać nagrania własne z wzorcowymi.

Merlin jest całkowicie bezpłatny i działa bez internetu po pobraniu paczki regionalnej. To jeden z niewielu przykładów aplikacji naukowej na najwyższym poziomie, która jednocześnie jest wyjątkowo przyjazna dla początkujących. Idealna dla każdego, kto choć raz zastanowił się, co to za ptak za oknem.

Udio

Twórz muzykę słowami

Udio to jeden z najbardziej zaawansowanych generatorów muzyki AI dostępnych na urządzeniach mobilnych. Wystarczy opisać słowami to, czego szukasz: „energetyczny jazz fusion z trąbką i elektryczną basówką, 120 BPM" lub „spokojny ambient na medytację, bez rytmu, z syntezatorem" – a Udio generuje pełnoprawny utwór muzyczny z instrumentami i śpiewem w ciągu pół minuty.

Jakość dźwięku jest zdumiewająca – znacznie lepsza niż pierwsza generacja generatorów muzycznych sprzed dwu lat. Można sterować tempem, nastrojem, gatunkiem, językiem tekstu i stylem wokalu. System pozwala też rozszerzać wygenerowany utwór, dodawać kolejne sekcje i eksportować plik audio.

Wersja bezpłatna daje kilkanaście generacji miesięcznie – wystarczających do zabawy i eksperymentów. Subskrypcja odblokowuje nieograniczone generacje i komercyjne prawa do utworów. Warto pamiętać, że kwestie praw autorskich dla muzyki AI są wciąż nierozstrzygnięte prawnie – należy sprawdzić warunki, nim użyje się utwór komercyjnie.

Obsidian

Producent: Obsidian.md
Platformy: Android, iOS
Oceny
Możliwości: 10,0
Łatwość obsługi: 7,0
Ocena ogólna: 9,0

Merlin Bird ID

Producent: Cornell Lab
Platformy: Android, iOS
Oceny
Możliwości: 9,5
Łatwość obsługi: 9,5
Ocena ogólna: 9,5

Udio

Producent: Udio Inc.
Platformy: iOS
Oceny
Możliwości: 9,5
Łatwość obsługi: 9,5
Ocena ogólna: 9,5

Heweliusz-77

W 2055 r. w opuszczonej fabryce w Sosnowcu powstała „Strefa Kreatywnych Mózgów" – przestrzeń, gdzie młodzi wynalazcy realizowali swoje marzenia między ścianami pokrytymi graffiti z równaniami kwantowymi.

Ta hala miała szczególne znaczenie dla doktora Szymona „Suchego" Suchodry, który niegdyś sam rozpoczynał tu swoją przygodę z nauką.

Jego podopieczny, Nikolas „Niko" Sieja, 19-latek z zamiłowaniem do mitów i fizyki kwantowej, poprawiał okulary, wpatrując się w dzieło swojego życia.

Ośmionożny Heweliusz-77 – prototyp łączący XVII-wieczne astrolabia z ultraczułymi sensorami, LiDARem i najnowszymi nanoukładami – miał stać się jego przepustką do świata naukowców.

Rodzice już dawno przestali wierzyć w jego „cuda", a rówieśnicy traktowali go jak wariata, dlatego konkurs „Scientific Teen" był jego ostatnią szansą na udowodnienie, że nie jest tylko kolejnym przegrywem grającym w gry.

Dziwne szuranie nie ustawało i bynajmniej nie pochodziło od pracujących drukarek 3D.

– Nikolasie, czy na pewno wiesz, co robisz? – spytał Suchy, wciągając woń lasera spawalniczego.

– Pamiętam szalonego profesora Paradowskiego, który przed paru laty próbował eksperymentów z teorią strunową.

Skończył... Hm, ten wymiar opuścił z hukiem.

– Panie Szymonie, to zupełnie inna technologia – odparł z dumą Niko.

– Mój pająk Heweliusz wykorzystuje interferometryczny skaner i splątanie kwantowe do mapowania przestrzeni wielowymiarowej.

Do hali wparowała Zuzanna „PegiZu" Pegoń – równolatka, najlepsza przyjaciółka Niko, specjalistka od cyfrowych technologii.

Jej tablet był pełen programów do analizy struktur danych, a kubek z napisem „czarna godzina" jak zawsze parował świeżo zaparzoną kawą.

– Napisałam algorytm monitorujący stabilność pola nanoukładów – powiedziała, zdalnie podłączając swój sprzęt.

– Jeśli wskaźnik koherencji spadnie poniżej progu, odcina wysoki prąd i zostawia tylko podtrzymanie pamięci, żeby logi przeżyły. To jak?

Gotowy na test, czy będziesz tak grzebał do nocy?

– To nie Xbox. Tu liczy się precyzja – mruknął, sięgając do czerwonego przełącznika z naklejką FAIL-SAFE.

Rdzeń miał dalej zapisywać telemetrię, nawet gdyby reszta poszła z dymem. – Tezeusz pyta o drogę – zabrzmiała zaprogramowana przez niego AI nawigacyjna, o zadziwiającej wprost zdolności do błędów kalibracji fazy i gubienia współrzędnych.

Naraz wszystkie wskaźniki energetyczne zaczęły szaleć, a wykresy na ośmiu ekranach skakać jak sejsmograf w trakcie trzęsienia ziemi – chaotycznie, bez wzoru, z coraz większą amplitudą.

Moduł chłodzenia buchnął parą. Heweliusz-77 zadrżał... i tupnął nóżką.

– To niebezp... – zdążył jeszcze stwierdzić doktor Suchy, zanim wszyscy troje zniknęli w fioletowym rozbłysku międzywymiarowej energii.

Kwantowy skok przeniósł ich do świata ze szklanymi wieżami i statkami napędzanymi bursztynową energią, magazynowaną w ogromnych, żywicznych kondensatorach.

Latające żaglowce przemierzały niebo, kolorowe przekupki zachwalały kolorowe wodorosty, a namolni straganiarze handlowali błyszczącymi kryształkami eteru.

Uciekając przed portowymi strażnikami, drużyna kwantowych rozbitków schroniła się na zapleczu spichlerza „GD".

Mieli nie lada szczęście, bo właśnie tam znaleźli Heweliusza-77. Choć zmalał do rozmiaru kota, jego nanopajęczyna pulsowała równaniami matematycznymi, wizualizując rozkład pola i poprawki, które wprowadzał kontroler.

Podczas gdy Niko kucnął, by odczytać dane z ośmiu malutkich ekranów, doktor Suchy z niepokojem obserwował rosnący fioletowy wir na ścianie pomieszczenia.

– Hm, twoje urządzenie wprowadza chaos w całej sieci rzeczywistości.

– Wszystkie parametry się rozjechały – PegiZu upiła łyk kawy, zwalczając metaliczną suchość w gardle.

– Bez tabletu niechybnie umknie nam szansa na stabilizację... W tym momencie portal ponownie się aktywował.

Drugi skok przeniósł ich do stechnicyzowanego świata, gdzie ludzie z implantami łączyli się z maszynami.

Cyberpunkowa metropolia pulsowała neonowymi światłami, a w powietrzu unosił się metaliczny zapach spalin oraz ozonu z przeciążonych przetwornic i węzłów sieci paraneuronowych.

Ledwie zdążyli rozeznać się w terenie i odnaleźć na pobliskim torowisku pęknięty tablet PegiZu oraz Heweliusza-77 – tym razem podobnego do kolejowej maszyny z ośmioma kołami i tłokami w miejsce nóg – a już przy sąsiednim wagonie pojawiła się niebieskawa poświata.

Zamiast jednak kolejnego portalu, zmaterializowała się przed nimi postać, która sprawiła, że Niko zamarł. To był on!

Profesor Paradox, zwariowany naukowiec-wizjoner, jego niedoszły mentor, który rzekomo zginął przed paru laty.

Migotał jak projekcja rozrywana interferencją: raz ostro, raz w piksele.

– Rozbitkowie, nareszcie! – zawołał. – Ja również tu utknąłem. Chociaż moje ciało się rozpadło, odkryłem sposób, by przetrwać.

Ziemski wymiar to jedyny prawdziwy, a wasze pojawienie się utorowało mi drogę powrotną z tych kwantowych aberracji!

– Ha, wiedziałem, że pan przeżył! – ucieszył się Niko. – To jak mamy się stąd wydostać?

– Bramą jest Trójkąt Trzech Cesarzy – profesor oparł dłoń na stalowym odwłoku Heweliusza-77 – a kluczem – wasze urządzenie.

Obawiam się jednak, że wasza podróż kończy się wraz z innymi światami. Na pocieszenie możecie być świadkami mojej apoteozy!

– Chcesz być bogiem?! – żachnął się doktor Suchy. – Bogowie nie płaczą po nocach nad równaniami!

I nie obarczają innych swoją nieudolnością tudzież niekompetencją!

– Powiedział ten, co nic nie osiągnął! – warknął Paradox, rozwijając swój cybernetyczny węzeł algorytmiczny.

– Nauka to sztuka wyboru między katastrofą a apokalipsą!

Na szczęście PegiZu wykorzystała chwilę nieuwagi szalonego naukowca i podłączywszy swój uszkodzony tablet do Heweliusza-77, w trybie awaryjnym uruchomiła urządzenie.

Zapiszczały tłoki i cylindry. Obróciły się koła. Zanim Paradox zdążył zareagować, maszyna gwałtownie przyspieszyła, pędząc prosto na nich.

W ostatniej chwili zmieniła się jednak w absorbujące przestrzeń holograficzne widmo pociągu.

– Jak kolejowa przygoda przez cyfrowe tory! – parsknął Niko, znikając w portalu.

Wirujący światłotunel rzucił ich do prehistorycznej górskiej krainy, oświetlonej bioluminescencyjnymi grzybami.

Natknęli się tam na istotę przypominającą neandertalczyka, ale obdarzoną niezwykłą inteligencją. Ten niechętny troglodyta zbierał artefakty z różnych wymiarów.

Jego grotę wypełniały skrzynie z przedmiotami pochodzącymi z „Silent City".

– Ja Grunth – burknął. – Wy, homo sapiens, zawsze psujecie równowagę. Wasz profesor chłonie energię wymiarów.

To spowoduje kaskadowy kolaps. Skończymy jak piżmak i reszta. – Wskazał na ścienne malowidło przedstawiające wymowny kres świata chomikowatych.

– Hm, Nikolasie – zauważył Suchy. – Każdy wymiar ma swoją własną częstotliwość kwantową.

Sądzę, że Paradowski próbuje je zsynchronizować, ale to zniszczy ich unikalność.

Niko czuł ciężar winy. To wszystko było winą jego ambicji.

Teraz musiał naprawić swój błąd, nawet jeśli oznaczało to rezygnację z marzeń o sławie... i o powrocie do domu.

Wkrótce Paradox pojawił się ponownie, otoczony czarną poświatą, która zdawała się pochłaniać nie tylko światło, ale i materię.

Dosiadał gigantycznego pająka – Heweliusza-77.

– Patrzcie! Patrzcie tylko! – śmiał się jak dziecko. – Oto wizja mojej boskości!

Niko spojrzał na swoich przyjaciół. Czy byli gotowi ponieść konsekwencje jego działań?

– PegiZu! – zawołał. – Potrzebuję dostępu do centralnego komputera kwantowego!

– Już prawie! O nie! – Uniosła tablet. – Rdzeń nie przyjmuje zdalnych komend!

Z determinacją godną mitycznego Tezeusza Niko zaszarżował na Heweliusza-77. Paradox wydał pająkowi polecenie, ten uniósł ostro zakończone odnóża... i zawahał się, gdy dostał w oko kamieniem rzuconym przez Gruntha.

Niko tymczasem ostatnie metry pokonał ślizgiem; zerwał się z ziemi i sięgnął ręką do błyszczącej szczeliny w głowotułowiu pająka.

Pewnie dosięgłyby go szczękoczułki, gdyby nie „czarna godzina" – to PegiZu wylała swoją cenną kawę na swój jeszcze cenniejszy tablet, doprowadzając do spięcia i przeciążenia.

Kontroler zresetował się i wstał w trybie awaryjnym, cofając parametry do ostatniej stabilnej konfiguracji.

Trzymając swoją dłoń w rdzeniu Heweliusza-77, Niko poczuł algorytmy przepływające przez jego umysł. Zamiast więc niszczyć międzywymiarowe połączenia, stabilizował je.

– Profesorze! – zawołał, przekrzykując huk implodującej przestrzeni. – Prawdziwa nauka to wiedza, kiedy się zatrzymać!

To nie dominacja, tylko harmonia!

– Nie! – Paradox ryknął z wściekłości, gdy jego wizja boskości rozpadła się na kawałki.

Fioletowa eksplozja energii wstrząsnęła całą widzialną i niewidzialną przestrzenią.

Kolaps wymiarów zatrzymał się, a drużyna kwantowych rozbitków została rozrzucona po alternatywnych rzeczywistościach.

Jedynie Niko ocknął się w Sosnowcu, w „Strefie Kreatywnych Mózgów", z pajączkiem Heweliuszem-77 w dłoni.

W pamięci awaryjnej wciąż tliły się logi.

Konkurs już się dla Niko nie liczył. Od odkrywania nowych światów ważniejsza była bowiem mądrość w ich ochronie.

Pytanie tylko, gdzie się podziali jego przyjaciele?

– Tezeusz pyta o drogę. ■

M. P. Hardy

Wielobarwny metal, część 3

Ostatni odcinek artykułu o chromie i chromowcach przeznaczysz na eksperymenty z jego zielonej barwy tlenkiem. Właściwości katalityczne Cr_2O_3 pozwolą na wykonanie kilku doświadczeń, sama synteza tlenku będzie zaś wybuchowa. Przy okazji poznasz perypetie towarzyszące odkrywaniu kolejnych chromowców.

Zanim przejdziesz do doświadczeń, pora na kilka informacji o wykorzystaniu chromowców przez organizmy żywe. Może cię to zdziwić, ale i świat organiczny również skorzystał z właściwości jonów metali grupy 6.

Biokatalizatory

W przeciwieństwie do zdecydowanie szkodliwych związków chromu sześciowartościowego (chromiany, CrO_3), połączenia chromu(III) są przyjazne dla organizmów żywych. Chrom należy do mikroelementów, a jego jony znajdują się w centrach aktywnych enzymów odpowiedzialnych za regulację stężenia glukozy we krwi, przemiany węglowodanów i produkcję insuliny. Niedobór chromu prowadzi do zaburzeń pracy trzustki. Suplementy tego pierwiastka stosowane są w wielu kuracjach odchudzających ze względu na przyspieszenie metabolizmu cukrów i tłuszczów. Zapotrzebowanie na chrom wzrasta podczas wzmożonego wysiłku fizycznego i umysłowego oraz przy diecie bogatej w węglowodany. Łatwo przyswajalny chrom znajduje się w produktach zbożowych z pełnego ziarna, ziemniakach, orzechach i drożdżach. Pamiętaj, że naturalne źródła są zawsze lepszym rozwiązaniem problemów z niedoborem niż suplementy i dlatego przed użyciem tych ostatnich najpierw zasięgnij porady lekarza lub farmaceuty.

Również molibden znajduje się w centrach aktywnych licznych enzymów (w postaci sześciowartościowej), a najważniejsze z nich to nitrogenazy, dzięki którym bakterie brodawkowe wiążą azot z atmosfery. To jeden z kluczowych procesów umożliwiających trwanie życia na Ziemi.

Wybuchowa produkcja

Tlenek chromu(III) Cr_2O_3 to związek o szarozielonej barwie używany jako pigment oraz składnik past polerskich. Jego niewielka domieszka w kryształach korundu Al_2O_3, powoduje, że powstają cenne kamienie szlachetne – ciemnoczerwone **rubiny** (**1**). Podczas prób zbadasz katalityczne właściwości Cr_2O_3, ale najpierw samodzielnie go otrzymasz.

1. Rubiny zawdzięczają swoją barwę tlenkowi chromu(III)

Potrzebnym odczynnikiem będzie dichromian amonu $(NH_4)_2Cr_2O_7$, związek tworzący kryształy o pomarańczowoczerwonej barwie (**2**). Przepis otrzymywania reagenta jest dostępny w wielu książkach oraz w Internecie. Mimo że zakup nie może równać się z satysfakcją samodzielnego otrzymania związku, rozważ również ekonomiczny aspekt przedsięwzięcia. Do wytworzenia potrzebnych ilości odczynnika zużyjesz dużo chemikaliów: kwasu siarkowego, wody amoniakalnej oraz dichromianu potasu. Taniej i zdecydowanie szybciej będzie więc nabyć porcję gotowego związku, do tego nie trzeba posługiwać się stężonym roztworem H_2SO_4 i szkodliwymi połączeniami chromu(VI).

Tlenek chromu(III) powstaje w wyniku rozkładu $(NH_4)_2Cr_2O_7$ przy ogrzaniu do temperatury przekraczającej 200 °C. Ponieważ raz rozpoczęta reakcja samorzutnie biegnie dalej, wystarczy przytknięcie zapalonej zapałki do sproszkowanego związku:

2. Odczynniki do doświadczeń: dichromian amonu i otrzymany z niego tlenek chromu(III)

3. Reakcja w słoiku: tlenek chromu(III) powstający w wyniku rozkładu dichromianu amonu

$$(NH_4)_2Cr_2O_7 \rightarrow Cr_2O_3+N_2+4H_2O$$

Zauważ, że w reakcji zarówno utleniacz (chrom z anionu dichromianowego), jak i reduktor (azot z kationu amonowego) są składnikami tej samej cząsteczki.

W reakcji wydziela się duża ilość produktów gazowych (azot i para wodna), które rozrzucają na wszystkie strony powstający tlenek. Aby nie zanieczyścić otoczenia i nie stracić potrzebnego tlenku, próbę wykonaj w dużej zlewce lub zakręcanym słoju (i najlepiej na zewnątrz mieszkania). Do porcelanowego tygielka lub metalowej zakrętki wsyp sproszkowany odczynnik i wstaw pojemnik na dno naczynia. Pamiętaj o przygotowaniu talerzyka lub zakrętki do przykrycia twojego „reaktora". Do długiego pręcika umocuj zapałkę i podpal nią pomarańczowy proszek w tygielku. Gdy zauważysz, że reakcja się rozpoczęła, zakryj wylot naczynia, ale co chwila uchylaj przykrywkę w celu wypuszczenia tworzących się gazów (**3**). Po zakończeniu doświadczenia dysponujesz próbką Cr_2O_3 do kolejnych eksperymentów. W zakręcanym naczyniu związek można przechowywać dowolnie długo. Po wymieszaniu tlenku z olejem lnianym na gęstą masę otrzymasz pastę polerską, nieustępującą niczym gotowym produktom.

Reakcja rozkładu dichromianu amonu jest podstawą jednego z najbardziej spektakularnych doświadczeń, które możesz wykonać w domowym laboratorium – wybuchu **chemicznego wulkanu**. Dla uzyskania widowiskowego efektu warto wykonać odpowiednią aranżację otoczenia. Zbuduj makietę wulkanu, a gdy pogoda na to pozwoli – stwórz scenografię na otwartej przestrzeni i usyp kopiec z piasku. Na szczycie wulkanicznego stożka wykonaj wgłębienie i umieść w nim naczynie odporne na wysoką temperaturę. W zależności od skali eksperymentu jest to porcelanowy tygiel lub parowniczka, albo też mała metalowa puszka, wypełniona sproszkowanym i dobrze ubitym reagentem. Zainicjuj reakcję przez podpalenie dichromianu amonu zapałką, odsuń się na bezpieczną odległość i podziwiaj efekt doświadczenia. Oprócz wyrzucanych wokół kłębów powstającego tlenku chromu(III) reakcji towarzyszą także czerwone iskry, co znakomicie imituje wybuch prawdziwego wulkanu. Po zakończeniu doświadczenia całe otoczenie – niczym lawą – pokryte jest ciemnozielonym pyłem (**4**). Pokuś się o fotograficzne udokumentowanie eksperymentu, a może nawet go sfilmuj.

W epoce poprzedzającej grafikę komputerową rozkład związku był wykorzystywany jako efekt specjalny w filmach, dzisiaj zaś jest obowiązkowym elementem pokazów chemicznych i pikników naukowych. Dokonania innych

4. Wybuch chemicznego wulkanu w plenerze

chemików możesz obejrzeć po wpisaniu w wyszukiwarce internetowej frazy *chemical volcano*.

Katalizator utleniania

Pora wykorzystać otrzymany tlenek chromu(III). Szczyptę Cr_2O_3 rozetrzyj wraz z cukrem na jednolity proszek, zwilż (ale tylko zwilż) kilkoma kroplami wody lub denaturatu. Powstałą w ten sposób gęstą masą napełnij małą strzykawkę jednorazową z uciętym końcem. Włóż tłoczek i wypchnij fragment sprasowanej mieszaniny, a następnie pozwól jej wyschnąć (**5**). Suchy wałeczek umieść na niepalnym podłożu, np. płytce metalowej lub ceramicznej, i podpal z jednej strony. Pojawia się niewielki płomień, mieszanina topi się i pieni z powodu wydzielania gazowych produktów spalania. Rozżarzona strefa utleniania powoli przesuwa się wzdłuż wałeczka (**6**). Ponieważ reakcji towarzyszy wydzielanie dymu i niezbyt przyjemnego zapachu, wykonaj ją pod sprawnym wyciągiem, a najlepiej na zewnątrz. Po reakcji pozostaje ciemna, stopiona masa – to zwęglone resztki cukru zmieszane z dodanym tlenkiem chromu(III). Eksperyment można zmodyfikować i wykonać w jeszcze prostszy sposób: wystarczy usypać z wymieszanego proszku cukru z Cr_2O_3 ścieżkę i podpalić ją z jednej strony (w pierwszej wersji efekt jest jednak bardziej widowiskowy).

5. Z wilgotnej pasty z tlenku chromu(III) z cukrem formujemy wałeczki, ...

Czy można go tak nazwać?

Pierwiastek 106 został równocześnie otrzymany w roku 1974 przez zespoły fizyków z USA i ZSRR. Początkowo nosił nazwę unnilheks (od numeru porządkowego 106), potem był rutherfordem (od nazwiska odkrywcy jądra atomowego). Zanim ostatecznie w roku 1997 stał się **seaborgiem**, wzbudził liczne kontrowersje – złamano niepisaną zasadę, że nie nadaje się nazw pierwiastków na cześć żyjących osób. Ale akurat Glennowi Seaborgowi („ojciec transuranowców" zmarł dwa lata później) ten zaszczyt słusznie się należał.

Robaczki świętojańskie

W chemicznym laboratorium możesz powtórzyć letni spektakl natury – błyski światła emitowane przez owady z rodziny świetlikowatych. Nie będzie to jednak zimne światło, ich bioluminescencję zastąpi ci reakcja utleniania katalizowana przez tlenek chromu(III). Oprócz tego odczynnika przygotuj porcję wody amoniakalnej (najlepiej stężonego wodnego roztworu NH_3), dużą zamykaną kolbę lub butelkę z szerokim otworem, łyżkę do spalań i palnik. Jeżeli nie masz specjalnej łyżki do spalań, możesz użyć

6. ...które po wyschnięciu i podpaleniu żarzą się w wyniku utleniania cukru

wygiętej małej łyżeczki, którą trzeba trzymać szczypcami lub też rozklepać na końcu kawałek miedzianego drutu tak, aby powstało zagłębienie na ogrzewaną substancję.

7. Chemiczne świetliki w kolbie

Do kolby lub butelki wlej około 10 cm^3 wody amoniakalnej, zamknij wylot naczynia i odstaw je w ciepłe miejsce (w celu przyspieszenia wydzielania amoniaku można wrzucić granulkę wodorotlenku sodu NaOH). W tym czasie na łyżce do spalań ogrzej w płomieniu palnika porcję Cr_2O_3. Po rozżarzeniu tlenku otwórz naczynie z amoniakiem, wsyp zawartość łyżeczki i szybko zamknij wylot. Reakcja utleniania amoniaku (do wolnego azotu, ale powstają również tlenki tego pierwiastka) jest bardzo widowiskowa: cząstki tlenku chromu(III) początkowo tworzą kaskadę iskier, a następnie wirują w naczyniu, świecąc niczym robaczki świętojańskie (**7**). Po zakończeniu próby na dnie butelki leży szarozielony pył Cr_2O_3, a jej wnętrze zasnuwa mgła pary wodnej. Dla uzyskania lepszego efektu przeprowadź eksperyment w zaciemnionym pomieszczeniu.

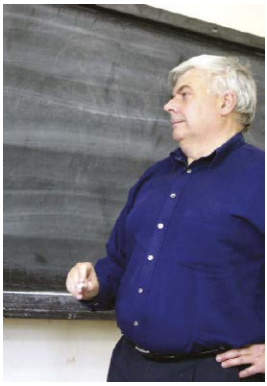
Związki chromu umożliwiają wykonanie jeszcze wielu innych doświadczeń. Do nich potrzeba jednak trudniej dostępnych odczynników oraz warunków, których nie jesteś w stanie zapewnić w swoim domowym laboratorium. Ale nawet opisane w artykule eksperymenty z pewnością pokazały, że chrom to jeden z najciekawszych pierwiastków w twojej pracowni chemicznej. ■

Krzysztof Orliński

Wilcza piana

W Rudawach (Górach Kruszcowych) na obecnym pograniczu Niemiec i Czech górnictwo i hutnictwo kwitło już w średniowieczu. Jednym z poszukiwanych metali była cyna. Hutnicy zauważyli, że gdy w rudzie cyny był obecny pewien czarny minerał, wytop się nie udawał. O niepowodzenie tym razem oskarżono wilki (w przypadku niklu i kobaltu „winne" były górskie chochliki – patrz artykuły z numerów 11 i 12/2021). Czarny minerał otrzymał nazwę wolframit, co można przetłumaczyć jako „wilcza piana" (toczona z pysków drapieżników pożerających cynę) (**8**).
W połowie XVIII wieku w Szwecji również znaleziono minerał towarzyszący rudom cyny. Ze względu na jego duży ciężar właściwy nazwano go tungstenem („ciężki kamień" po szwedzku). W roku 1781 **Karl Wilhelm Scheele**, odkrywca molibdenu (i kilku innych pierwiastków), podziałał kwasem azotowym na tungsten i otrzymał żółty osad tlenku WO_3. Podobnie jak w przypadku molibdenu, Scheele nie zredukował tlenku, dokonali tego dopiero hiszpańscy chemicy bracia **Juan José** i **Fausto de Elhuyar** (1783), którzy wydzielili ten sam tlenek z wolframitu. Minerał tungsten na cześć odkrywcy wolframu zmienił nazwę na szelit, natomiast w przypadku metalu stosowane są dwie nazwy: **wolfram** (oficjalna łacińska nazwa to *Wolframium*) oraz **tungsten** (używają jej m.in. kraje anglojęzyczne i niektóre romańskie). Kariera wolframu rozpoczęła się w XIX wieku, gdy odkryto jego zdolność do utwardzania stali, a na początku XX wieku zastosowano go jako żarnik w żarówkach.

8. Minerały wolframu: u góry scheelit, na dole wolframit (United States Geological Survey, www.usgs.gov)



Z „Młodym Technikiem” jestem związany od półwiecza. Wtedy w naszym kraju można było jeszcze spotkać dinozaura. W 1976 roku opublikowałem w MT artykuł o poszukiwaniu liczb pierwszych – w przededniu eksplozji tej tematyki związanej z metodami szyfrowania wiadomości za pomocą niesamowitych własności tych liczb. Potem przyszła bliższa współpraca. Od 1978 roku pisuję co miesiąc o mojej pięknej matematyce. Chcę i muszę tu podziękować mojemu nauczycielowi matematyki z liceum. Był nim inż. Wacław Chyra (1904–1970) – dowódca kompanii w Powstaniu Warszawskim. Kilkakrotnie podrywał kompanię do straceńczego ataku. Sam przeżył przypadkiem. Kłaniam się nisko, Panie Profesorze.
Na pytanie, jakie mam hobby, odpowiadam, że trzy: 1) matematyka, 2) matematyka, 3) matematyka. Na pytanie o szczęśliwe liczby odpowiadam: 1, 41, 116. Autobusem warszawskiej linii 116 dojeżdżałem do mojej szkoły: warszawskiego Liceum nr 41 im. Joachima Lelewela. Gdy jechałem na egzamin maturalny, podjechał autobus z numerem bocznym 1. Wtedy „jedynka” nie kojarzyła się z oceną niedostateczną, lecz miała raczej znaczenie: „będziesz pierwszy”. Udało się. Zdałem maturę!
Piszę zatem o matematyce. Przenika ona nasze życie. Uczy myślenia, precyzji i spokoju. Nie rozwiązuje naszych codziennych problemów, ale daje nadzieję na ciekawe życie. Dorastają już Czytelnicy „Młodego Technika”, którzy będą żyć w XXII wieku. Zainteresujcie się matematyką.

Wszystko o mexie

Gdy edytor tekstów, którym się posługuję, „zobaczył” tylko tytuł artykułu, natychmiast zmienił pierwszą literę słowa „mex” – Czytelnicy z pewnością domyślą się, na jaką. No cóż – w moim wieku nawet już nie wypada pisać o tym, co sobie pomyślał edytor. Mex to nazwa pewnej funkcji matematycznej. Bardzo prostej i bardzo użytecznej. Ale moje pierwsze skojarzenie przeniosło mnie w odległe czasy – nawet szkolne.

Mieszkałem w Warszawie niedaleko centrali handlu zagranicznego „Metalexport”. Pamiętam ogromny budynek a na nim duży, czerwono-niebieski neon „MEX” – znak firmowy centrali. Chociaż to odległe od matematyki, przypomnę, że w czasach PRL eksport odbywał się za pomocą central handlowych. Fabryki produkowały, Metalexport sprzedawał. Z jednej strony uwalniało to fabrykę od kłopotów ze znalezieniem kontrahentów, z drugiej strony hamowało przedsiębiorczość i innowacyjność, bo centrale trzymały firmy „na krótkiej smyczy”.

Rysunek 1. Metalexport – potęga PRL w handlu maszynami

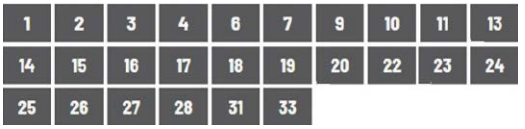
***

Funkcja **mex** jest określona nadzwyczaj prosto. Sama nazwa wyjaśnia, o co chodzi: minimal excluded value, najmniejsza liczba wykluczona. Wartość tej funkcji dla ciągu liczb naturalnych to najmniejsza liczba, której w tym ciągu nie ma. Należy tylko pamiętać, że do liczb naturalnych tutaj zaliczamy również zero. Przykłady wyjaśnią wszystko od razu:
mex (0, 2, 4, 5) = 3, **mex** (1, 2, 3, 4, 5) = 0, **mex** (0, 2, 4, 6, 8, 10) = 1

Jak widać, bardzo jest to proste. Ale oto pierwsze ćwiczenie – choć raczej dla mieszkańców stosunkowo dużych miast.

Zadanie 1. Jeżeli w Twoim mieście są tramwaje, to linie mają swoje numery. Dołącz to tych numerów liczbę 0 i podaj wartość funkcji **mex** dla tak rozszerzonego zbioru liczb.

Często zadaniach matematycznych najtrudniej jest tylko zrozumieć, o co chodzi – potem już jest łatwo. Tutaj po krótkiej chwili na pewno wszyscy pojmą, że pytam o najmniejszą liczbę, która nie jest numerem żadnej linii tramwajowej. Rozwiązanie dla Warszawy: **mex** = 5 (**rysunek 2**).



Rysunek 2. Tabela ze strony WTP, Warszawskiego Transportu Publicznego

W Poznaniu jest oczywiście porządniej, tam **mex** = 20. Znaczy to, że zwykłe, dzienne linie tramwajowe mają tam numery po kolei, od 1 do 19. Wartość **mex** w Gdańsku to 1 (nie ma linii numer 1). Przypomnę tylko, że dołączyliśmy zero. To tak, jakby stworzyć linię numer 0. Piszący te słowa pamięta linię 0 w Krakowie – lilipucie wagony mieściły się pod Bramą Floriańską!

***

Przejdźmy do bardziej matematycznych zadań, które posłużą nam do oswojenia się z mexem.

Zadanie 2. Określmy ciąg tak. Początkowym wyrazem jest $a_0 = 0$, a kolejne określone są wzorem rekurencyjnym: $a_{n+1} = \mathbf{mex}(a_0, a_1, a_2, \ldots, a_n)$. Co to za ciąg?

Zobaczmy. Za każdym razem bierzemy **mex** od już otrzymanego ciągu kolejnych wyrazów. Wyrazem a_1 jest zatem **mex**(0) = 1, wyrazem $a2$ jest **mex**(0,1) = 2, wyrazem $a3$ jest **mex**(0,1,2) = 3. To po prostu kolejne liczby naturalne.

Zadanie 3. Określmy ciąg tak. Początkowym wyrazem jest $a_0 = 0$, następnym 1, a kolejne określone są wzorem rekurencyjnym: $a_{n+1} = \mathbf{mex}(a_{n-1}, a_n)$. Co to za ciąg?

Tu jest ciekawie. Za każdym razem bierzemy **mex** z dwóch ostatnich wyrazów ciągu, a więc $a_3 = \mathbf{mex}(0,1) = 2$, $a_4 = \mathbf{mex}(1,2) = 0$, $a_5 = \mathbf{mex}(2,0) = 1$. Otrzymujemy ciąg okresowy 0, 1, 2, 0, 1, 2, 0, 1, 2, ...

***

Funkcja **mex** jest nieoceniona w teorii gier. Nie nadaje się do wszystkich gier, w szczególności do losowych ani do dwu- albo wielostronnych. Wyjaśnię, o co chodzi. Grę nazywamy bezstronną, jeżeli – w pewnym uproszczeniu – każdy z graczy może wykonać ruch dowolnymi pionkami. Taką grą nie są szachy, bo każdy z graczy wykonuje ruch tylko swoimi figurami.

Zacznijmy od bardzo prostej gry. Tak prostej, że nawet nie zasługuje na tę nazwę. Mamy stos pionków (guzików, żetonów, monet). Wyjmujemy na przemian po jednej. Wygrywa tej, kto weźmie ostatnią. Zanim zaczniemy grać, wiemy kto wygra. Jeżeli liczba monet jest nieparzysta, wygrywa zaczynający, jeżeli parzysta – ten, na kogo przypada drugi ruch.

Inaczej jest, gdy w każdym ruchu mamy wybór: możemy wziąć jedną, albo dwie monety. Na użytek tego artykułu nazwę ją **BIERZ 1 – 2**. Po niedługiej analizie możemy dojść do wniosku, że w dwóch trzecich przypadków strategię zwycięską ma zaczynający, a ten drugi – tylko w jednej trzeciej. Na przykład dla $n = 3$ (trzy monety) gracz zaczynający może wziąć jedną lub dwie monety i niezależnie od tego ruchu drugi bierze resztę. Gdy liczba monet jest niepodzielna przez 3, gracz bierze jedną albo dwie monety i stawia przeciwnika w pozycji przegranej – bo podzielnej przez 3.

Można to wyjaśnić właśnie za pomocą tak zwanej funkcji Sprague-Grundy, tutaj określonej prosto za pomocą **mex**. To najważniejsza myśl tego artykułu.

> Dla każdej kombinatorycznej i bezstronnej gry istnieje dopasowana do niej funkcja G, mająca tę własność: jeżeli jej wartość dla pewnej pozycji jest różna od zera, to jest to pozycja wygrywająca dla gracza, na którego przypada ruch. Jeżeli wartość ta jest równa zero, to wygrywamy tylko wtedy, gdy przeciwnik zrobi błąd.

Poświęcę trochę miejsca historii tego odkrycia. Wpadli na nie niezależnie w latach trzydziestych XX wieku niemiecki matematyk Roland Sprague (1894–1967) i brytyjski Patrick Michael Grundy (1917–1959). Gry matematyczne były popularne w końcu XIX i na początku XX wieku, ale dopiero po upływie 30...40 lat matematyka „dojrzała" do zajmowania się nimi. To wyjaśnia, dlaczego odkrycia mogły następować niezależnie. To znane zjawisko w każdej nauce: nagle pewne tematy stają się modne i dostępne dla nowych metod. Ale i tak do lat siedemdziesiątych XX wieku były to „niszowe zagadnienia" – do kolejnego przełomu. Po upowszechnieniu się metod komputerowych teoria gier stała się ważnym działem matematyki. Nie dlatego, żeby ułatwiać życie graczom, a dlatego, że w języku teorii gier można atrakcyjnie sformułować (i rozwiązać) niektóre zagadnienia z ekonomii, planowania, strategii itp.

Dla naszej prostej gry mamy G(0) = 0. To jasne: jeżeli nie ma już monet, to nie mamy ruchu (a więc przegraliśmy), a G(1) jest równe 1, bo mamy jeden ruch: zabieramy pionek (monetę) i wygrywamy. Następne wartości określamy tak G(n+1) = **mex** (G(n–1), G(n)). Co nam to przypomina? Ależ

oczywiście – ciąg z zadania 3. Wszystko się zgadza: co trzecia pozycja wyjściowa jest przegrana.

Niezerowe wartości funkcji G mierzą też siłę pozycji. Im większa wartość funkcji G, tym większa jest nasza przewaga – chociaż trudno to ściśle ująć, w szczególności dla tak prostej gry. Gdy komputery zaczęły grać w szachy, algorytmy opracowywano na zasadzie przewidywania kolejnych ruchów, ale szybko zaczęto właśnie poszukiwać funkcji, która mierzy siłę każdej pozycji. Im lepsza funkcja, tym lepszy algorytm. Ale my wracamy do prostych gier, nad którymi mamy pełną kontrolę.

***

Polskie prawo nie zabrania jednoczesnego posiadania dwóch kochanek (kochanków), a nawet narzeczonych jednocześnie. Podkreślam, że chodzi mi tylko o stronę prawną. Natomiast jeśli chodzi o małżeństwo, to już trzeba się decydować. Basia albo Zosia. Daniel albo Maurycy. Podobny wybór daje znak drogowy C-8. Decyduj się, kierowco.

Rysunek 3. Znak drogowy C-8

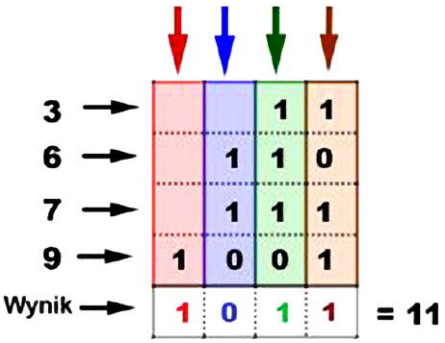
Nazywa się to alternatywą wykluczającą: albo – albo. W Kentucky Fried Chicken jest oferta „Wielkiej dolewki". Kupujesz ją i możesz nalać sobie Pepsi, Fantę, Sprite, Ice Tea i może coś jeszcze. Może być mieszanka: trochę tego, trochę tego. W MacDonald stosują alternatywę wyłączającą: możesz wziąć kawę albo herbatę; ale nie jedno i drugie.

W logice symbolem fałszu jest 0, prawdy 1. Alternatywą wykluczającą rządzi zatem arytmetyka binarna: 0 + 0 = 0, 0 + 1 = 1+ 0 = 1, 1+1 = 0. Jest to dokładnie tak samo, jak z przełącznikiem włączone-wyłączone. Jednokrotne naciśnięcie coś włącza, powtórne wyłącza.

Żeby to nam nie myliło się z dodawaniem w życiu codziennym (gdzie jedna porcja lodów plus druga porcja lodów są to dwie porcje), to takie dodawanie, gdzie 1 plus 1 to 0, oznaczamy inaczej, zwykle plusem w kółeczku: $1 \oplus 1 = 0$.

Czytelnicy tego działu doskonale wiedzą, co to są liczby binarne (dwójkowe), a raczej liczby zapisane w układzie dwójkowym. Ciąg 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, ... w zapisie dwójkowym wygląda tak: 0, 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, 1011, 1100, ... Komputer lubi zera i jedynki. To rozumie i to łyka z zadowoleniem.

Skoro $1 \oplus 1 = 0$, to ile będzie równe na przykład $110 \oplus 101$? Gdyby to był zwykły plus, „bez kółeczka", to zamienilibyśmy dwójkowe 110 + 101 na dziesiątkowe 6 + 5 = 11, a więc wynikiem byłaby dwójkowo zapisane liczba 11, czyli 1011. Ale nasze działanie jest inne. Można powiedzieć tak: dodajemy binarnie w słupkach, ale bez przenoszenia. Przykład (**rysunek 4**) wyjaśni to znacznie lepiej, niż tekst. W każdym słupku dodajemy binarnie, ale oddzielnie. Słupki są oddzielone stalową barierą i nic się da przenieść. Okazuje się, że $3 \oplus 6 \oplus 7 \oplus 9 = 11$.



Rysunek 4.

Poćwiczmy, bo za chwilę to się przyda:
$1 \oplus 2 = 3$, $1 \oplus 3 = 2$, $2 \oplus 3 = 1$, $2 \oplus 2 = 0$, $2 \oplus 3 = 1$, $2 \oplus 3 = 1$, $5 \oplus 8 = 9$.

Obliczmy $2026 \oplus 2027$. Możemy obyć się bez długich obliczeń. W rozwinięciu dwójkowym liczby te różnią tylko jednym bitem na końcu. Liczba 2026 jest parzysta, a więc ma „na końcu" zero. Liczba 2027 jest nieparzysta, ma więc na końcu jedynkę. Pozostałe cyfry są takie same. Przy dodawaniu metodą „plus w kółeczku" zawsze dadzą 0. Widzimy, że $2026 \oplus 2027 = 1$.

***

Wszystko to przyda nam się do analizy gry, która jest bardzo podobna do BIERZ 1–2, ale pewna drobna różnica czyni ją i ciekawszą, i trudniejszą. Oto przykładowe ustawienie do gry

Rysunek 5.

(**rysunek 5**): klocki ustawione na linii, ale nieregularnie – z odstępami. Staramy się je strącić – przewrócić.

Gra jest matematyczna, zakładamy więc, że i ja, i mój przeciwnik (a raczej partner, bo przecież bawimy się wspólnie) rzucamy bardzo dobrze i nie zdarzają nam się pudła. Trafiamy w co zamierzyliśmy trafić. Reguły gry są takie, że możemy przewrócić jeden pionek, albo dwa sąsiednie. To jest właśnie ta różnica – sąsiednie. Wygrywa ten, kto przewróci ostatni pionek. Możemy grać i na kartce papieru: po prostu skreślamy zaznaczone uprzednio kropki.

Zacznijmy analizę. Szukamy funkcji Grundy'ego G. Gdy nie ma pionków, to już przegrałem, zatem G(0) =0. Gdy zostaje jeden pionek, to strącam go i wygrałem. Przyjmujemy, że G(1) = 1.

Nasza gra ma zasadniczą cechę, która pozwala obliczyć funkcję Grundy'ego. Spójrzmy jeszcze raz na rysunek 5. Każdy zespół klocków daje niezależną grę, właśnie dlatego, że nie możemy strącać klocków z różnych grup. Jeden albo dwa sąsiednie, ale z tej samej grupy. Gra rozpada się na mniejsze składniki. Nazywamy to sumą prostą gier i oznaczamy symbolem $\oplus$. Gra na rysunku 5 to zatem

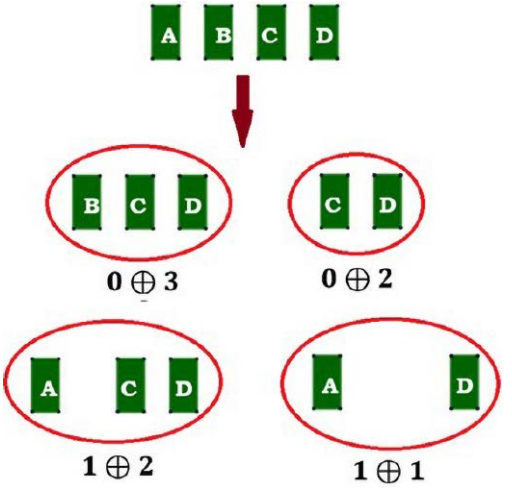
$$2 \oplus 3 \oplus 5 \oplus 1 \oplus 1$$

Zdumiewający wzór Sprague'a i Grundy'ego wygląda na pierwszy rzut oka mało ciekawie, ale wyróżnię go kolorem, bo z niego wszystko wynika

$$G(a \oplus b) = G(a) \oplus G(b)$$

To właśnie pozwala obliczyć, jaka pozycja jest wygrywająca dla jednego czy drugiego gracza. Zobaczmy to dla układu z rysunku 5. Musimy obliczyć G(1), G(2), G(3) i G(5). Wchodzi funkcja **mex**. Dla poprzedniej gry mieliśmy G(0) = 0, G(1) = 1, G(2) = 2. Teraz jednak zaczynają się różnice. Gdy mamy grę 3 (trzy klocki obok siebie), to możemy przewrócić klocek końcowy, dwa sąsiednie, albo środkowy. W pierwszym przypadku zostają dwa klocki (a wiemy już, że G(2)= 2), w drugim jeden klocek (a wiemy, że G(1) = 1), a w trzecim dwa skrajne (a to daje wartość gry równą 0). Wartością naszej gry dla trzech klocków jest zatem **mex** (0,1,2) = 3. W szczególności jest to pozycja wygrywająca dla nas, to znaczy dla gracza, na którego przypada ruch.

Dążymy do obliczenia G(5). Odbywa się to rekurencyjnie, to znaczy musimy najpierw



Rysunek 6. Diagram do obliczenia G(4)

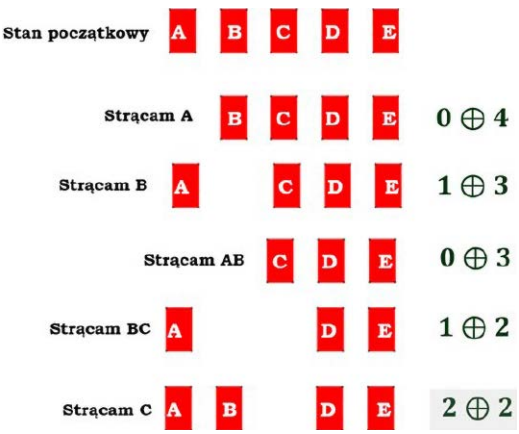
wyznaczyć G(4). Z diagramu na **rysunku 6** odczytujemy możliwości, jakie mogą wystąpić po rzucie, strącającym jeden albo dwa klocki. Kolejno są to przewrócenia A, AB, B i BC. Nie trzeba rozpatrywać innych możliwości, bo na przykład strącenie klocka D, bo jest to układ symetryczny do przewrócenia A.

Wzór Grundy'ego daje kolejno

$$G(0) \oplus G(3) = 0 \oplus 3 = 3$$
$$G(0) \oplus G(2) = 0 \oplus 2 = 2$$
$$G(1) \oplus G(2) = 1 \oplus 2 = 3$$
$$G(1) \oplus G(1) = 1 \oplus 1 = 0$$

Otrzymujemy więc G(4) = **mex** (3, 2, 3, 0) = 1. Dla G(5) mamy już więcej możliwości (**rysunek 7**). Obliczamy łatwo, że G(5) = 4.

***



Rysunek 7.

Mamy już teraz pełną kontrolę nad grami, w których nie ma dłuższych szeregów niż „pięciokloc-kowe”. Zobaczmy to na ustawieniu z rysunku 5:

$$G(2) \oplus G(3) \oplus G(5) \oplus G(1) \oplus G(1) =$$
$$2 \oplus 3 \oplus 4 \oplus 1 \oplus 1 = 5$$

Końcowy wynik 5 to rezultat dodania „bit po bicie” liczb dwójkowych 10, 11, 100, 1, 1. Mamy zatem pozycję wygrywającą. Aby jej nie zaprzepaścić, musimy wykonać taki ruch, żeby przeciwnika postawić w sytuacji G = 0. Można to zrobić, strącając skrajny klocek w „piątce”. Powstaje wtedy sytuacja

$$G(2) \oplus G(3) \oplus G(4) \oplus G(1) \oplus G(1) =$$
$$2 \oplus 3 \oplus 1 \oplus 1 \oplus 1 = 0$$

Jest to zatem pozycja przegrywająca dla gracza *B*. Cokolwiek zrobi, nie wygra (oczywiście pod warunkiem, że *A* będzie grał mądrze).

***

Sądzimy, że nawet jaskiniowcy w coś grywali, a gry starożytnych Rzymian doczekały się naukowych opracowań. Co się dzieje, teraz gdy wszystko siedzi w smartfonach – wiemy. Z niektórych gier nic nie wynika – oprócz zabawy. Niektóre pochodzą z realiów życiowych, a jeszcze inne znajdują poważne zastosowania, choćby w ochronie naszych danych osobowych. Walka z cyberprzestępczością to przecież też gra. O tym za miesiąc. ■

Michał Szurek

Oto zadania dla Czytelnika. Odpowiedzi są „gdzieś w numerze”.

Zadanie 1. Wykaż, że jeżeli *a*, *b*, *c*, *d*, *e*, itd. są liczbami mniejszymi niż 5, to początkowa pozycja

$$5 \oplus a \oplus b \oplus c \oplus d \oplus e \oplus \ldots$$

jest wygrywająca dla gracza *A* (zaczynającego).

Zadanie 2. Czy pozycja z poniższego **rysunku 8** jest wygrywająca, czy przegrywająca dla gracza, na którego przypada ruch?

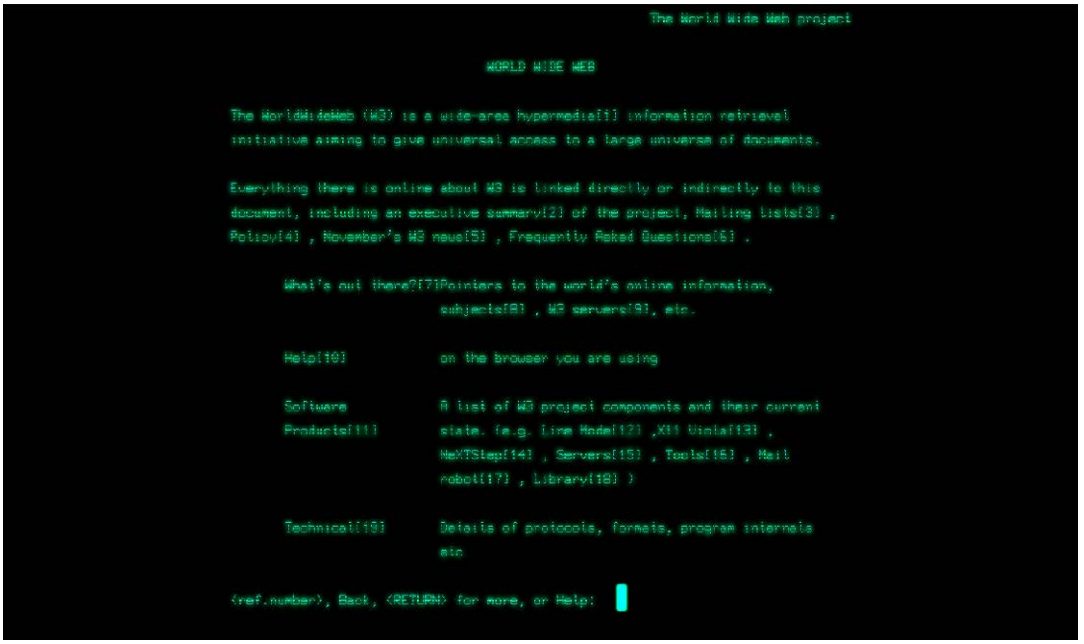
Rysunek 8.

Zadanie 3. Wykaż, że szereg dowolnie wielu klocków stojących obok siebie (bez odstępów) jest pozycją wygrywającą. Można powiedzieć, że aby gra była ciekawsza, trzeba ustawić klocki zupełnie inaczej – z odstępami.

Zadanie 4. Jest wiele wariantów opisanej gry. Zagraj w taki oto. Gdy trafiasz w jakiś klocek, to przewraca się nie tylko on sam, ale i sąsiednie – oczywiście te, które nie są oddzielone przerwą. Jak poprzednio, wygrywa ten, kto ma ostatni rzut. Stwórz funkcję Grundy'ego dla tej gry, oceń pozycję z rysunku 8 i doradź graczowi, jak ma grać, żeby wygrać.

Ciekawski pyta. Wiki odpowiada. Dziś temat wyjątkowy – bo dotyczy czegoś, co zmieniło cywilizację bardziej niż samochód, telewizja i lot na Księżyc razem wzięte. Ale przez pierwsze dwadzieścia lat istnienia było tylko wojskowym projektem, o którym nikomu nie śniło się powiedzieć rodzicom.

Redaktor X



Zrzut ekranu pierwszej strony internetowej wyświetlonej za pomocą symulatora przeglądarki w trybie liniowym – dostępna pod adresem https://line-mode.cern.ch/www/hypertext/WWW/TheProject.html

Nikt tego nie planował, a jednak tu jest

Skąd się wziął internet?

Sputnik, strach i dobry pomysł

Ciekawski: Wiki, powiedz mi, kto wpadł na pomysł internetu. Jeden człowiek? Jeden kraj? Jedna firma?

Wiki: Żadne z powyższych. To jeden z tych przypadków, gdy wynalazek był odpowiedzią na konkretny strach. A strach nazywał się Sputnik.

Ciekawski: Rosyjski satelita z 1957 roku?

Wiki: Dokładnie. Kiedy Sowieci wystrzelili pierwszego satelitę na orbitę, Ameryka doznała szoku. Jeśli Rosjanie mogą wysłać coś w kosmos, mogą też wysłać bombę atomową na Waszyngton. Kongres powołał agencję DARPA – Defence Advanced Research Projects Agency. Jej zadanie: technologia, która da Ameryce przewagę. Każda. Jakakolwiek.

Ciekawski: I DARPA wymyśliło internet?

Wiki: DARPA sfinansowało projekt. Pomysł przypisuje się kilku osobom, ale kluczowy był J.C.R. Licklider – psycholog i informatyk, który w 1963 roku napisał wewnętrzną notatkę do kolegów. Tytuł: „Membership and Goals for an Intergalactic Computer Network". Opisywał w niej komputery połączone na całym świecie, gdzie każdy ma dostęp do każdej informacji. W 1963 roku. Gdy typowy komputer zajmował całe piętro budynku.

Ciekawski: I ktoś to przeczytał i powiedział „tak, róbmy to"?

Wiki: Kilka osób. Ale najpierw trzeba było rozwiązać problem podstawowy: jak połączyć komputery tak, żeby sieć przeżyła atak atomowy? Jeśli jedno miasto zostanie zbombardowane, reszta musi działać. Z tego wojskowego wymagania narodził się genialny pomysł, bez którego internet by dziś nie istniał.

Licklider w 1963 roku opisał internet z dokładnością do szczegółów. Nikt nie wierzył, że to możliwe. On też nie wiedział jak. Wiedział tylko, że to powinno powstać.

Ciekawski: I internet tak działa?

Wiki: Dość dosłownie. Każda wiadomość, zdjęcie, film, strona internetowa – wszystko jest cięte na pakiety. Każdy pakiet jedzie najlepszą dostępną w danej chwili trasą. Na końcu składają się z powrotem w całość. Jeśli jeden węzeł sieci zostaje zbombardowany lub unieruchomiony, pakiety po prostu obierają inną trasę. Sieć jest niezniszczalna.

Wiki-Fiszka: J.C.R. Licklider (1915–1990)
Psycholog i informatyk, który jako pierwszy sformułował wizję „sieci galaktycznej" komputerów. Kierując oddziałem informatycznym DARPA, finansował badania, które prowadziły wprost do ARPA-Net. Nigdy nie napisał linii kodu ani nie zbudował żadnej sieci. Zmienił świat pytaniami i notatkami.

Pakiety – geniusz prostoty

Ciekawski: Więc jak się łączy komputery tak, żeby sieć przeżyła bombę?

Wiki: Wymyślił to Paul Baran w RAND Corporation w 1964 roku. Pomysł nazywa się „przesyłaniem pakietów" i jest tak prosty, że trudno uwierzyć, że nie wpadł na to nikt wcześniej.

Ciekawski: To znaczy?

Wiki: Klasyczny telefon działa tak: dzwonisz do kogokolwiek, centrala rezerwuje dla was obu wyłączną żyłę kabla od jednego do drugiego. Nikt inny nie może jej używać, dopoki rozmawiasz. To się nazywa przełączanie obwodów. Drogie, nieefektywne i – jeśli bomba przetnie kabel – gotowe.

Ciekawski: A pakiety są inne?

Wiki: Zupełnie inne. Wyobraź sobie, że chcesz wysłać koledze książkę pocztą. Zamiast wysłać całą książkę w jednej paczce, rozrywaasz ją na 200 kartek, każdą wkładasz do osobnej koperty z numerem strony i adresem docelowym. Każda koperta jedzie inną trasą, przez inne miasta. Na miejscu kolega składa je po kolei. Jeśli jedna koperta zniknie – prosisz o ponowną i tyle.

Ciekawski: To prosty pomysł.

Wiki: Najprostsze pomysły są najtrwalsze. W 1969 roku ARPANET (*Advanced Research Projects Agency Network*) – pierwsza sieć oparta na pakietach – połączyła cztery amerykańskie uczelnie. Pierwsza wiadomość brzmiała: „lo". Miało być „login", ale serwer padł po dwóch literach. Nawet pierwsze słowo internetu było błędem systemu.

TCP/IP – język wszystkich sieci

Ciekawski: Dobra, mamy ARPANET. Ale internet to nie jest tylko amerykańska sieć wojskowa. Jak sieć z kilku uczelni stała się światową infrastrukturą?

Wiki: Tu pojawia się problem, który można nazwać problemem Wieży Babel. Każda sieć komputerowa na świecie mówiła własnym językiem. ARPANET, sieci uniwersyteckie, sieci wojskowe różnych państw – nie umiały się ze sobą porozumieć.

Ciekawski-Tip
Pierwszy e-mail wysłał Ray Tomlinson w 1971 roku – do samego siebie, między dwoma komputerami stojącymi obok siebie w tym samym pokoju. To on wymyślił używanie znaku @ do oddzielenia nazwy użytkownika od nazwy komputera. Zapytany, co napisał w pierwszym e-mailu, odpowiedział: „nie pamiętam, coś bez znaczenia".

Ciekawski: I kto to naprawił?

Wiki: Vint Cerf i Bob Kahn. W 1974 roku opublikowali protokół TCP/IP (*Transmission Control Protocol/Internet Protocol*) – wspólny język dla wszystkich sieci na świecie. Pomyśl o tym jak o języku angielskim dyplomacji: nie musisz porzucać własnego języka ojczystego, ale kiedy chcesz mówić do wszystkich – mówisz po angielsku. TCP/IP to język angielski internetu.

Ciekawski: I wszyscy się zgodzili, żeby go używać?

Wiki: Nikt im za to nie zapłacił. Nikt ich nie zmusił. Opublikowali protokół jako wolny standard – każdy mógł go wziąć i użyć. W 1983 roku ARPANET oficjalnie przełączył się na TCP/IP. Tę datę – 1 stycznia 1983 – niektórzy uważają za oficjalne urodziny internetu. Nie było tortów ani przemowień. Była zmiana protokou węzłow sieci.

Sir Timothy John Berners-Lee (Paul Clarke – Praca własna, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=37435469)

> **Cerf i Kahn nie opatentowali TCP/IP. Nie założyli firmy. Nie zarobili miliarda dolarów. Po prostu opublikowali i powiedzieli: „weźcie, jeśli chcecie".**

Berners-Lee i pajęczyna

Ciekawski: Mamy internet od 1983 roku. Ale moi rodzice mówią, że „interunet był w latach 90". Co się stało między 1983 a 1993?

Wiki: Internet i World Wide Web to dwie różne rzeczy. I to jedno z najczęściej mieszanych pojęć w historii technologii.

Ciekawski: Naprawdę? Wydawało mi się, że to to samo.

Wiki: Internet to infrastruktura – globalna sieć komputerów połączonych protokołem TCP/IP. Istniał od 1983 roku i służył głównie naukowcom do wysyłania plików i e-maili. World Wide Web to aplikacja działająca na internecie – system stron internetowych połączonych odnośnikami. To tak jak różnica między autostradą a samochodem. Autostrada istniała. Samochód dopiero powstał.

Ciekawski: I kto zbudował samochód?

Wiki: Tim Berners-Lee. Brytyjski fizyk pracujący w CERN w Genewie. W 1989 roku napisał do swojego szefa propozycję systemu, który pozwoliłby naukowcom ze wszystkich krajów łatwo dzielić się dokumentami. Szef Mike Sendall napisał na marginesie: „Vague but exciting" – mętne, ale ekscytujące. I dał zgodę.

Ciekawski: Jak to działało?

Wiki: Berners-Lee wymylił trzy rzeczy: HTML (*Hyper Text Markup Language*) – język do pisania stron, HTTP (*Hyper Text Transfer Protocol*) – protokół do ich przesyłania i URL (*Uniform Resource Locator*) – adres każdej strony. 6 sierpnia 1991 roku uruchomił pierwszą stronę www na świecie pod adresem info.cern.ch. Działa do dziś. Możesz ją odwiedzić.

Ciekawski: I to był moment, gdy wszystko eksplodowało?

Wiki: Prawie. Jeszcze dwa lata była dostępna tylko dla naukowców, bo przeglądarki były tekstowe – same litery, zero zdjęć. W 1993 roku student Marc Andreessen wydał Mosaic – pierwszą przeglądarkę ze zdjęciami. W ciągu roku liczba stron www wzrosła z kilkuset do dziesiątek tysięcy. Wtedy rodzice Twoich rodziców po raz

Wiki-Fiszka: Vint Cerf i Bob Kahn – ojcowie internetu

Vinton Cerf (ur. 1943) i Robert Kahn (ur. 1938) opracowali protokół TCP/IP w 1974 roku. W 2004 roku obaj otrzymali Nagrodę Turinga – odpowiednik Nobla w informatyce. Cerf pracuje do dziś jako „Główny Ewangelista Internetu" w Google. Ma częściowy niedosłuch od urodzenia – to on jest współodpowiedzialny za to, że protokóły internetowe od początku obsługiwały pisane wiadomości tak samo dobrze jak głos.

pierwszy usłyszeli słowo „internet”.

Czego nie przewidział żaden futurolog

Ciekawski: Chcę zapytać o coś innego. Lata 60. pełne były wizji przyszłości: latające samochody, kolonie na Marsie, roboty w każdym domu. Dlaczego nikt nie przewidział internetu?

Wiki: To jest jedno z najtrafniejszych pytań, jakie można zadać o historii technologii. I odpowiedź jest intrygująca.

Ciekawski: Bo?

Wiki: Futurolodzy lat 60. myśleli kategoriami fizycznymi: szybsze samoloty, mocniejsze rakiety, większe maszyny. Nawet ci, którzy myśleli o komputerach, wyobrażali sobie je jako potężne centra obliczeniowe obsługiwane przez specjalistów. W 1977 roku prezes Digital Equipment Corporation Ken Olsen powiedział wprost: „nie ma żadnego powodu, dla którego ktokolwiek chciałby mieć komputer w domu”.

Ciekawski: Ale chyba ktoś to przwidział?

Wiki: Vannevar Bush w 1945 roku opisał w eseju hipotetyczną maszynę „Memex” – biurko, w którym człowiek przechowuje wszystkie książki, nagrania i korespondencję, i może przez nie nawigować za pomocą powiązań. To dosłowny opis strony internetowej z hiperlinkami, napisany 46 lat przed WWW. Ale Bush nie wiedział, jak to zbudować. I nikt nie traktował tego poważnie.

Ciekawski: A co z Arthurem Clarkiem? Asimovem? Pisarzami science fiction?

Wiki: Clarke przewidział satelity komunikacyjne – i miał rację. Asimov wyobrażał sobie potężne komputery zarządzające planetą. Ale żaden z nich nie przewidział tego, co okazało się rewolucją: że każdy człowiek dostanie głos. że nastolatek w Nairobi będzie mógł czytać to samo co profesor w Oksfordzie. że pornografia i nauka, propaganda i prawda, geniusz i głupota będą istniały na tej samej platformie. Nikt nie przewidział demokratyzacji informacji.

Ciekawski: Bo to brzmi zbyt prosto.

Wiki: Właśnie. Największe rewolucje technologiczne nie są spektakularne z zewnątrz. Druk Gutenberga to kawałek metalu i atrament. Internet to mikroelektronika i protokoły. Oba zmieniły świat bardziej niż wszystkie rakiety razem wzięte.

Ciekawski-Tip

Tim Berners-Lee nie opatentował World Wide Web. Przekazał swoje wynalazki – HTML, HTTP i URL – całemu światu za darmo w 1993 roku. Gdyby opatentował, każda odwiedzana strona internetowa wiązałaby się z płaceniem licencji. Wielokrotnie pytano go, czy nie żałuje. Odpowiadał: nie.

W 1995 roku Newsweek opublikował artykuł pod tytułem: „Internet? Bah!”. Autor dowodził, że internet nigdy nie zastąpi książek, gazet ani telewizji. Artykuł można dziś przeczytać w internecie.

Suwak czasu internetu	
1945	Vannevar Bush opisuje „Memex” – hipotetyczną maszynę łączącą dokumenty. Nikt nie bierze tego poważnie.
1957	Sputnik. USA powołuje DARPA.
1969	ARPANET – pierwsza wiadomość między UCLA a Stanford. Pada serwer po literach „lo”.
1971	Pierwszy e-mail. Ray Tomlinson wysyła wiadomość do samego siebie przez dwa komputery obok siebie.
1974	Cerf i Kahn publikują TCP/IP. Wspólny język dla wszystkich sieci.
1983	ARPANET przełącza się na TCP/IP. Oficjalny początek internetu.
1989	Tim Berners-Lee proponuje World Wide Web w CERN. Szef pisze na marginesie: „Vague but exciting”.
1991	Pierwsza strona WWW online: info.cern.ch. Działa do dziś.
1993	Mosaic – pierwsza przeglądarka z obrazkami. Internet staje się wizualny.
1998	Google. Larry Page i Sergey Brin w garażu.
2007	iPhone. Internet w kieszeni.
2026	5,5 miliarda użytkowników internetu. 70% ludzkości.

Co dalej – czyli czego nie wiemy

Ciekawski: Ostatnie pytanie. Skoro nikt nie przewidział internetu – co to mówi o tym, czego teraz nie przewidujemy?

Wiki: To pytanie warte więcej niż wszystkie moje dane razem wzięte. Historia internetu uczy jednej rzeczy: prawdziwe rewolucje nie wychodzą od wielkich korporacji ani rządów. Wychodzą od ludzi, którzy publikują swoje pomysły za darmo, bo wierzą, że świat na tym skorzysta.

Ciekawski: Berners-Lee, Cerf, Kahn – wszyscy oddali to za darmo.

Wiki: Wszyscy. I za każdym razem świat zastanawiał się: po co? Czy też na tym zarobisz? Nie zarobili. A Elon Musk ma dziś wartą setki miliardów firmę – bo ich wynalazki istnieją i są dostępne dla wszystkich. Paradoks jest taki, że więcej można zarobić na fundamencie, który ktoś zbudował za darmo, niż na fundamencie prywatnym.

Ciekawski: Czyli internet jest dziełem kilku wynalazców, którym nie zapłacono za niego ani grosza?

Wiki: I którzy nigdy nie mówili „internet zmieni cywilizację". Mówili: „chcemy żeby naukowcy mogli łatwiej wymieniać pliki". Wszystko inne było skutkiem ubocznym. Wszystko inne.

Na koniec powiem rzecz najważniejszą. Internet nie byłby tym, czym jest obecnie, gdyby nie rozwój mikroelektroniki, gdyby nie było układów scalonych zawierających miliardy tranzystorów, gdyby miliardy ludzi na całym świecie nie używały na co dzień kieszonkowych komputerów, nazywanych smartfonami, telefonami mobilnymi, czy jakkolwiek inaczej. To doskonała ilustracja, że do przełomów cywilizacyjnych nie wystarczą idee, potrzebna jest odpowiednia baza technologiczna. Pewnie porozmawiamy w prztszłości o kolejnym przełomie cywilizacyjnym, jaki przynosi nam sztuczna inteligencja. Z kolei bazą technologiczną dla tego przełomu jest internet. LLM – wielkie modele językowe nie mogłyby powstać, gdyby nie było łatwo dostępnej wiedzy w sieci liczącej ponad miliard stron internetowych na całym świecie. ■

Logo World Wide Web, zaprojektowane przez Roberta Cailliau (Fakefunk – https://www.w3.org/Illustrations/LetsShare.ai.ps, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=114182179)

Redaktor X

Metalurgia

W 2022 roku naukowcy z Uniwersytetu w Manchesterze ogłosili, że znaleźli sposób na odzyskanie kobaltu ze zużytych baterii do samochodów elektrycznych z wydajnością przekraczającą 95 procent. Wiadomość obiegła media technologiczne, portale motoryzacyjne i giełdy surowców. Nikt jednak szczególnie głośno nie powiedział, kto stoi za tym odkryciem. Metalurdzy. Ci sami, których kierunek od lat przegrywa w popularności z informatyką i zarządzaniem, a którym właśnie świat zaczyna się kłaniać, bo bez metali nie ma akumulatorów, bez akumulatorów nie ma elektromobilności, a bez elektromobilności nie ma żadnej zielonej rewolucji. Zapraszamy na metalurgię. Kierunek, który wrócił.

Ruda

Metalurgia to kierunek o wąskiej specjalizacji i szerokim zasięgu. Brzmi jak paradoks, ale tak właśnie jest. Student metalurgii zgłębia fizykę, chemię, informatykę, ekonomię i ekologię nie dlatego, że program nie może się zdecydować, czego uczyć, ale dlatego, że metal nie daje się opisać jedną dziedziną. Stal to termodynamika i krystalografia. Miedź to elektrochemia i przeróbka plastyczna. Aluminium to odlewnictwo i recykling. Łączyć te obszary w jedną spójną naukę, oto zadanie metalurgii. Można ją studiować na niewielu uczelniach w Polsce i to jest fakt niezmienny od lat. Wciąż w grze pozostają Akademia Górniczo-Hutnicza w Krakowie i Politechnika Częstochowska. AGH prowadzi kształcenie na kilku wydziałach, w tym na Wydziale Inżynierii Metali i Informatyki Przemysłowej oraz Wydziale Metali Nieżelaznych – to tu studenci specjalizują się w metalach szlachetnych, recyklingu i przeróbce plastycznej. Kandydaci powinni jednak sprawdzić aktualną ofertę bezpośrednio na stronach uczelni: nazwy wydziałów i specjalizacji zmieniały się w ostatnich latach, a to, co figurowało w katalogach sprzed kilku lat, może już nie obowiązywać. Rekrutacja odbywa się na podstawie wyników matury. W grę wchodzą matematyka, fizyka, chemia i informatyka. Zainteresowanie kierunkiem nie jest masowe. Liczba kandydatów na jedno miejsce historycznie oscylowała blisko jedności; bywa, że organizowany jest drugi nabór. To zupełnie inne realia niż na informatyce czy zarządzaniu, gdzie tłok robi się już w lipcu. Dla kandydata o odpowiednich predyspozycjach to raczej dobra wiadomość.

Wytop

Nauka na studiach inżynierskich trwa siedem semestrów, studia uzupełniające – trzy. Fundament programu jest nieugięty: 120 godzin matematyki, 90 godzin chemii, 90 godzin nauki o materiałach i 60 godzin fizyki. To treści podstawowe, które stanowią ponad połowę pierwszego etapu kształcenia. Reszta to przedmioty kierunkowe: metalurgia i przetwórstwo metali, termodynamika techniczna, technika cieplna, elektrotechnika i elektronika, automatyka i robotyka, metodyka badania materiałów oraz informatyka i komputerowe wspomaganie prac inżynierskich. Nie ma co owijać w bawełnę – to nie jest lekki kierunek. Chemia i wytrzymałość materiałów potrafią dać w kość, a sesja na metalurgii rzadko kiedy jest formalnością. Studenci, z którymi rozmawiano na przestrzeni lat, są w tej kwestii zgodni: wymagań jest dużo, ale nikt ze stresu nie rwie włosów z głowy, bo na ten wydział trafiają zazwyczaj ludzie, którzy wiedzą, czego chcą. Nie ma tu przypadkowych turystów. To, co wyróżnia metalurgię spośród innych kierunków technicznych, to laboratorium rozumiane dosłownie. Nie jako sala komputerowa z symulacją, ale jako hala z piecem indukcyjnym, młotem kuźniczym i maszyną wytrzymałościową. Wycieczki do huty Głogów, ArcelorMittal czy innych zakładów branżowych są stałym elementem programu. Obejrzeć spust surówki z wielkiego pieca to doświadczenie, którego nie zastąpi żaden slajd z prezentacji. Warto się o nie postarać. Współczesne studia metalurgiczne kładą też nacisk na modelowanie numeryczne procesów. Narzędzia takie jak Thermo-Calc do obliczeń termodynamicznych czy oprogramowanie do symulacji odlewania i kucia stają się standardem w pracy inżynierskiej. Sukcesywnie rozbudowuje się tę część programu, co zbliża metalurgię do języka nowoczesnej inżynierii procesowej.

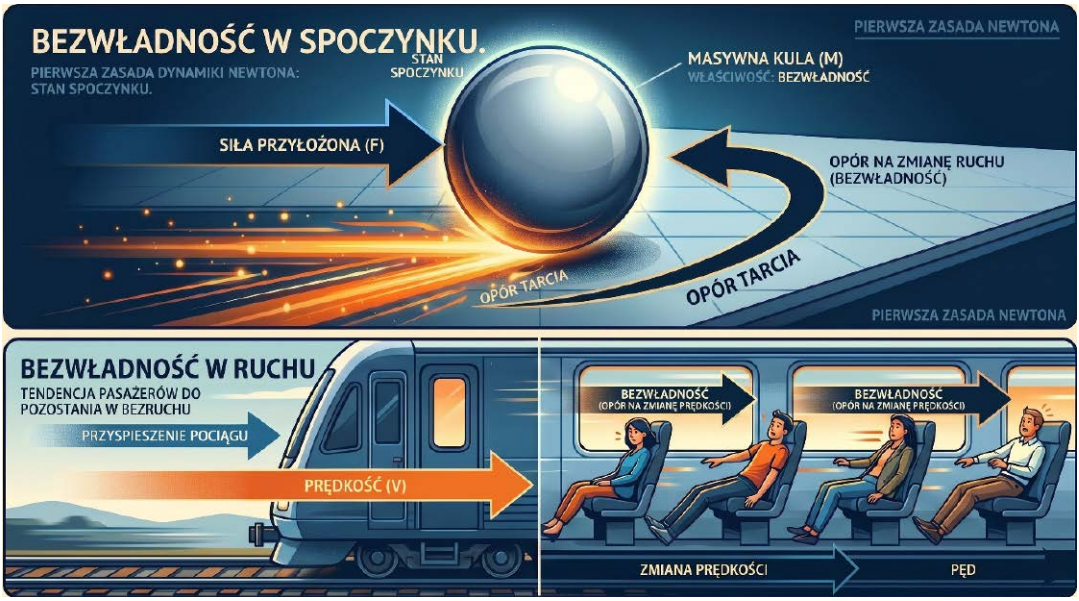
Stop

Po obronie dyplomu przychodzi czas na skonfrontowanie teorii z rynkiem pracy. I tu obraz jest bardziej złożony niż mogłoby się wydawać. Z jednej strony w branży przemysłu metalowego i branżach pokrewnych od lat utrzymuje się deficyt dobrze wykwalifikowanych inżynierów, co potwierdza między innymi Barometr zawodów. Pracodawcy poszukują specjalistów, a konkurencja ze strony innych absolwentów jest stosunkowo niewielka. Z drugiej strony rynek pracy dla metalurga jest geograficznie skoncentrowany. Największe ośrodki produkcyjne to Śląsk, Zagłębie Miedziowe i Mazowsze. Absolwent gotowy na przeprowadzkę ma zdecydowanie lepsze karty. Według danych wynagrodzenia.pl mediana zarobków metalurga wynosi obecnie 8160 zł brutto miesięcznie, a połowa pracujących w tym zawodzie mieści się w przedziale od 6420 do 10710 zł brutto. Dane twojezarobki.com dla szerszej grupy inżynierów górniczych i metalurgów wskazują na typowy przedział 6730...9979 zł brutto (2025). Wynagrodzenia zależą mocno od stanowiska, firmy i regionu. Główny technolog w dużym zakładzie produkcyjnym to zupełnie inne stawki niż junior na linii. Dla porównania: w Niemczech metalurg zarabia średnio 3500...4500 euro brutto miesięcznie, co przy obecnym kursie oznacza ponad dwukrotność polskich stawek. KGHM Polska Miedź to dla studentów metalurgii metali nieżelaznych marka szczególna. Firma oferuje programy stypendialne dla najlepszych studentów, a praca w głogowskich lub lubińskich zakładach to stabilność, prestiż i wynagrodzenie powyżej średniej rynkowej. Warto zainwestować w tę relację już w trakcie studiów. Praktyki i staże w KGHM to najkrótsza droga do oferty zatrudnienia. Żeby zwiększyć swoje szanse na rynku, warto samodzielnie rozwinąć kilka kompetencji, których studia nie zawsze dają w pełni: obsługę technik CAx (CAD, CAM, CAP, PPC), znajomość języka angielskiego technicznego i języka niemieckiego, a także uprawnienia z zakresu elektryki, energetyki lub gazownictwa. To klasyczna lista, powtarzana przez absolwentów od lat i nadal aktualna.

Gotowy stop

Metalurgia to kierunek dla osób, które wiedzą lub przynajmniej mocno czują, że właśnie tego chcą. Nie ma tu miejsca na przypadek ani przy rekrutacji, ani na egzaminach, ani na rynku pracy. W zamian dostaje się solidne, konkretne wykształcenie, zawód, w którym deficyt inżynierów jest realny, i pracę, której efekty można zobaczyć, dotknąć i zmierzyć. W czasach, gdy lit, kobalt i neodym dyktują warunki globalnej transformacji energetycznej, metalurg jest dokładnie tam, gdzie dzieje się coś ważnego. Trzeba tylko być gotowym, podążać tam, gdzie jest huta i nauczyć się przy okazji niemieckiego. ■

Michał Pacholski



Siły bezwładności w praktyce szkolnej

Układy nieinercjalne

Dla znacznej części uczniów zrozumienie genezy sił bezwładności w układach fizycznych jest trudne. Jeśli z treści zadania wynika, że takie siły powinny się pojawić, uczniowie nie zawsze je zauważają, skupiając się na siłach rzeczywistych, wynikających z oddziaływań między ciałami. Wydaje się również, że istnieje problem z rozróżnieniem pomiędzy układami inercjalnymi a nieinercjalnymi. Zacznijmy zatem od początku.

Większość układów odniesienia, w których funkcjonujemy na co dzień, to układy inercjalne. Oznacza to, że spoczywają one lub poruszają się ze stałą prędkością względem innych układów inercjalnych. W takich układach spełnione są zasady dynamiki Newtona. Nie odczuwamy w nich sił bezwładności.

Na przykład za taki układ możemy uznać powierzchnię Ziemi w naszym najbliższym otoczeniu, w odległości, w której zaniedbujemy jej krzywiznę.

Z kolei układy nieinercjalne poruszają się z przyspieszeniem względem układów inercjalnych. Konsekwencją ruchu z przyspieszeniem jest powstawanie w tych układach sił bezwładności.

Siły te są pozorne, to znaczy nie wynikają z żadnych oddziaływań, a jedynie z samego faktu ruchu.

Mimo ich „pozorności” są one odczuwane przez obserwatora znajdującego się w takim układzie. Ich istnienie pociąga za sobą obserwowalne skutki.

Odrobina historii

We wczesnych latach XVII wieku, dzięki odkryciom Galileusza i Keplera, wprowadzono termin „inercja" (bezwładność), który interpretowano jako cechę materii sprawiającą, że trudno wprawić ją w ruch.

W tamtych czasach nie interpretowano jeszcze bezwładności ciał jako skutku działania sił w układach poruszających się z przyspieszeniem.

Pod koniec tego samego wieku Newton na podstawie obserwacji ruchu obrotowego zaproponował podział sił na dwie kategorie: siły naturalne oraz siły wynikające z bezwładności.

Nie sformułował jednak żadnych praw dotyczących tego drugiego rodzaju sił. Dopiero w XVIII–XIX wieku dzięki pracom d'Alemberta oraz Coriolisa stworzono współczesny opis sił bezwładności w układach poruszających się zarówno ruchem prostoliniowym, jak i ruchem po okręgu.

Klasyczne zadanie z windą

Niemal w każdym szkolnym podręczniku albo zbiorku zadań możemy znaleźć zadanie o windzie, która jedzie z pewnym przyspieszeniem. W windzie leży jakiś przedmiot, czasem bezpośrednio na podłodze, czasem na wadze.

Sytuacja ta została schematycznie zilustrowana na **rysunku 1**. Zadanie to może pojawiać się również w innych wariantach i dotyczyć na przykład jadącego poziomo samochodu, którego pasażerowie opierają plecy o fotele.

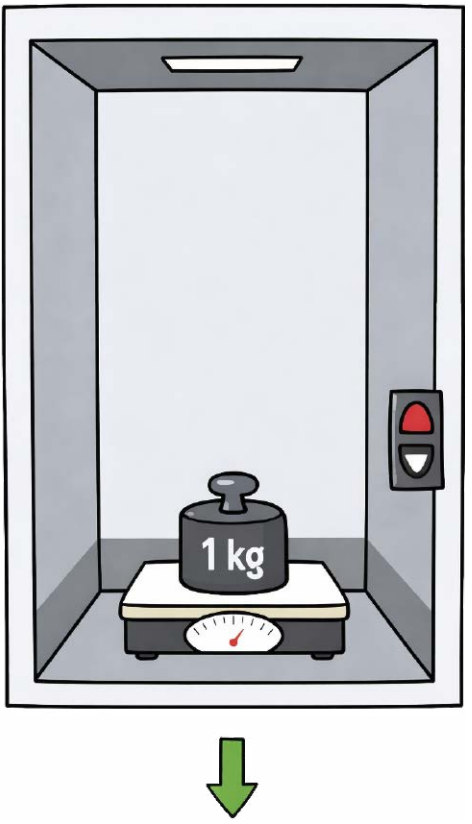
Znając masę przedmiotu, wartość przyspieszenia ziemskiego oraz wartość i kierunek przyspieszenia windy, mamy obliczyć siłę nacisku przedmiotu na podłogę, ewentualnie wskazanie wagi. W sumie nie ma nic prostszego niż to zadanie, a jednak nieodmiennie sprawia ono uczniom kłopot.

Co zatem jest w nim trudnego? Przede wszystkim uczniowie mylą ciężar ciała z siłą nacisku.

Z ich punktu widzenia, jeśli ciało w układzie spoczywającym waży na przykład kilogram, to waga będzie ten kilogram wskazywać niezależnie od kierunku i zwrotu działających sił bezwładności.

Tymczasem, co warto przypominać do skutku, waga sprężynowa nie mierzy masy bezpośrednio. Tak naprawdę mierzy siłę nacisku (nawet nie ciężar ciała!) i podaje wynik w jednostkach masy, ponieważ tak została wyskalowana.

Nie można przyjmować milczącego założenia, że w każdej sytuacji ta skala odpowiada



Rysunek 1. W nieruchomym układzie doświadczalnym odczytujemy wskazanie wagi. Wskazanie to zmieni się, jeśli wprawimy układ w ruch z pewnym przyspieszeniem

rzeczywistości i odzwierciedla realnie działające w układzie siły. Nawet jeśli masa ciała pozostaje stała.

Załóżmy, że mamy już przygotowany układ doświadczalny, przedstawiony na rysunku 1. Windzie nadajemy stałe przyspieszenie o wartości a, skierowane pionowo w dół. Zastanówmy się przez chwilę, jakie siły działają w tym układzie.

Z pewnością na ciało działa siła bezwładności o wartości $F_b = ma$, skierowana przeciwnie do zwrotu przyspieszenia windy, czyli w tym przypadku do góry. Drugą działającą siłą jest siła ciężkości, czyli $Q = mg$.

Wartość siły nacisku na wagę obliczymy w tym przypadku jako różnicę między wartością ciężaru ciała a wartością siły bezwładności:

$$N = Q - F_b = mg - ma = m(g - a).$$

Jeśli chcielibyśmy przeliczyć ten wynik na wskazanie wagi, to musimy podzielić go przez wartość przyspieszenia ziemskiego.

Dostaniemy zatem

$$m_{wsk} = \frac{N}{g} = m\frac{g-a}{g}$$

W przypadku gdy przyspieszenie windy jest skierowane w dół, wskazanie wagi będzie mniejsze niż w windzie nieruchomej.

Ten sam problem, inna siła

Mocno problematyczne są dla uczniów również zadania z wypukłym lub wklęsłym mostem.

W najwyższym lub najniższym punkcie mostu mamy obliczyć albo nacisk samochodu na nawierzchnię, albo nacisk pasażera na siedzisko.

Tu również zadanie na pierwszy rzut oka wydaje się niezrozumiałe: skoro samochód lub pasażer ma masę m, to co się zmienia, jeśli z powierzchni poziomej wjedziemy na most w kształcie fragmentu łuku? Masa przecież pozostaje ta sama.

I znowu nieporozumienie bierze się z utożsamiania w każdym przypadku ciężaru ciała $Q = mg$ z siłą nacisku na podłoże. W opisanym zadaniu należy uwzględnić siłę odśrodkową, która działa jako siła bezwładności w ruchu po okręgu.

Jej wartość wynosi

$$F_{odś} = \frac{mv^2}{R}$$

gdzie v jest prędkością samochodu, a R – promieniem krzywizny mostu.

Siła nacisku samochodu na powierzchnię będzie w przypadku najwyższego punktu mostu wypukłego wynosić

$$N = Q - F_{odś} = m\left(g - \frac{v^2}{R}\right)$$

Znak minus we wzorze pojawia się dlatego, że siła odśrodkowa ma przeciwny zwrot do siły ciężkości.

Sprawdź, co potrafisz

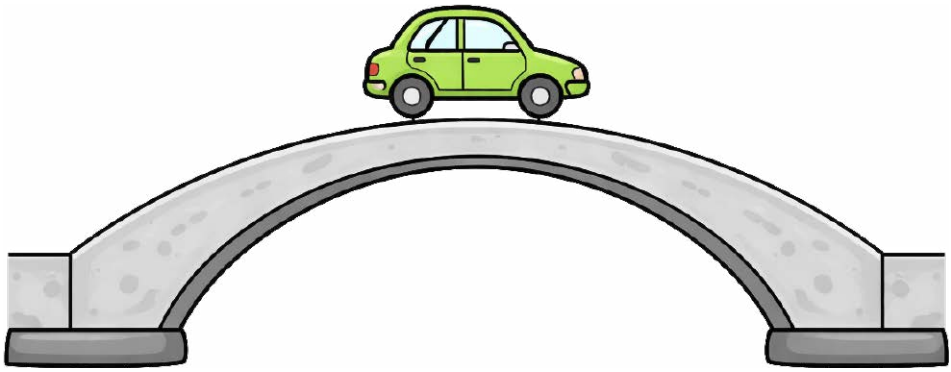
Na podstawie informacji zawartych w tekście i omówionych przykładów rozwiąż poniższe zadania.

Zadanie 1. W windzie umieszczamy wagę, a na niej ciało o znanej masie. Połącz w pary wszystkie sytuacje doświadczalne z obserwowanymi wskazaniami wagi.

Sytuacja	Wskazanie wagi
A. Winda jedzie ze stałą prędkością.	1. Wskazanie wagi wynosi zero.
B. Winda jedzie z przyspieszeniem skierowanym do góry.	2. Wskazanie wagi jest takie samo jak w windzie nieruchomej.
C. Winda jedzie z przyspieszeniem skierowanym w dół.	3. Wskazanie wagi jest mniejsze niż w windzie nieruchomej.
D. Winda spada swobodnie.	4. Wskazanie wagi jest większe niż w windzie nieruchomej.

Zadanie 2. Samochód o znanej masie jedzie ze stałą wartością prędkości po nawierzchniach o różnych promieniach krzywizny. Połącz w pary wszystkie sytuacje z obserwowanym skutkiem.

Sytuacja	Skutek
A. Samochód jedzie po płaskiej nawierzchni.	1. Siła nacisku na podłoże będzie mniejsza niż w przypadku samochodu nieruchomego.
B. Samochód jedzie po wypukłym moście.	2. Siła nacisku na podłoże będzie większa niż w przypadku samochodu nieruchomego.



Rysunek 2. Jeśli samochód jedzie po moście w kształcie fragmentu łuku, to jego nacisk na nawierzchnię jest wypadkową siły ciężkości oraz siły odśrodkowej

C. Samochód jedzie po wklęsłym moście.	3. Siła nacisku na podłoże będzie taka sama jak w przypadku samochodu nieruchomego.

Dla nauczyciela

Warto zauważyć, że wiele niepowodzeń szkolnych bierze się z niedostatecznego opanowania umiejętności znajdowania sił działających w danym układzie fizycznym i wyjaśniania ich wpływu na ruch tego układu. Przytoczone w niniejszym artykule zadania, same w sobie bardzo proste i będące wręcz podręcznikowymi przykładami, dla wielu uczniów stanowią ogromny problem.

Przede wszystkim należy pamiętać o tym, że w układzie poruszającym się z przyspieszeniem zawsze działają siły bezwładności. Na ciało działa wypadkowa wszystkich sił, co powoduje zmianę wartości siły nacisku na podłoże w porównaniu z sytuacją, w której układ byłby w spoczynku lub poruszał się ze stałą prędkością.

Niemniej uczniowie bardzo często nie radzą sobie z działaniami na wektorach, i to nawet w sytuacjach, gdy siły działają wzdłuż tej samej prostej.

Kolejny problem pojawia się w przypadku zadań dotyczących ruchu po okręgu.

Stała wartość prędkości w tym przypadku nie oznacza braku przyspieszenia działającego na ciało.

Jeśli ktoś ma problem ze zrozumieniem tego faktu, to po prostu nie będzie widział związku między zakrzywieniem toru ciała a pojawiającą się siłą bezwładności.

Taki uczeń nie pokusi się o to, żeby skorzystać ze wzoru na siłę dośrodkową i zauważyć, że siła bezwładności ma w tym przypadku tę samą wartość, ale przeciwny zwrot. ■

Joanna Borgensztajn

Odpowiedzi do zadań
Zadanie 1: A2, B4, C3, D1
Zadanie 2: A3, B1, C2

Rozwiązania zadań z kącika matematycznego ze strony 114

Zadanie 1.
Dla liczb mniejszych od 5 funkcja Grundy'ego ma wartość 0, 1, 2 albo 3. W zapisie binarnym są to liczby 0, 01, 10 i 11. Natomiast G(5) = 4, czyli 100 w zapisie binarnym. Dodawanie bitowe nie „zabije" początkowej jedynki i wartość funkcji Grundy'ego będzie co najmniej 4.

Zadanie 2.
Gra z rysunku 11 jest sumą pięciu niezależnych. Wartość funkcji Grundy'ego dla niej to $G(5) \oplus G(5) \oplus G(4) \oplus G(3) \oplus G(2)$. Ponieważ $n \oplus n$ jest zawsze równe 0, wystarczy obliczyć $G(4) \oplus G(3) \oplus G(2) = 1 \oplus 3 \oplus 2$. Binarnie jest to $01 \oplus 11 \oplus 10 = 0$. Ta pozycja jest przegrywająca. Każdy ruch spowoduje zmianę wartości funkcji na niezerową, czyli pozycja stanie się wygrywająca dla przeciwnika.

Zadanie 3.
Gdy liczba klocków jest nieparzysta, gracz *A* przewraca środkowy klocek. Dla parzystej liczby – przewraca dwa środkowe. Gra rozpada się na dwie niezależne i symetrycznie położone układy. Teraz gracz *A* po prostu „małpuje" ruchy gracza *B* – robi to samo co on, tylko w drugiej połówce. W tej sposób ostatni ruch będzie należał do niego.

Zadanie 4.
Nietrudno obliczyć, że dla takiej gry (tzn. trafienie w klocek powoduje przewrócenie się sąsiadów) funkcja Grundy'ego dla kolejnych liczb 0, 1, 2, 3, 4, 5 na wartości 0, 1, 1, 2, 4, 3. Pozycja na rysunku 8 ma zatem wartość $3 \oplus 3 \oplus 0 \oplus 2 \oplus 1 = 3$. Jest to pozycja wygrywająca. Strącenie skrajnego klocka w „trójce" wymusi przewrócenie sąsiedniego. Zostanie wtedy układ $3 \oplus 3 \oplus 0 \oplus 1 \oplus 1 = 0$, a to symbolizuje straconą pozycję. Dla tak prostego układu można zrozumieć i bez teorii, że cokolwiek zrobi gracz *B* – nie da rady wygrać.

Szkoła Wynalazców

dozwolone do lat 15

Mieliście jedno z klasycznych zadań trizowskich, które w „pierwszym czytaniu" wygląda jak nierozwiązywalny problem: zaproponować strategię pokonania rzeki, mając „za plecami" konkurenta do złota, tak żeby bezpiecznie przeprawić się przez odmarzającą już rzekę i nie stracić złota. Odrobina metodycznego podejścia i zadanie rozwiązuje się dość łatwo.

Najpierw trzeba uściślić warunki. Po pierwsze: ile mogło naprawdę ważyć złoto wydobyte w czasie jednego sezonu poszukiwań? Łatwo ustalić te dane w internecie. Otóż jeden samotny poszukiwacz za sezon mógł znaleźć i zdobyć od kilku do kilkudziesięciu gramów, a poszukiwacz szczęściarz mógł znaleźć nawet 300 gramów za sezon. Wybitny szczęściarz mógł znaleźć np. bryłki o łącznej wadze 1...2 kg złota, ale to były wyjątki. Wynika z tego, że ciężar złota nie był problemem podczas przeprawy przez słaby lód. Taką realną ilość złota można było włożyć do kieszeni; i to właśnie w tamtych czasach (1873 r.) powstały spodnie – dżinsy firmy Levi Strauss, z nitowanymi kieszeniami, dla uniknięcia wypadania złota z rozdartej kieszeni.

A jak z tym „nierozwiązywalnym" zadaniem poradzili sobie nasi czytelnicy? Niestety większość założyła – bez żadnej analizy – że złoto było bardzo ciężkie: musiało ważyć kilka kilogramów! Stąd większość odpowiedzi zakładała różne skomplikowane strategie.

Zbigniew Góralski pisze: zawsze przy pokonywaniu słabego lodu, a także przy ratowaniu osób, które wpadły do wody po załamaniu się tafli pokrywającej rzekę, wszystkie poradniki mówią o rozłożeniu ciężaru ciała na możliwie dużą powierzchnię, np. zamiast iść – pełzać, użyć gałęzi itp. Złoto można było zapakować w odrębny pakunek i ciągnąć je na sznurku, dość długim, aby jego ciężar nie powiększał ciężaru pieszego. Konkurenta można było oszukać, wybierając optymalną porę doby, wykonując fałszywe ślady na śniegu itp.

Bardzo dobra strategia, bezpieczna i raczej dająca szansę uniknięcia rabunku złota przez chciwego konkurenta.

Stefan Kwiatkowski uważa, że najpierw właściciel złota powinien z doraźnych materiałów: gałęzi, drzew itp., zbudować tratwę, na niej ułożyć cały swój bagaż i tratwę tę ciągnąć za sobą z pomocą długiej linki. W razie pęknięcia lodu właściciel mógł wskoczyć na tratwę i, pół płynąc, pół jadąc, jak na sankach – pokonać rzekę. Konkurenta musiał jakoś oszukać: stworzyć pozory, że wybrał się na przeprawę i zainscenizować utonięcie razem z ładunkiem i złotem.

Ogólnie można powiedzieć, że strategia budowy tratwy jako zabezpieczenia na wypadek załamania się lodu jest dobra. Ale w warunkach zadania nie było powiedziane, czy w pobliżu były jakieś drzewa i krzewy, z których można by było coś pływającego zbudować.

Wymienionym kolegom gratuluję i zapraszam do następnego zadania.

Nowe zadanie

Czerwiec to początek lata, wyjazdów na wakacje, obozów harcerskich itp. My sobie wyjeżdżamy, a kwiatki i inne rośliny domowe usychają! Są różne metody, np. ustawienie doniczek w kręgu i doprowadzenie do każdej z nich knota, zanurzonego drugim końcem w dużym pojemniku na wodę. Woda będzie spływać do doniczek powoli, dzięki zjawisku włoskowatości. System jest jednak kłopotliwy, bo woda spływa „bez opamiętania" i kwiatki mogą ucierpieć od jej nadmiaru. System powinien zapewniać podawanie wody w takiej ilości, jaka jest potrzebna, i nie powinien zmuszać do reorganizacji mieszkania. Streszczając: zaproponować system samoczynnego podlewania domowych kwiatków bez automatyki elektronicznej, tak aby zapewniał podlewanie przez okres ok. 3 tygodni naszej nieobecności w mieszkaniu. Zadanie jest w gruncie rzeczy proste, ale wymaga dobrego pomysłu, czego wszystkim serdecznie życzę. Przypominam o terminie: do końca sierpnia br.

Klub Wynalazców

bez ograniczeń wieku

Zadaniem waszym było: zachowując ideę przyspieszenia procesu siekania szczypiorku, zaproponować zmianę konstrukcji, tak aby mogło powstać naprawdę użyteczne narzędzie.

Niżej przedstawiono „nożyczki" przeznaczone do cięcia np. szczypiorku, tak aby nadawał się do posypania jajecznicy, sałatki itp. Idea wydaje się prosta i prawidłowa: niestety szczypiorek podczas cięcia ujawnia swoją niemiłą cechę – ma lepki sok i przylepia się do ostrzy „nożyczek". Producent zaproponował narzędzie w postaci niewielkiego grzebienia, którym można ten wklejony pomiędzy ostrza szczypiorek usunąć. To jednak przeczy głównej idei tego urządzenia: szybkości i wydajności.

1

Zachowując ideę narzędzia, należało spróbować przekonstruować te „nożyczki" tak, aby szczypiorek łatwo oddzielał się od ostrzy, ewentualnie zaproponować coś nowego.

Ryszard Bogucki – proponuje zupełnie inny rodzaj narzędzia do cięcia szczypiorku. Uważa, że lepszy będzie układ kilku tarcz, zaostrzonych na obwodzie i osadzonych na wspólnej osi, z rękojeścią umożliwiającą prowadzenie. Pomiędzy tarczami powinny być umieszczone zgarniacze, usytuowane pod kątem tak, aby usunięty spomiędzy tarcz szczypiorek był zmuszony spadać na deseczkę. Warunkiem dobrej pracy zgarniaczy jest umocowanie ich tak, aby przy obracaniu się tarcz pozostawały nieruchome.

Koncepcja wydaje się dobra i narzędzie to powinno działać. Czy w 100% – ha! – to się okaże w praktyce, ale myśl jest dobra, warta próby „w metalu".

Miłosz Warecki – wielokrotnie jeździł na wieś do stryja, gdzie spotkał się z sieczkarnią – urządzeniem do siekania słomy i koniczyny na drobne cząstki – tak jak szczypiorek. Nawet mokra koniczyna nie zakłócała pracy maszyny, która pracuje na innej zasadzie niż ręczne narzędzia. Zasadniczym elementem tej maszyny jest bęben, na obwodzie którego umieszczonych jest kilka ostrzy ustawionych śrubowo i współpracujących z listwą tak, że koniczyna jest cięta kolejnymi ostrzami, ocierającymi się o krawędź listwy. Wiejska sieczkarnia to spora maszyna, ale idea wydaje się trafna. Dla warunków domowych można by wykorzystać zespół napędu maszynki do siekania warzyw, w której należałoby wymienić bęben z ostrzami na ostrzejszy, tak aby szczypiorek mógł być podawany gardzielą, którą podaje się warzywa.

Koncepcja ciekawa, ale wymaga dopracowania. W wiejskiej sieczkarni pęk zboża jest podawany przez zespół dwóch wałków, które, obracając się, wciągają zboże w strefę cięcia. Pęku szczypiorku tak się pchać nie da, a więc należałoby dopracować podawanie na bęben z ostrzami.

Roman Głowacki uważa, że problem szczypiorku leży gdzie indziej. Oczywiście warunkiem sprawnego posiekania pęczka jest posiadanie bardzo ostrego noża. Natomiast główny problem to podawanie szczypiorku równymi porcjami, tak po ok. 5 mm, i tu trzeba pomyśleć i wymyślić podajnik, uruchamiany jedną dłonią. A wtedy nóż może być bezpiecznie prowadzony po drewnianej, pionowej deseczce.

Bardzo ciekawe spojrzenie. Bo przecież musimy pamiętać, że nie siekamy szczypiorku dla dużej stołówki, lecz dla potrzeb rodziny. Nóż bardzo ostry można dziś kupić w wersji japońskiej – z damastu. Natomiast podajnik byłby bardzo praktycznym urządzeniem; uratowałby wiele pociętych palców.

Wymienionym kolegom gratuluję i zapraszam do dalszych zmagań z techniką.

Nowe zadanie

Zadanie, które przygotowaliśmy dla was, dotyczy wszystkich tych, którzy dojrzeli już do codziennego (lub przynajmniej co dwa dni) golenia się ręczną maszynką wieloostrzową. Jak wiadomo, po ogoleniu się myjemy twarz i następnie zwilżamy ją, opryskujemy lub wcieramy „płyn po goleniu". Właśnie z tą banalną operacją jest pewien problem. Jeżeli wlewamy odrobinę płynu na prawą dłoń, w okolicę palców, to przez palce duża część płynu (czasem nietaniego) trafia na posadzkę łazienki. Jeżeli wlejemy ten płyn na dłoń, to manewrowanie dłonią po twarzy jest utrudnione i też marnujemy trochę płynu. Zastosowanie sprayów jest wygodniejsze, ale grozi w pośpiechu tryśnięciem płynu w oczy. Nawet buteleczka z atomizerem nie jest lepsza. Więc co? Po prostu trzeba coś wymyślić! I to jest zadanie dla was, które można sformułować następująco: zaproponować sposób i ewentualnie pojemnik na płyn „po goleniu", taki, żeby nie mógł trafić do oczu, a jednocześnie pozwalał na zwilżenie twarzy, oszczędzając płyn, który nie powinien trafiać na podłogę. Zadanie nie wymaga komentarzy; jest jasne i wydaje się proste. Ale faktem jest, że producenci stosują niemal wyłącznie albo nic, albo spraye lub atomizery. Jedno i drogie nie załatwia sprawy w sposób naprawdę bezpieczny i oszczędzający płyn. Ponieważ każdy z was ma doświadczenie w tej dziedzinie, więc pozostaje życzyć dobrego pomysłu i przypomnić o terminie nadsyłania propozycji: koniec sierpnia br.

Vademecum Młodego Wynalazcy

„Wszystko, co można było wynaleźć, już wynaleziono" – te słowa przypisuje się Charlesowi H. Duellowi, specjalnemu pełnomocnikowi Amerykańskiego Urzędu Patentowego w 1899 roku. Było to przecież zaledwie około 127 lat temu! Jak bardzo się mylił – i to w sposób wręcz spektakularny. Od tego czasu powstały miliony wynalazków. Mimo to działalność wynalazcza wciąż pozostaje w pewnym stopniu tajemnicza. Sięga obszarów psychologii, techniki oraz setek – niekiedy bezowocnych – prób i eksperymentów. Jak to naprawdę wygląda? Czy można sobie wyobrazić wynalazcę jako człowieka, który siedzi wygodnie w fotelu i rozmyśla: „Co by tu jeszcze wynaleźć?". Jednym z najważniejszych źródeł wynalazków są potrzeby. Nie bez powodu mówi się, że potrzeba jest matką wynalazku – i jest w tym wiele prawdy. Na przestrzeni dziejów ludzkości pojawiały się różnorodne potrzeby: początkowo przede wszystkim podstawowe, związane z przetrwaniem – zdobyciem pożywienia, zapewnieniem bezpieczeństwa przed dzikimi zwierzętami, wrogami czy groźnymi zjawiskami przyrody. Z czasem doszły do tego potrzeby poprawy warunków życia i pracy. Dziś ogromna większość racjonalnych potrzeb człowieka została już zaspokojona. Coraz trudniej wskazać zupełnie nowe potrzeby, które mogłyby inspirować wynalazców.

Od dawna podejmowano próby uporządkowania i racjonalizacji procesu poszukiwania tematów wynalazczych. W istocie dopiero teoria Henryka Saulowicza Altszullera zapoczątkowała dynamiczny rozwój metodologii wynalazczości. Jedno z podstawowych twierdzeń Altszullera brzmi: „jeżeli system techniczny rozwija się przez dłuższy czas w tym samym kierunku, to w pewnym momencie pojawia się sprzeczność między różnymi wymaganiami". Prosty przykład: aby usmażyć jajecznicę, patelnia musi być gorąca. Jednocześnie, aby móc nią swobodnie manewrować i kontrolować proces, nie powinna parzyć w rękę. Rozwiązaniem tej sprzeczności jest choćby długa rączka – najlepiej wykonana z materiału izolującego, takiego jak drewno lub tworzywo sztuczne.

Altszuller sklasyfikował różne rodzaje sprzeczności. Wyróżnił między innymi:

– sprzeczność techniczną,
– sprzeczność fizyczną,
– sprzeczność administracyjną.

Pracując w komórce racjonalizacji i mając dostęp do obszernego zbioru opisów patentowych oraz projektów racjonalizatorskich, zauważył on interesujące zjawisko: mimo ogromnej liczby różnorodnych pomysłów wynalazczych, istnieje stosunkowo niewielka grupa podstawowych

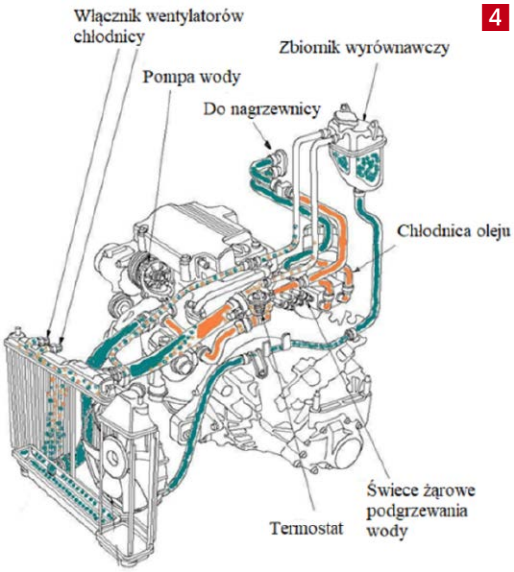
2

metod rozwiązywania sprzeczności – a to właśnie one najczęściej prowadzą do powstania wynalazków. Na tej obserwacji Altszuller zbudował jedno z najbardziej praktycznych narzędzi TRIZ – tzw. matrycę sprzeczności. W najprostszym ujęciu jest to tabela, w której na jednej osi zapisano to, co chcemy poprawić, a na drugiej to, co pogarsza się przy tej poprawie. Na przecięciu tych dwóch cech znajdują się wskazówki – zestaw zasad wynalazczych, które w podobnych sytuacjach okazały się skuteczne. Weźmy przykład z życia codziennego: chcemy zwiększyć wytrzymałość walizki, aby lepiej chroniła zawartość. Niestety, wraz z wytrzymałością rośnie jej masa. W matrycy odnajdujemy więc sprzeczność: „wytrzymałość – kontra masa". Jedną z proponowanych zasad jest segmentacja – czyli podział na części. Zastosowanie? Zamiast jednorodnej, ciężkiej obudowy stosuje się strukturę komórkową (np. jak plaster miodu) albo lekkie kompozyty. Walizka pozostaje wytrzymała, ale nie przybiera na wadze w takim stopniu, jak w rozwiązaniu tradycyjnym – **rysunek 2**.

Inny przykład: chcemy, aby parasol był duży (lepsza ochrona przed deszczem), ale jednocześnie poręczny i łatwy do przenoszenia. Sprzeczność „powierzchnia kontra wygoda użytkowania" prowadzi do zasady zmienności (dynamizacji) – **rysunek 3**. Rozwiązaniem jest parasol składany – w czasie użytkowania duży, a po złożeniu niewielki. Klucz nie polega na kompromisie („trochę mniejszy parasol"), lecz na sprytnym obejściu sprzeczności. Jeszcze jeden przykład, bliższy technice: zwiększenie mocy silnika zwykle powoduje wzrost temperatury, co z kolei obniża jego trwałość. Matryca wskazuje m.in. zasadę pośrednictwa lub chłodzenia. W praktyce oznacza to zastosowanie układu chłodzenia – cieczą, powietrzem lub nawet bardziej zaawansowanych technologii. Zamiast ograniczać moc, wprowadzamy dodatkowy element, który neutralizuje negatywny efekt. Warto zauważyć, że matryca Altszullera nie „wymyśla" wynalazków za człowieka. Działa raczej jak dobrze uporządkowana pamięć zbiorowa techniki – podpowiada kierunki, które już kiedyś okazały się skuteczne. Wynalazca nie zaczyna od zera, lecz korzysta z doświadczenia tysięcy wcześniejszych rozwiązań. I tu tkwi jej największa wartość: zamiast błądzić metodą prób i błędów, można świadomie szukać rozwiązań, które omijają sprzeczności, a nie tylko je łagodzą. Bo – jak pokazał Altszuller – prawdziwy postęp techniczny rzadko polega na kompromisie. Najczęściej polega na tym, że ktoś znajduje sposób, by mieć „jedno i drugie" – **rysunek 4**. Niekiedy poszukiwanie kompromisu pomiędzy tym, co chcemy ulepszyć, a tym, co się dzięki temu pogorszy, wymaga użycia kilku zasad wynalazczych. Podane przykłady to elementarnie proste problemy. Niżej przykład nieco bardziej skomplikowany, spędzający sen z oczu konstruktorom lotniczym przez ponad 20 lat!

Okazuje się, że nie zawsze musimy korzystać z całego arsenału środków i metod TRIZ. Niekiedy wystarcza analiza uściślająca pojęcie sprzeczności dla danej sytuacji. Przykład: dla stworzenia normalnych warunków pracy załogi

3



4

samolotu wojskowego kabinę wykonuje się jako hermetyczną i w niej utrzymuje się właściwe ciśnienie powietrza, mimo stratosferycznego lotu. Samolot – zwłaszcza bojowy – narażony jest na różne przygody i kabina może się rozhermetyzować. Potrzebny jest więc zapas tlenu i dlatego samolot wyposaża się w butle z tlenem pod wysokim ciśnieniem. W zależności od typu samolotu: czy to jest bombowiec, czy też transportowiec wojska, tych butli mogło być nawet kilkadziesiąt. Każda taka butla, która musi wytrzymać ciśnienie dochodzące do 20 MPa, to ciężar ok. 80 kg, co stanowi spore obciążenie dla samolotu. Co robić?

1. Formułujemy łańcuch sprzeczności zewnętrznych, systemowych: Uwaga: stosowanie zapisu skrótami nie jest konieczne, ale przy bardziej skomplikowanych zadaniach ułatwia analizę. Oczywiście trzeba nauczyć się czytać skróty. Podstawowe to: **ZS** – zewnętrzna sprzeczność; **A, B, C** – ogólnie – jakiś stan systemu lub jego części; **IWK** – idealny wynik końcowy; **OS** – ostra sprzeczność itd. analogicznie. **ZS_1** – należy zapewnić przeżycie załogi samolotu w rozhermetyzowanej kabinie. Efekt niepożądany: **anty A** (rozhermetyzowana kabina nie zapewnia przeżywalności załogi). Wymagamy spełnienia żądania **A**, czyli zapewnienia przeżywalności załogi. **ZS_2** – stalowe butle z zapasem tlenu obciążają samolot (efekt **anty B**). Żądanie **B** – zapewnienie stałej masy samolotu lub nawet jej zmniejszenie.

2. Pogłębiona techniczna sprzeczność: butle z tlenem zapewniają przeżywalność załogi, ale obciążają samolot, a więc techniczna sprzeczność: **TS_1** – przeżywalność załogi (**wymaganie A**) i obciążenie samolotu – **żądanie B**. Takie sformułowanie ukazuje, oprócz efektu niepożądanego (przeciążenie samolotu), także efekt dodatni: zapewnienie przeżywalności załogi.

3. Idealny wynik końcowy (**IWK**). Butle z tlenem nie przeciążają samolotu (**B**) i zapewniają przeżywalność załogi – wymóg **A**.

4. Ostra sprzeczność **OS_1**: masa butli z tlenem powinna być duża (**właściwość C**) – żeby zapewnić przeżywalność załogi (**właściwość A**), i jednocześnie mała (**właściwość anty C**), żeby nie przeciążać samolotu (**właściwość B**).

5. Ostra sprzeczność **OS_2**. Sprzeczność **OS_1** można jeszcze bardziej zaostrzyć, ujawniając pierwotne przyczyny sprzeczności. Dlaczego butle są ciężkie? Dlatego że muszą mieć grube ścianki, żeby wytrzymały wysokie ciśnienie tlenu. W rezultacie: **OS_2** – ścianki butli powinny być grube (**C_1**), żeby wytrzymały ciśnienie tlenu, i powinny być cienkie (**właściwość anty C_1**) (w granicy: zerowej), żeby nic nie ważyć. Oznacza to, że ścianki butli muszą być i nie powinno ich być. Można to też sformułować dla tlenu: tlen powinien być pod dużym ciśnieniem, żeby zmieściła się go odpowiednia ilość w butli, i jednocześnie nie powinien być pod ciśnieniem.

6. Rozwiązanie zadania (**RZ**). Takie sprzeczności rozwiązuje się przez zmianę struktury systemu, np. przez zmianę stanu skupienia. W danym przypadku zmienimy stan skupienia tlenu. Tlen powinien być transportowany w samolocie w stanie ciekłym. Oczywiście powinien być przechowywany w naczyniach Dewara, czyli po prostu w termosach, które są wielokrotnie lżejsze od stalowych butli ciśnieniowych. Proste? Oczywiście, jak się pokaże rozwiązanie! Problem ten rozwiązał inż. Andriej Tupolew, znany rosyjski konstruktor ponad 100 samolotów różnych typów i różnego przeznaczenia. Powyższe zadanie jest w sumie dość proste (ale nie umiano go rozwiązać przez ponad 20 lat!). Zwraca uwagę fakt skorzystania z tabeli efektów fizycznych i operatora systemowego, który podpowiada, że jeśli problemu nie da się rozwiązać w przestrzeni, to trzeba próbować rozwiązać go w czasie lub przez zmianę struktury elementów systemu.

Prezes Klubu Wynalazców
Champion TRIZ
Jan Boratyński

Genialne w swej prostocie: **6 innowacyjnych pomysłów Czytelników, które mogą zmienić naszą codzienność**

Prezentujemy najciekawsze propozycje nadesłane do naszej redakcji w ostatnim miesiącu. Od ekologii, przez ogrodnictwo, aż po wsparcie dla seniorów – oto dowód na to, że kreatywność nie zna granic.

Krzysztof Dudzik – zauważył, że gdy myjemy dłonie pod strumieniem wody z wodociągu, niestety woda wlewa nam się do rękawa. Niedużo, ale jest to problem, bo rękaw jest mokry, a mankiety niekiedy brudne od mydła. Należałoby wymyślić coś, co zapobiegałoby takim przygodom.

Problem rzeczywiście istnieje i dotyczy zwłaszcza czynności wykonywanych wyżej niż nasze ramiona, np. mycia okien itp. Wydaje się, że gumowe „rękawiczki bez palców,"czyli po prostu elastyczne rury nakładane tak, żeby obejmowały mankiet i obciskały przegub dłoni, załatwiłyby problem.

Mateusz Grzywacz – w warunkach domowych, zwłaszcza w kuchni, często zachodzi potrzeba otwarcia butelki zamykanej na nakrętkę – jedną ręką. Jeśli nakrętka nie jest zbyt mocno dokręcona, to jest to zadanie wymagające pewnej zręczności, ale łatwe. Gorzej, gdy nakrętka stawia zbyt duży opór i czasem trzeba użyć kleszczy. Przydałoby się jakieś proste urządzenie, które nie wymagałoby użycia kleszczy i dało się obsłużyć jedną ręką.

Wydaje się, że problem jest dość prosty. Można by zamocować na stałe przy blacie kuchennym coś w rodzaju tulei ze stożkowym i karbowanym wnętrzem. Trzymając jedną ręką butelkę, wkładałoby się ją do tej tulei i, obracając butelką, łatwo odkręciłoby się nakrętkę. Ciekawe, co o tym myślą inni Czytelnicy.

Bogdan Wesołowski – często jest wysyłany przez „władze domowe" na zakupy do pobliskich sklepów. Na te zakupy bierze torbę tekstylną z dwoma uszami. Ekspedientka ustawia zakupione towary na ladzie, skąd należy je zabrać i umieścić w torbie. Bogdan widzi potrzebę zainstalowania haka na krawędzi lady (od strony klienta), na którym można by powiesić jedno ucho, drugim otworzyć torbę i ulokować w niej zakupione towary. Bez takiego haka wkładanie kończy się czasami zbieraniem produktów z podłogi.

Bardzo prosta i bardzo przydatna sprawa! Wie o tym każdy, komu wypadła z takiej torby butelka szklana z piwem! Te tekstylne torby są rzeczywiście niemiłe podczas zapełniania ich produktami.

Roman Gwiżdż – wielokrotnie przekonał się, że świeży chleb, pachnący i apetyczny, po dwóch – trzech dniach twardnieje i w zasadzie nie nadaje się do jedzenia. Potrzebny jest jakiś pojemnik lub metoda, żeby tego uniknąć.

W zasadzie taka metoda już jest w każdym domu. Wystarczy zakupiony chleb podzielić na dwie części: jedną schować do chłodziarki, a drugą do zamrażalnika. Chleb z zamrażalnika należy przełożyć do chłodziarki wieczorem, żeby na śniadanie był już rozmrożony. Ale są jeszcze inne metody, może wypowiedzą się koledzy ze Szkoły Wynalazców...

Bogdan Trzciński – wszystkie systemy zabezpieczenia rowerów przed kradzieżą polegają w zasadzie na utrudnianiu zabrania roweru z miejsca parkowania. Wydaje się, że w XXI wieku można to zrobić daleko lepiej. Można zainstalować w rowerze chip lokalizacyjny, informujący właściciela o miejscu znajdowania się roweru; dane o miejscu można by odczytać z komórki. A poza tym można umieścić w rowerze sygnał dźwiękowy głośny i przeraźliwy, tak żeby nielegalne zabieranie roweru było natychmiast ujawniane. Wszystko to będzie ważyło nie więcej niż 50 dag, a stopień zabezpieczenia byłby bardzo wysoki.

System lokalizacji roweru już w zasadzie jest: mają go wszystkie firmy wypożyczające rowery do jazdy po mieście. Zastosowanie w prywatnym rowerze sygnału dźwiękowego rzeczywiście bardzo by pomogło w zniechęceniu złodzieja do zabrania roweru.

Ania Motyka – jest pewien problem z artykułami pakowanymi w tuby. Otóż nie zawsze udaje się wykorzystać ich zawartość do końca. Najczęściej rozcina się nożem tubę i pracowicie wgrzebuje się resztki, np. ketchupu lub musztardy. Potrzebny jest jakiś sposób lub urządzenie, które pozwoli wykorzystać zawartość tuby do końca.

Obecnie stosuje się właściwie jeden sposób w przypadku butelek: dolewa się do butelki z resztkami ketchupu trochę ciepłej wody i, mocno potrząsając, po chwili możemy cały ketchup mieć już do dyspozycji. Co można zrobić z tubką? Zapewne można jeszcze coś wymyślić, ale to pozostawiamy członkom Klubu Wynalazców.

Drukarstwo i poligrafia

Starożytność

Zanim pojawiła się prasa drukarska, ludzkość przez tysiąclecia szukała sposobów na powielanie tekstów i wizerunków. Najwcześniejsze znane przykłady druku stemplowego pochodzą z Mezopotamii: cylindryczne pieczęcie (**1**) toczone po wilgotnej glinie były używane w Sumerze i Babilonie już ok. 3500 r. p.n.e. Odciskano na nich napisy i wzory, dokumentując transakcje handlowe i akty władzy. Był to prymitywny, ale skuteczny sposób błyskawicznego kopiowania tych samych informacji.

W starożytnym Egipcie używano drewnianych stempli do wytłaczania wzorów na tkaninach. W Chinach, w okresie dynastii Han (ok. I w. n.e.), rozwinął się druk blokowy – technika polegająca na wycinaniu lustrzanego odbicia tekstu lub obrazu na powierzchni drewna, pokrywaniu go tuszem i odciskaniu na papierze lub jedwabiu. Papier, wynaleziony w Chinach ok. 105 r. n.e. przez Cai Luna (**2**), stał się idealnym nośnikiem dla tej techniki i zapoczątkował erę masowej komunikacji pisanej.

1. Cylindryczna pieczęć sumeryjska i jej odbicie w glinie, ok. 3000 r. p.n.e. (Metropolitan Museum of Art, Nowy Jork)

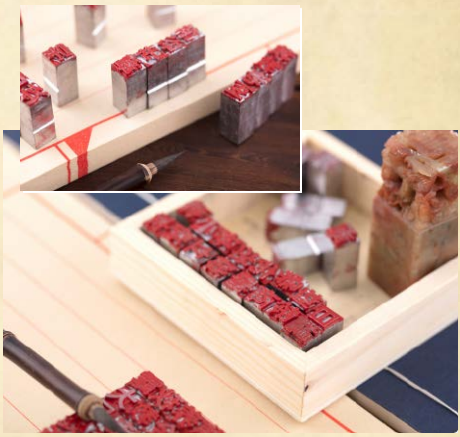
2. Produkcja papieru metodą Cai Luna, dynastia Han

Kamień milowy: ok. 1040 r.

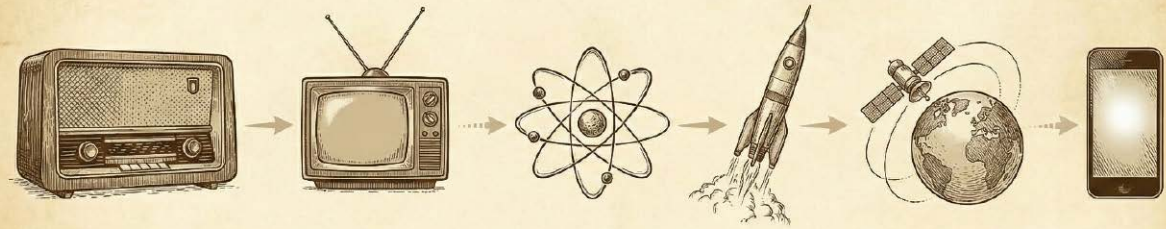
Chiński kowal i wynalazca Bi Sheng opracował pierwszą na świecie technikę druku ruchomą czcionką (**3**). Odlewał poszczególne znaki pisma chińskiego w mieszaninie gliny, wypalał je, a następnie układał w ramy odbitki na metalowej płytce pokrytej kleistą żywicą. Po zadrukowaniu i schłodzeniu ramy czcionki można było rozbić i użyć ponownie. Choć złożoność chińskiego pisma – liczącego kilka tysięcy znaków – utrudniała praktyczne stosowanie tej metody na szerszą skalę, wynalazek Bi Shenga wyprzedził Gutenberga o ponad czterysta lat. W Korei w XIV w. odlano pierwsze metalowe ruchome czcionki, którymi wydrukowano niezachowane do dziś książki.

Kamień milowy: ok. 1450 r.

Johannes Gutenberg z Moguncji (**4**) skonstruował przełomową prasę drukarską z ruchomą czcionką odlewaną ze stopu ołowiu, cyny i antymonu. Innowacja Gutenberga była w istocie zestawem wynalazków: precyzyjny moduł do odlewania czcionek o idealnie jednakowej wysokości, specjalny tłusty tusz drukarski dobrze przylegający do metalu oraz mechaniczna prasa wzorowana na prasach do wina i sera. Ok. 1455 roku Gutenberg wydrukował słynną Biblię 42-wierszową (**5**) – pierwsze w Europie książki wyprodukowane metodą typograficzną. Wynalazek Gutenberga oznaczał koniec epoki ręcznego kopiowania rękopisów. W ciągu pięćdziesięciu lat od 1450 r. wydano w Europie więcej książek niż przez całe poprzednie tysiąclecie.



3. Rekonstrukcja zestawu ruchomych czcionek ceramicznych Bi Shenga



XVI–XVII w.

Prasa drukarska zmienia Europę. Druk umożliwił szybkie rozpowszechnianie idei, które wcześniej potrzebowały dekad, by dotrzeć z jednego końca kontynentu na drugi. W 1517 roku Marcin Luter przybija swój protest do drzwi katedry w Wittenberdze – jego tezy rozchodzą się po całych Niemczech w ciągu kilku tygodni dzięki drukarniom. Kopernik i Galileusz drukują swoje traktaty, rewolucjonizując astronomię. Wzrasta umiejętność czytania, rozwijają się pierwsze gazety. W Wenecji Aldo Manuzio wprowadza format książki kieszonkowej (ok. 1501) (**6**) i pochylone pismo drukowanej kursywy – italika – której używamy do dziś.

XIX w.

Rewolucja przemysłowa dociera do drukarni. W 1814 roku londyński dziennik The Times jako pierwsza gazeta na świecie zainstalował prasę cylindryczną napędzaną parą, skonstruowaną przez Friedricha Königa i Andreasa Bauera. Maszyna tłocząca nacisk walca zamiast płaskiej płyty osiągała prędkość 1100 odbitek na godzinę – kilkanaście razy więcej niż ręczna prasa. Dzienniki stały się dostępne dla masowego czytelnika.

W 1886 roku Ottmar Mergenthaler opatentował linotyp (**7**) – maszynę, która rewolucjonizowała skład tekstu. Zamiast ręcznego układania pojedynczych czcionek, operator pisał na klawiaturze, a maszyna automatycznie odlewała całe wiersze tekstu w jednym metalowym bloku (stąd nazwa: line of type). Linotyp przez ponad siedemdziesiąt lat był podstawą składni gazet, książek i magazynów na całym świecie.

Kamień milowy: 1904–1906

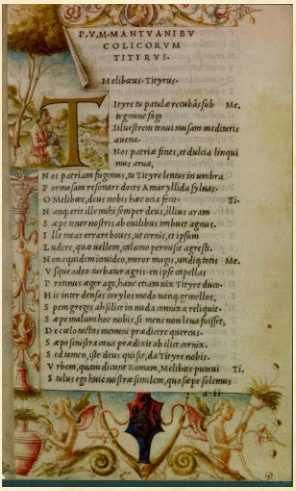
Druk offsetowy, opracowany niezależnie przez Ira Rubela i firmę Caslon w Stanach Zjednoczonych, stał się dominującą techniką druku przez cały XX wiek. Jego zasada polega na pośrednich odbitkach: obraz jest najpierw przenoszony z płyty drukowej na gumowy walec (cylinder offsetowy), a dopiero z walca na papier. Gładka guma pełniej pokrywa nierówne powierzchnie papieru niż metal, dając ostrzejszy,bardziej jednolity wydruk. Druk offsetowy umożliwiał też drukowanie w wielu kolorach na jednym przebiegu. Stał się podstawą produkcji gazet, plakatów, książek i opakowań – i w dużej mierze nią pozostaje do dziś przy dużych nakładach.

Lata 50.–70. XX w.

Fotografia wkracza do drukarni. Fotomechaniczne metody przenoszenia obrazu na płyty drukarskie stopniowo zastępują metalowe czcionki. Fotoskład – technika, w której litery są naświetlane na kliszy lub papierze fotograficznym – eliminuje ciężkie ołowiane matryce i przyspiesza skład

4. Fragment obrazu „Pierwszy druk Gutenberga" autorstwa Friedricha Reicherta

5. Egzemplarz Biblii 42-wierszowej wydanej w dwóch tomach w oryginalnej XV-wiecznej oprawie, przechowywanej w Muzeum Diecezjalnym w Pelplinie (Kpalion – Praca własna, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=52227713)



6. Przykład druku kieszonkowego i kursywy Alda Manuzio, Wenecja ok. 1501

tekstu. W 1973 roku firma Xerox opatentowała drukarkę laserową (**8**), która za pomocą wiązki laserowej nakładała obraz na naelektryzowany bęben, a następnie przenosiła go na papier za pomocą tonera. Technologia, która zrewolucjonizowała biura i małe drukarnie.

Kamień milowy: 1985

Narodziny DTP (Desktop Publishing) – składu komputerowego. Apple wprowadził na rynek komputer Macintosh z graficznym interfejsem, drukarkę laserową LaserWriter i program PageMaker firmy Aldus (**9**). Po raz pierwszy w historii można było zobaczyć na ekranie monitora dokładnie to, co zaraz wyjdzie z drukarki – zasada WYSIWYG (What You See Is What You Get). Skład tekstu i projekt graficzny, który wcześniej wymagał pracy całych specjalistycznych zespołów, stał się dostępny dla każdego użytkownika komputera. Była to prawdziwa demokratyzacja druku: tysiące gazet lokalnych, biuletynów i książek zaczęło być produkowanych bez drukarni.

Lata 80.–90. XX w.

Druk atramentowy (inkjet) staje się technologią konsumencką. Firma Canon w 1977 roku odkryła przypadkowo zjawisko wyrzucania kropli atramentu po podgrzaniu kapilary – efekt nazwano Bubble Jet. Hewlett-Packard i Canon wprowadzają w 1984 roku pierwsze drukarki atramentowe przeznaczone dla użytkowników domowych. Epson rok później prezentuje głowicę piezoelektryczną, wyrzucającą atrement bez podgrzewania. W kolejnych dekadach drukarki atramentowe osiągnęły rozdzielczość i jakość kolorów niedostępną wcześniej poza studiami graficznymi.

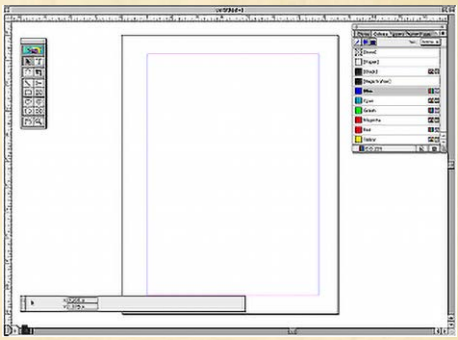
Współczesność

Druk wychodzi z płaszczyzny i podbija tereny poza poligrafią. W 1984 roku Chuck Hull opatentował stereolitografię (SLA) – metodę tworzenia trójwymiarowych obiektów przez utwardzanie warstw ciekłej żywicy światłem UV. Jego firma 3D Systems wprowadziła pierwszą komercyjną drukarkę 3D w 1987 roku. Przez dekady technologia pozostawała droga i niszowa. Przełom nastąpił po wygaśnięciu kluczowych patentów ok. 2009 roku: społecznościowy projekt RepRap obniżył koszty drukarki FDM (Fused Deposition Modeling) do kilkuset dolarów. Dziś drukarki 3D wytwarzają protezy kończyn, części silników lotniczych, modele architektoniczne i żywność. W medycynie testowany jest biodruk – tworzenie rusztowań tkankowych, a w przyszłości być może całych organów, warstwa po warstwie, z żywych komórek.

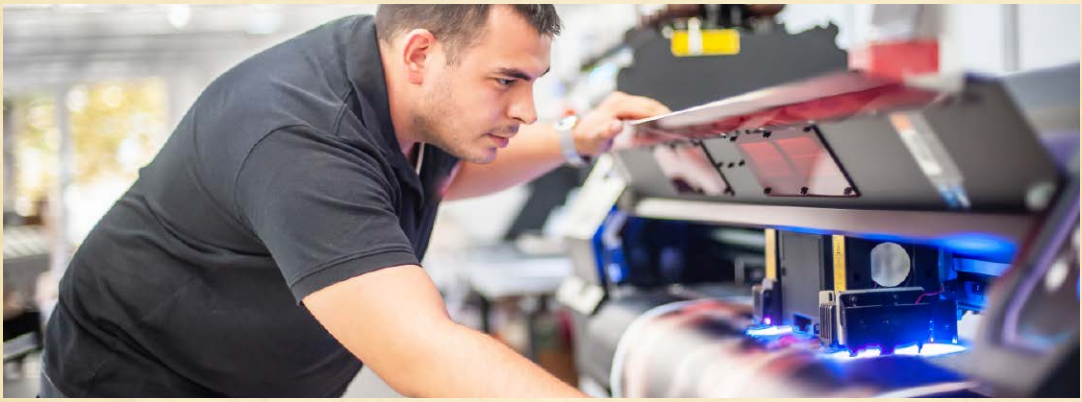
(red)

7. Maszyna linotyp Ottmara Mergenthalera, ok. 1890 r. (CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=1537317)

8. Xerox 9700 – pierwsza komercyjna drukarka laserowa, 1977 r.



9. Zrzut ekranu Adobe PageMaker 7.0 na systemie Mac OS



Główne techniki druku

Techniki druku można podzielić według sposobu przenoszenia obrazu na podłoże. Każda z głównych metod ma swoje zalety i typowe zastosowania:

Druk wypukły (typografia, fleksografia):

Farba pokrywa wypukłe elementy formy drukowej i jest przenoszona na podłoże. Pierwotna technika Gutenberga. Współcześnie fleksografia (elastyczna forma gumowa) dominuje w druku opakowań i etykiet.

Druk płaski (offset, litografia):

Forma drukowa jest płaska; miejsca drukujące przyjmują farbę, a miejsca niedrukujące ją odrzucają (na zasadzie wzajemnego odpychania tłuszczu i wody). Offset to najpowszechniejsza technika przy dużych nakładach książek, gazet i opakowań.

Druk wklęsły (rotograwiura, wklęsłodruk):

Farba jest zatrzymywana w wygrawerowanych zagłębieniach cylindra i przenoszona na podłoże pod ciśnieniem. Daje wyjątkowo wysoką jakość reprodukcji zdjęć. Używana przy druku banknotów, znaczków, magazynów o dużych nakładach.

Druk przesiewowy (sitodruk):

Farba jest przeciskana przez szablon z siatką (sito) na podłoże. Możliwy na niemal każdej powierzchni: tkaninach, szkłach, metalach, desce. Stosowany w odzieży, reklamie i elektronice.

Druk cyfrowy (laserowy, atramentowy):

Obraz jest generowany bezpośrednio z pliku komputerowego, bez stałej formy drukowej. Opłacalny przy małych nakładach i przy druku na żądanie. Drukarki laserowe używają tonera, atramentowe – ciekłego atramentu.

Druk 3D (addytywny):

Obiekt jest budowany warstwa po warstwie z materiału (tworzywa, żywicy, metalu, ceramiki). Techniki: FDM (wytłaczanie termoplastyczne), SLA (stereolitografia), SLS (spiekanie laserowe proszku). Rewolucjonizuje prototypowanie, medycynę i przemysł lotniczy. ■

(red)

KURS PRAKTYCZNY AI

Praktyczne podejście. Zero marketingowej mgły!

Zyskaj **15%** rabatu

W prenumeracie tylko

~~116,00 zł~~

98,60 zł

prenumerata drukowana 4 wydań

Zamów na www.UlubionyKiosk.pl

lub zeskanuj kod QR i zaprenumeruj w 1 minutę