

KRYPTOWALUTY

FUNKCJONOWANIE KRYPTOWALUT

Czym są kryptowaluty?

Kryptowaluty z każdym rokiem coraz bardziej zyskują na popularności. Proporcjonalnie powiększa się grupa osób, które chciałyby je zakupić i z nich korzystać albo zyskać na wzroście ich wartości. Jednakże niewielu ludzi zdaje sobie sprawę, czym tak naprawdę są kryptowaluty i skąd bierze się ich wartość. W tym temacie nie pomagają ani wpisy w Wikipedii, których nikt nie rozumie, ani redaktorzy z tradycyjnych mediów, którzy omawiają to zagadnienie dość powierzchownie. W ich przekazie pojawia się wiele nieścisłości, a jedyne, co się dla nich liczy, to aktualna wycena kryptowalut. Tymczasem inwestowanie w dane aktywo powinniśmy rozpocząć od jego zrozumienia. Właśnie dlatego napisałem ten rozdział – aby każdy czytelnik mojej książki, nawet ten z zerową wiedzą na temat kryptowalut, mógł zrozumieć, czym one są.

Kryptowaluty to wirtualne pieniądze internetowe, które nie mają postaci fizycznej i istnieją wyłącznie w świecie cyfrowym. Podstawą ich funkcjonowania jest kryptografia. Służy ona do zabezpieczania transakcji oraz zapewnia nas, że raz zatwierdzona transakcja nie może zostać zmieniona. To właśnie od kryptografii swoją nazwę wzięły kryptowaluty.

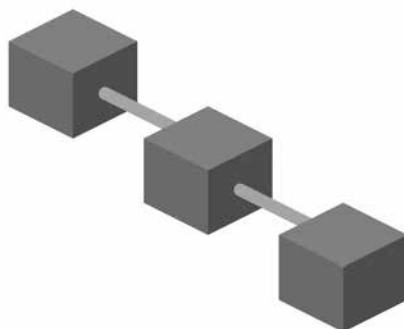
Kryptowaluty od początku swojego istnienia miały służyć ludziom jako jednostka wymiany wartości, która byłaby niezależna od banków, instytucji finansowych czy rządzących. Z tego powodu zazwyczaj nie stoi za nimi żaden emitent, który miałby władzę nad wszystkimi środkami. Kryptowaluty są niezależnym pieniądzem, nad którym kontrolę sprawuje społeczność. Dodatkowo za ich pomocą możemy przysyłać wartość do innych osób bez żadnych

pośredników, czym cechuje się również gotówka. Każda kryptowaluta ma swoją oddzielną społeczność oraz system księgowy z ustalonymi zasadami, znany jako „blockchain”.

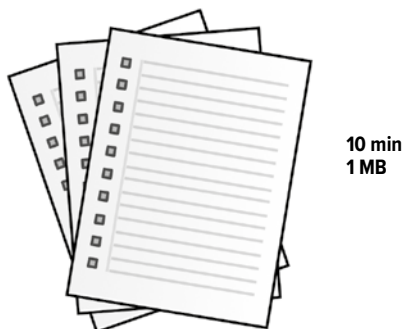
Czym jest blockchain i jak działa?

Blockchain to zdecentralizowany system księgowy, na którym bazują kryptowaluty. Jego nazwę tłumaczy się z języka angielskiego jako „łańcuch bloków” (rysunek 2.1). Ta rozproszona baza danych rejestruje wszystkie transakcje i umieszcza je w blokach o określonej wielkości. System ten nie posiada żadnej jednostki centralnej, która by go kontrolowała. Tak jak wspominałem – kontrolę nad nim sprawuje społeczność. Na system blockchain składa się bowiem sieć komputerów, w której każdy komputer stanowi osobny węzeł i jest równy innym jednostkom. Jest to tzw. model peer-to-peer (P2P). Osoby obsługujące blockchain i stojące za tymi komputerami są nazywane górnikami (ang. *miners*).

Górnicy zajmują się księgowaniem transakcji i ustalaniem ich jednej, wspólnej kolejności. Na każdym komputerze podłączonym do sieci przechowywana jest księga rozrachunkowa, w której zapisane są wszystkie dokonane przez użytkowników transakcje, a zatem również informacja o ich stanie posiadania. Taki model uniemożliwia oszukanie systemu i dopisanie sobie środków, ponieważ wówczas nasza księga rozrachunkowa będzie różniła się od tych zapisanych na pozostałych maszynach, co doprowadzi do odłączenia takiego węzła oraz uznania przesyłanych przez niego informacji za fałszywe. Zdecentralizowana charakterystyka blockchaina czyni go odpornym na wszelkiego rodzaju awarie. Jeśli dana jednostka zostanie odłączona od systemu, to inne komputery zajmą się dalszym księgowaniem, ponieważ mają zapisane niezbędne informacje. Jeśli natomiast prześlemy komuś bitcoina, to taka



Rysunek 2.1. Łańcuch bloków – graficzne zobrazowanie blockchain. Źródło: Licencja Canva Pro



Rysunek 2.2. Porównanie stron zeszytu do bloków bitcoina. Źródło: opracowanie własne

transakcja również będzie widoczna na wszystkich maszynach, ale dalej nikt nie będzie w stanie ustalić, do kogo należy dany portfel.

Wspominałem już wcześniej, że blockchain jest łańcuchem bloków, w których zapisane są wszystkie transakcje dokonane kiedykolwiek przez kogokolwiek z użytkowników. Jeden blok można porównać do kartki zeszytu, w którym zapisujemy transakcje. Każda kartka ma jakiś określony rozmiar. Będzie to np. format A4, A5 czy B5. Podobnie jest z blokami w blockchainie – one również mają określoną wielkość. Przykładowo, jeden blok bitcoina to 1 MB. Bloki bitcoina są zabezpieczane za pomocą kryptografii co mniej więcej 10 minut (rysunek 2.2).

To tak, jakbyśmy zapisywali stronę zeszytu i przechodzili do kolejnej, gdy skończy się na niej miejsce lub upłynie 10 minut. W ten sposób blockchain zapisuje wszystkie transakcje. Cały ich spis to ogromna liczba bloków, które tworzą razem łańcuch. Stąd właśnie wzięła się nazwa tego systemu. Swoje wysokie bezpieczeństwo zawdzięcza on temu, że nie jesteśmy w stanie zmienić jednego bloku czy jednej transakcji bez zmiany całego łańcucha.

Czym jest bitcoin?

Bitcoin jest pierwszą kryptowalutą, która odniosła sukces – i przy okazji najbardziej popularną. Zajmuje on także pierwsze miejsce na rynku kryptowalut pod względem kapitalizacji, czyli możemy powiedzieć, że jest również największą kryptowalutą. Został utworzony w 2009 roku przez osobę o pseudonimie Satoshi Nakamoto, choć tak naprawdę historia bitcoina rozpoczęła się nieco wcześniej. Już w październiku 2008 roku Satoshi Nakamoto opublikował bowiem w sieci liczący 9 stron dokument opowiadający o idei tej kryptowaluty. Przedstawiał on zarys alternatywnego systemu płatniczego, który ma powstać w przyszłości.



Rysunek 2.3. Logo kryptowaluty bitcoin. Źródło: wikipedia.org (dostęp: 23.09.2025)

Bitcoin jest globalną, transgraniczną księgą rozrachunkową. Dzięki niemu możemy przesyłać nasze środki do każdej osoby na świecie bez żadnych pośredników i ograniczeń. Dodatkowo posiada on otwarty kod źródłowy. Tak naprawdę jest więc rozbudowanym programem komputerowym, który działa nieustannie na milionach podłączonych do internetu komputerów na całym świecie. Mimo że kod bitcoina jest publicznie dostępny i każdy może go zobaczyć (model oprogramowania open source), to nikomu dotychczas nie udało się go złamać. Model otwartego kodu źródłowego nadaje tej kryptowalucie dodatkowej transparentności i pozwala na współpracę społeczności w celu jej udoskonalenia. Jednakże do dziś nie znaleziono w nim żadnego błędu, co świadczy o znakomitej wiedzy osoby, która go opracowała.

Ponadto sam twórca bitcoina, którego prawdziwa tożsamość pozostaje nieujawniona, nie może w żadnym stopniu zmienić kodu kryptowaluty czy dodrukować sobie więcej jednostek. Ma jedynie kontrolę nad swoimi środkami trzymanymi w bitcoinie, aczkolwiek nie wykonały one żadnego ruchu od 2010 roku.

Bitcoin jest najbardziej niezależnym środkiem przekazywania wartości, który w wielu aspektach podobny jest do gotówki. Na rynku kryptowalut można spotkać się z powiedzeniem, że bitcoin to cyfrowe złoto, co nie jest błędem, gdyż cały jego kod był wzorowany właśnie na tym kruszcu. Wydobycie złota z czasem spada i staje się droższe. Podobnie jest z bitcoinem, ponieważ także pojawia się coraz mniej jednostek, a do tego ich wydobycie jest znacznie mniej opłacalne, niż to było na początku¹. W żaden sposób nie da się przyspieszyć czy zwiększyć liczby wykopywanych bitcoinów. Dzięki temu ta kryptowaluta nie doświadcza problemów związanych z nadmierną podażą pieniądza, tak jak ma to miejsce w przypadku tradycyjnych walut.

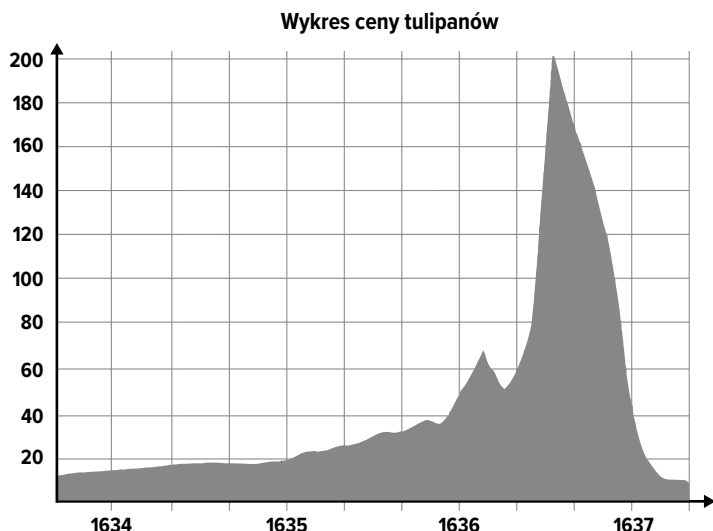
¹ Więcej o wydobywaniu kryptowalut przeczytasz w rozdziale na temat górników *Kim są górnicy i walidatorzy?*, który znajdziesz w tej części książki.

Na rynku istnieje wiele projektów podszywających się pod bitcoina, na które musisz uważać podczas dokonywania inwestycji. Nieświadomie możesz bowiem zakupić coś, czego nie chciałeś. Przykładem takich kryptowalut może być bitcoin cash, bitcoin gold czy bitcoin SV. Są to tzw. forki bitcoina. Projekty podobne do tej kryptowaluty, ale nieznacznie się różniące. Jeśli chcesz zakupić prawdziwego bitcoina, to zwróć uwagę na skróconą nazwę (zwaną również tickerem kryptowaluty), którą w tym przypadku powinno być BTC. Tyle wystarczy, aby zabezpieczyć się przed podszywającymi się kryptowalutami.

Zazwyczaj, jeśli ludzie słyszą o rynku kryptowalut, to w pierwszej kolejności dowiadują się o istnieniu bitcoina, a dopiero później o innych kryptowalutach. Bitcoin – podobnie jak i pozostałe projekty – poddawany jest dość dużym wahaniom wyceny. Nagłe zmiany wartości kryptowalut wywołują u inwestorów wiele emocji. Im wyżej jest bitcoin i im większe wzrosty osiąga, tym więcej osób chce go kupować. W końcu dochodzi do utworzenia się tzw. bańki inwestycyjnej. Bańka inwestycyjna bądź spekulacyjna to swego rodzaju gorączka na rynku danego aktywa, na którym każdy inwestor liczy na szybki zysk i przepełniony jest euforią oraz optymistycznym nastawieniem względem swojej inwestycji. Panuje wówczas ogromna chciwość – każdy chce jak najszybciej nabyć dane aktywo i osiągnąć satysfakcjonujące zyski, takie jak inni, którzy zainwestowali swoje oszczędności już wcześniej.

Nierzadko w takiej sytuacji dochodzi do przewartościowania aktywa, czyli wycena zaczyna przekraczać realną wartość przedmiotu inwestycji. Charakterystyczne dla bańki spekulacyjnej jest to, że pod koniec jej trwania do inwestycji przystępują osoby, które nigdy wcześniej nie miały do czynienia z danym aktywem i mają zerową wiedzę na jego temat.

Pierwszym przypadkiem bańki spekulacyjnej na dużą skalę była tulipomania, która nastąpiła już w XVII wieku. Wysoko wycenianym aktywem stały się cebulki tulipanów, masowo skupowane przez Holendrów ze względu na ich wielką słabość do tego kwiatu. We wczesnych latach XVII wieku cebulki tulipanów potrafiły osiągać niewiarygodne wyceny nawet tysiąca guldenów za sztukę w przypadku rzadkich odmian. Tulipany zaczęły być uważane za symbol statusu i bogactwa oraz produkt luksusowy, na który niewiele osób mogło sobie pozwolić. Prawdziwa gorączka przysłała w 1637 roku, gdy cena jednej cebulki osiągnęła astronomiczne 4 tysiące guldenów. W tym czasie miesięczna pensja wykwalifikowanego rzemieślnika oscylowała w granicach 300 guldenów rocznie. Wykres bańki spekulacyjnej na tulipanach prezentuje rysunek 2.4.



Rysunek 2.4. Wykres cenowy cebulki tulipana podczas tulipomanii. Źródło: opracowanie własne na podstawie artykułu *Behavioral Finance part 4: Herding* ze strony csspension.com (dostęp: 23.09.2025)

Holandia w tamtym czasie była krajem przodującym w rozwoju technologii finansowych. Z tego powodu Holendrzy byli zdolni do wprowadzania towarów na giełdę i szerokiej spekulacji na ich wycenach. Naturalną kolejną rzeczą zrobiono to również z tulipanami, co z pewnością przyczyniło się do tak potężnych wzrostów.

O wielkości kwiatowej bańki spekulacyjnej mogły świadczyć również zarobki handlarzy, których wynagrodzenie dochodziło do 6 tysięcy guldów. W tamtym okresie przeciętny Holender osiągał zarobki na poziomie jedynie 12,5 guldów miesięcznie.

Handel tulipanami rozrósł się do takich rozmiarów, że cebulka zmieniała właściciela średnio 10 razy dziennie, a większość transakcji dotyczyła cebulek, które jeszcze nie wyrosły. Dodatkowo płacono za nie notami kredytowymi bez pokrycia. Osoby, które kupiły tulipany na początku bańki, mogły liczyć na zwrot z inwestycji w postaci 10-krotności wydanej kwoty.

Bańki mają to do siebie, że możemy doświadczać szybkich wzrostów, ale i równie nagłych spadków. Każda bańka kiedyś pęka i dokładnie tak samo stało się z tulipomanią. Wiele osób potraciło oszczędności życia czy domy, które sprzedawano lub zastawiano, żeby nabyć więcej cebulek. Wszystko to wydarzyło się jednego dnia (3 lutego 1637 roku), kiedy na rynku rozszły się pogłoski, że nikt nie chce odkupywać tulipanów. Ponieważ uczestniczący w transakcjach uwierzyli w to, co głoszone, ostatecznie dokładnie tak się stało – nikt już nie był zainteresowany nabyciem cebulek.

Kwestię wyceny bitcoina nierzadko przyrównuje się do bańki spekulacyjnej. Pomijając fakt, że wykres przedstawiający sytuację na rynku kwiatowym podczas tulipomanii niemal odzwierciedla wykres bitcoina z 2017 roku, rzeczywiście w pewnym sensie jest to prawda. Znalazłem nawet dość ciekawe porównanie baniek inwestycyjnych, których doświadczyła ludzkość, uwzględniające bitcoina (rysunek 2.5).

Bitcoin okazuje się podstawą największej z nich. Niemniej jednak w przypadku tej kryptowaluty co jakiś czas bańka pęka, by później ponownie zacząć narastać – dzięki temu przy odpowiedniej wiedzy jesteśmy w stanie korzystać z niej wielokrotnie. Dodatkowo, zawsze w historii bitcoina działa się tak, że powracał on do swojego poprzedniego szczytu cenowego. Zatem, nawet jeśli ktoś dokonał zakupu w nieodpowiednim momencie, ale był wystarczająco cierpliwy, to i tak nie stracił na tej inwestycji.

Ludzie podczas wszystkich baniek spekulacyjnych często zachowują się nielogicznie i podejmują nieracjonalne decyzje. Zamiast kupować bitcoina, gdy jest on tani, wolą nabyć go po rekordowych wycenach. Tę sytuację można przyrównać do zrezygnowania z zakupu marynarki, gdy jest w promocji –50%, a nabycia jej, kiedy zaczyna drożeć. Tłumaczymy sobie, że to optymalna decyzja, bo jutro ta marynarka może kosztować 100 złotych więcej i z tego powodu należy kupić ją dzisiaj. Dokładnie w ten sposób postępują ludzie na rynkach finansowych.



Rysunek 2.5. Porównanie wyceny bitcoina z sytuacją na rynku podczas innych baniek spekulacyjnych. Źródło: opracowanie własne na podstawie danych z: Bloomberg, International Center for Finance at Yale School of Management, Peter Garber

Bitcoin swój pierwszy ogromny cykl wzrostowy przeżył w 2013 roku, kiedy to jego cena podskoczyła z poziomu 2 do aż 1100 dolarów². Następnie doświadczyliśmy gwałtownych spadków do wyceny około 200 dolarów. W ten sposób bitcoin zakończył swoją pierwszą bańkę spekulacyjną.

Od tamtego czasu bitcoin zyskał na popularności. Dziś istnieją setki giełd kryptowalutowych, na których możemy dokonać nabycia różnych kryptowalut, w tym oczywiście tej najpopularniejszej.

Dlaczego bitcoin ma wartość?

Po przeczytaniu fragmentu na temat bańki spekulacyjnej większość ludzi może utwierdzić się w przekonaniu, że wartość bitcoina wzięta się z powietrza i zniknie tak szybko, jak się pojawiła. Nic bardziej mylnego. Bitcoin w porównaniu do wielu innych aktywów, które dotknęła bańka, wnosi realną użyteczność do otaczającego nas świata. Zgodzę się z tym, że niektórzy inwestorzy nabywają tę kryptowalutę bez znajomości jej zalet. Jednakże każdy z nich powinien je poznać, aby wiedzieć, skąd wzięły się tak wielkie wzrosty wyceny bitcoina oraz jego popularność.

Bitcoin zyskał tak ogromną popularność ze względu na to, że jest:

- **Poręczny.**

Do korzystania z kryptowalut, w tym z bitcoina, wystarczy jedynie smartfon czy komputer. To urządzenia, które towarzyszą nam praktycznie nieustannie, co sprawia, że posługiwanie się kryptowalutami jest niezwykle wygodne i poręczne. Zazwyczaj wychodząc z domu, bierzemy ze sobą smartfon, zatem możemy mieć także pod ręką nasze kryptowaluty.

- **Przenośny.**

Ta cecha w pewien sposób odwołuje się do poprzedniej. Nasze kryptowaluty możemy trzymać na urządzeniu mobilnym czy komputerze, ale to nie wszystkie możliwości. Możemy je także „zgromadzić” na karcie SD, pendrivie czy w portfelu sprzętowym lub po prostu skorzystać z kartki. Piszząc o „trzymaniu kryptowalut”, mam na myśli przechowywanie w danym miejscu klucza prywatnego, który uprawnia nas do zarządzania własnymi kryptowalutami.

Dzięki tak wielu opcjom kryptowaluty stały się niezwykle mobilnym pieniądzem. Pionierami w tym obszarze były certyfikaty na złoto, a później

² Ilekcioć podaję jakieś wartości w dolarach, mam na myśli dolary amerykańskie – chyba że zaznaczam inaczej.

gotówka. Teraz kryptowaluty kompletnie je deklasują, bo możemy przewozić przez granicę jakiegokolwiek państwa na świecie dowolną kwotę, a zainteresowane służby się nawet o tym nie dowiedzą. To ogromna zaleta, której pozbawione są wszystkie inne formy pieniądza, poza pieniądzem cyfrowym banków.

- **Jednolity.**

Każda jednostka kryptowaluty jest taka sama, zatem reprezentuje sobą taką samą wartość. Bitcoina możemy zakupić na jednej giełdzie i za chwilę sprzedać na drugiej. Każda moneta jest jednolita, co jest niezwykle ważną cechą pieniądza. Przy okazji kryptowaluty nie ulegają zużyciu jak gotówka czy monety, więc nie musisz się martwić o straty z tego powodu.

- **Trwały.**

Kryptowaluty są niezwykle trwałym pieniądzem. Tak naprawdę nie jesteśmy w stanie ich zniszczyć. Możemy zniszczyć jedynie urządzenie przechowujące nasze klucze, zgubić je lub zapomnieć nasze hasła dostępowe (seedy).

- **Zamienny.**

Dzięki giełdom kryptowalutowym z wielką łatwością możemy zamieniać kryptowaluty między sobą czy wymieniać je na tradycyjne waluty. To czyni bitcoina niezwykle płynnym aktywem, które da się spieniężyć w bardzo krótkim czasie. Przy okazji nie obawiamy się, że przez potrzebę szybkiej sprzedaży upłynniemy aktywo po zaniżonej cenie, gdyż zawsze możemy skorzystać z innej giełdy, która oferuje korzystniejsze kursy.

- **Podzielny.**

Bitcoin jest bardziej podzielny niż tradycyjne waluty, ponieważ dzieli się do aż ośmiu miejsc po przecinku. Najmniejsza część bitcoina to jeden satoshi (rysunek 2.6). Podobnie jest z innymi kryptowalutami. Dzięki temu możemy dokonywać mikrotransakcji i przekazywać między użytkownikami niewielkie wartości. To także daje szansę na zainwestowanie nawet małej kwoty, mimo tak wysokiej wyceny bitcoina.

Wartość 1 satoshi w złotych	
Wartość 1 satoshi w bitcoinach	0,00000001 BTC
Wartość 1 satoshi w złotych	0,027 zł

Rysunek 2.6. Kurs 1 satoshi względem polskiego złotego na dzień pisania książki. Źródło: opracowanie własne na podstawie danych coingecko.com (dostęp: 23.09.2025)

- **Miernikiem wartości.**

Już dzisiaj jesteśmy w stanie w wielu miejscach zapłacić za pomocą kryptowalut, a co za tym idzie – mierzyć przy ich użyciu wartość poszczególnych dóbr. To coraz częstsze wykorzystanie ich do płatności sprawia, że powoli zaczynają przypominać „prawdziwe” pieniądze.

- **Transgranicznym środkiem wymiany i płatności.**

Ta cecha również nadaje ogromną wartość kryptowalutom, gdyż koszt płatności do osoby obok nas i tej z drugiego końca świata wynosi dokładnie tyle samo. Dla blockchaina nie ma znaczenia, gdzie znajduje się odbiorca płatności. Nieistotne jest także to, jakiej waluty używa on na co dzień. To czyni przesyłanie wartości za granicę szybszym, łatwiejszym i tańszym.

- **Rzadki.**

Bitcoin jest bardzo rzadkim aktywem – posiada on bowiem ograniczoną podaż w wysokości 21 milionów sztuk, przy czym nie wszystkie zostały jeszcze wykopane. Ponadto wiele z nich nigdy nie zostanie użytych przez swoich właścicieli. Te pochodzą z początków bitcoina, kiedy nikt nie przykładał tak wielkiej wagi do zapamiętywania kluczy do swoich portfeli, w wyniku czego zostały one zapomniane bądź zgubione. Obecnie w obiegu dostępnych jest ponad 94% wszystkich jednostek, czyli do wydobywania pozostało ich już niewiele, a popyt na bitcoina wciąż rośnie. Można zatem śmiało stwierdzić, że bitcoin jest zdecydowanie trudniej dostępny niż złoto. Stąd także wynika jego wartość i cena.

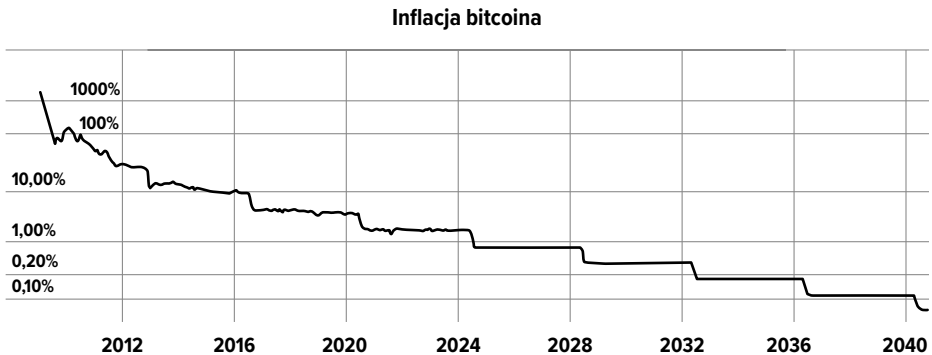
- **Środkiem tezauryzacji.**

Bitcoin w długim terminie znakomicie przechowuje wartość i zachowuje funkcję tezauryzacyjną pieniądza³, którą przestały spełniać waluty fiducjarne⁴. Dotyka je przecież nieustanna inflacja, z którą rządy bezskutecznie walczą. Tymczasem o zachowywanie wartości przez bitcoina nie musi nikt dbać, ponieważ został on odpowiednio zaprogramowany. Jeszcze w 2024 roku inflacja bitcoina ma spaść poniżej poziomu inflacji złota. Po halvingu⁵ w 2024 roku jej poziom wynosi 0,80–0,85%, co jest znakomitą wynikiem w porównaniu z tradycyjnymi walutami, i nadal będzie sukcesywnie maleć w perspektywie do 2040 roku (rysunek 2.7).

³ Funkcja tezauryzacyjna pieniądza polega na jego przechowywaniu jako środka do gromadzenia oszczędności i bogactwa.

⁴ Więcej o walutach fiducjarnych przeczytasz w rozdziale *FIAT-y, czyli waluty fiducjarne*, w części zatytułowanej *Podstawowe zagadnienia. Terminologia w świecie kryptowalut*.

⁵ Halving oznacza zmniejszanie o połowę nagrody otrzymywanej przez górnika za poprawne zaksięgowanie całego bloku. Szerzej przeczytasz o tym w rozdziale *Halvingi bitcoina*, w części zatytułowanej *Podstawowe zagadnienia. Funkcjonowanie kryptowalut*.



Rysunek 2.7. Wykres inflacji bitcoina do 2040 roku. Źródło: opracowanie własne na podstawie danych portalu Bitbo (dostęp: 23.09.2025)

- **Zdecentralizowany.**

Bitcoin jest zdecentralizowanym środkiem płatności, co czyni go najbardziej niezależnym pieniądzem ze wszystkich, które zostały dotychczas stworzone. Bardzo trudnym zadaniem jest odebranie kryptowalut innemu człowiekowi, o ile je dobrze zabezpieczył. W nasze ręce może dostać się portfel, ale nic nam to nie da, jeśli nie znamy klucza prywatnego. Inaczej jest z gotówką. Kiedy ktoś włamie się do naszego domu, gotówka z łatwością zmieni właściciela. Kryptowaluty nie.

Portfeli kryptograficznych nie da się zablokować, więc jesteś na 100% zabezpieczony przed różnymi działaniami rządzących, którzy ostatnimi czasy coraz chętniej blokują nam dostęp do kont bankowych. Znako- mitym przykładem jest Kanada, gdzie protestującym przeciwko lock-downom oraz osobom, które wspierały ten ruch, bezprawnie odebrano dostęp do ich własnych kont bankowych. W świecie kryptowalut to użytkownicy bezpośrednio między sobą dokonują transakcji. Bitcoin czyni cię niezależnym i wolnym obywatelem, gdyż to ty masz pełną kontrolę nad swoimi pieniędzmi, a nie banki, instytucje finansowe czy rządy.

- **Anonimowy.**

Na dziś kryptowaluty, w tym bitcoin, gwarantują anonimowość, ponieważ jedynym identyfikatorem użytkownika w transakcjach przeprowadzanych z pomocą blockchaina jest klucz publiczny. Jednak z każdym rokiem będzie to coraz trudniejsze, gdyż rządzący na całym świecie starają się pozbawić nas prywatności poprzez wprowadzanie licznych regulacji dotyczących kryptowalut. Pojawiają się doniesienia, że władze pracują nad algorytmami pozwalającymi ustalać tożsamość osób wykonujących transakcje z pomocą kryptowalut. We wszystkim ma pomagać sztuczna

inteligencja. Jeśli takie rozwiązanie wejdzie w życie, zachowanie anonimowości będzie naprawdę niełatwym zadaniem.

- **Transparentny.**

Wszystkie transakcje przeprowadzane za pomocą bitcoina są publiczne i weryfikowalne. Każda osoba na świecie może zobaczyć przepływy między portfelami i potwierdzenie autentyczności danych jednostek. To buduje zaufanie oraz transparentność względem kryptowalut, mimo że w tym procesie nie są ujawniane żadne dane personalne nadawców i odbiorców płatności.

Podsumowując, możemy stwierdzić, że bitcoin zyskał tak wielką popularność i idącą za tym wartość, ponieważ jest:

- poręczny i przenośny;
- jednolity i trwały;
- zamienny i podzielny;
- miernikiem wartości i transgranicznym środkiem płatności;
- rzadki i spełnia funkcję tezauryzacyjną;
- zdecentralizowany i anonimowy;
- transparentny.

Wszystkie te zalety bitcoina były kiedyś podstawowymi cechami pieniądza, które każdy uważał za niezbędne. Dzisiaj waluty tradycyjne tracą tak naprawdę funkcje pieniądza, a prawdziwym pieniądzem staje się bitcoin.

Bitcoin od samego początku dążył do tego, by stać się godnym rywalem złota. Dzisiaj w wielu aspektach zaczyna przewyższać ten kruszec, stąd jego wartość rośnie jeszcze w większym tempie. Obecnie możemy stwierdzić, że bitcoin jest najlepszą formą pieniądza, jaka istniała dotychczas na świecie.

Jak wyglądają transakcje kryptowalutowe?

Wszystkie transakcje kryptowalutowe odbywają się między **portfelami kryptograficznymi**, które można porównać do kont bankowych w tradycyjnym systemie. Jednakże w odróżnieniu od bankowości tradycyjnej portfele te nie są podpisane imieniem i nazwiskiem posiadacza. Powiązane są natomiast z dwoma kluczami – publicznym i prywatnym. **Klucz publiczny** to numer konta. Dzięki niemu inne osoby mogą przelewać nam kryptowaluty. Natomiast klucz prywatny służy do odblokowania naszego portfela. To on



Rysunek 2.8. Przykładowy wygląd klucza publicznego. Źródło: coldcryptowallet.com (dostęp: 23.09.2025)

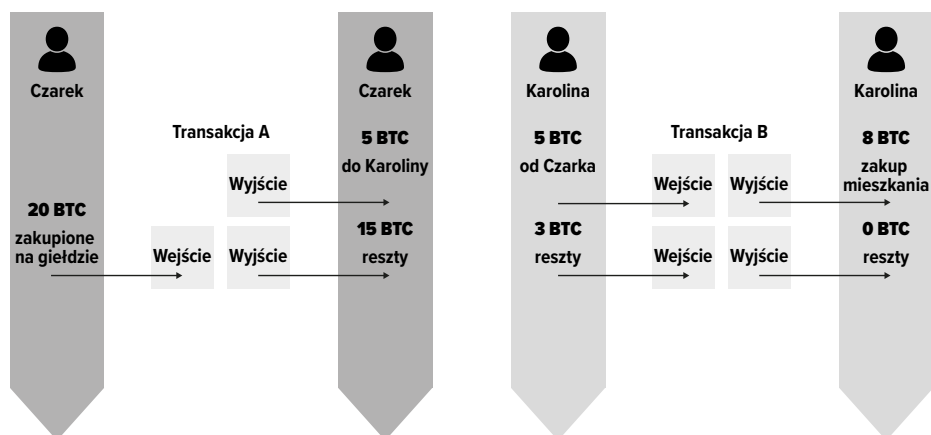
umożliwia wykonywanie transakcji. Działa to dość podobnie jak w przypadku zwykłej bankowości internetowej. Wówczas także posiadamy numer konta, bez którego nikt nie będzie w stanie przelać nam pieniędzy, oraz hasło, bez którego nie jesteśmy w stanie wykonać żadnej płatności. Oczywiście te porównania są dość prymitywne, ale wydaje mi się, że zdecydowanie pomogą ci zrozumieć istotę tego procesu.

Klucz publiczny może być zapisany w formie ciągu alfanumerycznego (długi szereg cyfr i liter połączonych bez spacji) lub kodu QR, który zdecydowanie przyspiesza proces, zmniejsza ryzyko pomyłki i jest wygodniejszy.

Jeśli masz już przygotowany klucz publiczny portfela, na który chcesz wysłać kryptowalutę, przychodzi pora na to, aby wybrać wysokość tej transakcji. Po określeniu tego parametru system sprawdza tzw. wejścia – weryfikuje, czy dysponujesz odpowiednią kwotą do pokrycia transakcji. Wejścia (inputs) to suma części bitcoina, które dają ci posiadaną wartość. Załóżmy, że jesteś w posiadaniu 1 bitcoina. Twoje wejścia mogłyby wyglądać w ten sposób – 0,4 bitcoina i 0,6 bitcoina. Potem przechodzisz do kolejnego etapu, jakim jest określenie wyjść (outputs). Każda transakcja ma ich co najmniej dwa – odbiorcę i resztę. Odbiorca to ta część kryptowaluty, którą przekazujesz do wyznaczonego portfela, a reszta to pozostała część środków do twojej dyspozycji. Jeśli wysłałbyś swojemu przyjacielowi 0,9 bitcoina, wówczas reszta wyniosłaby 0,1 bitcoina. Suma wartości wejść musi być zawsze równa sumie wyjść danej transakcji lub być od niej większa. Natomiast każde wyjście jest wejściem dla kolejnej operacji. Ten proces może wydawać się zawity, ale na pewno świetnie zobrazuje go rysunek 2.9.

Wcześniej posłużyłem się analogią do tradycyjnego systemu bankowości, aby lepiej ci to wyjaśnić. Tak naprawdę chodzi tu jedynie o przekazanie własności, gdyż środki nigdy nie opuszczają systemu blockchain danej kryptowaluty. Natomiast inaczej jest w tradycyjnej bankowości, ponieważ możemy

Transakcje w systemie blockchain



Rysunek 2.9. Transakcje w systemie blockchain. Źródło: opracowanie własne

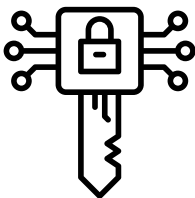
wypłacić gotówkę w bankomacie i opuścić elektroniczny system (dopóki rządy jeszcze tego nie zabroniły).

Klucz prywatny to z kolei najważniejsze zabezpieczenie twojego portfela. Jest to rodzaj hasła dający dostęp do posiadanych środków. Składa się on zazwyczaj z 12 lub 24 angielskich słów, które tworzą niemożliwą do złamania kombinację. Klucz prywatny powinien być przechowywany w bezpiecznym miejscu, gdyż po jego utracie nie jesteś w stanie odzyskać dostępu do swoich kryptowalut.

Kim są górnicy i walidatorzy?

Wcześniej wspominałem o górnikach. To właśnie oni zajmują się kopaniem kryptowalut (ang. *crypto mining*), przez co zatwierdzają transakcje, dbając o cały blockchain. Sam proces kopania kryptowalut włącznie z górnikami występuje jedynie wśród projektów, które oparte są na konsensusie Proof of Work (z ang. dowód pracy). Górnikiem lub walidatorem staje się osoba, która podłącza swój komputer do sieci. Kopanie kryptowalut wymaga udostępnienia mocy obliczeniowej swojego komputera, w którym w zależności od aktywa będą używane konkretne podzespoły. Zazwyczaj są to karty graficzne (GPU) lub wyspecjalizowane procesory ASIC. Nasz komputer podczas crypto miningu będzie rozwiązywał skomplikowane problemy matematyczne, aby zweryfikować transakcję i dodać ją do łańcucha bloków. Jej trudność rośnie wraz z zwiększaniem się dostępnej mocy obliczeniowej. Dzieje się tak, ponieważ

Klucz prywatny (private key)



Kod stosowany w kryptografii, funkcjonujący jako ciąg alfanumeryczny bądź kombinacja 12 lub 24 angielskich słów. Klucz prywatny to hasło stworzone w celu autoryzacji transakcji i potwierdzenia własności kryptowalut.

Przykładowy klucz prywatny:

**BELIVE STONE SUCCESS DUST PATIENT WHERE STADIUM DIRT ABOUT
SOLID STRIKE HEART CANDY START SENSE SCORPION GOLD HAPPY
USELESS SLENDER FILE PIPE HIGHWAY TRACK**

Rysunek 2.10. Postać klucza prywatnego. Źródło: opracowanie własne

do sieci podłączane są coraz nowsze i lepsze komputery, które nierzadko budowane są wyłącznie pod kopanie kryptowalut. Nazywa się je koparkami. Gdy odnajdą one odpowiedni ciąg znaków, dochodzi do zaksięgowania wszystkich możliwych transakcji w bloku. Za poprawne rozwiązanie bloku otrzymujemy nagrodę w postaci jednostek danej kryptowaluty oraz prowizję od transakcji. O wysokości nagrody w przypadku bitcoina decydują tzw. halvingi, o których będziemy mówić w następnym rozdziale. Podsumowując, głównym zajęciem górników jest zatwierdzanie transakcji oraz utrzymywanie sieci danej kryptowaluty.

Obecnie istnieje niewielka liczba górników, którzy są w stanie samodzielnie rozwiązać zagadkę i zaksięgować blok. Dzieje się tak zwłaszcza w przypadku bitcoina. Dlatego właśnie powstały federacje górnicze lub kopalnie (ang. *mining pool*). Są to organizacje, do których możesz dobrowolnie dołączyć i podłączyć swój komputer. Gdy dowolne urządzenie z kopalni zaksięguje blok i otrzyma nagrodę, jest ona dzielona pomiędzy wszystkich górników proporcjonalnie do wprowadzonej mocy obliczeniowej. Oczywiście od danej kwoty jest pobierana niewielka prowizja dla kopalni. Taki mechanizm pozwala na generowanie zarobku przez górników z komputerem o mniejszej mocy obliczeniowej.

Opłacalność kopania kryptowalut w Polsce

Obecnie opłacalność wydobywania kryptowalut w Polsce dla większości osób jest znikoma i zazwyczaj nie przynosi realnych zysków. Jest to spowodowane głównie wysokimi kosztami energii elektrycznej. Na moment pisania tej książki cena jednej kilowatogodziny waha się między 1,30 zł a 1,80 zł. Ponadto dochodzą dodatkowe czynniki wpływające na

opłacalność inwestycji, takie jak kosztowny zakup wyspecjalizowanego sprzętu do wydobywania kryptowalut, rozwinięta konkurencja na rynku górników przemysłowych (farmy miningowe), zwłaszcza z krajów o tańszej energii elektrycznej (np.: USA, Rosja, Kazachstan, Chiny, Norwegia) oraz rosnąca trudność wydobycia bloku.

WYLICZENIA OPŁACALNOŚCI KOPANIA KRYPTOWALUT W POLSCE

Urządzenie:	Antminer S19 Pro
Zużycie energii:	2340 kWh/miesiąc
Koszt energii:	1,50 zł/kWh
Potencjalna liczba wykopanych jednostek bitcoina:	0,0066 BTC/miesiąc
Przychody przy kursie bitcoina około 140 000 dol.:	3300 zł
Koszt prądu przy cenie 1,50 zł/kWh:	3510 zł
Bilans:	Strata –210 zł miesięcznie

Nieopłacalność wydobywania kryptowalut w naszym kraju dobitnie pokazują przedstawione wyliczenia. Sama cena energii elektrycznej sprawiła, że nasza inwestycja stała się nierentowna, pomimo nieuwzględnienia wysokich kosztów zakupu sprzętu do kopania, które mogą sięgać nawet 40 tysięcy złotych. Ponadto w obliczeniach przyjąłem bardzo optymistyczne warunki, zakładające utrzymywanie się ceny bitcoina na poziomie 140 tysięcy dolarów.

Historycznie kopanie kryptowalut w Polsce było opłacalne zwłaszcza podczas hossy w 2017 roku. Na tamten moment system kopania oferowała kryptowaluta ethereum, której wydobycie opierało się na zwykłych układach graficznych GPU. Ethereum umożliwiało otrzymywanie większej liczby nagród za obliczenia, oferowało niższy próg wejścia oraz przyciągało do siebie rzesze inwestorów, przez co mieliśmy pewność, że odsprzedamy wydobyte jednostki po korzystnej cenie. Wszystko trwało do 2022 roku, kiedy to ethereum zrezygnowało z opierania swojego blockchaina na modelu oferującym wydobycie jednostek kryptowaluty.

Podsumowując, kopanie kryptowalut w Polsce jest w większości przypadków nierentowną inwestycją. Wydobycie dla zarobku jest opłacalne wyłącznie

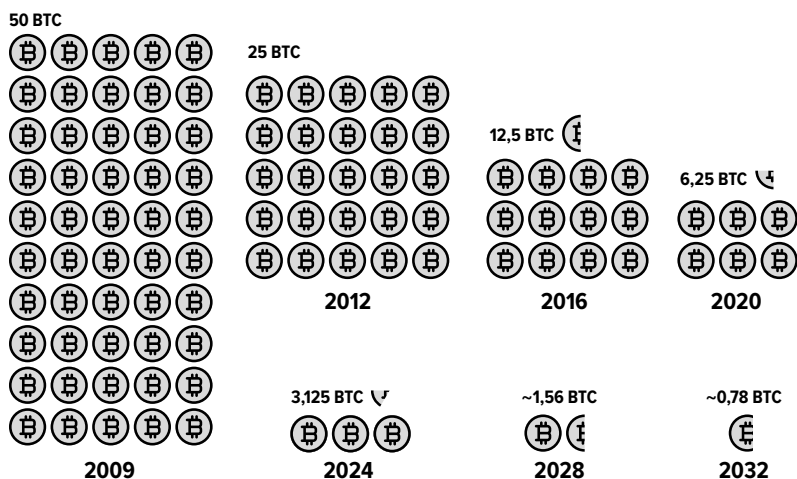
przy dostępie do bardzo taniej energii elektrycznej (np. gdy posiada się własną farmę paneli fotowoltaicznych), podczas kopania niszowych projektów z nastawieniem na spekulację bądź przy prowadzeniu działalności na skalę przemysłową.

Halvingi bitcoina

Halving bitcoina to jedno z najważniejszych wydarzeń w świecie kryptowalut. Termin ten pochodzi z języka angielskiego i wywodzi się od słowa *half*, czyli „połowa”. Oznacza on zmniejszanie o połowę nagrody otrzymywanej przez górnika za poprawne zaksięgowanie całego bloku. To wydarzenie zachodzi co 210 tysięcy bloków, czyli mniej więcej w okresie 4 lat. Z każdym halvingiem liczba monet wprowadzanych do obiegu maleje. To czyni bitcoina walutą deflacyjną, co stanowi istotny czynnik wpływający na jego wartość. Pierwszy halving nastąpił w 2012 roku, gdy nagroda za wykopanie bloku zmniejszyła się z 50 do 25 bitcoinów. Następnie w lipcu 2016 roku nagroda spadła do 12,5 bitcoina. Trzeci halving odbył się w maju 2020 roku i sprowadził ją do poziomu 6,25 bitcoina. Ostatnim był ten z kwietnia 2024 roku, kiedy nagroda została ponownie zredukowana i wynosi obecnie 3,125 bitcoina. Najbliższy halving odbędzie się w 2028 roku. Dojdzie wtedy do zmniejszenia się nagrody z 3,125 do 1,5625 bitcoina. Natomiast ostatnie podzielenie nagrody dla górników tej kryptowaluty wydarzy się w 2136 roku. Wynagrodzenie za wydobywanie bloku będzie wynosić wtedy dokładnie 0,00000001 bitcoina. Wizualizację wysokości nagrody dla górnika za wydobywanie bloku bitcoina przedstawia rysunek 2.11.

Warto jednak zauważyć, że mimo nominalnie zmniejszającej się nagrody jej realna wartość rośnie. Przykładowo, w 2016 roku cena bitcoina oscylowała w granicach 650 dolarów. Przy takiej wartości 12,5 bitcoina wyceniane było na około 8 tysięcy dolarów. W 2020 roku cena bitcoina wahała się w okolicach 10 tysięcy dolarów, zatem po halvingu nagroda dla górnika była warta ponad 62 tysiące dolarów. Natomiast gdy nastąpiło czwarte dzielenie nagrody w 2024 roku, wydobywający otrzymywał już blisko 220 tysięcy dolarów. Obecnie wspomniana nagroda dawno przekroczyła wycenę 300 tysięcy dolarów i osiąga coraz wyższe wartości (rysunek 2.12). Niemniej jednak nie możemy zapominać, iż wraz ze wzrostem jej realnej wysokości pojawia się także większa liczba górników zainteresowanych kopaniem bitcoina, a tym samym trudność wydobycia bloku rośnie. Prowadzi to z kolei do konieczności inwestowania w coraz bardziej zaawansowany i kosztowny sprzęt, który umożliwi efektywne kopanie kryptowaluty.

Halvingi bitcoina

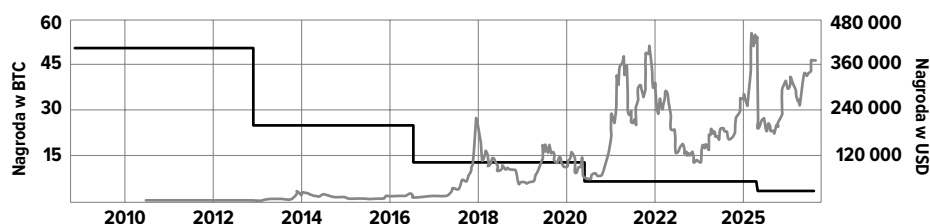


Rysunek 2.11. Wizualizacja wysokości nagrody dla górnika za wydobycie jednego bloku bitcoina po każdym halvingu w latach 2009–2032. Źródło: opracowanie własne

Halvingi bitcoina zostały świetnie zaprojektowane, ponieważ zapobiegają nadpodaży waluty i jej inflacji. Dzięki nim bitcoina dotyka niewielka inflacja sięgająca około 1%. Natomiast po ostatnim halvingu będzie to jedynie 0,001%. Są to wartości praktycznie niespotykane w ostatnich latach na papierowych walutach.

Halvingi są bardzo istotnym wydarzeniem, które wpływa na wiele czynników na specyficznym rynku kryptowalut. Dzieje się tak m.in. poprzez zachowanie górników. Gdy zmienia się wysokość ich nagrody, często decydują się nie sprzedawać aktualnie otrzymanych jednostek. To powoduje pogłębienie się spadku podaży bitcoina, który został wywołany halvingiem, i wzrost wartości bitcoina. Wykres podaży bitcoina przedstawia rysunek 2.13.

Wysokość nagrody dla górnika za wydobycie bloku bitcoina



Rysunek 2.12. Wykres nagrody dla górników za wydobycie bloku bitcoina w bitcoinach (BTC) oraz dolarach amerykańskich (USD). Źródło: opracowanie własne na podstawie danych Bitcoin Visuals