# **Wszystko o blockchain**

**ENCYKLOPEDIA BLOCKCHAIN**

MATEUSZ ZDUNEK

(Imprint Logo)

Copyright © 2023 by Mateusz Zdunek.

All rights reserved. No part of this book may be used or reproduced in any form whatsoever without written permission except in the case of brief quotations in critical articles or reviews.

Printed in the United States of America.

For more information, or to book an event, contact :

(Email & Website)

<http://www.website.com>

Book design by (Name of Designer)

Cover design by Name of Designer)

ISBN - Paperback: 123456789

ISBN - Hardcover : 123456789

Pierwsza Edycja: Sierpień 2023

# CONTENTS

[1 1](#_Toc98233615)

[2 7](#_Toc98233616)

[3 13](#_Toc98233617)

[About the Author 19](#_Toc98233618)

[Acknowledgments 20](#_Toc98233619)

ROZDZIAŁ 1

**1.WPROWADZENIE**

**1.1 Czym jest blockchain?**

Blockchain to zaawansowana technologia informatyczna, która służy do przechowywania, zabezpieczania i zarządzania danymi w sposób zdecentralizowany i niezmienialny. Jest to rodzaj rozproszonej bazy danych, która składa się z bloków informacji połączonych w łańcuch. Każdy blok zawiera dane transakcji, zapisane w postaci kryptograficznych funkcji skrótu, oraz odniesienie (hash) do poprzedniego bloku, co zapewnia integralność i chroni przed możliwością zmiany wcześniejszych danych.

**Podstawowe pojęcia związane z blockchainem:**

**Blok:** Jest to jednostka danych w blockchainie, która zawiera zestaw transakcji lub informacji. Blok posiada unikalny identyfikator (hash), który odnosi się do poprzedniego bloku w łańcuchu.

**Hash:** To unikalny ciąg znaków, który jest wynikiem przeliczenia danych za pomocą kryptograficznej funkcji skrótu. Umożliwia on weryfikację, czy dane w bloku nie zostały zmienione.

**Sieć rozproszona:** Oznacza, że dane w blockchainie są przechowywane na wielu węzłach (komputerach) w sieci, a nie w centralnym serwerze. Każdy węzeł posiada kopię całego łańcucha bloków, co zapewnia redundancję i odporność na awarie.

**Konsensus:** Jest to mechanizm, który pozwala na osiągnięcie zgodności między wszystkimi węzłami w sieci co do stanu danych. Mechanizm konsensusu jest kluczowy dla utrzymania integralności i bezpieczeństwa blockchaina.

**Dlaczego jest tak ważny w dzisiejszym świecie?**

Blockchain zdobył ogromne znaczenie w dzisiejszym świecie z kilku kluczowych powodów:

Bezpieczeństwo: Blockchain zapewnia wysoki poziom bezpieczeństwa dzięki wykorzystaniu kryptografii. Dane są zabezpieczone za pomocą zaawansowanych algorytmów, co utrudnia możliwość ingerencji lub fałszowania informacji.

Transparencja: Wszystkie transakcje w blockchainie są jawne i dostępne dla wszystkich uczestników sieci. To sprawia, że blockchain jest transparentny i umożliwia weryfikację działania bez zaufania do jednej centralnej instytucji.

Brak pośredników: W tradycyjnych systemach finansowych lub prawniczych wymagana jest obecność pośredników, takich jak banki czy notariusze. Blockchain pozwala na bezpośrednie przesyłanie wartości między stronami bez konieczności zaufania do pośredników.

Niemożliwość cenzurowania: Ze względu na rozproszoną naturę blockchaina, dane są odporne na cenzurę i trudne do usunięcia. To może mieć ogromne znaczenie w przypadku przechowywania informacji publicznych czy ochrony praw człowieka.

Innowacje i nowe zastosowania: Blockchain otwiera drogę do nowych zastosowań i innowacyjnych rozwiązań w różnych dziedzinach, takich jak finanse, opieka zdrowotna, logistyka, czy zarządzanie danymi.

Wartość blockchaina jako technologii przyszłości rośnie z każdym rokiem, a jej zastosowania stale się rozszerzają. Blockchain ma potencjał do rewolucjonizacji wielu aspektów naszego życia, zmieniając sposób, w jaki przechowujemy, dzielimy się i zaufamy danym.

**1.2 Historia i powstanie technologii blockchain**

**Geneza blockchaina**

Idea blockchaina sięga początku lat 90. XX wieku, kiedy to Stuart Haber i W. Scott Stornetta opublikowali badania dotyczące bezpiecznego przechowywania czasowych pieczęci dla dokumentów elektronicznych. Ich prace związane z technologią łańcucha bloków miały na celu zapobieganie fałszerstwom i manipulacjom w przechowywanych danych.

Prawdziwy przełom w historii blockchaina nastąpił jednak w 2008 roku, kiedy to osoba lub grupa o pseudonimie "Satoshi Nakamoto" opublikowała biały papier opisujący koncepcję kryptowaluty Bitcoin oraz jej technologiczne podstawy. To właśnie w tym dokumencie po raz pierwszy pojawił się opis blockchaina jako rozproszonej, niezmienialnej bazy danych.

**Pierwsze zastosowanie w kryptowalutach**

W styczniu 2009 roku uruchomiono sieć Bitcoin, która stała się pierwszym komercyjnym zastosowaniem technologii blockchain. Bitcoin był pionierską kryptowalutą, której podstawową funkcją była możliwość bezpośredniego przesyłania wartości między uczestnikami sieci, bez pośrednictwa instytucji finansowych.

W sieci Bitcoin każda transakcja jest grupowana w bloki, które zawierają informacje o nadawcy, odbiorcy, kwocie oraz sygnaturze czasowej. Następnie bloki są łączone ze sobą w łańcuch, co tworzy niezmienialny i publiczny rejestr transakcji.

Sukces Bitcoin spowodował, że pojawiły się kolejne kryptowaluty oparte na technologii blockchain, takie jak Ethereum, Litecoin czy Ripple. Każda z nich wykorzystuje blockchain w inny sposób, co umożliwiło rozwój różnorodnych zastosowań w obszarze finansów, rozwiązywania problemów społecznych i biznesowych.

Poza sektorem kryptowalut, blockchain znalazł zastosowanie w innych dziedzinach, takich jak opieka zdrowotna, łańcuchy dostaw, głosowanie, zarządzanie danymi i wiele innych. Jego unikalne cechy, takie jak bezpieczeństwo, niemożliwość cenzurowania oraz transparentność, sprawiły, że coraz więcej przedsiębiorstw i instytucji zaczęło eksplorować potencjał tej technologii.

Od momentu powstania Bitcoin, blockchain przeżywał dynamiczny rozwój i ewolucję, a jego znaczenie w dzisiejszym świecie nie przestaje rosnąć. Technologia ta może mieć znaczący wpływ na przyszłość wielu dziedzin życia, rewolucjonizując sposób, w jaki zarządzamy danymi, transakcjami i relacjami między ludźmi i instytucjami.

ROZDZIAŁ 2

2.ZASADY DZIAŁANIA BLOCKCHAIN

**2.1 Struktura bloku**

Blockchain składa się z serii bloków, a każdy blok jest fundamentalną jednostką danych w tej technologii. Struktura bloku w blockchainie jest dobrze zdefiniowana i składa się z kilku kluczowych elementów.

**Transakcje i dane przechowywane w bloku:**

Głównym zadaniem blockchaina jest rejestrowanie transakcji, czyli wszelkich operacji przekazywania wartości między uczestnikami sieci. Te transakcje są grupowane w bloki, które następnie są dodawane do łańcucha bloków.

Każdy blok zawiera zestaw transakcji, które zostały wykonane w określonym okresie czasu. Na przykład w przypadku blockchaina Bitcoin, blok może zawierać wiele transakcji, które zostały przeprowadzone w ciągu około 10 minut, a następnie zostają zgrupowane w jeden blok.

Ponadto w bloku znajduje się także nagłówek, który zawiera metadane, takie jak znacznik czasu, numer wersji bloku, dowód wykonanej pracy (Proof-of-Work) oraz dowód poprzedniego bloku (hash poprzedniego bloku). Nagłówek ten umożliwia łączenie bloków w łańcuch i zapewnia spójność całej sieci.

**Powiązania między blokami - łańcuch bloków:**

Istotnym aspektem blockchaina jest łączenie bloków w łańcuch. Każdy blok zawiera unikalny identyfikator (hash) wyliczony z danych transakcji oraz nagłówka bloku. Ten hash pełni rolę ogniwia łączącego jeden blok z poprzednim, tworząc tym samym łańcuch bloków.

Gdy nowy blok zostaje dodany do łańcucha, jego hash jest również zawarty w nagłówku kolejnego bloku. To powiązanie między blokami sprawia, że zmiana danych w jednym bloku wymagałaby zmiany wszystkich kolejnych bloków w łańcuchu, co jest praktycznie niemożliwe do wykonania.

Dzięki tej właściwości, blockchain jest niezmienialny, a raz dodane dane stają się trwałe i niemożliwe do modyfikacji. To daje użytkownikom pewność, że informacje przechowywane w blockchainie są bezpieczne i nie podlegają fałszowaniu.

Powiązania między blokami sprawiają, że blockchain jest odporne na ataki typu 51% oraz zapewnia spójność i bezpieczeństwo całej sieci. Dzięki tym cechom, blockchain stał się fundamentem dla wielu kryptowalut oraz innych zastosowań w różnych dziedzinach, które wymagają niezmienialnych i bezpiecznych danych.

**2.2 Mechanizm konsensusu**

W blockchainie, mechanizm konsensusu odgrywa kluczową rolę w zapewnieniu zgodności między wszystkimi węzłami w sieci co do stanu danych. Mechanizm ten jest odpowiedzialny za wybór wersji łańcucha bloków, która jest uznawana za najdłuższą i najbardziej wiarygodną. Głównym celem mechanizmu konsensusu jest zapobieganie podwójnym wydatkom (double spending) oraz atakom na integralność sieci.

Współcześnie stosowane mechanizmy konsensusu to m.in.:

**Dowód Pracy (Proof-of-Work - PoW)**

Dowód Pracy jest najstarszym i najbardziej znanym mechanizmem konsensusu, używanym m.in. przez Bitcoin. W tym algorytmie, kopiący (ang. miner) muszą rozwiązać skomplikowany problem matematyczny, który wymaga dużej mocy obliczeniowej. Rozwiązanie tego problemu jest bardzo trudne do znalezienia, ale łatwe do zweryfikowania. Pierwszy kopiący, który rozwiąże problem, ma prawo dodać nowy blok do łańcucha i otrzymać nagrodę w postaci nowo wygenerowanych kryptowalut.

Zaletą PoW jest to, że utrudnia ataki na sieć, ponieważ atakujący musiałby posiadać większość mocy obliczeniowej w sieci, co jest bardzo kosztowne i nierealne. Jednak ten mechanizm jest bardzo energochłonny i generuje duże zużycie energii elektrycznej.

**Dowód Udziału (Proof-of-Stake - PoS)**

W tym mechanizmie konsensusu, nowy blok jest wybierany na podstawie udziału (stake) posiadanych kryptowalut przez uczestników sieci. Właściciele kryptowalut są wybierani losowo do potwierdzenia transakcji i dodania bloku do łańcucha. Im więcej kryptowalut posiada dany użytkownik, tym większe prawdopodobieństwo, że zostanie wybrany jako kopiący.

Dowód Udziału jest bardziej energooszczędny niż PoW, ponieważ nie wymaga ogromnej mocy obliczeniowej. Jednak w tym modelu bogatsi użytkownicy mogą mieć większy wpływ na decyzje w sieci, co nie zawsze jest postrzegane jako sprawiedliwe.

**Inne algorytmy konsensusu:**

Oprócz PoW i PoS, istnieje wiele innych algorytmów konsensusu, takich jak Delegated Proof-of-Stake (DPoS), Proof-of-Authority (PoA), Proof-of-Space (PoSpace) i wiele innych. Każdy z nich ma swoje unikalne cechy i zastosowania, które mogą być odpowiednie dla różnych typów blockchainów i sieci.

Wybór odpowiedniego mechanizmu konsensusu zależy od konkretnego zastosowania i celu danej sieci blockchain. Każdy z tych mechanizmów ma swoje zalety i ograniczenia, a ich rozwój i doskonalenie trwa wciąż, aby sprostać wymaganiom rosnącej liczby zastosowań i użytkowników blockchaina.

**2.3 Sieć rozproszona**

**Rola węzłów w sieci:**

Węzły stanowią fundament sieci blockchain i pełnią kluczową rolę w utrzymaniu integralności i zabezpieczeniu danych. Każdy węzeł to indywidualny komputer, który jest połączony z innymi węzłami w sieci. Wszystkie węzły posiadają kopię całego łańcucha bloków, co oznacza, że cała sieć rozproszona przechowuje dane. Każdy węzeł wykonuje pewne zadania, które różnią się w zależności od rodzaju mechanizmu konsensusu i roli w sieci.

W sieci Proof-of-Work, węzły (kopiący) konkurują ze sobą, rozwiązując skomplikowane problemy matematyczne, aby dodawać nowe bloki do łańcucha i otrzymywać nagrody w postaci kryptowalut. Węzły Proof-of-Stake są wybierane losowo do potwierdzania transakcji w oparciu o ilość posiadanych przez nie kryptowalut. Inne mechanizmy konsensusu mają swoje unikalne role i obowiązki dla węzłów w sieci.

Węzły pełnią funkcję weryfikacji i przekazywania transakcji, a także utrzymują historię wszystkich przeprowadzonych transakcji w blockchainie. Poprzez proces weryfikacji, węzły dbają o to, aby jedynie poprawne transakcje były dołączane do łańcucha bloków, a próby fałszerstwa lub podwójnego wydatku były wykrywane i odrzucane.

**Zalety i wady rozproszenia:**

**Zalety:**

**1. Bezpieczeństwo**: Sieć rozproszona zapewnia wysoki poziom bezpieczeństwa. Atak na pojedynczy węzeł lub grupę węzłów nie jest w stanie zakłócić integralności całej sieci. Dane są rozproszone na wielu węzłach, co utrudnia ich manipulację.

**2. Odporność na awarie:** W przypadku awarii jednego lub kilku węzłów, pozostałe węzły nadal działają i utrzymują sieć w funkcjonującym stanie. To sprawia, że sieć rozproszona jest bardziej odporna na uszkodzenia i awarie.

**3. Niemożliwość cenzurowania:** Węzły w sieci rozproszonej są niezależne, co oznacza, że żadna pojedyncza instytucja lub osoba nie ma pełnej kontroli nad całą siecią. To zapewnia niemożliwość cenzurowania lub blokowania dostępu do danych.

**4. Skalowalność:** Dzięki rozproszeniu danych na wielu węzłach, sieć blockchain jest bardziej skalowalna, umożliwiając obsługę większej liczby transakcji i użytkowników.

**Wady:**

**1. Wysoki koszt energii:** W mechanizmie Proof-of-Work, proces kopania jest bardzo energochłonny, co generuje duże zużycie energii elektrycznej.

**2. Wymagane zasoby:** Każdy węzeł musi posiadać odpowiednie zasoby obliczeniowe, pamięć i łącze internetowe, co może stanowić wyzwanie w przypadku sieci o dużym rozmiarze.

**3. Wolniejsze tempo transakcji:** W niektórych blockchainach, ze względu na mechanizmy konsensusu i weryfikacji transakcji przez węzły, czas przetwarzania transakcji może być wolniejszy w porównaniu do tradycyjnych systemów płatności.

Mimo wad, rozproszona natura sieci blockchain ma znaczące zalety i przyczyniła się do rewolucji w wielu dziedzinach, a technologia ta nadal rozwija się i znajduje coraz szersze zastosowanie w dzisiejszym świecie.

ROZDZIAŁ 3

KLUCZOWE CECHY BLOCKCHAIN

**3.1 Bezpieczeństwo**

**Kryptografia w blockchainie:**

Kryptografia odgrywa kluczową rolę w zapewnieniu bezpieczeństwa w blockchainie. To gałąź nauki zajmująca się technikami szyfrowania i zabezpieczania danych. W blockchainie, kryptografia jest używana w wielu miejscach, aby chronić informacje i zapewnić poufność, integralność i autentyczność transakcji.

**Główne elementy kryptografii w blockchainie to:**

**1.** **Funkcje skrótu**: Są to matematyczne algorytmy, które przekształcają dane wejściowe (np. dane transakcji) w unikalny ciąg znaków, który jest nazywany "hashem". Hash to identyfikator bloku, który jest używany jako odniesienie do poprzedniego bloku i łączy kolejne bloki w łańcuch.

**2.** **Klucze kryptograficzne**: W blockchainie wykorzystuje się parę kluczy - klucz prywatny i klucz publiczny. Klucz prywatny jest używany do podpisywania transakcji i jest przechowywany tylko przez właściciela. Klucz publiczny jest rozpowszechniany w sieci i służy do weryfikacji podpisów transakcji. Kryptografia klucza zapewnia, że tylko właściciel klucza prywatnego może podpisywać transakcje.

**3.** **Szyfrowanie danych:** W niektórych blockchainach można stosować szyfrowanie, aby dodatkowo zabezpieczyć dane przed dostępem osób trzecich. Szyfrowanie pozwala na przechowywanie poufnych informacji, takich

jak dane medyczne czy dane osobowe, w

bezpieczny sposób.

**Odporność na ataki i ingerencję zewnętrzną:**

Bezpieczeństwo w blockchainie jest osiągane dzięki wielu aspektom, które zapewniają odporność na ataki i ingerencję zewnętrzną:

**1. Decentralizacja:** Sieć rozproszona blockchaina jest odporna na ataki, ponieważ dane nie są przechowywane w jednym miejscu. Wprowadzenie zmian lub fałszerstwo jednego bloku wymagałoby zmiany wszystkich kolejnych bloków, co jest praktycznie niemożliwe do wykonania.

**2. Mechanizm konsensusu:** Mechanizmy konsensusu, takie jak Proof-of-Work i Proof-of-Stake, wymagają zaangażowania zasobów, takich jak moc obliczeniowa lub posiadane kryptowaluty. Atakujący musiałby posiadać znaczną część zasobów sieci, aby zakłócić jej integralność.

**3. Otwartość i transparentność:** Dane w blockchainie są jawne i dostępne dla każdego uczestnika sieci. Każdy może śledzić historię transakcji i weryfikować działania sieci, co wprowadza dodatkową przejrzystość i zaufanie.

**4. Kryptografia:** Zastosowanie kryptografii zapewnia bezpieczeństwo i poufność danych. Hashowanie i podpisy cyfrowe utrudniają manipulację danymi i zapobiegają fałszerstwom.

**5. Bezpieczne protokoły komunikacyjne:** Sieci blockchain wykorzystują zaawansowane protokoły komunikacyjne, które zapewniają bezpieczną wymianę informacji między węzłami.

Mimo że blockchain jest bardzo bezpieczną technologią, nie jest całkowicie odporny na ataki. Są znane przypadki incydentów związanych z kradzieżą kryptowalut lub atakami na mniejsze i mniej zabezpieczone sieci. Dlatego też ciągły rozwój i doskonalenie technologii oraz świadomość użytkowników są kluczowe dla utrzymania wysokiego poziomu bezpieczeństwa

w blockchainie.

**3.2 Niezmienność danych**

**Mechanizm chainceqingu (Chain Chaining):**

Chain Chaining to mechanizm, który zapewnia, że każdy nowy blok w blockchainie jest powiązany z poprzednim, tworząc tym samym ciągły i niezmienny łańcuch bloków. Głównym celem tego mechanizmu jest zapewnienie niemożliwości zmiany już zapisanych danych. Po dodaniu bloku do łańcucha, jest on ściśle powiązany z poprzednim blokiem, co oznacza, że jego zawartość staje się niezmienną i chronioną przed ingerencją.

Właściwość chainceqingu jest zapewniana dzięki użyciu unikalnych identyfikatorów (hashy) dla każdego bloku. Hash każdego bloku zawiera informację o poprzednim bloku, co tworzy ciągłą i niezmienialną strukturę. Gdyby dane w dowolnym bloku zostały zmienione, spowodowałoby to zmianę jego hashu oraz

hashów wszystkich kolejnych bloków, co jest niepraktyczne i praktycznie niemożliwe do wykonania, biorąc pod uwagę ogromną moc obliczeniową, która byłaby wymagana do przeliczenia hashów wszystkich bloków od tego momentu.

**Korzyści wynikające z niemutowalności danych:**

Niemutowalność danych w blockchainie ma wiele korzyści:

**Bezpieczeństwo**: Niemożliwość zmiany danych po ich dodaniu do blockchainu sprawia, że informacje są bezpieczne i chronione przed fałszowaniem. To zapewnia zaufanie i bezpieczeństwo danych w sieci.

**Integryty**: Niemutowalność danych zapewnia integralność całej sieci. Użytkownicy mogą być pewni, że dane nie zostały zmienione lub usunięte przez niepożądane osoby.

**Historia transakcji:** Niemutowalność umożliwia śledzenie historii wszystkich transakcji w sieci od samego początku. To pozwala na weryfikację i

audyt, co jest szczególnie ważne w sektorze finansowym i innych dziedzinach, które wymagają szczególnej troski o śledzenie operacji.

**Wiarygodność:** Niemutowalność danych sprawia, że blockchain staje się bardziej wiarygodny dla użytkowników. Niezmienni stan informacji jest weryfikowalny przez każdego, co wprowadza przejrzystość i zaufanie.

**Odporność na cenzurę:** Ponieważ dane w blockchainie są niezmienne, sieć staje się odporna na cenzurę i blokowanie dostępu do danych przez niepożądane podmioty.

**Niemutowalność** danych w blockchainie jest kluczową cechą tej technologii, która umożliwia przechowywanie i zarządzanie danymi w sposób bezpieczny, niezawodny i bezpieczny. To właśnie dzięki tej właściwości blockchain zyskuje coraz większe zastosowanie w różnych dziedzinach, które wymagają niezmienialnych i wiarygodnych danych.

**3.3 Anonimowość i prywatność**

**Identyfikacja użytkowników w sieci blockchain:**

Sieć blockchain jest znana z pewnego stopnia anonimowości, jednak w rzeczywistości nie jest ona absolutna. W blockchainie, użytkownicy są identyfikowani za pomocą swoich kluczy kryptograficznych. Każdy użytkownik posiada unikalny klucz prywatny i odpowiadający mu klucz publiczny. Klucz publiczny jest używany do identyfikacji uczestników sieci, ale nie ujawnia ich tożsamości. Oznacza to, że transakcje są wykonywane między kluczami publicznymi, a nie między nazwiskami czy adresami e-mail.

Choć tożsamość użytkowników nie jest publicznie znana, to jednak blockchain jest w pełni przezroczysty. Oznacza to, że wszystkie transakcje są dostępne publicznie w łańcuchu bloków i można je śledzić. Transakcje są zapisane na zawsze i można je prześledzić od samego początku istnienia blockchaina. W związku z tym, choć identyfikacja użytkowników jest trudna do przeprowadzenia bez odpowiednich informacji dodatkowych, takie

 jak dane z zewnątrz blockchaina, wszystkie operacje są widoczne dla wszystkich uczestników sieci.

**Prywatność a transparentność:**

Prywatność i transparentność w blockchainie są dwoma sprzecznymi cechami, które stanowią wyzwanie w tej technologii.

Z jednej strony, blockchain jest transparentny, ponieważ wszystkie transakcje są publiczne i dostępne dla wszystkich uczestników sieci. To zapewnia przejrzystość i zaufanie, ponieważ każdy może zweryfikować historię transakcji i działania w sieci.

Z drugiej strony, blockchain ma pewien poziom prywatności, ponieważ użytkownicy są identyfikowani tylko za pomocą kluczy kryptograficznych, a nie za pomocą swoich personalnych danych. To daje pewien stopień anonimowości i chroni tożsamość użytkowników. Jednak w przypadku, gdy użytkownik ujawni swoje dane osobowe lub powiąże swoją tożsamość z kluczem publicznym, jego działania

w sieci mogą zostać ujawnione.

Dlatego też w przypadku blockchaina, prywatność i transparentność są postrzegane jako dwie różne cechy, które można regulować i dostosowywać do konkretnego zastosowania. Istnieją również innowacyjne rozwiązania, takie jak tzw. "prywatne blockchainy" (private blockchains), które ograniczają dostęp do danych tylko do określonych uczestników, co pozwala na zachowanie większego poziomu prywatności, ale kosztem częściowej transparentności.

**3.4 Efektywność i wydajność**

**Porównanie z tradycyjnymi bazami danych:**

Blockchain a tradycyjne bazy danych mają różnice zarówno w strukturze, jak i w sposobie działania, co wpływa na ich efektywność i wydajność w różnych zastosowaniach.

**Struktura:** W tradycyjnych bazach danych dane są zazwyczaj przechowywane w centralnym repozytorium, podczas gdy w blockchainie

dane są rozproszone na wielu węzłach. Ta decentralizacja w blockchainie zapewnia większe bezpieczeństwo i odporność na awarie, ale może wpływać na wydajność w przypadku dużych sieci.

**Transakcje:** W tradycyjnych bazach danych transakcje są wykonywane w obrębie pojedynczej bazy danych i są zazwyczaj szybkie. W blockchainie transakcje muszą być potwierdzone i uwzględnione przez wiele węzłów, co może prowadzić do nieco wolniejszego tempa przetwarzania transakcji.

**Skalowalność:** W tradycyjnych bazach danych można łatwo skalować pojemność i moc obliczeniową poprzez zwiększenie zasobów serwera. W blockchainie skalowalność jest bardziej złożona, ponieważ każdy węzeł musi utrzymywać kopię całego łańcucha bloków. W przypadku publicznych blockchainów, problem skalowalności jest jednym z głównych wyzwań.

**Bezpieczeństwo:** Blockchain zapewnia wysoki poziom bezpieczeństwa dzięki mechanizmom kryptograficznym i rozproszeniu danych.

Tradycyjne bazy danych są bardziej podatne na ataki, ponieważ wszystkie dane są przechowywane w jednym miejscu.

**Koszty:** W tradycyjnych bazach danych koszty utrzymania infrastruktury są często niższe, zwłaszcza w mniejszych skalach. W blockchainie koszty mogą być wyższe, ze względu na potrzebę utrzymywania wielu węzłów i zasobów obliczeniowych.

**Czynniki wpływające na wydajność blockchaina:**

Na wydajność blockchaina może wpływanć wiele czynników:

**Mechanizm konsensusu:** Niektóre mechanizmy konsensusu, takie jak Proof-of-Work, mogą być bardziej czasochłonne i wymagać większej mocy obliczeniowej. Inne mechanizmy, takie jak Proof-of-Stake, mogą być bardziej energooszczędne, ale wymagają odpowiedniej ilości kryptowalut jako wkładu.

**Rozmiar bloku:** Większy rozmiar bloku może

pomieścić więcej transakcji, ale może również wpłynąć na czas wymagany do propagacji bloku przez sieć.

**Liczba węzłów:** Im większa liczba węzłów w sieci, tym dłużej może trwać proces potwierdzania i propagacji transakcji.

**Poziom aktywności:** Wielkość ruchu i ilość przeprowadzanych transakcji w danej sieci blockchain może wpływać na wydajność.

**Technologie i protokoły:** Wydajność blockchaina może być również wpływana przez zastosowane technologie i protokoły komunikacyjne.

**Skalowalność:** Brak skalowalności może ograniczać wydajność blockchaina, zwłaszcza w przypadku dużych i rozbudowanych sieci.

Ogólnie rzecz biorąc, wydajność blockchaina jest wynikiem różnych kompromisów między bezpieczeństwem, skalowalnością i szybkością transakcji. Istnieją różne rozwiązania i

technologie, które są rozwijane w celu poprawy wydajności blockchaina, aby sprostać różnorodnym potrzebom i zastosowaniom.

ROZDZIAŁ 4

4.Rodzaje blockchain

**4. Rodzaje Blockchain**

**4.1 Publiczny, prywatny i konsorcjalny**

Blockchain może występować w różnych konfiguracjach w zależności od poziomu dostępności, kontroli i uczestnictwa w sieci. Trzy główne rodzaje sieci blockchain to: publiczny, prywatny i konsorcjalny. Poniżej opisane są różnice między nimi oraz przykłady zastosowań dla każdego typu:

**1. Publiczny blockchain:**

**Różnice:**

- Publiczny blockchain jest otwarty dla wszystkich użytkowników i każdy może dołączyć do sieci, tworzyć transakcje oraz weryfikować dane.

- Węzły w publicznym blockchainie działają anonimowo, a tożsamość użytkowników jest identyfikowana tylko za pomocą kluczy kryptograficznych.

- Mechanizmy konsensusu, takie jak Proof-of-Work (PoW) lub Proof-of-Stake (PoS), zapewniają bezpieczeństwo i integralność danych.

**Przykłady zastosowań:**

- Najbardziej znane przykłady to Bitcoin i Ethereum - publiczne blockchainy wykorzystywane jako kryptowaluty i platformy do tworzenia inteligentnych kontraktów.

- Śledzenie łańcucha dostaw, gdzie każdy uczestnik może śledzić drogę produktu od producenta do konsumenta.

- Elektroniczne głosowanie, gdzie każdy głos jest

publicznie zapisany, a anonimowość

uczestników jest zachowana.

**2. Prywatny blockchain:**

**Różnice:**

- Prywatny blockchain jest zamknięty i dostępny tylko dla wybranych użytkowników lub organizacji.

- Zazwyczaj wymaga zgody na uczestnictwo i może być bardziej scentralizowany niż publiczny blockchain.

- Użytkownicy są identyfikowani, co zapewnia wyższy poziom kontroli i bezpieczeństwa.

**Przykłady zastosowań:**

- Korporacje mogą używać prywatnego blockchainu do zarządzania danymi wewnątrz firmy, ułatwiając szybkie i bezpieczne transakcje między oddziałami.

- Banki mogą używać prywatnego blockchainu do przyspieszenia rozliczeń między sobą.

- Systemy medyczne mogą wykorzystywać prywatny blockchain do przechowywania

danych medycznych pacjentów w bezpieczny

sposób.

**3. Konsorcjalny blockchain:**

**Różnice:**

- Konsorcjalny blockchain łączy cechy publicznego i prywatnego blockchainu.

- Uczestnicy są wybrani i wymagana jest ich zgoda na uczestnictwo, ale w przeciwieństwie do prywatnego blockchainu, węzły mogą działać anonimowo.

- Używa mechanizmów konsensusu, które są bardziej energooszczędne niż Proof-of-Work.

**Przykłady zastosowań:**

- Współpraca między różnymi instytucjami w celu zarządzania danymi w sposób transparentny i bezpieczny.

- Konsorcjum banków, które wspólnie wdraża rozwiązania blockchain w celu poprawy efektywności i bezpieczeństwa transakcji między bankami.

- Branża ubezpieczeniowa, która może korzystać z konsorcjalnego blockchainu do dzielenia się danymi i redukcji oszustw.

Warto zauważyć, że istnieje wiele różnych implementacji i konfiguracji blockchainów, a niektóre sieci mogą mieć cechy kilku typów jednocześnie. Wybór odpowiedniego rodzaju blockchainu zależy od specyficznych potrzeb i wymagań projektu lub zastosowania.

**4.2 Blockchain Bitcoin i Ethereum**

**Bitcoin:**

Bitcoin jest jednym z pierwszych i najbardziej znanych blockchainów. Został wprowadzony w 2009 roku przez osobę (lub grupę osób) znającą się pod pseudonimem Satoshi Nakamoto. Bitcoin jest głównie wykorzystywany jako kryptowaluta, ale jego blockchain jest jednym z najważniejszych elementów tej technologii.

**Cechy wyróżniające Bitcoin:**

**1.** **Pierwsza kryptowaluta:** Bitcoin był pierwszą kryptowalutą, która zdobyła ogromną popularność i stała się symbolem całej branży blockchain.

**2.** **Mechanizm konsensusu:** Bitcoin używa Proof-of-Work jako swojego mechanizmu konsensusu. Kopacze (miners) rozwiązują skomplikowane problemy matematyczne, aby potwierdzić transakcje i utworzyć nowe bloki.

**3.** **Ograniczenie podaży:** W systemie Bitcoin istnieje ograniczenie ilości Bitcoinów do 21 milionów. To sprawia, że jest to aktyw o ograniczonej podaży, co może wpływać na cenę i atrakcyjność jako wartościowy zasób.

**4.** **Podstawowa funkcja:** Głównym zastosowaniem Bitcoin jest jako cyfrowa waluta, która umożliwia przesyłanie wartości między uczestnikami bez pośredników.

**Ograniczenia:**

**1.** **Wydajność i skalowalność:** Blockchain Bitcoin może obsłużyć około 7 transakcji na sekundę,

co jest stosunkowo niską wartością w porównaniu do tradycyjnych systemów płatności.

**2.** **Wolny czas transakcji:** Transakcje w blockchainie Bitcoin wymagają czasem potwierdzenia przez wiele bloków, co może spowodować wolniejszy czas przetwarzania transakcji, szczególnie w okresach dużego ruchu.

**Ethereum:**

Ethereum zostało wprowadzone w 2015 roku przez Vitalika Buterina. Jest to platforma blockchain, która umożliwia programistom tworzenie inteligentnych kontraktów oraz aplikacji zdecentralizowanych (DApps).

**Cechy wyróżniające Ethereum:**

**1.** **Platforma programowalna:** Ethereum umożliwia programistom tworzenie inteligentnych kontraktów, które są samoegzekwującymi się umowami cyfrowymi, co pozwala na automatyzację różnych

procesów biznesowych.

**2.** **Mechanizm konsensusu:** Ethereum planuje przesiadkę z Proof-of-Work na Proof-of-Stake, co ma przyczynić się do zmniejszenia zużycia energii i zwiększenia wydajności sieci.

**3.** **Token ERC-20:** Ethereum stało się podstawową platformą dla tworzenia tokenów ERC-20, które są używane w wielu projektach Initial Coin Offering (ICO).

**Zastosowania:**

**1.** **DeFi (Decentralized Finance):** Ethereum jest używane do tworzenia różnych aplikacji finansowych, takich jak wypożyczanie i pożyczanie kryptowalut, giełdy decentralizowane i inne usługi finansowe.

**2.** **NFT (Non-Fungible Tokens):** Ethereum jest główną platformą dla tworzenia NFT, czyli unikalnych, niezamienialnych tokenów, które są używane w dziedzinach sztuki, gier i innych branż.

**Ograniczenia:**

**1.** **Wydajność:** Podobnie jak w przypadku Bitcoin, skalowalność i wydajność Ethereum są wyzwaniem, zwłaszcza gdy sieć jest obciążona dużą ilością transakcji.

**2.** **Koszty transakcji:** Ceny transakcji na Ethereum mogą czasami być wysokie, szczególnie w okresach dużego zainteresowania DApps lub NFT.

Podsumowując, zarówno Bitcoin, jak i Ethereum mają swoje unikalne cechy i zastosowania. Bitcoin jest głównie cyfrową walutą, podczas gdy Ethereum to platforma dla tworzenia inteligentnych kontraktów i aplikacji decentralizowanych. Obydwie platformy stają jednak w obliczu wyzwań związanych z wydajnością i skalowalnością, które są obecnie przedmiotem intensywnych prac i rozwijają się wraz z postępem technologicznym i zwiększającym się zainteresowaniem kryptowalutami i blockchainem.

**4.3 Blockchain w innych dziedzinach**

**Rozwój i zastosowanie blockchaina poza kryptowalutami:**

Mimo że blockchain zyskał popularność głównie dzięki kryptowalutom, jego zastosowania wykraczają daleko poza ten obszar. W ostatnich latach, blockchain stał się obiekt intensywnych badań i eksploracji w różnych dziedzinach. Poniżej przedstawione są przykłady zastosowań blockchaina w biznesie, edukacji i innych dziedzinach:

**1. Biznes i łańcuch dostaw:**

**- Śledzenie łańcucha dostaw:** Blockchain może być używany do monitorowania i śledzenia ścieżki produktów od producenta do konsumenta. To pozwala na większą przejrzystość i autentyczność produktów oraz pomaga w walce z podróbkami.

**- Zarządzanie danymi i dokumentami:** Blockchain może ułatwić zarządzanie danymi i dokumentami w firmach, eliminując

 konieczność wielokrotnego wprowadzania danych oraz zapewniając bezpieczne przechowywanie i dzielenie się dokumentami.

**- Inteligentne kontrakty biznesowe:** Możliwość tworzenia inteligentnych kontraktów na blockchainie pozwala na automatyzację wielu procesów biznesowych, co przyspiesza i ułatwia działania przedsiębiorstw.

**2. Edukacja:**

**- Weryfikacja dyplomów i certyfikatów:** Blockchain może służyć do przechowywania danych o dyplomach i certyfikatach w sposób bezpieczny i niezmienialny, co ułatwia weryfikację osiągnięć edukacyjnych.

**- E-learning:** Blockchain może być wykorzystany do stworzenia platform e-learningowych, które oferują bezpieczne środowisko dla uczestników kursów i dzielą się z nimi nagrodami w postaci kryptowalut za osiągnięcia edukacyjne.

**3. Opieka zdrowotna:**

**- Przechowywanie danych medycznych:** Blockchain może pomóc w bezpiecznym przechowywaniu i udostępnianiu danych medycznych, co zapewnia większą prywatność i kontrolę pacjentów nad swoimi informacjami.

**- Śledzenie łańcucha dostaw w medycynie:** W przypadku leków, szczepionek i urządzeń medycznych, blockchain może pomóc w śledzeniu łańcucha dostaw, zapewniając autentyczność i bezpieczeństwo tych produktów.

**4. Przemysł muzyczny i sztuka:**

**- NFT w sztuce:** Blockchain umożliwia wydawanie NFT, które są unikalnymi, niezamienialnymi tokenami, co otwiera nowe możliwości sprzedaży i zarządzania dziełami sztuki.

**-** **Zarządzanie prawami autorskimi:** Blockchain może służyć do śledzenia i zarządzania prawami autorskimi w sposób bezpieczny i transparentny, co pomaga artystom i twórcom w zarządzaniu ich własnymi prawami do swoich prac.

**5. Głosowanie elektroniczne:**

**-** **Bezpieczne głosowanie:** Blockchain może zapewnić bezpieczne i anonimowe głosowanie, eliminując możliwość oszustw i manipulacji wynikami.

**6. Energetyka i ekologia:**

**-** **Handel energią:** Blockchain może wspomagać handel energią między różnymi producentami i konsumentami, umożliwiając bezpośrednie transakcje i rozliczenia.

**-** **Monitorowanie i zarządzanie emisjami:**

Blockchain może pomóc w monitorowaniu i zarządzaniu emisjami gazów cieplarnianych, co wspiera cele ekologiczne i zrównoważony rozwój.

Warto zauważyć, że rozwój blockchaina jest dynamiczny, a nowe zastosowania są odkrywane i rozwijane na bieżąco. Technologia ta ma potencjał do przekształcenia wielu aspektów naszego życia i oferuje różnorodne możliwości w wielu dziedzinach.

#

# About the Author

Accumsan sit amet nulla facilisi morbi tempus iaculis urna. Porta non pulvinar neque laoreet. Pellentesque adipiscing commodo elit at. Consectetur adipiscing elit pellentesque habitant morbi tristique. Facilisis sed odio morbi quis commodo odio. Quis hendrerit dolor magna eget est lorem ipsum dolor sit. Convallis convallis tellus id interdum velit laoreet.

Sed ullamcorper morbi tincidunt ornare massa eget egestas. Nisl suscipit adipiscing bibendum est ultricies. Morbi leo urna molestie at elementum. Dignissim cras tincidunt lobortis feugiat vivamus at augue eget arcu. Aliquam nulla facilisi cras fermentum odio. Elit duis tristique sollicitudin nibh sit amet commodo nulla facilisi.

www.YourAuthorWebsite.com

# Acknowledgments

Ac ut consequat semper viverra nam libero justo laoreet sit. Adipiscing tristique risus nec feugiat in. Nulla posuere sollicitudin aliquam ultrices sagittis orci a scelerisque. Ultricies lacus sed turpis tincidunt id aliquet risus feugiat in. Ullamcorper eget nulla facilisi etiam dignissim diam quis. Purus in mollis nunc sed id semper risus. Accumsan sit amet nulla facilisi morbi tempus iaculis urna.