

Projekt Kryptografia - Blockchain

Sebastian Knap Hubert Łazaj
Cyberbezpieczeństwo II Rok 2022/2023 r.

Spis treści:

Krótką Historią.....	2
- Początki - 1991 r. - RPoW - 2004 r. - Start BitCointa - 2008-2009 r. - 2013 r. - Vitalik Buterin - Ethereum	
Smart Kontrakty.....	5
- Jak działa smart contract?	
Mechanizmy konsensusu.....	6
- Rodzaje mechanizmów konsensusu - Proof-of-Work - Proof-of-Stake	
Działanie Blockchain.....	9
- Co to jest blok? - Co chroni blok przed dodaniem fikcyjnej transakcji? - Co zapobiega skopiowaniu już podpisanej transakcji? - Dlaczego blockchain jest siecią zdecentralizowaną? - Jak zapewnić, żeby wszystkie Node'y w sieci posiadały te same transakcje, w tej samej kolejności? - Jak ustalany jest poziom trudności obliczania hasha w Bitcoinie? - Co zapobiega zmianie kolejności bloków w blockchainie? - Co to jest atak 51%?	
Zastosowanie Blockchain w praktyce.....	13
- Przechowywanie i zarządzanie danymi z użyciem blockchain - Zarządzanie łańcuchem dostaw - Tokeny NFT - Usługi Finansowe z wykorzystaniem Blockchain - Energetyka + technologia Blockchain	
Bibliografia.....	16

Przykładowa implementacja Bloku Bitcoina z jego podstawowymi własnościami i funkcjonalnościami + utworzenia bloku Genesis oraz kolejnych bloków znajduje się w osobnym pliku jupyter notebook dołączonym do projektu. Dodatkowo załączony został plik ".txt" zawierający listę transakcji.

Poniżej dodatkowo link do samego, czystego kodu który został zaimplementowany:

gist.github.com/sebuszqo/07aa4db2dc10ab0a177baade71567b88

Krótka Historia

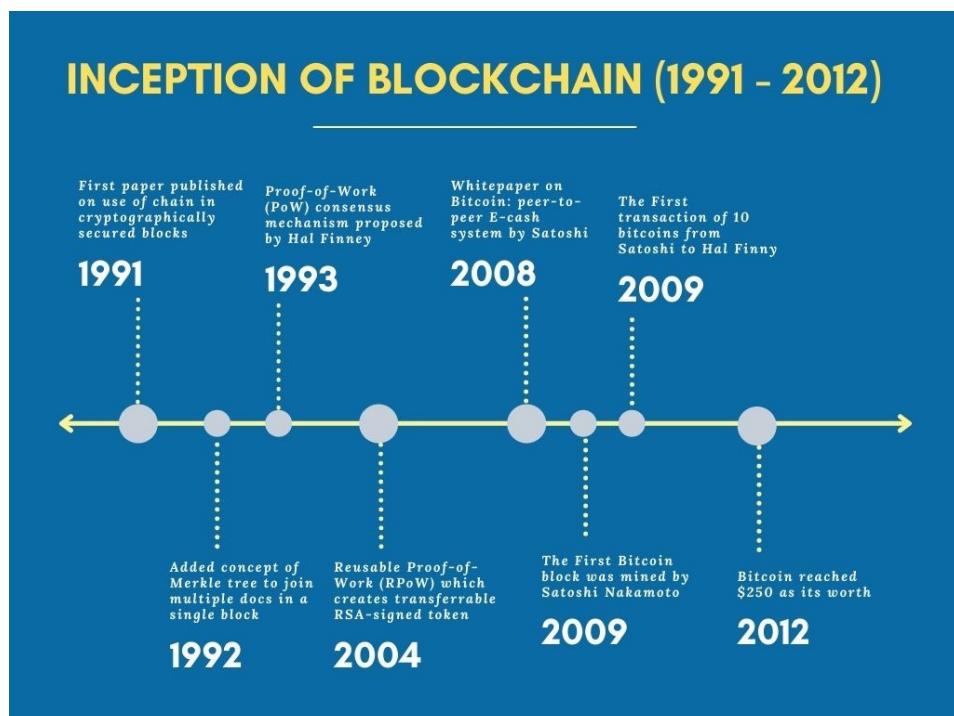
Początki - 1991 r.

Naukowcy Stuart Haber, kryptograf i informatyk oraz Wakefield Scott Stornetta, fizyk prezentują światu rozwiązanie umożliwiające zabezpieczenie dokumentów przed ich przerobieniem lub sfałszowaniem, dzięki użyciu cyfrowego znaczenia czasu. Dokumenty były przechowywane w łańcuchu bloków.

System, który został przedstawiony przez dwóch naukowców wykorzystywał kryptograficznie zabezpieczony łańcuch bloków do przechowywania dokumentów opatrzonych tzw. stemplami czasu.

W roku 1992 do projektu zostały dołączone Merkle Trees (pl. Drzewa Merkle - Drzewa Skrótów), dzięki którym wzrosła efektywność oraz umożliwiło to gromadzenie wielu dokumentów w jednym "bloku".

Pomimo dobrego wykonania, technologia nie została uznana zawartą zainteresowania przez największe banki amerykańskie. Skutkiem był upadek całego projektu jak i również wygaśnięcia patentu na tę technologię w 2004 roku.



RPoW - 2004 r.

Informatyk, kryptograf i pasjonat, Hal Finney, postanowił wprowadzić system o nazwie RPoW (ang. Reusable Proof Of Work). Głównym założeniem koncepcji Finneya było oparcie systemu na tzw. "Hashcashu" (Kryptograficzny algorytm sprawdzania poprawności oparty na hashowaniu, opracowany w 1997 roku przez Adama Backa). System miał polegać na otrzymywaniu Hashcashy, w zamian za stworzenie tokenu podpisanej kluczem RSA, który można było przenosić z osoby na osobę.

Dzięki użyciu RPoW, udało się rozwiązać problem tzw. podwójnego wydatkowania, poprzez zachowanie praw własności do tokenów na zaufanym serwerze, który był specjalnie zaprojektowany w celu umożliwienia użytkownikom na całym świecie dokonania weryfikacji, poprawności i integralności w czasie rzeczywistym.

Start BitCaina - 2008-2009 r.



Rok 2008 - na jednej z list mailingowych dot. Kryptografii, zostaje opublikowany dokument techniczny tzw. whitepaper, opisujący zdecentralizowaną sieć "peer-to-peer" (P2P), która nazywała się BitCoin. Do dziś nie wiadomo kim jest twórca lub twórcy. Wiemy tylko, że działał pod pseudonimem **Satoshi Nakamoto**.

Twórcy sieci Bitcoin zaimplementowali inne podejście, jeśli chodzi o zabezpieczenie sieci i jej użytkowników przed wystąpieniem problemu podwójnego wydatkowania.

Pomysłem na rozwiązanie problemu było, użycie zdecentralizowanego protokołu "peer-to-peer", służącego do śledzenia i weryfikacji dotychczasowych transakcji. W dużym skrócie, bitcoiny są "kopane" przez w celu uzyskania nagrody przez górników, a następnie weryfikowane przez zdecentralizowane węzły sieci (Node'y).

Dnia 03.01.2009 r. powstał oficjalnie Bitcoin. Wtedy, Satoshi Nakamoto dokonał "wykopania" pierwszego bloku, za który otrzymał zapłatę w wysokości 50 BTC. Pierwszym odbiorcą transakcji był Hal Finney, 12 stycznia tego samego roku otrzymał on 12 Bitcoinów, której nadawcą był Satoshi Nakamoto.

2013 r. - Vitalik Buterin - Ethereum

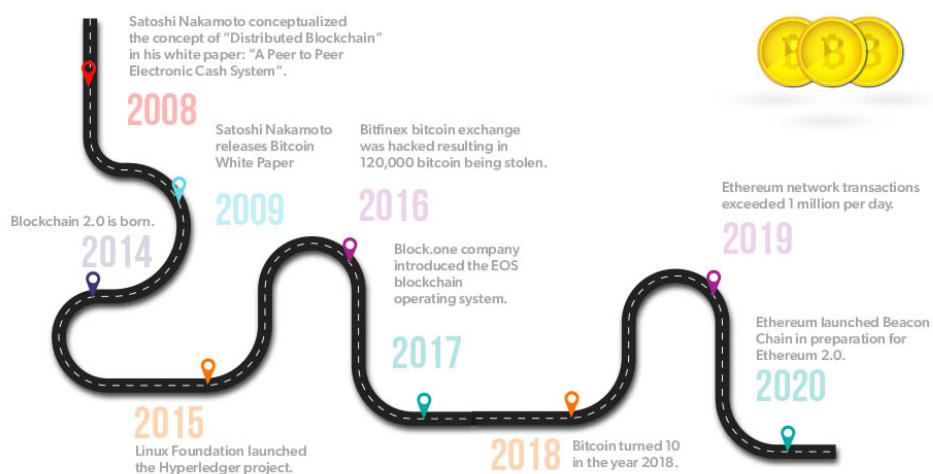


Programista i współzałożyciel magazynu Bitcoin oświadczył, że Bitcoin potrzebuje języka skryptowego, który pozwoliłby budować zdecentralizowane aplikacje z użyciem tej technologii. Niestety nie został on wzięty na poważnie przez ówczesną społeczność Bitcoina. Konsekwencją było rozpoczęcie przez niego własnych prac nad nową, rozproszoną i zdecentralizowaną platformą, która służyła do przetwarzania danych za pomocą technologii Blockchain.



Projekt który powstał w ten sposób został nazwany Ethereum. Był zupełnie inny od dotychczas znanych. Nie polegał tylko i wyłącznie na obsłudze określonej kryptowaluty. Był również platformą umożliwiającą uruchamianie zdecentralizowanych aplikacji. Ethereum zawiera funkcjonalności umożliwiające tworzenie i zarządzanie **smart kontraktami**. Został wprowadzony na rynek w 2015 roku przez Vitalika i zespół ludzi, którzy byli współtwórcami projektu Bitcoin.

Kryptowaluta Ethereum nazywa się Ether - może być zarówno przenoszona między kontami użytkowników, jak i również służy do pobierania opłat za moc obliczeniową wykorzystywaną w trakcie wykonywania operacji zawartych w "inteligentnych kontraktach".



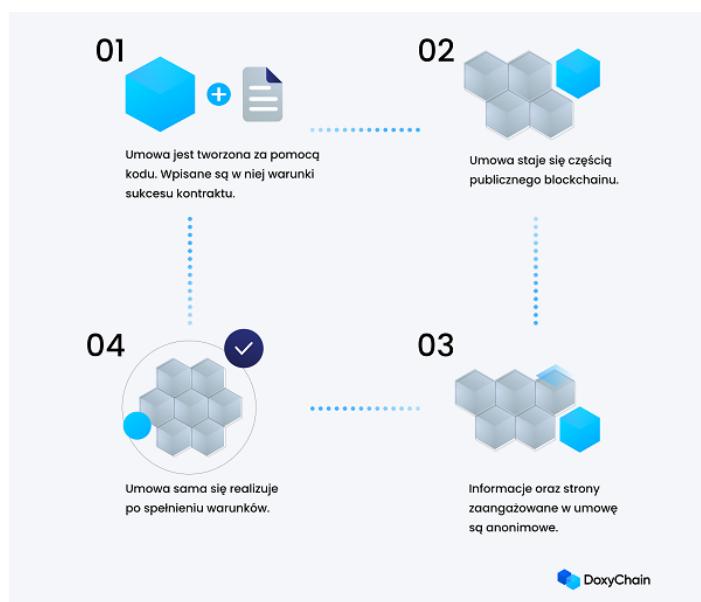
Smart Kontrakty

Smart Kontrakty, jako skrypty na blockchain:

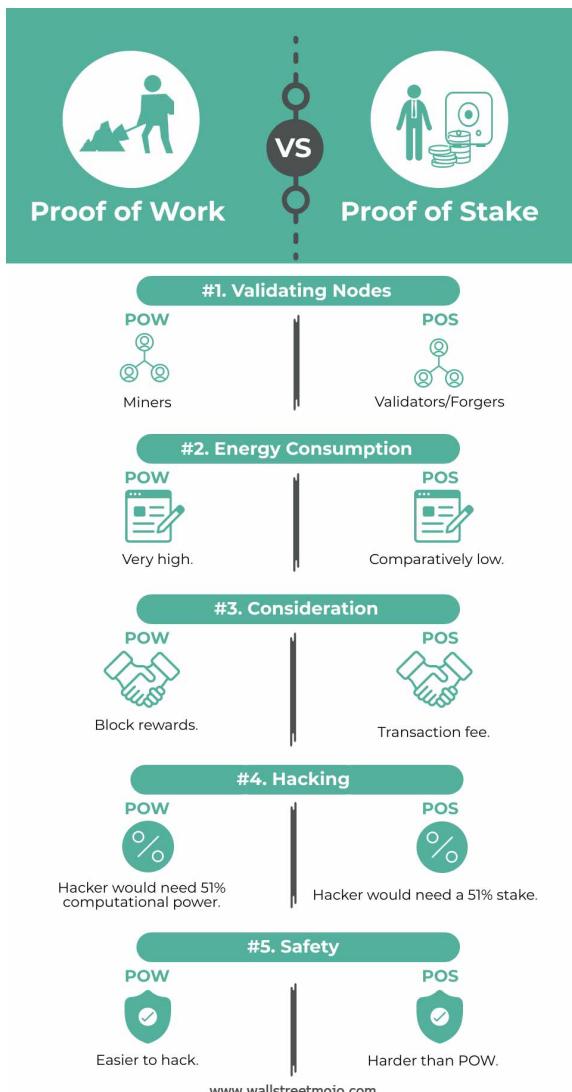
Są to programy lub skrypty, które są wdrażane i uruchamiane na Blockchainie. Przykładem użycia może być transakcja, która zostanie sfinalizowana tylko w przypadku spełnienia określonych warunków. "Inteligentne kontrakty" są pisane głównie w języku "Solidity", a następnie komplikowane do kodu maszynowego. Jest on wykonywany przez zdecentralizowaną wirtualną maszynę. W przypadku Ethereum ta maszyna została nazwana EVM - Ethereum Virtual Machine.

Jak działa smart contract?

Smart Kontrakt, w uproszczeniu, działa w oparciu o prosty warunek: „jeśli wydarzy się X, to wtedy wydarzy się Y”. Warunek (lub ich cały zestaw) jest zapisany w kodzie na blockchainie. Jeśli zostanie on spełniony i zweryfikowany, program uruchamia określone działania.



Mechanizmy Konsensusu



Mechanizmy konsensusu - znane również, jako protokoły konsensusu lub algorytmy konsensusu, umożliwiają współpracę systemów rozproszonych (np. sieci komputerów) oraz zachowanie bezpieczeństwa.

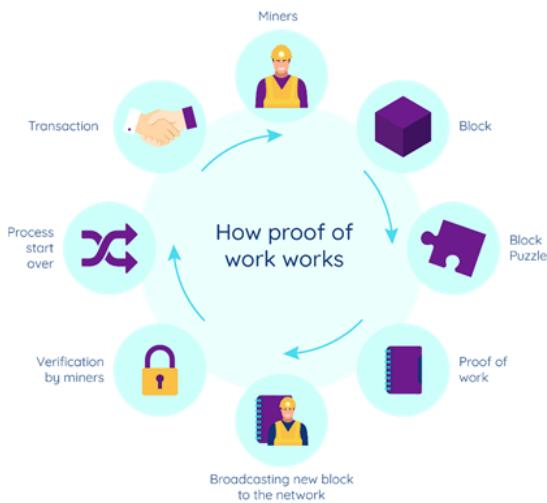
Od dziesięcioleci mechanizmy te są wykorzystywane do ustanawiania konsensusu między węzłami baz danych, serwerami aplikacji i inną infrastrukturą przedsiębiorstw. W ostatnich latach wynaleziono nowe protokoły konsensusu, aby umożliwić systemom krypto-ekonomicznym, takim jak Ethereum ciągłe i bezpieczne uzgadnianie stanu sieci.

Rodzaje mechanizmów konsensusu



Rodzajów mechanizmów konsensusu zaimplementowanych w różnych blockchainach jest wiele. Dwa podstawowe i najczęściej stosowane to **Proof-Of-Work** (Bitcoin) oraz **Proof-of-Stake** (Ethereum).

Proof-of-work



Proces tworzenia bloku:

Proof-of-work jest wykonywany przez górników, którzy konkurują o tworzenie nowych bloków, pełnych przetworzonych transakcji. Zwycięzca dzieli się nowym blokiem z resztą sieci i zarabia dzięki temu BTC. Wyścig wygrywa komputer każdego, kto najszybciej rozwiąże zagadkę matematyczną – w ten sposób powstaje połączenie kryptograficzne między bieżącym blokiem, a poprzednim blokiem. Rozwiążanie tej zagadki to praca w „proof-of-work”.

Bezpieczeństwo:

Sieć jest bezpieczna dzięki zapewnieniu, że aby doszło do „złamania” łańcucha, jeden „node” potrzebowałby posiadać minimum 51% mocy obliczeniowej całej sieci. Wymagałoby to tak ogromnych inwestycji w sprzęt i energię, że sumarycznie koszt takiego ataku wyniósłby więcej niż potencjalny zysk.

Proof-of-stake

Proof of stake



The probability of validating a new block is determined by how large of a stake a person hold.



The validators do not receive a block reward, instead they collect network fees as their reward.



Proof of stake systems can be much more cost and energy efficient than proof of work, but are less proven.

Proces tworzenia bloku:

Proof-of-stake są przeprowadzane przez validatorów, którzy zaangażowali się w uczestnictwo w sieci poprzez posiadanie ETH. Końcowy validator jest wybierany losowo, odpowiada on za utworzenie nowego bloku oraz udostępnienie go w sieci, w nagrodę zdobywa nagrodę w postaci ETH. W porównaniu do Proof of Work jest to rozwiązanie o wiele bardziej ekologiczniejsze oraz ekonomiczniejsze. Zamiast wykonywać intensywną pracę obliczeniową (liczenie hashy), wystarczy stać się stake-holderem ETH w sieci.

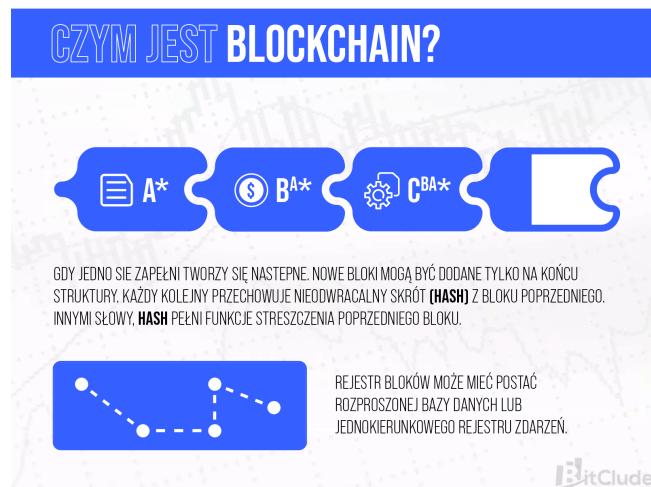
Bezpieczeństwo:

System proof-of-stake jest bezpieczny dzięki zapewnieniu, że aby doszło do oszustwa na łańcuchu, jeden node potrzebuje 51% wszystkich zgromadzonych w sieci przez stake-holderów środków ETH. Dodatkowe bezpieczeństwo, gwarantuje automatyczne zabezpieczenie, które w momencie wykrycia próby oszustwa, automatycznie obniża stawkę nagrody, ze względu na złośliwe zachowanie.

Działanie Blockchaina

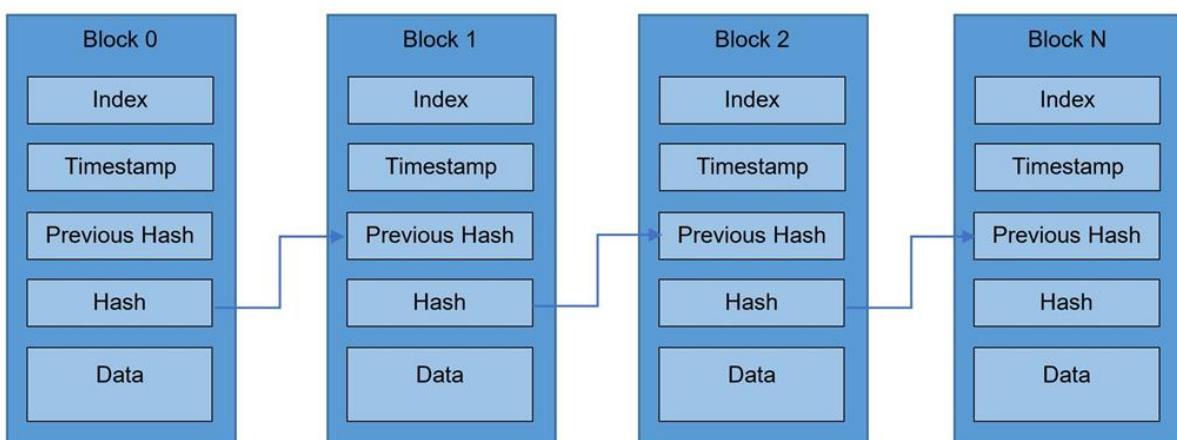
Blockchain - inaczej łańcuch bloków, jest to technologia, która służy do przechowywania oraz przesyłania informacji o transakcjach zawartych w sieci.

Przykładowy blok BTC: www.blockchain.com/explorer/blocks/btc/764266



Co to jest blok?

Blok zawiera określoną liczbę transakcji. Transakcje te są dostępne publicznie. Każdy może dodać nową transakcję do bloku. Każdy blok zawiera indeks bloku, odpowiednią liczbę transakcji, timestamp (zawiera czas i datę stworzenia bloku) oraz hash poprzedniego bloku - łączy on wszystkie bloki ze sobą tworząc łańcuch, który zapewnia trwałą i niezmienną historię transakcji w blockchainie.



Co chroni blok przed dodaniem fikcyjnej transakcji?

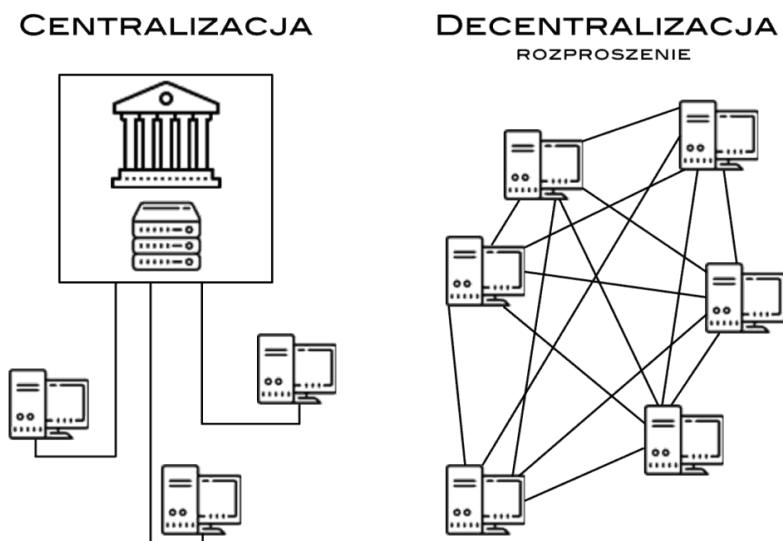
Każdy Node w sieci posiada parę kluczy. Klucz publiczny - widoczny dla wszystkich oraz prywatny, który należy tylko do konkretnej osoby oraz musi być on tajny. Każda transakcja w blockchainie musi zostać podpisana przez osobę, która ma wysłać transakcję. Transakcja jest podpisywana za pomocą klucza prywatnego, który zapobiega modyfikacji danej transakcji i potwierdza nas, jako osobę, która podpisała transakcję. Podpis cyfrowy jest generowany przez połączenie klucza prywatnego z danymi, które są wysyłane w transakcji. Dodatkowo, transakcja może zostać zweryfikowana za pomocą klucza publicznego. Weryfikację danej transakcji wykonują automatycznie wszystkie Node'y w sieci. Natomiast, niepoprawna transakcja zostaje przez sieć odrzucona.

Co zapobiega skopiowaniu już podpisanej transakcji?

Każda transakcja zawiera dodatkowo unikalny identyfikator, który jest dodawany do transakcji przed jej podpisaniem. Identyfikator transakcji jest niepowtarzalny, dzięki czemu zapobiega skopiowaniu już podpisanej transakcji.

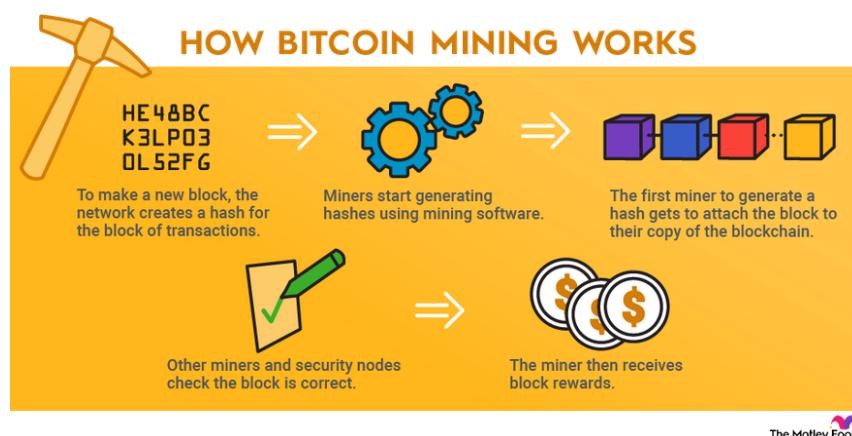
Dlaczego blockchain jest siecią zdecentralizowaną?

Ponieważ każdy Node zawiera historię bloków oraz każda nowa transakcja jest weryfikowana przez wszystkie Node'y w sieci i następnie dodawana przez nie do ich historii bloków.



Jak zapewnić, żeby wszystkie Node'y w sieci posiadały te same transakcje, w tej samej kolejności?

Rozwiązaniem są mechanizmy konsensusu. W bitcoin jest to Proof of Work, polegający na znalezieniu liczby, która dodawana jest na końcu listy transakcji w bloku, z którego to końcowego bloku liczona jest funkcja skrótu. Jako funkcję skrótu Bitcoin wykorzystuje SHA256. Liczba ta musi tworzyć hash, który spełnia odpowiednią trudność. Trudność dotycząca znajdowania hasha jest regularnie zmieniana, aby dodawanie kolejnych bloków nie było ani zbyt proste, ani zbyt trudne. Każda nowa transakcja całkowicie zmienia hash, przez to cała moc obliczeniowa, musi zacząć od nowa. Node, który znajdzie odpowiednią liczbę, spełniającą odpowiednią trudność hasha, dostaje zapłatę za poświęcony czas, moc obliczeniowa oraz energię. Taki node zostaje również validatorem danego bloku, który jest następnie dodawany do blockchaina i propagowany w sieci.

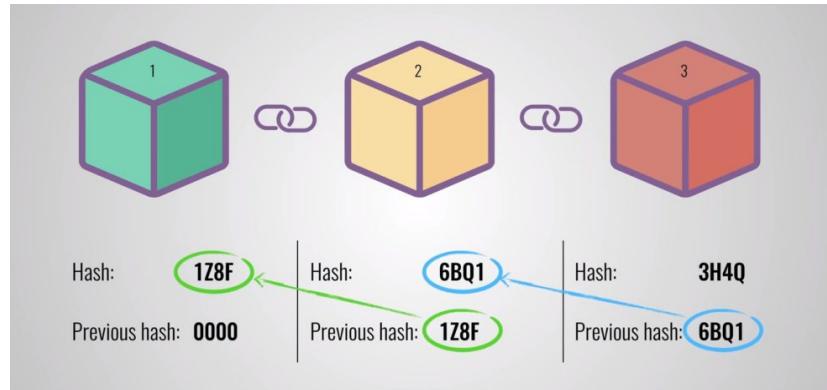


Jak ustalany jest poziom trudności obliczania hasha w Bitcoinie?

Kryptowaluty używające Proof-of-Work posiadają górników, którzy żeby potwierdzić blok, muszą znaleźć taką liczbę (nonce), żeby po obliczeniu hasha z tego bloku, spełniała ona odpowiednią trudność. Dostosowanie trudności znalezienia hasha w Bitcoinie powinno działać tak, aby średnio co 10 minut był "wykopywany" nowy blok. Zmiana trudności wykopywania bloku zachodzi co każde około 2 tygodnie. Wtedy to, jeżeli średni czas liczenia odpowiedniego hasha bloku nie jest spełniony następuje zwiększenie lub zmniejszenie trudności. Średni czas "wykopywania" bloku zależy od mocy obliczeniowej sieci, im większa moc, tym czas obliczania hasha bloku spada.

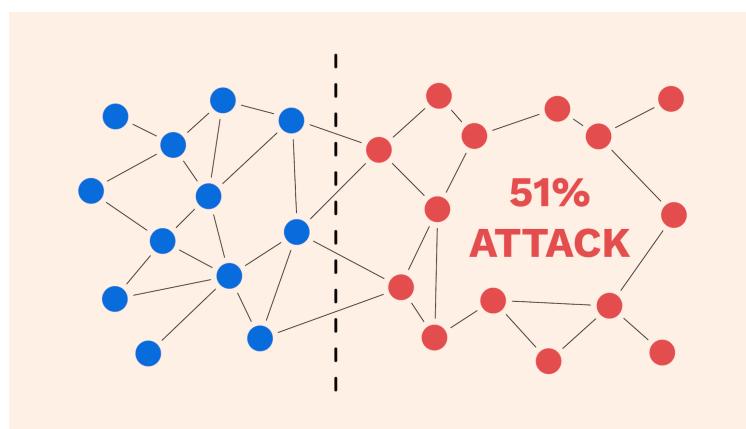
Co zapobiega zmianie kolejności bloków w blockchainie?

Każdy blok zawiera hash swojego poprzednika, z którego później jest liczona funkcja skrótu. Zapobiega to wszelkim zmianom w blockchainie, ponieważ każda drobna zmiana powoduje zmianę we wszystkich kolejnych blokach.



Co to jest atak 51%?

Atak 51% jest to atak na daną kryptowalutę przez grupę minerów, którzy kontrolują ponad 50% mocy obliczeniowej sieci lub stake-holderów, którzy posiadają ponad 50% zebranych środków. Posiadanie takiej mocy daje kontrolę nad możliwością zmiany blockchaina, ponieważ można spowodować, że Node'y będą wybierały, jako poprawny, zawsze zmanipulowany przez atakującego blok i dodawały go do łańcucha. Atakujący będą mogli także uniemożliwić nowym transakcjom uzyskanie potwierdzenia, wstrzymując tym samym płatności w całej sieci.



Zastosowanie technologii Blockchain w życiu codziennym - świecie nas otaczającym

Przechowywanie i zarządzanie danymi z użyciem blockchain:

Technologia blockchain jest używana jako rozwiązanie do przechowywania danych osobowych, dokumentów, faktur etc. Zapewnić może większe bezpieczeństwo i integralność dzięki przechowywaniu ich w sposób zdecentralizowany, dzięki czemu ciężej jest się włamać do danych lub spowodować ich usunięcie. Z drugiej strony oznacza to większy dostęp do danych, dzięki niezależności od dostępności jednej z firm przechowujących nasze dane. Dotyczy to zarówno możliwości przechowywania danych medycznych, finansowych, jak i również każdego innego rodzaju.

Przykładowe implementacje:

Polski Start-up, zajmującym się tworzeniem infrastruktury dla zdigitalizowanych dokumentów oraz sposobem na ich zarządzanie:
doxychain.com

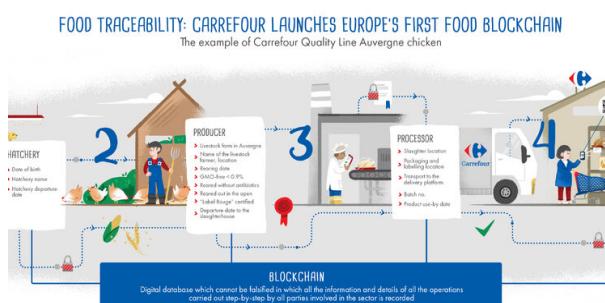


Zarządzanie łańcuchem dostaw:

Technologia blockchain jest używana do śledzenia przemieszczania się towarów i materiałów w trakcie drogi do klienta końcowego. Co więcej istnieją zastosowania blockchain, jako elementu świadczącego o jakości produkty, dzięki zapisywaniu danych z poszczególnych etapów produkcji, np. jedzenia, konsument końcowy, może sprawdzić dokładne dane na temat kupowanego produktu.

Przykładowe implementacje:

Takie rozwiązanie w Polsce wprowadził Carrefour, który dzięki blockchain, znakuje proces produkcji ziemniaków dostępnych w ich sklepach



Tokeny NFT:

NFT ogólnie są sposobem na przekazywanie praw własności. Są powszechnie stosowane w np. prawach do sztuki cyfrowej, prawach dostępu do społeczności, ogólnie prawach dostępu i przynależności, jak i również aktów własności (domu, mieszkania, ziemi), prawach do transmisji wideo, muzyki, lub np. jako bilet na wydarzenie. Opierają się na gwarancji, jaką zapewnia Blockchain, czyli zapobieganiu istnienia tych samych danych w dwóch różnych miejscach. Umieszczenie NFT na blockchain gwarantuje, że istnieje tylko jedna kopia danego NFT i możemy mieć pewność, że należy ona do nas. Dodatkowym atutem tego rozwiązania, jest możliwość odsprzedaży NFT na rynku wtórnym.

Przykładowe implementacje:

- Największy MarketPlace dot. NFT - opensea.io



- Najbardziej znana na świecie społeczność NFT - boredapeyachtclub.com



- Polski pomysł zastosowania NFT w edukacji - eduworlds.com



- Zastosowanie NFT jako elementu Kolekcjonerskiego dla fanów sportu - [Dapper Labs](https://dapperlabs.com)



Usługi Finansowe z wykorzystaniem Blockchain:

Blockchain jest wykorzystywany w branży usług finansowych, aby zwiększyć bezpieczeństwo transakcji finansowych, a także zmniejszyć koszty i poprawić efektywność systemów finansowych. Przykładem tego jest użycie technologii blockchain w międzynarodowych transferach pieniędzy. Dzięki zastosowaniu rozproszonego systemu blockchain, transfery pieniędzy mogą być zakończone szybciej i z niższymi opłatami w porównaniu z tradycyjnymi metodami opierającymi się na sieci pośredników.



Energetyka + technologia Blockchain:

Technologia blockchain jest wykorzystywana również w branży energetycznej, aby poprawić efektywność, przejrzystość i bezpieczeństwo transakcji energii oraz tworzyć nowe modele biznesowe dla produkcji, dystrybucji i konsumpcji energii.

Przykładowe zastosowania:

Przykładem jest użycie technologii blockchain w handlu certyfikatami odnawialnej energii (RECs). Certyfikaty te służą do śledzenia generowania i konsumpcji odnawialnej energii i mogą być kupowane i sprzedawane na platformie opartej na blockchainie. To pozwala na bardziej efektywny i przejrzysty handel odnawialną energią i może przyczynić się do zwiększenia adopcji źródeł odnawialnej energii.

Technologia blockchain jest również wykorzystywana w implementacji "inteligentnych" systemów energetycznych, które wykorzystują technologię czujników oraz IoT do optymalizacji zużycia energii i zmniejszania kosztów. Blockchain może też być używany do bezpiecznego przechowywania i udostępniania danych z tych systemów, co pozwala na bardziej efektywne zarządzanie zasobami energii.



Bibliografia:

<https://eduworlds.com>
<https://www.dapperlabs.com>
<https://boredapeyachtclub.com/#/>
<https://doxychain.com>
<https://opensea.io>
<https://bitpay.com/blog/proof-of-work-vs-proof-of-stake/>
<https://dailyweb.pl/blockchain-to-nie-bitcoin/>
<https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/bitcoin-mining/>
<https://xcoins.com/en/blog/proof-of-work-vs-proof-of-stake-the-pros-and-cons/>
<https://ethereum.org/pl/developers/docs/consensus-mechanisms/>
<https://ethereum.org/pl/developers/docs/intro-to-ethereum/>
<https://pl.wikipedia.org/wiki/Bitcoin>
<https://www.blockchain.com/explorer/blocks/btc/764266>
<https://bitcoin.org/bitcoin.pdf>
<https://www.youtube.com/watch?v=bBC-nXj3Ng4>
<https://www.investopedia.com/terms/1/51-attack.asp>
<https://www.investopedia.com/terms/d/difficulty-cryptocurrencies.asp>
<https://academy.bit2me.com/en/what-is-bitcoin-mining-difficulty/>
<https://academy.binance.com/pl/articles/what-are-smart-contracts>