Uniwersytet Ekonomiczny w Katowicach
Wydział Informatyki i Komunikacji
Kierunek: Informatyka i Ekonometria

DAWID JANIK

GENEZA, ZASADY DZIAŁANIA, ZASTOSOWANIE I IMPLEMENTACJA TECHNOLOGII BLOCKCHAIN

ORIGIN, PRINCIPLES OF OPERATION, APPLICABILITY AND IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY

Praca licencjacka
napisana w Katedrze Badań Operacyjnych
pod kierunkiem dr inż. Tomasza Błaszczyka

KATOWICE 2018

Katowice, dnia 21.06.2018r.

SPIS TREŚCI

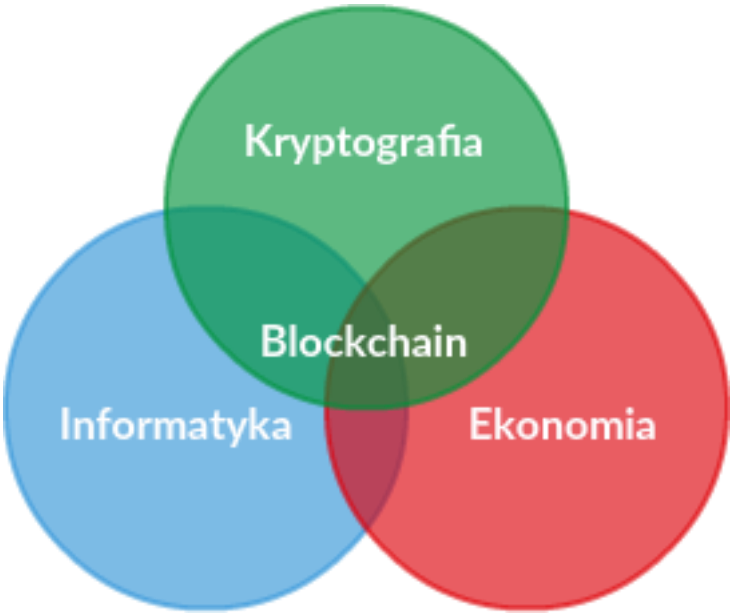
WSTĘP

Przez pierwsze lata swojego istnienia, blockchain przez zdecydowaną większość osób nie był postrzegany jako nic ponad technologią, umożliwiającą działanie coraz większej liczby pojawiających się kryptowalut, czyli sposobem na tworzenie zdecentralizowanych form e-pieniądza. Zaczęło się to zmieniać w drugiej połowie 2015 roku, kiedy wraz z powstaniem Ethereum, udostępnione zostały narzędzia umożliwiające wdrażanie inteligentnych kontraktów jak i zdecentralizowanych aplikacji i organizacji. Mimo, że nadal były to rozwiązania, które początkowo wykorzystywane były wyłącznie w sferze finansowej, zaczęto dostrzegać potencjał samego blockchaina jako uniwersalnej bazy do tworzenia bezpiecznych, zdecentralizowanych rozwiązań. Od tego momentu narodziło się wiele projektów, które nie są już jak Bitcoin wyłącznie środkiem przechowywania wartości podobnie do złota (choć na ten moment zdecydowanie mniej bezpiecznym ze względu na duże wahania ceny), ale starają się rozwiązać problemy dotyczące wielu sfer codziennego życia lub usprawnić i rozszerzyć możliwości działających już technologii. Z rosnącą częstotliwością pojawiają się projekty, które oferują rozwiązania nie tylko z sfery finansów i bankowości, ale także energetyki, transportu, handlu, administracji i usług publicznych, prawa, nieruchomości i wielu innych.

Wybór tego tematu pracy dyplomowej wiązał się bezpośrednio z dużym zinteresowaniem tą dziedziną. Stąd, pojawiła się chęć dokładnego poznania i zrozumienia zasad działania mechanizów składających się na technologię łańcucha bloków. Praca ma na celu zunifikowanie i usystematyzowanie wiedzy na ten temat z wielu rozproszonych źródeł. To w rezultacie miałoby umożliwić wykorzystanie blockchaina w próbie opracowania własnego projektu kryptowaluty, różniącego się jednak zdecydowanie od powszechnie spotykanych, bo opartego dodatkowo o znajome narzędzia i technologie wykorzystywane w środowisku web developerów. Całość pracy zostanie podzielona na trzy części. W pierwszej z nich zaznajomić będzie się można z kluczowymi pojęciami używanymi w dziedzinie blockchaina i kryptowalut, co ułatwić ma przestudiowanie reszty. Następnie przedstawione krótko zostaną dzieje pieniądza, a bardziej szczegółowo nakreślone zostanie tło historyczne Bitcoina jako prekusorskiego rozwiązania opartego o blockchain. Po czym opisane zostaną zasady działania elementów składających się na technologię łańcucha blokowego. W drugiej części uwaga zostanie skupiona na dziedzinach i przykładach zastosowania blockchaina, a także rozważane będzie, w jakich przypadkach może on zastąpić tradycyjne bazy danych. Ostatnią częścią stanowić będzie przedstawienie zaimplementowanego projektu kryptowaluty o nazwie Motus.

ROZDZIAŁ I. HISTORIA I MECHANIZM DZIAŁANIA TECHNOLOGII BLOCKCHAIN

Blockchain jest technologią, której podwaliny stanowi połączenie trzech dziedzin nauki: kryptografii, ekonomii i informatyki, a tym samym jej tematyka jest bardzo rozległa. Sprawia to, że aby dobrze zrozumieć jak działa blockchain i jakie korzyści płyną z korzystania z niego, należy najpierw przyswoić sobie zbiór pojęć z tych właśnie dziedzin poszerzony o wiele nowych, które pojawiły się na etapie jego dynamicznego rozwoju. Dlatego też poniżej zawarty został leksykon kluczowych pojęć, z którym powinno się zaznajomić przed przejściem do dalszych rozważań. Niektóre z nich zostały wyjaśnione dość ogólnie i zostaną rozwinięte przy przedstawianiu związanych z nimi kwestii. Blockchain nadal ewoluuje, a rozwiązania oparte na nim oparte właściwie dopiero powstają, więc z biegiem czasu pojawiać się będą kolejne terminy, a przez to przedstawiony leksykon będzie coraz bardziej niekompletny.



Rys. 1. Diagram Venna przedstawiający dziedziny nauki obecne w blockchainie.

Źródło: Opracowanie własne.

1.1. Leksykon kluczowych pojęć

Adres (address) - służy do przekazywania i otrzymywania środków w sieci peer-to-peer opartej na blockchainie. Jest to hash generowany z klucza publicznego składający się z ciągu liter i cyfr, zazwyczaj ok. 30 znaków. Standardową praktyką, w celu pozostania anonimowym, jest korzystanie z innego adresu przy każdej transakcji.[1]

Altcoin - ogólnie przyjęta nazwa dla wszystkich kryptowalut stanowiących alternatywę dla Bitcoina.[2]

ASIC - skrót od Application Specific Integrated Circuit. Jak sama nazwa wskazuje są to specjalne układy scalone, które cechują się większą niż procesory i karty graficzne wydajnością i energooszczędnością w wyliczaniu hashy funkcji kryptograficznych, a przez to używane są wyłącznie do kopania (miningu) kryptowalut.[3]

Atak 51% - sytuacja, w której więcej niż połowa mocy obliczeniowej sieci jest kontrolowana przez jednostkę lub grupę jednostek. Pozwala na przejęcie pełnej kontroli nad siecią, a tym samym m.in. na manipulację transakcjami, w tym double-spending, czy ustanowienie monopolu na tworzenie kolejnych bloków.[4]

BIPs - skrót od Bitcoin Improvement Proposals. Jest to zbiór propozycji członków społeczności bitcoin dotyczających jego usprawnienia. Schemat „bips" jest powielany przez wiele innych projektów kryptowalut. Niemal zawsze propozycje te zbierane są w przygotowanym do tego repozytorium na platformie GitHub.

Bitcoin (BTC) - pierwsza i na ten moment najpopularniejsza zdecentralizowana kryptowalutą opartą o sieć peer-to-peer. Została ona stworzona w 2009r. przez Satoshi Nakamoto.[5]

---

[1] Rosic A. (2017): *Blockchain Glossary: From A-Z.* Blockgeeks. Dostęp: https://blockgeeks.com/guides/blockchain-glossary-from-a-z/
[2] Odinsky J. (2017): *Blockchain Dictionary.* Hackernoon. Dostęp: https://hackernoon.com/blockchain-dictionary-f4d098c9ef89 [9.04.2018r.]
[3] Middelman M. (2016): *21 Terms to Understand Cryptocurrency.* Medium. Dostęp: https://medium.com/the-mission/21-terms-to-understand-cryptocurrency-8bee30aa8dfc [9.04.2018r.]
[4] Antonopoulos A. (2017): *Mastering Bitcoin (Second Edition): Programming the Open Blockchain*. Wydawnictwo O'Reilly Media, Sebastopol. s. 137-138
[5] Lai V., Wong V. (2018): *Cryptocurrency and Blockchain Glossary.* CrushCrypto. Dostęp: https://crushcrypto.com/glossary/ [9.04.2018r.]

Blok (block) - pakiet danych, dla kryptowalut grupa zatwierdzonych transakcji, wraz ze znacznikiem czasowym (timestamp) i sygnaturą poprzedniego bloku, który po dodaniu do blockchaina staje się permanentnie jego integralną częścią w niezmienionej formie.

Blok genesis (genesis block) - pierwszy blok, który stanowi początek blockchaina, zazwyczaj numerowany jako blok 0. Jako jedyny nie posiada sygnatury poprzedniego bloku, a jedynie własną, która zdefiniowana jest bezpośrednio w kodzie źródłowym.

Blockchain - jest zdecentralizowanym, współdzielonym i zazwyczaj publicznym rejestrem chronologicznie ułożonych bloków danych, które są ze sobą połączone w ciąg sygnaturami kryptograficznymi. Stanowi niezmienny zapis historyczny wszystkich przeprowadzonych transakcji od najnowszego bloku aż do bloku genesis.[6]

Block Explorer - narzędzie dostępne online, które pozwala na przejrzenie wszystkich transakcji, które zostały zapisane w blockchainie. Bardzo często dodatkowo udostępnia także informacje o czasie wygenerowania, ilości trasakcji i wielkości bloków, a także aktualnym stanie sieci w postaci hash rate, transakcji w ostatnich 24h, listy niezatwierdzonych trasakcji i wielu innych.

Chłodnia (cold storage) - portfel offline, zapewnia najwyższy poziom bezpieczeństwa zgromadzonych środków i zakłada przechowywanie cyfrowego portela (kluczy prywatnych) w bezpiecznym, niepodłączonym do sieci miejscu. Popularnymi metodami cold storage jest porfel papierowy – wydruk z kodami QR adresu i jego klucza prywatnego, portfel sprzętowy (np. Leger Nano S lub Trenzor), a także przeniesienie plików portfela na pamięć USB lub komputer nie będący podłączony do sieci.[7]

Konsensus (consensus) - stan, w którym większość węzłów (wymagane jest 51%), a zazwyczaj wszyscy członkowie sieci, potwierdzają prawidłowość transakcji upewniając się, że wszystkie lokalne wersje blockchaina są identyczne.[8]

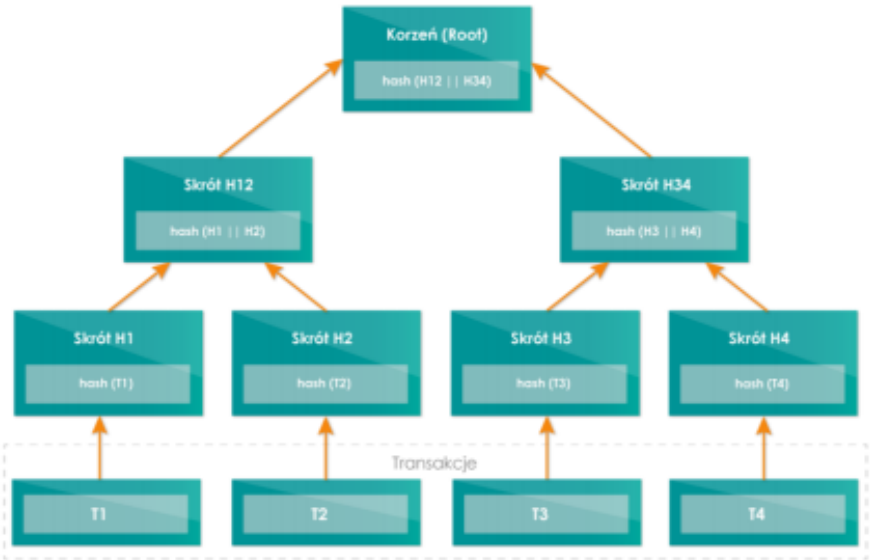
DApps - skrót od Decentralized Applications. Rodzaj oprogramowania działającego autonomicznie, którego dane składowane są w blockchainie. Od inteligentnych kontraktów

[6] Yii-Huumo J., Ko D., Choi S., Park S., Smolander K. (2016): *Where is Current Research on Blockchain Technology? – A Systematic Review. Wydawnictwo Plos One,* San Francisco. s. 1-4. Dostęp: http://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0163477&type=printable [9.04.2018r.]
[7] Antonopoulos A. (2017): *Mastering Bitcoin (Second Edition): Programming the Open Blockchain*. Wydawnictwo O'Reilly Media, Sebastopol. s. 5
[8] Berentsen A., Schär F. (2018): *A Short Introduction to the World of Cryptocurrencies*. Federal Reserve Bank of St. Louis, Saint Louis. s.7. Dostęp: https://files.stlouisfed.org/files/htdocs/publications/review/2018/01/10/a-short-introduction-to-the-world-of-cryptocurrencies.pdf [9.04.2018r.]

wyróżnia go nieograniczona liczba uczestników, a także fakt, iż nie musi mieć przeznaczenia finansowego. Popularną platformą do tworzenia DApps jest Ethereum.[9]

DAO - skrót od Decentralised Autonomous Organizations. Podobnie jak DApps jest to oprogramowanie działającego autonomicznie na blockchainie, jednak w tym wypadku posiada on zasady zarządzania i logiki biznesowej. DAO zostały zaprojektowane jako zdecentralizowany odpowiednik funduszy kapitału podwyższonego ryzyka (VC funds). W kodzie źródłowym największej DAO (nazywanej „The DAO"), której łączny kapitał wynosił 168 milionów dolarów, znajdował się błąd umożliwiający atak hackerski, którego skutkiem była kradzież 55 milionów dolarów przelewając je na DAO-dziecko (child DAO). Początkowo zaproponowano soft fork, który miał wprowadzić poprawkę uniemożliwiającą hackerom wypłatę skradzionych środków z ich DAO. Finalnie większość społeczności zdecydowała, aby w celu odwrócenia skutków ataku wykonany został hard fork. Narodził się wtedy bliźniaczy blockchain, Ethereum Classic, którego społeczność pogodziła się z atakiem.[10]

Drzewo skrótów (merkle tree) - drzewiasta struktura danych powstała przez hashowanie par danych (gałęzi), a następnie dalsze parowanie i hashowanie rezultatów aż do momentu otrzymania pojedynczego hasha – korzenia (merkle root). Blok w nagłówku musi posiadać poprawny merkle root powstały z danych wszystkich transakcji w tym bloku.[11]



[9] Lannquist A. (2017): *Blockchains, Cryptocurrencies & New Decentralized Economy: Part 2 – Blockchain-Based Apps.* Uniwersytet Kalifornijski, Berkeley. Dostęp: https://blockchainatberkeley.blog/blockchains-cryptocurrencies-the-new-decentralized-economy-part-2-blockchain-based-apps-e6ea71236ca [9.04.2018r.]
[10] Bashir I. (2017): *Mastering Blockchain*. Wydawnictwo Packt Publishing, Birmingham. s. 44
[11] González B. (2017): *From Alan Turing to Cyberpunk: The History of Blockchain.* BBVA. Dostęp: https://www.bbva.com/en/alan-turing-cyberpunk-history-blockchain/ [9.04.2018r.]

Rys 2. Schemat struktury merkle tree.

Źródło: Klinger B., Szczepański J. (2017): *Blockchain – Historia, Cechy i Główne Obszary Zastosowań.* UKSW, Warszawa. s. 15. Dostęp: http://czasopisma.uksw.edu.pl/index.php/cwc/article/view/1858 [9.04.2018r.]

ECDSA - skrót od Elliptic Curve Digital Signature Algorithm. Rodzaj algorytmu kryptograficznego używanego w Bitcoinie do zapewnienia bezpieczeństwa środków, tak aby mogły być wydawane jedynie przez ich prawowitego właściciela przy użyciu klucza prywatnego.[12]

ERC20 - technologiczny standard tokenów używany w smart contractach i aplikacjach na platformie Ethereum. Wiele popularnych kryptowalut działa jako tokeny ERC20, ze względu na szerokie możliwości tworzenia dodatkowych funkcjonalności, dopóki nie zostanie ukończona implementacja ich własnych blockchainów.[13]

Etherum - jest kryptowalutą opartą o blockchain działającą dodatkowo jako zdecentralizowana platforma dla inteligentnych kontraktów, aplikacji i autonomicznych organizacji. Została stworzona przez programistę Vitalika Buterina.[14]

Fork - znany także jako przypadkowy fork, ma miejsce gdy dwa lub więcej bloków mających tą samą wysokość, tworząc przez to tymczasowo równoważne alternatywne wersje blockchaina. Zazwyczaj jego przyczyną jest znalezienie bloków przez dwóch lub więcej górników w niemal tym samym czasie.[15]

Górnik (miner) - często określany także jako kopacz, jest węzłem, który aktywnie uczestniczy w procesie potwierdzania transakcji i dodawania nowych bloków do blockchaina w zdefiniowanej formie Proof of Work, Proof of Stake lub innych ich odmian. W zamian miner otrzymuje nagrodę w postaci nowo utworzonych tokenów lub/i sumę opłat za transakcje przechowywane w tym bloku.

Hard fork - jest trwałą rozbieżnością w blockchainie. Powstaje, gdy niezaktualizowane węzły nie mogą potwierdzić bloków wygenerowanych przez zaktualizowane węzły, które do osiągnięcia consensusu kierują się zmodyfikowym zbiorem zasad, który jest sprzeczny z

[12] Antonopoulos A. (2017): *Mastering Bitcoin (Second Edition): Programming the Open Blockchain*. Wydawnictwo O'Reilly Media, Sebastopol. s. 7
[13] Lai V., Wong V. (2018): *Cryptocurrency and Blockchain Glossary.* CrushCrypto. Dostęp: https://crushcrypto.com/glossary/ [9.04.2018r.]
[14] Buterin V. (2014): *Ethereum White Paper - a Next Generation Smart Contract & Decentralized Application Platform*. Ethereum Foundation. Dostęp: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [9.04.2018r.]
[15] Antonopoulos A. (2017): *Mastering Bitcoin (Second Edition): Programming the Open Blockchain*. Wydawnictwo O'Reilly Media, Sebastopol. s. 8

poprzednim. Wymaga przez to zaktualizowania oprogramowania przez wszystkie węzły w sieci.[16]

Hash - wynik działania funkcji kryptograficznej przyjmującej na wejściu dowolną porcję danych (wiadomość) i produkującej deterministyczny (zawsze taki sam dla tej samej wiadomości) ciąg znaków o stałej długości, z którego nie można odtworzyć wprowadzonych danych. W sieci p2p jest używany jako cyfrowy identyfikator ze względu na fakt, iż niemal niewykonalne jest znalezienie dwóch różnych wiadomości posiadających ten sam hash.[17]

ICO - skrót od Initial Coin Offering. Jest to przedsięwzięcie, w którym twórcy projektu kryptowaluty zbierają środki na rozwój od osób, które chcą ich wesprzeć finansowo (zainwestować). Osoby te są w zamian nagradzane ilością tokenów odpowiadającą wysokości wpłaty. Najpopularniejszą aktualnie platformą do przeprowadzanie ICO jest Ethereum.[18]

Inteligentny kontrakt (smart contract) - mechanizm działający w blockchainie, który obejmuje dwie lub więcej stron, których cyfrowe zasoby są w nim umieszczane, a następnie później redestrybuowane na podstawie formuły i zdarzenia wyzwalającego zdefiniowanych w kodzie napisanym w języku programowania (dla Ethereum jest to Solidity). Zawarty kontrakt jest realizowany automatycznie, bez osób trzecich, przestojów i możliwości oszustwa.[19]

Klucz prywatny (private key) - nazywany także sekretnym kluczem (sekret key) jest ciągiem znaków chroniącym dostępu do środków, które znajdują się na przypisanym do niego adresie. Powinien go posiadać tylko i wyłącznie właściciel tego adresu.[20]

Klucz publiczny (public key) - jest hashem wygenerowanym z klucza prywatnego. Używany jest pod cyfrowego podpisywania transakcji wysyłanych na odpowiadający mu adres. W przeciwieństwie do klucza prywatnego może zostać udostępniony.[21]

---

[16] Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. (2016): *Bitcoin and Cryptocurrency Technologies*. Wydawnictwo Princeton University Press, Princeton. s. 96
[17] https://en.wikipedia.org/wiki/Cryptographic_hash_function [9.04.2018r.]
[18] Lannquist A. (2017): *Blockchains, Cryptocurrencies & New Decentralized Economy: Part 1 – a Gentle Introduction.* Uniwersytet Kalifornijski, Berkeley. Dostęp: https://blockchainatberkeley.blog/blockchains-cryptocurrencies-the-new-decentralized-economy-part-1-a-gentle-introduction-edcb4824b174 [9.04.2018r.]
[19] Voshmgir S. (2017): *Blockchains & Distributed Ledger Technologies.* BlockchainHub. Dostęp: https://blockchainhub.net/blockchain-intro/ [9.04.2018r.]
[20] Rosic A. (2017): *Blockchain Glossary: From A-Z.* Blockgeeks. Dostęp: https://blockgeeks.com/guides/blockchain-glossary-from-a-z/ [9.04.2018r.]
[21] Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. (2016): *Bitcoin and Cryptocurrency Technologies*. Wydawnictwo Princeton University Press, Princeton. s. 41

Mempool (memory pool) - jest zbiorem transakcji, które zostały zweryfikowane przez węzły, ale nie są jeszcze potwierdzone przez dodanie ich do bloków.[22]

Nieaktualne bloki (stale blocks) - powstają, gdy nowy blok zostaje zatwierdzony i dodany do blockchaina. Stanowią pulę pozostałych wersji tego bloku, nad którymi pracowali górnicy i które nie są już potrzebne.[23]

Osierocony blok (orphan block) - nazywany także oderwanym blokiem, był przyjęty do blockchaina w pewnym momencie w czasie, ale później został odrzucony, gdy dłuższa wersja blockchaina, która się pojawiła już go nie zawierała. Powstają w momencie, gdy sieć skoryguje forka, który wcześniej wystąpił.[24]

Podwójne użycie (double-spending) – rezultat udanej wielokrotnej płatności tą samą jednostką waluty/tokenem (lub jego kopią). Był to ogromny problem dla wirtualnych walut, który został finalnie rozwiązany dopiero przez mechanizm weryfikacji transakcji będący częścią implementacji blockchaina, na którym opiera się Bitcoin.

Portfel (wallet) - oprogramowanie przechowujące adresy, klucze publiczne i odpowiadające im klucze prywatne używane do przeprowadzania transakcji.

Potwierdzenie (confirmation) – w momencie znalezienia się transakcji w bloku, który został dołączony do blockchaina ma ona jedno potwierdzenie. Gdy wykopany zostanie kolejny blok, transakcja ma dwa potwierdzenia itd. W zależności od parametrów blockchaina 6-20 potwierdzeń gwarantuje, że transakcja nie zostanie cofnięta.[25]

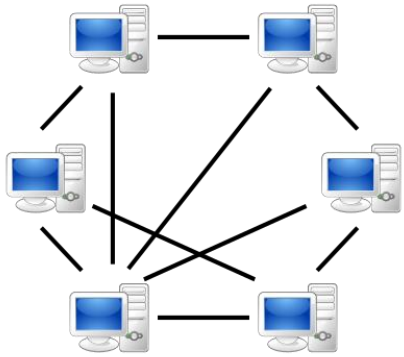
Satoshi - jednostka satoshi jest najmniejszą podzielną częścią możliwą do zapisania na blockchainie Bitcoin stanowiącą 0.00000001 bitcoina. Została nazwana po jego twórcy, Satoshi Nakamoto.

Satoshi Nakamoto - pseudonim używany przez osobę lub grupę osób, która zaprojektowała i zaimplementowała pierwszą wersję Bitcoin Core. Jej/ich tożsamość nadal pozostaje tajemnicą.[26]

---

[22] Antonopoulos A. (2017): *Mastering Bitcoin (Second Edition): Programming the Open Blockchain*. Wydawnictwo O'Reilly Media, Sebastopol. s. 11
[23] Bashir I. (2017): *Mastering Blockchain*. Wydawnictwo Packt Publishing, Birmingham. s. 155
[24] Bashir I. (2017): *Mastering Blockchain*. Wydawnictwo Packt Publishing, Birmingham. s. 155
[25] Antonopoulos A. (2017): *Mastering Bitcoin (Second Edition): Programming the Open Blockchain*. Wydawnictwo O'Reilly Media, Sebastopol. s. 5
[26] Antonopoulos A. (2017): *Mastering Bitcoin (Second Edition): Programming the Open Blockchain*. Wydawnictwo O'Reilly Media, Sebastopol. s. 12

Sieć peer-to-peer (p2p) - odnosi się do zdecentralizowanych interakcji między dwiema stronami. Uczestnicy sieci p2p (węzły) są równorzędni, współpracują bezpośrednio ze sobą bez centralnego serwera, który mającego rolę mediatora między nimi.[27]



Rys. 3. Schemat sieci peer-to-peer.

Źródło: https://commons.wikimedia.org/wiki/File:P2P-network.svg [9.04.2018r.]

Soft fork - w przeciwieństwie do hard forka jest sytuacją tymczasową. Wprowadza zmiany, które nie wymagają aktualizacji oprogramowania węzłów do prawidłowego zatwierdzania nowo powstałych bloków, bo jest on wstecznie kompatybilny.[28]

Token - odnosi się projektów kryptowalut, jest ogólną nazwą waluty wyrażającej posiadanie cyfrowych zasobów. Tokeny mogą być przekazywane między użytkownikami sieci, są generowane w procesie zatwierdzania bloków jako nagroda dla górników lub dystrybuowane przez twórców projektu w ramach początkowej dystrybucji.[29]

Transakcja - w uproszczenie przekazanie środków z jednego adresu na inny. Dokładniej rzecz ujmując, transakcja jest podpisaną cyfrowo strukturą danych wyrażającą transfer wartości. Transakcje są przesyłane przez sieć peer-to-peer, gromadzone i weryfikowane przez węzły, a następnie umieszczane w blokach, które stają się częścią blockchaina.[30]

[27] Rosic A. (2017): *Blockchain Glossary: From A-Z.* Blockgeeks. Dostęp: https://blockgeeks.com/guides/blockchain-glossary-from-a-z/ [9.04.2018r.]
[28] Rosic A. (2017): *Blockchain Glossary: From A-Z.* Blockgeeks. Dostęp: https://blockgeeks.com/guides/blockchain-glossary-from-a-z/ [9.04.2018r.]
[29] Ting K. (2018): *A Glossary of all the Cryptocurrency Terms you need to know. Cryptominded.* Dostęp: https://cryptominded.com/glossary-cryptocurrency-terms-need-know/ [9.04.2018r.]
[30] Antonopoulos A. (2017): *Mastering Bitcoin (Second Edition): Programming the Open Blockchain.* Wydawnictwo O'Reilly Media, Sebastopol. s. 13

Trudność (difficulty) - ustawienie sieci blockchaina, które definiuje ile obliczeń jest wymagane do uzyskania dowodu pracy (Proof of Work). Ma swój cel (target), który określa jaki średni przedział czasowy następuje między kolejnymi blokami.[31]

White paper - dokument informacyjny, który przedstawia filozofię, technologię i cele konkretnego projektu, na podstawie którego czytelnicy mogą ocenić jego użyteczność i przyszłą wartość. Zazwyczaj, chociaż nie jest to regułą, white paper publikowany jest jeszcze przed oficjalnym uruchomieniem projektu, którego dotyczy.[32]

Wspólne wydobywanie (pooled mining) - stanowi podejście, w którym wielu użytkowników przyczynia się do wygenerowania bloku jako pojedynczy węzeł, a następnie nagrodę dzieli według wniesionej mocy obliczeniowej.[33]

Wysokość bloku (block height) - inkrementacyjna liczba wskazująca ile bloków zostało połączonych ze sobą tworząc blockchain.[34]

Zaopatrzenie (supply) - wielkość wyrażająca ilość kryptowaluty. Na ogół wyraża się ją trzema liczbami:

- **circulated supply** – ilość aktualnie dostępna w obiegu,
- **total supply** - ilość, która została dotychczas wytworzona (większa lub równa ilości w obiegu),
- **max supply** – maksymalna możliwa do wytworzenia ilość.[35]

1.2. Historia pieniądza

„Pieniądz to nie monety i banknoty - to wszystko, co ludzie są skłonni użyć do kompleksowego wyrażania wartości określonych rzeczy w celu wymiany towarów i usług.”[36]

[31] Antonopoulos A. (2017): *Mastering Bitcoin (Second Edition): Programming the Open Blockchain*. Wydawnictwo O'Reilly Media, Sebastopol. s. 5
[32] Lai V., Wong V. (2018): *Cryptocurrency and Blockchain Glossary.* CrushCrypto. Dostęp: https://crushcrypto.com/glossary/ [9.04.2018r.]
[33] Antonopoulos A. (2017): *Mastering Bitcoin (Second Edition): Programming the Open Blockchain*. Wydawnictwo O'Reilly Media, Sebastopol. s. 10
[34] Odinsky J. (2017): *Blockchain Dictionary.* Hackernoon. Dostęp: https://hackernoon.com/blockchain-dictionary-f4d098c9ef89 [9.04.2018r.]
[35] Lai V., Wong V. (2018): *Cryptocurrency and Blockchain Glossary.* CrushCrypto. Dostęp: https://crushcrypto.com/glossary/ [9.04.2018r.]
[36] Harari Y. (2011): *Sapiens. Od zwierząt do bogów*. Wydawnictwo PWN, Warszawa. s. 218.

Pieniądz wynaleziono wiele razy, w wielu różnych miejscach. Nic w tym dziwnego, bo jego powstanie nie wymagało żadnego przełomu technologicznego. Idea pieniądza jako środka wyrażającego wartość innych dóbr jest naturalnym ułatwieniem w handlu.

Rys. 4. Oś czasowa przedstawiająca skróconą historię pieniądza.

Źródło: Li K. (2018): *The History of Money & The Future of Bitcoin and The Cryptocurrency Economy.* Hackenoon. Dostęp: https://hackernoon.com/the-history-of-money-the-future-of-bitcoin-and-the-cryptocurrency-economy-5cc25e808275 [9.04.2018r.]

1.2.1. Handel wymienny

Ogólnie przyjęta teoria głosi, że człowiek rozumny (homo sapiens) pojawił się w Afryce ok. 150 tys. lat temu. Przez ponad 90% swej historii ludzie prowadzili koczowniczy tryb życia jako samowystarczalne plemiona łowców-zbieraczy rozprzestrzeniając się stopniowo po całym globie.[37] Wszystko uległo zmianie, gdy 10-4 tys. lat p.n.e. nastąpiła rewolucja neolityczna, czyli przejście człowieka do osiadłego trybu życia i produkcji żywności – czyli rolnictwa i hodowli zwierząt. Te dużo bardziej efektywne sposoby wytwarzania jedzenia szybko spowodowały znaczny wzrost zaludnienia i dały możliwość wyspecjalizowania się części ludności w zajęciach, które nie były już związane wyłącznie z bezpośrednim zapewnieniem przetrwania, co w efekcie dało początek pierwszym cywilizacjom. Zaczęło wtedy dochodzić do najprostszej formy transakcji, wymiana towaru za inny towar. Tak właśnie tysiące lat temu narodził się handel wymienny, czyli barter.

1.2.2. Pierwsze formy pieniądza

Wraz z rozwojem handlu zwykła wymiana towarów przestała być wystarczająca, bo wymagała znalezienia osoby, która posiadałaby porządane dobro i była skłonna wymienić je

[37] Harari Y. (2011): *Sapiens. Od zwierząt do bogów*. Wydawnictwo PWN, Warszawa. s. 27.

na posiadane przez drugą osobę. Tym samym rosło zapotrzebowanie na środki wyrażające wartość towarów, co spowodowało, że część dóbr deficytowych, takich bydło, skóry, zboże, płótno, sól, barwniki, paciorki i inne zaczęto używać jako środków płatniczych. Znaczącą rolę zaczęły tutaj odgrywać muszelki kauri należące do ślimaków morskich z rodziny porcelanek (crowry shells). Były one ogólno akceptowane przez blisko 4 tysiące lat w Afryce, Azji Południowo-Wschodniej i Oceanii. W brytyjskiej Ugandzie używano ich jako waluty aż do XIX wieku.[38]

1.2.3. Monety

Pieniądz zaczął stopniowo ewoluować, zaczęto szukać trwałej i uniwersalnie akceptowanej jego formy. Lidyjczycy (dzisiejsza zachodnia Turcja) ze Starożytnej Grecji są pierwszą znaną grupą ludzi, która zaczęła korzystać ok. 600 r. p.n.e. ze złotych okrągłych spłaszczonych odlewów – monet. Musiało minąć jeszcze kilkaset lat, aby wszystkie większe greckie miasta, w szczególności Ateny także zaczęły z nich korzystać. Poza złotem, do produkcji monet używano także niewiele mniej rzadkiego srebra, a także miedzi czy żelaza. Zaczęto na nich także pieczętować przeróżne wizerunki, początkowo głównie zwierząt, później władców.[39]

1.2.4. Banknoty

W 100 r. p.n.e. w Chinach wynaleziono pierwszą formę papieru. Tam właśnie ok. IX w. pojawiła się także idea certyfikatów kupieckich. Kupcy, aby nie musieć przewozić dużej ilości ciężkich monet, deponowali je w skarbcu w jednej prowincji i otrzymywali poświadczenie dające im prawo do otrzymania określonej sumy w innej. Praktyka ta została zaadaptowana w Mongolii po jej inwazji na Chiny. W XIII wieku wenecki podróżnik i kupiec Marco Polo jako jeden z pierwszych przedstawicieli kontynentu europejskiego dotarł do Chin, gdzie pieczołowicie opisał papierowe pieniądze, które później stały się środkiem płatniczym także w

[38] Li K. (2018): *The History of Money & The Future of Bitcoin and The Cryptocurrency Economy.* Hackenoon. Dostęp: https://hackernoon.com/the-history-of-money-the-future-of-bitcoin-and-the-cryptocurrency-economy-5cc25e808275 [9.04.2018r.]
[39] Robertson J. (2007): *The History of Money From Its Origins to Out Time.* Autrement, Paryż. s. 3. Dostęp: http://www.jamesrobertson.com/book/historyofmoney.pdf [9.04.2018r.]

Europie. Oficjalnie pierwsze banknoty pojawiły się w Europie w XVII w., kiedy to w krajach zaczęły powstawać banki centralne jako jedyne posiadające prawo do ich emisji.[40]

1.2.5. Pieniądz plastikowy i elektroniczny

Wraz z rozwojem technologii informatycznych pojawiła się możliwość przechowywania wartości w postaci cyfrowej, na dysku komputera. Pierwsze karty płatnicze zostały wprowadzone w USA w 1950r. i wydawane były przez firmę US Diners Club do regulowania rachunków w ich sieci restauracji. Pomysł ten bardzo szybko został podchwycony przez banki, które zaczęły wydawać je klientom, by ci za ich pośrednictwem mieli dostęp do pieniędzy na swoich rankunkach bankowych. Błyskawiczna ewolucja cyfrowych technologii sprawiła, że w 2006 r. ponad 90% wszystkich pieniędzy istniało jedynie na rachunkach bankowych zapisanych na serwerach banków.[41]

1.2.6. Bitcoin

„Jedna z rzeczy, której brakuje, ale na pewno niedługo zostanie opracowana, to niezawodny e-pieniądz, metoda, gdzie używając internetu można przekazać środki od A do B bez znajomości tożsamości między A i B - sposób, w jaki mogę wziąć banknot 20 dolarowy i przekazać go tobie, możesz przy tym nie wiedzieć kim jestem."[42]

[40] Robertson J. (2007): *The History of Money From Its Origins to Out Time.* Autrement, Paryż. s. 8-11. Dostęp: http://www.jamesrobertson.com/book/historyofmoney.pdf [10.04.2018r.]
[41] Harari Y. (2011): *Sapiens. Od zwierząt do bogów*. Wydawnictwo PWN, Warszawa. s. 218-219.
[42] Friedman M. (1999). Wywiad z NTU/F. Dostęp: https://www.youtube.com/watch?v=mlwxdyLnMXM [10.04.2018r.]

ACC	CyberCents	iKP	MPTP	Proton
Agora	CyberCoin	IMB-MP	Net900	Redi-Charge
AIMP	CyberGold	InterCoin	NetBill	S/PAY
Allopass	DigiGold	Ipin	NetCard	Sandia Lab E-Cash
b-money	Digital Silk Road	Javien	NetCash	Secure Courier
BankNet	e-Comm	Karma	NetCheque	Semopo
Bitbit	E-Gold	LotteryTickets	NetFare	SET
Bitgold	Ecash	Lucre	No3rd	SET2Go
Bitpass	eCharge	MagicMoney	One Click Charge	SubScrip
C-SET	eCoin	Mandate	PayMe	Trivnet
CAFÉ	Edd	MicroMint	PayNet	TUB
CheckFree	eVend	Micromoney	PayPal	Twitpay
ClickandBuy	First Virtual	MilliCent	PaySafeCard	VeriFone
ClickShare	FSTC Electronic Check	Mini-Pay	PayTrust	VisaCash
CommerceNet	Geldkarte	Minitix	PayWord	Wallie
CommercePOINT	Globe Left	MobileMoney	Peppercoin	Way2Pay
CommerceSTAGE	Hashcash	Mojo	PhoneTicks	WorldPay
Cybank	HINDE	Mollie	Playspan	X-Pay
CyberCash	iBill	Mondex	Polling	

Rys. 5. Lista prekursorskich rozwiązań dot. systemów płatności i e-pieniędzy.

Źródło: Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. (2016): *Bitcoin and Cryptocurrency Technologies*. Wydawnictwo Princeton University Press, Princeton. s. 3

Ścieżka prowadząca do pojawienia się Bitcoina usłana jest wieloma mniej lub bardziej udanymi próbami stworzenia bezpiecznych elektronicznych walut i systemów płatności. Idea zastosowania kryptografii do zabezpieczania transakcji pojawiła się w 1982 r., kiedy to David Chaum opublikował pracę naukową na ten temat elektroniczej gotówki i podpisu cyfrowego (blind signature). Była to pierwsza podstawa do stworzenia waluty kryptograficznej – kryptowaluty. W 1990 r. założył on firmę DigiCash, której owocem prac była waluta o nazwie Ecash oparta na zaproponowanym przez niego wcześniej protokole[43]. Jednakże problemy technologiczne, trudność z zaadaptowaniem tego rozwiązania zarówno ze strony banków jak i sklepów, a także brak możliwości bezpośrednich transakcji między jej użytkownikami sprawiła, że nie przyjęło się ono.[44]

Bitcoin (a wraz z nim technologia blockchain) oficjalnie narodził się 31 października 2008 r., kiedy to osoba (lub grupa osób) o pseudonimie Satoshi Nakamoto[45] za pośrednictwem listy mailingowej o tematyce kryptograficznej opublikował 9-stronicowy white paper

[43] Finley K. (2018): *The WIRED Guide to the Blockchain*. WIRED. Dostęp: https://www.wired.com/story/guide-blockchain/ [10.04.2018r.]
[44] Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. (2016): *Bitcoin and Cryptocurrency Technologies*. Wydawnictwo Princeton University Press, Princeton. s. 8-11
[45] Pisa M., Juden M. (2017): Blockchain and Economic Development: Hype vs. Reality. Wydawnictwo CGD, Waszyngton. s. 6. Dostęp: https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf [10.04.2018r.]

zatytułowany „Bitcoin: A Peer-to-Peer Electronic Cash System”[46]. Dokument ten zawierał opis protokułu elektronicznej waluty opartej na zdecentralizowanej peer-to-peer, w której do przeprowadzania transakcji między użytkownikami nie jest potrzebne zaufanie, bo ich integralność jest gwarantowana przez zastosowane mechanizmy kryptograficzne, w tym algorytm Proof of Work.[47]

Satoshi w publikowanych później postach przyznał, że prace nad Bitcoinem rozpoczął w okolicach maja 2007 r. Sama domena bitcoin.org została zarejestrowana w sierpniu 2008 r. Kolejne kamienie milowe pojawiały się dość szybko. Jeszcze 9 listopada 2008 r. projekt o nazwie Bitcoin został zarejestrowany w serwisie SourceForge.net. 3 stycznia 2009 r. o godz. 18:15:05 wygenerowany został inicjalny blok (tzw. genesis block), w którego polu coinbase znalazł się nagłówek dziennika The Times: „The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”. Następnie 6 dni później ponownie za pośrednictwem tej samej listy mailingowej wydana został pierwsza stabilnie działająca wersja oprogramowania Bitcoin Core oznaczona wersją 0.1. Pierwsza transakcja przesłania kryptowaluty w ilości 10 Bitcoinów miała miejsce 12 stycznia. Środki te trafiły na adres należący do Hala Finneya, znanego w środowisku kryptografów aktywisty.[48] Satoshi Nakamoto, którego tożsamość nadal pozostaje tajemnicą, opuścił projekt w kwietniu 2011 r. pozostawiając odpowiedzialność za jego dalszy rozwój w rękach zaufanej grupy ochotników.[49]

[46] Nakamoto S. (2008): *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin Project. Dostęp: https://bitcoin.org/bitcoin.pdf [10.04.2018r.]
[47] Źródło: Klinger B., Szczepański J. (2017): *Blockchain – Historia, Cechy i Główne Obszary Zastosowań.* UKSW, Warszawa. s. 12. Dostęp: http://czasopisma.uksw.edu.pl/index.php/cwc/article/view/1858 [10.04.2018r.]
[48] Klinger B., Szczepański J. (2017): *Blockchain – Historia, Cechy i Główne Obszary Zastosowań.* UKSW, Warszawa. s. 13. Dostęp: http://czasopisma.uksw.edu.pl/index.php/cwc/article/view/1858 [10.04.2018r.]
[49] Antonopoulos A. (2017): *Mastering Bitcoin (Second Edition): Programming the Open Blockchain*. Wydawnictwo O'Reilly Media, Sebastopol. s. 24

Bitcoin P2P e-cash paper

Satoshi Nakamoto satoshi at vistomail.com
Fri Oct 31 14:10:00 EDT 2008

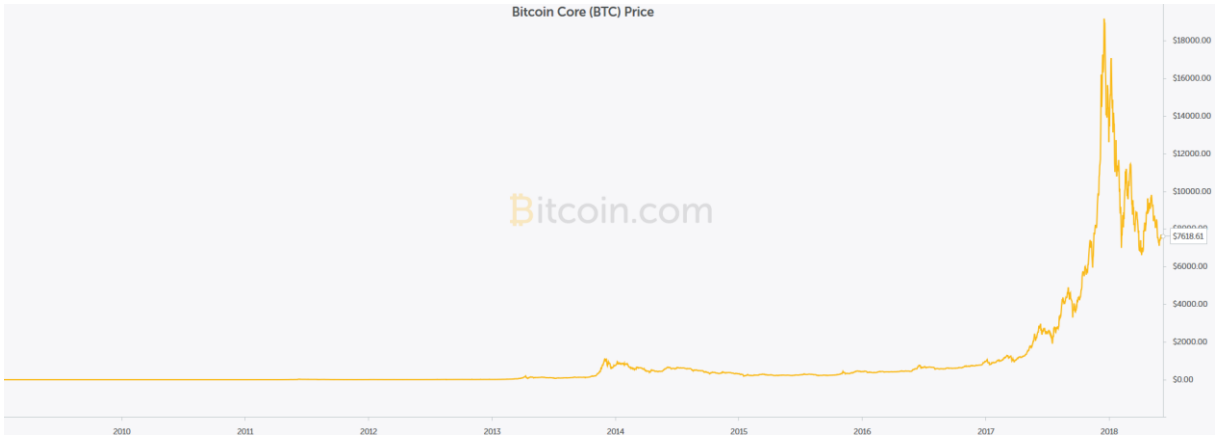
- Previous message: Fw: SHA-3 lounge
- **Messages sorted by:** [date] [thread] [subject] [author]

```
I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the
    network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract.  A purely peer-to-peer version of electronic cash would
allow online payments to be sent directly from one party to another
without the burdens of going through a financial institution.
Digital signatures provide part of the solution, but the main
benefits are lost if a trusted party is still required to prevent
double-spending.  We propose a solution to the double-spending
problem using a peer-to-peer network.  The network timestamps
transactions by hashing them into an ongoing chain of hash-based
proof-of-work, forming a record that cannot be changed without
redoing the proof-of-work.  The longest chain not only serves as
proof of the sequence of events witnessed, but proof that it came
from the largest pool of CPU power.  As long as honest nodes control
the most CPU power on the network, they can generate the longest
chain and outpace any attackers.  The network itself requires
minimal structure.  Messages are broadcasted on a best effort basis,
and nodes can leave and rejoin the network at will, accepting the
longest proof-of-work chain as proof of what happened while they
were gone.

Full paper at:
http://www.bitcoin.org/bitcoin.pdf

Satoshi Nakamoto

------------------------------------------------------------------------
The Cryptography Mailing List
Unsubscribe by sending "unsubscribe cryptography" to majordomo at metzdowd.com
```

Rys. 6. Treść oryginalnego emaila wysłanego przez Satoshi Nakamoto.

Źródło: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html [10.04.2018r.]

Dotychczasowa historia Bitcoina nie była drogą bez przeszkód. 15 sierpnia 2010r. w bloku nr 74638 znalazła się transakcja, w której na dwa adresy trafiło po 92.2 miliarda Bitcoinów[50] – w odniesieniu do 21 milionów możliwych do wytworzenia. Było to możliwe przez błąd typu integer overflow (przekroczenie zakresu liczb całkowitych) w części kodu weryfikującej transakcje, które miały wejść w skład nowego bloku. Efektem tego zdarzenia był hard fork, którego celem było wprowadzenie poprawki w kodzie i cofnięcie blockchaina do momentu sprzed tego incydentu. Swój udział mieli także hackerzy, którzy wielokrotnie przeprowadzali ataki mające na celu kradzież Bitcoinów – zarówno bezpośrednio od użytkowników jak i giełd kryptowalutowych. Największy z nich miał miejsce w pierwszych dniach lutego 2014 roku, kiedy to hackerom udało się wykraść, z giełdy o nazwie Mt. Gox, w sumie ok. 850 tys. Bitcoinów, których wartość już wtedy wynosiła powyżej 460 milionów dolarów[51]. Pod koniec miesiąca firma ogłosiła bankructwo. Poza tymi przykrymi wydarzeniami miały miejsce także o wiele bardziej pozytywne, jak chociażby w maju 2010 roku próba zaadoptowania Bitcoina jako należytego środka płatniczego i słynny zakup pizzy za 10 tys. Bitcoinów przez Laszlo Hanyecza, użytkownika forum BitcoinTalk pod pseudonimem laszlo.[52]



Rys. 7. Wykres ceny Bitcoina w latach 2009 - 2018

Źródło: https://charts.bitcoin.com [5.06.2018r.]

Należy przyznać, że największe zainteresowanie Bitcoin zawdzięcza nie tyle rewolucyjnej technologii, na której się opiera, co możliwości bardzo szybkiego wzbogacenia się i nie ma się czemu dziwić. W połowie 2010 roku Bitcoin był wyceniany na 0,06 dolara. 9 lutego 2011 roku, więc na miesiąc przed odejściem Satoshi Nakamoto cena przekroczyła 1

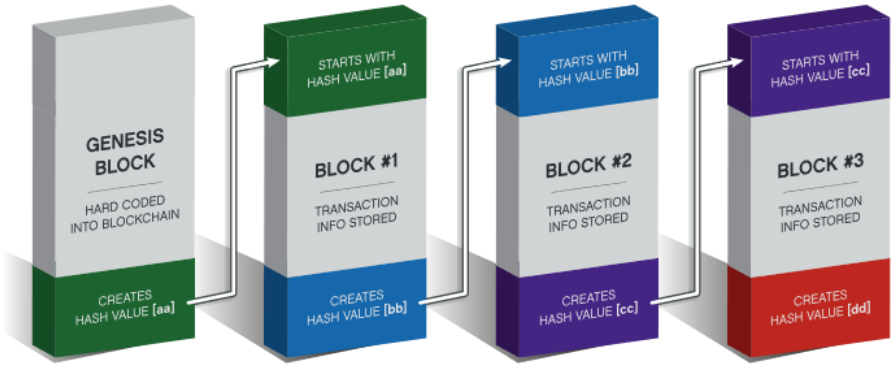
[50] https://bitcointalk.org/index.php?topic=822.0 [5.06.2018r.]
[51] McMillan R. (2014). *The Inside story of Mt. Gox Bitcoin's 460$ million dollar disaster*. WIRED. Dostęp: https://www.wired.com/2014/03/bitcoin-exchange/ [5.06.2018r.]
[52] https://bitcointalk.org/index.php?topic=137.0 [5.06.2018r.]

dolara[53], a zaledwie 4 miesiące później 10 dolarów. Na kolejne duże wzrosty trzeba było poczekać do kwietnia 2013 roku, kiedy to Bitcoin był wyceniany na 100 dolarów za sztukę, a na przełomie listopada i grudnia tego roku w dużym przypływie popularności przekroczył barierę 1000 dolarów. Po tym okresie przez dłuższy czas cena była niższa niż 500 dolarów, a w pewnym momencie nawet poniżej 200. Na ponowne osiągnięcie 1000 dolarów trzeba było czekać aż do 3 stycznia 2017 roku. Rok 2017 był jak dotychczas szczytem popularności tej kryptowaluty, kiedy to przekraczane były kolejne bariery ceny - w czerwcu 2500 dolarów, w październiku 5 tys., w listopadzie 10 tys., aż do najwyższej w historii ceny 19,783.21 dolarów zanotowanej 17 grudnia 2017 roku. Od tego momentu Bitcoin notował kolejne duże spadki w wartości i na dzień 7 czerwca 2018 r. wyceniany jest na 7705 dolarów, czyli niespełna 28 tys. złotych za sztukę.

1.3. Wyjaśnienie zasad działania blockchaina

Blockchain jest zdecentralizowanym współdzielonym rejestrem bloków danych, które połączone są ze sobą sygnaturami kryptograficznymi w chronologiczny ciąg. Stanowi on niezmienny zapis historyczny wszystkich przeprowadzonych operacji od najnowszego bloku aż do pierwszego – bloku genesis. Swoje działanie opiera na sieci peer-to-peer (p2p), czyli topologi, w której wszyscy użytkownicy są równorzędni (peer – rówieśnik) i mogą wymieniać między sobą informacje. Blockchain jest bezpieczny dzięki działającym węzłom (node), z których każda przechowuje identyczną kopię całego łańcucha bloków. Węzły weryfikują poprawność wszystkich transakcji, a dzięki protokołowi konsensusu generują bloki zawierające kolejne zbiory transakcji i dodają je do łańcucha.[54]

[53] Finley K. (2018): *The WIRED Guide to Bitcoin.* WIRED. Dostęp: https://www.wired.com/story/guide-bitcoin [5.06.2018r.]
[54] Bashir I. (2017): *Mastering Blockchain*. Wydawnictwo Packt Publishing, Birmingham. s. 21



Rys. 8. Schemat blockchaina.

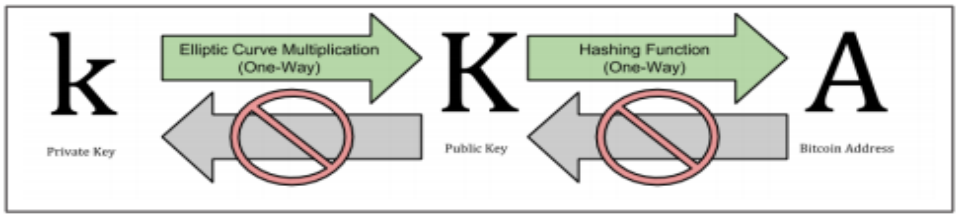
Źródło: Territt H., Obie S., Ahern C. (2017): Blockchain for Business. Jones Day, Nowy Jork. Dostęp: http://www.jonesday.com/files/upload/Blockchain%20for%20Business%20White%20Paper2.pdf [5.06.2018r.]

1.3.1. Adres, klucz publiczny i prywatny

Adresy są jednym z podstawowych elementów blockchaina umożliwiającym jego działanie. Każdy adres jest unikalnym identyfikatorem używanym w transakcjach do jednoznacznego wskazania nadawcy i odbiorcy. Bardzo często, w celu zachowania anonimowości, praktykuje się generowanie nowego adresu dla każdej transakcji. Do każdego adresu przypisana jest para kluczy kryptograficznych: prywatny i publiczny[55]. Klucze te nie są przechowywane na blockchainie, a wygenerowanie adresu i pary kluczy jest możliwe bez konieczności połączenia z nim. Klucz prywatny jest losowym ciągiem znaków, zazwyczaj 256-bitowym, z którego z użyciem kryptografii krzywych eliptycznych (ECC), czyli funkcji asymetrycznej (jednostronnej) generowany jest klucz publiczny. Już sam klucz publiczny mógłby być używany jako adres, jednakże ze względu na jego długość (taka sama jak klucz prywatny) jest to niepraktyczne[56]. Przykładowo Bitcoin generuje adres hashując klucz publiczny algorytmem SHA256, następnie RIPEMD160, a na koniec, dla poprawienia czytelności, Base58Check. Powstały adres jest już tylko 160 bitowy, jest określany jako Pay To Public Key Hash (P2PKH)[57]. Klucz prywatny nie jest używany wyłącznie do

[55] Bashir I. (2017): *Mastering Blockchain*. Wydawnictwo Packt Publishing, Birmingham., s. 19
[56] Rosic A. (2017): Blockchain Adress 101: *What are Addresses on Blockchains?* Blockgeeks. Dostęp: https://blockgeeks.com/guides/blockchain-address-101/ [5.06.2018r.]
[57] Antonopoulos A. (2017): *Mastering Bitcoin (Second Edition): Programming the Open Blockchain*. Wydawnictwo O'Reilly Media, Sebastopol. s. 63-70

wygenerowania klucza publicznego i adresu, jego zdecydowanie ważniejsza funkcja to ochrona środków zgromadzonych na danym adresie – jest używany do podpisywania transakcji, których ten adres jest nadawcą. W przypadku jego utraty niemożliwy jest jakikolwiek dostęp do tych środków.



Rys. 9. Generowanie adresu z klucza prywatnego.

Źródło: Antonopoulos A. (2017): *Mastering Bitcoin (Second Edition): Programming the Open Blockchain*. Wydawnictwo O'Reilly Media, Sebastopol. s. 63

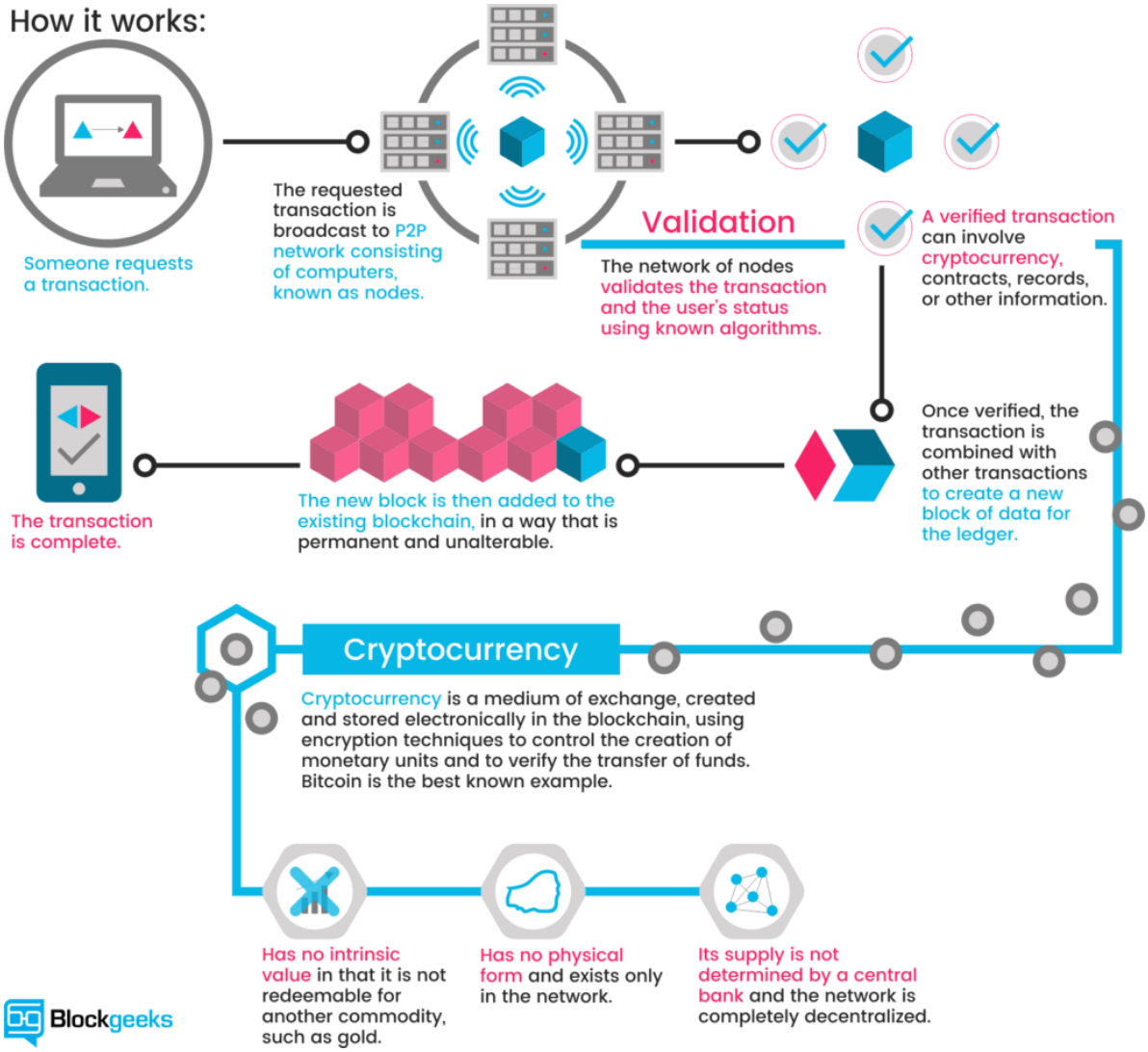
1.3.2. Cykl życia transakcji

Do ułatwienia przeprowadzania transakcji, a tym samym zapisywania porcji danych w blockchainie używane jest oprogramowanie pośredniczące – portfel. Znaleźć można portfele działające na komputerach, urządzeniach mobilnych, a nawet w formie stron internetowych. Portfel zawiera zbiór adresów i odpowiadających im par kluczy. Oprogramowanie to pozwala po popełnieniu adresu odbiorcy, kwoty i prowizji na wygenerowanie transakcji i podpisanie jej kluczem prywatnym, a następnie wysłanie jej do jednego z węzłów sieci p2p. Transakcja nie zawiera żadnych poufnych informacji, dlatego może być wysłana z portfela nawet z użyciem niezabezpieczonej sieci – jak np. publiczne Wifi[58]. Węzeł, do którego trafi transakcja weryfikuje jej poprawność. W przypadku błędu podczas weryfikacji transakcji zostaje ona odrzucona. Jeśli zostanie ona potwierdzona, węzeł ten rozpropagowuje ją do połączonych z nim nodów, które rozsyłają ją do połączonych z nimi, aż do momentu, gdy transakcja trafi do wszystkich węzłów połączonych w sieci peer-to-peer – dzieje się to błyskawicznie. Następnie node działające jako minerzy (górnicy) dołączają transakcje do kolejnego bloku, który ma zostać wykopany, zazwyczaj sortując je pod względem wysokości prowizji transakcyjnej – im wyższa tym szybciej transakcja trafi do bloku.[59]

Nowy blok zostaje wykopany, gdy któryś z górników rozwiąże problem wygenerowany przez protokół konsensusu. Blok zostaje wtedy rozpropagowany do sieci i jeśli zostanie

[58] Antonopoulos A. (2017): *Mastering Bitcoin (Second Edition): Programming the Open Blockchain*. Wydawnictwo O'Reilly Media, Sebastopol. s. 112
[59] Bashir I. (2017): *Mastering Blockchain*. Wydawnictwo Packt Publishing, Birmingham. s. 118-120

pozytywne zweryfikowany przez pozostałe węzły, zostaje on dołączony do blockchaina[60]. W tym momencie transakcje zawarte w bloku mają jedno potwierdzenie, każdy następny dodany do łańcucha blok to kolejne potwierdzenie. Już po pierwszym odbiorca ma dostęp do przekazanych środków, jednakże istnieje teoretyczna możliwość forka, a tym samym zmiany ostatnich bloków. Przy transakcjach w systemach wykorzystujących blockchain wymagana jest odpowiednia liczba potwierdzeń, kiedy to blok zawierający daną transakcję jest uznawany za niemożliwy do zmiany i staje się permanentną częścią łańcucha. Przykładowo dla Bitcoina, gdzie bloki generowane są średnio co 10 minut, za bezpieczną uważa się liczbę 6 potwierdzeń (60 minut). Jednakże dla BitShares, gdzie bloki generowane są znacznie częściej, bo co 3 sekundy, ta liczba wynosi już 20 potwierdzeń (1 minuta).[61]



[60] future[inc] (2017): *The Future of Blockchain: Applications and Implications of Distrubuted Ledger Technology*. Cartered Accountants, Canberra. s. 9. Dostęp: https://www.charteredaccountantsanz.com/-/media/c1430d6febb3444192436ffc8b685c7c.ashx [5.06.2018r.]
[61] Bashir I. (2017): *Mastering Blockchain*. Wydawnictwo Packt Publishing, Birmingham. s. 130-131

Rys. 10. Schemat transakcji w kryptowalucie.

Źródło: Rosic A. (2016): *What is Cryptocurrency: Everything You Need To Know*. Blockgeeks. Dostęp: http://blockgeeks.com/guides/what-is-cryptocurrency/ [5.06.2018r.]

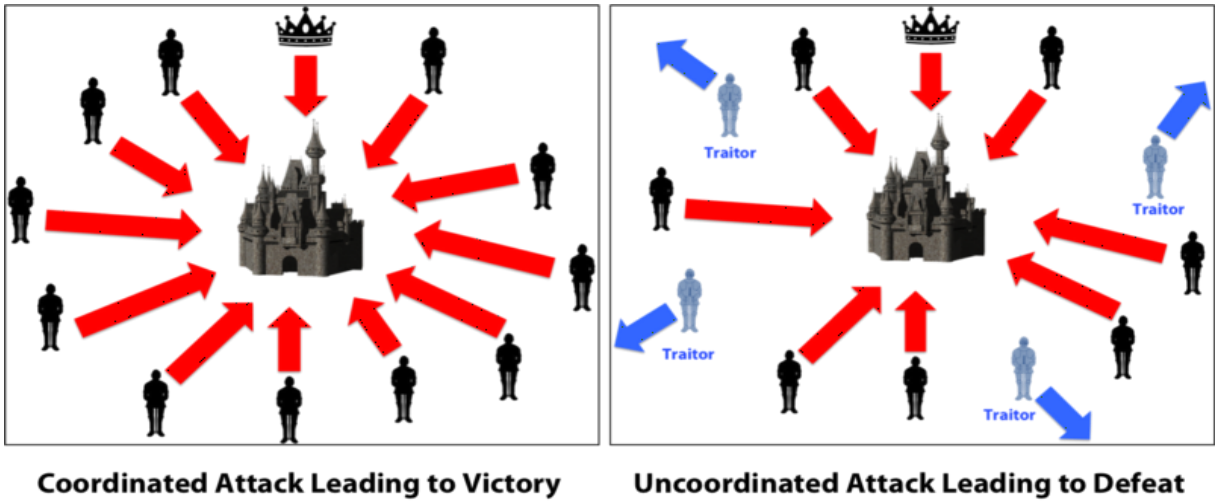
1.3.3. Konsensus

Mechanizm konsensusu był jednym z większych wyzwań jakie stało na drodze do zbudowaniem w pełni zdecentralizowanych systemów. Zostało ono sformułowane w 1982 roku jako tzw. problem bizantyjskich generałów w pracy naukowej wydanej pod takim właśnie tutyłem przez trzech badaczy z Uniwersytetu Berkeley[62]. Przedstawiał on hipotetyczną sytuację, w której grupa generałów przewodzących częściom bizantyjskiej armii miała zaplanować atak na miasto lub się wycofać. Jedynym sposobem komunikacji między nimi jest posłaniec, za pośrednictwem którego, muszą dojść po porozumienia do co dokładnego czasu ataku, co jest jedyną szansą na zwycięstwo. Problem polega na tym, że jeden lub więcej generałów może być zdrajcą i wysyłać mylące komunikaty, które doprowadzą do porażki. Stąd też należy znaleźć efektywny sposób zawarcia porozumienia między generałami nawet w obecności zdrajców w trakcie komunikacji. Problem ten można odnieść do zdecentralizowanych systemów, gdzie generałowie to węzły, a posłaniec to kanał komunikacji sieci peer-to-peer. Został on rozwiązany w 1999 roku, kiedy to Miguel Castro i Barbara Liskov zaprezentowali algorytm PBFT (Practical Byzantine Fault Tolerance)[63]. Prawidłowo działający protokuł konsensusu spełnia pięć wymagań:

- Porozumienie – wszystkie uczciwe węzły przyjmują tą samą wartość jako prawidłową,
- Rozwiązywalność - wszystkie uczciwe węzły kończą jednocześnie realizację procesu i podejmują ostateczną decyzję,
- Prawidłowość - wartość uzgodniona przez wszystkie uczciwe węzły musi być taka sama jak w przypadku wartość początkowa zaproponowana przez co najmniej jeden uczciwy węzeł,
- Spójność – wymóg, aby każdy z węzłów nie mógł podjąć decyzji więcej niż raz w ramach jednego cyklu całego procesu,

[62] Wright A, De Filippi P. (2015): *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. Wydawnictwo SSRN, Rochester. s. 5. Dostęp: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 [5.06.2018r.]
[63] Bashir I. (2017): *Mastering Blockchain*. Wydawnictwo Packt Publishing, Birmingham. s. 13

- Tolerancyjność na błędy – powinien działać prawidłowo nawet jeśli częścią sieci są szkodliwe węzły.



Rys. 11. Problem generałów bizantyjskich.

Źródło: Ghosh D. (2016): How the Byzantine General Sacked the Castle: A Look Into Blockchain. Dostęp: https://medium.com/@DebrajG/how-the-byzantine-general-sacked-the-castle-a-look-into-blockchain-370fe637502c [5.06.2018r.]

Pierwsza praktyczna implementacja algorytmu PBFT nastąpiła w 2009 roku jako mechanizm konsensusu o nazwie **Proof of Work (PoW)** będący częścią Bitcoina[64]. PoW jest do teraz używany jako protokuł konsensusu przez największe kryptowaluty: Bitcoin (i wszystkie jego forki, np. Bitcoin Cash), Ethereum, Litecoin, Monero i wiele innych. Polega on rozwiązaniu zagadki matematycznej przez wyliczaniu hashy kryptograficznych do momentu osiągnięcia żądanej przez sieć trudności. Węzeł, który jako pierwszy ją rozwiąże otrzymuje nagrodę w postaci nowo wytworzonych tokenów, a dodatkowo opłaty za transakcje znajdujące się w tym bloku. Trudność jest dobierana tak, aby bloki były generowane w mniej więcej równych odstępach czasu, im mniejsza wartość trudności, tym dłużej trwa tworzenie bloku – odstęp między blokami nazywany jest celem. Mechanizm ten ma jednak niewątpliwie wady, największą z nich jest fakt, iż wymaga on ogromnej mocy obliczeniowej, co przekłada się na duże koszty sprzętu i energii elektrycznej[65] – zużycie energii ciągle rośnie i aktualnie wynosi ok. 71.1 TWh rocznie, co odpowiada Chile, państwu zamieszkanemu przez niemal 18 milionów osób[66]. Ze względu na specyfikę wykorzystywanych funkcji hashujących jest on także słabo

[64] Antonopoulos A. (2017): *Mastering Bitcoin (Second Edition): Programming the Open Blockchain*. Wydawnictwo O'Reilly Media, Sebastopol. s. 4
[65] Tapscott D., Tapscott A. (2017): *Realizing the Potential of Blockchain*. Światowe Forum Ekonomiczne, Davos. Dostęp: http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf, s. 14 [14.06.2018r.]
[66] Dostęp: https://digiconomist.net/bitcoin-energy-consumption [14.06.2018r.]

skalowalny – teoretyczny limit transakcji na sekundę dla Bitcoina wynosi 7, dla jednego z jego forków, czyli Bitcoin Cash to już 60, jednak nadal jest to bardzo mało w porównaniu do systemu Visa, który może przetwarzać nawet 24 tys. transakcji na sekundę.

Nie jest to jednak jedyny funkcjonujący w sferze blockchaina mechanizm konsensusu. Innym, który jest często spotykany jest **Proof of Stake (PoS)**. Algorytm ten opiera się na założeniu, że węzeł, który zainwestował wystarczająco dużo i jest posiadaczem znacznej ilości tokenów, więcej straciłby na próbie złośliwego ataku niż potencjalnie zyskał[67]. PoS został zaproponowany przez jednego z użytkowników bitcointalk.org, jako rozwiązanie problemu ogromnych strat i kosztów energii elektrycznej jakie generuje PoW[68]. Po raz pierwszy zaimplementowali go twórcy kryptowaluty PeerCoin. Ten mechanizm konsensusu stał integralną częścią kilku powstałych później, a aktualnie jednych z czołowych kryptowalut jak Dash, NEO, PIVX, Stratis czy NAV Coin. Zapowiedziano także, że Ethereum przejdzie niedługo z PoW na PoS – sieć testowa o nazwie Casper już powstała. Ważnym terminem w odniesieniu do PoS jest wiek monet (coin age), który określa ilość czasu i liczby tokenów, które pozostają nienaruszone na danych adresie. Wraz z rosnącym wiekiem monet zwiększa się szansa wykopania kolejnego bloku – w uproszczeniu, im więcej tokenów i im dłużej znajdują się one na jednym adresie, tym większa szansa na wylosowanie do wykopania kolejnego bloku[69].

Proof of Stake doczekało się własnego rozwinięcia w postaci **Delegated Proof of Stake (DPoS)**. Jest to aktualnie najszybszy, najbardziej wydajny, najbardziej przyjazny środowisku i najbardziej elastyczny z dostępnych modeli konsensusu. DPOS jest częściowo demokratyczny, każdy użytkownik sieci posiadający tokeny może zagłosować na swojego przedstawiciela – delegata, jednak jako rozszerzenie PoS, użytkownicy z większą liczbą tokenów mają większą siłę głosu[70]. Wszystkie parametry sieci, od wysokości opłat do interwałów między blokami i wielkości transakcji, można dostosowywać za pośrednictwem wybranych delegatów. Węzły delegatów są jedynymi uprawnionymi do tworzenia nowych bloków, w jednej rundzie każdy z nich po kolei tworzy jeden blok[71]. Taki deterministyczny dobór producentów bloków pozwala

[67] Bashir I. (2017): *Mastering Blockchain*. Wydawnictwo Packt Publishing, Birmingham. s. 29
[68] QuantumMechanic (2011): *Proof of stake instead of proof of work*. Dostęp: https://bitcointalk.org/index.php?topic=27787.0 [14.06.2018r.]
[69] Bashir I. (2017): *Mastering Blockchain*. Wydawnictwo Packt Publishing, Birmingham. s. 29
[70] Bashir I. (2017): *Mastering Blockchain*. Wydawnictwo Packt Publishing, Birmingham. s. 30
[71] Khatwani S. (2018): *What is Proof-of-Work & Proof-of-Stake?* Dostęp: https://coinsutra.com/proof-of-work-vs-proof-of-stake-pow-vs-pos/ [14.06.2018r.]

na potwierdzanie transakcji średnio w mniej niż 10 sekund. Dużymi kryptowalutami, które używają DPoS są m.in. EOS, BitShares, Lisk i Ark.

1.3.4. Smart contract

Inteligentne kontrakty nie są niczym nowym, po raz pierwszy pomysł ten przedstawił jeszcze w 1994 roku Nick Szabo, który określił je jako skomputeryzowany protokół transakcji realizujący warunki umowy[72]. Idea ta odrodziła się dopiero 20 lat później, kiedy to pojawiło się Ethereum, a wraz z nim zdecentralizowana platforma służącą do zawierania smart contractów z użyciem języka programowania Solidity, a w konsekwencji także DApps i DAO. Bitcoin od samego początku także pozwalał na tworzenie tego typu kontraktów, jednak w bardzo ograniczonej formie. Ze względu na niewątpliwe korzyści, jakie inteligentne konkrakty mogą przynieść branży usług finansowych (i nie tylko jej) m.in. w postaci obniżenia kosztów transakcji i uproszczenia skomplikowanych umów, przez różne instytucje finansowe jak i akademickie prowadzone są rygorystyczne badania, a to wszystko w celu sformalizowania i uczynienia wdrażania smart contractów praktycznym i prostym jak najszybciej to możliwe[73]. Ponieważ jedną z właściwości blockchaina jest niezmienność dodanych bloków, uzgodniony inteligentny kontrakt może zostać anulowany lub zmodyfikowany wyłącznie na warunkach już dozwolonych w samym jego kodzie[74].

Umowy tradycyjne dają możliwość wyboru spłaty należności zgodnie z umową lub zerwania jej ponosząc przez to konsekwencje, być może związane z postępowaniem sądowym.

Jeśli jednak płatność jest zautomatyzowana w inteligentnym kontrakcie, taka forma rozwiązania umowy nie jest możliwa, o ile jej instrukcje w postaci kodu nie przewidują takiej możliwości[75].

Pojawiły się propozycje jakoby inteligentne kontrakty traktować jako prawo: autonomiczne i samoegzekwowalne. Miało by to ciekawe implikacje, traktowanie smart contractu jako prawa oznaczałaoby, że, wszelkie błędy lub przypadkowe podatności w nim zawarte również stają się jego obowiązującą częścią. Wykorzystywanie takich błędów np. do

[72] Boucher P. (2017): *How blockchain technology could change our lives*. Biuro Analiz Parlamentu Europejskiego, Bruksela. s. 14. Dostęp: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf [14.06.2018r.]
[73] Bashir I. (2017): *Mastering Blockchain*. Wydawnictwo Packt Publishing, Birmingham. s. 198-199
[74] Swan M. (2015): *Blockchain: Blueprint for a New Economy*. Wydawnictwo O'Reilly Media, Sebastopol. s. 17
[75] Maxwell W., Salmon J. (2017): *A guide to blockchain and data protection*. Hogan Lowells, Londyn. s. 7. Dostęp: https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf [14.06.2018r.]

przejęcia kontroli nad aktywami nie mogłoby być uznawane za kradzież, ponieważ błąd, który umożliwiłby ich wypłatę, jest częścią kontraktu, a tym samym, z definicji, częścią prawa. Bardziej realistyczny wariant zakłada, że inteligentne kontrakty zostałyby włączone jako element systemu prawnego. Podobnie jak w przypadku tradycyjnych umów papierowych, mogą zostać nałożone dodatkowe wymogi, a klauzule mogą zostać unieważnione lub ponownie zinterpretowane w oparciu o intencje stron i ogólnie obowiązujący kodeks prawny. Obowiązujące prawo zawsze znajdowałoby się powyżej "prawa" zapisanego w postaci kodu smart contractu, nawet w przypadku, gdy postępowanie sądowe i egzekucja mogłyby okazać się trudne. W związku z tym, w większości dyskusji na temat inteligentnych kontraktów uznaje się, że przyniosą one korzyści w zakresie efektywności w kilku obszarach, ale nie zastąpią tradycyjnego prawa, ani tradycyjnych umów[76].

1.3.5. Typy blockchaina

Obecnie zdecydowanie najpopularniejszym typem łańcucha blików jest otwarty blockchain, do którego wszyscy mają dostęp, w którym wszyscy użytkownicy sieci są równi i mają możliwość sprawdzenia wszystkich informacji. Typy blockchaina dzieli się zasadniczo na dwie kategorie:

ze względu na dostęp do blockchaina:

- Publiczny - każdy może podłączyć się do sieci,
- Prywatny – dostęp do niego mają jedynie podmioty wewnątrz organizacji lub grupy organizacji,
- Częściowo-prywatny – jest rozszerzeniem prywatnego łańcucha bloków, poza podmiotami należącymi do organizacji dostęp do niego mogą także uzyskać partnerzy biznesowi lub podmioty regulacyjne (np. instytucje rządowe),
- Federacyjny (konsorcjum) – zdefiniowana jest lista węzłów, po jednym dla każdej instutycji, która jest częścią konsorcjum[77],

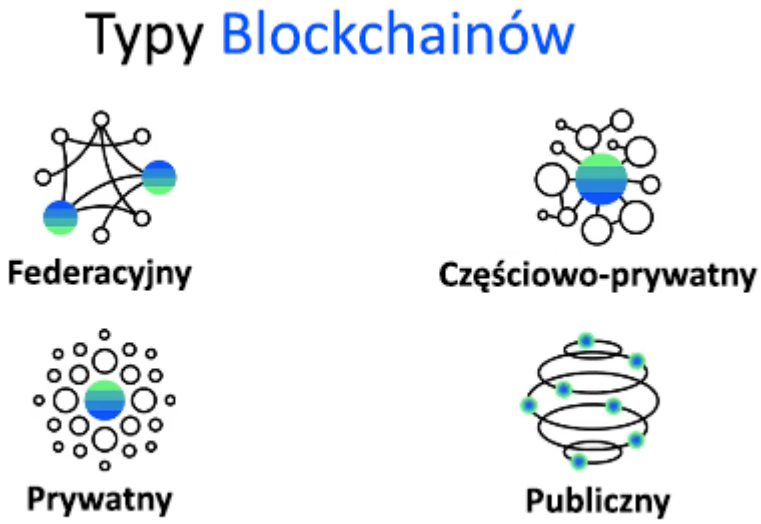
[76] Boucher P. (2017): *How blockchain technology could change our lives*. Biuro Analiz Parlamentu Europejskiego, Bruksela. s. 15-16. Dostęp: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf [14.06.2018r.]

[77] Dobson D. (2018): *The 4 Types of Blockchain Networks Explained*. International Legal Technology Association. Dostęp: https://www.iltanet.org/blogs/deborah-dobson/2018/02/13/the-4-types-of-blockchain-networks-explained [14.06.2018r.]

ze względu na obecność uprawnień:

- Z uprawnieniami – każdy z węzłów ma określone prawa dostępu do zawartych w blockchainie danych,
- Bez uprawnień – brak jakichkolwiek restrykcji dostępu do informacji[78].

Ostateczny typ jest połączeniem obu tych kategorii, przykładowo opisany powyżej najpopularniejszy z nich to blockchain **publiczny bez uprawnień (public permissionless blockchain)**.



Rys. 12. Typy łańcuchów blokowych.

Źródło: Opracowanie własne.

[78] Graham W. (2018): *Building it Better: A Simple Guide to Blockchain Use Cases.* Uniwersytet Kalifornijski, Berkeley. Dostęp: https://blockchainatberkeley.blog/building-it-better-a-simple-guide-to-blockchain-use-cases-de494a8f5b60

ROZDZIAŁ II. DZIEDZINY I PRZYKŁADY ZASTOSOWANIA TECHNOLOGII BLOCKCHAIN

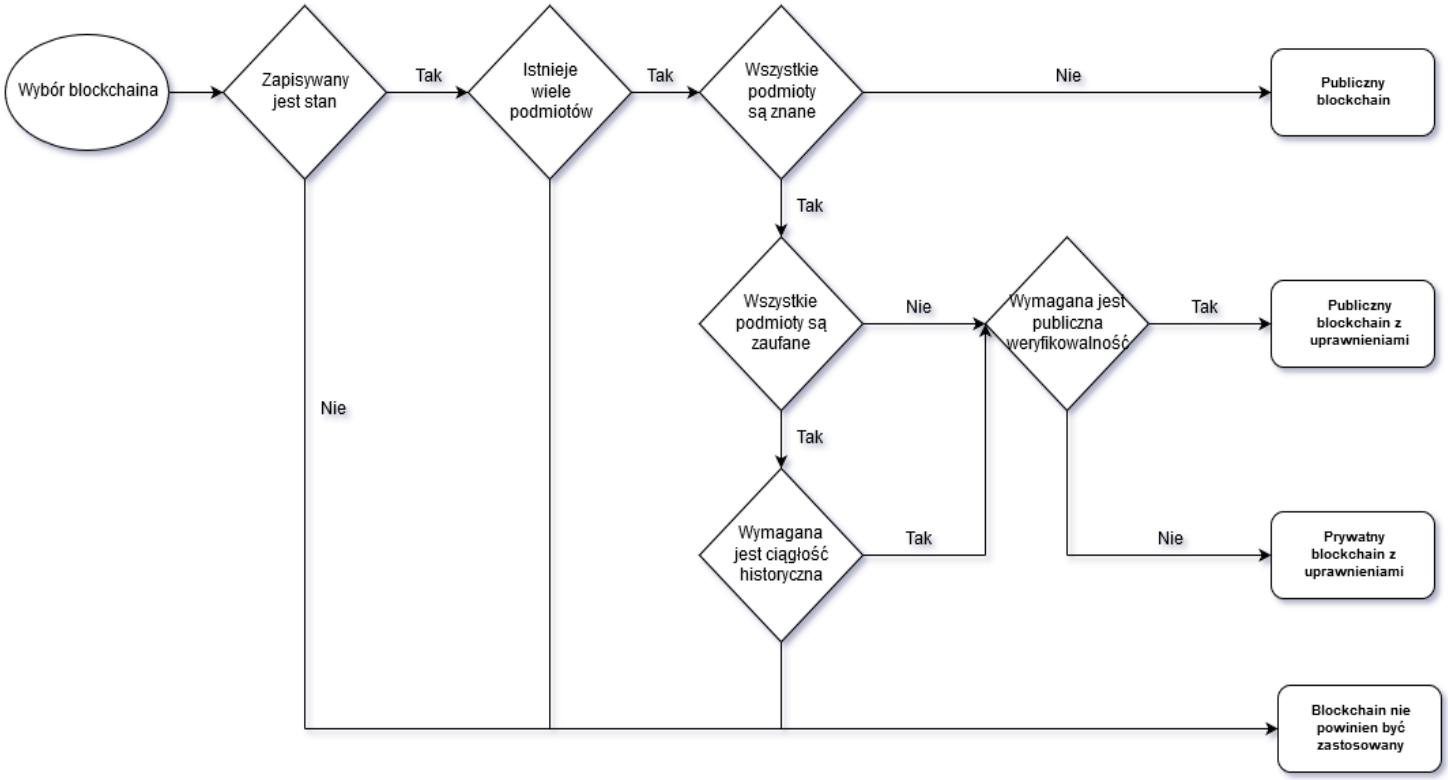
Bitcoin i jego blockchain umożliwiły wzajemnie nieufnym podmiotom na dokonywanie szybkich płatności finansowych, 24 godziny na dobę i 7 dni w tygodniu, przy okazji znacząco zmniejszając opłaty transakcyjne. A to wszystko bez polegania na zaufanej centralnej instytucji, oferując jednocześnie w pełni przejrzyste i bezpieczne przechowywanie danych w zdecentralizowanym rejestrze będącym odpornym na złośliwe ataki[79]. Niektóre osoby stosunkowo szybko zdały sobie sprawę, że kryptowaluty nie są wszystkim, co oferuje blockchain, a jego unikalne właściwości sprawiają, że ta technologia może mieć zastosowanie w wielu dziedzinach i to nie tylko związanych z finansami.[80]

2.1. Blockchain versus baza danych

Blockchain jako technologia budząca aktualnie duże zainteresowanie, w szczególności inwestorów, podobnie jak uczenie maszynowe (machine learning), sztuczna inteligencja (AI), wirtualna rzeczywistość (VR), rozszerzona rzeczywistość (AR) jest wykorzystywana do promocji produktów i usług, w których czasem nie ma żadnego realnego zastosowania. Ogólnie przyjmuje się, że blockchain, bez względu na to, czy będzie publiczny czy prywatny, otwarty lub z uprawnieniami, ma sens użycia, gdy wiele, zazwyczaj wzajemnie nieufnych podmiotów, chce oddziaływać i zmieniać stan systemu bez interakcji z zaufaną stroną trzecią[81]. Jeśli nie ma potrzeby składowania żadnych danych, blockchain jako forma struktury danych nie ma zastosowania. Podobnie w przypadku, gdy istnieje tylko pojedyncza jednostka wpływająca na zapisywane dane, standardowa baza danych będzie lepszym rozwiązaniem, ponieważ zapewnia lepszą wydajność pod względem przepustowości i opóźnień. Jeśli wszystkie podmioty są znane i zaufane, tj. żaden z nich nie jest nawet potencjalnie szkodliwy, współdzielona baza danych z

[79] Wüst K., Gervais A. (2017): *Do you need a Blockchain?* ETH Zürich, Zurych. s. 1. Dostęp: https://eprint.iacr.org/2017/375.pdf [13.06.2018r.]
[80] Weadt H. (2017): *Blockchain Use Cases*. Dostęp: http://holgerwaedt.com/blockchain-use-cases/ [13.06.2018r.]
[81] Maxwell W., Salmon J. (2017): *A guide to blockchain and data protection*. Hogan Lowells, Londyn. s. 17. Dostęp: https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf [13.06.2018r.]

odpowiednimi uprawnieniami dostępu jest najprawdopodobniej najlepszą opcją[82]. Natomiast gdy nie wszystkie ze stron są zaufane, blockchain z uprawnieniami ma jak najbardziej zastosowanie, aby zapewnić pełną integralność danych. W zależności od tego, czy wymagana jest publiczna weryfikowalność, każdy może mieć dostęp do odczytu aktualnego stanu danych (publiczny blockchain z uprawnieniami), wszyscy mogą weryfikować, ale jedynie część zapisanych informacji (częściowo prywatny blockchain z uprawnieniami) lub grupa podmiotów mających możliwość weryfikacji jest ograniczona (prywatny blockchain z uprawnieniami)[83]. Wpływ może mieć tutaj także fakt, czy ważna jest ciągłość historyczna składowanych informacji. Ostatnią opcją, gdy liczba uczestniczących jednostek, ani one same nie są znane, a przez to wzajemnie są względem siebie nieufne, jest publiczny blockchain bez żadnych uprawnień – który to jest podstawą działania wszystkich kryptowalut, w tym wielokrotnie wspomnianego Bitcoina.



Rys. 13. Proces wyboru blockchaina.

Źródło: Opracowanie własne. Na podstawie: Wüst K., Gervais A. (2017): Do you need a Blockchain? ETH Zürich, Zurych. s. 3. Dostęp: https://eprint.iacr.org/2017/375.pdf [13.06.2018r.]

[82] Ray S. (2017): *Blockchains versus Traditional Databases.* Hackernoon. Dostęp: https://hackernoon.com/blockchains-versus-traditional-databases-c1a728159f79 [13.06.2018r.]
[83] Wüst K., Gervais A. (2017): Do you need a Blockchain? ETH Zürich, Zurych. s. 2-3. Dostęp: https://eprint.iacr.org/2017/375.pdf [13.06.2018r.]

2.2. Bankowość i finanse

Pierwsze zastosowanie blockchaina, Bitcoin, dotyczyło sfery płatności i walut. Kryptowaluty są cyfrową, bezpieczną, zdecentralizowaną, pozbawioną organu zarządczego i odporną na manipulacje alternatywą dla banków i tradycyjnych metod transakcji finansowych. Z tego właśnie powodu światowy sektor finansowy szybko zainteresował się tą rodzącą się technologią, zwiastującą nową erę w historii bankowości.[84]

Aktualnie system bankowy mimo, że przez większość osób postrzegany jest jako nowoczesny, w sporej mierze opiera się aplikacjach napisanych w języku COBOL w latach 60 i 70 dwudziestego wieku[85]. Taki stan rzeczy utrzymuje się nadal głównie przez bardzo wysoki koszt modernizacji – w 2012 roku australijski bank Comonwealth zastąpił swój centralny system nowym, a cały proces pochłonął w okolicach 750 milionów dolarów.[86] Przelewy bankowe są darmowe i natychmiastowe zazwyczaj tylko w zakresie transakcji wewnątrz-bankowych, tj. konto źródłowe i docelowe znajduje się w jednym banku. Przelewy krajowe realizowane są w trakcie trzech sesji ELIXIR, tylko w dni robocze. Każdą trasakcję między bankami zatwierdza krajowy bank centralny. Sprawia to, że zazwyczaj transakcja zostanie zaksięgowana dopiero po około 24 godzinach od jej wysłania. Istnieje opcja przelewu natychmiastowego, lecz jest ona dodatkowo płatna i nie obsługują jej wszystkie banki. Ostatni typ, czyli przelew międzynarodowy wiąże się zazwyczaj z najdłuższym czasem oczekiwania i największym kosztem – nie funkcjonują darmowe przelew międzynarodowe[87]. Wewnątrz Unii Europejskiej działają systemy SEPA (najpopularniejszy) i EOG, które pozwalają na wysłanie transakcji, która zostanie zaksięgowana po dwóch dniach roboczych. Wymagają one zlecenia transakcji w walucie euro, co oczywiście w Polsce oznacza dodatkową prowizję za przewalutowanie. Przelewy z/do krajów spoza UE obsługuje międzynarodowy system SWIFT, w którym czas księgowania trwa od trzech do nawet kilkunastu dni roboczych i wiąże się z największymi opłatami transakcyjnymi.[88]

---

[84] Lisk Foundation (2018): *Blockchain in Banking*. Dostęp: https://lisk.io/academy/blockchain-basics/use-cases/blockchain-in-banking [13.06.2018r.]
[85] Territt H., Obie S., Ahern C. (2017): *Blockchain for Business*. Jones Day, Nowy Jork. s.3. Dostęp: http://www.jonesday.com/files/upload/Blockchain%20for%20Business%20White%20Paper2.pdf [13.06.2018r.]
[86] Maack M. (2017): *Acient programming language COBOL can make you bank, literally*. Dostęp: https://thenextweb.com/finance/2017/04/10/ancient-programming-language-cobol-can-make-you-bank-literally/ [13.06.2018r.]
[87] Wüst K., Gervais A. (2017): *Do you need a Blockchain?* ETH Zürich, Zurych. s. 5. Dostęp: https://eprint.iacr.org/2017/375.pdf [13.06.2018r.]
[88] Dostep: https://www.mbank.pl/pomoc/faq/uslugi/przelewy/przelewy/ [13.06.2018r.]

Wiele instytucji finansowych na całym świecie już zaczęły stosować technologię blockchain w mniejszym lub większym zakresie. Szacuje się, że do 2022 roku może ona pomóc zaoszczędzić bankom 15-20 miliardów dolarów rocznie przez zmniejszenie kosztów regulacyjnych, rozliczeniowych i transgranicznych[89]. Powstał projekt mający na celu stworzenia cyfrowej waluty dla instytucji finansowych, który został wspólnie zapoczątkowany przez Deutsche Bank, UBS, Santander i nowojorski Mellon, w celu tańszego, bezpieczniejszego, bardziej przerzystego i szybszego rozliczania transakcji.[90] Innym przykładem udanego zastosowania technologii łańcucha bloków jest Ripple, który pomaga bankom w obsłudze płatności międzynarodowych. Jest to system rozliczeń działający w czasie rzeczywistym, który obsługuje wymiany walut i przekazy pieniężne[91]. Ripple to także kryptowaluta, z której pomocą wykonywane są transakcje, aktualnie będąca trzecią największą po Bitcoinie i Ethereum. Polskim akcentem jest w tej dziedzinie BIK – Biuro Informacji Kredytowej we współpracy z firmą Billon wdraża system obiegu dokumentów w postaci tzw. trwałego nośnika informacji, zdefiniowanego przez szereg dyrektyw unijnych, w tym RODO, opartego o blockchain[92]. Ostatnim z kolei przykładem jest startup R3 CEV. Jest to konsorcjum, które zrzesza ponad 100 banków, a także tysiące partnerów i regulatorów z całego świata. Głównym jego celem jest stworzenie platformy i komercyjnych aplikacji z wykorzystaniem technologii blockchain, które to staną się podwaliną dla nowego systemu rynków finansowych.[93]

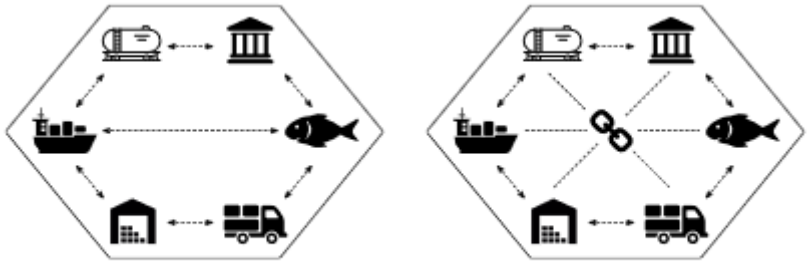
Korzyści płynące z technologii łańcucha bloków dla sektora bankowego to:

- Zmniejszone koszty,
- Krótszy czas rozliczenia transakcji,
- Łatwiejszy nadzór,
- Zwiększone bezpieczeństwo i lepsza jakość danych[94]

[89] Botsman R. (2017): *How Blockchain is Redefining Trust.* WIRED. Dostęp: https://www.wired.com/story/how-the-blockchain-is-redefining-trust/?mbid=GuidesLearnMore [13.06.2018r.]
[90] Tania H. (2018): *Implementing blockchain in business*. Dostęp: https://rubygarage.org/blog/implementing-blockchain-in-business [13.06.2018r.]
[91] Wüst K., Gervais A. (2017): *Do you need a Blockchain?* ETH Zürich, Zurych. s. 5. Dostęp: https://eprint.iacr.org/2017/375.pdf [13.06.2018r.]
[92] Stahl A. (2018): *Unikalna na światową skalę, pro-kliencka implementacja technologii blockchain w obszarze finansów*. Biuro Informacji Kredytowej. Dostęp: https://media.bik.pl/informacje-prasowe/390581/bik-i-billon-unikalna-na-swiatowa-skale-pro-kliencka-implementacja-tec [13.06.2018r.]
[93] Tania H. (2018): *Implementing blockchain in business*. Dostęp: https://rubygarage.org/blog/implementing-blockchain-in-business [13.06.2018r.]
[94] Territt H., Obie S., Ahern C. (2017): *Blockchain for Business*. Jones Day, Nowy Jork. s. 2. Dostęp: http://www.jonesday.com/files/upload/Blockchain%20for%20Business%20White%20Paper2.pdf [13.06.2018r.]

2.3. Łańcuchy dostaw

Zarządzanie łańcuchem dostaw (supply chain management – SCM) jest po bankowości i finansach najczęściej wymienianą sferą, która może skorzystać na zaadoptowaniu blockchaina. Możliwości jakie blockchain oferuje w kwestii działania łańcuchów dostaw są bardzo szerokie. Technologia ta pozwala na bezpieczne i przejrzyste śledzenie całej historii dóbr, przez cały proces ich produkcji, aż do sprzedaży - w tym wszelkich użytych komponentów dostarczonych przez inne firmy[95]. Blockchain jest tutaj wykorzystywany do rejestrowania rodzaju, ilości i przepływu towarów, śledzenia zamówień, rachunków, informacji o wysyłce, certyfikatów i ewidencji fizycznych właściwości produktów, jak również przypisywania im numerów seryjnych, kodów kreskowych lub tagów RFID[96]. Każda firma będąca elementem łańcucha dostaw ma przez to dostęp do zawsze aktualnego statusu dotyczących jej produktów i związanych z nimi procesów. Ta wiedza może pomóc w dalszym obniżeniu kosztów produkcji, optymalizacji tras i poprawieniu jakości samych produktów. Niektóre przedsiębiorstwa, jak Provevance[97], idą nawet o krok dalej i monitorują, poza pochodzeniem, warunki, w jakich towary (szczególnie te łatwo psujące się) są składowane w trakcie transportu, dzięki czemu zarówno firma i jak i konsumenci końcowi mają możliwość wglądu w szczegółowe informacje na temat stanu produktu[98].



Rys. 14. Porównanie tradycyjnego SCM do napędzanego przez blockchain.

Źródło: Wüst K., Gervais A. (2017): Do you need a Blockchain? ETH Zürich, Zurych. s. 4. Dostęp: https://eprint.iacr.org/2017/375.pdf [13.06.2018r.]

[95] Wüst K., Gervais A. (2017): *Do you need a Blockchain?* ETH Zürich, Zurych. s. 4. Dostęp: https://eprint.iacr.org/2017/375.pdf [13.06.2018r.]
[96] Territt H., Obie S., Ahern C. (2017): *Blockchain for Business*. Jones Day, Nowy Jork. s. 3. Dostęp: http://www.jonesday.com/files/upload/Blockchain%20for%20Business%20White%20Paper2.pdf [13.06.2018r.]
[97] Tania H. (2018): *Implementing blockchain in business.* Dostęp: https://rubygarage.org/blog/implementing-blockchain-in-business [13.06.2018r.]
[98] Lisk Foundation (2018): *Blockchain in Banking*. Dostęp: https://lisk.io/academy/blockchain-basics/use-cases/blockchain-in-banking [13.06.2018r.]

Istnieje wiele dużych projektów, które starają się udoskonalić mechanizm działania łańcuchów dostaw z wykorzystaniem blockchaina, kilka z nich to:

1. **Everledger** – w pełni działająca platforma, która wykorzystuje technologię łańcucha bloków do rejestrowania diamentów, a dokładniej ich właściwości fizycznych, pochodzenia, obróbki i historii sprzedaży[99]. Pozwala to na natychmiastową weryfikację pod względem autentyczności każdego z ponad 3 milionów zapisanych w blockchainie kamieni szlachetnych, będących dobrami o pokaźnej wartości, a przez to wyeliminowanie ryzyka oszustwa czy wykrycie próby sprzedaży skradzionego lub „krwawego" diamentu[100].
2. **WAVE** – firma zapewniająca znaczące wsparcie logistyczne umożliwiając bezpośrednią wymianę dokumentów pomiędzy członkami łańcucha dostaw w ramach zdecentralizowanej sieci opartej o blockchain. Dzięki pełnej przejrzystości i bezsprzecznemu potwierdzaniu własności dokumentów, eliminuje wszelkie spory, próby fałszerstwa i zbędne ryzyko.[101]
3. **Waltonchain** – jeden z najbardziej ambitnych projektów w zakresie SCM, który za swój cel postawił sobie opracowanie całkowicie nowego ekosystemu nazwanego VIoT (Value Internet of Things), który ma łączyć świat fizyczny z cyfrowym przy użyciu kombinacji blockchaina i technologii RFID. Rozwiązanie to ma stworzyć nowy model biznesowy dla firm będących elementami łańcucha dostaw, oparty o bezpieczeństwo, wiarygodność, identyfikowalność i pełną przejrzystość współdzielonych informacji. Blockchain WTC wykorzystuje do transakcji własną kryptowalutę i system trzech typów węzłów, co ma zapewnić pełną decentralizację i stabilność sieci. Waltonchain jest rozwijany we współpracy z wieloma czołowymi chińskimi producentami, projekt jest podzielony na cztery fazy, z których ostatnia ma się zakończyć w 2020 roku. [102]
4. **Modum** - kolejne rozwiązanie w zakresie zarządzania łańcuchem dostaw, zaprojektowane specjalnie dla przemysłu farmaceutycznego. Łączy ono czujniki IoT z blockchainem w celu zapewnienia integralności danych w ramach transakcji

[99] Crosby M., Pattanayak P., Verma S., Kalyanaraman V. (2015): *Blockchain Technology: Beyond Bitcoin*. Uniwersytet Kalifornijski, Berkeley. s. 14-15. Dostęp: http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf [13.06.2018r.]
[100] Everledger Limited (2018). Dostęp: https://diamonds.everledger.io/ [13.06.2018r.]
[101] Tania H. (2018): *Implementing blockchain in business*. Dostęp: https://rubygarage.org/blog/implementing-blockchain-in-business [13.06.2018]
[102] Khatwani S. (2018): *Top Supply Chain Management Cryptocurrency Projects*. Dostęp: https://coinsutra.com/supply-chain-management-cryptocurrency-blockchain-projects/ [13.06.2018r.]

dotyczących sprzedaży leków. Może to w ogromnym stopniu wyeliminować problemy związane z umowami, bezpieczeństwem i kontrolą, które są bardzo potrzebne w przypadku produktów farmaceutycznych. Czujniki wykorzystywane przez Modum rejestrują warunki środowiskowe, którym towary są poddawane podczas transportu. Kiedy towar zmienia właściciela, dane z czujników są weryfikowane na podstawie wcześniej ustalonych warunków z wykorzystaniem inteligentnego kontraktu. Smart contract zarządza takimi działaniami jak: powiadomienia nadawcy i odbiorcy, płatność i wydanie towaru.[103]

Korzyści płynące z technologii blockchain dla zarządzania łańcuchem dostaw i przemysłu detalicznego:

- Przejrzystość w logistyce, możliwość przechowywania i śledzenia wszystkich danych,
- Dowód wytworzenia i odsprzedaży produktu na określonych warunkach, a przez to łatwiejsze rozstrzyganie ewentualnych sporów,
- Automatyzacja części procesów biznesowych,
- Usprawnione śledzenie nawyków zakupowych[104]

2.4. Administracja i usługi publiczne

Rządy mogą być siłą napędową w popularyzacji technologii blockchain i czerpaniu z niej korzyści lub wręcz przeciwnie, ogromną przeszkodą na tej drodze. Zaadoptowanie jej w administracji i usługach publicznych może przyczynić się do ograniczenia biurokracji, korupcji, kosztów i skrócenia czasu, prowadząc do zwiększenia wydajności i przejrzystości na wielu szczeblach[105]. Niektóre państwa już dostrzegły potencjał blockchaina w tych sferach i opracowują, zazwyczaj wspólnie z prywatnymi firmami, odpowiednie rozwiązania. Chiny dodały blockchain jako priorytet do Trzynastego Pięcioletniego Narodowego Planu Informatyzacji w 2016 roku - dowód determinacji w dążeniu do zastosowania tej technologii

[103] Khatwani S. (2018): *Top Supply Chain Management Cryptocurrency Projects*. Dostęp: https://coinsutra.com/supply-chain-management-cryptocurrency-blockchain-projects/ [15.06.2018r.]
[104] Tania H. (2018): *Implementing blockchain in business*. Dostęp: https://rubygarage.org/blog/implementing-blockchain-in-business [15.06.2018r.]
[105] Lisk Foundation (2018): *Decentralized Government*. Dostęp https://lisk.io/academy/blockchain-basics/use-cases/decentralization-in-governments [15.06.2018r.]

do potencjalnego przyspieszenia rozwoju kraju. Innym przykładem jest Dubaj, miasto ogłosiło, także w 2016 r., projekt o nazwie Smart Dubai. Ma on na celu budowę systemu rządowego opartego o blockchain, który zapewni początkowo zdigitalizowany obieg dokumentów, w tym rejestru nieruchomości, dokumentacji zdrowotnej, rejestracji działalności gospodarczej, licencji, praw własności i wniosków wizowych – ponad 100 milionów dokumentów rocznie[106]. Warto też wspomnieć tutaj o rządzie Estonii, który jest niejako prekursorem zastosowania łańcucha bloków i infrastrukturze publicznej. Od 2012 roku blockchain jest integralną częścią krajowego projektu cyfryzacji administracji i usług publicznych znanego pod nazwą e-Estonia. Blockchain jest wykorzystywany w systemach opieki zdrowotnej, sądownictwa, podatkowych, głosowania i związanych z działalnością gospodarczą, przy czym planuje się rozszerzenie jego zastosowania na inne dziedziny[107].

Raport IBM wyróżnia w sumie aż osiem obszarów rządowych, w których zastosowanie blockchaina może przynieść znaczącą poprawę funkcjonowania[108]:

1. Zarządzanie tożsamością (cyfrowa tożsamość)[109]
2. Gospodarowanie zasobami,
3. Zarządzanie własnością,
4. System głosowania,
5. Usługi finansowe (podatki[110]),
6. Zapewnienia zgodności z przepisami,
7. Obsługa dokumentów i informacji,
8. Usługi publiczne (służba zdrowia, edukacja).

Podsumowanie niektórych z korzyści jakie niesie ze sobą zaadoptowanie technologii blockchain w strukturach usług i administracji publicznej:

- Brak konieczności angażowania instytucji pozarządowych
- Wyeliminowanie zjawiska korupcji na szczeblu administracyjnym

[106] Weadt H. (2017): *Blockchain Use Cases*. Dostęp: http://holgerwaedt.com/blockchain-use-cases/ [15.06.2018r.]
[107] Piech K, Zyga P. (2018): Wykorzystanie blockchain przez rząd estoński. Uczelnia Łazarskiego, Warszawa. Dostęp: https://www.lazarski.pl/pl/wydzialy-i-jednostki/instytuty/wydzial-ekonomii-i-zarzadzania/centrum-technologii-blockchain/wykorzystanie-blockchain-przez-rzad-estonski/ [15.06.2018r.]
[108] IBM Institute for Business Value. Dostęp: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03801USEN& [15.06.2018r.]
[109] Kosba A., Miller A., Shi E., Wen Z., Papamanthou C. (2015): *Decentralizing Privacy: Using Blockchain to Protect Personal Data.* Wydawnictwo IEEE, Piscataway Township. s. 2. Dostęp: http://ieeexplore.ieee.org/document/7163223/ [15.06.2018r.]
[110] Frankowski E., Barański P. (2017): *Technologia Blockchain i jej potencjał w podatkach.* Deloitte, Katowice. s. 13-16. Dostęp: https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_Blockchain-technology-and-its-potential-in-taxes-2017-PL.PDF [15.06.2018r.]

- Zabezpieczenie zasobów i zapewnienie prywatności danych,
- Umożliwienie przejrzystych, szybkich i opłacalnych procedur transakcyjnych
- Uproszczenie i upsrawnienie działań związanych z biurokracją.[111]

2.5. Nieruchomości

Słabości związane z nieruchomościami obejmują imponującą ilość formalności, występowanie pomyłek w ewidencji publicznej, stosowanie niejasnych praktyk, a także próby nadużyć i oszustw - ogólny brak przejrzystości. Blockchain posiada mechanizmy, które mogą skutecznie przeciwdziałać tym zjawiskom. Przyjazna zarówno dla nabywców jak i właścicieli możliwa jest także automatyzacja istotnych procesów z wykorzystaniem inteligentnych kontraktów i to nie tylko dotyczących sprzedaży, ale także wynajmu nieruchomości[112]. Funkcjonuje i rozwija się już kilka projektów, które adresują te właśnie kwestie, dwa najciekawsze z nich to:

1. **velox.RE** – projekt pilotażowy stworzony w Chicago, który ma na celu rozwój sektora nieruchomości poprzez poprawę przejrzystości wszystkich dokumentów, danych i transakcji. W oparciu o technologię blockchain, velox.RE proponuje rozwiązanie umożliwiające zmniejszenie liczby papierowych dokumentów, przyspieszenie transakcji i uczynienie ich tańszymi, a także umożliwienie zdigitalizowanej rejestracji własności i wymiany danych dotyczących nieruchomości.
2. **Ubitquity** - przedsiębiorstwo wspólnie z brazylijskim rządem opracowało rozwiązanie wykorzystujące blockchain Bitcoina do stworzenia zdecentralizowanego systemu ewidencji gruntów i nieruchomości. Projekt ma na celu zwiększenie bezpieczeństwa i skuteczności działania agencji nieruchomości i ewidencji nieruchomości poprzez skrócenie czasu dochodzenia prawa własności, zwiększenie zaufania i przejrzystości w sektorze. Firmy mogą bezpiecznie rejestrować i śledzić zapisy dotyczące swoich nieruchomości w zdecentralizowanym rejestrze, a także dzielić się tymi informacjami z wybranymi partnerami w obrębie sieci.[113]

[111] Tania H. (2018): *Implementing blockchain in business*. Dostęp: https://rubygarage.org/blog/implementing-blockchain-in-business [15.06.2018r.]
[112] Lisk Foundation (2018): *Blockchain in Real Estate*. Dostęp: https://lisk.io/academy/blockchain-basics/use-cases/blockchain-real-estate [15.06.2018r.]
[113] Tania H. (2018): *Implementing blockchain in business*. Dostęp: https://rubygarage.org/blog/implementing-blockchain-in-business [15.06.2018r.]

Możliwości jakie oferuje technologia blockchain dla tej branży:

- Większa przejrzystość wszystkich rejestrów nieruchomości, a także umów i transakcji z nimi związanych,
- Brak pośredników, a tym samym obniżenie kosztów,
- Ograniczenie formalności i przyspieszenie procesów,
- Zapobieganie nadużyciom finansowym.[114]

2.6. Energetyka

Duże przedsiębiorstwa energetyczne zaczynają dostrzegać wartość blockchaina, szczególnie w zakresie jego niezmienności i redundancji i widzą perspektywę większej elastyczności, poprawy wydajności i zwiększonego bezpieczeństwa danych, którą może przynieść temu sektorowi. Czynione są poważne inwestycje w tym kierunku, tylko w samym 2017 roku w start-upy opracowujące rozwiązania dla branży energetycznej zainwestowano w sumie ponad 320 milionów dolarów[115]. Główne zakresy jakie są eksplorowane to zdecentralizowana wymiana energii, automatyczne reagowanie na zwiększony popyt energii, elastyczność sieci, zarządzanie dystrybucją, handel energią w modelu p2p i ładowanie pojazdów elektrycznych. Dwa z wielu interesujących przedsięwzięć to[116]:

1. **SolarCoin** – założenie tego projektu jest takie, że wartość użytkowa energii elektrycznej może być stabilniejszym magazynem majątku w przyszłości niż chociażby złoto. SolarCoin działa jako kryptowaluta, w której tokeny tworzone są po zweryfikowaniu wygenerowania odpowiedniej ilości energii pochodzącej ze źródeł odnawialnych. Każdy token – 1 SLR, jest w teorii wymienialny na 1kWh energii możliwej zarówno do zużycia jak i odsprzedaży.
2. **PowerLedger** – australijski start-up, który zamierza zbudować opartą o blockchain platformę p2p, która ma umożliwić prosumentom (jednostkom będącym jednocześnie

[114] Doubleday K. (2018): *Blockchain for 2018 and Beyond: A (growing) list of blockchain use cases.* Medium. Dostęp: https://medium.com/fluree/blockchain-for-2018-and-beyond-a-growing-list-of-blockchain-use-cases-37db7c19fb99 [15.06.2018r.]
[115] Lacey S/ (2018): *Energy Blockchain Startups Raised $324 Million in the Last Year. Where's the Money Going?* Grand Tech Media. Dostęp: https://www.greentechmedia.com/articles/read/energy-blockchain-startups-raised-324-million-since-2017 [15.06.2018r.]
[116] Mulligan S. (2018): *Energy, Blockchain, And The Role Of Tokens*. Dostep: https://www.investinblockchain.com/energy-blockchain-tokens/ [15.06.2018r.]

producentem i konsumentem – np. gospodarstwa domowe korzystające z paneli słonecznych) zarabianie poprzez odsprzedaż wytworzonego nadmiaru energii elektrycznej. Platforma ma nawet na celu umożliwienie wymiany międzynarodowej poprzez wykorzystanie dwóch tokenów. Pierwszy - POWR, który sfinansuje rozwój platformy i będzie regulować barierę wejścia nia nią, będąc jednocześnie zbywalnym na całym świecie. Drugi został nazwany Sparkz i będzie wymienialny na dostępną lokalnie energię.

Wartość dodana blockchaina zastosowanego w branży energetycznej to m.in.:

- Zapewnienie decentralizacji i bezpieczeństwa systemów,
- Eliminacja pośredników i umożliwienie współdzielenia energii,
- Wsparcie alternatywnych źródła energii.[117]

2.7. Inne

Blockchain może mieć zastosowanie w wielu innych sferach, zazwyczaj oferując bezpieczniejsze, szybsze i tańsze niż obecnie stosowane rozwiązania. Poniżej znajduje się lista zaledwie kilku wybranych projektów, o których warto wspomnieć.

- IPFS[118] i SAFE Network[119] - mają na celu zbudowanie globalnych zdecentralizowanych sieci opartych o alternatywy protokołu http korzystających z p2p, a tym samym potencjalnie mogłyby stać się nowym internetem.
- Storj[120] i Sia[121] – platformy oferujące szyfrowane przechowywanie plików w zdecentralizowanej chmurze w cenach o ok. 90% niższych niż czołowi dostawcy usług przechowywania w chmurze jak Amazon, Google, Microsoft czy Dropbox.
- Matrix[122] – zdecentralizowana sieć komunikacji z szyfrowaniem end-to-end.
- Golem[123] – projekt polskiego zespołu, superkomputer wykorzystujący do działania moc obliczeniową globalnej zdecentralizowanej sieci.

[117] Tania H. (2018): *Implementing blockchain in business*. Dostęp: https://rubygarage.org/blog/implementing-blockchain-in-business [15.06.2018r.]
[118] Dostęp: https://ipfs.io/ [15.06.2018r.]
[119] Dostep: https://maidsafe.net/ [15.06.2018r.]
[120] Dostęp: https://storj.io/ [15.06.2018r.]
[121] Dostęp: https://sia.tech/ [15.06.2018r.]
[122] Dostęp: https://matrix.org/ [15.06.2018r.]
[123] Dostęp: https://golem.network/ [15.06.2018r.]

- Status[124] – mobilny system operacyjny przekształcający smartfona w węzeł kliencki łączący się z Ethereum. Umożliwia bezpieczne przechowywanie tokenów i przeprowadzanie transakcji, dostęp do wszystkich DApps, a także prywatnej platformy komunikacyjnej opartej o protokół Whisper będący częścią sieci Ethereum.
- Bounties[125] – platforma umożliwiająca całkowicie bezpłatne zamieszczanie zleceń do wykonania.
- Steem[126] – zdecentralizowana sieć społecznościowa, w której użytkownicy tworzący wartościowe treści są nagradzani tokenami mającymi realną wartość pieniężną.
- Brave[127] – przeglądarka natywnie blokująca wszelkie reklamy i trackery. Posiada wbudowany system płatności oparty o kryptowalutę BAT (Basic Attention Token), który umożliwia bezpośrednie wspieranie wybranych zweryfikowanych twórców i wydawców ze stale rosnącej listy, a tym samym próbuje stworzyć nowy model dystrybucji i monetyzacji treści.

[124] Dostęp: https://status.im/ [15.06.2018r.]
[125] Dostęp: https://bounties.network/ [15.06.2018r.]
[126] Dostęp: https://steem.io/ [15.06.2018r.]
[127] Dostęp: https://brave.com/ [15.06.2018r.]

ROZDZIAŁ III. IMPLEMENTACJA BLOCKCHAINA

Jako ostatnia część opisana zostanie autorska implementacja blockchaina. Opracowany został do tego celu demonstracyjny, ale w pełni funcjonalny, projekt kryptowaluty nazwanej Motus (z łacińskiego – ruch), a jej token MTS. Na początku przedstawione zostaną założenia i zarys technologiczny, a następnie kolejno zaprezentowany zostanie każdy z głównych komponentów składających się na całość implementacji.

3.1. Założenia i technologia

Idąc za przykładem niemal wszystkich projektów ze sfery blockchaina, a zarazem branżowej praktyki programistycznej, jako baza języka naturalnego został wykorzystany został język angielski. Natomiast w przeciwieństwie do standardowo używanych do implementacji blockchaina języków programowania jak C, C++, czy Golang, zastosowany został tutaj język Javascript, który pozwolił znaczne skrócenie kodu źródłowego a zarazem uczynienie go łatwiejszego do ogólnej analizy, a przy tym projekt nadal jest wieloplatformowy i możliwy do uruchomienia w we wszystkich środowiskach (Windows, Linux i MacOS) z użyciem Node.js w wersji co najmniej 6.x. Taka zmiana umożliwiła także na użycie z menadżera pakietów NPM (Node Package Manager) i skorzystanie z dobrodziejstw nieznacznej liczby gotowych bibliotek, które jeszcze bardziej przyspieszyły proces implementacji.

Nazwa	Wersja	Krótki opis funkcjonalności
body-parser	1.18.3	Middleware (pośrednik) przetwarzające sekcję body żądań HTTP.
chalk	2.4.1	Pozwala na kolorowanie treści wyświetlanych w terminalu.
elliptic	6.4.0	Zawiera gotowe zoptymalizowane implementacje algorytmów z zakresu kryptografii krzywych eliptycznych.
es6-error	4.0.2	Klasa, która przez jej rozszerzanie pozwala na proste tworzenie niestandardowych klas błędów.
express	4.16.2	Web framework do tworzenia aplikacji opartych o Node.js.
fs-extra	6.0.1	Rozszerza pólę metod do obsługi działań na plikach.

pug	2.0.0-rc.4	Silnik szablonów działający z frameworkiem Express.
ramda	0.25.0	Zapewnia możliwość programowania funkcyjnego udostępniając bogate API.
statuses	1.3.1	Umożliwia uproszczoną interakcję z kodami statusów HTTP.
superagent	3.5.2	Pozwala na wysyłanie żądań HTTP.
threads	0.10.0	Dodaje możliwość wykorzystania wielowątkowości.
timeago.js	3.0.2	Przetwarza znacznik czasowy na czytelną formę relatywnej daty.
yargs	11.0.0	Zawiera API dodające przejrzystą obsługę parametrów w linii poleceń.

Tabela 1. Wykaz bibliotek wykorzystanych w projekcie Motus.

Źródło: Opracowanie własne.

Wszystkie użyte biblioteki zostały sprawdzone pod względem bezpieczeństwa przez wbudowane w NPM narzędzie audytujące. Nie wykryto żadnych znanych podatności.

```
PS C:\Motus> npm audit

                       === npm audit security report ===

found 0 vulnerabilities
```

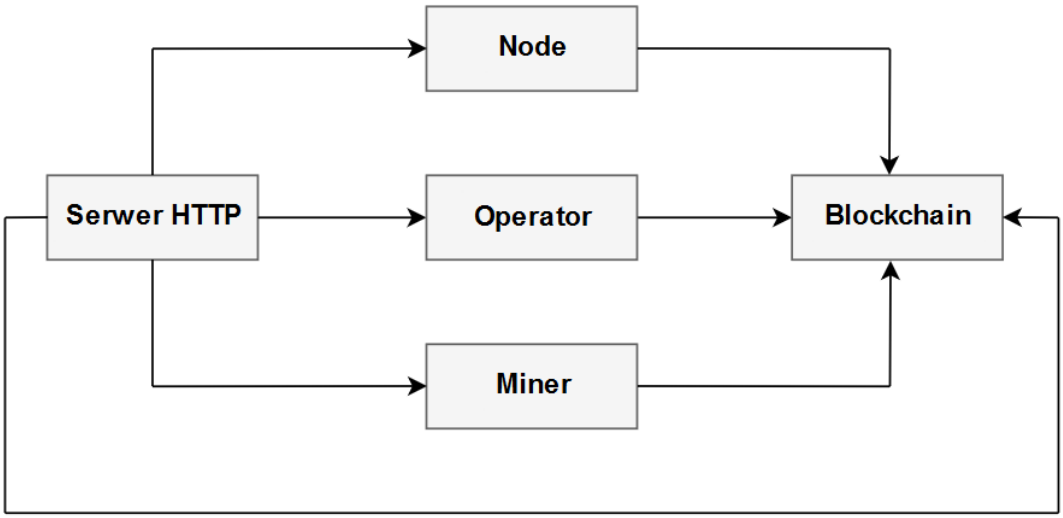
Rys. 15. Wynik audytu bezpieczeństwa bibliotek.

Źródło: Opracowanie własne.

Poza różnicą w wybranym języku programowania, znacząco różni się także ogólna architektura sieci Motus. Zwyczajowo do komunikacji w sieci p2p kryptowalut wykorzystywane są takie protokoły jak TCP, UDP i RCP. W tym przypadku jedynym używanym protokołem jest HTTP i służy on zarówno do komunikacji jak i interakcji z wszystkimi komponentami. Cała implementacja jest podzielona na pięć głównych komponentów:

- Serwer HTTP (API)
- Blockchain (łańcuch bloków, transakcje)
- Operator (zarządca portfeli)
- Node (węzeł sieci)

- Miner (górnik bloków)



Rys. 16. Schemat komunikacji między komponentami.

Źródło: Opracowanie własne.

3.2. Serwer HTTP

Serwer HTTP jest warstwą pośredniczącą wszystkich interakcji z czterema pozostałymi komponentami. Zapewnia interfejs REST API, obsługujący dane w formacie JSON, do zarządzania i pobierania informacji o blockchainie, portfelach, adresach, transakcjach, połączeniach z peerami (innymi węzłami) i umożliwia tworzenie bloków z użyciem minera. Serwer jest możliwy do uruchomienia z poziomu wiersza poleceń komendą node motus.js lub npm start. Dostępne są przy tym parametry umożliwiające konfigurację hosta (domyślnie localhost), portu (domyślnie 3000, w przypadku zajętego portu sprawdzane są kolejne do momentu znalezienie wolnego), lista peerów, z którymi ma się połączyć, nazwa node i poziom debugowania wątku wykorzystywanego przez miner. Poniżej została zawarta dokumentacja wszystkich funkcjonalności, jakie udostępnia API.

Metoda	URL	Opis
GET	/blockchain/blocks	Pobiera wszystkie bloki.
GET	/blockchain/blocks/{index}	Pobiera blok o określonym indeksie.
GET	/blockchain/blocks/{hash}	Pobiera blok o określonym hashu.
GET	/blockchain/blocks/latest	Pobiera najnowszy blok.
PUT	/blockchain/blocks/latest	Dodaje nowy blok (synchronizacja między węzłami).
GET	/blockchain/blocks/transactions/{transactionId}	Pobiera transakcję o określonym identyfikatorze.
GET	/blockchain/blocks/transactions/{transactionId} /confirmations	Pobiera liczbę potwierdzeń dla transakcji o określonym identyfikatorze.
GET	/blockchain/transactions	Pobiera wszystkie niezatwierdzone transakcje.
POST	/blockchain/transactions	Tworzy nową transakcję (synchronizacja między węzłami).
GET	/blockchain/transactions/unspent	Pobiera wszystkie niewykorzystane transakcje.

Tabela 2. Dokumentacja dostępnych metod API komponentu Blockchain.

Źródło: Opracowanie własne.

Metoda	URL	Dodatkowe parametry	Opis
GET	/operator/wallets	Brak	Pobiera wszystkie portele i zawarte w nich adresy.
POST	/operator/wallets	password – hasło portfela	Tworzy portfel z podanego hasła.
GET	/operator/wallets/{walletId}	Brak	Pobiera portfel o określonym identyfikatorze.
GET	/operator/wallets/{walletId} /addresses	Brak	Pobiera adresy portfela o określonym identyfikatorze.
POST	/operator/wallets/{walletId} /addresses	password – hasło portfela	Tworzy nowy adres w określonym portfelu.
POST	/operator/wallets/{walletId} /transactions	password – hasło portfela	Tworzy nową transakcję.

		fromAddress – adres źródłowy toAddress – adres docelowy amount – liczba tokenów	
GET	/operator/{addressId}/balance	Brak	Pobiera stan konta o określonym adresie.

Tabela 3. Dokumentacja dostępnych metod API komponentu Operator.

Źródło: Opracowanie własne.

Metoda	URL	Dodatkowe parametry	Opis
GET	/node/peers	Brak	Pobiera wszystkie peery połączone z tym nodem.
POST	/node/peers	peer – host:ip nowego peera	Dodaje nowego peera, z którym node tworzy połączenie (synchronizacja).

Tabela 4. Dokumentacja dostępnych metod API komponentu Node.

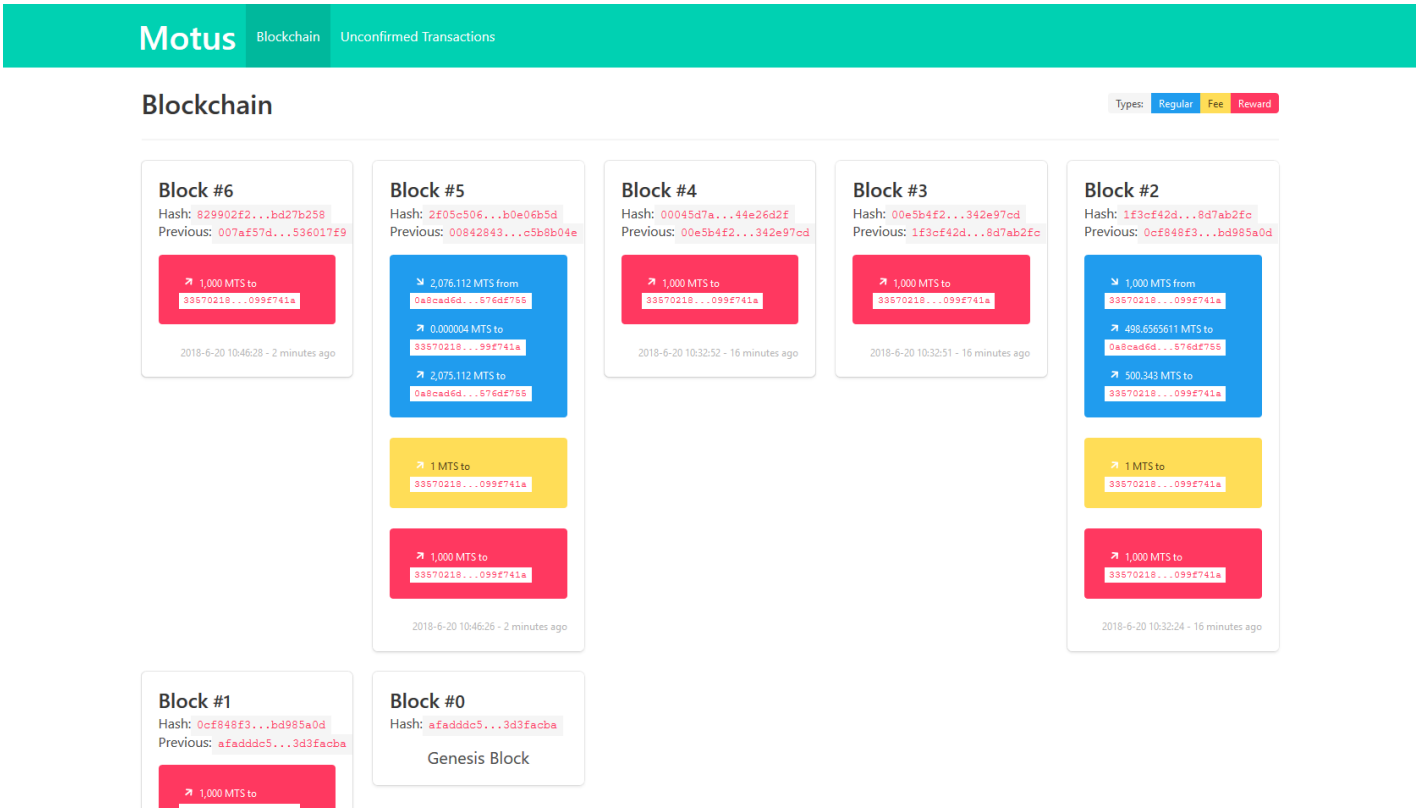
Źródło: Opracowanie własne.

Metoda	URL	Dodatkowe parametry	Opis
POST	/miner/mine	rewardAddress – adres, na który ma trafić nagroda za wykopany blok i ewentualne prowizje za transakcje	Tworzy i kopie nowy blok.

Tabela 5. Dokumentacja dostępnych metod API komponentu Miner.

Źródło: Opracowanie własne.

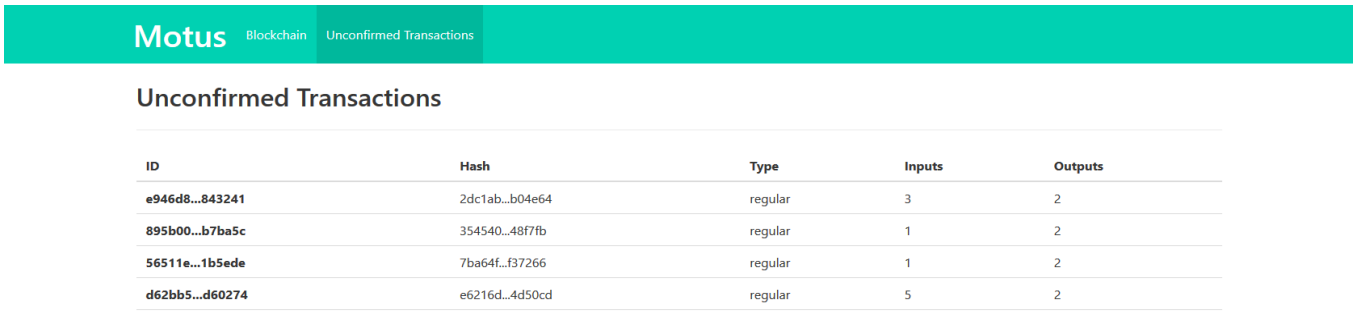
Pod ścieżką URL /blockchain, a także pod każdą inną, której nie obsługuje dostępne API (za pośrednictwem dodatkowej ścieżki typu wildcard i przekierowania), dostępny jest Blockchain Explorer.



Rys. 17. Blockchain explorer – lista bloków wraz z transakcjami.

Źródło: Opracowanie własne.

Można w nim prześledzić cały blockchain: wszystkie bloki posortowane od najnowszego aż do bloku genesis i zawarte w nich transakcje, a także sprawdzić listę transakcji, które czekają na zawarcie w bloku (mempool).



Rys. 18. Blockchain explorer - mempool.

Źródło: Opracowanie własne.

3.3. Blockchain

Komponent ten przetrzymuje w pamięci informacje podzielone na dwie części: listę bloków – blockchain w postaci listy powiązanej (linked list) i zbiór niepotwierdzonych transakcji list jako tablicę z hashowaniem (hash map). Są one po każdej zmianie i synchronizacji odkładane, w folderze o nazwie data, jako pliki w formacie JSON.

Blockchain posiada mechanizmy, które są odpowiedzialne za:

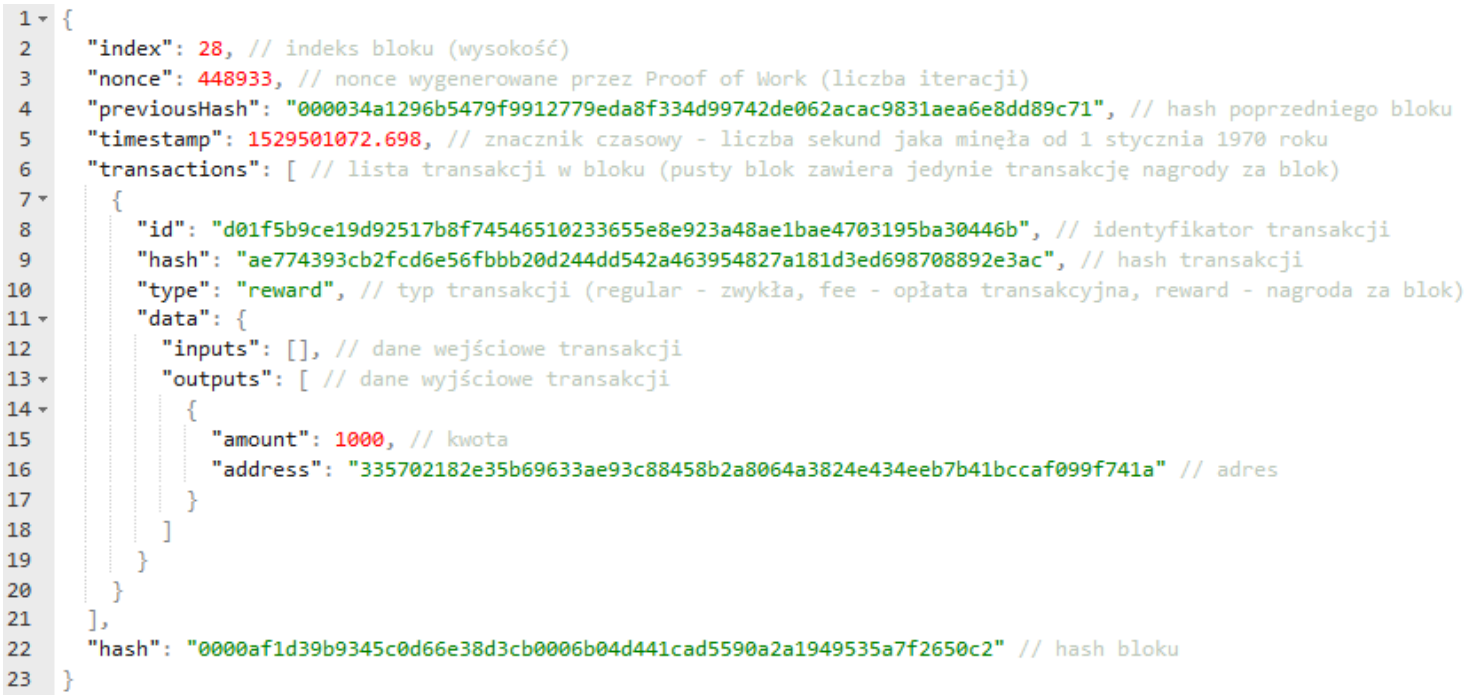
- Weryfikację dostarczonych bloków,
- Weryfikację dostarczonych transakcji,
- Synchronizację listy bloków,
- Synchronizację listy transakcji.

3.3.1. Blok

Każdy blok repezentuje grupę transakcji i zawiera informację - hash, który bezpośrednio łączy go z poprzednim blokiem (wyjątkiem jest wyłącznie blok 0 – genesis). Nowy blok zastaje dodany do blockchaina, jeśli pomyślnie przejdzie proces weryfikacji, w czasie którego sprawdzane jest czy:

1. Blok jest najnowszy (indeks jest równy indeksowi ostatniego zatwierdzonego bloku powiększonemu o jeden),
2. Poprzedni blok jest poprawny (hash poprzedniego bloku jest równy hashowi ostatniego zatwierdzonego bloku),
3. Hash jest poprawny (hash bloku zgadza się z wyliczonym hashem weryfikacyjnym),
4. Poziom trudności bloku związany z Proof of Work jest odpowiedni (trudność musi być mniejsza lub równa wymaganej trudności dla bloku o tym indeksie),
5. Wszystkie transakcje wewnątrz bloku są prawidłowe,
6. W zbiorze wszystkich transakcji nie występuje podwójne użycie (double-spending),
7. Suma transakcji wyjściowych jest równa sumie transakcji wejściowych powiększonej o nagrodę dla wytwórcy bloku,
8. Istnieje tylko i wyłącznie jedna transakcja z nagrodą za blok i maksymalnie jedna z sumą opłat transakcyjnych.

Nagroda za blok jest stała i została ustalona na 1000 MTS. Opłata transakcyjna także jest stała i wynosi 1 MTS – w przeciwieństwie do przykładowo Bitcoina, gdzie jest ona zależna od wielkości transakcji w bajtach. Po dodaniu nowego bloku z puli transakcji oczekujących usuwane są wszystkie zatwierdzone transakcje.



Rys. 19. Struktura bloku.

Źródło: Opracowanie własne.

3.3.2. Transakcja

Transakcja zawiera zestaw danych wejściowych i wyjściowych odzwierciedlających transfer tokenów pomiędzy właścicielem adresu źródłowego a adresu docelowego. Dane wejściowe zawierają stan konta danego adresu źródłowego i sygnaturę potwierdzającą użycie klucza prywatnego przypisanego do tego adresu. Dane wyjściowe zawierają adres docelowy transakcji, na który trafić mają tokeny i w razie konieczności, adres zwrotny, na który trafia różnica między liczbą tokenów wysłaną na adres docelowy a liczbą tokenów na adresie źródłowym – domyślnie jest to adres źródłowy, jednak nie musi nim być.

Aby transakcja została zweryfikowana i trafiła do puli transakcji możliwych do umieszczenia w bloku, musi spełniać następujące warunki:

1. Transakcja nie znajduje się jeszcze na liście transakcji,

2. Hash jest poprawny (hash transakcji zgadza się z wyliczonym hashem weryfikacyjnym),
3. Sygnatura zawarta w danych wejściowych jest poprawna (jest weryfikowana na podstawie klucza publicznego, który jest jednocześnie adresem),
4. Suma tokenów w danych wejściowych jest równa sumie tokenów w danych wyjściowych pomniejszonych o opłatę transakcyjną,
5. Transakcja nie znajduje się już w blockchainie,
6. Na adresie źródłowym znajduje się wystarczająco dużo tokenów do wykonania tej transakcji.

```
{
  "id": "cc12eb9c45df0f9cbfef578c2f593fda63550569e65d59b7fd2204f50c34d8a3", // identyfikator transakcji
  "hash": "b11c2babf3d1f6b3a512ec9875acf1444bffa2716f5ee2b798af4cf1485362f6", // hash transakcji
  "type": "regular", // typ transakcji
  "data": {
    "inputs": [ // dane wejściowe transakcji
      {
        "transaction": "23ce019f5128f707b91c67e96018628cfe1c866761ecb4c6c40f6478d4c1e23d", // hash poprzedniej transakcji
        "index": 1, // indeks transakcji
        "amount": 2559.36867, // stan konta adresu źródłowego
        "address": "0a8cad6dbeb558f373b5ee9a7828b97f76438bf8d380d9355a2a3e06576df755", // adres źródłowy
        "signature": "724c58f51c0ead7db3510dc6b213d53e82350ce60925eff636a9fe3d755e7fef1c48ec783d8d8d6dfb748cd60039ba1cd8b6
          cf9ee4a2a8dfa4c21549a1a7e001" // sygnatura wygenerowana z klucza prywatnego adresu źródłowego i hasha transakcji
      }
    ],
    "outputs": [ // dane wyjściowe transakcji
      {
        "amount": 149.40320004, // kwota transakcji
        "address": "335702182e35b69633ae93c88458b2a8064a3824e434eeb7b41bccaf099f741a" // adres docelowy
      },
      {
        "amount": 2408.9654699599996, // kwota zwrotna
        "address": "0a8cad6dbeb558f373b5ee9a7828b97f76438bf8d380d9355a2a3e06576df755" // adres zwrotny
      }
    ]
  }
}
```

Rys. 20. Struktura transakcji.

Źródło: Opracowanie własne.

3.4. Operator

Operator jako komponent ma za zadanie obsługę portfeli i adresów oraz tworzenie transakcji, które zostały omówione przy okazji komponentu Blockchain. Wygenerowane adresy i portfele, podobnie jak łańcuch bloków i zbiór niepotwierdzonych transakcji, są składowane w folderze data jako plik JSON. Jednakże w przeciwieństwie do nich, Operator

posiada jedynie własną listę adresów i portfeli, co oznacza, że nie są one zsynchronizowane pomiędzy węzłami sieci.

3.4.1. Portfel

Każdy portfel oznaczony unikalnym losowym identyfikatorem. Portfel generuje się używając hasła (ciągu znaków składającego się z co najmniej pięciu słów), które jest następnie hashowane z użyciem funkcji SHA-256. Dodatkowo tworzony jest 1024 bajtowy sekret, który jest później używany do generowania par kluczy. Powstaje on przez wykorzystanie algorytmu mieszającego PBKDF2 przyjmującego jako argumenty hash hasła, sól (salt – 64 bajtowy ciąg znaków) i używającego funkcji SHA-512 z 10 tys. cykli. To wszystko sprawia, że sekret portfela jest statystycznie niemożliwy do złamania używając metody brute-force. Portfel używany jest do przechowywania kluczy publicznych i prywatnych.

```
{
  "id": "f00383766587874a153d07fbbceb9ac820f5e3f05b7dd6dff23ca31a80b7d955", // identyfikator portfela
  "passwordHash": "5ba9151d1c24e03b25bb3b92dab736790159d1489160e310e72b001424be8e2c", // hash hasła
  "secret": "1ed852cf1da6cdfce274b541a57179...34d6403ede562f61333f19a4db7fe05", // sekret - skrócony z 1024 do 64 bajtów
  "keyPairs": [
    {
      "index": 1, // indeks pary kluczy
      "secretKey": "1ed852cf1da6cdfce274b541a57179..0381ac98b1ad5a026934d6403ede562f", // klucz prywatny - skrócony z 1024
        do 64 bajtów
      "publicKey": "335702182e35b69633ae93c88458b2a8064a3824e434eeb7b41bccaf099f741a" // klucz publiczny - adres
    }
  ]
},
```

Rys. 21. Struktura portfela z jednym adresem.

Źródło: Opracowanie własne.

3.4.2. Adres

Pary kluczy: publiczny (64 bajtowy - będący jednocześnie adresem) i prywatny (1024 bajtowy) generowane są przy pomocy algorytmu EdDSA. Pierwszy adres tworzony jest zawsze na podstawie zawartego w porfelu sekretu, który powstał przez kolejne hashowanie hasła. Pozostałe adresy tworzone są w sposób deterministyczny, co oznacza, że każdy kolejny adres generowany jest na podstawie poprzedniego.

3.5. Node

Node zawiera listę połączonych z nim peerów i pośredniczy w wymianie wszystkich danych między węzłami, w tym pobiera (przy starcie), otrzymuje i zarządza dodaniem nowych:

- peerów,
- bloków,
- transakcji,

Węzeł retransmituje także każdą otrzymaną informację do wszystkich połączonych z nim peerów, chyba że nic z nią nie robi, tj. nowy peer znajduje się już na liście, transakcja jest już w puli oczekujących lub blok jest już częścią blockchaina.

3.6. Miner

Górnik otrzymuje pólę oczekujących transakcji i kopie nowy blok zawierający zestaw wybranych z nich przez uzyskanie dowodu pracy (Proof of Work). Proces tworzenia nowego bloku jest następujący:

1. Pobierany jest ostatni blok, inkrementowany jest jego indeks i zapisywany jest hash poprzedniego bloku,
2. Z listy niepotwierdzonych transakcji wybierane są kolejno transakcje kandydackie, czyli takie które nie znajdują się jeszcze w blockchainie, nie zostały jeszcze wybrane i są zweryfikowane pod względem poprawności (brak podwójnego zużycia),
3. Z puli transakcji kandydackich wybierane jest pierwsze 3 tys. pozycji (limit transakcji jaką może zawierać jeden blok – wynika z konfiguracji blockchaina Motus),
4. Dodawana jest nowa transakcja zawierającą sumę opłat transakcyjnych (1 MTS za każdą transakację), która trafia na adres należący do minera,
5. Dodawana jest nowa transakcja dodająca na adres górnika nagrodę za wykopanie bloku (1000 MTS),
6. Przez wykonanie odpowiedniej ilości obliczeń matematycznych (wyliczania hashy kryptograficznych) uzyskiwany jest Proof of Work i ostatecznie ustalany jest hash bloku.

3.6.1. Proof of Work

Zaimplementowany mechanizm konsensusu Proof of Work polega na obliczaniu wartości przez konwersję pierwszych 14 znaków hasha bloku na liczbę całkowitą z heksadecymalnej i zwiększaniu nonce w celu manipulacji hashem, aż wyliczona wartość będzie mniejsza lub równa niż trudność dla bloku o tym indeksie. Hash bloku jest tworzony z użyciem funkcji SHA-256, której parametrem jest skonkatenowany ciąg znaków zawierający następujące dane z bloku:

- indeks,
- poprzedni hash,
- timestamp (znacznik czasu),
- dane transakcji,
- nonce.

```
do {
      block.timestamp = new Date().getTime() / 1000;
      block.nonce++;
      block.hash = block.toHash();

      blockDifficulty = block.getDifficulty();
  } while (blockDifficulty >= difficulty);
```

Rys. 22. Implementacja pętli generującej dowód pracy.

Źródło: Opracowanie własne.

Wartość trudności, która musi zostać osiągnięta dla bloku o danym indeksie, czyli zmiennej **difficulty** w powyższej implementacji, jest wyliczana przez następują metodę:

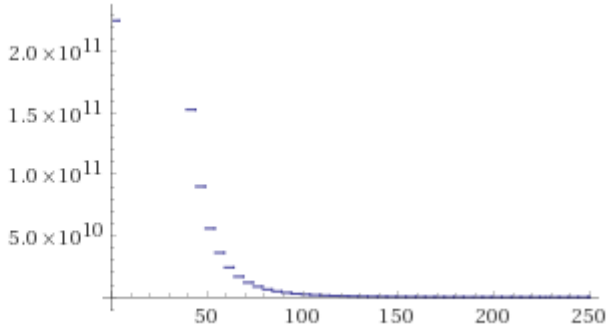
```
getDifficulty: (blocks, index) => {
    const BASE_DIFFICULTY = Number.MAX_SAFE_INTEGER;
    const EVERY_X_BLOCKS = 5;
    const POW_CURVE = 5;

    return Math.max(
        Math.floor(
            BASE_DIFFICULTY / Math.pow(
                Math.floor(((index || blocks.length) + 1) / EVERY_X_BLOCKS) + 1,
                POW_CURVE)
        ),
    0);
}
```

Rys. 23. Implementacja metody określającej trudność blokową dla dowodu pracy.

Źródło: Opracowanie własne.

Number.MAX_SAFE_INTEGER jest stałą równą 2^{53}**-1**, **EVERY_X_BLOCKS** określa co ile bloków zmieniana jest trudność, natomiast **POW_CURVE** wpływa na nachylenie krzywej. Powyższa implementacja odpowiada ona funkcji matematycznej o następującym wzorze i wykresie, gdzie **y** jest wartością trudności, a **x** indeksem bloku:

$$y = \max\left(\left\lfloor \frac{2^{53}-1}{\left(\left\lfloor \frac{x+1}{5} \right\rfloor + 1\right)^5} \right\rfloor, 0\right)$$



Rys. 24. Wzór i wykres funkcji określającej trudność blokową.

Źródło: https://www.wolframalpha.com/ [20.06.2018]

Początkowo bloki generowane są bardzo szybko ze względu na duże wartości trudności blokowej, czas uzyskiwania Proof of Work, a tym samym tworzenia nowego bloku, jest często krótszy niż 1 sekunda. Po około 100 blokach odstęp czasowy między kolejnymi blokami wynosi średnio 60 sekund, co przy limicie 3 tys. transakcji na blok daje blockchainowi Motus teoretyczną wydajność na poziomie 50 TPS (transakcji na sekundę) – dla Bitcoina wynosi ona 7 TSP, dla Ethereum 15 TPS.

ZAKOŃCZENIE

Jak się okazuje i co ilustruje ostatni rozdział, po przyswojeniu stosownej ilości informacji na temat łańcucha blokowego i zasad jego działania, z powodzeniem można zaprojektować i zaimplementować w pełni funkcjonalny projekt, który jest jego integralną częścią. To wszystko przy wykorzystaniu powszechnie znanych wielu programistom technologii, osiągając przy tym rezultaty, które w pewnych kwestiach przewyższają największe istniejące rozwiązania oparte o blockchain – tutaj w zakresie liczby transakcji na sekundę.

Technologia łańcucha blokowego rozwija się w niebywałym tempie, ale nadal jest właściwie na początku drogi do adaptacji w powszechnie wykorzystywanych rozwiązaniach. Czas pokaże, blockchain może się okazać się jednym z najważniejszych wynalazków od momentu powstania internetu, który całkowicie zrewolucjonizował światową wymianę informacji. W związku z rosnącą liczbą projektów z nim związanych w tak wielu różnych dziedzinach, a także zainteresowaniem nie tylko ze strony banków i dużych korporacji, ale też rządów państw, dość oczywistym wnioskiem wydaje się stwierdzenie, że technologia ta nie zniknie, a wręcz przeciwnie, będzie zyskiwać na popularności. Niewykluczone, że inicjatywy z blockchainem jako ich integralną częścią, których efektem będą rozwiązania, które wywrą największy wpływ na życie ludzi, nawet jeszcze nie powstały i nie narodzą się przez najbliższe kilka lub nawet kilkanaście lat.

LITERATURA

1. Antonopoulos A. (2017): *Mastering Bitcoin (Second Edition): Programming the Open Blockchain*. Wydawnictwo O'Reilly Media, Sebastopol.
2. Bashir I. (2017): *Mastering Blockchain*. Wydawnictwo Packt Publishing, Birmingham.
3. Berentsen A., Schär F. (2018): *A Short Introduction to the World of Cryptocurrencies*. Federal Reserve Bank of St. Louis, Saint Louis. Dostęp: https://files.stlouisfed.org/files/htdocs/publications/review/2018/01/10/a-short-introduction-to-the-world-of-cryptocurrencies.pdf
4. Botsman R. (2017): *How Blockchain is Redefining Trust.* WIRED. Dostęp: https://www.wired.com/story/how-the-blockchain-is-redefining-trust/?mbid=GuidesLearnMore
5. Boucher P. (2017): *How blockchain technology could change our lives*. Biuro Analiz Parlamentu Europejskiego, Bruksela. Dostęp: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf
6. Buterin V. (2014): *Ethereum White Paper - a Next Generation Smart Contract & Decentralized Application Platform*. Ethereum Foundation. Dostęp: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
7. Crosby M., Pattanayak P., Verma S., Kalyanaraman V. (2015): *Blockchain Technology: Beyond Bitcoin*. Uniwersytet Kalifornijski, Berkeley. Dostęp: http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf
8. Dobson D. (2018): *The 4 Types of Blockchain Networks Explained.* International Legal Technology Association. Dostęp: https://www.iltanet.org/blogs/deborah-dobson/2018/02/13/the-4-types-of-blockchain-networks-explained
9. Doubleday K. (2018): *Blockchain for 2018 and Beyond: A (growing) list of blockchain use cases.* Medium. Dostęp: https://medium.com/fluree/blockchain-for-2018-and-beyond-a-growing-list-of-blockchain-use-cases-37db7c19fb99
10. Finley K. (2018): *The WIRED Guide to Bitcoin.* WIRED. Dostęp: https://www.wired.com/story/guide-bitcoin

11. Finley K. (2018): *The WIRED Guide to the Blockchain*. WIRED. Dostęp: https://www.wired.com/story/guide-blockchain/
12. Frankowski E., Barański P. (2017): *Technologia Blockchain i jej potencjał w podatkach.* Deloitte, Katowice. Dostęp: https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_Blockchain-technology-and-its-potential-in-taxes-2017-PL.PDF
13. future[inc] (2017): *The Future of Blockchain: Applications and Implications of Distrubuted Ledger Technology.* Cartered Accountants, Canberra. Dostęp: https://www.charteredaccountantsanz.com/-/media/c1430d6febb3444192436ffc8b685c7c.ashx
14. González B. (2017): *From Alan Turing to Cyberpunk: The History of Blockchain.* BBVA. Dostęp: https://www.bbva.com/en/alan-turing-cyberpunk-history-blockchain/
15. Graham W. (2018): *Building it Better: A Simple Guide to Blockchain Use Cases.* Uniwersytet Kalifornijski, Berkeley. Dostęp: https://blockchainatberkeley.blog/building-it-better-a-simple-guide-to-blockchain-use-cases-de494a8f5b60
16. Harari Y. (2011): *Sapiens. Od zwierząt do bogów.* Wydawnictwo PWN, Warszawa
17. Jeffries D. (2017): *Why Everyone Missed the Most Mind-Blowing Feature of Cryptocurrency.* Hackernoon. Dostęp: https://hackernoon.com/why-everyone-missed-the-most-mind-blowing-feature-of-cryptocurrency-860c3f25f1fb
18. Khatwani S. (2018): *What is Proof-of-Work & Proof-of-Stake?* Dostęp: https://coinsutra.com/proof-of-work-vs-proof-of-stake-pow-vs-pos/
19. Klinger B., Szczepański J. (2017): *Blockchain – Historia, Cechy i Główne Obszary Zastosowań.* UKSW, Warszawa. Dostęp: http://czasopisma.uksw.edu.pl/index.php/cwc/article/view/1858
20. Kosba A., Miller A., Shi E., Wen Z., Papamanthou C. (2015): *Decentralizing Privacy: Using Blockchain to Protect Personal Data.* Wydawnictwo IEEE, Piscataway Township. Dostęp: http://ieeexplore.ieee.org/document/7163223/
21. Lai V., Wong V. (2018): *Cryptocurrency and Blockchain Glossary.* CrushCrypto. Dostęp: https://crushcrypto.com/glossary/
22. Lannquist A. (2017): *Blockchains, Cryptocurrencies & New Decentralized Economy: Part 1 – a Gentle Introduction.* Uniwersytet Kalifornijski, Berkeley. Dostęp: https://blockchainatberkeley.blog/blockchains-cryptocurrencies-the-new-decentralized-economy-part-1-a-gentle-introduction-edcb4824b174

23. Lannquist A. (2017): *Blockchains, Cryptocurrencies & New Decentralized Economy: Part 2 – Blockchain-Based Apps.* Uniwersytet Kalifornijski, Berkeley. Dostęp: https://blockchainatberkeley.blog/blockchains-cryptocurrencies-the-new-decentralized-economy-part-2-blockchain-based-apps-e6ea71236ca
24. Li K. (2018): *The History of Money & The Future of Bitcoin and The Cryptocurrency Economy.* Hackenoon. Dostęp: https://hackernoon.com/the-history-of-money-the-future-of-bitcoin-and-the-cryptocurrency-economy-5cc25e808275
25. Maxwell W., Salmon J. (2017): *A guide to blockchain and data protection.* Hogan Lowells, *Londyn.* Dostęp: https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf
26. McMillan R. (2014). *The Inside story of Mt. Gox Bitcoin's 460$ million dollar disaster*. WIRED. Dostęp: https://www.wired.com/2014/03/bitcoin-exchange/
27. Middelman M. (2016): *21 Terms to Understand Cryptocurrency.* Medium. Dostęp: https://medium.com/the-mission/21-terms-to-understand-cryptocurrency-8bee30aa8dfc
28. Nakamoto S. (2008): *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin Project. Dostęp: https://bitcoin.org/bitcoin.pdf
29. Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. (2016): *Bitcoin and Cryptocurrency Technologies*. Wydawnictwo Princeton University Press, Princeton.
30. Narayanan V. (2018): *A brief history in the evolution of blockchain technology platforms.* Hackernoon. Dostęp: https://www.bbva.com/en/alan-turing-cyberpunk-history-blockchain/
31. Odinsky J. (2017): *Blockchain Dictionary.* Hackernoon. Dostęp: https://hackernoon.com/blockchain-dictionary-f4d098c9ef89
32. Pisa M., Juden M. (2017): *Blockchain and Economic Development: Hype vs. Reality*. Wydawnictwo CGD, Waszyngton. Dostęp: https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf
33. Ray S. (2017): *Blockchains versus Traditional Databases.* Hackernoon. Dostęp: https://hackernoon.com/blockchains-versus-traditional-databases-c1a728159f79
34. Robertson J. (2007): *The History of Money From Its Origins to Out Time.* Autrement, Paryż. Dostęp: http://www.jamesrobertson.com/book/historyofmoney.pdf
35. Rosic A. (2017): *Blockchain Adress 101: What are Addresses on Blockchains?* Blockgeeks. Dostęp: https://blockgeeks.com/guides/blockchain-address-101/

36. Rosic A. (2017): *Blockchain Glossary: From A-Z.* Blockgeeks. Dostęp: https://blockgeeks.com/guides/blockchain-glossary-from-a-z/
37. Swan M. (2015): *Blockchain: Blueprint for a New Economy*. Wydawnictwo O'Reilly Media, Sebastopol.
38. Tania H. (2018): Implementing blockchain in business. Dostęp: https://rubygarage.org/blog/implementing-blockchain-in-business
39. Tapscott D., Tapscott A. (2017): *Realizing the Potential of Blockchain*. Światowe Forum Ekonomiczne, Davos. Dostęp: http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf
40. Territt H., Obie S., Ahern C. (2017): *Blockchain for Business.* Jones Day, Nowy Jork. Dostęp: http://www.jonesday.com/files/upload/Blockchain%20for%20Business%20White%20Paper2.pdf
41. Ting K. (2018): *A Glossary of all the Cryptocurrency Terms you need to know. Cryptominded.* Dostęp: https://cryptominded.com/glossary-cryptocurrency-terms-need-know/
42. Voshmgir S. (2017): *Blockchains & Distributed Ledger Technologies.* BlockchainHub. Dostęp: https://blockchainhub.net/blockchain-intro/
43. Voshmgir S. (2017): *What is Blockchain?* BlockchainHub. Dostęp: https://blockchainhub.net/blockchain-intro/
44. Wright A, De Filippi P. (2015): *Decentralized Blockchain Technology and the Rise of Lex Cryptographia.* Wydawnictwo SSRN, Rochester. Dostęp: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664
45. Wüst K., Gervais A. (2017): *Do you need a Blockchain?* ETH Zürich, Zurych. Dostęp: https://eprint.iacr.org/2017/375.pdf
46. Yii-Huumo J., Ko D., Choi S., Park S., Smolander K. (2016): *Where is Current Research on Blockchain Technology? – A Systematic Review. Wydawnictwo Plos One,* San Francisco. Dostęp: http://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0163477&type=printable

WYKAZ RYSUNKÓW

		Zurych. s. 3. Dostęp: https://eprint.iacr.org/2017/375.pdf [13.06.2018r.]
14.	Porównanie tradycyjnego SCM do napędzanego przez blockchain.	Wüst K., Gervais A. (2017): Do you need a Blockchain? ETH Zürich, Zurych. s. 4. Dostęp: https://eprint.iacr.org/2017/375.pdf [13.06.2018r.]
15.	Wynik audytu bezpieczeństwa bibliotek.	Opracowanie własne
16.	Schemat komunikacji między komponentami.	Opracowanie własne
17.	Blockchain explorer – lista bloków wraz z transakcjami.	Opracowanie własne
18.	Blockchain explorer – mempool.	Opracowanie własne
19.	Struktura bloku.	Opracowanie własne
20.	Struktura transakcji.	Opracowanie własne
21.	Struktura portfela z jednym adresem.	Opracowanie własne
22.	Implementacja pętli generującej dowód pracy.	Opracowanie własne
23.	Implementacja metody określającej trudność blokową dla dowodu pracy.	Opracowanie własne
24.	Wzór i wykres funkcji określającej trudność blokową.	https://www.wolframalpha.com/ [20.06.2018r.]

WYKAZ TABEL

Nr	Tytuł	Źródło
1.	Wykaz bibliotek wykorzystanych w projekcie Motus.	Opracowanie własne
2.	Dokumentacja dostępnych metod API komponentu Blockchain.	Opracowanie własne
3.	Dokumentacja dostępnych metod API komponentu Operator.	Opracowanie własne
4.	Dokumentacja dostępnych metod API komponentu Node.	Opracowanie własne
5.	Dokumentacja dostępnych metod API komponentu Miner.	Opracowanie własne

WYKAZ ZAŁĄCZNIKÓW

Nr	Opis	Plik
1.	Kod źródłowy projektu kryptowaluty Motus.	https://github.com/TheDoctor0/Motus