Podstawy Blockchain

Ta Część będzie służyła jako podstawa, zanim „rozpoczniesz” w kierunku rozwoju. Wprowadzi podstawowe pojęcia, które pomogą Ci zrozumieć technologię blockchain. Jest podzielona na cztery części.

- Wprowadzenie do kryptoekonomii

- Wyjaśnienie Blockchain

- Przeciążenie Kryptowalut

- Sieć Blockchain P2P

Aby zrozumieć kryptoekonomikę, musisz najpierw zrozumieć pojęcia, takie jak szyfrowanie i deszyfrowanie, klucze prywatno-publiczne, kryptografia, aktywa cyfrowe, kryptografia i kryptowaluta. Kiedy zrozumiesz te podstawowe pojęcia, omówię blockchain. Omówię elementy, które składają się na pojedynczy blockchain, takie jak bloki i sposób, w jaki bloki są ze sobą powiązane, a także problemy z blockchainem, takie jak podwójne wydatki. Wyjaśnię również wydobywanie kryptowalut, kryptominerów i portfele kryptowalut. Następnie omówię różne rodzaje kryptowalut: bitcoin, tokeny i alternatywne monety kryptowaluty (altcoiny). Na koniec omówię sieć P2P używaną z technologią blockchain i różne warstwy, które tworzą sieć: warstwę konsensusu, warstwę górniczą, warstwę propagacji, warstwę semantyczną i warstwę aplikacji.

Wprowadzenie do kryptoekonomii

Świat krypto jest pełen technicznego żargonu, który może zmylić nawet najbardziej doświadczonych technologów ninja. Bitcoin wprowadził pojęcie kryptoekonomii i utorował drogę do stworzenia wielu platform blockchain. Zanim zagłębimy się w to, jak działa blockchain, zrozummy, czym jest kryptoekonomia i jakie koncepcje kryją się za blockchainem. Komunikacja werbalna polega na doborze słów opisujących wiadomość, którą chcesz przekazać. Czasami jednak chcesz komunikować się tylko z niektórymi osobami, wykluczając innych. Dobrym przykładem jest czas wojny; dowódca komunikuje się z żołnierzami stacjonującymi na linii frontu, upewniając się, że wróg nie może słuchać. Dowódca mógł użyć szyfrowania do tej komunikacji. Mówiąc elektronicznie, dziś wszystkie strony handlowe oferują swoje towary za pośrednictwem protokołu szyfrowania, zwanego Secure Sockets Layer (SSL), który może chronić Twoje dane osobowe przed hakerami. Szyfrowanie i odszyfrowywanie wideo są powszechne, aby zapewnić dostarczanie wideo tylko do autoryzowanych członków, a na komputerach osobistych ludzie często używają szyfrowania do tworzenia kopii zapasowych i ochrony plików i haseł. Co więcej, jako programista prawdopodobnie wysyłałeś zaszyfrowane wiadomości, a także odszyfrowałeś wiadomości przychodzące za pomocą bibliotek, ponieważ wszystkie języki programowania oferują funkcje szyfrowania i deszyfrowania ciągów. Przyjrzyjmy się więc niektórym definicjom:

- Szyfrowanie: Szyfrowanie to proces przekształcania wiadomości w kod, dzięki czemu dostęp do niej mają tylko upoważnione strony.

- Deszyfrowanie: odszyfrowywanie polega na odwróceniu procesu szyfrowania, dzięki czemu wiadomość może zostać przekonwertowana na oryginalną wiadomość.

- Kryptografia: wykorzystuje techniki szyfrowania i deszyfrowania do wysyłania i odbierania wiadomości.

- Kryptowaluta: wykorzystuje kryptografię w taki sam sposób, jak we wcześniejszym przykładzie SSL lub wideo, ale specjalnie w celu dostosowania do potrzeb zasobu cyfrowego.

- Kryptoekonomia: Jest to połączenie kryptografii i ekonomii w celu zapewnienia platformy do przekazywania zasobów cyfrowych.

Uwaga : zasób cyfrowy może być dowolną wartością, na przykład kombinacją do sejfu domowego, tajnym hasłem, listą, wiadomością, gotówką elektroniczną, dokumentem, zdjęciem i tak dalej.

Ig-pay Atin-lay

Na początek cofnijmy się w czasie. Czy kiedykolwiek jako dziecko mówiłeś po łacinie świńskiej? Tajny język Pig Latin jest prosty. Usuwasz pierwszą literę słowa, które chcesz wypowiedzieć, a następnie przenosisz ją na koniec słowa, a także dodajesz dźwięk „ay".

Na przykład:

- „Pig" staje się „ig-pay".

- „Latin" staje się „atin-lay".

To, co właśnie zrobiliśmy, to szyfrowanie. Następnie, aby zrozumieć słowa, które zaszyfrowaliśmy, musimy cofnąć się.

- „Ig-pay" staje się „pig", usuwając „ay" z końca i biorąc ostatnią literę i umieszczając ją jako pierwszą.

- Podobnie „atin-lay" staje się „Latin".

To, co właśnie zrobiliśmy, to odszyfrowanie. Dzieci mogą używać tych technik do szyfrowania i deszyfrowania słów w prostej formie kryptografii.

Szyfrowanie/odszyfrowywanie

Szyfrowanie umożliwia bezpieczne przekazywanie wiadomości między określonymi stronami, dzięki czemu wykluczone strony ich nie zrozumieją. Na przestrzeni dziejów istniała potrzeba wysyłania tajnych wiadomości między stronami. Jedna strona wysyła zaszyfrowaną wiadomość w jednym miejscu, a druga strona może odebrać i odszyfrować wiadomość w innym miejscu. W rzeczywistości szyfrowanie było często używane podczas I wojny światowej i II wojny światowej. Naziści używali maszyny zwanej Enigma do szyfrowania i deszyfrowania wiadomości. Alianci wymyślili sposób na złamanie tajnego kodu nazistowskiej maszyny Enigmy i odszyfrowanie wiadomości. Uważa się, że skróciło to o lata II wojnę światową. Szyfrowanie i deszyfrowanie przeszło z użycia wyłącznie w armii do użytku publicznego dzięki opracowaniu przez IBM w 1970 roku standardu szyfrowania danych (DES) i wynalezieniu kryptografii klucza w 1976 roku. W rzeczywistości kryptografia i szyfrowanie były w przeszłości synonimami.

Szyfrowanie + Deszyfrowanie = Kryptografia

Jak wspomniano, kryptografia to proces wykorzystujący techniki szyfrowania i deszyfrowania. Słowo kryptografia pochodzi od greckiego słowa kryptos, które oznacza ukrycie lub sekret. W przykładzie języka Pig Latin opisałem, jak można szyfrować i odszyfrowywać słowa. Ta technika usuwania pierwszej litery i dodawania jej na końcu „ay", a następnie na odwrót, to kryptografia. Bez znajomości tej techniki nie byłbyś w stanie zrozumieć języka Pig Latin. Większość ludzi jest prawdopodobnie na tyle sprytna, aby odkryć sekretny język świńskiej łaciny, ponieważ jest on prosty z natury; jednak skomplikowany przykład szyfrowania byłby inną historią. Na przykład, wracając do maszyny Enigmy z czasów II wojny światowej, naziści przesyłali wiadomości drogą powietrzną. Alianci byli w stanie odbierać te

wiadomości (wiadomości były „kluczami publicznymi"), ale bez możliwości ich odszyfrowania („klucze prywatne") to nie wystarczyło. Naukowiec imieniem Turing i inni zajęli pięć i pół miesiąca, aby odszyfrować tajne wiadomości nazistów. Wkład Turinga polegał na zautomatyzowaniu maszyny, która była w stanie ustalić różne ustawienia, które naziści dokonali w swojej Enigmie, aby mogli odszyfrować wiadomości. Innymi słowy, zautomatyzował proces wyszukiwania klucza prywatnego. Ta maszyna nazywała się bomba.

Uwaga: do zaszyfrowania wiadomości można użyć klucza kryptograficznego. Zaszyfrowaną wiadomość można następnie odszyfrować tylko przy użyciu drugiego klucza (klucza prywatnego), który jest znany tylko odbiorcy.

Zasoby cyfrowe + Kryptografia = Kryptowaluta

Kryptowaluta to zasób cyfrowy zaprojektowany tak, aby można było wymieniać elektroniczną gotówkę przy użyciu silnej kryptografii (szyfrowanie i deszyfrowanie), aby zapewnić bezpieczeństwo środków, transakcji i tworzenia nowych środków. Mechanizm klucza prywatnego kryptografii musi być wystarczająco silny, aby jego rozgryzienie było prawie niemożliwe (innymi słowy, wymagałoby zbyt wiele czasu i wysiłku). W przeciwnym razie wszyscy użytkownicy mogliby potencjalnie stracić swoją elektroniczną gotówkę, gdyby kryptografię można było rozgryźć w ciągu kilku miesięcy, tak jak w przypadku maszyny Enigma. Przykładem kryptowaluty jest bitcoin. Chociaż bitcoin nie był pierwszą wynalezioną kryptowalutą, jest powszechnie uważany za pierwszą odnoszącą sukcesy kryptowalutę. Sukces Bitcoina przypisuje się następującym cechom: nikt nie może złamać klucza publiczno-prywatnego, jest rozpowszechniany bez kontrolowanego rządu, jest publicznie dostępny i jest publikowany jako kod open source.

Uwaga: Bitcoin został wynaleziony w 2008 roku przez Satoshi Nakamotoi wraz z publikacją białej księgi zatytułowanej „Bitcoin: elektroniczny system gotówkowy peer-to-peer"

Kryptografia + Ekonomia = Kryptoekonomia

Kryptoekonomia to połączenie kryptografii i ekonomii w celu zapewnienia platformy, która daje motywację do utrzymania platformy, jej skalowalności i bezpieczeństwa; ponadto nie podlega kontroli władz centralnych lub samorządowych. Innymi słowy, jest zdecentralizowany. Sieć składa się ze zbioru wielu komputerów zamiast jednego komputera centralnego.

Uwaga: Zdecentralizowany jest przeciwieństwem kontroli centralnej; oznacza to brak kontroli ze strony władz centralnych lub lokalnych.

Bitcoin jest w stanie osiągnąć cele kryptoekonomii przy użyciu koncepcji klucza prywatno-publicznego; kryptograficzne i kryptograficzne funkcje mieszające są używane pośrednio. W rzeczywistości związek między kryptografią a kryptowalutą jest pośredni nie tylko dla bitcoina, ale dla większości kryptowalut. Na przykład kryptografia jest używana w bitcoinie na inne sposoby, takie jak:

- Bitcoin używa kluczy prywatnych (bitcoin nazywa te podpisy cyfrowe) za pomocą funkcji algorytmu (zwanej krzywą eliptyczną ECDSA) w celu udowodnienia własności.

- Algorytmy haszujące służą do przechowywania struktury danych księgowych bazy danych (lub łańcucha bloków) za pomocą generatora skrótów o nazwie SHA256.

- Algorytmy mieszające służą do generowania zagadek matematycznych, które komputer próbuje rozwiązać, aby zdobyć nagrodę. Po rozwiązaniu zagadki wybierany jest komputer, który pomaga w obsłudze transakcji.

- Algorytmy haszujące są również używane do generowania adresów kont.

- Istnieje koncepcja drzew Merkle, które wykorzystują klucze haszujące dużych danych w małych kawałkach. Jest to przydatne w przypadku lekkich portfeli, które są potrzebne na ograniczonych urządzeniach sprzętowych, takich jak urządzenia mobilne.

Bitcoin nie gromadzi informacji o tożsamości swoich użytkowników; jednak transakcje są publiczne, co oznacza, że wszystkie informacje są przekazywane i dostępne online. Pomyśl ponownie o przykładzie Enigmy; oznacza to, że każdy może przechwycić przesyłane wiadomości. Jednak bez klucza prywatnego nikt nie może odszyfrować wiadomości. Od czasu wydania bitcoina w 2009 r. istnieje wiele innych platform, które wykorzystują różne rodzaje prywatności do przesyłania informacji w bezpieczny sposób i używają szyfrowania w większej liczbie części procesu, dzięki czemu mniej informacji jest udostępnianych publicznie. Platformy takie jak Monero i Zcash wykorzystują anonimowość za pomocą kryptografii nawet do przesyłania informacji o transakcjach

Wyjaśnienie Blockchain

Jak wspomniałem, bitcoin był pierwszą udaną cyfrową gotówką typu open source. Blockchain to podstawowa technologia lub serce stojące za bitcoinem, a właściwie za wszystkimi platformami kryptowalutowymi.

Ale czym jest blockchain?

Krótko mówiąc, blockchain to współdzielona cyfrowa księga. Pomyśl o bazie danych, która zamiast przechowywać wszystkie wpisy bazy danych na jednym komputerze, przechowuje dane na wielu komputerach. Bardziej zaawansowaną definicją byłoby to, że blockchain jest zdecentralizowaną i rozproszoną globalną księgą.

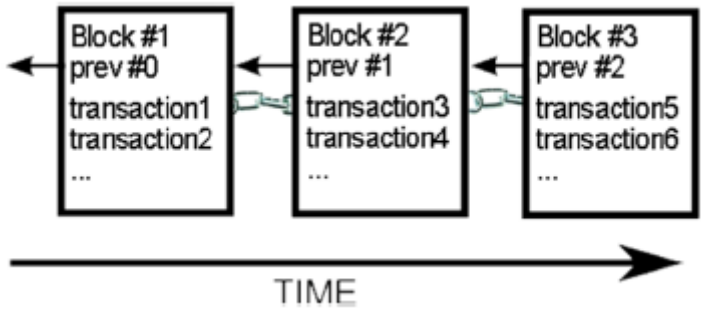
Bloki + Łańcuch = Blockchain

Każdy blok zawiera rekordy i transakcje; bloki te są współdzielone przez wiele komputerów i nie należy ich zmieniać bez porozumienia (konsensusu) całej sieci. Sieć jest zarządzana zgodnie z określoną polityką. Komputery są połączone w jedną sieć i nazywane są równorzędnymi lub węzłami.

Uwaga: co to jest blockchain? Blockchain to cyfrowo zdecentralizowane (brak zaangażowanych instytucji finansowych) i rozproszone księgi. W kategoriach laika jest to baza danych, która przechowuje rekordy i transakcje na wielu komputerach bez jednej strony kontrolującej i zgodnie z uzgodnioną polityką. Przechowywane dane to blok, a bloki są połączone (połączone) w łańcuch bloków.

Połączone bloki

Łańcuch bloków składa się ze zbioru danych (bloku) połączonego z poprzednim blokiem. Jak są połączone? Blok zawiera dane, a każdy blok odwołuje się do poprzedzającego go bloku, więc są one połączone tak, jak ogniwo łańcucha było połączone z poprzedzającym go ogniwem łańcucha. Spójrz na rysunek; jak widać, każdy blok odwołuje się do poprzedniego bloku.



Tak więc blockchain zawiera bloki, które przechowują zapisy transakcji. Klucze prywatne są przechowywane przez właściciela, aby pokazać dowód własności (jest to podpis cyfrowy), więc nikt bez klucza prywatnego nie może odszyfrować ciągu i zgłosić prawa własności. Ta kombinacja kluczy publicznych i kluczy prywatnych reprezentuje gotówkę elektroniczną. Jak powiedziałem, zasoby cyfrowe mogą być wszystkim — plikiem muzycznym, plikiem wideo, dokumentem elektronicznym i tak dalej. W kryptowalucie zasób cyfrowy jest reprezentowany jako gotówka elektroniczna; możesz myśleć o kluczu publicznym jako o koncie bankowym i numerze rozliczeniowym, ao kluczu prywatnym jako o rzeczywistej gotówce na koncie. Tak, możesz udostępniać informacje o swoim banku innym, ale środki pozostaną na Twoim koncie. Aby odebrać gotówkę, musisz udowodnić, że jesteś właścicielem. Idziesz do banku, okazujesz dowód tożsamości i udowadniasz, że to Ty w formie podpisu; tylko wtedy możesz wyciągnąć pieniądze ze swojego konta. Podobny proces ma miejsce w przypadku kryptowalut. Istnieje adres publiczny reprezentujący Twoje konto, a tylko właściciel posiada klucz prywatny do udowodnienia własności.

Uwaga: peers tworzą sieć węzłów, więc w tekście może zobaczyć słowo peer lub węzeł. Te słowa są synonimami na nasze potrzeby

Problem z podwójnymi wydatkami

Podpis cyfrowy (klucze publiczne i klucze prywatne) bezpiecznie zapewnia zachowanie poufności tożsamości strony i przechowywanie gotówki elektronicznej. Ta koncepcja kombinacji kluczy prywatno-publicznych umożliwia szyfrowanie i odszyfrowywanie ciągów znaków oraz ich bezpieczne przechowywanie, tak jak w przypadku maszyny Enigma. Jednak to wciąż za mało, aby rozwiązać największy problem podwójnego wydawania waluty cyfrowej. Kiedy używasz pieniądza fiducjarnego (papierowego pieniądza zatwierdzonego przez rząd), takiego jak dolary amerykańskie lub euro, papier jest niewymienialny, co oznacza, że po oddaniu papieru nie możesz go ponownie wydać. W kryptowalucie, co się stanie, jeśli udowodnisz własność i wyślesz Twój zasób cyfrowy dwa razy w tym samym czasie? Może to prowadzić do podwójnych wydatków. Hakerzy mogą próbować odtworzyć zasoby cyfrowe, a także potencjalnie je dwukrotnie wydać, co kryptowaluta musiała rozwiązać, zanim mogła zostać użyta jako waluta cyfrowa.

Uwaga: Podwójne wydawanie oznacza ryzyko, że waluta cyfrowa może zostać wydana dwa razy, ponieważ podpis cyfrowy może zostać odtworzony i - można udowodnić własność i wysłać zasób cyfrowy dwa razy w tym samym czasie.

Bloki, które przechowują klucze, nie wystarczą, aby zapewnić bezpieczeństwo i rozwiązać potencjalny problem podwójnego wydatkowania w celu utworzenia waluty cyfrowej. Bitcoin rozwiązuje ten problem, tworząc sieć komputerów i udowadniając, że nie doszło do żadnych prób podwójnego wydatkowania. Odbywa się to poprzez informowanie wszystkich komputerów w sieci o każdej transakcji. Wszystkie transakcje są udostępniane wszystkim komputerom w sieci.

Rozwiązanie dotyczące podwójnych wydatków: sieć P2P

W kryptowalucie użycie sieci peer-to-peer zapewniło rozwiązanie problemu podwójnego wydatkowania.

Uwaga : Sieć P2P to rozproszona architektura aplikacji, w której zadania, które należy wykonać, są dzielone na różne elementy równorzędne, przy czym każdy z nich ma te same uprawnienia. Razem peery tworzą sieć węzłów P2P. Każdy komputer podłączony do sieci jest nazywany komputerem równorzędnym. Urządzeniem równorzędnym może być dowolny komputer spełniający wymagania sieciowe, taki jak laptop, urządzenie mobilne lub serwer. Komputery są połączone ze sobą w Internecie za pomocą protokołu sieciowego P2P i tworzą sieć węzłów. Protokół sieciowy P2P nie jest nowy. Jest szeroko stosowany w sieci od lat, od pobierania plików przez sieci Kazaa lub LimeWire po prowadzenie wideorozmów przez Skype. Jak wspomniałem, bitcoin był pierwszą realną kryptowalutą i rozwiązał problem podwójnych wydatków, a także umożliwia przechowywanie elektronicznej gotówki bez przechodzenia przez instytucje finansowe, wykorzystując P2P do utworzenia protokołu blockchain.

Wersja elektronicznej gotówki czysto peer-to-peer umożliwiłaby przesyłanie płatności online bezpośrednio od jednej strony do drugiej bez przechodzenia przez instytucję finansową". -Satoshi Nakamoto, Bitcoin: elektroniczny system gotówkowy peer-to-peer

Wydobywanie kryptowalut przez Cryptominerów

Jak wspomniano, każdy komputer, który przechowuje kopię współdzielonej księgi i jest podłączony do sieci P2P, jest równorzędny. Peer może pomóc w dodawaniu rekordów i weryfikacji transakcji. Proces ten nazywa się kopaniem kryptowalut, a peer, który pomaga rejestrować i weryfikować transakcje, jest nazywany kopaczem kryptowalut lub w skrócie kopaczem. Każdy górnik pomaga w weryfikacji i dodawaniu transakcji do cyfrowej księgi blockchain. Górnicy są często wynagradzani opłatą za pracę, a aby utrzymać konkurencyjność w stosunku do innych górników, górnik zazwyczaj potrzebuje komputera ze specjalistycznym sprzętem.

Portfel kryptowalut

Omówiłem, czym są klucze publiczne i prywatne oraz w jaki sposób są używane do szyfrowania i odszyfrowywania ciągów. Ciągi znaków to cyfrowa waluta lub kryptowaluta, a klucze reprezentują cyfrowe pieniądze. Portfel kryptowaluty przechowuje jedną lub wiele kombinacji klucza publicznego i prywatnego i służy do otrzymywania lub wydawania kryptowaluty. Dobrą analogią jest myślenie o portfelu jak o koncie bankowym. Kryptowalutę można stworzyć, otrzymując nagrodę za wykonanie pracy górnika, lub można ją kupić.

Przeciążenie kryptowalut

Zanim zagłębisz się w sieć blockchain P2P, powinieneś wiedzieć, że inną koncepcją, która może powodować zamieszanie, jest różnica między monetami a tokenami. Według Coinmarketcap.com, w momencie pisania tego artykułu, notowane są 1833 kryptowaluty z kapitalizacją rynkową w wysokości 200 miliardów dolarów. Wiele z tych monet z pewnością zniknie w nadchodzących latach, ponieważ mają niewielką wartość, a projekty te zostaną zakończone z powodu braku zainteresowania lub oszustwa. Może to być mylące i onieśmielające, a większość ludzi nie rozumie pojęcia bitcoin, nie mówiąc już o dużej liczbie monet i tokenów. Aby pomóc zrozumieć te pojęcia, podzielmy kryptowaluty na trzy typy: bitcoin, tokeny i alternatywne monety kryptowaluty (altcoiny).

Bitcoin cyfrowa gotówka

Bitcoin był pierwszą udaną implementacją zdecentralizowanej ,rozproszonej walutya cyfrowej. W sumie jest 21 milionów monet. Monety zastępują tradycyjną walutę fiducjarną.

Tokeny

Tokeny to zdecentralizowana oferta produktów. Jest to kolejna opcja podobna do pierwszej oferty publicznej (IPO) lub finansowania społecznościowego. Tokeny można tworzyć w dowolnym miejscu na świecie i dostarczać za pośrednictwem Ethereum, EOS lub innej wydajnej platformy blockchain. Tokeny są zwykle tworzone i rozpowszechniane publicznie za pośrednictwem początkowej oferty monet (ICO). Tokeny oznaczają narzędzie lub zasób, który zwykle znajduje się na szczycie natywnego łańcucha bloków. Może reprezentować dowolny zasób cyfrowy, w tym punkty lojalnościowe, kryptowaluty lub dowolny towar lub towar z pojedynczymi jednostkami, które są zasobem wymiennym, zamiennym lub zbywalnym. Możesz utworzyć token, korzystając z istniejącego szablonu łańcucha bloków, takiego jak platforma Ethereum, lub możesz tworzyć własne tokeny na istniejącym natywnym łańcuchu bloków i wydawać własne tokeny. Możesz wykorzystać inteligentne kontrakty, aby uprościć proces tworzenia tokenów.

Uwaga : Inteligentne kontrakty to programowalny kod, który działa samodzielnie bez potrzeby korzystania z usług osób trzecich. Na przykład Solidity jest językiem programowania zorientowanym na kontakt i może być wdrażany na wielu łańcuchach bloków.

Alternatywne monety kryptowaluty (altcoiny)

Alternatywne monety kryptowaluty (w skrócie altcoiny) to monety, które pochodzą z kodu źródłowego bitcoin core poprzez forking (soft fork lub hard fork). Przykładami są litecoin (który był rozwidleniem podstawowego klienta bitcoin), dogecoin (dogecoin 1.10 to kompletna przebudowa oparta na wersji bitcoin 0.11), bitcoinX, bitcoin cash i bitcoin gold. Istniało 26 altcoinów. Litecoin był rozwidleniem głównego klienta bitcoina. Litecoin zmienił czas wysyłania bloków z 10 minut na 2,5 minuty, umożliwiając przesyłanie transakcji szybciej i wydajniej niż bitcoin. Litecoin może następnie kontynuować i dodawać funkcje, ponieważ nie polega już na kodzie bitcoina. Na przykład w przyszłości litecoin umożliwi atomic swap, umożliwiając ludziom konwersję Litecoina na bitcoin za pomocą inteligentnych kontraktów bez konieczności wymiany. Jednak zmiany w rdzeniu bitcoin będą wymagały ręcznej implementacji, aby te zmiany zostały uwzględnione w litecoin. Powiedziawszy to, wielu będzie twierdziło, że Litecoin i wiele z tych altcoinów nie oferuje wystarczającej wartości, aby przetrwać i zostały stworzone w celu wzbogacenia programistów, którzy stworzyli fork. Tylko czas powie. EOS to kolejny dobry przykład altcoinów. Tym razem altcoin zamienia się w token, ponieważ po jego wydaniu firma EOS wydała tokeny Ethereum, ale ponieważ EOS buduje własną platformę blockchain, zastępuje token Ethereum własnymi tokenami EOS. Krótko mówiąc, główna różnica między altcoinami a tokenami polega na ich strukturze. Altcoin jest własną walutą, taką jak bitcoin lub Litecoin, z własnym dedykowanym łańcuchem bloków sieci i zapotrzebowaniem na górników. Tokeny, takie jak tokeny Ethereum, działają na istniejącym blockchainie, który zapewnia token i infrastrukturę (taką jak Ethereum) do tworzenia zdecentralizowanej aplikacji (dapp). Przykładem tokena Ethereum jest token binance (BNB). W odniesieniu do tokenów Ethereum, Ethereum oferuje tworzenie różnych standardów tokenów lub Ethereum Request for Comments (ERC), takich jak ERC-20, ERC-223 lub ERC-777. W przykładzie tokena BNB zastosowano ERC-20. Standardy te różnią się i zostaną omówione bardziej szczegółowo.

Uwaga: Hard forki są niekompatybilne wstecz, ponieważ zmiany dzielą kod sieci na dwa — sieć P2P z oryginalnym kodem i nową sieć P2P z nowym kodem. Soft forki są kompatybilne wstecz, co oznacza, że poprzednio ważne bloki/transakcje stają się nieważne, a stare węzły rozpoznają nowe bloki jako ważne. To rozwidlenie zdarza się często, gdy deweloperzy nie zgadzają się co do kierunku. Na przykład,

niektórzy programiści chcieliby wprowadzić zmiany, z którymi inni programiści się nie zgadzają lub konieczne jest zaimplementowanie poważnej poprawki.

Sieć Blockchain P2P

Teraz, gdy lepiej rozumiesz kluczowe koncepcje, możesz głębiej zagłębić się w zrozumienie, w jaki sposób blockchain wykorzystuje sieć P2P do rozwiązania problemu podwójnych wydatków, a także do wykluczenia instytucji finansowych. W tej sekcji zobaczysz, jak działa kryptowalutowa sieć P2P. Zbadasz w szczególności różne polityki blockchain i ogólnie sieć P2P, dzieląc sieć P2P na pięć warstw.

• Warstwa konsensusu

• Warstwa górnicza

• Warstwa propagacyjna

• Warstwa semantyczna

• Warstwa aplikacyjna

Przegląd tutaj utoruje drogę do następnych sekcji, w których będziesz wykorzystywać API bitcoin core do konfigurowania i uruchamiania peera. To fundamentalne zrozumienie może pomóc Ci zrozumieć, jak działa każda sieć blockchain, wykorzystując różne zasady, takie jak NEO i EOS.

Mechanizm konsensusu

W tradycyjnym scentralizowanym systemie, takim jak bank, istnieje komputer główny, któremu ufa księga transakcji. Bank oczywiście może zaufać własnemu komputerowi, dlatego nie ma problemu z tym, że jest odpowiedzialny za bezpieczeństwo i integralność komputera głównego. Kiedy masz do czynienia z niezaufanymi partnerami współdzielącymi księgę, istnieje potrzeba ustanowienia reguł, które zapewnią bezpieczeństwo i zapewnią integralność księgi, aby zapobiec podwójnym wydatkom i innym potencjalnym atakom hakerskim. Te zasady i porozumienia nazywane są mechanizmem konsensusu.

Uwaga: mechanizm konsensusu to porozumienie potrzebne do prawidłowego działania sieci nawet w przypadku awarii. Musi być w stanie osiągnąć porozumienie w sprawie danych sieci w ramach rozproszonej sieci P2P.

Łańcuch bloków nie jest tylko jednym komputerem nadrzędnym i ma działać globalnie. Osiąga integralność dzięki konsensusowi danych przez wszystkie komputery podłączone do sieci. Rozproszony konsensus oznacza, że pula równorzędnych, oddalonych geograficznie, zgadza się w sposób zdecentralizowany, zamiast jednego komputera głównego (scentralizowanego). Zamiast przepisów istnieją reguły, które zwykle są ustalane w środowisku open source, a nie przez jednostkę rządową. Sieć P2P umożliwia prowadzenie księgi rachunkowej. Aby osiągnąć ten cel w bezpieczny sposób, sieć P2P przechowuje reguły i zabezpieczenia księgi cyfrowej. Mechanizm konsensusu zapewnia nie tylko zasady, ale także zachęty do wykonywania pracy polegającej na przechowywaniu danych i tworzeniu transakcji poprzez nagradzanie górników. Sieć P2P działa globalnie przy użyciu połączenia internetowego i jest w stanie zapewnić platformę do osiągnięcia globalnie rozproszonego mechanizmu konsensusu. W kryptowalutach konsensus/umowa dotyczy tego, czy bloki są ważne, czy nie. Jeśli blok jest poprawny, zostanie dodany do łańcucha bloków. Jeśli blok jest nieprawidłowy, zostanie odrzucony przed dodaniem do łańcucha bloków. W tym miejscu w grę wchodzi polityka konsensusu. Większość peerów w sieci posiada te same bloki w swoim sprawdzonym najlepszym łańcuchu bloków i przestrzega tych samych zasad (reguły konsensusu); w ten sposób blockchain zapewnia

bezpieczeństwo. Najtrudniejszy do odtworzenia łańcuch znany jest jako najlepszy blockchain

Dowód pracy, dowód stawki i delegowany dowód stawki

Wraz ze wzrostem popularności blockchain powstało wiele polityk dotyczących mechanizmów konsensusu. Pierwszy z nich został stworzony przez bitcoina, a wiele innych zostało zbudowanych w celu rozwiązywania problemów, które istnieją w innych mechanizmach. W kolejnych sekcjach omówię kilka popularnych.

- Dowód pracy (PoW)

- Dowód stawki (PoS)

- Delegowany dowód udziału (DPoS)

Oprócz tych trzech, istnieje wiele innych mechanizmów konsensusu, które nie zostały, takich jak dowód ważności, dowód upływu czasu (PoET), dowód autorytetu (PoA), dowód wypalenia, dowód zdolności, dowód aktywności i tak dalej. Zachęcamy do samodzielnego odkrywania ich; każdy ma swoje plusy i minusy i pasuje do różnych potrzeb.

Dowód pracy

PoW to pierwszy i najpopularniejszy mechanizm; jest używany przez bitcoin i Ethereum, które są najpopularniejszymi kryptowalutami w momencie pisania tego tekstu. PoW osiąga się dzięki sieci górników i przedstawieniu górnikom problemu matematycznego. Kiedy górnicy rozwiązują problem, są nagradzani kryptowalutą. Nagroda jest dowodem wykonanej „pracy" i stąd nazwa. PoW określa, który partner wykonuje pracę, na podstawie mocy komputera (szybkość skrótu) i przydziela pracę jako procent, więc jest sprawiedliwy. PoW nie ufa żadnemu peerowi w sieci indywidualnie, ale sieć ufa każdemu z nich jako sieci kolektywnej. Nie oznacza to, że jeden górnik konkuruje z innym górnikiem. Sieć górników (zwana pulą) może konkurować o pracę z inną pulą górników. Im wyższy współczynnik haszowania ma pula, tym większe szanse na uzyskanie „pracy". Jak wspomniano wcześniej, kryptowaluty są zdecentralizowane i działają bez jednego zaufanego komputera odpowiedzialnego za księgę. PoW to mechanizm, który zapewnia integralność danych i zniechęca do złośliwych ataków. Dowód pracy (PoW) to matematyczna zagadka, którą musi rozwiązać górnik. Górnik musi znaleźć rozwiązanie złożonego problemu matematycznego, aby zostać liderem i móc stworzyć kolejny najlepszy blok, który zostanie dodany do łańcucha bloków. Im więcej górników istnieje w sieci, tym bardziej złożona jest matematyczna trudność, którą należy rozwiązać. W przypadku bitcoina co dziesięć minut dodawany jest tylko jeden blok z tylko jednym zwycięzcą, więc konkurencja jest zacięta. Rozwiązanie problemu uruchamia chipy w komputerze, które zużywają energię elektryczną i wytwarzają ciepło. Pomyśl o komputerze z intensywną grą wideo, która zawiera wiele multimediów lub komputerze przetwarzającym wideo do produkcji. Ta informacja jest przydatna do obliczania opłacalności wydobycia. Kiedy bitcoin pokazuje 5 bilionów jako poziom trudności, z szacowanym wzrostem trudności o +3,74% i całkowitym hash rate wynoszącym 43 bilionów GH/s. Pokazuje również, że utworzenie jednego bloku zajmuje 9,9 minuty i generuje około 25 bitcoinów. Szybkie obliczenia pokazują, że jeśli co 10 minut otrzymujemy blok o wielkości 4,2 MB rocznie, to 80 bajtów danych na blok $*$ 6 godzin $*$ 24 godziny $*$ 365 dni = 4,2 MB danych rocznie. Posiadanie bloku tworzonego co dziesięć minut jest czynnikiem ograniczającym, a liczba transakcji, które można uwzględnić w każdym bloku, jest ograniczona. Stwarza to problem skalowalności, który inne mechanizmy konsensusu próbowały poprawić. Podsumowując, każdy górnik ściga się, aby rozwiązać ten sam problem; po rozwiązaniu problemu proces zostaje uruchomiony ponownie. Ten problem to matematyczna zagadka

znana jako problem z dowodem pracy, a nagroda jest przyznawana pierwszemu górnikowi, który rozwiąże problem. Następnie zweryfikowane transakcje są przechowywane w księdze publicznej. Ten PoW ma swoje wady; ten typ algorytmu może stwarzać różnego rodzaju problemy w dzisiejszym świecie. Na przykład, jeśli jedna pula wydobywcza kontroluje ponad 51 procent całkowitej mocy wydobywczej, całe bezpieczeństwo blockchain jest zagrożone, ponieważ masz jeden centralny kolektyw nieznacznie różni się od posiadania jednego komputera. Atak DDOS na sieć może zagrozić całej wiarygodności sieci. To się rzeczywiście wydarzyło i nie jest to tylko teoria. W chwili pisania tego tekstu bitcoin gold, rozwidlona wersja bitcoina, ucierpiała w wyniku ataku DDOS.

Atak typu rozproszona odmowa usługi (DDoS) ma miejsce, gdy wiele systemów atakuje zasoby/przepustowość systemu docelowego.

Na PoW, wraz ze wzrostem trudności, oznacza to mniejszy zysk. Mniejszy zysk oznacza mniejszą zachętę do wydobywania monet. Kryptowaluta Ethereum boryka się z problemem zmniejszenia liczby kopaczy w sieci, a w 2018 roku Ethereum musiało zaplanować „bombę trudności", która zmniejszyła trudność (podniesienie zysku dla górników), a także przejść z PoW na PoS w celu zwiększenia skalowalności. Jak dochodzi do ataku? Pula, która stanowi 51 procent mocy haszującej sieci, jest w stanie stworzyć własny blok i opublikować go szybciej niż główne aktualizacje łańcucha bloków. Blok zawiera 51 procent sieci i jest w stanie podwoić wydawanie monet, usuwając transakcje po wydaniu, aby monety nie zostały zabrane z pierwotnego portfela. To zagrożenie jest realne. Bitmain, firma wydobywcza, kontrolowała ponad 40 procent całkowitego wskaźnika haszowania bitcoinów. Wielu uważa, że PoW jest niezrównoważony i niewystarczający ze względu na ilość energii elektrycznej zużywanej przez górników oraz niską prędkość transakcji w porównaniu z innymi algorytmami. Patrząc z perspektywy, obecne szacowane roczne zużycie energii elektrycznej przez Bitcoin wynosi około 60 do 73 terawatogodzin (TWh) rocznie. To podobna ilość energii elektrycznej, jaka jest potrzebna do zasilenia Szwajcarii w ciągu roku; wyobraź sobie, że wiele monet staje się tak popularnymi, jak bitcoin wykorzystujący PoW.

Dowód stawki

PoS został stworzony przez Sunny Kinga i Scotta Nadala w 2012 roku jako alternatywa dla rozwiązania wspomnianych wcześniej wad PoW. PoS opiera się na liczbie monet, które posiada peer. Partner musi postawić liczbę monet, które chce wydobyć. Zamiast mocy haszującej mamy moc udziałów i nie ma zależności od zużycia energii, ponieważ nie ma zagadki do rozwiązania. PoS zapewnia podobny schemat blokowania haszowania do PoW bitcoina, ale ogranicza liczbę peerów. Zapewnia to potrzebne bezpieczeństwo, a jednocześnie obniża koszty i zużycie energii. Opłata sieciowa jest przekazywana rówieśnikom zamiast nagradzania za rozwiązanie zagadki matematycznej, jak w PoW. PoS określa, jaki peer wykonuje pracę, według wielkości stawki, którą posiada peer. Osiąga to rozproszony konsensus przy mniejszym zużyciu energii i niższych kosztach. Ataki DDOS i oszustwa są nadal możliwe. Jednak osoby atakujące nie mogą dokonywać transakcji w większej liczbie walut cyfrowych, niż obstawiają. W przeciwnym razie straciliby swoje depozyty, więc szanse na atak są mniejsze. Pamiętaj, że atakujący mogą postawić monety innych ludzi i nie będą chcieli stracić tych monet, ponieważ nie są one ich, więc nadal istnieją sposoby na atak DDOS. Każdy partner może uczestniczyć w procesie wydobycia, obstawiając monety w celu walidacji nowej transakcji. Aby zostać górnikiem, istnieją dwie opcje; możesz postawić swoje monety do wykorzystania przez godny zaufania węzeł (ale możesz stracić monetę poprzez oszustwo sieci PoS przez węzeł) lub możesz przesłać pełny węzeł, aby został wybrany jako górnik. Decentralizacja jest ograniczona, ponieważ tylko kilku górników może posiadać większość monet i sprawować kontrolę nad większością. Do pracy każdy górnik jest wybierany losowo; nie opiera się na rozwiązywaniu zagadek. Spójrz na tabelę , w której porównano PoW i PoS.

Kategoria : PoW : PoS

Generowanie nowych bloków: Pierwszy górnik, który rozwiąże problem wybrany na podstawie mocy haszującej: Losowy wybór w oparciu o moc stawki (ile monet posiada peer)

Nagroda: Nagroda za blokowanie: Opłaty sieciowe

Zużycie energii i zasobów : Koparka ASIC i duża powierzchnia : Niewielkie zasoby i niskie zużycie energii

Możesz ustawić portfel do stakowania, który zawiera monety potrzebne do PoS. Twoje monety mogą zarabiać co roku w niektórych sieciach blockchain. Oto lista niektórych popularnych monet kryptowalutowych korzystających z PoS:

• Dash: Potrzebujesz 1000 jednostek, aby być węzłem głównym. Daje roczny zwrot w wysokości około 7,5 procent rocznie.

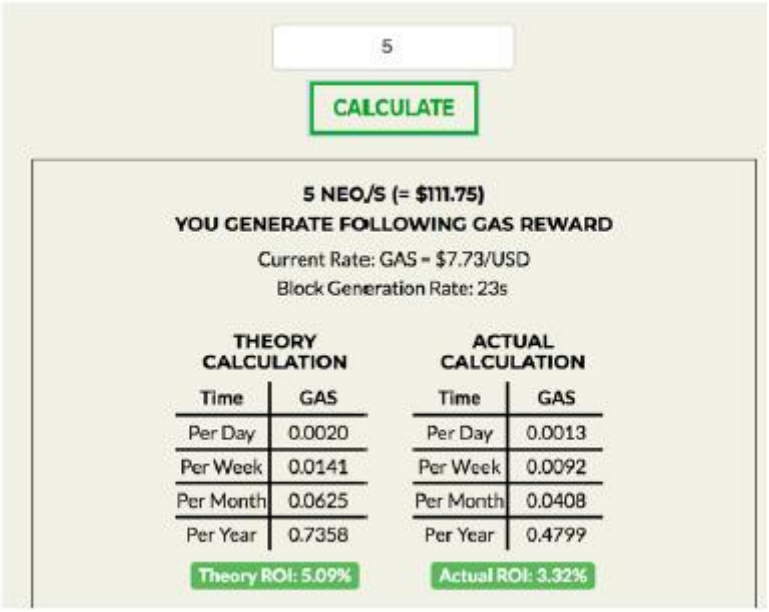
• NEO: Portfele z obstawianiem zwracają około 5,5 procent rocznie. Nie ma potrzeby kopać; otrzymujesz monety gazowe po prostu trzymając monety.

• Inne: LSK, PIVX, NAV, RDD, BEAN, Linda, DCR, NEBL, OK, STRAT.

Chociaż niektóre monety zapewniają roczne zwroty, należy pamiętać, że w przypadku, gdy kapitalizacja rynkowa monet pozostanie stabilna, pojedyncza moneta będzie z czasem mniej warta, ponieważ generowane są nowe monety. Stawienie portfela zmniejsza wartość portfela wstrzymanego (HODL), ponieważ otrzymujesz więcej monet, aby utrzymać wartość portfela. Podobnie jak bank daje ci X% oprocentowania, a inflacja wynosi X%, twoje saldo pokazuje więcej środków, ale realistycznie masz taką samą ilość pieniędzy.

Uwaga: HODL to slangowe określenie ukute w związku z kryptowalutą, aby opisać utrzymywanie kryptowaluty z pominięciem wahań cen.

Przyjrzyjmy się NEO jako przykład. Nie musisz kopać NEO, aby otrzymać nagrodę. Otrzymasz monetę gazową tylko za posiadanie monet jako nagrodę za pomoc w zawieraniu transakcji. Możesz obliczyć, ile monet gazowych otrzymasz, korzystając z tego adresu URL: https://neotogas.com/. W chwili pisania tego tekstu, jeśli kupisz pięć monet NEO i przetrzymasz je przez rok, otrzymasz 0,4799 monet gazowych (obecnie w cenie 7,73 USD), umieszczając je w portfelach do stakowania. Zobacz rysunek.



Delegowany dowód stawki

Delegowany dowód stawki to metoda algorytmu spisu wymyślona przez Dana Larimera, omówiona w białej księdze pod adresem :

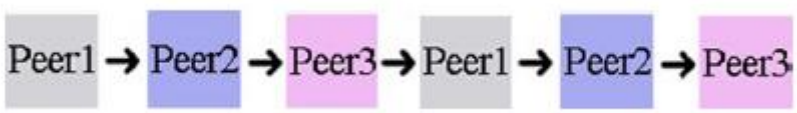
https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md. DPoS ma na celu poprawę wad PoS poprzez zapewnienie demokracji zamiast losowego procesu wyboru górnika. Uwaga: W DPoS górnicy nazywani są producentami bloków.

DPoS osiąga demokrację technologiczną, dzieląc proces wydobycia na dwie części.

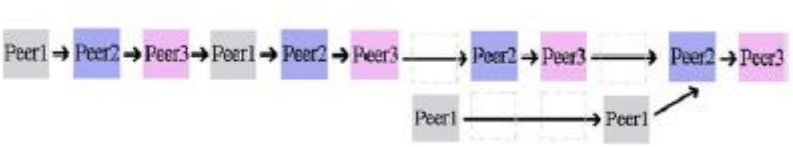
• Wybory: Wybierając grupę producentów bloków, jest tylko 21 producentów bloków zamiast nieograniczonej liczby, jak w przypadku PoW.

• Planowanie produkcji: Każdy z 21 producentów bloków na zmianę produkuje blok co 3 sekundy.

Proces wyborczy zapewnia technologiczną demokrację i gwarantuje, że interesariusze sprawują kontrolę, ponieważ duzi interesariusze mają najwięcej do stracenia w przypadku awarii sieci. Każdy producent bloku wykonuje kolejkę w produkcji bloku i przyjmuje się najdłuższy możliwy łańcuch (tak jak w PoW). Spójrz na normalną operację, jak pokazano na rysunku.



Zobaczysz, że każdy rówieśnik od 1 do 3 ma swoją kolej na wyprodukowanie najdłuższego bloku łańcucha. Za każdym razem, gdy uczciwy węzeł równorzędny zobaczy prawidłowy, ściśle dłuższy łańcuch, przełączy się z obecnego rozwidlenia na dłuższy. DPoS jest w stanie kontynuować i działać nawet wtedy, gdy większość producentów zawiedzie. Rysunek pokazuje rozwidlenie mniejszościowe, gdzie partner 2 może umieścić najdłuższy łańcuch tylko raz w cyklu.



Podczas procesu niepowodzenia społeczność może głosować i zastępować uszkodzonego producenta równorzędnego, w tym przypadku równorzędnego 1 lub równorzędnych producentów, dopóki sieć nie powróci do normalnego działania.

Niniejsza biała księga szczegółowo opisuje ten proces i sposób działania bloków produkowanych i zasady obsługi łańcuchów awarii: https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper. Ustanowienie społeczności producentów bloków i zainteresowanych użytkowników, którzy zgadzają się na te zestawy reguł, zapewnia wydajność PoS przy zdecentralizowanym sposobie działania PoW. DPoS wykorzystuje uprawnienia interesariuszy do zatwierdzania głosowania zasad algorytmu konsensusu, takich jak opłaty motywacyjne, interwały blokowe, widelce i rozmiary transakcji. Wybrani delegaci mogą doprecyzować te zasady. Ten rodzaj konsensusu może znacznie skrócić czas transakcji (1 sekunda w porównaniu do 10 minut dla PoW). Ponadto protokół konsensusu ma na celu ochronę wszystkich uczestników przed niepożądaną ingerencją grupy węzłów, jak to możliwe w POW. Przykładami popularnych łańcuchów bloków DPOS są

Bitshares, Steem i EOS.

Warstwa górnicza

To, co górnicy robią za kulisami w sieciach, można opisać jako konkurencję o wykonanie pracy blockchain, co jest naprawdę prowadzeniem księgowości sieciowej. W przypadku bitcoinów i większości monet, które wykorzystują PoW, każdy peer musi posiadać całą księgę publiczną, która zawiera zapis wszystkich transakcji, które kiedykolwiek zostały przeprowadzone. Koparki PoW opierają się na mocy obliczeniowej i pulach, podczas gdy inne sieci biorą pod uwagę inne względy. W przypadku bitcoina transakcje muszą zostać zweryfikowane przez górników, którzy sprawdzają księgę, upewniają się, że nadawca nie przekazuje środków, których nie ma, a dopiero potem dodają transakcję do księgi. Wreszcie, aby zapewnić ochronę przed hakerami, górnicy zamykają te transakcje pod wieloma warstwami pracy obliczeniowej, co wymaga zbyt wiele pracy dla hakera. Ta usługa jest nagradzana dostarczaniem bitcoinów jako opłaty dla górnika. W przypadku bitcoina wielkość każdej partii monet spada o połowę mniej więcej co cztery lata; około 2140 roku (chyba, że odkryte zostaną szybsze obliczenia niż SHA2), zostanie ono zredukowane do zera, a całkowita liczba bitcoinów w obiegu wyniesie 21 milionów.

Warstwa propagacji

Warstwa propagacji jest odpowiedzialna za decydowanie o tym, jak współdzielona księga i bloki są przesyłane w sieci P2P. Ta warstwa jest szczegółowo opisana w oficjalnych dokumentach dotyczących blockchain. Każdy z peerów może przesłać nową transakcję do innych węzłów w sieci. Ta architektura umożliwia węzłom komunikację pośrednią. Na przykład możesz wysłać transakcję dotyczącą dwóch portfeli bez bezpośredniego połączenia każdego portfela. Każdy węzeł, który otrzyma prawidłową transakcję, której wcześniej nie widział, natychmiast przekaże ją do wszystkich innych węzłów, z którymi jest połączony. Jest to technika propagacji znana jako powódź. W ten sposób transakcja szybko rozprzestrzenia się w sieci P2P, docierając do dużego procentu węzłów w ciągu kilku sekund.

Warstwa semantyczna

Warstwa semantyczna dba o to, jak nowe bloki odnoszą się do poprzednich bloków i zapewnia protokół weryfikacji reguł konsensusu. Jak widać, istnieją różne rodzaje mechanizmów konsensusu w zależności od liczby podłączonych zaufanych maszyn, stakowania, szybkości, mocy mieszającej i innych, ale działają one podobnie do tego, jak nowe bloki są powiązane z poprzednimi blokami, aby zapewnić bezpieczeństwo. Każdy blockchain ma specyfikacje. W tej warstwie transakcje mają miejsce, gdy monety/tokeny są przesyłane między kontami. Omówiłem najlepszy łańcuch bloków i sposób, w jaki każdy blok zawiera dane, a łańcuch bloków ma odniesienia do każdego bloku poprzedzającego go bloku. Konsensus w łańcuchu bloków zawiera te same bloki w ich zwalidowanym najlepszym łańcuchu bloków i podlega tym samym regułom (reguły konsensusu). W ten sposób blockchain zapewnia bezpieczeństwo.

Warstwa aplikacji

Ta warstwa zajmuje się wdrażaniem aplikacji na szczycie łańcucha bloków. Na przykład dappy, inteligentne kontrakty, giełdy i witryny, które dostarczają informacji o łańcuchu bloków, to aplikacje zbudowane na łańcuchach bloków. W warstwie aplikacji blockchain musi ujawniać interfejsy API. Różne łańcuchy bloków są podobne, ponieważ wszystkie umożliwiają klientowi komunikację z siecią. Bitcoin oferuje pełny węzeł, który obecnie ma około 27 GB i zawiera w pełni wymuszony węzeł i wszystkie zasady blockchain. Jest to potrzebne do wydobywania, a także do upewnienia się, że uruchamiany peer, który łączy się z warstwą aplikacji, jest zsynchronizowany z najnowszymi blokami. Te pełne węzły przyczyniają się do funkcjonalności sieci P2P i pomagają wspierać sieć i jej bezpieczeństwo. Często blockchain oferuje również „lekką" wersję węzła. W rzeczywistości klient bitcoin light odwołuje się do zaufanej kopii pełnego węzła łańcucha bloków. Lekki klient pozwala użytkownikom na interakcję z łańcuchem bloków bitcoina oraz dokonywanie i potwierdzanie transakcji bez angażowania dużej przestrzeni dyskowej 27 GB, co pomaga mniej wydajnym urządzeniom, takim jak telefony komórkowe. Ważne jest, aby zrozumieć, że lekki klient jest godny zaufania i nie obejmuje wszystkich zasad konsensusu. Pełny węzeł jest bez zaufania i odrzuca bloki, które naruszają zasady konsensusu, nawet jeśli wszystkie inne węzły w sieci uznają transakcję za prawidłową. wykorzystał NEO jako przykład popularnego blockchaina PoS. NEO dostarcza również NEO-CLI, który zawiera API obsługujące funkcję konsensusu, która może być używana w warstwie aplikacji. Podobnie delegowany dowód stawki EOS zapewnia opcję pełnego i lekkiego węzła. Zaczniesz zauważać, że chociaż istnieje wiele opcji blockchain, istnieje wiele podobieństw w sposobie implementacji blockchain.

Streszczenie

Tu położyliśy fundamenty i wyjaśniliśmy podstawowe pojęcia dotyczące blockchain; Wyjaśniono pojęcia takie jak szyfrowanie i deszyfrowanie, kryptografia, zasoby cyfrowe, kryptografia i kryptowaluta. Omówiono elementy, które składają się na blockchain, w tym bloki, podwójne wydatki, kryptowalutę, wydobywanie kryptowalut, kryptokoparki i portfele kryptowalut. Omówiono różne rodzaje kryptowalut: bitcoin, tokeny i altcoiny. Na koniec omówiono sieć blockchain P2P i różne warstwy, które tworzą sieć: warstwę konsensusu, warstwę górniczą, warstwę propagacji, warstwę semantyczną i warstwę aplikacji. Poznałeś także logikę rdzenia sieci peer-to-peer i dowód pracy (PoW), dowód stawki (PoS) i delegowany dowód stawki (DPOS). Przedstawiono wiele terminów, które będą przydatne, takie jak zasoby cyfrowe, klucze publiczne i prywatne, zdecentralizowane, podwójne wydatki, inteligentne kontrakty i HODL.