Politechnika Wrocławska

Wydział Elektroniki, Fotoniki i Mikrosystemów

KIERUNEK: Automatyka i Robotyka (AIR)

PRACA DYPLOMOWA INŻYNIERSKA

TYTUŁ PRACY:

Uwierzytelnianie w systemie IoT za pomocą technologii Blockchain

AUTOR:

Bartosz Piech

PROMOTOR:

dr inż. Wojciech Domski, K29W12ND02

WROCŁAW 2021

Pragnę podziękować dr inż. Wojciechowi Domskiemu za cenne rady oraz wskazówki, które pomogły mi w rozwijaniu niniejszej pracy.

Składam również podziękowania moim rodzicom Basi i Krzysztofowi za to, że wspierali mnie podczas całego procesu kształcenia.

Spis treści

Rozdział 1

Wstęp

1.1 Wprowadzenie

Powstanie Internetu spowodowało gwałtowny wzrost ilości wymienianych danych pomiędzy ludźmi na całym świecie. Jest to narzędzie, które pomogło cywilizacji pokonać bariery odległościowe podczas komunikacji międzyludzkich.

Aktualnie większość populacji używa Internetu na co dzień, często nawet nie będąc tego w pełni świadomymi. Internet stał się już dobrem ogólnodostępnym, źródłem informacji dla wielu ludzi, pozwala w szybki sposób uzyskać szczegółowe wiadomości na każdy temat. Jego użytkownicy spędzają godziny używając mediów społecznościowych lub portali streamingowych zapewniających rozrywkę w wolnym czasie. Dzięki aplikacjom telekonferencyjnym oraz technologii VoIP (z ang. *Voice over Internet Protocol*), Internet umożliwił wprowadzenie nauki zdalnej podczas globalnej pandemii dla uczniów w wielu krajach, dzięki czemu byli w stanie kontynuować swoje kształcenie. Pracodawcy dostrzegli możliwość przeniesienia całej infrastruktury biurowej do przestrzeni wirtualnej, pozwoliło to na ciągłość w rozwijaniu projektów przy zachowaniu zasad bezpieczeństwa podczas trwającej na całym świecie pandemii. Pozwoliło to również na zaoszczędzenie czasu, który pracownicy poświęciliby na dojazdy do miejsc pracy. Zwiększony przesył (wrażliwych) danych był powodem do poprawienia zabezpieczeń w wielu firmach.

Stworzenie tego systemu stało się kamieniem milowym w rozwoju cywilizacji, spowodowało powstanie wielu dziedzin pochodnych, takich jak: bankowość elektroniczna, kryptowaluty, czy Internet Rzeczy. Aby każdy z tych systemów mógł prawidłowo funkcjonować, należy go dobrze zabezpieczyć.

Bankowość elektroniczna używa szyfrowanych połączeń, maskowania haseł, oraz uwierzytelniania dwuskładnikowego przy pomocy innego urządzenia, najczęściej telefonu komórkowego. Do zapewnienia autentyczności oraz zwiększenia prywatności coraz więcej osób używa podpisów elektronicznych, profilów zaufanych, bądź kluczy PGP, których działanie jest oparte o podpisy cyfrowe. Pozwalają one dodatkowo wykryć zmiany dokumentu lub wiadomości po podpisaniu pliku przez autora. Aby podpis cyfrowy był poprawny, wykorzystuje się asymetryczne metody kryptograficzne działające w oparciu generowanie par kluczy dla użytkownika – publicznego oraz prywatnego. Stworzenie podpisu cyfrowego polega na wyliczeniu skrótu (z ang. *hash*) wiadomości, następnie zaszyfrowaniu go przy użyciu klucza prywatnego, dzięki temu przy odszyfrowaniu skrótu z pomocą klucza publicznego można w prosty sposób zweryfikować, czy podpis cyfrowy należy do danej osoby. Posiadanie klucza publicznego przez użytkownika umożliwia otrzymywanie zaszyfrowanych wiadomości, dzięki kluczowi prywatnemu można je deszyfrować. Fakt, że klucz prywatny znajduje się najczęściej bezpośrednio na komputerze użytkownika powoduje,

że jest chroniony tylko przez wewnętrzne metody zabezpieczeń na komputerze, najczęściej hasło, oprogramowanie antywirusowe oraz zaporę sieciową (z ang. *firewall*), co może potencjalnie wprowadzić dodatkowe możliwe luki w zabezpieczeniach, na przykład gdy oprogramowanie jest nieaktualne.

Kryptowaluty również bazują na kryptografii klucza publicznego, która pozwala na dokonywanie transakcji pomiędzy rachunkami. Każda transakcja posiada adres odbiorcy – jej klucz publiczny. Główną strukturą używaną w implementacji kryptowalut jest łańcuch bloków przechowujący dziennik wszystkich wykonanych transakcji.

Przeciwwagą dla kryptografii asymetrycznej jest Kerberos, czyli protokół uwierzytelniania oparty na protokole kluczy symetrycznych. Nie występuje w nim wymiana kluczy pomiędzy urządzeniami znajdującymi się w sieci, zamiast tego zaufany serwer po uwierzytelnieniu generuje tymczasowe klucze maszynom znajdującym się w sieci, aby te mogły komunikować się między sobą. Zaletą kryptografii symetrycznej jest jej szybkość. Nie bez powodu przy wykorzystaniu kryptografii asymetrycznej szyfruje się jedynie skrót wiadomości. Jednak aby protokół mógł funkcjonować, serwer musi być dostępny przez cały czas działania systemu, jednocześnie jest on punktem wysokiego ryzyka w sieci.

Internet ciągle się rozwija, dzięki czemu powstają nowe technologie. Blockchain [11] ustanowił innowację w przechowywaniu danych w sposób rozproszony. Używanie systemów rozproszonych niesie za sobą wiele zalet [5]. Pozwala to na łatwiejsze skalowanie systemu, umożliwia zredukowanie kosztów utrzymania oraz zapewnia większą niezawodność, gdyż dane są przetrzymywane na wielu urządzeniach jednocześnie.

Blockchain jest technologią, która została opracowana w latach 90. XX wieku. Opiera się na niej architektura najbardziej znanej kryptowaluty, czyli Bitcoina. Blockchain umożliwia przetrzymywanie danych rozproszonych na wielu urządzeniach. Pozwala to na zachowanie niezmienności danych, dane mogą być tylko dodawane na koniec łańcucha bloków. Ta struktura danych składa się z bloków zawierających dane podzielone na nagłówek, który zawiera skrót poprzedniego bloku i znacznik czasowy powstania, oraz ciało bloku przetrzymujące resztę danych, w przypadku kryptowalut jest to zbiór wykonanych transakcji. Nagłówek stanowi część tworzącą drzewo skrótów, w którym każdy element obliczany jest przy użyciu wartości skrótu przodka. Przy zastosowaniu takiego rozwiązania podczas budowy sieci rozproszonej można wykryć czy dane przechowywane w łańcuchu bloków są poprawne oraz czy były modyfikowane. Blockchain przypomina listę jednokierunkową z tą różnicą, że możliwe jest tylko dodawanie elementów na jej końcu.

Dodawanie nowych bloków do łańcucha może odbywać się na wiele sposobów. Kryptowaluty oparte na publicznych sieciach Blockchain nie mają ograniczeń dostępu, dlatego każdy użytkownik może wykonywać transakcje oraz brać udział w ich uwierzytelnianiu. Do tego najczęściej używa się metod „Proof of Work" lub „Proof of Stake", używając mocy obliczeniowej sieci komputerowe rozwiązują różne zadania, dzięki którym zdobywają wynagrodzenie, walutę, której bloki uwierzytelniają.

Innym rodzajem są prywatne łańcuchy bloków [9], dostęp zewnętrznych użytkowników do takiej sieci jest ograniczony, a urządzenia uwierzytelniające dodawanie kolejnych bloków są wybierane przez administratorów. Przypomina to rozproszoną bazę danych i ma zastosowanie w zamkniętych instytucjach, firmach, czy sieciach prywatnych, gdzie najczęściej przetrzymywane są poufne dane, które nie powinny być udostępniane publicznie.

Zaletami stosowania technologii Blockchain jako rozproszonej bazy danych są: przejrzystość – każdy użytkownik sieci ma dostęp do danych znajdujących się w łańcuchu, bezpieczeństwo – oszuści nie mogą zmienić danych w łańcuchu, samodzielność – uwierzytelnianie nowych bloków może być przeprowadzane za pomocą różnych metod, nie trzeba polegać na scentralizowanych systemach.

Do wad Blockchainu można zaliczyć reduntantność danych. Każdy węzeł przechowuje kopię całej struktury danych, przez co złożoność pamięciowa takiego rozwiązania jest bardzo wysoka w porównaniu do klasycznych rozwiązań (baz danych). Kolejną wadą jest zwiększone zużycie energii w rozwiązaniach „Proof of work", pracujące urządzenia rozwiązując kryptograficzne zadania obliczeniowe używają najczęściej algorytmów typu „brute force".

1.2 Teza pracy

Celem projektu jest zapoznanie się z nowymi technologiami, takimi jak Blockchain, Internet Rzeczy, oraz poznanie różnych metod uwierzytelniania.

Projekt obejmuje połączenie technologii opartych na działaniu Internetu, uwierzytelniania za pomocą technologii Blockchain dla urządzeń działających w sieci Internetu rzeczy.

Celem pracy jest pokazanie, że możliwe jest stworzenie systemu Internetu Rzeczy przy użyciu technologii Blockchain do uwierzytelniania węzłów w sieci.

Rozdział 2

Internet Rzeczy

Komputery od samego ich powstania są zależne od ludzi. Są to urządzenia wykonujące zadany zbiór instrukcji przechowywanych w pamięci wewnętrznej, zapisujące dane i wyniki operacji na rejestrach, następnie są umieszczane w pamięci głównej (z ang. *Random Access Memory*). Przed powstaniem terminali, urządzeń wejścia/wyjścia, pozwalających na wprowadzanie danych w prosty sposób, używano papierowych taśm i kart perforowanych. Spowodowało to duży skok technologiczny w metodach przechowywania i tworzenia danych. Ówcześnie ma to wpływ na każdego człowieka, komputery zmieniły koncept tworzenia i edycji dokumentów. W dzisiejszych czasach używane są edytory tekstu, narzędzia do składania i formatowania dokumentów WYSIWYG (z ang. *What You See Is What You Get*), oraz edytory Online, pozwalające na współpracę wielu osób nad dokumentami. Maszyny do pisania zostały wyparte przez sprzęt elektroniczny, komputery i drukarki.

Rozwój różnego rodzaju czujników spowodował, że zbieranie informacji może odbywać się bez udziału człowieka, który popełnia błędy, ma ograniczony czas, oraz łatwo się rozprasza. Przechwycanie oraz przechowywanie danych pochodzących ze świata zewnętrznego możliwe jest właśnie dzięki Internetowi Rzeczy [1].

Internet Rzeczy tworzą najczęściej urządzenia o niewielkiej mocy obliczeniowej, posiadają one wbudowane czujniki pozwalające na zbieranie oraz przetwarzanie danych pochodzących z otoczenia. Technologia Internetu Rzeczy wykorzystywana jest podczas tworzenia inteligentnych budynków. Pozwala ona na kontrolowanie temperatury w pomieszczeniach, systemów zabezpieczeń, sprzętów gospodarstwa domowego takich jak pralki, lodówki, telewizory, bądź oświetlenie, odczyt i przesył pomiarów z czujników. W skład Internetu Rzeczy wchodzą również urządzenia noszone (z ang. *wearables*). Pozwalają one na monitorowanie funkcji życiowych, takich jak puls, ciśnienie tętnicze, czy saturację krwi. Najbardziej popularnymi urządzeniami noszonymi są inteligentne zegarki (z ang. *smartwatches*). Użycie zaawansowanych technologii pozwala na wykrywanie nieprawidłowości w działaniu narządów wewnętrznych. Pozwalają one na wykrycie stanów zagrażających zdrowiu użytkownika, ponadto zastosowanie magnetometrów i akcelerometrów umożliwia na wykrycie upadku, co z kolei pozwala na lokalizację osoby oraz wczesne wezwanie pomocy w razie wypadku. Zastosowanie urządzeń Internetu Rzeczy pomaga rolnikom w zarządzaniu uprawami. Stacje pogodowe i czujniki umieszczone w glebie pozwalają na monitorowanie stanu roślin i usprawnienie procesu nawożenia upraw. Dodatkowo systemy monitorowania stanu gleby używane są w ogrodnictwie, dzięki czemu można ograniczyć rolę czynnika ludzkiego oraz zautomatyzować rozwój flory.

2.1 Protokoły komunikacyjne

Podstawą działania urządzeń należących do sieci Internetu Rzeczy jest komunikacja pomiędzy węzłami, które są zazwyczaj oddalone od kilku metrów, do kilkudziesięciu kilometrów od siebie. Dlatego powstały różne protokoły komunikacyjne [12], pozwalające na dobranie odpowiedniego narzędzia do konkretnych potrzeb. Najważniejszymi wymaganiami podczas dobierania technologii sieciowej w systemie Internetu Rzeczy jest zasięg oraz przepustowość. Im większa odległość dzieląca urządzenia, tym mniejsza prędkość transmisji. Wiąże się to również z pasmem przenoszenia, protokoły działające na większych częstotliwościach pozwalają na większy przesył danych, kosztem zwiększonego poboru energii oraz tłumienia sygnału.

Protokoły komunikacyjne można podzielić ze względu na zasięg, jaki oferują. System komunikacji bezprzewodowej dalekiego zasięgu LoRa (z ang. *Long Range*), Sigfox, sieć komórkowa GSM (z ang. *Global System for Mobile Communications*) oraz przesył pakietów za pomocą techniki GPRS (z ang. *General Packet Radio Service*) należą do protokołów dalekiego zasięgu (odległości ponad 100km), technologia Bluetooth i sieci Wi–Fi pracują na odległościach rzędu kilkudziesięciu metrów, RFID (z ang. *Radio Frequency IDentification*) i NFC (z ang. *Near Field Communication*) działają w przypadku odległości od kilku centymetrów do kilku metrów.

Często wykorzystywanym protokołem podczas implementacji sieci Internetu Rzeczy jest LoRaWAN, charakteryzuje się względnie małą szybkością transmisji danych, na poziomie kilku $\frac{kb}{s}$, lecz dużym, zazwyczaj kilkunastokilometrowym zasięgiem. Charakteryzuje się bardzo małym zużyciem energii, dzięki czemu pozwala na projektowanie urządzeń mających zasilanie z baterii lub ogniw fotowoltaicznych. Protokół wykorzystruje nielicencjonowane pasmo 868MHz w Europie. Topologia sieci LoRaWAN oparta jest o tzw. rozszerzoną gwiazdę, bramki komunikują się z czujnikami – węzłami końcowymi, a następnie przesyłają odebrane pakiety danych dalej, na przykład na serwer. Ograniczeniem modułów radiowych LoRa jest wysoka cena, z tego względu nie są używane przy projektowaniu budżetowych konstrukcji urządzeń Internetu Rzeczy.

Kolejnym protokołem działającym na dużych odległościach jest Sigfox rozwijany przez francuską firmę o tej samej nazwie. Jest on komercyjnym odpowiednikiem LoRa, różni się typem modulacji przesyłanego sygnału. Wykorzystuje BPSK (z ang. *Binary Phase Shifting Key*) – binarne kluczowanie fazy, która może kodować wartość 0 lub 1, z kolei LoRa używa widma rozproszonego Chirp. Aby uzyskać dostęp do serwisu Sigfox, należy wykupić coroczną subskrypcję. Koszta subskrypcji są zależne od ilości dziennie wysyłanych paczek danych oraz ilości połączonych urządzeń.

Protokół GPRS stanowi alternatywę dla innych rozwiązań dalekiego zasięgu. Oferuje prędkości transmisji na poziomie kilkudziesięciu $\frac{kb}{s}$. Wykorzystuje pasma o częstotliwości 900MHz. Ma rozbudowaną infrastrukturę ze względu na powszechnie używaną sieć telefonii komórkowej do wykonywania rozmów telefonicznych na całym świecie. Urządzenia wyposażone w moduły GPRS używają więcej energii w porównaniu z modułami wyposażonymi w LoRa, bądź Sigfox, dlatego najczęściej stosuje się ten protokół w urządzeniach, które nie potrzebują zasilania bateryjnego.

Technologia Bluetooth jest jednym z najczęściej wykorzystywanych protokołów komunikacji pomiędzy urządzeniami Internetu Rzeczy. Bluetooth można znaleźć w niemal każdym nowoczesnym smartfonie, dzięki temu protokół jest często wykorzystywany w urządzeniach noszonych. Moduły Bluetooth cieszą się popularnością ze względu na niską cenę. Można wykorzystywać je przy przesyle danych pomiędzy węzłami oddalonymi o kilkadziesiąt metrów, przy czym oferują relatywnie dużą prędkość transmisji danych na

poziomie kilku $\frac{Mb}{s}$. Komunikacja poprzez Bluetooth wykorzystuje pasmo częstotliwości 2,4GHz.

Bezprzewodową komunikację z dużą prędkością pomiędzy urządzeniami Internetu Rzeczy umożliwia technologia Wi–Fi. Ponadto oferuje nowoczesne, wbudowane w protokół mechanizmy szyfrowania danych. Jest wykorzystywana w urządzeniach przesyłających duże ilości danych w czasie rzeczywistym, na przykład kamery bezpieczeństwa. Wi–Fi ze względu na dobrą infrastrukturę jest używane w urządzeniach Internetu Rzeczy montowanych w inteligentnych budynkach. Wadą tego rozwiązania jest duże zużycie energii, dlatego powstają moduły o obniżonym poborze mocy, lecz również o obniżonej prędkości przesyłu danych. Komunikacja odbywa się na paśmie 2,4GHz oraz 5GHz.

Technologia RFID umożliwia komunikację pomiędzy czytnikiem oraz etykietą, wyposażoną w antenę. Jest stosowana w logistyce do monitorowania różnego rodzaju produktów, w sklepach używa się etykiet, aby zabezpieczyć produkty przed kradzieżą. Komunikacja bliskiego zasięgu NFC działa w oparciu o technologię RFID, z tą różnicą, że czytniki NFC mogą również działać jako etykiety. Pozwala to na obustronną wymianę informacji. Stosuje się ją przy płatnościach zbliżeniowych.

Rozdział 3

Technologia Blockchain

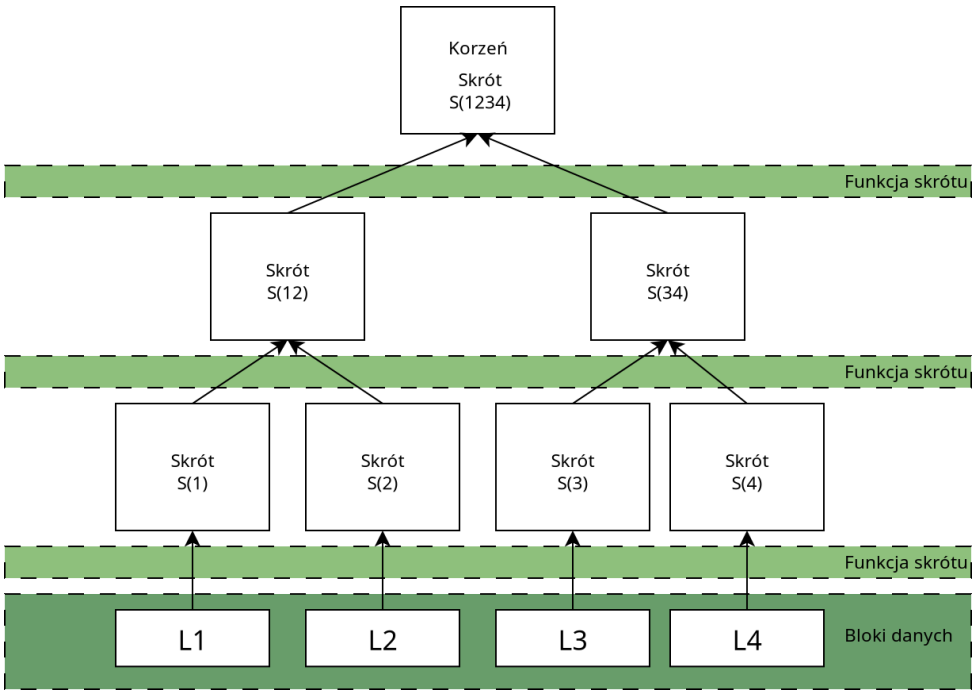
Propozycja opracowania protokołu działającego podobnie do technologii łańcucha bloków została przedstawiona po raz pierwszy przez Davida Chauma w jego pracy doktorskiej [4] z 1982 roku. Technologia zyskała popularność w 2008, gdy została użyta jako główny komponent pierwszej kryptowaluty stworzonej przez osobę, lub grupę osób nazwaną Satoshi Nakamoto. Blockchain zrewolucjonizował sposób, w jaki postrzegana jest dzisiejsza bankowość elektroniczna, transakcje nie muszą odbywać się za pomocą pośredników – korporacji i banków. Wykorzystanie takiego systemu pozwala na uniknięcie prowizji i zmniejszenie kosztów związanych z wykonywaniem transakcji. Waluty fiducjarne (*Fiat*), produkowane przez banki centralne, używane wśród społeczeństwa, w odróżnieniu do walut opartych o technologię Blockchain, są narażone na zniszczenie, próby fałszerstwa oraz kradzież.

Codziennie powstają nowe kryptowaluty (z ang. *altcoins*), umożliwiające handel w rozproszonej sieci, używające technologii łańcucha bloków zawierającego rejestr transakcji, tzw. *ledger*. Ułatwiają wymianę dóbr pomiędzy użytkownikami Internetu, Ich zaletą jest fakt, że zapewniają anonimowość i nie są zależne od żadnych rządów ani instytucji. Są również bardziej przenośne od pieniędzy fiducjarnych, nie muszą być przechowywane w skarbcach ani bankach, zamiast tego cały dziennik płatności umieszczony jest w łańcuchu bloków rozproszonym na wielu urządzeniach. Do wad kryptowalut można zaliczyć fakt, że ich wartość jest zmienna, podobnie do notowań akcji na Giełdzie Papierów Wartościowych. Ponadto najpopularniejsza kryptowaluta – Bitcoin, nie jest skalowalna, wielkość jednego bloku została ograniczona do 1MB. Konsekwencją tego jest wysoki koszt wykonywania transakcji, aczkolwiek to ograniczenie zmniejsza jego rozmiar, co wpływa na zredukowanie kosztów przechowywania oraz transferu całego łańcucha bloków [3]. Poprzez to ograniczenie powstała inna gałąź (z ang. *fork*) nazywająca się „Bitcoin Cash", mająca limit wielkości 8MB. Bitcoin używa znanego algorytmu tworzenia skrótów nowych bloków – SHA256, przez co powstają dedykowane urządzenia ASIC (z ang. *Application Specific Integrated Circuit*), stworzone tak, aby uzyskać jak największą moc obliczania funkcji skrótów (z ang. *hash rate*) z prędkością setek $\frac{TH}{s}$. Skutkiem tego jest powstawanie serwerowni specjalizujących się w „kopaniu" tej kryptowaluty. W ten sposób szanse na dodanie nowego bloku do łańcucha przez zwykłe maszyny, takie jak domowe komputery lub urządzenia Internetu Rzeczy są nikłe i cały system staje się coraz bardziej scentralizowany. Jedynym sposobem na generowanie nowych jednostek waluty Bitcoin jest dodanie bloku do łańcucha przez urządzenie, które poprawnie rozwiąże zadanie „Proof of Work", w nowo powstałym bloku dopisywany jest adres portfela właściciela, który otrzyma nagrodę w postaci nowych Bitcoinów. Osoby odpowiedzialne za rozwój tej kryptowaluty stworzyły ograniczenie w ilości monet możliwych do „wykopania" na 21 milionów

Bitcoinów. Do trzeciego kwartału 2021r. do wydobycia zostało około 2.3 miliona monet. Twórcy tej kryptowaluty zabezpieczyli ją przed inflacją za pomocą mechanizmu zmniejszania wynagrodzenia za odnalezienie nowego bloku o połowę co 210,000 bloków dodanych do łańcucha, czyli ok. co cztery lata. Przewiduje się, że cała pula monet Bitcoin zostanie wyczerpana do 2140r. Po tym czasie wynagrodzeniem za „odnalezienie" nowych bloków będzie prowizja od transakcji pomiędzy użytkownikami.

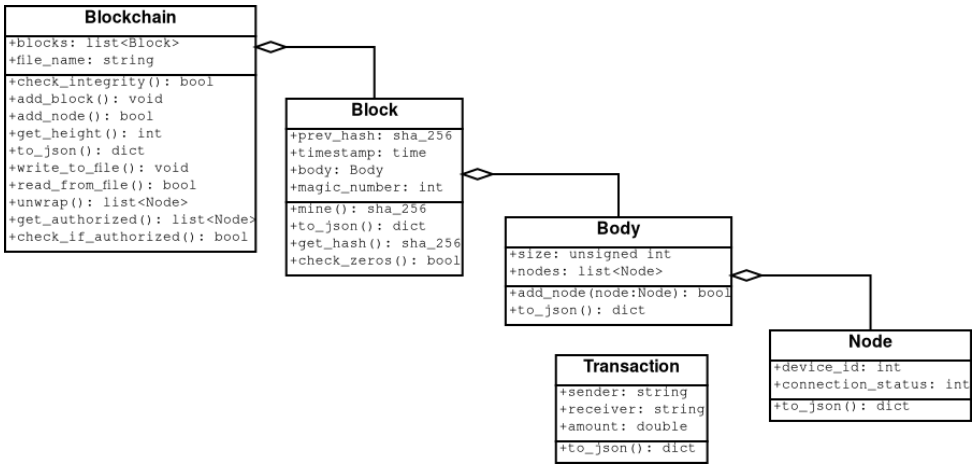
3.1 Definicja

Blockchain stał się przełomowym wynalazkiem, który umożliwia stworzenie systemu, gwarantującego zachowanie integralności danych, oraz pozwala na przechowywanie danych w strukturze łańcucha bloków na wielu urządzeniach. W ten sposób dane są zabezpieczone przed utratą, gdyby jedna kopia łańcucha została zniszczona, inne kopie są przechowywane na wielu urządzeniach jednocześnie. Jest to łańcuch bloków połączonych ze sobą przy pomocy kryptograficznych funkcji skrótu (z ang. *cryptographic hash functions*), które działają jako ochrona przed zmianą danych przechowywanych w aktualnym łańcuchu. Poprzednikiem tej struktury danych jest drzewo skrótów (z ang. *Merkle Tree*), które pozwala na weryfikację niezmienności przechowywanych danych. Korzeń drzewa skrótów umożliwia sprawdzenie poprawności wszystkich potomków (rys. 3.1).



Rysunek 3.1 Schemat drzewa skrótów.

Łańcuch składa się najczęściej z jednokierunkowej listy bloków. Bloki dzielą się na nagłówek oraz ciało, Nagłówek przetrzymuje skrót swojego poprzednika oraz znacznik czasowy powstania (z ang. *timestamp*). Ciało bloku stanowią dane, które ma przechowywać Blockchain. W projektowanym systemie (rys. 3.2) przechowywana jest lista węzłów połączonych do sieci. Każdy węzeł ma swój numer identyfikacyjny, oraz status połączenia. Rozmiar ciała bloku przechowywany jest w zmiennej rozmiar (z ang. *length*), ogranicza dodawanie nowych węzłów do ciała bloku. Po przekroczeniu limitu serwer przeprowadza operację „kopania" bloku. Losuje numer „magiczny" (z ang. *magic number*), następnie za



Rysunek 3.2 Diagram struktury łańcucha bloków.

pomocą funkcji skrótu SHA256 otrzymuje ciąg znaków bloku, sprawdzając czy pierwsze n znaków w zapisie heksadecymalnym skrótu bloku stanowią zera, jeżeli nie – numer specjalny jest losowany na nowo. Gdy blok zostanie wykopany, tworzony jest nowy. Łańcuch bloków umożliwia operacje dodawania nowych transakcji oraz bloków, sprawdzania integralności danych zawartych w łańcuchu, oraz sprawdzania jego wysokości (z ang. *height*). Kryptowaluty używają wysokości łańcucha w celu estymacji czasu istnienia całego Blockchainu, bloki Bitcoina są tworzone co 10 minut, pomnożenie czasu tworzenia pojedynczego bloku przez wysokość łańcucha umożliwia oszacować czas istnienia oraz daty aktualizacji sieci.

3.2 Algorytm konsensusu

Podstawą działania publicznej sieci opartej o technologię Blockchain jest algorytm konsensusu. Stanowi on sposób zabezpieczenia sprawiając, że sieć staje się w pełni zdecentralizowana. Sama technologia łańcucha bloków nie zapewnia decentralizacji sieci, tylko stanowi podstawę w postaci bazy danych. Istnieje wiele typów algorytmów konsensusu, każdy ma swoje wady i zalety. Kluczowym aspektem przy projektowaniu zdecentralizowanej sieci używającej technologię Blockchain jest wybór prawidłowego algorytmu konsensusu, w prywatnych sieciach Blockchain powinny być używane algorytmy ograniczające możliwość uwierzytelniania bloków przez niezaufane węzły, dobrym przykładem takiego algorytmu jest „Proof of Authority". W przypadku sieci publicznych uczestnictwo potwierdzaniu bloków nie powinno być ograniczone, dlatego użycie algorytmu „Proof of Work", bądź „Proof of Stake" jest popularną metodą. Najczęściej używanym algorytmem konsensusu w przypadku kryptowalut jest „Proof of Work". Jest on wykorzystywany między innymi w uwierzytelnianiu bloków w łańcuchu sieci Bitcoin.

Konsensus jest „*porozumieniem osiągniętym w wyniku dyskusji i kompromisu*", ta definicja odnosi się również do technologii Blockchain, niezaufane węzły osiągają porozumienie o stanie danych (łańcucha bloków), dzięki algorytmowi konsensusu. Do osiągnięcia konsensusu [2] wymagane jest: **osiągnięcie porozumienia**, **współpraca pomiędzy stronami**, oraz **niewrażliwość na ingerencję osób trzecich**.

Istniejące algorytmy konsensusu można podzielić na dwa typy: oparte na dowodzie (z ang. *proof-based*), oraz oparte na tolerancji błędów (z ang. *fault tolerance-based*). Działanie metod opartych na dowodzie sprowadza się do wykonania losowego wyboru węzła, który

decyduje o wyglądzie całego łańcucha bloków. Węzły są wybierane na podstawie wykonanej pracy (Proof of Work), posiadanych zasobów (Proof of Stake) bądź posiadanego autorytetu (Proof of Authority).

Algorytmy oparte na tolerancji są mniej skomplikowane niż te opierające się na dowodzie, węzły będące w sieci komunikują się ze sobą (najczęściej w sposób synchroniczny), używając podpisów cyfrowych, aby każdy użytkownik miał pewność kto jest autorem wiadomości. Po przeprowadzeniu komunikacji w określonym oknie czasowym, decyzja jest podejmowana na podstawie większości głosów. Algorytmy te nawiązują do problemu bizantyjskich generałów. Aby sieć używająca algorytmu konsensusu opartego na tolerancji działała prawidłowo, musi posiadać $3m + 1$ aktywnych węzłów, gdzie m stanowi liczbę węzłów złośliwych w sieci. Przykładami takich algorytmów są: praktyczny algorytm bizantyjski toleracji błędów (z ang. *Practical Byzantine Fault Tolerance*), uproszczony algorytm bizantyjski tolerancji błędów (z ang. *Simplified Byzantine Fault Tolerance*), oraz delegowany algorytm bizantyjski tolerancji błędów (z ang. *Delegated Byzantine Fault Tolerance*).

Istnieje wiele typów algorytmów opartych na dowodzie. Są to między innymi:

- „Proof of Work" – dowód wykonanej pracy,
- „Proof of Stake" – dowód posiadanych zasobów,
- „Delegated Proof of Stake" – delegowany dowód posiadanych zasobów,
- „Proof of Authority" – dowód posiadanego autorytetu,
- „Proof of Capacity" – dowód oparty o dostępność zasobów,
- „Proof of Activity" – dowód aktywności,
- „Proof of Burn" – dowód wypalenie,
- „Proof of Weight" – dowód ważonego udziału w posiadanych zasobach.

Dowód wykonanej pracy polega na stworzeniu problemu, który wykorzystuje dużą ilość zasobów obliczeniowych, na przykład znalezieniu rezultatu, jaki daje funkcja skrótu pojedynczego bloku. Skrót zapisany w formacie heksadecymalnym powinien mieć określoną ilość zer na początku, przez co skrót zamieniony na system dziesiętny będzie jak najmniejszą liczbą. Algorytm konsensusu wykorzystujący metodę „Proof of Work" pozwala na zabezpieczenie sieci przed atakami *Sybil*, czyli stworzeniu wielu sztucznych węzłów do uzyskania dużego wpływu. Dowód pracy nie jest podatny na ten atak ze względu na fakt, iż atakujący musiałby posiadać conajmniej 51% zasobów obliczeniowych całej sieci. Jednakże wadą takiego rozwiązania jest znaczne zużycie energii potrzebnej na wykonanie obliczeń. Kolejnym problemem jest centralizacja całej sieci, coraz większe zużycie energi powoduje, że tworzone są ogromne centra danych wyposażone w maszyny o dużych zasobach obliczeniowych pozwalające na zmniejszenie kosztów, a przez to zwiększenie przychodów z „kopania" w sieci.

Kolejnym algorytmem konsensusu jest dowód posiadanych zasobów. Polega na zapewnieniu użytkownikom proporcjonalnej szansy na walidację nowych bloków do posiadanych zasobów. Duża inwestycja ze strony użytkownika sprawia, że działania na szkodę sieci są dla niego nieopłacalne. Proces wyboru węzła weryfikującego jest losowy, lecz bierze pod

uwagę wartość portfela przypisanego do niego. Dowód posiadanych zasobów stanowi również dobre zabezpieczenie przed atakami *Sybil*, ponieważ ich przeprowadzenie byłoby bardzo kosztowne i wymagałoby posiadania dużych zasobów sieci. Nie wymaga on wielkich nakładów mocy obliczeniowej, jest bardziej energooszczędny od „Proof of Work".

Dowód aktywności jest hybrydą algorymu „Proof of Work" oraz „Proof of Stake". Początkowo system używa dowodu wykonanej pracy do osiągania konsensusu, w kolejnych etapach algorytm zmieniany jest na dowód posiadanych zasobów. Taki algorytm pozwala na osiągnięcie wysokiego poziomu bezpieczeństwa z jednoczesnym mniejszym zużyciem energii niż w przypadku „Proof of Work".

Algorytm „Proof of Authority" wykorzystuje wybrane węzły zapewniające konsensus całej sieci. To one mają autorytet i odpowiadają za dodawanie nowych bloków do łańcucha.

3.3 Właściwości

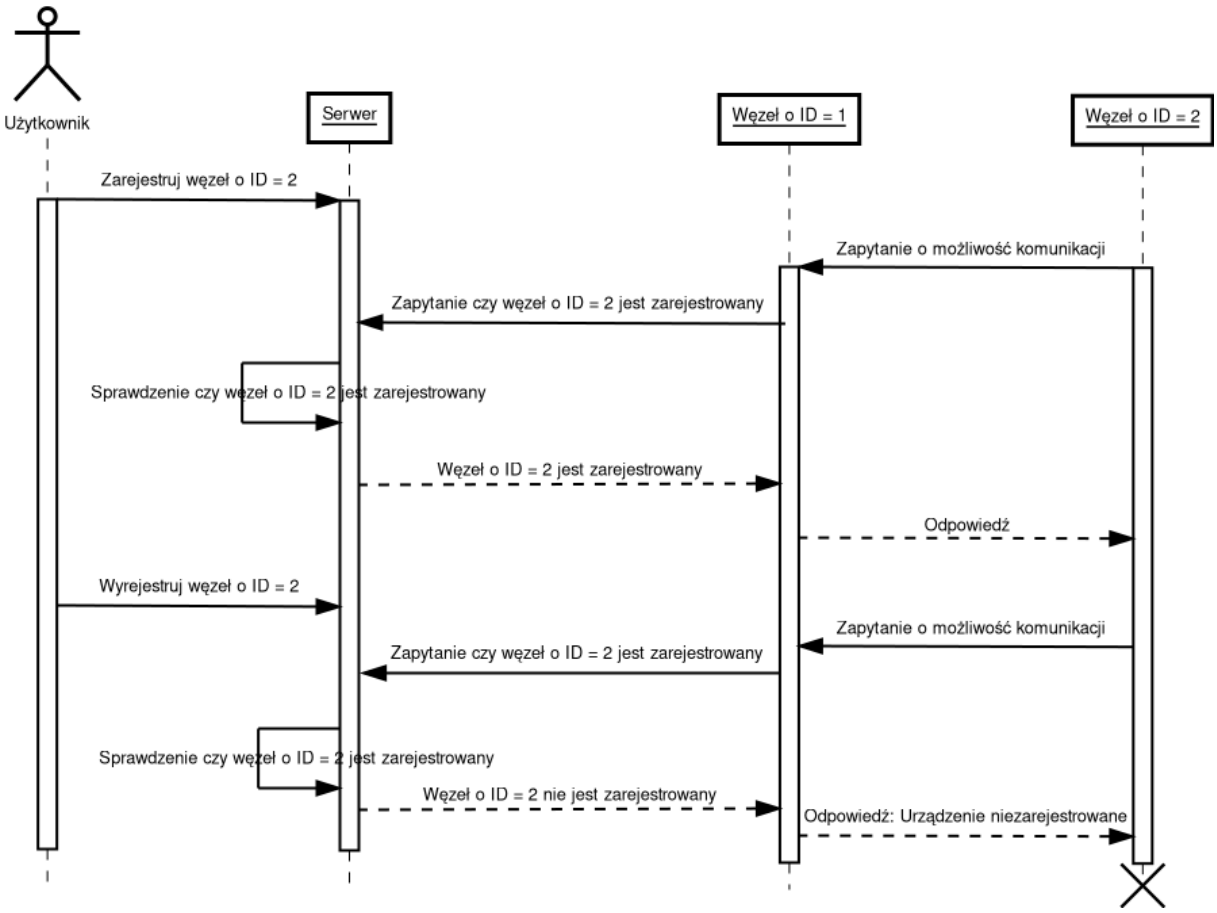
Technologia Blockchain posiada cechy, dzięki którym może być uznawana za doskonałe narzędzie do implementacji systemów rozproszonych. Zdecentralizowane sieci Blockchain umożliwiają dostęp do przechowywanych danych każdemu urządzeniu podłączonemu do sieci. Użycie technologii Blockchain zapewnia bezpieczeństwo danych, użycie metod „Proof of Work", bądź „Proof of Stake" znacząco utrudnia zmianę aktualnych danych przechowywanych w łańcuchu, aby zmienić dane przechowywane w strukturze, należałoby odnaleźć wszystkie skróty bloków znajdujących się w łańcuchu. Blockchain w łatwy sposób umożliwia ukrycie danych użytkowników korzystających z systemu, zastępując je skrótami wygenerowanymi przy użyciu kryptografii, np. asymetrycznych par kluczy.

3.4 Użycie Blockchainu w IoT

Internet Rzeczy jest ciągle rozwijającą się technologią. W połączeniu z łańcuchem bloków umożliwia na stworzenie rozproszonej sieci urządzeń mających dostęp do zdecentralizowanej bazy danych. Zastosowanie Blockchainu w budowie sieci urządzeń Internetu Rzeczy umożliwia na zapisywanie danych odczytywanych z czujników, prowadzenie rejestru zdarzeń, lub stworzenie dziennika urządzeń, które mają dostęp do sieci.

Blockchain pozwala na zdecentralizowanie sieci urządzeń IoT oraz redukcję kosztów poprzez możliwość wyeliminowania centralnej jednostki [10], ponadto dzięki takiemu rozwiązaniu awaria pojedynczego punktu w sieci nie powoduje awarii całego systemu. Sprawia również, że węzły należące do sieci są bardziej anonimowe, zapewnia bezpieczeństwo i możliwość skalowania sieci dzięki wykorzystaniu zasobów wszystkich użytkowników. Zastosowanie tej technologii zwiększa odporność całego systemu przed atakami typu DoS (z ang. *Denial of Service*) oraz man-in-the-middle. Połączenie tych technologii nie jest trywialne, ponieważ zazwyczaj urządzenia IoT dysponują niewielką mocą obliczeniową, a użycie algorytmu „Proof of Work" do zapewnienia konsensusu wymaga dużej mocy obliczeniowej. Dodatkowo „kopanie" nowych bloków za pomocą tej metody jest czasochłonne i może generować opóźnienia w całej sieci.

Ze względu na fakt, że urządzenia wbudowane mają niewielką moc obliczeniową, oraz dysponują ograniczonym miejscem, w projekcie (rys. 3.3) użyto komputera stacjonarnego jako serwera – jednostki centralnej, do której węzły IoT mogą wysyłać zapytania na temat innych urządzeń, dostając odpowiedź od serwera, czy dane urządzenie znajduje się w sieci. Diagram sekwencji 3.3 pokazuje dwie sytuacje: pomyślną komunikację pomiędzy



Rysunek 3.3 Diagram sekwencji sieci Internetu Rzeczy

urządzeniami Internetu Rzeczy po zarejestrowaniu węzła przez użytkownika, oraz błąd w komunikacji, gdy urządzenie zostanie wyrejestrowane z łańcucha bloków.

Rozdział 4

Architektura programowa urządzeń Internetu Rzeczy

Aby urządzenia wbudowane z systemem operacyjnym współpracowały ze sobą, muszą posługiwać się protokołem komunikacyjnym. Przy wyborze protokołu należy kierować się czynnikami takimi jak: wielkość pakietu czy możliwość retransmisji. Komunikacja pomiędzy urządzeniami Internetu Rzeczy jest ważnym czynnikiem, pozwalającym na odbieranie informacji zbieranych z otoczenia, wykonywanie obliczeń na wielu urządzeniach, czy sterowanie urządzeniami zewnętrznymi. Do prowadzenia komunikacji pomiędzy urządzeniami w sieci używającej technologii Blockchain wykorzystano bibliotekę ZeroMQ działającą w oparciu o protokół TCP/IP (z ang. *Transmission Control Protocol/Internet Protocol*).

W ekosystemie urządzeń IoT ważne jest, aby podzielić poszczególne moduły, które można traktować później jako osobne urządzenia [2]. Architektura urządzeń należących do sieci Internetu Rzeczy dzieli się na:

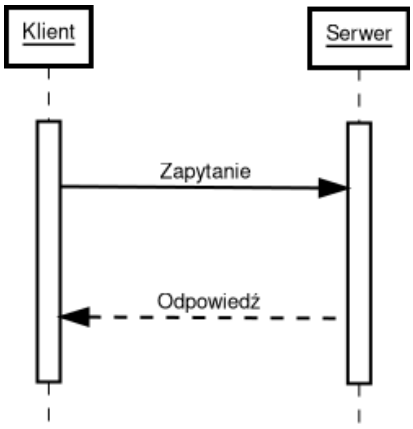
- Warstwa urządzenia (z ang. *Device layer*) jest odpowiedzialna za interakcję z otoczeniem, w tej warstwie znajdują się różnego rodzaju czujniki, siłowniki, zazwyczaj wymagane jest zastosowanie przetwornika analogowo–cyfrowego (z ang. *Analog to Digital Converter*) aby przetworzyć sygnały analogowe odbierane ze świata rzeczywistego na cyfrowe, zrozumiałe dla mikrokontrolerów. Siłowniki i serwomechanizmy pozwalają oddziaływać na otoczenie,

- warstwa sieciowa (z ang. *Network layer*) składa się z różnego rodzaju urządzeń pozwalających na wymianę informacji. Warstwę sieciową można podzielić na dwa typy komunikacji: z człowiekiem lub innymi urządzeniami,

- warstwa zarządzająca (z ang. *Management layer*) wysyła zapytania do serwera dostając w odpowiedzi informację, czy inne urządzenie próbujące nawiązać połączenie z tym urządzeniem jest zarejestrowane w sieci.

4.1 Komunikacja międzyprocesowa przy użyciu gniazd

Gniazda (z ang. *sockets*) zostały opracowane jako interfejs programowania aplikacji do komunikacji internetowej pomiędzy urządzeniami. Gniazda powstały podczas rozwijania systemu Unix BSD na Uniwersytecie Kalifornijskim w Berkeley, dzięki któremu uzyskały swoją nazwę – gniazda BSD. Aby uniknąć reimplementacji tych samych funkcjonalności



Rysunek 4.1 Wygląd wzorca Request – Reply przedstawiony jako diagram sekwencji

bazujących na gniazdach, opracowano bibliotekę ZeroMQ, która rozszerza interfejs programowy gniazd BSD, oraz umożliwia tworzenie aplikacji przy użyciu nowoczesnych języków programowania.

ZeroMQ [7] jest uniwersalną biblioteką, o otwartym kodzie źródłowym, pozwalającą na tworzenie komunikacji pomiędzy urządzeniami. Charakteryzuje się dużą prędkością, możliwością zastosowania wielu protokołów komunikacji, małym rozmiarem, asynchronicznością oraz obszerną dokumentacją. Biblioteka ZeroMQ eliminuje krzywą uczenia się (z ang. *learining curve*), która występuje podczas programowania przy pomocy gniazd BSD. Pozwala również na osiągnięcie wydajności podobnej do gniazd BSD. Ze względu na wymienione cechy biblioteki ZeroMQ zdecydowano się na wykorzystanie jej w projekcie.

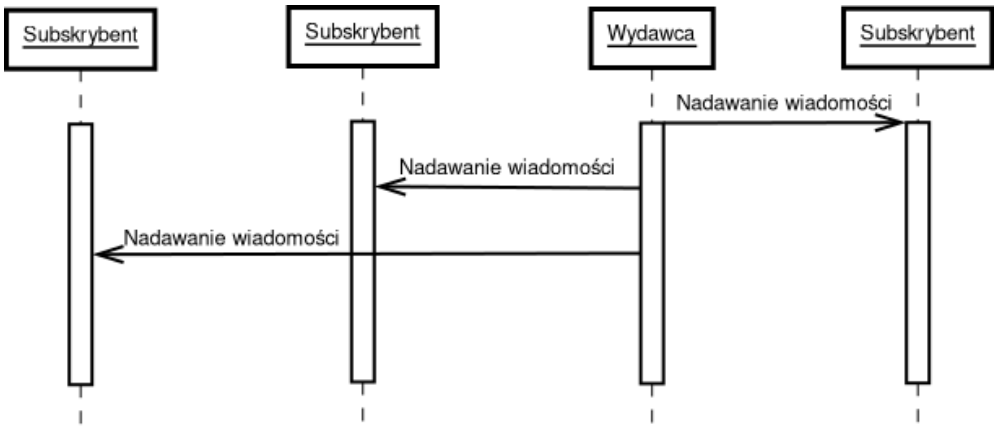
4.2 Wzorce projektowe komunikacji internetowej

Komunikacja pomiędzy urządzeniami IoT przy użyciu biblioteki ZeroMQ może przebiegać na wiele sposobów, dlatego stworzono wzorce projektowe pozwalające na połączenie urządzeń za pomocą gniazd, aby te mogły przesyłać dane między sobą. ZeroMQ w porównaniu do klasycznego protokołu TCP pozwala na rozszerzenie komunikacji między węzłami z jeden do jednego, na jeden do wielu.

Podstawowymi wzorcami projektowymi do komunikacji pomiędzy węzłami w bibliotece ZeroMQ są: Request – Reply, Publish – Subscribe, Push – Pull, oraz „Exclusive Pair". Wszystkie wzorce zostały stworzone w taki sposób, aby umożliwić skalowalność systemu.

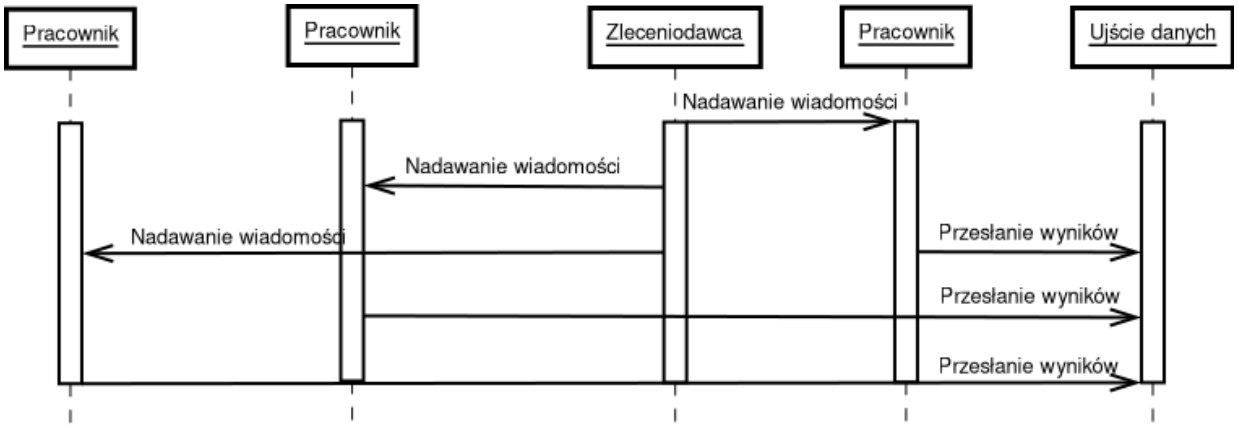
Wzorzec Request – Reply przedstawiony na rysunku 4.1, działa w ten sposób, że serwer nasłuchuje zapytań (z ang. *request*) na wskazanym porcie, odbiera dane w nieskończonej pętli za pomocą funkcji recv(), gdy otrzyma zapytanie, przetwarza je, i wysyła odpowiedź (z ang. *response*) używając zapewnionej przez bibliotekę ZeroMQ funkcji send(). Pozwala to na połączenie urządzeń za pomocą gniazd. Na każde poprawne zapytanie serwer wysyła odpowiedź.

Wzorzec Publish – Subscribe pokazany na rysunku 4.2, pozwala na połączenie urządzeń w trybie jeden do wielu. Gniazda nasłuchują wiadomości wysyłanych na konkretny port protokołu w nieskończonej pętli. Wydawca wysyła wiadomości, które trafiają do każdego subskrybenta. Wadą takiego rozwiązania jest fakt, że podczas ustalania połączenia, pierwsze wiadomości nie dotrą do subskrybenta, ze względu na potrzebę wykonania tzw. „Handshake" – ustalenia parametrów komunikacji. Czas potrzebny do ustanowienia połą-



Rysunek 4.2 Wygląd wzorca Publish – Subscribe przedstawiony jako diagram sekwencji

czenia pomiędzy urządzeniami wynosi około $5ms$, w tym czasie około 5000 wiadomości wysyłanych przez wydawcę nadającego z pełną prędkością $40\frac{Mbit}{s}$ nie zostanie odebrane przez subskrybenta.



Rysunek 4.3 Wygląd wzorca Push – Pull przedstawiony jako diagram sekwencji

Wzorzec Push – Pull swoje działanie opiera na zasadzie „Dziel i rządź", która jest powszechnie wykorzystywana w różnych algorytmach, aby usprawnić ich działanie. Wygląd tego wzorca pokazano na rysunku 4.3. Zleceniodawca (z ang. *ventilator*) wysyła zadania stworzone w taki sposób, aby mogły być wykonywane równolegle. Następnie pracownicy (z ang. *workers*) wykonują równocześnie te zadania, przesyłając wyniki do ujścia danych (z ang. *sink*), które zbiera je równomiernie od każdego pracownika.

4.3 Implementacja serwera

Serwer jest urządzeniem dysponującym większą mocą obliczeniową od węzłów należących do sieci, dlatego za pomocą protokołu TCP/IP komunikuje się z nimi udostępniając informacje o łańcuchu bloków w postaci interfejsu programowania aplikacji (z ang. *Application Programming Interface, API*). Serwer jest skonfigurowany w ten sposób, aby nasłuchiwał zapytań na domyślnym porcie protokołu dla modułu Flask 5000 [6].

Serwer udostępnia następujący interfejs programowania aplikacji:

- **"/api/blockchain"** – ścieżka zwraca informację na temat aktualnego stanu łańcucha bloków w postaci danych w formacie JSON (z ang. *JavaScript Object Notation*). Dzięki temu inne urządzenia są w stanie skopiować Blockchain do swojej pamięci i indywidualnie sprawdzać integralność łańcucha bloków, zapytanie nie modyfikuje łańcucha bloków,

- **"/api/blockchain/height"** – zwraca wysokość łańcucha bloków, czyli aktualną ilość bloków znajdujących się w łańcuchu w postaci liczby całkowitej, zapytanie nie modyfikuje łańcucha bloków,

- **"/api/blockchain/check"** – to zapytanie uruchamia procedurę sprawdzenia integralności całego Blockchainu. Zwraca informację czy łańcuch bloków nie jest naruszony w postaci True/False. Zapytanie nie modyfikuje łańcucha bloków,

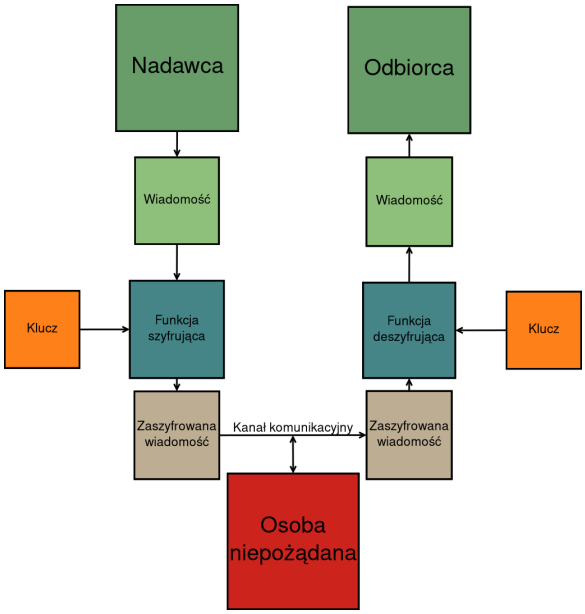
- **"/api/check/<int:device_id>"** – ścieżka zwraca informację, czy dane urządzenie jest zarejestrowane w sieci, aby zapytanie było prawidłowe, w polu device_id należy wpisać identyfikator danego urządzenia. Informacja na temat urządzenia zwracana jest w postaci True/False. Zapytanie nie modyfikuje łańcucha bloków,

- **"/api/logs"** – zwraca informacje o ilości zapytań obsłużonych przez serwer, czasu startu serwera, oraz czasu pracy serwera w sekundach (z ang. *uptime*). Dane zwracane są w postaci pliku JSON, zapytanie nie modyfikuje łańcucha bloków,
- **"/api/open/<int:device_id>"** – sprawdza, czy urządzenie o identyfikatorze device_id jest zarejestrowane w sieci, jeżeli nie, serwer rejestruje dane urządzenie poprzez dodanie do ciała ostatniego bloku węzła z identyfikatorem oraz statusem mówiącym o aktywnym połączeniu. Zwraca status operacji mówiący, czy procedura się powiodła. Zapytanie modyfikuje łańcuch bloków,
- **"/api/close/<int:device_id>"** – jeśli urządzenie o identyfikatorze device_id jest zarejestrowane w sieci, serwer wyrejestrowuje dane urządzenie poprzez dodanie węzła z identyfikatorem device_id oraz statusem mówiącym o nieaktywnym połączeniu. Zwraca status operacji mówiący, czy procedura się powiodła. Zapytanie modyfikuje łańcuch bloków.

Rozdział 5

Metody uwierzytelniania

Kryptografia jest nauką pozwalającą na zabezpieczenie dostępu do poufnych informacji przed nieupoważnionymi osobami. Algorytmy szyfrowania [8] są używane do zmiany danych w taki sposób, aby były bezużyteczne w razie ich przechwycenia przez osoby niepożądane. Funkcje kryptograficzne używane są w zabezpieczeniu systemów opartych o technologię blockchain. Funkcja skrótu pozwala na zachowanie integralności danych, szyfrowanie symetryczne i kryptografia klucza publicznego pozwala na tworzenie transakcji pomiędzy użytkownikami i zapewnienie dostępu do prywatnych zasobów, a podpisy cyfrowe umożliwiają na potwierdzenie tożsamości użytkowników podczas wykonywania operacji w sieci opartej o technologię Blockchain.



Rysunek 5.1 Standardowy model szyfrowania wiadomości

Do przesyłania zaszyfrowanych wiadomości pomiędzy użytkownikami używane są klucze symetryczne lub asymetryczne, na rys. 5.1 pokazano model komunikacji pomiędzy użytkownikami. Kryptografia symetryczna używa takich samych kluczy do szyfrowania i deszyfrowania zawartości, kryptografia asymetryczna tworzy pary kluczy prywatny i publiczny. Wiadomość jest szyfrowana przy użyciu jednego klucza, a deszyfrowana za pomocą jego pary.

5.1 Kryptografia symetryczna

Używanie klucza symetrycznego do szyfrowania i deszyfrowania wiadomości ma zalety, takie jak: szybkość wykonywania, długość takich kluczy wynosi zazwyczaj 128 lub 256 bitów oraz możliwość przesyłania dużych ilości zaszyfrowanych danych. Wadami takiego rozwiązania jest to, że klucz jest współdzielony pomiędzy dwiema stronami, wpływa to na zmniejszenie bezpieczeństwa, ponieważ klucz musi być udostępniony drugiej stronie w bezpieczny sposób. Istnieją metody blokowego szyfrowania danych w sposób symetryczny, to znaczy, że dane są zbierane w bloki o konkretnym rozmiarze, na przykład 128 bitów, następnie informacje są szyfrowane i przesyłane drugiej stronie. Innym sposobem na szyfrowanie symetryczne jest algorytm strumieniowy, szyfrujący oddzielnie każdy bit przesyłanej wiadomości. Taki algorytm używa generatora bitów, oraz elementu dodającego bit wiadomości z bitem wygenerowanym, na przykład operacji bitowej XOR.

5.2 Kryptografia asymetryczna

Kryptografia asymetryczna polega na generowaniu pary kluczy: prywatnego oraz publicznego. Działanie tego algorytmu polega na szyfrowaniu wiadomości przy użyciu jednego klucza, wiadomość deszyfruje się kluczem komplementarnym. Odbiorca i nadawca mając pary kluczy, mogą udostępnić klucze publiczne między sobą, następnie po zaszyfrowaniu danych za pomocą swojego klucza prywatnego, nadawca ponownie może zaszyfrować wiadomość kluczem publicznym odbiorcy, w ten sposób odbiorca po podwójnym odszyfrowaniu wiadomości ma pewność kto jest nadawcą, oraz, że nie została przez nikogo odszyfrowana, pod warunkiem, że nie wyciekły klucze prywatne. Wadą takiego zastosowania jest większa złożoność obliczeniowa, dlatego najczęściej kryptografia klucza publicznego używana jest do szyfrowania jedynie skrótów wiadomości.

Rozdział 6

Testy sieci

Na podstawie działającej sieci urządzeń Internetu Rzeczy wykorzystującej technologię Blockchain przeprowadzono testy sieci. Do napisania serwera operującego na łańcuchu bloków użyto języka programowania Python wraz z modułem Flask. Do stworzenia komunikacji pomiędzy węzłami w sieci posłużyła biblioteka ZeroMQ.

6.1 Efektywność sieci

Stworzona sieć została przetestowana w środowisku laboratoryjnym, gdzie uzyskano średnie wartości liczbowe prędkości poszczególnych operacji. Średnia prędkość pomiędzy węzłami uwierzytelnionymi w sieci wynosi $3.603\frac{kB}{s}$. Jest to bardzo ważny czynnik mówiący ile informacji może zostać przesłane pomiędzy dwoma urządzeniami. Sprawdzanie integralności całego łańcucha bloków zajmuje średnio $11.8\frac{\mu s}{block}$. Przy małych wielkościach łańcucha, na przykład w systemie urządzeń Internetu Rzeczy, sprawdzanie integralności jest operacją natychmiastową, lecz przyjmując wysokość łańcucha kryptowaluty Bitcoin sprawdzenie integralności zajmowałoby każdorazowo kilka sekund. Średnia prędkość dodawania węzłów wynosi $4.23\frac{node}{s}$, podobnie do prędkości usuwania węzłów, która zajmuje $4.82\frac{node}{s}$. Są one wyłącznie zależne od ilości zer wymaganych na początku każdego skrótu i mogą być modyfikowane poprzez zmianę tej wartości.

6.2 Prędkość komunikacji

Pomiędzy dwoma urządzeniami zarejestrowanymi w sieci nawiązano połączenie używając wzorca projektowego Request – Response. Po każdym zapytaniu, węzeł wysyła zapytanie do serwera, który odpowiada czy jego klient jest zarejestrowany w sieci, jeśli tak, wysyła ramkę losowo wygenerowanych danych o temperaturze i wilgotności w pomieszczeniu. Za każdym razem przesłano 1000 ramek danych oraz zmierzono całkowity czas, który upłynął. Wyniki z poszczególnych prób umieszczono w tabeli 6.2. Analizując dane można zauważyć niewielkie odchylenie standardowe czasu, które wynosi $0.11s$.

Na podstawie przeprowadzonych testów wyliczono średnią szybkość komunikacji, która wynosi około $3.603\frac{kB}{s}$. Należy podkreślić fakt, że testy zostały przeprowadzone w środowisku laboratoryjnym, co w znacznym stopniu może odbiegać od rzeczywistych warunków panujących w sieci Internet. Jednakże na potrzeby pracy przytoczona sieć jest adekwatna, ponieważ może być w całości odizolowana od sieci zewnętrznej, co dodatkowo pozytywnie wpływa na bezpieczeństwo przesyłanych informacji.

Numer próby	Ilość przesłanych bajtów	Czas [s]
1	25923	7.312
2	25904	7.115
3	25897	7.046
4	25908	7.208
5	25937	7.276

Tabela 6.1 Dane zmierzone podczas testów prędkości komunikacji

Numer próby	Ilość dodanych węzłów	Czas [s]
1	100	24.012
2	100	27.710
3	100	19.197

Tabela 6.2 Dane zmierzone podczas testów dodawania nowych węzłów do łańcucha bloków

6.3 Sprawdzanie integralności łańcucha

Integralność łańcucha bloków jest kluczowa podczas używania Blockchaina. Jeśli łańcuch bloków był modyfikowany, funkcja sprawdzająca integralność każdego bloku zwróci wartość False, co spowoduje błąd podczas uruchamiania serwera. Czas trwania tej operacji jest liniowo zależny od liczby bloków umieszczonych w łańcuchu. Średni czas potrzebny na sprawdzenie integralności całego łańcucha posiadającego 160 „wykopanych" bloków wynosi około $19ms$. Biorąc pod uwagę, że funkcja sprawdzająca integralność łańcucha wywoływana jest tylko raz po wczytaniu łańcucha z pliku przy uruchamianiu serwera, jest to dopuszczalny wynik.

6.4 Dodawanie węzłów

Dodawanie węzłów do sieci jest operacją wymagającą większej mocy obliczeniowej oraz wykonującą się dłużej niż inne operacje, ponieważ gdy zapełni się miejsce w ciele bloku, należy go „wykopać". Ustalono, że operacja ta wykonuje się tak długo, aż skrót bloku osiągnie 4 zera na początku w zapisie heksadecymalnym. Zmierzono średni czas dodawania węzłów do sieci poprzez uruchomienie skryptu, który dodaje 100 węzłów do sieci. Próbę powtórzono trzykrotnie. Wyniki pokazane w tabeli 6.4 ukazują duże odchylenie standardowe czasu równe $4.26s$. Powodem tego jest duża losowość w „wykopywaniu" bloków. Każdy blok po osiągnięciu zadanej pojemności zostaje „wykopany". To znaczy, że dopóki zadana ilość zer na początku skrótu nie zostanie osiągnięta, inkrementowany jest numer „magiczny", który powoduje zmianę wyniku otrzymanego przez funkcję skrótu. Szansa na wylosowanie bloku jest określana przez ilość zer na początku skrótu bloku.

Na podstawie przeprowadzonych testów wyliczono, że średni czas dodawania nowego węzła do sieci to około $4.23\frac{node}{s}$. Należy mieć jednak na uwadze, że w przypadku dodawania pojedynczego węzła czas ten jest pomijalnie mały w przypadku, gdy blok nie został jeszcze zapełniony.

6.5 Usuwanie węzłów

Usuwanie węzłów jest operacją analogiczną do dodawania, dlatego powtórzono pomiary, tak jak poprzednio dla 100 węzłów. Wyniki otrzymane podczas testów są podobne do

Numer próby	Ilość usuniętych węzłów	Czas [s]
1	100	22.297
2	100	16.491
3	100	23.447

Tabela 6.3 Dane zmierzone podczas testów usuwania będących węzłów z łańcucha bloków

operacji dodawania nowych węzów. Odchylenie standardowe wynosi około $3.72s$ i jest podobne do odchylenia standardowego czasu potrzebnego na dodanie nowego węzła do sieci.

Na podstawie przeprowadzonych testów obliczono średni czas usuwania węzłów $4.82\frac{node}{s}$. Podobnie jak w przypadku dodawania węzłów czas dodawania nowego węzła wydłuża się jedynie, gdy blok zostanie zapełniony.

6.6 Bezpieczeństwo sieci

Stworzona sieć jest odporna na węzły, które nie są zarejestrowane w łańcuchu. Urządzenie otrzymujące zapytanie z próbą komunikacji wysyła zapytanie do serwera, po otrzymaniu odpowiedzi, wysyła odpowiedź do węzła, że urządzenie jest niezarejestrowane zamiast przesłania informacji na temat temperatury oraz wilgotności. Dodawanie węzłów już zarejestrowanych w sieci jest operacją niemożliwą, tak samo jak usuwanie węzłów, które już są nieaktywne. Serwer po każdej modyfikacji łańcucha bloków zapisuje zmiany w formacie JSON w pliku „blockchain.json”. Po uruchomieniu serwera, próbuje on odczytać dane zapisane w pliku. Jeśli blockchain wczytany z pliku jest uszkodzony – integralność bloków nie jest zachowana, serwer nie uruchamia się i zwraca błąd krytyczny. Jeśli plik nie zostanie odnaleziony, tworzony jest nowy łańcuch bloków, do którego dodawane są nowe wpisy o zarejestrowaniu, bądź wyrejestrowaniu węzła z sieci.

Rozdział 7

Podsumowanie

Celem pracy było stworzenie sieci Internetu Rzeczy opartej o technologię łańcucha bloków. Wszystkie cele postawione w tezie pracy udało się zrealizować. Zaimplementowano sieć IoT oraz łańcuch bloków posiadający dane na temat węzłów należących do sieci, stworzono komunikację pomiędzy węzłami, oraz przeprowadzono testy działającej sieci. Wybór języka programowania Python oraz modułów ZeroMQ i Flask znacznie usprawnił rozwój projektu ze względu na fakt, że język ten jest interpretowany oraz zarządzanie pamięcią nie należy do obowiązków użytkownika.

Testy wykonane z użyciem Raspberry Pi 4 uruchomionego w sieci lokalnej jako serwer, oraz komputera stacjonarnego symulującego węzły będące urządzeniami IoT należącymi do sieci wykazały poprawne działanie całego środowiska. Osiągnięte małe prędkości transmisji danych spowodowane są najprawdopodobniej ciągłą potrzebą odpytywania serwera czy dany węzeł należy do sieci. Dodanie pamięci podręcznej (z ang. *cache*) w postaci kilkuminutowych żetonów (z ang. *tokens*) pozwalających na zwiększenie czasu pomiędzy zapytaniami wysyłanymi do serwera umożliwiłoby usprawnienie działania całej sieci oraz przyspieszenie komunikacji pomiędzy węzłami. Uruchomienie węzłów, które nie łączyły się z łańcuchem bloków wykazało znaczący wzrost prędkości przesyłu danych z $3.603\frac{kB}{s}$ do około $163\frac{kB}{s}$.

Projekt w aktualnej postaci funkcjonuje prawidłowo, jednak istnieją możliwości rozszerzenia pracy, takie jak: wprowadzenie algorytmu konsensusu, dodanie większej ilości jednostek centralnych – serwerów operujących na łańcuchu bloków, dodanie interfejsu webowego aplikacji, który pozwalałby na dodawanie/usuwanie węzłów z sieci. Ponadto można przeprowadzić serię ataków na sieć, zebrać dane po takich atakach oraz przeprowadzić analizę otrzymanych rezultatów. Następnie na podstawie tej analizy wdrożyć rozwiązania podnoszące bezpieczeństwo sieci w kontekście przeprowadzonych typów ataków.

Literatura

[1] K. Ashton. That 'internet of things' thing, Jun 2009.

[2] I. Bashir. *Mastering blockchain: A deep dive into distributed ledgers, consensus protocols, Smart Contracts, Dapps, cryptocurrencies, Ethereum, and more*. Packt Publishing, 2020.

[3] Bitcoin Magazine. What is the Bitcoin block size limit?, Aug 2020. `https://bitcoinmagazine.com/guides/what-is-the-bitcoin-block-size-limit`.

[4] D. L. Chaum. *Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups*. University of California, Berkeley, 1982. Praca doktorska.

[5] D. Drescher, L. Sielicki. *Blockchain: Podstawy Technologii łańcucha bloków w 25 Krokach*. Helion, 2021.

[6] R. Haider. *Web API Development With Python, A Beginner's Guide using Flask and FastAPI*. CloudBytes, 2021.

[7] P. Hintjens. *ZeroMQ: Messaging for many applications*. O'Reilly Media, 2013.

[8] R. Mardisalu. Introduction to cryptography: Simple guide for beginners, Oct 2020. `https://thebestvpn.com/cryptography/`.

[9] R. Marvin. Blockchain: The invisible technology that's changing the world, Aug 2017. `https://au.pcmag.com/enterprise/46389/blockchain-the-invisible-technology-thats-changing-the-world`.

[10] A. Rot. *Zastosowanie technologii Blockchain w kontekście bezpieczeństwa rozwiązań Internetu rzeczy*, strony 57–71. Wydawnictwo Politechniki Częstochowskiej, 2018.

[11] M. Swan, M. Lipa. *Blockchain: Fundament nowej gospodarki*. Helion SA, 2020.

[12] D. Tomaszewski. Protokoły komunikacyjne wykorzystywane w systemach IoT, Feb 2020. `https://elektronikab2b.pl/technika/51992-protokoly-komunikacyjne-wykorzystywane-w-systemach-iot`.

Załącznik A

Do pracy dołączono płytę CD zawierającą w poszczególnych katalogach:

- /praca_inzynierska.pdf – wersja cyfrowa pracy,
- /kod_zrodlowy/serwer – kod źródłowy serwera,
- /kod_zrodlowy/serwer/blockchain.json – struktura łańcucha bloków zapisana w formacie JSON.
- /kod_zrodlowy/wezly – kod źródłowy węzłów,