POLITECHNIKA WROCŁAWSKA
WYDZIAŁ ELEKTRONIKI, FOTONIKI I MIKROSYSTEMÓW

KIERUNEK: Automatyka i Robotyka (AIR)
SPECJALNOŚĆ: Robotyka (ARR)

PROJEKT INŻYNIERSKI

Uwierzytelnianie w systemie IoT za pomocą technologii Blockchain

Authentication in IoT using Blockchain technology

AUTOR:
Bartosz Piech

PROWADZĄCY PROJEKT:
dr inż. Wojciech Domski, K29W12ND02

WROCŁAW 2021

To jest przykładowa treść opcjonalnej dedykacji, należy ją zmienić lub usunąć w całości polecenie `\dedication`

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 codzień, 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 (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 Internetu, 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 (internetu) 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 dwupoziomowego 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 (hash'u) wiadomości, następnie zaszyfrowaniu go przy użyciu klucza prywatnego, dzięki temu przy odszyfrowaniu skrótu z pomocą klucza publicznego można w prosty sposób sprawdzić czy podpis cyfrowy należy do danej osoby.Klucz publiczny umożliwia otrzymywanie zaszyfrowanych wiadomości, dzięki kluczowi prywatnemu można je odszyfrować. 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, co wprowadza 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 fakt, iż jest ona odporna na złamanie przez technologię komputerów kwantowych w przeciwieństwie do kryptografii klucza publicznego. Jednak aby protokół mógł funkcjonować, serwer musi być dostępny przez cały czas działania systemu.

Internet ciągle się rozwija, dzięki czemu powstają nowe technologie. Blockchain [3] ustanowił innowację w przechowywaniu danych w sposób rozproszony. Używanie systemów rozproszonych niesie za sobą wiele zalet [1]. 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 do końca 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 [2], 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 (bazy 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 Cel i zakres pracy

Teza pracy

Celem projektu jest zapoznanie się z nowymi technologiami, takimi jak Blockchain, Internet rzeczy, oraz poznanie różnych metod uwierzytelniania. Ponadto rozwój projektu pozwoli pogłębienie wiedzy dotyczącej sieci komputerowych oraz protokołów komunikacyjnych.

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

Proszę jednym zdaniem postawić tezę. Celem pracy jest pokazanie, że możliwe jest .....

Rozdział 2

Internet rzeczy

2.1 Definicja

2.2 Wzorce projektowe komunikacji

ZeroMQ ... ... Publish - Subscribe
Klient - serwer
Push - pull Fan - out Komunikacja między węzłami

Rozdział 3

Technologia Blockchain

3.1 Właściwości

3.2 Użycie Blockchainu w IoT

3.3 Struktura Danych

Rozdział 4

Metody uwierzytelniania

4.1 Wybrana metoda public/private key

Rozdział 5

Testy sieci

5.1 Uwierzytelnianie nowych węzłów

5.2 Prędkość komunikacji

5.3 Dodawanie węzłów

5.4 Usuwanie węzłów

5.5 Kwestie bezpieczeństwa

Rozdział 6

Zakończenie

Bibliografia

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

[2] R. Marvin. Blockchain: The invisible technology that's changing the world, Aug 2017.

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