Politechnika Krakowska im. Tadeusza Kościuszki

Wydział Inżynierii Elektrycznej i Komputerowej

Programowanie w języku Java

Projekt

Zdecentralizowany system transakcji finansowych

Opracowali:

Bodziony Norbert
Cichocki Wojciech
Smalec Bartłomiej

Spis treści

Wstęp

Cele dokumentacji

Dokumentacja pierwszego raport systemu realizowanego w ramach projektu z przedmiotu Programowanie w Języku Java ma na celu wstępne przedstawienie ogólnego opisu produktu, zakresu projektu oraz elementów składowych i funkcji systemu.

Cel projektu

Celem projektu jest stworzenie nowoczesnego systemu płatności opartego o kryptografię, który oferuję możliwość przechowywania i transferu funduszy w sposób bezpieczny i nie wymagający zaufania osób trzecich. Końcowy produkt jest kierowany do współpracujących ze sobą firm, dając im zamknięty system transakcji finansowych. Pragnąc osiągnąć wyższą jakość porozumienia między firmami, realizowany system wychodzi naprzeciw centralnym instytucjom bankowości oferując szybkie, bezpieczne oraz publiczne formy płatności.

Słownik pojęć

Aplikacja portfela	Aplikacja kliencka, pozwala użytkownikowi m.in. na dokonywanie transakcji.
Węzeł sieci	Węzeł sieci jest serwerem zgodne z protokołem sieci. Odpowiada za wszystkie zadania realizowane w procesie przetwarzania transakcji.
Rozproszona baza danych	baza danych istniejąca fizycznie na dwóch lub większej liczbie komputerów, traktowana jednak jak jedna logiczna całość.
Sieć peer-to-peer	Model komunikacji w sieci komputerowej zapewniający wszystkim hostom te same uprawnienia.
Skrót, hash	Unikalny ciąg znaków, który jest wynikiem szyfrowania wejściowego zestawu informacji.
Algorytm kryptograficzny	Jest to funkcja używana do szyfrowania i deszyfrowania.
Łańcuch bloków, blockchain	Zdecentralizowana i stała baza danych działająca w sieci o architekturze peer-to-peer, bez centralnych komputerów i niemająca scentralizowanego miejsca przechowywania danych zakodowana za pomocą algorytmów kryptograficznych.
Blok	Jest pojedynczym komponentem łańcucha bloków. Reprezentuje cyfrowe kodowanie transakcji.
Blok genezy	Jest pierwszym blokiem dodany do łańcucha bloków, posiada początkowe saldo konta.
Sygnatura, podpis cyfrowy	Podpis cyfrowy to matematyczny odpowiednik podpisu fizycznego, wiąże tożsamość właściciela konta z transakcją.
Konsensus	konsensusu, czyli porozumienie, które normuje sposób dodawania informacji w rozproszonym systemie.
Klucz prywatny	służy do cyfrowego podpisywania transakcji, który gwarantuje że treść została zatwierdzona przez właściciela konta.
Klucz publiczny	Reprezentuje adres konta, jest również wykorzystywany do weryfikacji poprawności transakcji.
SHA256	Kryptograficzny algorytm zwracający 256-biotwą wartość skrótu.
GUI	Określa sposobu prezentacji informacji przez komputer oraz interakcji z użytkownikiem.

TCP	Protokół sterowania transmisją operuje w warstwie transportowej. Jest połączeniowy, niezawodny, strumieniowy.
UDP	Protokół warstwy transportowej. Jest bezpołączeniowy oraz nie posiada mechanizmów kontroli przepływu i retransmisji.

Zakres produktu

Zakres działania systemu ogranicza się do zamkniętej sieci łączącej współpracujące firmy. System nie posiada nadrzędnego właściciela, a prawa do niego są współdzielone między kilka firm. Również rozproszony charakter produktu powoduje, że sprzęt działający po stronie serwera jest własnością firmy ale jest częścią wspólnego systemu. Działanie systemu wspiera pracę w zakresie:

- tworzenia oraz zarządzania kontami
- realizacji szybkich transakcji finansowych
- weryfikować poprawność transakcje polegającej na komunikacji między wszystkim węzłami sieci
- pozwalać na wgląd w historię transakcji zrealizowanych w obrębie całej sieci
- posiada zabezpieczenia kryptograficznych gwarantujących niezmienność historii zapisów księgowych
- posiadać oprogramowanie umożliwiające wsparcie w rozbudowie systemu
- pozostawać sprawnym pomimo awarii cześć oprogramowania
- powinien radzić sobie z konfliktowymi transakcjami oraz opierać się złośliwym atakom
- system mimo zdecentralizowanego charakteru ma zachować transparentność

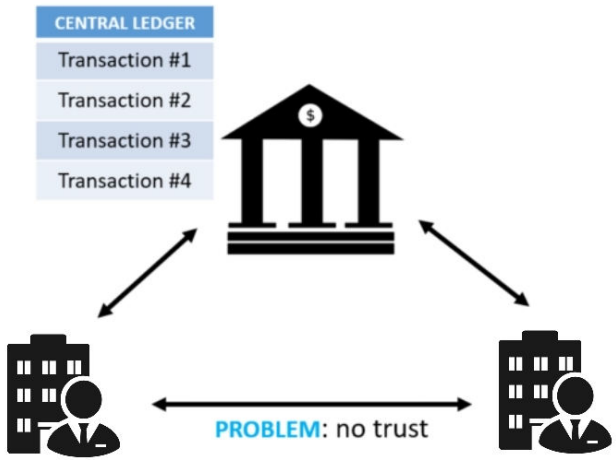
Opis problemu

Charakterystyka użytkowników

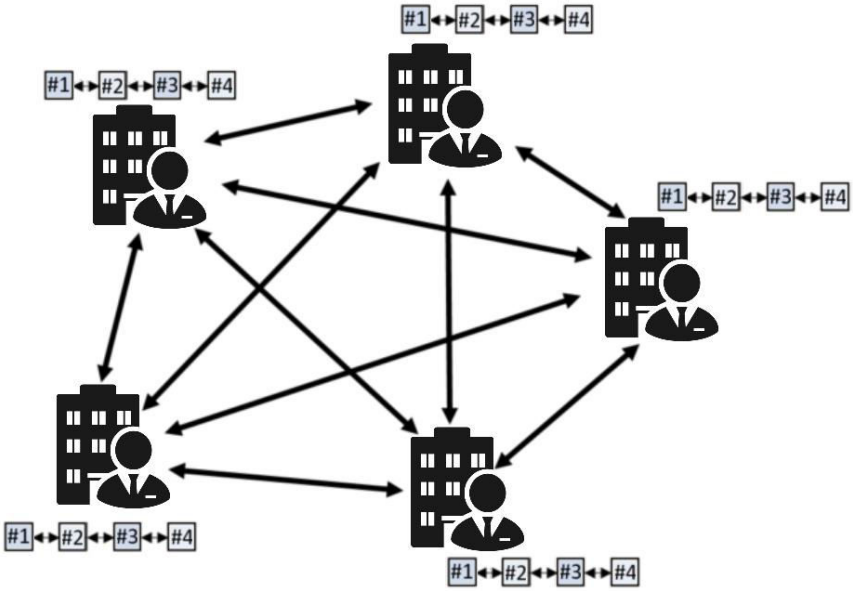
W systemie wyróżnione są dwie grupy użytkowników: administratorzy sieci oraz właściciele konta. Do grupy administratorów sieci należą instancję mające możliwości ingerencji w sieć. Tej grupie użytkowników system oferuje oprogramowanie wspierające działania związane z rozbudową i utrzymaniem sieci oraz kontrolowaniem dostępności serwerów. Oprogramowanie po stronie klienckiej adresowane jest do pracowników firmy. Właścicielem konta może być pojedynczy pracownik, oddział firmy lub być własnością całej firmy. W systemie nie występuje żaden podział użytkowników ze względu na możliwości konta, ponieważ zakłada się że każde konto powinno mieć równorzędne prawa. Z perspektywy właściciela konta system daje możliwość zarządzania kontem, dokonywania transakcji oraz wgląd w księgę transakcji obejmującą całą sieć.

Motywacja do stworzenie rozproszonego systemu

Przedstawiony opis problemu ujawnia zalety oraz motywację do zaprojektowania systemu opartego na rozproszonej architekturze. Poniżej znajduję się analiza dwóch form płatności elektronicznej.



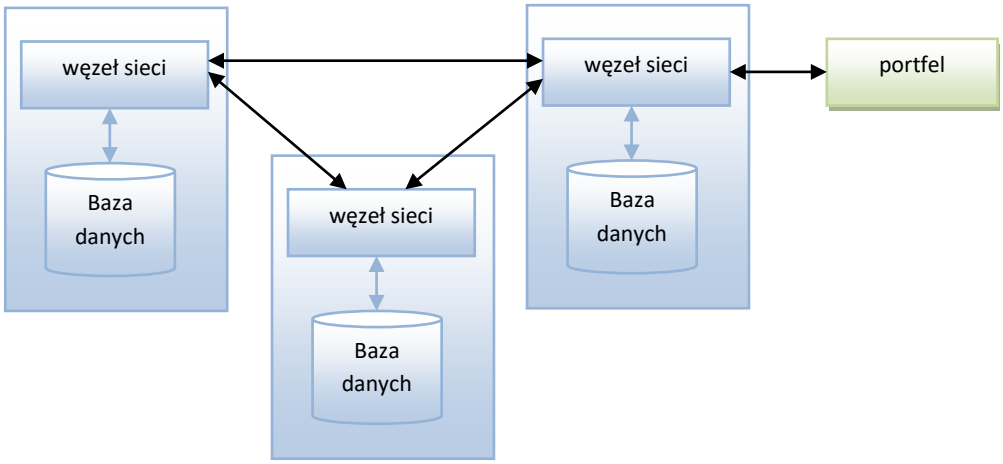
Pierwsze przykład przedstawia porozumienie między firmami, które odbywa się przez pośredniczący, zaufany system. System jak na przykład bank posiada bazę danych ze scentralizowaną księgą transakcji. W tym przypadku problem nieufności rozwiązuje pośredniczący system. To podejście ukazuje kilka wad. Po pierwsze transakcję są obarczone dodatkowe koszty związane z udziałem pośredników. Co więcej istnie centralnego podmiotu w systemie powoduje, że jest bardziej narażony na ataki. Problemem jest również brak możliwości ingerencji w system.



W drugim przypadku przedstawiony jest zdecentralizowany system transakcji finansowych. W tej sytuacji operacja finansowa jest dokonywana bezpośrednio między użytkownikami, przy czym niezawodnością operacji jest gwarantowana przez technologię użytą w systemie. W tej architekturze nie występuje centralny podmiot, przeciwnie wszystkie transakcje wymagają komunikacji w sieci indywidualnych hostów wspólnie uzgadniających aspekty wdrążenia i stosowania protokołów. Użycie bezpośredniej formy transakcji oferuję znaczne zwiększoną szybkość oraz zminimalizowany koszt, dzięki wykluczeniu pośredników. Użycie technologii łańcucha bloków opartego na kryptografii powoduje zwiększenie bezpieczeństwa, ponieważ każda operacja jest weryfikowana przez wszystkich uczestników sieci. Również architektura sieci oraz brak nadrzędnego właściciela przyczynia się do zauważalnego zwiększenia skalowalności całego systemu.

Opis elementów składowych systemu

Ogólny schemat systemu



Portfel

Cały system podzielony jest na dwie części: kliencką oraz serwerową. Część kliencka oparta jest na aplikacji portfela, który umożliwia dokonywanie operacji finansowych oraz wszystkich działań związanych z zarządzaniem kontem. Każdy użytkownik ma również dostęp do pełnej historii dokonanych płatności w obrębie całej sieci. Użytkownik wykorzystując ten sam proces portfela będzie mógł kontrolować wiele kont.

Węzeł sieci

Częścią oprogramowanie działającego po stronie serwera są węzły, czyli komunikując się maszyny zgodne z protokołem sieci. Każdy węzeł sieci posiada własną bazę danych przechowującą konta użytkowników oraz niemodyfikowalną księgę dokonanych transakcji. Do zadań węzłów należy weryfikacja, przetwarzanie oraz akceptacja transakcji. W procesie dokonywania dowolnej transakcji udział biorą wszystkie węzły, które między sobą wymieniają decyzję dotyczącą poprawności transakcji. Zabieg ten ma na celu osiągnięcie konsensusu, czyli porozumienie, które normuje sposób dodawania informacji w rozproszonym systemie. Algorytm osiągnięcia konsensusu jest główną mechanizmem pozwalającym na odejście od scentralizowanego systemu i sposobem na osiągnięcie spójności w rozproszonej bazie danych. Dodanie jakiejkolwiek transakcji jest możliwa tylko i wyłącznie w momencie, gdy węzły dojdą do zgody, iż transakcja jest prawidłowa.

Konto

Z kontem związane są dwie wartości: klucz publiczny oraz klucz prywatny. Publiczny klucz, zwany również adresem, jest udostępniany innym uczestnikom sieci, a klucz prywatny jest trzymany w tajemnicy, przechowywany na lokalnej maszynie oraz nigdy nie zostaje przesłany przez sieć. Jeden użytkownik może kontrolować wiele kont, ale tylko jeden adres publiczny może istnieć dla jednego konta.

Blok

Pojedynczy blok odnosi się do cyfrowego kodowania transakcji. Transakcje są podpisywane przez klucz prywatny należący do konta, na którym przeprowadzana jest transakcja. Podpisany cyfrowo pakiet danych gwarantuje, że treść została zatwierdzona przez właściciela klucza prywatnego Z każdą transakcją skojarzone są dwa bloki. Blok typu send przywiązany do łańcucha po stronie nadawcy oraz blok typu receive znajdujący się po stronie odbiorcy. O ile jeden z tych bloków jest informacją nadmiarową, jego istnienie jest motywowane zwiększoną szybkością obliczania salda konta oraz większą możliwość kontrolowania błędów.

Łańcuch bloków(blockchain)

Jest zasadniczą technologią wykorzystaną w rozproszonej bazie danych. Blockchain jest stałą oraz rozproszoną strukturą danych działającą w sieci o architekturze peer-to-peer. Każde konto będzie posiadać swój własny łańcuch bloków równoważny historii transakcji salda konta, a aktualizacje tego łańcucha są możliwie asynchronicznie względem reszty sieci. Każdy z węzłów sieci przechowuję dokładną kopię tej struktury, która jest podstawą do weryfikacji przyszłych transakcji.

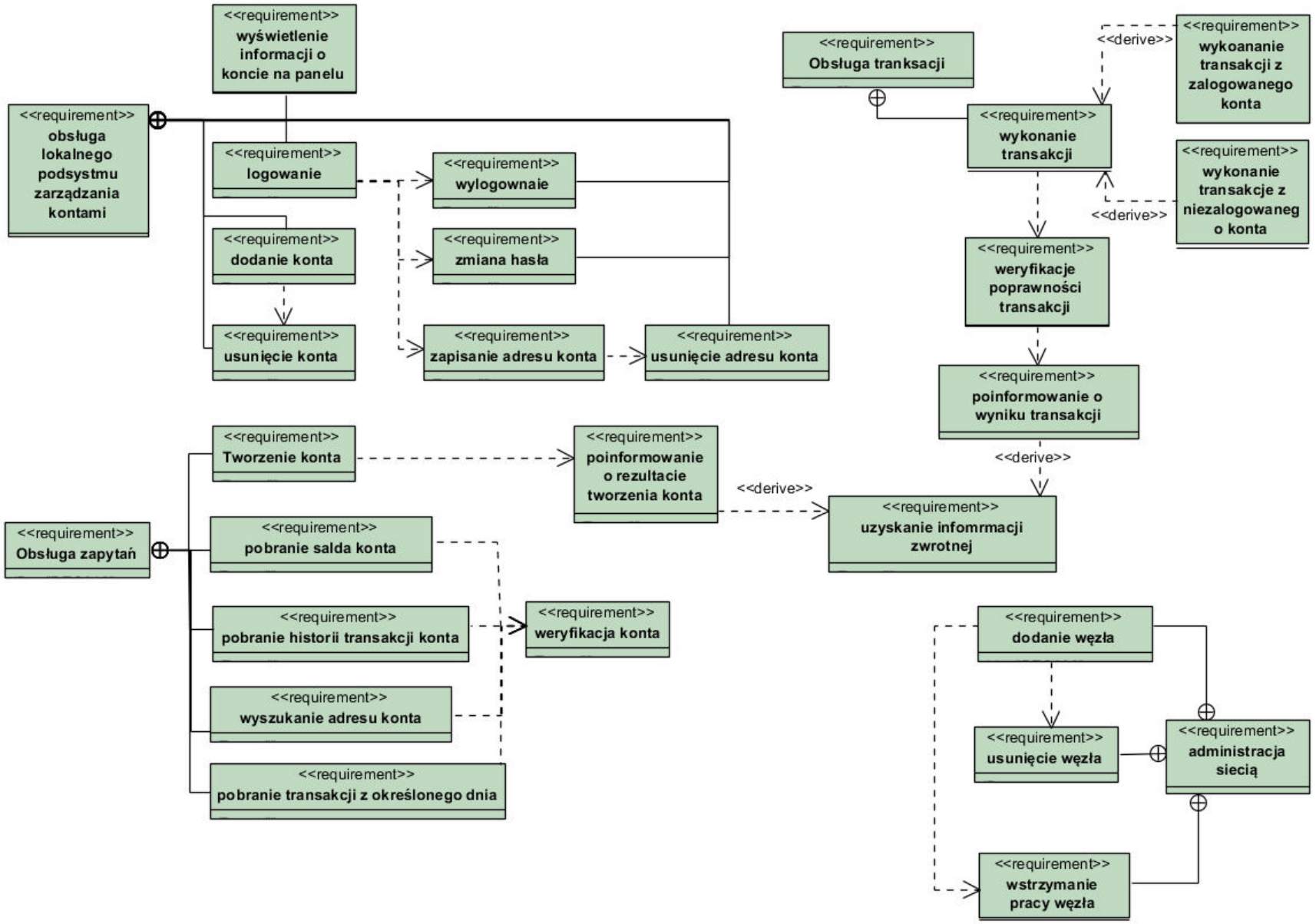
Blok genezy

Jest pierwszym blokiem dodany do łańcucha bloków, posiada początkowe saldo konta. Istnienie tego bloku jest uwarunkowane przez technologię blockchain.

Wymagania projektu

Najważniejszym zadaniem systemu jest zapewnienie szybkiej i niezawodnej możliwości wykonywania transakcji na zdecentralizowanej sieci połączonych ze sobą nodów o niezależnym organie autoryzacji. System posiada również możliwość rozszerzenia sieci o nowe nody ,tworzenia nowych kont oraz modyfikacja już istniejących. Wszelkie operacje są generowane i transmitowane przez wygodny graficzny interfejs.

Wymagania funkcjonalne:


<<requirement>>
wyświetlenie informacji o koncie na panelu
<<requirement>>
obsługa lokalnego podsystmu zarządzania kontami
<<requirement>>
logowanie
<<requirement>>
wylogownaie
<<requirement>>
dodanie konta
<<requirement>>
zmiana hasła
<<requirement>>
usunięcie konta
<<requirement>>
zapisanie adresu konta
<<requirement>>
usunięcie adresu konta
<<requirement>>
Obsługa tranksacji
<<derive>>
<<requirement>>
wykoananie transakcji z zalogowanego konta
<<requirement>>
wykonanie transakcji
<<derive>>
<<requirement>>
wykonanie transakcje z niezalogowaneg o konta
<<requirement>>
weryfikacje poprawności transakcji
<<requirement>>
poinformowanie o wyniku transakcji
<<derive>>
<<requirement>>
Tworzenie konta
<<requirement>>
poinformowanie o rezultacie tworzenia konta
<<derive>>
<<requirement>>
uzyskanie infomrmacji zwrotnej
<<requirement>>
Obsługa zapytań
<<requirement>>
pobranie salda konta
<<requirement>>
pobranie historii transakcji konta
<<requirement>>
weryfikacja konta
<<requirement>>
wyszukanie adresu konta
<<requirement>>
pobranie transakcji z określonego dnia
<<requirement>>
dodanie węzła
<<requirement>>
usunięcie węzła
<<requirement>>
administracja siecią
<<requirement>>
wstrzymanie pracy węzła

Specyfikacja wymagań funkcjonalnych

Numer porządkowy	Nazwa	Treść
REQ001	Administracja siecią	Zapewnia instancjom administracyjnym oprogramowanie automatyzujące proces zarządzające siecią
REQ002	Dodanie węzła	Zapewnia automatyczne wdrążenie nowego węzła do sieci. Możliwość dodania węzłów nie wstrzymuje pracy reszty sieci
REQ003	Usunięcie węzła	Zapewnia automatyczne usunięcie węzła z sieci. Nie wstrzymuje pracy reszty sieci.
REQ004	Wstrzymanie pracy węzła	Zapewnia okresowe zatrzymanie pracy węzła. System nie przerywa działania
REQ005	Obsługa lokalnego podsystemu zarządzania kontami.	Podsystem ma za zadanie ułatwić aplikacji klienckiej zarządzanie kontem oraz dokonywania operacji finansowych. Oprogramowanie nie korzysta z transmisji sieciowej ani bazy danych. Podsystem istnieje z uwagi na wykorzystaną technologię, która sama w sobie nie posiada mechanizmu logowania, a zadania weryfikacji czy transakcja została dokonana przez właściciela konta zapewnia podpis cyfrowy
REQ006	Wyświetlenie informacji o koncie w panelu.	System udostępnia interfejs z wszystkim informacji o koncie
REQ007	Logowanie	System pozwala na zalogowanie na konto po podaniu poprawnej nazwy użytkownika i hasła.
REQ008	Dodanie konta	System pozwala na dodanie konta po podaniu nazwy użytkownika oraz hasła
REQ009	Usunięcie kotna	System pozwala na usunięcie konta po podaniu prawidłowego hasła
REQ010	Wylogowanie	System pozwala na wylogowanie
REQ011	Zmiana hasła	System pozwala na zmianę hasła pod warunkiem podania poprawnego aktualnego hasła
REQ012	Zapisanie adresu konta	System pozwala na zapisanie na stałe kilku adresów kont
REQ013	Usunięcie adresu konta	System pozwala na usunięcie adresu konta pod warunkiem podania poprawnego hasła konta
REQ014	Obsługa zapytań	Zapewnienie oprogramowani po stronie klienckiej do komunikacji z serwerem
REQ015	Weryfikacja konta	Pozwala systemowi na sprawdzenie czy podany adres konta znajduje się w systemie
REQ016	Tworzenia konta	Pozwala na utworzenie konta po pomyślnej weryfikacji.
REQ017	Pobranie salda konta	Umożliwia klientowi sprawdzenia salda dowolnego konta
REQ018	Pobranie historii transakcji konta	Umożliwia klientowi pobranie uporządkowanej historii transakcji
REQ019	Wyszukanie adresu konta	Pozwala klientowi na wyszukanie adresu konta na podstawie nazwy właściciela konta

REQ020	Pobranie transakcji z określonego dnia	Zapewnia pobranie listy zawierającej transakcje z podanego dnia
REQ021	Uzyskanie informacji zwrotnej	System winien informować o rezultacie akcji
REQ022	Poinformowanie o rezultacie tworzenia konta	System winien odesłać informację o rezultacie tworzenia konta. Konto może zostać poprawnie utworzone lub nie zostać utworzone
REQ023	Obsługa transakcji	Umożliwienie transferu środków między kontami
REQ024	Wykonanie transakcji	Pozwala na dokonanie transakcji pod warunkiem poprawnej weryfikacji
REQ025	Wykonanie transakcji z zalogowanego konta	Umożliwia wykonanie transakcji po podaniu adresu konta docelowego oraz kwoty
REQ026	Wykonanie transakcji z niezalogowanego konta	Umożliwia wykonanie transakcji po podaniu klucza prywatnego, adresu konta docelowego oraz kwoty
REQ027	Weryfikacja poprawności transakcji	Funkcja gwarantuje poprawność transakcji przez weryfikację czy transakcja została zatwierdzona przez właściciela konta. Sprawdza dostępność funduszy oraz poprawność adres konta docelowego. W weryfikacji transakcji udział bierze sieć
REQ028	Poinformowanie o wyniku transakcji	System winien odesłać informację o rezultacie transakcji

Wymagania niefunkcjonalne

Nazwa wymagania	Opis
Użyteczność	Łatwo przyswajalna obsługa systemu przez użytkowników oraz estetyczny interfejs
Wydajność	Krótki czas oczekiwania na zaksięgowanie transakcji
Przejrzystość systemu	System ukrywa swój rozproszony charakter udostępniają wspólny interfejs niezależnie od serwera z którym łączy się klient
Niezawodność	Awaria jednego z węzłów sieci nie powoduje wstrzymania pracy całej sieci
Bezpieczeństwo	System do zagwarantowania bezpieczeństwa używa algorytmu SHA256
Dostępność	System powinien być dostępny dla użytkownika przez 24 godziny na dobę, 7 dni w tygodniu. System powinien pracować stale, nawet mimo wstrzymania pracy niektórych serwerów. Dopuszczalne są przerwy konserwacyjne całości sieci, jednakże tylko w okresach najmniejszej aktywności użytkownika.
Skalowalność	System powinien zapewnić łatwą rozbudowę sieci
Modyfikowalność	System powinien być łatwo modyfikowalny, a więc silnie zmodularyzowany
Odporność na błędy	Każdy moduł powinien samodzielnie zapewnić poprawność danych wejściowych
Niezależność	Praca systemu bez udziału osób trzecich
Wieloplatformowość	system powinien działać niezależnie od architektury sprzętowej oraz oprogramowania

Wymagania interfejsu

Interfejs użytkownika po stronie klienckiej zostanie zrealizowany w formie graficznego interfejsu (GUI). Z poziomu portfela dostępne będą opcję tworzenia, logowania się na konto oraz wszystkie operację zarządzania nim. Ponadto dokonywani transakcji będzie nieskomplikowane, dzięki transparentności systemu. Co więcej na każdym z zalogowanych kont możliwy będzie wgląd w księgę rachunkową w obrębie całej sieci.

Opis technologii

Algorytm SHA256

Kryptograficzna funkcja skrótu, której słowem wyjściowym jest 256-biowy ciąg, zapisany heksadecymalnie w postaci 64-znakowego słowa. Jest generycznym algorytmem haszującym, co oznacz że niezależnie o typu oraz rozmiaru danych, słowem wyjściowym jest ciąg 256-bitowy. Do funkcji skrótu podawany jest blok danych, czyli cyfrowa reprezentacja transakcji. SHA256 został wybrany jako funkcja skrótu z przyczyny na cechy jakie posiada:

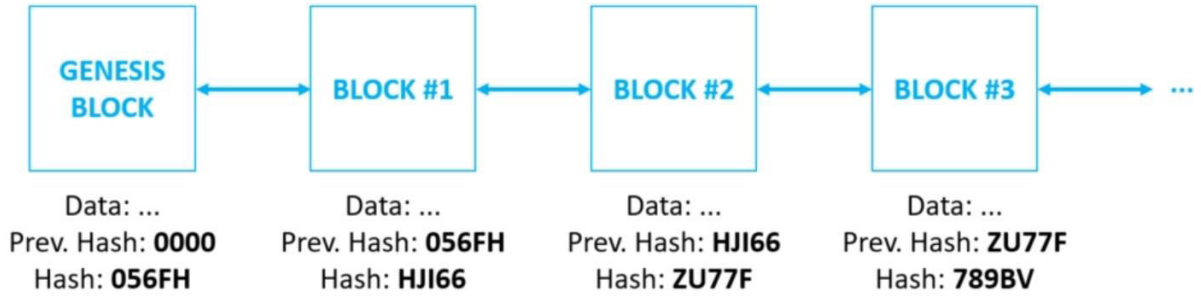
- Deterministyczny: wynikiem tego samego zestawu danych wejściowych jest ten sam skrót.
- Jednokierunkowy: łatwo generowany skrót, lecz duża złożoność obliczeniowa odwrotnej operacji polegającej na uzyskania wartości wejściowej ze skrótu.
- Odporność na kolizji: w praktyce kolizję między skrótami dla różnych wartość wejściowy są bardzo mało prawdopodobne.
- Efekt lawinowy(avalanche effect): niewielka zmiana danych wejściowych powoduje otrzymanie kompletnie innej wartości skrótu.

Algorytm podpisu cyfrowego

Algorytm podpisu cyfrowego jest realizowany za pomocą kryptografii krzywych eliptycznych. Algorytm generuję klucza prywatnego oraz publicznego, stanowiącego adres konta. Klucz prywatny wykorzystywany jest do cyfrowego podpisywania transakcji, który gwarantuje że treść została zatwierdzona przez właściciela konta. Uwierzytelnienie transakcji może odbywać się jedynie przy użyciu publiczny klucz. Technologia pozwala zabezpieczyć dostęp do konta dzięki kluczowi prywatnemu jednocześnie dając łatwy mechanizm weryfikacji transakcji z wykorzystaniem klucza publicznego.

Blockchain

Łańcuch bloków jest rosnącą listą rekordów, nazywanych blokami. Łańcuch bloków jest połączony kryptograficznymi wartościami skrótów. Każdy z bloków posada dwie wartości skrótu. Pierwsza wartość jest wartością funkcji skrótu poprzedniego bloku, zaś druga jest hashem obliczonym na podstawie zawartości aktualnie dodawanego bloku wliczając do zawartości bloku również wartość poprzedniego hashu. Zatem wartości skrótów są używane przy wykrywaniu zmian w bloku lub zmian w połączeniach łańcucha bloków.



Zmiana dowolnej wartości bloku lub modyfikacje w łańcuchu pociągają za sobą zmianę wartości skrótu, a zamian skrótu spowoduje, że wszystkie kolejny bloki w łańcuchu staną się nieprawidłowe. Stąd wynika, że łańcuch bloków posiada własność polegającą na tym, że raz umieszczone dane w bloku są niezwykle trudne do modyfikacji.

Protokoły komunikacji sieciowej

Do komunikacja sieciowej wykorzystane są protokółu warstwy transportowej TCP i UDP. Wymian danych między aplikacją kliencką, a serwerem odbywa się przez protokół UDP, zaś komunikacja wśród sieci złożonej z węzłów za pomocą TCP.

Technologia bazodanowa

W projekcie wykorzystana zostanie relacyjna baza danych. System zarządzania bazą danych będzie oprogramowanie firmy Oracle. Język stosowanym do zapytań oraz tworzenia schematu oraz dodawania danych będzie SQL. Również PL/SQL zostanie zastosowany do definiowania procedur, funkcji, triggerów.

Model szkieletu aplikacji

Diagram związków encji:

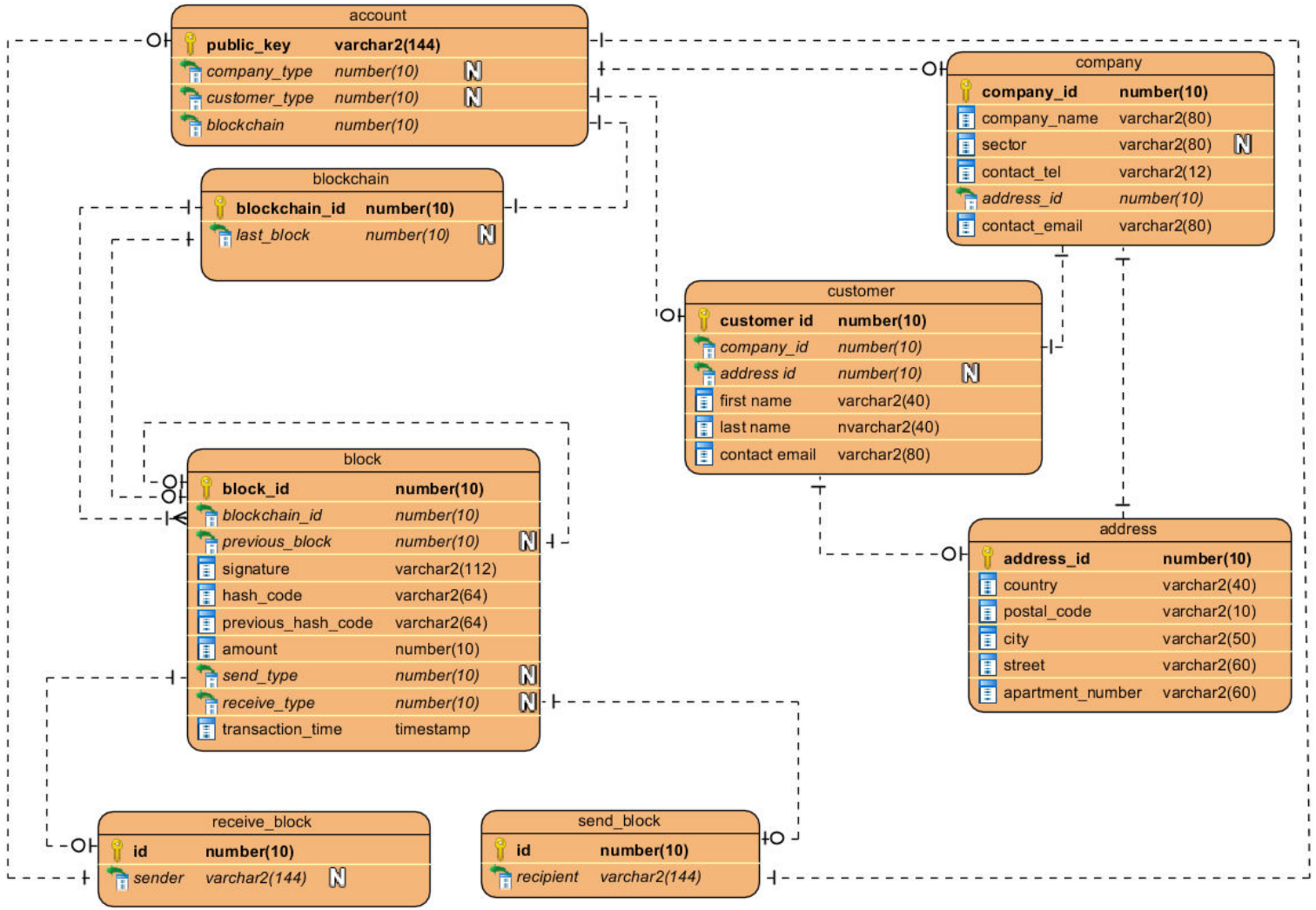


Diagram klas: