

Architectuur Document

Pedro Marques | s31 | fhict

# Documenthistorie

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Versie |  |  | Wijzigingen | Auteur | Datum | Verzendlijst | Verzoek |
|  |  |  |  |  |  |  |  |
| 0.1 |  |  | Opzet document, Inleiding, Domeinmodel | Pedro  Marques | 27-11 |  |  |
| 0.2 |  |  | Componenten, Persistentie | Pedro Marques | 28-11 |  |  |
|  |  |  |  |  |  |  |  |

Inhoud

[Documenthistorie 1](#_Toc499761182)

[Inleiding 5](#_Toc499761183)

[Context van het project 5](#_Toc499761184)

[Applicatie 6](#_Toc499761185)

[Niet-functionele eisen 7](#_Toc499761186)

[Performance 7](#_Toc499761187)

[Betrouwbaarheid 7](#_Toc499761188)

[Compatibiliteit 7](#_Toc499761189)

[Beveiligbaarheid 7](#_Toc499761190)

[Onderhoudbaarheid 7](#_Toc499761191)

[Doel van dit document 7](#_Toc499761192)

[Domeinmodel 8](#_Toc499761193)

[Klassendiagram 8](#_Toc499761194)

[Klassenuitleg 8](#_Toc499761195)

[Coin: 8](#_Toc499761196)

[Opdeling in Componenten 10](#_Toc499761197)

[Component diagram 11](#_Toc499761198)

[11](#_Toc499761199)

[Koppeling tussen componenten 12](#_Toc499761200)

[Synchronisatie tussen componenten 12](#_Toc499761201)

[Services per component 12](#_Toc499761202)

[Allocatie van objecten 12](#_Toc499761203)

[Remote objecten 13](#_Toc499761204)

[Packagestructuur 13](#_Toc499761205)

[H4 Communicatie tussen componenten 14](#_Toc499761206)

[Persistentie per component 15](#_Toc499761207)

[Persistentie binnen CryptoHelper 15](#_Toc499761208)

[Data opslag tijdens gebruik van CryptoHelper 15](#_Toc499761209)

[H6 Detailed design per component 16](#_Toc499761210)

[H7 Realisatie niet-functionele eisen 17](#_Toc499761211)

[H8 Deployment 18](#_Toc499761212)

[H9 Specificatie van interfaces 19](#_Toc499761213)

# Inleiding

## Context van het project

Om de waarde van mijn project duidelijk uit te leggen het is belangrijk om te snappen wat blockchain technologie is.

**Blockchain technologie** is een soort van databasesysteem (heel primitief gezegd) dat gebruikt kan worden om waarde (geld of digitale items) te sturen naar een derde partij op een veilige manier, zonder een middenman (iemand dat de transactie voor je uitvoert – denk aan banken of services zoals PayPal).

Tegenwoordig gebruiken mensen middenmannen omdat ze de derde partij aan wie het sturen van goederen is bedoeld niet vertrouwen. Middenmannen geven de zekerheid dat een transactie werd uitgevoerd, zodat de derde partij deze informatie niet kan falsificeren - bijvoorbeeld door het communiceren dat het overgeschreven bedrag niet genoeg of helemaal niet binnen gekomen is. Het klinkt allemaal goed en nuttig, maar dit betekent ook dat banken en zulke instituties ook controle hebben over het uitvoeren van transacties en kunnen dus servicekosten invoeren of zelfs transacties blokkeren.

Blockchain technologie betekent dus een “bypass” op de middenman bij het uitvoeren van een transactie, onder andere voordelen, zoals:

* Het publiek en transparant stellen van alle transacties die worden gemaakt door een gebruiker. Bijvoorbeeld: In het geval van een overheidsinstitutie is dit nuttig, omdat dan kan iedereen zien waar er geld wordt besteden. (Blockchain records zijn voor iedereen beschikbaar).
* Het makkelijk kunnen verifiëren van eigendom.
* Toepassing op letterlijk alle services die tegenwoordig bestaan. (Er bestaat tegenwoordig een blockchain project voor bijna alles – verkoop van games (Enjin), het maken van andere blockchain projecten (ARK), anoniem dingen kopen (Monero), etc.

**Cryptocurrency** is een elektronische eenheid dat wordt “gecreëerd” op het moment dat een miner (iemand die zijn computer gebruikt om te contribueren voor de werking van een blockchain network) een transactie confirmeert.

Een miner confirmeert een transactie door een block (een series wiskundige problemen) op te lossen met behulp van een krachtige computer. Een transactie is altijd geassocieerd aan een block, en het aantal confirmaties van een transactie is de hoeveelheid aangemaakte blocks sinds de block die geassocieerd is aan de transactie. Een transactie moet tenminste 6 keer worden geconfirmeerd om als geldig te worden beschouwd.

## Applicatie

Tegenwoordig ervaart de cryptocurrency markt een explosieve groei. Bedrijven beseffen steeds meer de potentieel dat blockchain technologie te bieden heeft. Dit betekent dat er steeds meer significante investeringen in deze technologieën worden gemaakt, wat ook betekent dat er prijsfluctuaties ontstaan in de cryptocurrency markt.

Crytophelper is een project met als doel het maken van een gedistribueerde app dat gebruikt kan worden om:

* **Geïnformeerde investeringen binnen het cryptocurrency wereld te maken;**
  + Cryptohelper beschikt van een overzicht scherm die alleen maar **relevante** cryptocurrencies op de markt aan de gebruiker toont. Door informatie (prijzen, trends, etc.) over de cryptocurrencies aan de gebruiker te presenteren en alles bij elkaar in een fatsoenlijke GUI te presenteren wordt het maken van een slimme investering makkelijker. Daardoor wordt de kans om winst te maken ook groter.
* **De gebruikers IDatabaseHelper te controleren en een overzicht daarvan te geven;**
  + Een overzicht over welke investeringen die al gemaakt zijn is noodzakelijk om goede beslissingen te maken. Cryptohelper helpt hierbij door dit makkelijk zichtbaar aan de user te stellen, zodat hij/zij makkelijk een accuraat analyse van de situatie van zijn IDatabaseHelper kan maken.
* **Up to date te blijven met de laatste nieuws over de crypto wereld.**
  + Cryptohelper beschikt van een News tab waar relevante nieuws over cryptocurrency aan de user worden getoond. Vaak hebben gebeurtenissen in de cryptowereld een heel opmerkelijk invloed op de prijs van cryptocurrencies en hun respectieve market cap.

Cryptohelper is een driedelige product: Het houdt in een server die informatie vanuit API rest calls haalt voor gebruik in de client, de client zelf en een database component die verbinding maakt met de database server (DAL).

## Niet-functionele eisen

De volgende niet-functionele eisen zullen worden besproken in deze document:

### Performance

Alle netwerk-afhankelijk handelingen worden met een vertraging van maximaal 1 seconden uitgevoerd (URS. Q.1). Daarnaast worden alle GUI handelingen uitgevoerd met een vertraging van maximaal 500ms (URS. Q.2).

### Betrouwbaarheid

Het systeem moet 99% van de tijd beschikbaar zijn (URS Q.6). Per 24 uur moet het systeem 23 uur functioneel blijven (URS Q.7).

### Compatibiliteit

Documentatie van zowel interfaces als klassen is beschikbaar (URS Q.4)

### Beveiligbaarheid

Het systeem maakt gebruik van beveiligde verbindingen. (Q.8) Bovendien delen de componenten van het systeem geen niet-noodzakelijke klassen/gegevens met elkaar. (Q.9)

Database query’s worden vooraf bereid in het systeem om injectie problemen te voorkomen. (Q.10)

### Onderhoudbaarheid

Het systeem is modulair opgebouwd.(Q.11)

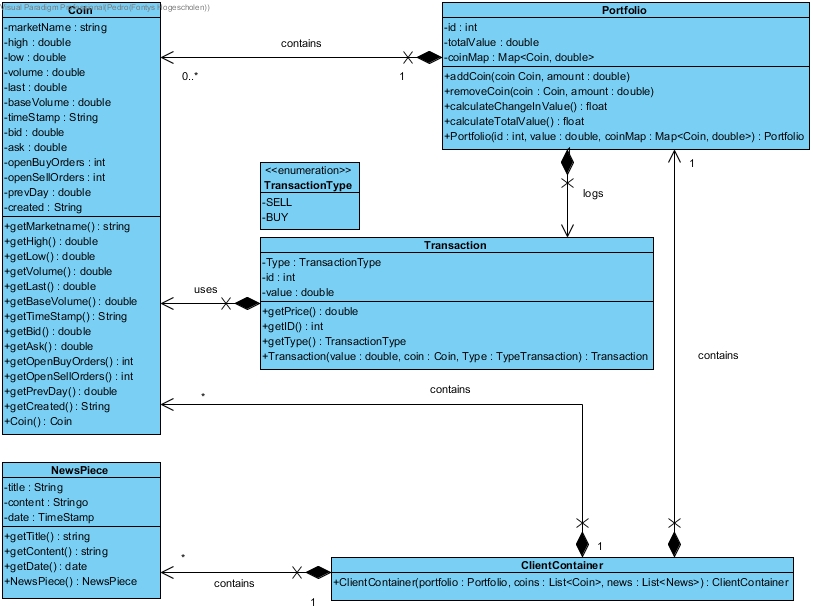
## Doel van dit document

Het doel van deze document is het verantwoorden van de software/hardware architectuur van de CryptoHelper applicatie.

De volgende aspecten van de architectuur van CryptoHelper zullen worden beschreven:

* Domeinmodel
* Persistentie
* Communicatie
* Realisatie van niet-functionele eisen
* Componenten
* Deployment
* Specificatie van Interfaces

# Domeinmodel



Figuur 1: Klassendiagram van het domein.

## Klassenuitleg

### Coin:

Representeert een cryptocurrency eenheid. Wordt vanuit een API call gevuld. Een coin heeft de volgende attributen:

* **MarketName**: de naam van de coin op de markt;
* **High**: de hoogste prijs van de coin op de uur waar de informatie werd aangevraagd;
* **Low**: de laagste prijs van de coin op de uur waar de informatie werd aangevraagd;
* **Volume**: de waarde van alle transacties van de blockchain waar de coin bij hoort in de laatste 24h;
* **BaseVolume**: de volume van de basis currency (BTC) in de laatste 24h;
* Last: de hoogste prijs van de coin in de laatste uur;
* **TimeStamp**: de tijdstip waarop de Coin informatie werd aangevraagd
* Bid: de hoogste koopprijs op de markt;
* **Ask**: de laagste verkooprijs op de markt
* **OpenBuyOrders**: hoeveel koop aanvragen actief zijn voor de coin;
* **OpenSellOrders**: hoeveel verkoop aanvragen actief zijn voor de coin;
* **PrevDay**: de hoogste prijs van de coin in de laatste dag;
* **Created**: de datum van wanneer de coin op de markt was gezet;

#### IDatabaseHelper:

Representeert de totale opsomming van alle investeringen dat de gebruiker heeft gemaakt. Bestaat uit een map van coins, een id, een double (totalValue) om de totale waarde van de IDatabaseHelper op te slaan en een lijst van transacties.

Een IDatabaseHelper kan zijn totale waarde berekenen, de algemene verandering in waarde berekenen en coins toevoegen of verwijderen door middel van het aanmaken van transacties.

#### Transaction:

Representeert een verandering in de hoeveelheid coins in het IDatabaseHelper. Bestaat uit een type (E.TransactionType) die aangeeft of het een verkoop of een koop transactie is, een id en het bedrag coins waar de transactie over gaat. Transacties worden opgeslagen in een IDatabaseHelper.

### NewsPiece:

Representeert een nieuws artikel. Bevat een titel, inhoud en een datum.

### ClientContainer:

Representeert een container voor een IDatabaseHelper, een lijst van coins en een lijst van nieuws.

# Opdeling in Componenten

*In dit hoofdstuk wordt de opdeling in software componenten besproken aan de hand van een Componentendiagram met toelichting. Daarnaast wordt koppeling en synchronisatie tussen de componenten besproken en de opdeling in software packages.*

*Een component is een modulair deel van het systeem dat beschreven wordt in termen van aangeboden en gevraagde interfaces. In principe kan een component vervangen worden door een andere component, mits die andere component aan dezelfde interfaces voldoet. Er wordt onderscheid gemaakt tussen componenten en subsystemen: een component is altijd een executeerbare eenheid, maar een subsysteem is geen executeerbare eenheid. Tip: kies voor iedere component een naam die duidelijk verschilt van de namen van de klassen die in die component zitten.*

*De volgende onderwerpen worden in dit hoofdstuk besproken:*

* *Componentendiagram (opdeling componenten)*
* *Soort koppeling (RMI, HTTP, SQL, …)*
* *Synchronisatie (zie ook persistentie/communicatie)*
* *Service(s) per component (voor welke component interessant; aanduiding van behoeften (naam methode) per interface)*
* *Allocatie objecten (binnen welke component)*
* *Remote objecten (welke objecten worden op afstand aangesproken)*
* *Packagestructuur*

*Er zijn verschillende manieren om componentdiagrammen te tekenen, zelfs binnen UML. Hier is gekozen voor componenten opgebouwd uit klassen en interfaces. Klassen kunnen interfaces realiseren of hebben behoefte aan interfaces. Deze interfaces kunnen binnen een component met elkaar verbonden worden en/of via een zogenaamde poort beschikbaar worden gesteld aan andere componenten. Een poort (engels: port) wordt weergegeven door middel van een vierkantje op de rand van de component. Een poort kan een interface aanbieden (aangeboden poort) of behoefte hebben aan een interface (benodigde poort). Een poort die zowel een interface aanbiedt als een interface nodig heeft noemen we een complexe poort. Meestal wordt een poort gerealiseerd door middel van een object dat de aanvraag van services doorgeeft naar een ander object binnen de component. Tijdens uitvoering van het programma zal een benodigde poort een verbinding leggen met een aangeboden poort van een andere component. Voor meer informatie over componentendiagrammen, zie Hoofdstuk 14 van Praktisch UML van Jos Warmer en Anneke Kleppe (vijfde editie, uitgever Pearson).*

## Component diagram

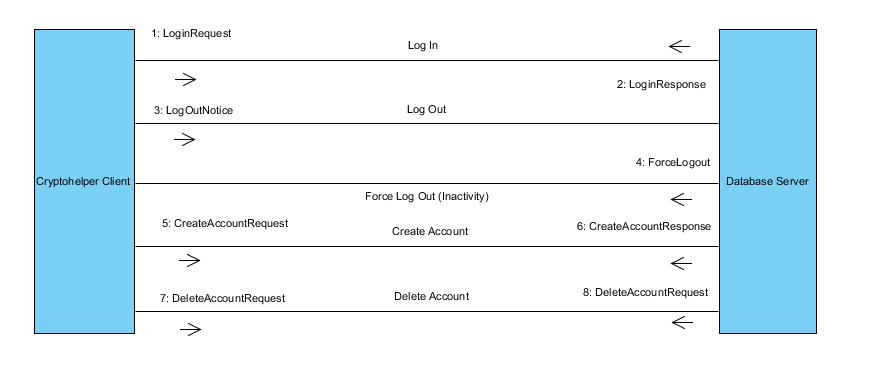
## C:\Users\Pedro\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Component Diagram.jpg

Figuur 2: Componentendiagram.

Het componentendiagram in Figuur 2 laat de 4 componenten van CryptoHelper zien met de klassen en interfaces die ze aanbieden/ontvangen. De componenten zijn:

* Database Server
  + Representeert de software applicatie die alle communicatie met de database behandelt. Dat houdt in het maken en verwijderen van accounts, het inloggen en uitloggen en het opslaan en laden van portfolio informatie. Bevat de class DatabaseHelper.
* Coin Server
  + Representeert de software applicatie die de cryptocurrency markt informatie ophaalt en vervolgens beschikbaar maakt. Bevat de class Wallet.
* News Server
  + Representeert de software applicatie die e nieuws ophaalt en vervolgens beschikbaar maakt. Bevat de class NewsFeed.
* CryptoHelper Client
  + Representeert de software applicatie voor de gebruiker. Bevat de classes Database Client, Coin Client en News Client.

## Koppeling tussen componenten

Om real-time communicatie uit te voeren worden er twee methodes toegepast: Het sturen van TCP pakketten met requests en responses tussen Client en DatabaseServer (Figuur 3), en Remote Method Invocation (Figuur 2). De RMI koppelingen tussen componenten worden gerealiseerd door gebruik te maken van twee interfaces: ICoinRetriever en INewsFeed.

Figuur 3: Versimpelde TCP communicatiediagram tussen Database Client en Database Server.

Alle servers worden gekoppeld aan de bijbehorende Client class in CryptoHelper Client. Ik heb hiervoor gekozen om aan de Single Responsibility Principle te houden. Zo blijft het programma modulair en worden de data streams in aparte klassen gehouden. De classes in elke Client worden dan waar nodig in het programma gebruikt. Dit wordt niet in het diagram opgenomen om het schema overzichtelijk te houden.

## Synchronisatie tussen componenten

Binnen de context van CryptoHelper is synchronisatie tussen de Coin Server en de Client belangrijk bij het berekenen van de waarde van een portfolio. Elke keer dat een berekening van portfolio waarde plaats vindt wordt er nieuwe informatie opgehaald zodat het prijs actueel is. Bovendien vindt er een automatisch update plaats elke 5 minuten.

## Services per component

De volgende services worden gerealiseerd door middel van de twee interfaces in het diagram:

* ICoinRetriever
  + Vraag referentie naar lijst van Coin
  + Vraag update van lijst van Coin
* INewsFeed
  + Vraag referentie naar lijst van News
  + Vraag update van lijst van News

De volgende services worden per component aangeboden:

* Coin Server: IWallet
* News Server: INewsFeed
* Database Server: IDatabaseHelper, LogInResponse, CreateAccountResponse, DeleteAccountResponse, ForceLogout.
* Database Client , LogInRequest, CreateAccountRequest, DeleteAccountRequest

**In CryptoHelper de enige component die services aanvraagt is de CryptoHelper Client.** Die vraagt namelijk voor alle aangeboden services door de andere componenten.

Verder vindt log in communicatie plaats tussen de Database Server en de Crypto Client in de vorm van het uitwisselen van TCP pakketten. Voor meer informatie hierover zie de hoofdstuk Communicatie.

### Allocatie van objecten

Hier worden beschreven waar welke instanties van welke objecten zijn gealloceerd.

* Coin Server: Instantie van CoinRetriever.
* News Server: Instantie van NewsFeed.
* Database Server: Instantie van DatabaseHelper.
* CryptoHelper Client: Instanties van DatabaseClient, CoinClient en NewsClient;

### Remote objecten

Alle remote objecten (CoinRetriever en NewsFeed) worden in CryptoHelper Client geïnstantieerd.

### Packagestructuur

Elke component heeft zijn eigen package. Daarnaast is er een Shared package voor klassen die in meer dan een component worden gebruikt, en een Network Package voor de requests en responses tussen twee connections.

Klassen/Interfaces per package:

* Shared: Coin, NewsPiece, IDatabaseHelper, IWallet, INewsFeed. Network (Bevat alle TCP Requests en Responses)
* Client: CoinClient, NewsClient, DatabaseClient.
* CoinServer: CoinServer, Wallet.
* NewsServer: NewsServer, NewsFeed.
* DatabaseServer: DatabaseServer, IDatabaseHelper;

# Communicatie tussen componenten

## Communicatie Library

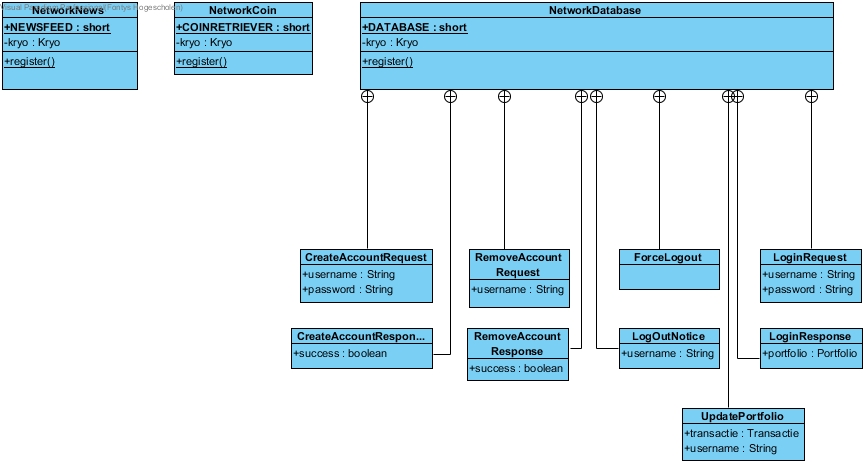
Communicatie binnen de componenten van CryptoHelper wordt gerealiseerd op twee manieren: Door middel van RMI en het gebruik van TCP communicatie.

Om dit te coderen er wordt gebruik gemaakt van de Kryonet networking library (<https://github.com/EsotericSoftware/kryonet>). Er werd hiervoor gekozen omdat Kryonet versimpelt het opstellen van RMI en TCP communicatie, en maakt gebruik van methoden die goed te combineren zijn met de observable pattern.

## Communicatie tussen componenten

Tijdens het gebruik van CryptoHelper staat de CryptoHelper Client verbonden aan de andere drie componenten (Database, News en CoinRetriever Servers). Deze drie comuniceren tussen elkaar niet. Alle servers zijn stateless.

Ik zal per component uitleggen welke eigenschappen van welke objecten worden gecommuniceerd**.**

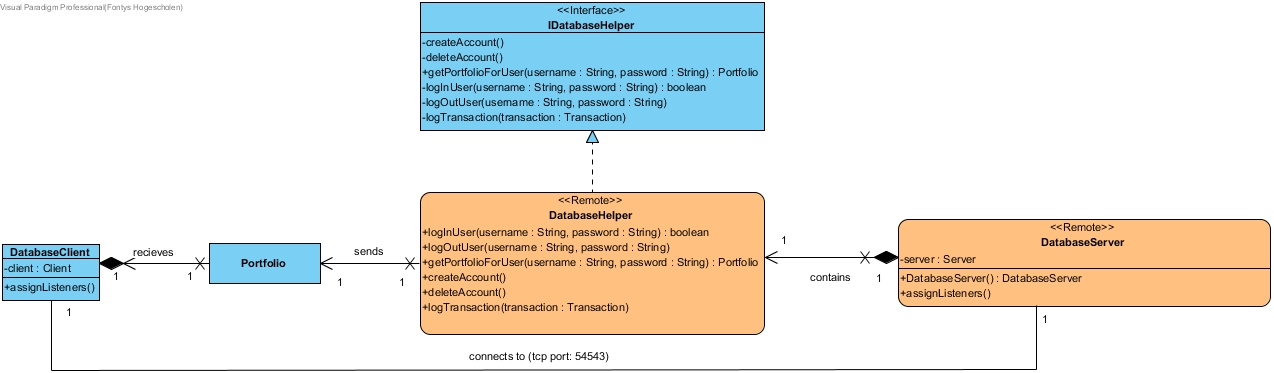


Figuur 8: Network klassen. Gebruikt om dezelfde klasses/return types op de registry te registreren op twee endpoints van een verbinding, zodat ze op beide kanten van een verbinding beschikbaar zijn. Requests en responses worden als inner klassen gerepresenteerd, zoals in de Kryonet voorbeelden.

(<https://github.com/EsotericSoftware/kryonet/tree/master/examples/com/esotericsoftware/kryonet/examples>)

**In de volgende diagrammen zal de Client als leidend object worden beschouwd.**

## Communicatie tussen Client en Database Server



Figuur 5: Klassendiagram van communicatie tussen Client en Database Server

Communicatie tussen de Client en DatabaseServer wordt gerealiseerd door middel van uitwisseling van TCP requests en responses. De requests en responses bevatten attributen die over het netwerk verstuurd worden. In dit geval worden er strings, booleans, Transactie en Portfolio objecten verstuurd.

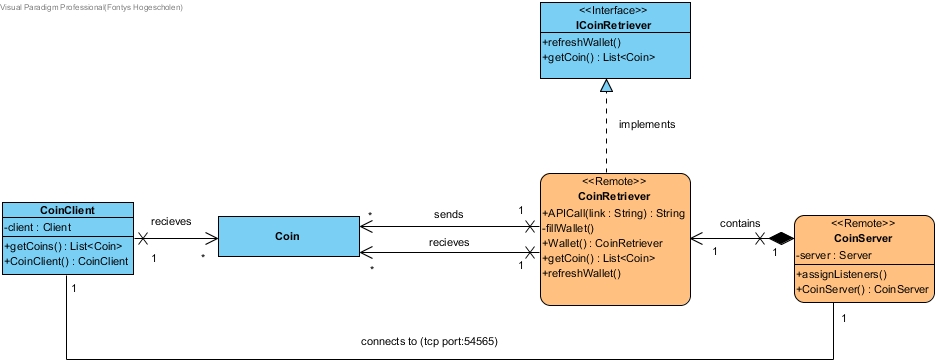
Het ontvangen van een request/response triggert een event in de connection endpoint waar het plaatsvindt. Deze events worden gebruikt om methoden uit te voeren binnen de klasse, om een response terug te sturen, of allebei. De Network klassen, requests en responses staan uitgebeeld in Figuur 8.

Er vindt communicatie plaats tussen de Client en de Database Server op de volgende momenten:

Note: De uitwisseling van pakketten staat beschreven in detail in de hoofdstuk interface specificatie, in de DatabaseHandler sectie.

* Bij het inloggen van een user:
  + Er wordt een pakket verstuurd met een username en een password en een ontvangen met een boolean die aangeeft of de gegevens correct zijn of niet.
  + Als de login succesvol is dan krijgt de actor een bericht hierover en krijgt hij/zij toegang tot de rest van het programma. Er wordt ook een sessie token gegenereerd en een portfolio opgeladen.
  + Als de login niet succesvol is dan krijgt de actor een bericht met het fout tijdens het inloggen.
  + Bij het inloggen wordt er een token gemaakt en in de database opgeslagen. Zolang als deze token bestaat kan niemand anders zich inloggen met de net ingevoerde gegevens.
* Bij het uitloggen van een user:
  + Er wordt een pakket verstuurd met een username bij het uitloggen in de app. Het ontvangen van het pakket triggert een event die de user uitlogt.
  + Als er geen handmatig logout wordt verstuurd dan wordt de disconnect van de client gedetecteerd door een listener op de server en wordt de client alsnog uitgelogd.
* Bij het aanmaken van een account:
  + Net als bij het inloggen, er wordt een pakket verstuurd naar de database server met een username en een wachtword. Het ontvangen van het pakket triggert een event op de server die een methode van DatabaseHandler uitvoert om een account te maken met de gekregen gegevens.
  + Als het aanmaken van een account niet lukt (bijv. door al bestaande gegevens) krijgt de user een message met de foutmelding.
* Bij het verwijderen van een account:
  + Er wordt een pakket verstuurd met een username. Het ontvangen van het pakket triggert een event op de server die een methode van DatabaseHandler uitvoert om een account te verwijderen met de gekregen username.
  + Als het verwijderen van een account niet lukt (geen verbinding) krijgt de user een message met de foutmelding.
* Bij het updaten van een portfolio (nieuwe transactie):
  + Er wordt een pakket verstuurd met een transactie en een username. Het ontvangen van het pakket triggert een event op de server die een methode van DatabaseHandler uitvoert om een transactie toe te voegen aan het portfolio van de gekregen username.
  + Als de update niet gelukt is krijgt de user een foutmelding.

## Communicatie tussen Coin Client en Coin Server



# Persistentie per component

*In dit hoofdstuk wordt de persistentie van de objecten beschreven voor iedere component. Beschrijf welke eigenschappen van welke objecten moeten worden bewaard. Beschrijf hoe opslag wordt gerealiseerd (database, serialiseren, XML, etc.). Dit kan verschillen per eigenschap. Voeg het ERD met beschrijving toe indien gegevens worden opgeslagen in een database. Beschrijf tot slot wanneer opslag plaatsvindt. Ook dit kan verschillen per eigenschap.*

## Persistentie binnen CryptoHelper

Om de login gegevens, sessie en de IDatabaseHelper van een klant op te slaan wordt er gebruik gemaakt van de Account data object. Een account bevat een ID, een naam, een wachtwoord, een IDatabaseHelper en een token veld om de status van een sessie op te slaan.

## Data opslag tijdens gebruik van CryptoHelper

Data opslag gebeurt binnen CryptoHelper op de volgende momenten:

**Bij het aanmaken van een account:**

Als een account wordt aangemaakt wordt het meteen opgeslagen in de database. De IDatabaseHelper is dan leeg.

**Bij het inloggen:**

Om log in sessies bij te houden en ongeoorloofde gebruik tegen te gaan, wordt een token gegenereerd en opgeslagen in de database. Als iemand probeert op een account in te loggen die al ingelogd is krijgt hij/zij een error message.

**Bij het uitvoeren van transacties:**

Tijdens gebruik van CryptoHelper worden alle updates aan de IDatabaseHelper van de klant opgeslagen op het moment dat ze uitgevoerd zijn. Dus elke keer dat de klant een transactie uitvoert wordt de IDatabaseHelper data entry op de database meteen geüpdatet.

**Bij het uitloggen:**

Op het moment dat een user zich uitlogt wordt de login token verwijdert van de database. **Dit kan ook gebeuren als de user 20 minuten inactief is.**

# H6 Detailed design per component

*In dit hoofdstuk wordt het detailed design (implementatiemodel) per component beschreven. Maak hiervoor gebruik van klassendiagrammen en sequence diagrammen. Voor specifieke doeleinden kun je gebruik maken van objectdiagrammen, statemachinediagrammen, activiteitendiagrammen, etc. Voor meer informatie over UML diagrammen, zie Praktisch UML van Jos Warmer en Anneke Kleppe (vijfde editie, uitgever Pearson).*

# H7 Realisatie niet-functionele eisen

*In dit hoofdstuk wordt de realisatie van (overige) niet-functionele eisen besproken. De volgende onderwerpen dienen tenminste te worden besproken: betrouwbaarheid, performance, beveiliging, schaalbaarheid. Eventueel kunnen nog extra niet-functionele eisen worden besproken.*

**Betrouwbaarheid**

**Performance**

**Beveiliging**

**Schaalbaarheid**

# H8 Deployment

*In dit hoofdstuk wordt de toekenning van software componenten aan hardware besproken aan de hand van een Deploymentdiagram met toelichting. Daarnaast wordt de koppeling (lokaal netwerk, internet, etc.) tussen de nodes besproken.*

**Deploymentdiagram**

Figuur X: Deploymentdiagram.

# H9 Specificatie van interfaces

*In dit hoofdstuk wordt de specificatie van interfaces besproken. Voor ieder interface wordt per methode gedefinieerd:*

* *Naam methode*
* *Naam en type argumenten*
* *Precondities*
* *Type returnwaarde*
* *Beschrijving*
* *Aanleiding voor excepties*