Onderzoek naar

# Gedistribueerde netwerken en identiteit binnen Blockchain technologie

Jeffrey van Hoven

10 september 2018

Quintor

# Voorwoord

Voor u ligt mijn afstudeerverslag; "*Onderzoek naar gedistribueerde netwerken en identiteit binnen Blockchain technologie*" waarin ik schrijf over de uitvoering van het onderzoek dat gedaan is ten behoeve van mijn afstuderen voor de opleiding Informatica aan de Haagse Hogeschool. Het betreft verslaglegging van het proces dat doorlopen is om de uitdagende opdracht zoals voorgesteld door Quintor uit te voeren.

In de opdracht is er na uitvoerig onderzoek tot de conclusie gekomen welke technieken geschikt zijn om toegepast te kunnen worden om de Blockchain onderdelen Distributed Network en Identity Management te realiseren. Gedurende het afstudeertraject kon ik altijd met vragen terecht bij zowel mijn bedrijfsbegeleider, Ben Ooms, als de Blockchain expert, Pim Otte.

Hierbij bedank ik mijn begeleiders, vanuit Quintor en vanuit de opleiding, voor hun begeleiding, inzichten en ondersteuning tijdens het afstudeertraject. Daarnaast wil ik graag mijn mede afstudeerders bedanken voor hun meedenken en inzichten in het vinden van oplossingen. In het bijzonder bedank ik mede afstudeerder Kevin Bos, waarmee de samenwerking gedurende de opdracht aangenaam en productief is geweest.

Als laatste bedank ik mijn familie en vrienden voor hun ondersteuning, indirect of direct, niet alleen tijdens het afstuderen, maar ook tijdens mijn studieloopbaan. Zonder hun ondersteuning zou dit niet mogelijk geweest zijn.

Ik wens u veel leesplezier toe.

Jeffrey van Hoven
Den Haag, 1 juni 2018

# Inhoudsopgave

# Lijst van figuren

# Lijst van tabellen

# Woordenlijst

**D**

**DApps** Distributed Applications – Applicaties die gebruik maken van een Blockchain technologie, bijv. Ethereum, om op gedecentraliseerde wijze te interacteren met gebruikers. 19

**F**

**fork** Splitsing in het netwerk dat veroorzaakt is door een kleine wijziging in het protocol. 22

**full node** Node die alle functionaliteit kan uitvoeren die de Blockchain implementatie aanbiedt. 23

**H**

**Hard Fork** Een verandering in het Blockchain protocol die een nieuwe regel in het netwerk introduceert, waardoor het protocol geen compatibiliteit heeft met eerder versies. 22

**I**

**IPv6** Zesde versie van het Internet Protocol (IP). 56

**M**

**majority attack** Een aanval waarbij meer als 51% van de voting power in handen is van een kwaadwillende deelnemer. 35

**mining node** Node die als enige taak heeft om het mining proces uit te voeren. vii, 23

**N**

**node** Computer dat in verbinding staat met het netwerk van de Blockchain. vii, 23, 34, 35

**O**

**OTAP** Best practice voor inrichting software ontwikkelstraat, waarbij er een Ontwikkelomgeving, Testomgeving, Acceptatieomgeving en Productieomgeving gehanteerd wordt. 43, 44

**P**

**packet** Een encapsulatie van data dat gebruikt wordt door Transmission Control Protocol (TCP) en User Datagram Protocol (UDP) implementaties.. 48

**S**

**selfish mining** Aanval waarbij er door een kwaadwillende mining node blocks achtergehouden worden. 37

**Smart Contract** Een protocol dat gebruikt wordt om een digitale onderhandeling te faciliteren, verifiëren of forceren van een contract. 18, 19

**Soft Fork** Een verandering in het Blockchain protocol die terugwaartse compatibiliteit heeft met eerdere versies van het protocol. 22

**stake** Investering in de Blockchain proportioneel naar het type consensus, meestal gebruikt in PoS implementaties. 34

**T**

**tunnel** Communicatiekanaal zoals in gebruik bij Monero. 38

**W**

**wallet (node)** Node die een gereduceerde staat van het Blockchain bevat, waarin alleen de transacties opgenomen worden die betrekking hebben op de public- en private key combinatie. 23

# Afkortingen

**A**

**ATDD** Acceptance Test Driven Development. 45

**B**

**BDD** Behaviour-driven development. 45

**C**

**CI** Continuous Integration. 46

**D**

**DAG** Directed Acyclic Graph. 55
**DHT** Distributed Hash Table. 21

**I**

**I2P** The Invisible Internet Project. 38
**ICOs** Initial Coin Investment. 52
**IDE** Integrated Development Environment. 43
**IP** Internet Protocol. vii

**J**

**JVM** Java Virtual Machine. 43, 49

**N**

**NAT** Network Address Translators. iv, 56

**P**

**P2P** Peer-to-Peer. 21, 23, 48, 56
**PoS** Proof of Stake. vii, 38

**T**

**TCP** Transmission Control Protocol. vii, 48, 49, 50
**TDD** Test-driven Development. 45

**U**

**UDP** User Datagram Protocol. vii, 48

# 1 Inleiding

Dit verslag is geschreven in het kader van mijn afstudeeropdracht bij Quintor en dient ter beoordeling van de werkzaamheden die uitgevoerd zijn voor de bachelorstudie Informatica aan de Haagse Hogeschool.

Door de snelle groei van het Blockchain domein heeft Quintor in 2017 in samenwerking met DUO/-MinOCW, Groningen Declaration Network, Stichting ePortfolio Support, TNO en Rabobank, het Blockchain Field-lab Education gestart in Groningen. Het Blockchain-lab is opgezet om expertise en kennis uit te wisselen op regionaal, nationaal en internationaal gebied. De oprichting van het Blockchain Field-lab Education heeft er mede voor gezorgd dat Quintor meer kennis wilt opdoen over het Blockchain domein om zo inzicht te krijgen in hoe Blockchain technologie ingezet kan worden binnen vraagstukken vanuit klanten.

In hoofdstuk 2 is de organisatie beschreven waar het afstudeertraject heeft plaatsgevonden. Vervolgens wordt in hoofdstuk 3 de opdracht gepresenteerd. In hoofdstuk 4 wordt de aanpak van de opdracht onderbouwd en in hoofdstuk 5 worden de werkzaamheden van het vooronderzoek besproken waarin de basis van Blockchain technologie ter sprake komt. In hoofdstuk 6 wordt er aan de hand van de informatie uit het vooronderzoek een selectie van protocollen gemaakt die verder onderzocht zullen worden. In hoofdstuk 7 worden de verschillende onderdelen van de protocollen uitgelicht. Hoofdstuk 8 presenteert het advies dat gegeven wordt naar aanleiding van het gedane onderzoek. Hoofdstuk 9 beschrijft de keuzes die gemaakt zijn voor de indeling van het Proof of Concept en beschrijft kort de realisatie van het Peer-to-Peer netwerk. In hoofdstuk 10 wordt er geëvalueerd over de producten, de aanpak en de geselecteerde beroepstaken. Tot slot wordt er in hoofdstuk 11 aanbevelingen gegeven voor vervolgonderzoek.

# 2 | Quintor

*In dit hoofdstuk zal er inzicht gegeven worden over het bedrijf Quintor waar het afstudeerproject heeft plaatsgevonden. Er wordt verteld over de diensten die Quintor levert en wat de doelen zijn van de organisatie. Er zal ook kort toegelicht worden waar de afstudeerder binnen het bedrijf opereert en welke werknemers vanuit Quintor betrokken zijn bij de afstudeeropdracht.*

Quintor is een toonaangevend bedrijf op het gebied van Agile software development, Enterprise Java / .NET technologie en mobile development. Het bedrijf is begonnen in 2005 in Groningen en is opgericht door Johan Tillema, de huidige CEO van het bedrijf. Sinds 2005 heeft het bedrijf een gezonde groei doorgemaakt en heeft inmiddels 150 medewerkers, verspreid over vestigingen in Groningen, Amersfoort en Den Haag. Vanuit deze vestigingen ondersteunt het bedrijf klanten bij de uitdagingen die grootschalige Enterprise projecten met zich meebrengen. Het succes van Quintor is te danken aan drie pijlers: techniek en architectuur, een hoogwaardige ontwikkelstraat en het Agile/Scrum proces. Tevens beschikt Quintor over een Software Factory waarin in-house projecten voor klanten worden uitgevoerd.

## 2.1 Software Factory

In de Software Factory staat alle kennis en expertise die Quintor heeft verzameld over de jaren heen. Het is een hoogwaardig platform waarin de tooling, standaarden en best practices en tevens een complete oplossing is voor het managen en hosten van Scrum projecten. Dit wordt onder andere gebruikt om klanten te helpen bij het professionaliseren en efficiënter inrichten van softwareontwikkeling. Een groot deel van de werkzaamheden die Quintor dan ook uitvoert voor klanten is consultatie bij o.a. het implementeren van Agile/Scrum werk- en denkwijze. Naast Java en .NET development behoort ook mobile development tot de kerncompetenties van Quintor, en is dan ook opgenomen in de Software Factory. Hieronder zijn een aantal onderdelen uitgelicht die voorkomen in de Software Factory.

**Enterprise architectuur** Vanuit een pragmatische insteek en op basis van jarenlange ervaring helpen de software architecten van Quintor organisaties bij het maken van de juiste keuzes op het gebied van architectuur. Hierbij gaat het om het zowel opstellen als implementeren van een architectuur.

**Informatie analyse** Het in kaart brengen van informatie door het gebruik van diverse analyse- en ontwerptechnieken zoals UML, user-stories en use-cases in een Agile omgeving.

**Java en .NET development** Het realiseren van duurzame IT-systemen, in-house of bij klanten, die naadloos aansluiten bij de wensen van de business. Hierbij zijn er een groot aantal van omvangrijke systemen ontwikkelt.

**Agile/Scrum** Agile/Scrum is een effectieve en flexibele methode die uitgaat van een iteratiefontwikkelproces. Het trainen van complete projectteams met een op maat gemaakte training, waarbij aansluitend support en coaching gegeven wordt.

**Mobile development** Mobiele applicaties voor iPhone, iPad en Android. Specifiek hiervoor is het 'Mobile development center' opgezet, waarin er apps ontworpen, ontwikkelt en beheert worden. Dit betreft de realisatie van stand-alone tot volledige geïntegreerde Enterprise apps.

## 2.2 Visie

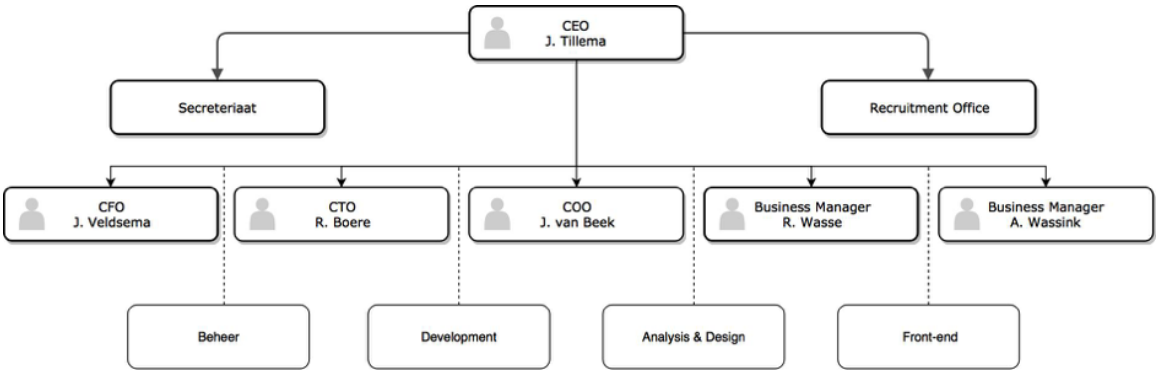
Een van de doelstellingen die Quintor heeft is het professionaliseren van software development. Aansluitend daarop probeert het bedrijf continu voor te lopen op de concurrentie door het opdoen van kennis op het gebied van nieuwe technologieën, waarbij professionalisering van de werkwijze voorop staat.

> "Onze ambitie: professionaliseren van software development."
> Johan Tillema, Chief Executive Officer

Door het aanbieden van uitdagende afstudeeropdrachten wordt er kennis opgebouwd die benodigd is om nieuwe technologieën, zoals bijvoorbeeld Machine Learning of Blockchain, in te zetten om klanten te adviseren bij de uitdagingen die grootschalige Enterprise projecten met zich meebrengen en zal, middels het volwassen genoeg is, opgenomen worden in de Software Factory.

## 2.3 Organisatie

In fig. 2.1 wordt de organisatie van Quintor weergegeven. Bovenaan staat Johan Tillema, de oprichter en CEO. Direct eronder staat het Secretariaat en het Recruitment Office. Hierin is te zien dat er vier segmenten zijn waarop er consultatie aangeboden wordt: development, analysis en design en front-end.




*Figuur 2.1: Organogram van Quintor.*

Zelf val ik onder het development segment, waarbij er aangestuurd wordt door Ben Ooms, (beschreven in 2.4). Er wordt zelfstandig gewerkt aan de opdracht waarbij er een aantal praktijken van Scrum toegepast zijn tijdens het afstudeertraject. Zo is er elke twee weken een zogenaamde demo dag waarbij iedere afstudeerder een demonstratie over waar hij of zij de afgelopen tijd mee bezig is geweest, en of er ergens tegenaan gelopen wordt zodat er samen nagedacht kan worden over mogelijke oplossingen.

## 2.4 Betrokkenen

Binnen Quintor zijn er een aantal medewerkers die nodig zijn om het project tot een geslaagd einde te brengen. Hieronder zijn deze medewerkers kort benoemd en wat hun rol is binnen het afstudeertraject.

**Ben Ooms** is de teamleider van Quintor Den Haag en is tevens de begeleider tijdens het afstudeertraject. Zijn uitvoerende taken hierbij zijn dan ook onder andere advies geven over de aanpak van de opdracht en waarbij mogelijk de voortgang van de opdracht te waarborgen.

**Pim Otte** is de Blockchain expert binnen Quintor en heeft veelal ervaring met de toepassing en realisatie van applicaties die gebruik maken van Blockchain technologie. Hij is beschikbaar gedurende de afstudeeropdracht om inzichten en feedback te geven op de uitgevoerde werkzaamheden.

**Kevin Bos** is afstudeerder afkomstig van Avans Hogeschool. Hij is verantwoordelijk voor het lokale gedeelte van de Blockchain opdracht. Tijdens de afstudeeropdracht is hij een stakeholder van het project en zal er een zekere mate van samenwerking aanwezig zijn.

## 2.5 Infrastructuur

Quintor maakt intensief gebruik van het Agile principe en dit is dan ook terug te vinden in de infrastructuur die ingericht is voor de consultanten binnen Quintor. Voor het uitvoeren van projecten wordt Atlassian JIRA gebruikt om het Agile proces te ondesteunen. Hierin is het mogelijk om taken te creëren en toe te wijzen aan projecten. Elke taak is dan individueel op te pakken door een team die op een bepaald project gezet is.

Voor het waarborgen van de kwaliteit van de software wordt er gebruik gemaakt van Atlassian BitBucket. BitBucket is een web-based versiebeheer systeem dat het Mercurial of Git revisiesystemen ondersteund. Daarnaast werkt het uitstekend samen met JIRA, waarbij het mogelijk is om naar taken die opgepakt zijn binnen JIRA te refereren binnen BitBucket.

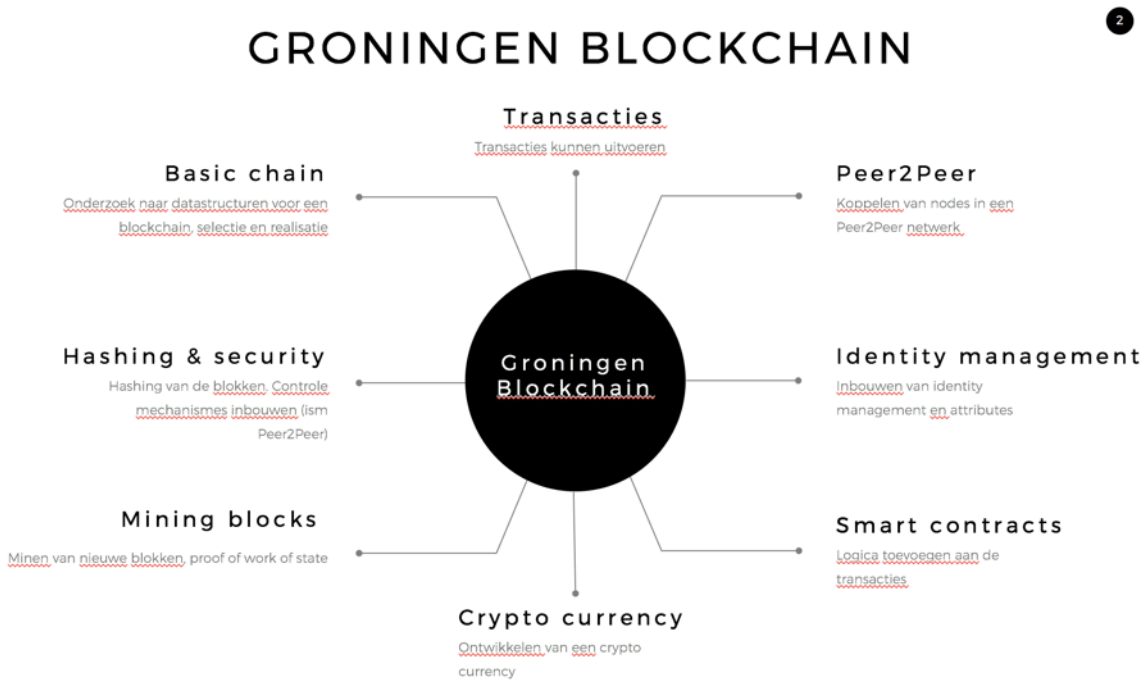
Communicatie binnen de organisatie gaat via het interne mail-systeem die functionaliteiten ondersteund zoals bijvoorbeeld het interne chat-systeem waarbij het mogelijk is om elke medewerker te benaderen en een kalender die het mogelijk maakt om afspraken te koppelen aan medewerkers en locaties.

# 3 Opdracht

*In dit hoofdstuk wordt de opdracht uitgelegd zoals gegeven door Quintor. Het betreft de aanleiding van de opdracht en het uiteindelijke doel Quintor wilt behalen door het faciliteren van de afstudeeropdracht.*

Sinds de opkomst van Bitcoin is de Blockchain technologie, de techniek die het mogelijk maakt om het op een gedecentraliseerde manier te laten werken, steeds populairder geworden. Alhoewel de Blockchain-technologie nog in de kinderschoenen staat, gaan de ontwikkelingen in het domein zeer snel. Zo worden er toepassingen bedacht die niet alleen voor de financiële markten interessant zijn, maar ook voor bijvoorbeeld het digitaliseren van contracten en contractbeheer.

Door de snelle groei van het Blockchain domein heeft Quintor in 2017 in samenwerking met DUO/-MinOCW, Groningen Declaration Network, Stichting ePortfolio Support, TNO en Rabobank, het Blockchain Field-lab Education gestart in Groningen. Het Blockchain-lab is opgezet om expertise en kennis uit te wisselen op regionaal, nationaal en internationaal gebied. De oprichting van het Blockchain Field-lab Education heeft er mede voor gezorgd dat Quintor afstudeeropdrachten aanbiedt voor het Blockchain domein om zo de huidige kennis over het domein uit te breiden en/of te toetsen.




*Figuur 3.1: De indeling van de Blockchain opdracht zoals gegeven door Quintor. Door het domein op te delen in segmenten is het mogelijk om elk individueel segment uit te lichten in de vorm van onderzoek, zoals te zien in bijlage* **??**.

Aangezien het Blockchain domein complex en veelomvattend is, is het domein opgedeeld in segmenten. De verschillende segmenten, zoals weergegeven in fig. 3.1, worden aangeboden als individuele afstudeeropdrachten. De focus van deze opdracht zijn de segmenten Peer2Peer en Identity Management, waarbij door middel van gestelde uitgangspunten op het gebied van snelheid, beveiligingsniveau en toepassingsmogelijkheden een Proof of Concept gerealiseerd dient te worden. Alvorens het Proof of Concept gerealiseerd kan worden, worden de alternatieve architecturen op het gebied van Peer2Peer en Identity Management in kaart gebracht. Dit wordt gedaan door het uitvoeren van literatuur onderzoek naar keuzes die gemaakt zijn in huidige Blockchain implementaties.

Daarnaast worden de volgende eisen gesteld aan het Proof of Concept:

1. Er worden geen Blockchain libraries gebruikt.
2. Het moet resistent zijn tegen aanvallen.
3. Het moet gedistribueerd zijn.
4. Er wordt op decentrale wijze consensus bereikt.

## 3.1 Probleemstelling

Aangezien de toepassing en adoptie van Blockchain technologie steeds groter wordt wil Quintor de toepassingsmogelijkheden en technieken onderzoeken om zo inzicht te kunnen krijgen in hoe het gebruikt kan worden in vraagstukken vanuit klanten. Dit brengt zich tot het probleem, namelijk dat Quintor onvoldoende kennis heeft van het Blockchain domein om de toepassing ervan te kunnen adviseren in vraagstukken vanuit klanten.

## 3.2 Doelstelling

Door het Blockchain domein op te delen in segmenten, te zien in fig. 3.1, is het mogelijk om de segmenten te behandelen in afstudeeropdrachten die Quintor aanbiedt. De focus in deze opdracht ligt op de Blockchain onderdelen Identity Management en Peer2Peer (Distributed Network). Hierdoor is er een globaal doel en een doel die specifiek voor deze opdracht geldt. Het streven van het globale doel is het opdoen van kennis omtrent het Blockchain domein door het realiseren van een Blockchain implementatie. Het doel van deze specifieke opdracht is middels het opstellen van een Proof of Concept van de Blockchain onderdelen Identity Management en Distributed Network, zonder gebruik te maken van bestaande Blockchain oplossingen, kennis te ontwikkelen voor Quintor op het gebied van Blockchain technologie.

## 3.3 Resultaat

Indien de opdracht succesvol afgerond is, zijn de segmenten Identity Management en het Distributed Network gerealiseerd en voldoen aan de volgende eisen die opgesteld zijn in de opdrachtformulering zoals gegeven door Quintor, in te zien in bijlage **??**.

1. Er worden geen Blockchain libraries gebruikt.
2. Het moet resistent tegen aanvallen zijn.
3. Het moet gedistribueerd zijn.
4. Er wordt op decentrale wijze consensus bereikt.

In samenwerking met de segmenten, Basic Chain, Hashing & security en Mining blocks, die gerealiseerd zullen worden door Kevin Bos wordt er een werkend Proof of Concept van een basale Blockchain implementatie gerealiseerd. Zowel het Proof of Concept als het onderzoek zal voor Quintor inzicht bieden in het Blockchain domein en de ontwikkelingen daarin.

### 3.3.1 Producten

Als onderdeel van de afstudeeropdracht zullen er verschillende producten worden opgeleverd aan Quintor en aan de Haagse Hogeschool. Deze staan hieronder gespecificeerd.

De op te leveren producten aan Quintor zijn:

- **Adviesrapport**
  Presentatie over de resultaten van het onderzoek waarin verschillende technieken geadviseerd worden die toegepast zijn in de realisatie van het Proof of Concept.

- **Sprint demo presentaties**
  Elke twee weken zal er een presentatie gegeven worden over de voortgang van het project waarbij het mogelijk is om feedback te krijgen over blokkades of aanpakken.

- **Broncode van het Proof of Concept**
  De gehele broncode van de applicatie waarin technieken vanuit het adviesrapport gerealiseerd zijn.

- **Onderzoeksrapport**
  De resultaten van het onderzoek dat uitgevoerd is om inzicht te krijgen in de segmenten Distributed Network en Identity Management.

De op te leveren producten aan de Haagse Hogeschool zijn:

- **Afstudeerscriptie**
  Beschrijving van het proces tijdens de uitvoering van de afstudeeropdracht ter beoordeling van de bekwaamheid van de student en de geselecteerde beroepstaken.

- **Verslag bedrijfsbezoek**
  Verslag van het bedrijfsbezoek dat tijdens het afstudeertraject gedaan wordt.

- **Voortgangsverslag**
  Verslag van de voortgang van de afstudeeropdracht.

# 4 | Aanpak

*In dit hoofdstuk wordt de aanpak van de opdracht besproken. Het beschrijft de beginsituatie zoals beschreven in het afstudeerplan, in te zien in bijlage* **??**.

## 4.1 Beginsituatie

De initiële beschrijving van de opdracht ging uit van criteria die nader gespecificeerd zou worden over aspecten van het Proof of Concept. Deze criteria zijn in de opdrachtomschrijving terug te vinden en gaan over snelheid, beveiliging en toepassingsmogelijkheden. Deze criteria zal gebruikt worden om de onderzoeksvragen op te stellen waarvan de antwoorden leiden tot de realisatie van het Proof of Concept.

De specificatie van deze criteria is de aanleiding geweest tot het houden van een serie gesprekken over waar Quintor heen wilt met de opdracht op het gebied van toepassingsmogelijkheden. Deze gesprekken zijn gehouden met de bedrijfsbegeleider en de Blockchain expert binnen Quintor waarbij er geprobeerd is een juiste toepassing te vinden die gerealiseerd kon worden binnen de beperkte tijd.

– Stukje over uiteindelijk situatie e.g. –

## 4.2 Projectinrichting

Binnen de opdracht zal er Agile gewerkt worden. Omdat een groot gedeelte van het project bestaat uit het doen van onderzoek zijn niet alle best practices overgenomen. Per twee weken zal er een demo gedaan worden met de huidige status van het project waarbij het mogelijk is om feedback te ontvangen over blokkades of werkzaamheden die uitgevoerd dienen te worden. Daarnaast wordt er onder de afstudeerders een dagelijkse stand-up gehouden over de status van het project, welke werkzaamheden er gepland staan en of er obstakels zijn.

## 4.3 Vooronderzoek

In het afstudeertraject wordt er met technologieën gewerkt welke onbekend zijn. Er is er dan ook voor gekozen om aan de hand van vooronderzoek kennis op te doen over het Blockchain domein.

Er zal eerst onderzocht worden wat een Blockchain is waarna er ingegaan wordt op de toepassingen ervan. Vervolgens zal er worden gekeken naar de architectuur van de Blockchain en uit welke componenten het bestaat. Uiteindelijk zal er kennis opgedaan worden voor de onderdelen Identity Management en Distributed Network om zo een afbakening te creëren van de onderdelen. Deze kennis zal gebruikt worden, in overleg met Quintor, om de opdracht vorm te geven en inzichten op te doen over de mogelijkheden met de opdracht.

Voor het opdoen van voorkennis zullen er gepubliceerde research papers, wiki's en blogs gebruikt worden. Hierna zal er een selectie van Blockchain implementaties gemaakt worden die bestudeerd zullen worden in het onderzoek.

## 4.4 Onderzoek

In de opdrachtomschrijving die aangeleverd is door Quintor zijn er geen duidelijke eisen en specificaties gesteld aan zowel de uitvoering als realisatie van de afstudeeropdracht. Dit heeft ertoe geleid dat er een gesprek gehouden is met de Blockchain expert en de bedrijfsbegeleider over de eisen, afbakening en in welke mate de samenwerking met de andere afstudeerder benodigd zal zijn. Hieruit is naar voren gekomen dat er wederom geen specifieke eisen zijn en dat de afstudeerder onderzoek dient te doen naar implementaties om een zo goed mogelijk functioneel overzicht te creëren van de onderdelen die toegekend zijn. Omdat de missie van Quintor het vooroplopen op het gebied van IT ontwikkelingen is, is ervoor gekozen om literatuuronderzoek te doen.

### 4.4.1 Opzet

Om een zo compleet mogelijk technische beschrijving van de werkingen van de gespecificeerde onderdelen te maken wordt er kwalitatief onderzoek uitgevoerd. Er wordt onderzoek gedaan door het uitvoeren van deskresearch. Er zullen specifieke cases, implementaties van de Blockchain technologie, geselecteerd worden aan de hand van de criteria die gesteld is in 'Inclusie- en exclusiecriteria'.

### 4.4.2 Adviesrapport

Om in overeenstemming met de opdrachtgever een toepassing te kiezen voor de functionaliteiten en/of technieken die onderzocht zijn in de geselecteerde protocollen, zal er een adviesrapport opgesteld worden waarin deze technieken en/of technologieën aangeraden worden.

## 4.5 Proof of Concept

De uitgekozen technieken zullen gerealiseerd worden in een Proof of Concept. Dit zal in samenwerking zijn met de andere afstudeerder, die het lokale gedeelte van de Blockchain ontwikkeld. De onderdelen dienen samen te werken tot een functionele Blockchain implementatie, waarbij er overlap zal zijn in de keuzes binnen de pakketselectie en realisatie.

**Requirements** Er dienen criteria opgesteld te worden aan de hand van het resultaat van het onderzoek die van toepassing zijn op de realisatie van het Proof of Concept. Om te achterhalen wat de eisen en de toepassing waaraan het Proof of Concept moet voldoen zullen er informele interviews gehouden worden waarin requirements achterhaald worden.

**Selecteren methoden** Voor het opzetten van een development workflow en de technieken die daarbij te pas komen in overeenstemming met Quintor zullen er beslissingen gemaakt worden op de manier waarop het Proof of Concept gerealiseerd gaat worden. Tevens zal hierbij gekeken worden naar de uitvoering van realisatie op bestaande implementaties.

## 4.6 Planning

Voor de uitvoering van het project is een globale planning opgezet die te vinden is in tabel 4.1.

| **Activiteit** | **Van** | **Tot** |
|---|---|---|
| Orientatie | Week 1 | Week 2 |
| Onderzoek | Week 3 | Week 7 |
| Advies | Week 8 | Week 9 |
| Selecteren methoden | Week 10 | Week 11 |
| Ontwikkelen | Week 11 | Week 15 |
| Testen | Week 16 | Week 17 |
| Overdracht | Week 17 | - |

*Tabel 4.1: Globale planning*

Waarbij de fases bestaan uit de volgende werkzaamheden:

- **Orientatie**
  - Opstart
  - Vooronderzoek
  - Plan van Aanpak
  - Onderzoeksopzet
  - Probleemanalyse
- **Onderzoek**
  - Onderzoek
  - Selectie implementaties
  - Theoretisch kader
  - Bezoek begeleidend examinator
- **Advies**
  - Adviesrapport
  - Orientatie indeling
  - Schrijven
  - Voorleggen
- **Selecteren methoden**
  - Orientatie ontwikkelen Blockchain
  - Selectie taal
  - Ontwikkelomgeving
  - Testen
- **Testen**
  - Integratie
- **Overdracht**

# 5 Vooronderzoek en resultaten

*In dit hoofdstuk wordt er een introductie gegeven in het Blockchain domein. Deze kennis is benodigd om het onderzoek uit te voeren en om het Proof of Concept te realiseren. Daarnaast zal deze kennis helpen om de uitvoering van de opdracht te begrijpen. Het vooronderzoek dient tevens om overeenstemming te krijgen met de opdrachtgever over de richting van het onderzoek. Zoals verteld in de aanpak zijn er weinig eisen gesteld aan de uitvoering en toepassing van de afstudeeropdracht, waardoor het wenselijk is om een gezamenlijke overeenstemming te krijgen van wat mogelijk is met het onderzoek.*

Het vooronderzoek betreft kwalitatief-, exploratief onderzoek dat uitgevoerd wordt door middel van deskresearch. Om de vragen te beantwoorden is er gebruikgemaakt van zowel blogs en websites en is ervoor gekozen om de definities welke in het vooronderzoek voorkomen te beschrijven vanuit het Bitcoin protocol, zoals beschreven door Nakamoto (2008). Om de technische kennis te versterken voor de realisatie van het Proof of Concept is er een Coursera course gevolgd, Bitcoin and Cryptocurrency Technologies, waarin het Bitcoin protocol uitgelegd wordt. Dit is gevolgd omdat de beschrijving van het Bitcoin protocol niet meer toereikend is naar de huidige staat van de implementatie.

Er wordt ingegaan op de basis van Blockchain technologie waarna er gekeken wordt naar de mogelijke toepassingen. Vervolgens komt de architectuur van een Blockchain aan bod, waarbij de vraag “Uit welke componenten bestaat een Blockchain implementatie?"wordt behandeld. Om een afbakening te maken voor het onderzoek wordt er gekeken naar wat de onderdelen Distributed Network en Identity Management bevatten. Concreet staan de vragen die behandeld worden in het vooronderzoek hieronder weergegeven.

1. Wat is Blockchain technologie?
2. Waarvoor wordt Blockchain technologie gebruikt?
3. Uit welke onderdelen bestaat een Blockchain?
4. Waaruit bestaat het onderdeel Distributed Network binnen Blockchain technologie?
5. Waaruit bestaat het onderdeel Identity Management binnen Blockchain technologie?

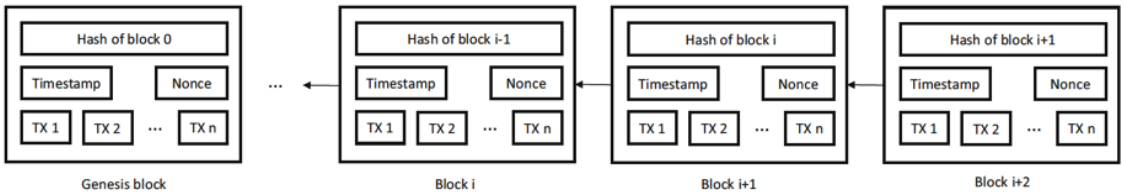
## 5.1 Blockchain

*In dit hoofdstuk wordt de vraag "Wat is Blockchain technologie?"behandeld. Het betreft het vergaren van kennis over de basis van het Blockchain begrip waarbij er ingegaan wordt op wat Blockchain is en welke eigenschappen het heeft. Door het beantwoorden van deze vraag wordt er een definitie vastgesteld van Blockchain technologie die gebruikt wordt in het gehele verslag.*

Een blockchain is een gedistribueerde database die bestaat uit een keten van in de computer of op internet vastgelegde en samengevoegde gegevens genaamd blocks. Om deze reden wordt blockchain technologie ook wel vergeleken met een grootboek. In zekere mate is dit correct maar het omschrijft niet het meest vooraanstaande aspect van blockchain, namelijk dat het gedecentraliseerd opereert.

Om de analogie voort te zetten; een grootboek is in handen van één organisatie waarin transacties van of naar de organisatie vastgelegd worden. Dit betekent dat er een centrale autoriteit is die kan bepalen of er überhaupt wel transacties plaatsvinden, of erger, het systeem buiten gebruik kan stellen. Daarnaast is de centrale autoriteit ook in staat misbruik te maken door bijvoorbeeld transacties te registreren naar de eigenaar van het grootboek. Dit brengt een risico met zich mee die blockchain technologie oplost door het grootboek te verspreiden over een netwerk dat ervoor zorgt dat deze centrale autoriteit niet meer nodig is.

Een traditionele blockchain is weergegeven in fig. 5.1. De keten van gegevens wordt bepaald door de volgorde waarin de gegevens zijn toegevoegd. Er is daarbij een eenvoudig te controleren systeem volgens welke voorafgaande blokken aan elkaar gerelateerd behoren te zijn. Door de inhoud van het vorige block crypto grafisch te versleutelen (ook wel hashen genoemd) en deze sleutel op te nemen in een opeenvolgend blok wordt ervoor gezorgd dat gegevens van eerdere blokken niet meer gemuteerd kunnen worden. Wanneer dit wel gebeurt zou de ketting verbroken worden omdat er een nieuwe sleutel gegenereerd wordt en opeenvolgende blokken zullen refereren naar een foutieve sleutel.




*Figuur 5.1: Voorbeeld van een blockchain (Zheng et al., 2016).*

### 5.1.1 Eigenschappen

Zheng, Xie, Dai, Chen en Wang (2017)[Key Characteristics of Blockchain, p.5] stelt dat er vier eigenschappen zijn die een Blockchain definiëren:

**Decentralisatie** In traditionele gecentraliseerde transactie systemen wordt iedere transactie gevalideerd door een centrale vertrouwde organisatie (e.g. banken), waardoor er een bottleneck gecreëerd wordt door de transacties te verwerken door centrale informatiesystemen. In contrast daarmee is een derde partij niet meer nodig in blockchain systemen. Consensus algoritmes zorgen ervoor dat data consistent is binnen het netwerk.

**Persisentie** Transacties kunnen snel gevalideerd worden en invalide transacties zullen niet toegelaten worden. Het is bijna onmogelijk om te transacties verwijderen of ongedaan te maken als ze zijn opgenomen in de blockchain.

**Anonimiteit** Elke gebruiker van het systeem kan interacteren zonder zijn ware identiteit kenbaar te maken.

**Controleerbaarheid** In bitcoin wordt de balans van een gebruiker opgeslagen door gebruik te maken van het Unspent Transaction Output (UTXO) model. Elke transactie refereert naar eerdere unspent transacties. Wanneer de huidige transactie is opgenomen in de blockchain, zal de staat van alle gerefereerde transacties verandert worden van “unspent"naar “spent". Hierdoor zijn transacties makkelijk te valideren en te traceren.

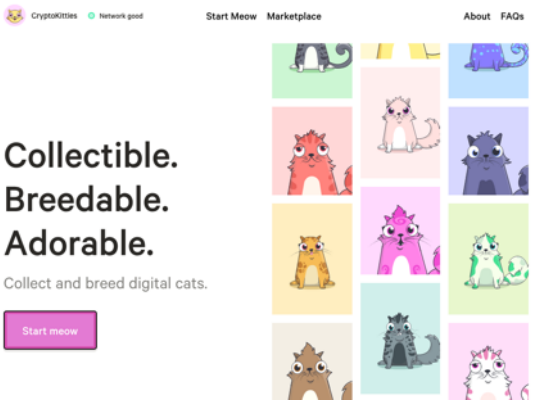
## 5.2 Toepassing

*In dit hoofdstuk wordt de vraag "Waarvoor wordt Blockchain technologie gebruikt?" beantwoord. Deze vraag is opgesteld omdat er geen toepassing bekend is voor de te realiseren Blockchain onderdelen, zoals aangegeven in de beschrijving van de aanpak. Het antwoord op deze vraag dient om de opdrachtgever te informeren in wat er mogelijk is met Blockchain technologie om zo een toepassing te kiezen voor het te ontwikkelen Proof of Concept.*

*Er is in het bijzonder aandacht geschonken aan Blockchain als development platform aangezien de opdrachtomschrijving, bijlage* **??***, spreekt over de realisatie van het onderdeel Smart Contract. Uitleg over het onderdeel Smart Contracts is beperkt gebleven aangezien het buiten de scope van de opdracht valt.*

Blockchain technologie wordt steeds vaker toegepast voor het opzetten van een gedecentraliseerd systeem. Aangezien de bekendste toepassing van blockchain technologie een financieel systeem is wordt het vaak gezien als technologie die specifiek bedoeld is om financiële diensten te ondersteunen. In de literatuur wordt er echter veel geëxperimenteerd en gespeculeerd over andere mogelijke toepassingen van blockchain technologie.

Zo stelt Atzori, (2015) bijvoorbeeld dat blockchain technologie ingezet kan worden om de politiek en de maatschappij te veranderen. In een andere studie gedaan door Crosby, Pattanayak, Verma en Kalyanaraman, (2016) wordt er onderscheid gemaakt tussen financiële en niet-financiële toepassingen die mogelijk veranderd kunnen worden door blockchain technologie. Een aantal voorbeelden die gegeven worden zijn de toepassingen bij verzekeringen, gedecentraliseerde opslag en domeinregistratie. In fig. 5.2 is een afbeelding te zien van de website van CryptoKitties, een van de eerste spellen die gebruik maakt van blockchain technologie, namelijk het Ethereum netwerk.




*Figuur 5.2: CryptoKitties, een spel dat gebruik maakt van Blockchain technologie.*

### 5.2.1 Ontwikkelplatform

Blockchains als Ethereum, EOS en HyperLedger bieden hun functionaliteit aan als development platform. Het stelt ontwikkelaars in staat om hun eigen toepassingen te realiseren, zogenaamde DApps.

*Listing 5.1: Smart contract voor "The Greeter" geschreven in Solidity, zoals gepresenteerd in een tutorial voor Smart Contracts op het Ethereum netwerk (Ethereum, 2017).*

```
contract Mortal {
  /* Define variable owner of the type address */
  address owner;

  /* This function is executed at initialization and sets the owner of the
      contract */
  function Mortal() { owner = msg.sender; }

  /* Function to recover the funds on the contract */
  function kill() { if (msg.sender == owner) selfdestruct(owner); }
}

contract Greeter is Mortal {
  /* Define variable greeting of the type string */
  string greeting;

  /* This runs when the contract is executed */
  function Greeter(string _greeting) public {
      greeting = _greeting;
  }

  /* Main function */
  function greet() constant returns (string) {
      return greeting;
  }
}
```

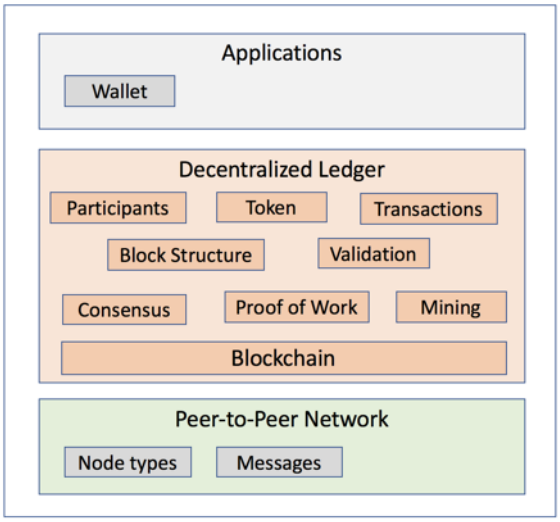
Door het gebruik van Smart Contracts, te zien in fig. 5.1, is het mogelijk om functionaliteit bij transacties te voegen om extra handelingen, die niet gerelateerd zijn tot de kern van een Blockchain implementatie, uit te voeren. Hieronder is een voorbeeld gegeven wat er mogelijk is met betrekking tot DApps.

**CryptoKitties** is een spel dat gebruikt maakt van het Ethereum platform, bestaand uit verzamelbare en fokbare digitale katten. De uitwisseling en het fokken van CryptoKitties wordt vastgelegd in het Ethereum netwerk door middel van Smart Contracts. Wanneer twee CryptoKitties gefokt worden, wordt het uiterlijk en de eigenschappen van hun nageslacht bepaald door het 256-bits genoom van elke ouder en een toeval element, wat leidt tot 4 miljard mogelijke genetische variaties (Zen, A., 2017).

## 5.3 Architectuur

*In dit hoofdstuk wordt de vraag "Uit welke componenten bestaat een Blockchain implementatie?" behandeld. Het antwoord op deze vraag dient om een duidelijk beeld te scheppen welke componenten betrekking hebben op de onderdelen Distributed Network en Identity Management en tevens gebruikt zal worden als afstemming met zowel de opdrachtgever als de medeafstudeerder, Kevin Bos.*

In fig. 9.1 is een overzicht weergegeven van de onderdelen en componenten waaruit een Blockchain bestaat. In de applicatie laag is de wallet te vinden die een gebruiker van de Blockchain doorgaans gebruikt om transacties te verrichten. De onderliggende functionaliteit van de wallet doet niets meer als het bijhouden van public- en private keys van de gebruiker waarop de nog niet uitgegeven tokens (cryptocurrency, contracten, diensten) geregistreerd staan.




*Figuur 5.3: Blockchain architectuur*

De Decentralized Ledger is de kern van de technologie en zorgt ervoor dat de globale blockchain consistent en fraudebestending blijft. De fundamentele structuur achter de gehele technologie is de blockchain, waar transacties gegroepeerd worden in blokken en elk blok crypto grafisch verbonden wordt met het vorige blok. Een transactie is een vorm van uitwisseling van tokens tussen deelnemers, ook wel nodes genoemd, van het systeem. Voordat transacties als valide worden beschouwd, ondergaan ze een validatie proces die uitgevoerd wordt door alle nodes in het systeem. Het proces van het groeperen van transacties in een blok dat toegevoegd wordt aan het einde van de blockchain wordt ook wel minen genoemd. Om er zeker van te zijn dat er overeenstemming is onder alle deelnemers over welke blockchain legitiem is, wordt er gebruik gemaakt van een Proof-of-Work algoritme tijdens het mining proces om te bepalen welke ketting de meeste inspanning vereist.

Het laatste component is het peer-to-peer netwerk, waarin verschillende node types gedefinieerd zijn. Zo heb je bijvoorbeeld de validatie node die transacties valideert en een mining node die het mining process uitvoert. Om de Decentralized Ledger bij te werken en te onderhouden communiceren de nodes met elkaar door middel van het versturen van berichten.

## 5.4 Gedistribueerd netwerk

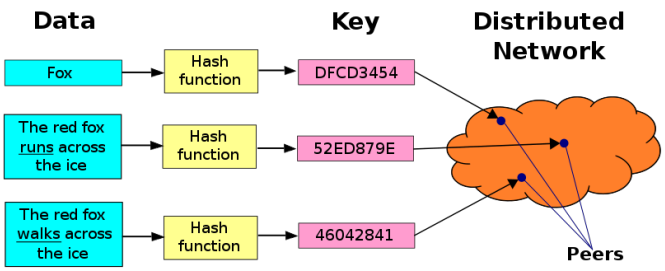
*In dit hoofdstuk wordt de vraag "Waaruit bestaat het onderdeel gedistribueerd netwerk binnen Blockchain technologie?" behandeld. Bij deze vraag wordt er gekeken naar de geïdentificeerde onderdelen uit hoofdstuk 5.3. Er wordt een korte introductie gegeven in peer-to-peer netwerken en waarom het een belangrijk onderdeel is bij het realiseren van de eigenschappen, behandeld in hoofdstuk 5.1, van een Blockchain implementatie. Het antwoord op deze vraag zal helpen bij het selecteren van zoektermen die gebruikt worden om inventarisatie te doen op de onderdelen die het Distributed Network omvat.*

Het onderdeel Distributed Network bestaat uit het verspreiden, uitbreiden en het behalen van consensus over de staat van de Blockchain tussen de deelnemers aan het netwerk. Om dit te doen wordt er gebruik gemaakt van een Peer-to-Peer (P2P) implementatie waarbij het mogelijk is om een lokale versie van de ketting aan te bieden aan andere nodes binnen het P2P netwerk, om zo de huidige chain up-to-date te houden met wijzigingen die gedaan zijn door de verschillende verbonden nodes. Dit leidt tot een complex probleem dat beschreven wordt als het Byzantine Generals Problem (Lamport et al., 1982), wat beschrijft aan de hand van een abstract voorbeeld dat het essentieel is voor een betrouwbaar computersysteem om te kunnen gaan met fouten die optreden in een of meer van de componenten, waardoor het kan voorkomen dat er conflicterende informatie verstuurd wordt naar de andere componenten van het systeem.

**Peer-to-Peer**

De term P2P betekend dat alle computers die deel uit maken van het netwerk, peers van elkaar zijn, gelijk aan elkaar zijn, er geen speciale "nodes"zijn en dat alle deelnemers in het netwerk de last delen van het leveren van netwerkdiensten (Antonopoulos, 2014, p.171). Het is een techniek die cruciaal is voor Blockchain en de doelen die het probeert te behalen. P2P systemen verdelen namelijk de kosten om data te delen – opslag voor bestanden en bandbreedte voor het versturen van de bestanden – over de deelnemers van het netwerk, waardoor applicaties kunnen schalen zonder krachtige, dure servers (Bawa et al., 2003).

Een van de bekendste toepassingen van een peer-to-peer netwerk is het creëren van een gedecentralizeerd file-sharing protocol. Implementaties hiervan zijn BitTorrent, LimeWire en Gnutella. Om een bestand te distribueren wordt het opgesplitst in delen, waarbij er een hash gecreëerd wordt voor elk deel. Wanneer een andere deelnemer van het netwerk een deel ontvangt wordt er gekeken aan de hand van de hash of het onderdeel geen fouten bevat. Bestanden worden geregistreerd in het netwerk door het opnemen van de hashes in een zogenaamde *tracker* die gebruik maakt van een Distributed Hash Table (DHT). Een voorbeeld van een DHT is te zien in fig. 5.4.




*Figuur 5.4: Door het vertalen van data naar een cryptografische sleutel is het mogelijk om aan de hand van de sleutel de data op te vragen aan peers die de data bezitten.*

**Consensus**

Consensus is een dynamische manier van het behalen van overeenstemming in een groep. In blockchain implementaties wordt het gebruikt om overeenstemming te behalen over de staat van het netwerk en de volgorde waarin transacties gedaan zijn. Met het consensus algoritme wordt er een zekere mate van veiligheid gewaarborgd, waardoor het voor een kwaadwillende deelnemer (bijna) onmogelijk dient te zijn om het netwerk te beïnvloeden. Het kan voorkomen dat een kwaadwillende deelnemer probeert het netwerk te beïnvloeden waardoor er tegenstrijdige consensus kan optreden en een fork ontstaat in het netwerk.

**Fork**

Een fork is een splitsing in het netwerk die veroorzaakt is door een verandering in het protocol of door het toedoen van kwaadwillende deelnemer(s). Er zijn hiervoor twee categorieën forks, een Hard Fork en een Soft Fork.

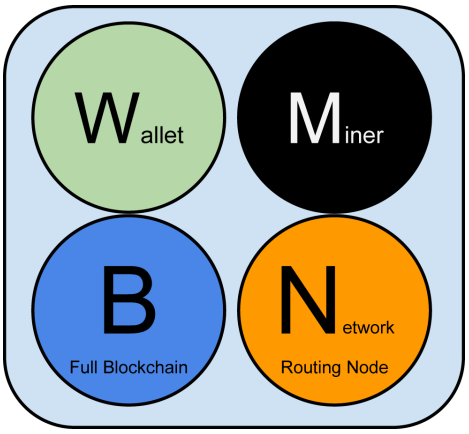
**Soft fork** is een verandering in het netwerk die terugwaartse compatibiliteit heeft met eerdere versies van het protocol. Als voorbeeld kan er voor gekozen worden dat in plaats van blocks een limiet hebben van 1MB, de regel aangepast wordt zodat blocks een grootte van 500K moeten hebben. Als een Soft Fork verkeerd gaat is het nog steeds mogelijk dat er een Hard Fork optreed ( Castor, A. , 2017, Soft Fork).

**Hard fork** is een protocol update waarbij een nieuwe regel geïntroduceerd wordt, waardoor het netwerk geen compatibiliteit heeft met oudere versies. Dit zorgt ervoor dat deelnemers in het netwerk die een oudere versie hebben, de nieuwe transacties als invalide beschouwen. Een voorbeeld van een regel waarbij een Hard Fork ontstaat is bijvoorbeeld het ophogen van de block grootte naar 2MB in plaats van 1MB ( Castor, A. , 2017, Hard Fork).

**Nodes**

Alhoewel de structuur van een Blockchain dezelfde structuur afdwingt voor de nodes in het netwerk, kunnen zij een verschillende rol spelen. Alle nodes binnen het netwerk valideren, verspreiden en ontdekken en onderhouden connecties met andere nodes binnen het netwerk. In fig. 5.5 is te zien welke services een full node in het Bitcoin netwerk aanbiedt.

Een **full node** is een collectie van functies, namelijk routing, de blockchain database, het mining proces en wallet services en bevat een gehele kopie van de actuele blockchain. Een **wallet (node)** is een deelnemer in het netwerk die een subset van de gehele blockchain bevat om transacties te versturen, verifiëren en ontvangen. De **mining nodes** concurreren voor het creëren van een nieuw block door het uitvoeren van het Proof-of-Work algoritme.




*Figuur 5.5: Een bitcoin netwerk node die alle functies bevat: wallet, mining, blockchain database en netwerk routing, (Antonopoulos, 2014, p. 172).*

Alle nodes binnen het netwerk bieden gelijke diensten aan en kunnen gebruik maken van dezelfde diensten terwijl ze samenwerken door middel van een consensus protocol.

De verschillende services binnen het netwerk en de node types die hieraan meewerken is dan ook een architecturale keuze over de indeling van het P2P netwerk.

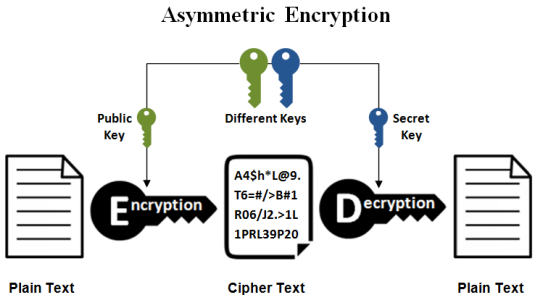
## 5.5 Identiteit

*In dit hoofdstuk wordt de vraag "Waaruit bestaat het onderdeel Identity Management binnen Blockchain technologie?" behandeld. Zoals beschreven in hoofdstuk 5.1 zijn anonimiteit en controleerbaarheid belangrijke eigenschappen van een Blockchain implementatie. Allereerst zal er beschreven worden wat identiteit inhoud binnen een Blockchain en welke mogelijke vormen van management er zijn. Het antwoord op deze vraag wordt gebruikt om zoektermen op te stellen en een afbakening te creëren voor de te onderzoeken protocollen.*

Identificatie wordt doorgaans gedaan aan de hand van de public key van een gebruiker. Public key cryptografie is een essentieel onderdeel van het Bitcoin protocol en wordt gebruikt voor verschillende doeleinden om de integriteit van berichten die verstuurd worden te waarborgen. Public key cryptografie bestaat uit twee onderdelen:

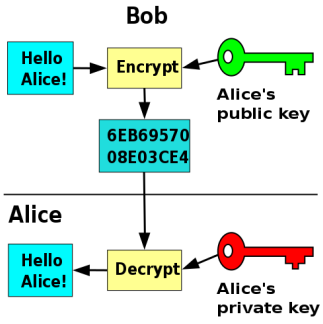
- Public key
  Een key die verstuurd wordt om aan te tonen dat een bericht daadwerkelijk verstuurd is door de maker van het bericht, door het ondertekenen van het bericht.

- Private key
  Een key die geheim wordt gehouden en gebruikt wordt om te valideren dat een public key valide is.




*Figuur 5.6: Asymmetrische encryptie door middel van Public key cryptografie zoals in gebruik bij het Bitcoin protocol.*

In fig. 5.6 is te zien hoe het gebruikt kan worden om tekst te versleutelen en alleen leesbaar te maken voor de ontvanger. Fig. 5.7 laat zien hoe dit in zijn werk gaat met twee actoren. Bob stuurt een bericht naar Alice, waarbij de public key van Alice gebruikt wordt om het bericht te versleutelen. Om het bericht te kunnen lezen kan Alice gebruik maken van haar eigen private key.




*Figuur 5.7: Het gebruik van asymmetrische encryptie om berichten die verstuurd worden op het netwerk te versleutelen.*

In het Bitcoin protocol is elke coin terug te leiden naar een eigenaar waarbij er gebruik gemaakt wordt van de public key. Wanneer er coins van eigenaar wisselen worden de coins overgezet naar de public key van de ontvanger en wordt het getekend met de private key van de verstuurder. Dit zorgt ervoor dat iedereen in het netwerk weet dat het bericht authentiek is (Bitcoin Wiki, 2010, “How bitcoin works”).

### 5.5.1 Autorisatie

Zheng et al. (2017) deelt Blockchain implementaties op in drie categorieën, waarin de zichtbaarheid en participatie in het consensus proces gelimiteerd.

**Public** In een public Blockchain zijn alle transacties publiekelijk inzichtbaar en iedereen in het netwerk maakt onderdeel uit van het consensus proces. Dit wordt ook wel gezien als een permissionless Blockchain.

**Consortium** In een consortium Blockchain is er een groep van vooraf geselecteerde nodes die deel uitmaken van het consensus proces. De consortium Blockchain wordt meestal gebruikt door meerdere organisaties en is gedeeltelijk gedecentraliseerd. Omdat bepaalde nodes geïdentificeerd dienen te worden wordt dit type Blockchain gezien als een permissioned Blockchain.

**Private** In een private Blockchain worden alleen nodes van een specifieke organisatie toegelaten tot het consensus proces. Het wordt ook wel als een centraal netwerk gezien omdat het in volledige controle is van één organisatie. Omdat het hier gaat om volledige restrictie tot het Blockchain netwerk wordt dit type Blockchain gezien als een permissioned Blockchain.

In een consortium en private Blockchain dient de gebruiker zich te identificeren aan de hand van een identiteit. Bitcoin maakt gebruik van public- en private keys om de gebruiker te identificeren. Dit hanteert in zekere mate een permissie model waarbij de autorisatie van een gebruiker vastgelegd word aan de hand van de identificatie (i.e. de public key) die het netwerk gebruikt.

#### Privacy

Een van de doelen van Blockchain is totale anonimiteit, alleen zijn er een aantal problemen die volledige anonimiteit tegengaan. Om de terminologie duidelijk te maken wordt hieronder het verschil tussen pseudoniem en anoniem uitgelegd aan de hand van voorbeelden vanuit het Bitcoin protocol.

> “Anonymity is the state of being not identifiable within a set of subjects, the anonymity set." Pfitzmann en Köhntopp (2001).

**Pseudoniem** Een pseudoniem is een referentie naar je ware identiteit. Een voorbeeld hiervan is het burgerservicenummer (BSN). Door het geven van je BSN is niet direct je ware identiteit terug te leiden.

**Anoniem** Wanneer je anoniem bent, ben je niet meer te identificeren binnen een set van soortgelijke identiteiten. Een voorbeeld hiervan is anoniem bellen. Hierbij wordt er gebruik gemaakt van het maskeren van het pseudoniem, namelijk het telefoonnummer.

In feite komt het neer op de identificatie van de handelingen die gedaan worden door de gebruiker. Hiervoor bestaat een term, unlinkability, dat beschrijft wanneer een gebruiker meerdere keren interacteert met het systeem deze handelingen niet terug te leiden zijn naar elkaar.

### Privacy in Bitcoin

In Bitcoin is de identiteit van de gebruiker, de public key(s), een pseudoniem. Aangezien Bitcoin een permissionless model heeft, waarbij iedereen elke transactie kan inzien, is het mogelijk om transacties die gedaan zijn door dezelfde public key terug te leiden naar elkaar.

Een analyse model geïntroduceerd door Reid en Harrigan (2013) maakt gebruik van twee modellen van het Bitcoin netwerk, waarbij er een model gemaakt wordt voor bitcoins tussen transacties, en bitcoins tussen gebruikers. Door het gebruik van de voortgestelde analyse is het mogelijk om meerdere public keys met elkaar te associëren.

## 5.6 Obstakels

In het vooronderzoek is er weinig gevonden over Identity Management en zelf wist ik dan ook niet goed wat dit onderdeel voor functionaliteiten bevat. In eerste instantie is er gekeken naar de verschillende types van Blockchain, waarbij gebruikers van het systeem autorisatie hebben tot bepaalde acties. Om een beter beeld te schetsen en de afbakening van het onderdeel compleet te maken voor het onderzoek is er besloten om een gesprek te houden met de Blockchain Expert.

Uit dit gesprek is naar voren gekomen dat het Identity Management gedeelte gaat over hoe de Blockchain implementatie met public keys (de identiteit van een gebruiker) omgaat. Als tip werd er gegeven om te kijken naar de wallet software indien beschikbaar. Dit is software die de public- en private key beheert voor een gebruiker. Daarnaast is er ook een tip gegeven over het onderdeel Distributed Network. Om een goed beeld te krijgen van de aanvallen waar het netwerk tegen bestand is, is het handig om een threat model op te stellen.

## 5.7 Conclusie

Naar aanleiding van de resultaten uit het vooronderzoek zijn er keuzes gemaakt die zich reflecteren in het onderzoek. Hieronder is per vraag beschreven over de implicaties die de resultaten gaven tegenover het onderzoek.

Uit de vraag “Waaruit bestaat het onderdeel Distributed Network binnen Blockchain technologie?” is gebleken dat het consensus proces invloed heeft op de structuur van het netwerk. Het soort consensus zal dan ook gebruikt worden om de verschillende type Distributed Networks te onderscheiden. Ook zullen de verschillende type van nodes onderzocht worden om te identificeren welke bijdrage een bepaald type node levert om het netwerk in stand te houden.

In de resultaten van de vraag “Waaruit bestaat het onderdeel Identity Management binnen Blockchain technologie?” is er geïdentificeerd dat er twee manieren zijn waarop de privacy van de gebruiker gewaarborgd wordt, namelijk of het een permissionless of permissioned Blockchain is en de identificatie van de gebruiker binnen het netwerk. Er wordt aangegeven dat het niveau van privacy en autorisatie ligt aan de categorie van waar de Blockchain deel van uitmaakt.

1. Zichtbaarheid van acties die de gebruiker onderneemt op de Blockchain.
2. Autorisaties voor acties die de gebruiker wilt ondernemen op de Blockchain.

# 6 | Selectie protocollen

Om het onderzoek binnen de beschikbare tijd te houden is er in overleg met de Blockchain Expert voor gekozen om een initiële selectie van de top 20 verhandelde cryptocurrencies te bekijken, waarna er een selectie van vier implementaties gemaakt wordt gebaseerd op de beschikbare informatie, het type consensus en hoe het omgaat met de identiteit van de gebruiker. Deze vier implementaties zullen vervolgens uitvoerig onderzocht en beschreven worden op de werking van de onderdelen Distributed Network en Identity Management.

### 6.0.1 Coinmarketcap

De selectie van de top 20 verhandelde cryptocurrencies wordt gedaan aan de hand van de website Coinmarketcap. Hierop zijn meerdere overzichten te zien die te maken hebben met de handelsvolume van cryptocurrencies.
Een van de overzichten is het maandelijkse handelsvolume zoals te zien in fig. 6.1. Deze lijst is gebruikt voor het selecteren van de initiële top 20 van cryptocurrencies. Door de architecturen achter de meest verhandelde cryptocurrencies te gebruiken wordt ervoor gezorgd dat er robuuste en volwassen implementaties bekeken worden.

| # | Name | Symbol | Volume (1d) | Volume (7d) | Volume (30d) |
|---|---|---|---|---|---|
| 1 | Bitcoin | BTC | $5,728,630,000 | $47,024,950,272 | $239,937,765,888 |
| 2 | Ethereum | ETH | $1,653,700,000 | $13,056,842,240 | $93,063,570,688 |
| 3 | Tether | USDT | $1,958,830,000 | $16,378,062,592 | $84,926,233,088 |
| 4 | Ripple | XRP | $357,324,000 | $4,156,748,960 | $39,850,125,664 |
| 5 | Litecoin | LTC | $1,285,160,000 | $6,746,461,952 | $26,736,620,416 |
| 6 | Bitcoin Cash | BCH | $376,441,000 | $2,973,709,568 | $20,046,743,072 |
| 7 | Ethereum Cla... | ETC | $646,646,000 | $5,532,372,672 | $15,749,806,368 |
| 8 | EOS | EOS | $188,493,000 | $1,532,097,920 | $15,605,236,864 |
| 9 | Cardano | ADA | $266,120,000 | $1,252,818,648 | $13,445,324,392 |
| 10 | NEO | NEO | $123,156,000 | $1,072,350,408 | $9,084,051,800 |
| 11 | Qtum | QTUM | $90,423,900 | $847,290,136 | $8,218,878,888 |
| 12 | TRON | TRX | $172,623,000 | $1,071,585,984 | $6,733,278,384 |
| 13 | Status | SNT | $29,635,700 | $199,291,636 | $6,500,340,332 |
| 14 | Stellar | XLM | $42,479,700 | $422,246,356 | $4,661,325,352 |
| 15 | Huobi Token | HT | $105,098,000 | $910,926,360 | $3,566,953,088 |
| 16 | ATMCoin | ATMC | $50,360,800 | $537,747,432 | $3,060,712,860 |
| 17 | Dash | DASH | $68,725,100 | $594,435,760 | $2,883,398,448 |
| 18 | VeChain | VEN | $92,665,100 | $599,619,288 | $2,767,577,812 |
| 19 | Lisk | LSK | $38,802,300 | $568,389,712 | $2,547,525,232 |
| 20 | Zcash | ZEC | $52,432,700 | $433,916,424 | $2,477,751,772 |
| 21 | Monero | XMR | $44,197,000 | $530,603,416 | $2,265,885,760 |
| 22 | Hshare | HSR | $55,382,500 | $412,009,240 | $2,249,269,776 |
| 23 | ICON | ICX | $39,998,600 | $223,640,806 | $2,201,559,444 |
| 24 | Nano | NANO | $125,487,000 | $1,053,026,588 | $1,979,299,038 |
| 25 | Binance Coin | BNB | $45,055,600 | $312,276,692 | $1,935,435,524 |

*Figuur 6.1: Meest verhandelde cryptocurrencies in de maand februari zoals gepresenteerd op de website van Coinmarketcap.*

#### Hard forks

Om te voorkomen dat er soortgelijke implementaties bekeken worden is ervoor gekozen om de hard forks niet mee te nemen in de initiële selectie. Een voorbeeld hiervan is Bitcoin Cash ten opzichte van Bitcoin. Alhoewel Bitcoin Cash een aantal veranderingen doorgemaakt heeft sinds de afsplitsing van het Bitcoin protocol, wordt het niet meegenomen omdat er in zekere mate overeenkomsten aanwezig zijn.

### 6.0.2 Attributen

Om een selectie te maken tussen de top 20 verhandelde cryptocurrencies is er gekeken naar attributen die nader beschreven zijn in onderstaand tabel.

*Tabel 6.1: Attributen opgesteld voor initiële selectie implementaties.*

| | |
|---|---|
| **Identity Management** | Of de implementatie actief iets onderneemt dat te maken heeft met Identity Management, e.g. het vergroten van de privacy van de gebruiker. |
| **Whitepaper** | Of de implementatie een technische whitepaper beschikbaar heeft. |
| **Open-source** | Of er een referentie implementatie open-source beschikbaar is voor het bestuderen van de code. |
| **In circulatie sinds** | Een indicatie van de volwassenheid van de implementatie. |
| **DApps platform** | Of het gebruikt kan worden als development platform. Hierbij zal er een zekere mate van modulariteit nodig zijn in de broncode. |
| **Consensus** | Welk consensus algoritme gebruikt wordt. Dit is van invloed op de werking van het onderdeel Distributed Network. |

Het doel van de attributen is een indicatie te krijgen over de hoeveelheid documentatie die een implementatie beschikbaar heeft. Dit is dan ook de doorslaggevende factor geweest bij het selecteren van vier implementaties die nader onderzocht zullen worden.

**Totstandkoming**

Hieronder wordt kort beschreven hoe de inventarisatie van de attributen gedaan is.

**Identity Management** Om vast te stellen of een implementatie iets onderneemt in de vorm van Identity Management wordt er gebruik gemaakt van bestaande literatuur over de implementatie. Door middel van het scannend lezen van de beschikbare literatuur wordt er vastgesteld of er beschrijvingen zijn van de identiteit binnen de Blockchain implementatie en hoe dit tot stand is gekomen.

**Whitepaper** Bijna elke Blockchain implementatie heeft een website waarin de functionaliteiten gepresenteerd worden voor de mogelijke gebruiker. Om erachter te komen of er een whitepaper beschikbaar is, is een scan van de website voldoende.

**Open-source** Om na te gaan of een implementatie open-source is wordt er gezocht op Github en Bitbucket op de aanwezigheid van de organisatie en/of protocol naam.

**In circulatie sinds** Om de circulatiedatum te achterhalen is gebruik gemaakt van Wikipedia. Hierbij is een schatting van de datum waarop de Blockchain implementatie actief is geworden al voldoende.

**DApps platform** Om na te gaan of de implementatie de ontwikkeling van gedistribueerde applicaties ondersteund is er gezocht naar development tutorials op de websites van de Blockchain implementatie.

**Consensus** Het type consensus dat gebruikt wordt is tevens te achterhalen uit de besschikbare documentatie en wordt achterhaald door scannend te lezen.

### 6.0.3 Selectie

Aan de hand van deze attributen is een lijst opgesteld, te zien in tabel **??**, waarin de initiële selectie te vinden is met bijbehorende attributen van de implementatie. Over sommige implementaties zoals VeChain is weinig informatie gevonden waardoor ze direct afvallen. Aan de hand van deze attributen zijn de volgende protocollen geselecteerd.

**Cardano** is een Blockchain protocol waarin onderzoek centraal staat. Het beweert dan ook het eerste blockchain platform te zijn die ontstaan is uit een filosofisch en onderzoek gedreven aanpak. De implementatie van het protocol is volledig open-source en er is een technische whitepaper beschikbaar. Daarnaast is er ook een platform om je eigen applicaties op het netwerk te creëren.

**Monero** is een implementatie die beweert dat de gebruiker volledig ontraceerbaar is. Het is net zoals Cardano een volledige open-source implementatie en maakt gebruik van egalitair Proof of Work. Daarnaast heeft het protocol een technische whitepaper.

**Bitcoin** is het originele protocol waarin de Blockchain technologie gerealiseerd is. Door de grote hoeveelheid onderzoek die gedaan is naar Bitcoin is er een overvloed van informatie, waarin niet alleen informatie over Bitcoin gegeven wordt maar ook over het Blockchain domein. De implementatie van het protocol is wederom volledig open-source en er is een technische whitepaper beschikbaar.

**EOS** is een relatief nieuw protocol die zojuist een test netwerk gelanceerd heeft. Ook deze implementatie is beschreven in een whitepaper, is volledig open-source en kan gebruikt worden als platform om applicaties op te ontwikkelen. Consensus binnen het protocol wordt bereikt door Delegated Proof of Stake.

# 7 Onderzoek

*In dit hoofdstuk worden de werkzaamheden met betrekking tot het uitvoeren van het onderzoek beschreven. De aanleiding voor het onderzoek is te vinden in hoofdstuk 4, waarin wordt beschreven waarom dit onderzoek meerwaarde heeft binnen de opdracht.*

Het onderzoek dient voor het opstellen van het adviesrapport waarin protocollen worden gepresenteerd aan Quintor die mogelijk geïmplementeerd kunnen worden tijdens de realisatie van het Proof-of-Concept. Het betreft exploratief onderzoek waarin case-study gebruikt wordt om een gedetailleerde omschrijving van de onderdelen Identity Management en Distributed Network op op te stellen van Blockchain implementaties die geselecteerd zijn in hoofdstuk 6. De kennis die hiermee wordt opgebouwd kan eventueel gebruikt worden in vervolgonderzoek.

In het onderzoek staat de onderstaande hoofdvraag centraal:

> Welke protocol implementaties kunnen toegepast worden om de onderdelen Distributed Network en Identity Management te realiseren voor een Blockchain implementatie?

Omdat de hoofdvraag te groot is om in een keer te beantwoorden is het opgesplitst in de volgende deelvragen:

1. "Welke soorten gedistribueerde netwerken worden er gebruikt?"
2. "Hoe werken de gedistribueerde netwerken en tegen welke gevaren zijn ze bestendig?"
3. "Hoe wordt er omgegaan met de identiteit van de gebruiker?

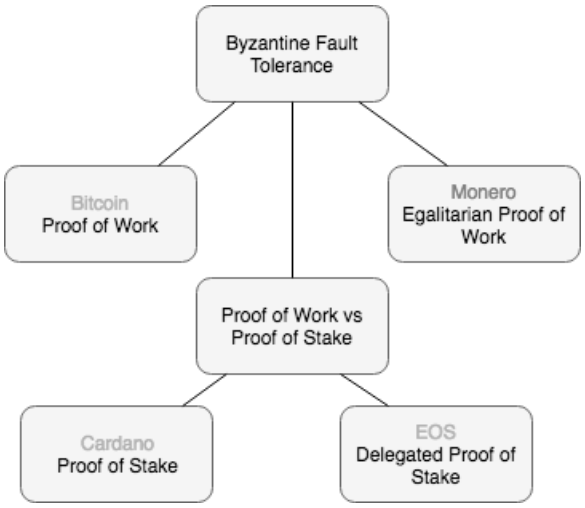
Op de volgende pagina's is per deelvraag behandeld wat de bijdrage van het antwoord oplevert aan de doelstelling, hoe de vraag beantwoord is en wordt er concreet de bevindingen besproken.

## 7.1 Soorten netwerken

*In dit hoofdstuk wordt de vraag "Welke soorten gedistribueerde netwerken worden er gebruikt?" behandeld. Het doel van de vraag is om de architectuurkeuzes op het gebied van het Distributed Network onderdeel op te stellen, en waar mogelijk is de implicaties van de keuze tegenover het Identity Management onderdeel.*

### 7.1.1 Aanpak

In fig. 7.1 is te zien welke (globale) termen er gebruikt zijn om de benodigde informatie te vinden. In de meeste gevallen is de beschikbare whitepaper van de implementatie voldoende geweest om de werking van het consensus te beschrijven. Hieronder is de werkwijze en denkwijze uitgeschreven per individueel onderdeel.




*Figuur 7.1: Termen die als leidraad gebruikt zijn om het resultaat te beschrijven*

#### Byzantine Fault Tolerance

Om deze vraag te beantwoorden is allereerst gezocht naar achtergrondinformatie over consensus en wat het doel ervan is. In het vooronderzoek is er informatie gevonden over het Byzantine Generals Problem (Lamport et al., 1982), waarin, vertaald naar de IT-wereld, wordt gesteld dat het essentieel is voor een betrouwbaar computersysteem om te gaan met fouten in de componenten, waardoor het kan voorkomen dat er conflicterende informatie verstuurd wordt naar de andere componenten van het systeem.

#### Proof of Work

Hierna zijn bij de implementaties de manier waarop consensus behaald wordt onderzocht. Voor het beschrijven van het Proof of Work algoritme is er gebruik gemaakt van de originele presentatie van het Bitcoin protocol door Nakamoto (2008), hierin was alle informatie te vinden die benodigd was. Het egalitarian Proof of Work zoals in gebruik bij Monero is beschreven in Van Saberhagen (2013) waarin de verschillen en tekortkomingen van het Proof of Work zoals in gebruik bij Bitcoin uiteengezet wordt.

**Proof of Stake**

Om een indicatie te geven van de grootste tekortkomingen op het gebied van Proof of Work en redenenen waarom Blockchain implementaties kiezen voor het implementeren van Proof of Stake is er gebruik gemaakt van de whitepaper van Cardano Kiayias et al. (2017), waarin de gemotiveerd wordt waarom er voor Proof of Stake is gekozen in plaats van Proof of Work. Naar aanleiding van de primaire reden, namelijk dat Proof of Work enorm veel stroom verspilt, is er gezocht naar een studie die deze claim kan bevestigen, waarbij de studie van O'Dwyer en Malone (2014) gebruikt is om dit te bevestigen.

Bij het beschrijven van Delegated Proof of Stake zoals in gebruik bij EOS, bleek de whitepaper niet voldoende informatie te bevatten om het functioneel te beschrijven. Hiervoor is er dan ook een artikel gebruikt dat geschreven is door Roman, K. (2018), waarin het algoritme uitgelegd wordt.

### 7.1.2 Conclusie

Een gedistribueerd netwerk binnen Blockchain is getypeerd aan het consensus protocol dat gebruikt wordt. In het onderzoek zijn er twee primaire soorten geïdentificeerd, netwerken die gebruik maken van Proof of Stake of van Proof of Work, waarbij Proof of Work gebruik maakt van de rekenkracht van een node en Proof of Stake gebruik maakt van de stake van een node.

## 7.2 Functionaliteit en gevaren

*In dit hoofdstuk wordt de vraag "Hoe werken de gedistribueerde netwerken en tegen welke gevaren zijn ze bestendig?" behandeld. Het doel van de vraag is om de werking van het gedistribueerd netwerk in kaart te brengen en tegenmaatregelen tegen aanvallen die in de functionaliteit verwerkt zitten te beschrijven.*

Deze vraag is opgesteld naar aanleiding van de criteria "het moet resistant zijn tegen aanvallen" die gesteld is in de opdrachtformulering zoals gegeven door Quintor, in te zien in bijlage **??**. Het eerste idee om deze vraag te beantwoorden was om een vergelijking te maken tussen de implementaties op het gebied van veiligheid, waarbij er onderzocht zou worden of een aanval op de implementatie uitgevoerd was. Dit zou uiteindelijk een "beste" implementatie opleveren die geadviseerd zou worden in het adviesrapport. Uiteindelijk is dit idee niet gebruikt omdat er een aantal redenenen zijn waarom dit niet zou werken:

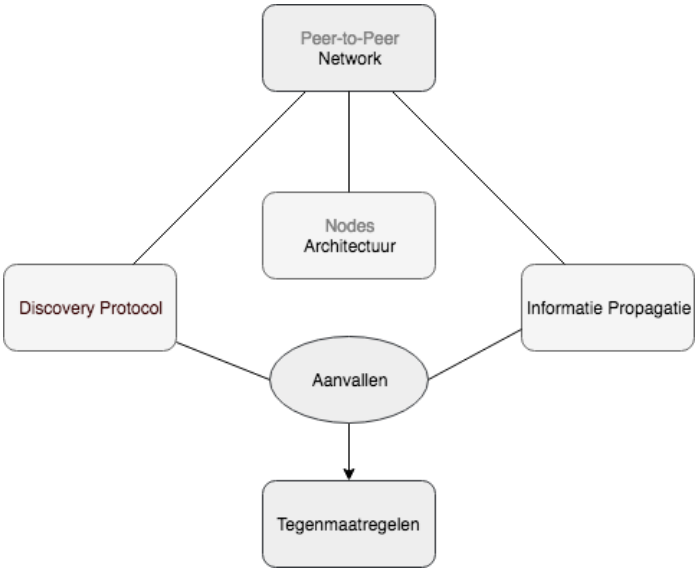
- **Protocol volwassenheid**
  Het Bitcoin protocol bestaat al sinds 2011, terwijl het Monero protocol sinds 2014 bestaat. In het begin heeft Bitcoin waarschijnlijk veel te verduren gehad qua aanvallen, waardoor het via bovenstaande vergelijking slecht uit zou komen. Daarentegen heeft Monero gedurende de drie jaar zowel verbeteringen als lessen getrokken uit het Bitcoin protocol.

- **Adoptie van de technologie**
  Proof of Work implementaties zijn vatbaar voor een majority attack, waarbij een gebruiker 51% van de rekenkracht binnen het netwerk in handen moeten hebben om transacties in de Blockchain te registreren zonder dat er validatie te pas komt. Hoe minder gebruikers, hoe minder de benodigde rekenkracht om dit uit te voeren.

Om deze reden is er besloten om met de Blockchain expert over de aanpak en uiteindelijke doel van deze vraag te discussiëren, wat ertoe heeft geleid dat de focus van de vraag veranderd is van een vergelijking doen op basis van de veiligheid, het een meer beschrijvende vorm heeft gekregen waar er gekeken wordt naar componenten van het netwerk: discovery protocol, hoe informatie verstuurd wordt tussen twee nodes en wanneer mogelijk de knelpunten met betrekking tot aanvallen binnen deze componenten.

### 7.2.1 Aanpak

In fig. 7.1 is te zien welke componenten er gebruikt zijn om de benodigde informatie te vinden. Hieronder is de werkwijze en denkwijze uitgeschreven per individueel onderdeel.




*Figuur 7.2: Componenten en termen die als leidraad gebruikt zijn om het resultaat te beschrijven.*

#### Aanvallen

Allereerst is er begonnen met het zoeken naar de verschillende aanvallen die mogelijk zijn op Blockchain implementaties. Binnen het gesprek met de Blockchain Expert is hierbij het woord threat model gevallen, en zijn er een aantal aanvallen aan bod gekomen:

- **Eclipse attack**
  Meer informatie en de definitie van een eclipse attack is gevonden in de studie van Heilman, Kendler, Zohar en Goldberg (2015).

- **Majority attack**
  De majority attack staat beschreven op de wiki van Bitcoin, waarbij er uitgelegd wordt wat het is, wat er mee mogelijk is en waarom het bijna niet uit te voeren is.

- **Denial of Service**
  Bij Denial of Service gaat het om meerdere manieren om de uitvoering van processen binnen het netwerk te verstoren, waardoor er niet een specifieke bron te vinden is voor alle mogelijke aanvallen.

- **Sybil attack**
  Voor het beschrijven van de sybil attack in relatie tot Blockchain is er gebruik gemaakt van de studie gedaan door Conti, Lal, Ruj et al. (2017).

- **Double spending**
  Informatie double spending is gevonden in de studie van Karame, Androulaki en Capkun (2012).

Een van de knelpunten bij het beschrijven van een aanval was een studie vinden die aantoonde wat het gevolg ervan was binnen een Blockchain implementatie.

**Network**

Voor het beschrijven van de verschillende netwerken is er gebruikt gemaakt van niet wetenschappelijke bronnen zoals wiki's of blogs. De reden hiervoor is dat een whitepaper van een Blockchain implementatie zelden de architectuur van het netwerk beschrijft. Deze informatie is dan ook gebruikt om de verschillende componenten van het netwerk te beschrijven.

### 7.2.2 Conclusie

**Bitoin** Het netwerk van Bitcoin communiceert via TCP/IP en maakt gebruik van bootstrap nodes waarmee connectie wordt gemaakt op het moment dat een nieuwe deelnemer het netwerk wilt toetreden. Informatie wordt verstuurd door een voorafgedefinieerde set aan berichttypes: *inv*, *tx*, *block*, *getdata*, waarbij een *inv* bericht gebruikt wordt ter inventarisatie over de beschikbaarheid van data, *tx* bericht om een transactie te versturen, *block* bericht om een block te versturen, *getdata* bericht om data op te vragen.

Op het Bitcoin netwerk zijn meerdere aanvallen in de loop der jaren uitgevoerd en geïdentificeerd, een studie uit 2015 gedaan door Heilman et al. (2015) toont aan dat het Peer Discovery mechanisme vatbaar is voor een Sybil Attack. Nakamoto (2008) stelt dat de voordelen van het uitvoeren van een majority attack niet opweegt tegen de kosten voor de benodigde hardware om de rekenkracht te behalen. Eyal en Sirer (2014) beschrijft dat het niet nodig is om een merendeel van de rekenkracht te bezitten en introduceert de aanval selfish mining.

**Cardano** Het netwerk van Cardano communiceert via TCP/IP en maakt gebruik van het Kademlia protocol waardoor het maar nodig is om één bootstrap node te gebruiken om het netwerk toe te treden. De achterliggende structuur van Kademlia is een Binary Tree waarbij de positie van een deelnemer in de Binary Tree bepaald wordt door een unieke prefix van de identificatiecode. Het protocol garandeert dat een deelnemer in verbinding staat met ten minste één andere deelnemer. Informatie wordt uitgewisseld door drie abstracte berichttypes: *inv*, *req*, en *data*. Het *inv* bericht wordt gebruikt om aan te geven dat er data beschikbaar is, het *req* bericht wordt gebruikt om beschikbare data op te vragen en het *data* bericht wordt vervolgens gebruikt om de data te versturen.

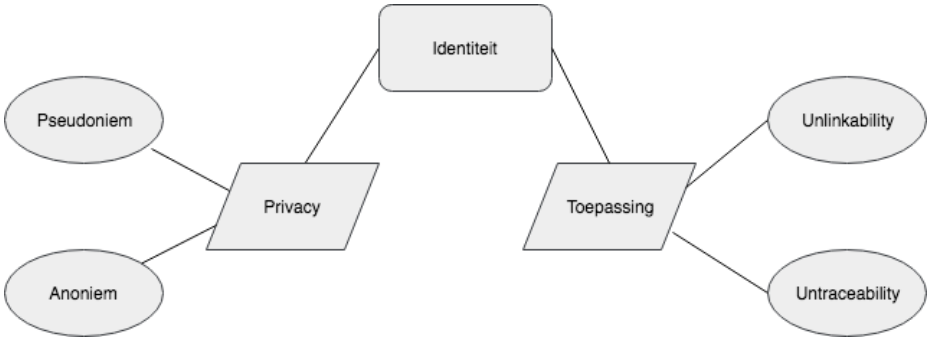
Implementaties die gebruik maken van PoS zijn afhankelijk van de manier waarop een leiderschapsverkiezing wordt gesimuleerd, waarbij er grote kans is dat het gevoelig is voor beïnvloedingen van kwaadwillende deelnemers in het netwerk in de vorm van een Sybil Attack. Cardano heeft een zwak punt in het Kademlia netwerk geïdentificeerd waardoor het mogelijk zou zijn om Eclipse Attack uit te voeren.

**Monero** Het netwerk van Monero maakt gebruik van het The Invisible Internet Project (I2P) protocol, dat zowel UDP/IP als TCP/IP ondersteund. Om het netwerk toe te treden wordt er gebruik gemaakt van bootstrap nodes die vastgelegd zijn in de broncode. Communicatie wordt gedaan door middel van Tunnels, waarbij elke deelnemer twee Tunnels, een inkomende en een uitgaande, heeft voor elke connectie.

**EOS** *Ten tijde van het onderzoek is er geen technische beschrijving beschikbaar over het netwerk component van EOS.*

## 7.3 Identiteit

*In dit hoofdstuk wordt de vraag "Hoe wordt er omgegaan met de identiteit van de gebruiker binnen de implementatie?" behandeld. Het doel van de vraag is om de mogelijkheden en toepassingen van identiteit te beschrijven aan de hand van de geselecteerde implementaties.*




*Figuur 7.3: Termen die als leidraad gebruikt zijn om het resultaat te beschrijven*

### 7.3.1 Aanpak

In fig. 7.3 is te zien welke componenten er gebruikt zijn om de benodigde informatie te vinden. In het vooronderzoek is er gevonden dat identiteit eigenlijk uit twee onderdelen bestaat binnen Blockchain implementaties. Het privacy gedeelte, wat bepaalt of de identiteit zoals in gebruik bij de implementatie pseudoniem of anoniem is. Daarnaast is de toepassing van de identiteit van belang. Een voorbeeld van de toepassing van de identiteit is bijvoorbeeld het ondertekenen van transacties.

#### Identiteit

In het vooronderzoek is er ook vastgesteld dat de identiteit van een gebruiker en hoe het gebruikt wordt is terug te leiden naar de architectuur van de Blockchain. De kern van Blockchain implementaties met betrekking tot identiteit en de toepassing daarvan is het gebruik van public- en private key cryptografie. Bij dit onderdeel was het belangrijk om niet teveel te beschrijven van de onderliggende cryptografie, omdat dit buiten de scope van de vraag valt.

### 7.3.2 Conclusie

**Bitcoin** is een public Blockchain waarbij de gehele historie van transacties publiekelijk in te zien is. Een deelnemer in het Bitcoin netwerk wordt geïdentificeerd aan de hand van zijn public key. Deze public key wordt onder andere opgenomen in transacties om de betaler en de ontvanger te registreren. In een studie gedaan door Reid en Harrigan (2013) wordt er een analyse model opgezet dat aantoont dat het Bitcoin protocol niet aan de untraceability eis voldoet.

**Cardano** is een public Blockchain waarbij de gehele historie van transacties publiekelijk in te zien is. Cardano maakt gebruik van public- en private key cryptografie om pseudonimiteit te waarborgen. Deze keys worden gebruikt om een transactie van een bestemming te voorzien, waarbij er drie definities van adressen gebruikt worden: een public key address, een script address en een redeem address.

**EOS** is een consortium Blockchain waarbij gebruikers zichzelf identificeren met een unieke naam van maximaal twaalf karakters. Om te participeren binnen het netwerk dient er toegang verleent te worden door een authenticatie proces alvorens de deelnemer wordt toegelaten. Handeling binnen het netwerk worden gevalideerd door een Role Based Permissie systeem, waarbij permissies gekoppeld zijn aan actions die vastgelegd zijn in de lokale database.

**Monero** is een public Blockchain waarbij de gehele historie van transacties publiekelijk in te zien is. Binnen Monero heeft elke deelnemer een account die gebaseerd is op twee keys: Spend Key en een View Key. Door het afleiden van een eenmalige public key, ook wel een Stealth Address genoemd, uit de Spend Key en View Key garandeert het Monero protocol unlinkability. Untraceability wordt behaald door het gebruik van Ring Signatures. Hierbij worden meerdere Stealth Addresses toegevoegd aan een transactie, waarbij een afkomstig van de verstuurder van de transactie en de rest aangevuld door eerder gebruikte Stealth Addresses in de Blockchain. Hierdoor wordt de herkomst van een transactie gemaskeerd.

## 7.4 Conclusie

In het onderzoek is er een selectie van Blockchain implementaties onderzocht op de onderdelen Identity Management en Distributed Network. Door het uitvoeren van exploratief onderzoek waarin case-study gebruikt is om een gedetailleerde omschrijving van desbetreffende onderdelen op te stellen. De hoofdvraag *Welke protocol implementaties kunnen toegepast worden om de onderdelen Distributed Network en Identity Management te realiseren voor een Blockchain implementatie?* is opgedeeld in deelvragen:

1. "Welke soorten gedistribueerde netwerken worden er gebruikt?"
2. "Hoe werken de gedistribueerde netwerken en tegen welke gevaren zijn ze bestendig?"
3. "Hoe wordt er omgegaan met de identiteit van de gebruiker?

Uit de resultaten van de deelvragen is uiteindelijk een antwoord op de hoofdvraag gekomen. Voor het onderdeel Distributed Network kan er gebruik gemaakt worden van:

**Kademlia** Een bestaand protocol gerealiseerd door Maymounkov en Mazieres (2002). Dit protocol heeft een aantal wijzigingen binnen Cardano, zoals het versturen van informatie gaat over TCP/IP en er is een uitbreiding gemaakt op de manier waarop identificatiecodes toegekend worden aan deelnemers om een mogelijke Sybil Attack uit te sluiten.

**Bitcoin** Communicatie binnen het Bitcoin netwerk verloopt over TCP/IP waarbij informatie wordt verstuurd door inv, tx, block en getdata berichten. Het maakt gebruik van Proof of Work om consensus te bereiken over de staat van de Blockchain.

**Monero** De Monero implementatie is gefocust op het bevorderen van de privacy binnen Blockchain implementaties. Voor het netwerk is dat dan ook niet anders. Het maakt gebruik van The Invisible Project om anonimiteit in het netwerk te waarborgen.

Voor het onderdeel Identity Management is het mogelijk om de volgende protocollen toe te passen:

**Bitcoin** het Bitcoin protocol maakt gebruik van het UTXO-model, waarin public- en private keys gebruikt worden om de betaler en ontvanger te registreren binnen een transactie. Door het gebruik van het analysemodel gepresenteerd door Reid en Harrigan (2013) is aangetoond dat Bitcoin niet aan de untraceability en unlinkability eis voldoet.

**EOS** maakt gebruik van een account-model, waarin een gebruiker een unieke naam van maximaal twaalf karakters hanteert als identiteit. Daarnaast hanteert EOS een Role Based Permission Management systeem, waarbij het mogelijk is actions en handlers te definiëren.

# 8 | Adviesrapport

*Aan het uitgeven van een officieel advies is niet toegekomen. Tijdens de laatste fase van het project is de tijd die bestemd was voor het adviesrapport, besteed aan het realiseren en ontwerpen van het Proof-of-Concept.*

In een gesprek met de bedrijfsbegeleider, Blockchain expert en medeafstudeerder Kevin Bos, is naar voren gekomen dat de belangrijkste eis van het Proof of Concept het aantonen van modulariteit is. Hiermee is dan ook rekening gehouden tijdens het ontwerpen van het Proof of Concept, waarbij het uitgangspunt een consortium Blockchain is met mogelijkheid tot autorisatie via een permissiemodel, geïnspireerd door EOS, een account-model waarin er gebruik wordt gemaakt van standaard public- en private key cryptografie. Het Distributed Network zal gebaseerd zijn op het Kademlia protocol waarbij de berichtenstructuur van Cardano gerealiseerd zal worden.

# 9 Proof of Concept

*In dit hoofdstuk komen de werkzaamheden omtrent het Proof of Concept aan bod. Het betreft de realisatie van Blockchain onderdelen Distributed Network en Identity Management zoals beschreven in bijlage* **??**. *Allereerst wordt er ingegaan op de keuzes bij het opzetten van de infrastructuur benodigd voor de realisatie van het Proof of Concept, waarna er ingegaan wordt op de inventarisatie van verschillende componenten binnen de benoemde Blockchain onderdelen.*

## 9.1 Ontwikkelstraat

Een ontwikkelstraat staat aan de basis van succesvolle softwareontwikkeling, en zorgt voor een duidelijke structuur tijdens de ontwikkeling van het Proof of Concept. Hierbij wordt er gebruik gemaakt van de OTAP aanpak, waarbij er voor elke fase van het ontwikkeltraject een omgeving beschikbaar is.

### 9.1.1 Programmeertaal

In de opdrachtformulering zoals beschreven door Quintor, te vinden in bijlage **??**, zijn er twee keuzes voor de programmeertaal voorgesteld, C# of Java, waarmee het Proof of Concept gerealiseerd dient te worden. De keuze hierbij is al snel gevallen op Java, aangezien de afstudeerder voldoende kennis heeft van de semantiek van de taal, waardoor er tijdswinst behaald wordt. Tevens is de bedrijfsbegeleider een Java ontwikkelaar en is het mogelijk om hem te benaderen wanneer er Java expertise benodigd is.

#### Kotlin

Gezien recente ontwikkelingen in de Java wereld is er in overeenstemming met de andere afstudeerder voorgesteld om het Proof-of-Concept te realiseren in Kotlin. Kotlin is een programmeertaal ontwikkeld door Jetbrains, een bedrijf dat bekend staat om hun wijde assortiment aan Integrated Development Environment (IDE)'s. Ze zochten een nieuwe programmeertaal die een verbetering op Java zou zijn, maar nog steeds compatible is voor migratiedoeleinden. Naar aanleiding hiervan heeft Jetbrains een team opgezet dat zich bezig ging houden met het ontwikkelen van deze nieuwe programmeertaal. Deze programmeertaal is Kotlin geworden en heeft in februari 2016 een 1.0 release gehad. De programmeertaal is volledig open-source en compileert naar de Java Virtual Machine (JVM), waardoor Java en Kotlin tegelijkertijd gebruikt kunnen worden. Dit is een belangrijk

punt aangezien dit betekend dat alle libraries die beschikbaar zijn voor Java, ook gebruikt kunnen worden in Kotlin (Pieter Otten, 2017).

Het doel van het gebruiken van Kotlin is dan ook om de adoptiesnelheid, de werking, en de ervaring aan te tonen aan Quintor, zodat ze kunnen overwegen om deze programmeertaal in te zetten. In overleg met de bedrijfsbegeleider is dit goed bevonden.

### 9.1.2 Versiebeheer

Quintor maakt gebruik van GitLab voor het toepassen van versiebeheer. GitLab is een applicatie met features voor de gehele software development en DevOps lifecycle. Het is een open-source project en wordt gebruikt door meer dan 100.000 organisaties en heeft een community van 1900 developers die bijgedraagt hebben aan de ontwikkeling van de code (GitLab, 2018). Aangezien alle functionaliteiten voor het opzetten van de OTAP omgeving, en ondersteuning tot virtualisatie indien nodig, aanwezig zijn, wordt er gebruik gemaakt van GitLab voor het toepassen van versiebeheer.

### 9.1.3 Testen

Hieronder worden de verschillende methoden en frameworks uitgelicht die gebruikt worden om de kwaliteit te waarborgen.

#### Test-driven Development (TDD)

TDD verwijst naar een programmeerstijl waarin drie activiteiten nauw met elkaar verweven zijn: ontwikkeling, testen (in de vorm van unit-tests) en ontwerp (in de vorm van refactoring) (Janzen & Saiedian, 2005). Het kan worden beschreven door met de volgende stappen:

- Schrijf een unit-test die een aspect van het programma beschrijft
- Voer de test uit, deze faalt omdat het programma de functionaliteit mist
- Schrijf code die het eenvoudigst mogelijk de test laat slagen
- "Refactor"de code totdat deze voldoet aan de architectuur criteria
- Herhaal de stappen

Een belangrijk voordeel van TDD is dat het promoot om kleine stappen te nemen bij het schrijven van software. Stel dat bijvoorbeeld een nieuwe functionaliteit wordt toevoegt, gecompileerd en getest. De kans is groot dat bestaande tests worden gebroken door defecten in de nieuwe code. Het is veel gemakkelijker om deze gebreken te vinden en op te lossen als je twee nieuwe coderegels hebt geschreven in plaats van 2000. De implicatie is dat hoe sneller je ontwikkeld en testen uitvoert, hoe aantrekkelijker het is om in kleinere stappen te werk te gaan.

#### Acceptance Test Driven Development (ATDD)

ATDD is een methode waarbij het hele team samen discussieert over acceptatiecriteria met voorbeelden en deze vervolgens in een reeks concrete acceptatietests verwerkt voordat de ontwikkeling begint (Aggarwal & Singh, 2014).

Deze acceptatietests vertegenwoordigen de requirements van de gebruiker en functioneren als een vorm van vereisten om te beschrijven hoe het systeem zal functioneren. Tevens dienen ze ook als een manier om te controleren of het systeem functioneert zoals bedoeld.

#### Behaviour-driven development (BDD)

BDD moet gericht zijn op het zakelijke gedrag dat de code implementeert: het 'waarom' achter de code (Wynne, Hellesoy & Tooke, 2017). BDD is een uitbreiding van TDD en ATDD. Net als bij TDD

wordt er in BDD eerst de tests geschreven en daarna de applicatiecode. Het grote verschil dat te zien is:

- Tests zijn geschreven in duidelijke beschrijvende taal (Nederlands, Engels, etc..)
- Tests worden geschreven op de toepassing en zijn meer op de gebruiker gericht
- Aan de hand van voorbeelden om de vereisten te verduidelijken

**Cucumber**

Cucumber is een test framework dat BDD ondersteunt (Wynne et al., 2017). Met Cucumber kan het applicatie gedrag in duidelijke, betekenisvolle tekst definiëren met behulp van een eenvoudige grammatica die wordt gedefinieerd door Gherkin. Cucumber zelf is geschreven in Ruby, maar het kan worden gebruikt om code geschreven in Ruby of andere talen te 'testen', inclusief maar niet beperkt tot Java/Kotlin, C# en Python.

**JUnit**

JUnit is een eenvoudig, open source framework voor het schrijven en uitvoeren van unit-tests. Dit framework zal worden ingezet om de unit-testen te schrijven voor de applicatie. JUnit is het meest populaire test framework van dit moment en heeft hierdoor een stabiele community die snel innoveert.

**Continous Integration**

Om de testen te koppelen aan het gebruikte versiebeheer waardoor testen automatisch uitgevoerd worden, wordt er gebruik gemaakt van Continuous Integration (CI). Quintor maakt gebruik van Bamboo waarbij GitLab en Bamboo al op elkaar ingesteld zijn. Om geen overbodige werkzaamheden uit te voeren is er dan ook voor gekozen om gebruik te maken van de beschikbare Bamboo omgeving.

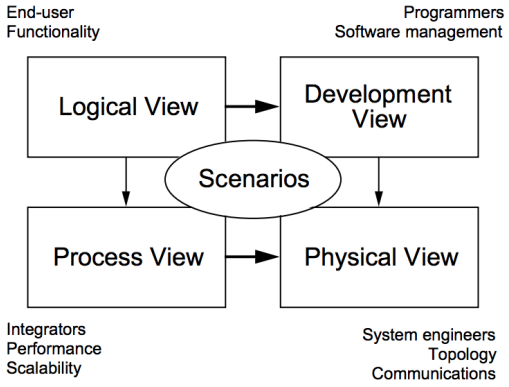
### 9.1.4 Ontwerp

Voor het ontwerp wordt gebruik gemaakt van het 4+1 view-model architectuur zoals beschreven door Kruchten (1995). Het 4+1 view-model organiseert een beschrijving van een software-architectuur met behulp van vijf gelijktijdige views, die elk een specifieke reeks problemen adresseren.

**Development view** beschrijft het systeem uit het perspectief van een ontwikkelaar en beschrijft aspecten die te maken hebben met de software matige indeling.

**Logical view** beschrijft hoe de eindgebruiker in staat zal zijn om de software te gebruiken. Hierbij worden vaak klassediagrammen en state diagrammen toegepast.

**Process view** beschrijft de dynamische aspecten van het systeem op gebied van schaalbaarheid, integratie en performance.




*Figuur 9.1: Het 4+1 view-model volgens Kruchten (1995).*

**Physical view** beschrijft hoe de softwarearchitectuur gaat werken op de benodigde hardware en focust zich met name op het gedistribueerde aspect ervan.

## 9.2 Inventarisatie

Zoals besproken in het adviesrapport wordt het Kademlia protocol gebruikt om de topologie van het netwerk op te zetten. Daarnaast wordt er een consortium Blockchain opgezet, waarbij de toegang tot het netwerk via een EOS geïnspireerd permissiemodel geregeld wordt. Het versturen van de data van de Blockchain over het netwerk zal gedaan worden via *data*, *inv* en *req* berichten, waarbij een *data* bericht verstuurd wordt om bijvoorbeeld nieuwe transacties of blocks uit te wisselen, het *inv* ter inventarisatie om duidelijk te krijgen of een andere deelnemer bepaalde data wilt hebben en een *req* om data op te vragen.

### 9.2.1 Peer-to-Peer

Om bovenstaande keuzes te realiseren dient eerst de basis van de architectuur gerealiseerd te worden, namelijk het Peer-to-Peer (P2P) netwerk. Er zijn een aantal keuzes mogelijk met de protocollen die het P2P netwerk ondersteund.

**TCP/IP** het Transmission Control Protocol (TCP) is het meest gebruikte protocol op het internet, het wordt namelijk gebruikt om data die benodigd is om een website te laden, te versturen. Een voordeel van TCP is dat het protocol de garantie geeft dat data in de juiste volgorde ontvangen wordt. Het protocol wacht namelijk op bevestiging dat een packet ontvangen is, alvorens een volgende packet verstuurd word. Tevens zorgt dit ervoor dat data nooit corrupt raakt of verloren gaat.

**UDP/IP** het User Datagram Protocol (UDP) werkt hetzelfde als TCP alleen zit in dit protocol niet de controle of een packet correct is aangekomen. Packets worden achter elkaar verstuurd zonder na te gaan of de ontvanger ze daadwerkelijk ontvangen heeft. Dit zorgt ervoor dat de overhead van het controleren niet aanwezig is, waardoor het sneller is als het TCP protocol.

Omdat binnen een Blockchain implementatie garantie dat een transactie geregistreerd wordt zeer belangrijk is, zal er gebruik gemaakt worden van TCP/IP. De fail-safe mechaniek die in het protocol zit zal helpen om de Blockchain in een betrouwbare staat te houden.

### 9.2.2 Serialisatie

Om data te versturen over het netwerk is het nodig om de entiteiten om te zetten naar een formaat dat verstuurd kan worden over TCP. Een de-facto standaard hiervoor is het omzetten van een entiteit naar bytes, door een proces genaamd serialiseren. Hierbij zal er gekeken worden naar toepassingen die gebruikt kunnen worden op de Java Virtual Machine (JVM).

1. Java Serializable
   De standaard manier van het implementeren van serialisatie binnen Java. Door het implementeren van een interface op een klasse is het mogelijk om een object out-of-the-box te serialiseren. Wanneer er gebruik wordt gemaakt van complexere entiteiten dient de programmeur de serialisatie zelf te implementeren.

2. Protobuf
   Protocol buffers zijn Google's programmeertaal-neutrale implementatie van serialisatie. Door het eenmalig definiëren van de structuur door middel van een proto-bestand, is het mogelijk om via de library eenvoudig complexe entiteiten om te zetten naar bytes en van bytes naar entiteit. Een voordeel van Protobuf is dat het samenwerkt met alle talen die de library ondersteund. Op dit moment zijn dat Java, Python, Objective-C en C++.

Er zal gebruikt worden gemaakt van Protobuf om entiteiten binnen de Blockchain applicatie te serialiseren. Het voordeel van Protobuf, namelijk dat het samenwerkt met alle talen die de library ondersteund, zorgt ervoor dat het serialisatieproces toekomstbestendig blijft.

## 9.3 Realisatie

*In dit hoofdstuk worden de werkzaamheden besproken die betrekking hebben tot de realisatie van het Proof of Concept.*

### 9.3.1 Peer-to-Peer netwerk

| **Scenarios** | UC03 - Connectie leggen deelnemer |
|---|---|
| **Componenten** | Node, Network |

*Tabel 9.1: Betrokken scenarios en componenten bij de realisatie van het Peer-to-Peer netwerk.*

Om het Peer-to-Peer netwerk te realiseren wordt er gebruik gemaakt van het Netty framework. Netty is een client server framework die het mogelijk maakt om snel en simpel een netwerk applicatie op te zetten die gebruik maakt van een TCP socket server. De voorstaande reden voor het gebruik van Netty is de ondersteuning voor asynchroon programmeren, wat benodigd is om de hoge performance te behalen die nodig is voor een Blockchain implementatie.

In de basis versie van het Peer-to-Peer netwerk is het alleen nog maar mogelijk om connectie te maken met een andere gebruiker waarvan je het adres weet. Om dit te valideren is het opgestelde scenario, beschreven in fig. 9.1, omgezet naar een cucumber test suite, te zien in listing 9.1. Deze test suite zal gedurende de ontwikkeling van de feature gebruikt worden om de gerealiseerde werking te implementeren.

```
Feature: Connect to participant
As a user
I want to connect to a participant
So that I can communicate with the participant

Scenario: Create connection
  Given there is no connection yet
  And I have entered the address
  When I press enter
  Then I should be connected with

Scenario: Create connection with unreachable address
  Given there is no connection yet
  And I have entered the address
  When I press enter
  Then I should receive a message "unreachable address"
```

*Listing 9.1: Scenario vertaald naar een Cucumber test suite.*

# 10 | Evaluatie

*In dit hoofdstuk worden de resultaten van de afstudeeropdracht geëvalueerd. Er wordt gekeken naar de opgeleverde producten en de kwaliteit hiervan. Vervolgens wordt de gekozen aanpak besproken en de mogelijke afwijkingen van het afstudeerplan. Als laatste wordt er gekeken naar de beroepstaken die uitgevoerd zijn.*

## 10.1 Producten

### 10.1.1 Plan van Aanpak

Het plan van aanpak is te vinden in bijlage **??** en bevat een beschrijving van de aanpak zoals in het begin van het afstudeertraject is opgezet. Het is niet meegenomen in het iteratieve proces, waardoor het geen gedetailleerde beschrijving van de aanpakken bevat. Het plan van aanpak bevat tevens alle werkzaamheden die doorlopen zijn om tot het eindresultaat te komen en is essentieel geweest voor de uitvoering van het project. Het gaf me namelijk een goed beeld van wat er nodig was om het project tot een succesvol einde te brengen, zonder de focus van het project uit het oog te verliezen.

### 10.1.2 Onderzoeksrapport

Het onderzoeksrapport is te vinden in bijlage **??** en bevat het resultaat van het onderzoek met als hoofdvraag “Welke protocol implementaties kunnen toegepast worden om de onderdelen Distributed Network en Identity Management te realiseren voor een Blockchain implementatie?”. Ten tijde van het opzetten van het afstudeerplan was er nog geen kennis over het Blockchain domein, en ik ben dan ook zeer tevreden met de kennis die vergaard is met het gedane onderzoek. Helaas heb ik niet alle vragen kunnen behandelen die ik in eerste instantie in gedachte had, maar niettemin bevat het een goede fundering voor kennis voor de onderdelen Identity Management en Distributed Network in de Blockchain implementaties Bitcoin, EOS, Monero en Cardano.

### 10.1.3 Adviesrapport

Het adviesrapport is te vinden in bijlage **??** en bevat interpretaties en technologieën die geadviseerd zijn voor het ontwikkelde Proof-of-Concept. Het document adviseert over technologieën waaruit de meeste waarde gehaald kon worden voor Quintor. Helaas is tijd hierbij ook een beperkende factor gebleken en is er niet uitgebreid verteld over de verschillende technologieën. Het was wel voldoende om aan de hand van discussie met de bedrijfsbegeleider en de Blockchain expert een selectie te maken van technologieën die gerealiseerd zijn in het Proof-of-Concept.

### 10.1.4 Proof of Concept

Het Proof of Concept bestaat uit technologieën die in overeenstemming met Quintor geselecteerd zijn uit het adviesrapport. Het betreft het realiseren van het Kademlia protocol om te functioneren als topologie voor het netwerk. Daarnaast is er gekozen voor een consortium Blockchain waarbij een permissiemodel geïnspireerd door EOS gerealiseerd is. Informatie wordt verstuurd op de wijze waarop Cardano het doet, namelijk met het gebruik van inv, data en req berichten. Dit was een zeer ambitieuze implementatie, losstaand van het feit dat de complexiteit van de implementatie lag in de samenwerking met de onderdelen die gerealiseerd waren door Kevin Bos. Over het algemeen ben ik tevreden met de realisatie van het Proof of Concept en de totstandkoming daarop.

## 10.2 Aanpak

Gedurende het afstudeertraject is de aanpak op Agile wijze uitgevoerd. Door de vele iteraties van zowel het vooronderzoek, de opzet van het onderzoek en het daadwerkelijke resultaat van het onderzoek is er veel tijd verloren gegaan, en zou ik in het vervolg ook niet voor een Agile aanpak kiezen bij het uitvoeren van onderzoek. Een groot valkuil waar ik mezelf op betrapte tijdens het onderzoeken van Blockchain protocollen is het feit dat ik teveel wil beschrijven en dat vervolgens ook wil uitlichten in het vooronderzoek om het concept duidelijk te maken voor de lezer.

### 10.2.1 Onderzoek

Het onderzoek is uitgevoerd door literatuurstudie waarbij geen toepassing bekend was. In andere afstudeerscripties komt het doorgaans voor dat er gebruik gemaakt wordt van toegepast onderzoek, waardoor het opzetten van de structuur in het gehele project nogal in de war kwam. Dit zorgde ervoor dat het onderzoeksrapport de grootste artefact van de afstudeeropdracht was en het Proof of Concept erbij kwam als bijkomstigheid. De keuzes die hiertoe geleid hebben konden in mijn ogen ook niet anders met hoe de opdracht vanuit Quintor gepresenteerd was, namelijk dat de insteek van de opdracht was om kennis op te doen van het Blockchain domein.

Daarnaast is het kiezen van EOS een fout geweest, dat oorzaak is geweest voor vele knelpunten in het onderzoeksproces. Dit is eigenlijk fout gegaan tijdens de selectie van implementaties en de bron die hiervoor gebruikt is. In het overzicht van coinmarketcap is mogelijk om alleen coins te tonen in plaats van de standaardweergave waarbij coins en tokens door elkaar heen weergegeven worden. Op het moment van schrijven is EOS een van de meest succesvolle Initial Coin Investment (ICOs) op het moment, waarbij het geen eigen coin heeft en dus ook geen eigen Blockchain implementatie. Hierdoor is de beschikbare documentatie van het protocol (bijna) beperkt tot een technische whitepaper die toch wel wat steken laat vallen voor het begrijp technisch.

## 10.3 Beroepstaken

De beroepstaken die uitgevoerd zoals opgegeven in het afstudeerplan, in te zien in bijlage **??**, zijn hieronder verantwoord. De complexiteit is ingedeeld naar de beschrijving van beroepstaken zoals gepresenteerd in het document "Beroepstaken van de opleiding Informatica – Academie voor ICT & Media, uitgave juni 2009".

- **Selecteren, methoden, technieken en tools.**

  Er zijn meerdere handelingen geweest die verantwoord kunnen worden onder deze beroepstaak. Tijdens het realiseren van het Proof of Concept zijn er zowel keuzes gemaakt op het gebied van de selectie van methoden, technieken en tools als bij het opstellen van de development workflow die gepaard ging met de realisatie.

  De complexiteit van dit onderdeel komt neer op niveau 4, aangezien het zelfstandig is uitgevoerd en van voldoende complexiteit is in samenwerking met de inventarisatie van bestaande Blockchain technieken.

- **Ontwerpen systeemdeel.**

  Het ontwerpen van het systeemdeel betrof het modelleren van de verschillende technologieën die uit de selectie van het adviesrapport gekomen zijn. De samenwerking tussen de technologieën dient modulair te zijn zodat elk losstaand deel vervangen kan worden. Het systeem dient tevens samen te werken met componenten die gerealiseerd zijn door een andere afstudeerder. Er is hierbij gebruik gemaakt van de ontwerpmethode 4+1 architectural view model zoals beschreven door Kruchten (1995).

  De complexiteit van dit onderdeel komt neer op niveau 4, aangezien het systeem rekening dient te houden met de geïdentificeerde gevaren in het gedane onderzoek en het 4+1 architectural view model beschrijft de architectuur vanuit verschillende gezichtspunten.

- **Bouwen applicatie.**

De realisatie van het Proof of Concept betreft het bouwen van een applicatie die aansluit op een ander deel van de Blockchain dat gerealiseerd is door een afstudeerder. Er wordt hierbij gebruik gemaakt van frameworks waarbij er redenatie aanwezig is voor gekozen frameworks. Er wordt gebruik gemaakt van versiebeheer dat gefaciliteerd is door Quintor, en er wordt containerization toegepast om een testomgeving te simuleren.

De complexiteit van dit onderdeel komt neer op niveau 4, aangezien het aansluit op bestaande software en er gebruik gemaakt wordt van een ontwikkelomgeving inclusief testomgeving en versiebeheertool.

- **Initiëren en plannen testproces.**

  Helaas is het niet meer mogelijk geweest om de kwaliteit aan te tonen door het uitvoeren van een opgesteld testplan. Binnen het architectuurdocument is er wel rekening gehouden met criteria die gesteld is aan de implementatie in de vorm van non-functional requirements. Daarnaast is er wel inventarisatie gedaan naar de mogelijkheden met betrekking tot het testen van de applicatie. Dit is beschreven in hoofdstuk 9.1.3.

# 11 Aanbevelingen

*Tijdens het onderzoek is er helaas geen tijd geweest om de actualiteiten in het Blockchain domein te behandelen. Hiernaar is wel een korte inventarisatie gedaan, waardoor er verdergewerkt kan worden op de werkzaamheden zoals gepresenteerd in dit document.*

## 11.1 Directed Acyclic Graph

De implementaties NANO en IOTA maken gebruik van een Directed Acyclic Graph (DAG), een nieuw soort architectuur die naar verluid de schaalbaarheid van Blockchain technologie dient te vergroten. Het is dan ook zeker interessant om te kijken of deze kennis van belang is voor Quintor.

## 11.2 Bitcoin Lightning Network

Bitcoin is al een tijd bezig met onderzoek naar verbetering van de transactie throughput. Dit netwerk is een tweede protocol laag bovenop een Blockchain implementatie die het mogelijk maakt om transacties direct door te zetten. Alhoewel het nog in de kinderschoenen staat en het nog vatbaar is voor bepaalde aanvallen zoals geïdentificeerd in dit onderzoek, is het een interessante techniek om te onderzoeken.

## 11.3 Ethereum Casper

Ethereum probeert van het Proof of Work consensus af te stappen, alleen willen ze hierdoor geen hard-fork veroorzaken. De eerste fase van Casper, Casper the Friendly Finality Gadget, is dan ook een hybride tussen Proof of Stake en Proof of Work die ingezet kan worden om het Ethereum netwerk te upgraden zonder een hard-fork te veroorzaken. Uiteindelijk zal Casper overgaan naar Casper the Friendly Ghost, een volledige implementatie van Proof of Stake.

## 11.4 EOS

Op 1 juni wordt EOS gepubliceerd waarbij het eindelijk mogelijk is om deel te nemen aan het netwerk. Aangezien Quintor Blockchain wilt inzetten als ontwikkelingsplatform, is het interessant om deze implementatie te volgen aangezien het primair gebouwd is om ingezet te worden als ontwikkelingsplatform.

## 11.5 Network Address Translators (NAT) Hole Punching

Ford, Srisuresh en Kegel (2005) presenteert een aantal technieken om Hole Punching toe te passen in P2P protocollen. In hoeverre dit gebruikt wordt in Blockchain implementaties is niet verder onderzocht waardoor deze studie waardevolle informatie kan bevatten. Tijdens het scannen van de tekst is er ook een stuk over IPv6 beschreven wat zeker interessant is voor toekomstige adoptie van het IPv6 adres.

# Literatuur


Castor, A. . (2017). *A short guide to bitcoin forks - coindesk.* Verkregen van `https://www.coindesk.com/short-guide-bitcoin-forks-explained/`

Roman, K. . (2018). *Understanding eos and delegated proof of stake — steemit.* Verkregen van `https://steemit.com/eos/@eosgo/understanding-eos-and-delegated-proof-of-stake`

Aggarwal, V. & Singh, M. (2014). Acceptance test driven development. *Journal of Advanced Computing and Communication Technologies (ISSN: 2347-2804) Volume*(2).

Antonopoulos, A. M. (2014). *Mastering bitcoin: Unlocking digital crypto-currencies* (1st dr.). O'Reilly Media, Inc.

Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary?

Bawa, M., Cooper, B. F., Crespo, A., Daswani, N., Ganesan, P., Garcia-Molina, H., ... others (2003). Peer-to-peer research at stanford. *ACM SIGMOD Record*, *32*(3), 23–28.

Bitcoin Wiki. (2010). *Bitcoin wikio.* Verkregen van `https://en.bitcoin.it/wiki`

Conti, M., Lal, C., Ruj, S. et al. (2017). A survey on security and privacy issues of bitcoin. *arXiv preprint arXiv:1706.00916*.

Crosby, M., Pattanayak, P., Verma, S. & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*, 6–10.

Ethereum. (2017). *Create a hello world contract in ethereum.* Verkregen van `https://www.ethereum.org/greeter` ([Online; benaderd op 3 april, 2018])

Eyal, I. & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security* (pp. 436–454).

Ford, B., Srisuresh, P. & Kegel, D. (2005). Peer-to-peer communication across network address translators. In *Usenix annual technical conference, general track* (pp. 179–192).

GitLab. (2018). *About us | gitlab.* Verkregen van `https://about.gitlab.com/about/` ([Online; benaderd op 10 april, 2018])

Heilman, E., Kendler, A., Zohar, A. & Goldberg, S. (2015). Eclipse attacks on bitcoin's peer-to-peer network. In *Usenix security symposium* (pp. 129–144).

Janzen, D. & Saiedian, H. (2005). Test-driven development concepts, taxonomy, and future direction. *Computer*, *38*(9), 43–50.

Karame, G. O., Androulaki, E. & Capkun, S. (2012). Double-spending fast payments in bitcoin. In *Proceedings of the 2012 acm conference on computer and communications security* (pp. 906–917).

Kiayias, A. et al. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual international cryptology conference* (pp. 357–388).

Kruchten, P. B. (1995). The 4+ 1 view model of architecture. *IEEE software*, *12*(6), 42–50.

Lamport, L. et al. (1982). The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, *4*(3), 382–401.

Maymounkov, P. & Mazieres, D. (2002). Kademlia: A peer-to-peer information system based on the xor metric. In *International workshop on peer-to-peer systems* (pp. 53–65).

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

O'Dwyer, K. J. & Malone, D. (2014). Bitcoin mining and its energy footprint..

Pfitzmann, A. & Köhntopp, M. (2001). Anonymity, unobservability, and pseudonymity—a proposal for terminology. In *Designing privacy enhancing technologies* (pp. 1–9).

Pieter Otten. (2017). *Kotlin vs java - mediaan.* Verkregen van `https://www.mediaan.com/nl/kotlin-vs-java/` ([Online; benaderd op 10 april, 2018])

Reid, F. & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks* (pp. 197–223). Springer.

Van Saberhagen, N. (2013). *Cryptonote v 2. 0.*

Wynne, M., Hellesoy, A. & Tooke, S. (2017). *The cucumber book: behaviour-driven development for testers and developers*. Pragmatic Bookshelf.

Zen, A. (2017). *Cryptokitties | collect and breed digital cats.* Verkregen van `https://www.cryptokitties.co/press`

Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Big data (bigdata congress), 2017 ieee international congress on* (pp. 557–564).

Zheng, Z., Xie, S., Dai, H.-N. & Wang, H. (2016). Blockchain challenges and opportunities: A survey. *Work Pap.–2016*.