

Onderzoek naar
Gedistribueerde netwerken en identiteits
management binnen Blockchain
technologie

Jeffrey van Hoven
27 mei 2018

Quintor



Voorwoord

Voor u ligt mijn afstudeerverslag; *"Het realiseren van een gedistribueerd netwerk met mogelijkheid tot identiteit management ter behoeve van 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 mogelijk geweest zijn.

Ik wens u veel leesplezier toe.

Jeffrey van Hoven
Den Haag, 1 juni 2018

Inhoudsopgave

1	Inleiding	1
2	Quintor	2
2.1	Software Factory	2
2.2	Visie	3
2.3	Organisatie	3
2.4	Betrokkenen	4
3	Opdracht	5
3.1	Probleemstelling	6
3.2	Doelstelling	6
3.3	Resultaat	6
3.3.1	Producten	7
4	Aanpak	8
4.1	Project	8
4.2	Vooronderzoek	8
4.3	Onderzoek	9
4.3.1	Opzet	9
4.3.2	Adviesrapport	9
4.4	Proof of Concept	9
4.5	Planning	11
5	Vooronderzoek en resultaten	12
5.1	Blockchain	13
5.1.1	Eigenschappen	14
5.2	Toepassing	15
5.2.1	Ontwikkelpatform	16
5.3	Architectuur	17
5.4	Gedistribueerd netwerk	18
5.5	Identiteit	21
5.5.1	Autorisatie	22
	Privacy	22
	Privacy in Bitcoin	23
5.6	Obstakels	24
5.7	Conclusie	24

6	Selectie protocollen	25
6.0.1	Coinmarketcap	25
	Hard forks	25
6.0.2	Attributen	26
6.0.3	Selectie	26
7	Onderzoek	28
	Literatuurlijst	29
	Bijlages	30
I	Opdrachtformulering	31
II	Afstudeerplan	34
III	Plan van Aanpak	39
IV	Implementatie selectie	52
V	Onderzoeksrapport	52
VI	Adviesrapport	78
VII	Voortgangsverslag	86
VIII	Bezoekverslag	88

Lijst van figuren

2.1	Organogram van Quintor.	4
3.1	Indeling opdracht Blockchain Quintor.	5
5.1	Blockchain structuur	13
5.2	CryptoKitties, een spel dat gebruik maakt van Blockchain technologie.	15
5.3	Blockchain architectuur	17
5.4	Distributed Hash Table	19
5.5	Bitcoin Node functionaliteiten	20
5.6	Asymmetrische encryptie	21
5.7	Gebruik van asymmetrische encryptie	21
6.1	Snapshot Coinmarketcap	25

Lijst van tabellen

6.1	Attributen opgesteld voor initiële selectie implementaties.	26
1	Bekeken implementaties uit de initiële selectie met de onderzochte attributen. . . .	77

Woordenlijst

D

DApps Distributed Applications – Applicaties die gebruik maken van een Blockchain technologie, bijv. Ethereum, om op gedecentraliseerde wijze te interacteren met gebruikers. 16

F

fork . 19

full node . 20

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. 19

M

mining node . 20

N

node . 20

S

Smart Contract . 15, 16

Soft Fork Een verandering in het Blockchain protocol die terugwaartse compatibiliteit heeft met eerdere versies van het protocol. 19

W

wallet (node) . 20

Afkortingen

D

DHT Distributed Hash Table. 18

P

P2P Peer-to-Peer. 18, 20

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.

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 iteratiefontwikkelp proces. 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

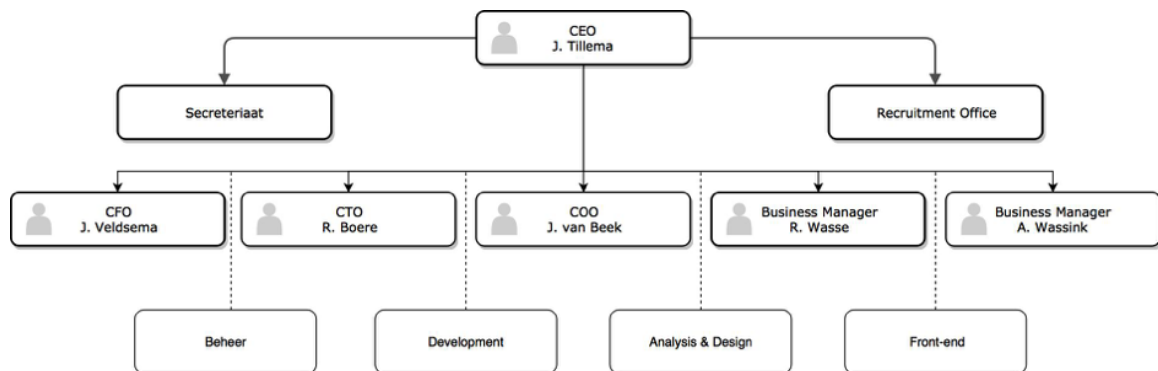
Een van de doelstellingen die Quintor heeft is het professionaliseren van software development. Aansluitend daarop probeert het bedrijf continu voor te lopen op de concurrentie door het opdoen van kennis op het gebied van nieuwe technologieën, waarbij professionalisering van de werkwijze voorop staat.

"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 begeleider van de afstudeeropdracht. Hij is een Java ontwikkelaar die als bijkomende taak heeft om de afstudeerders binnen Den Haag te begeleiden. 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 bevorderen.

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.

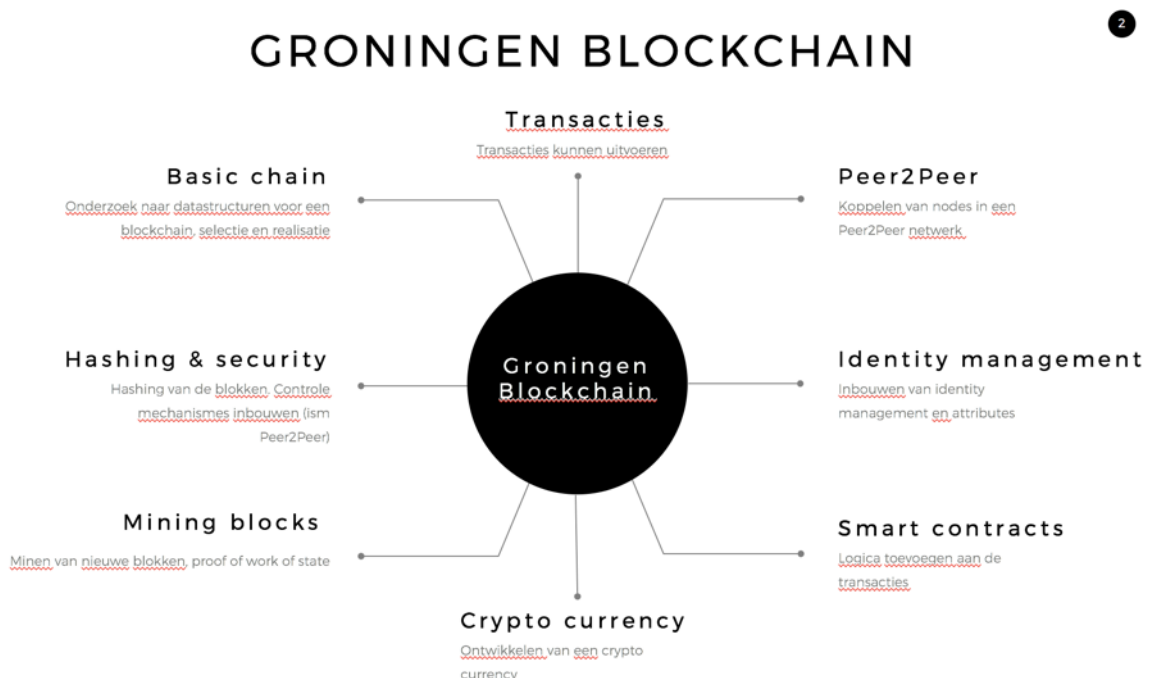
Kevin Bos is afstudeerder afkomstig van Avans Hogeschool. Hij is verantwoordelijk voor het lokale gedeelte van de Blockchain opdracht. Tijdens de afstudeeropdracht is hij een stakeholder van het project en zal er een zekere mate van samenwerking aanwezig zijn.

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 meer kennis wilt opdoen over het Blockchain domein.



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 I.

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 de aangeboden 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 elk individueel segment 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 I.

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 zijn 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 II.

4.1 Project

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 to 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.

4.2 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.

4.3 Onderzoek

In de opdrachtschrijving 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.

4.3.1 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'.

4.3.2 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.

4.4 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.

4.5 Planning

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

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?

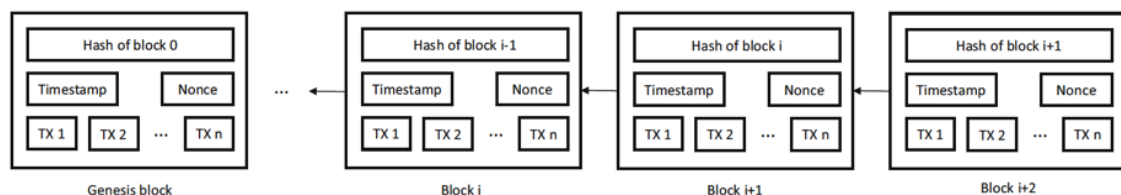
5.1 Blockchain

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.

Persistentie 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.

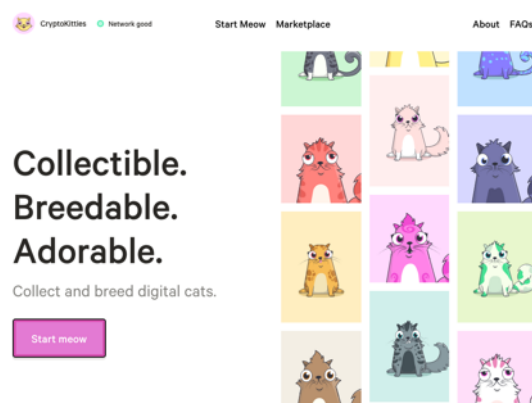
5.2 Toepassing

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 I, 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, Patanayak, 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).

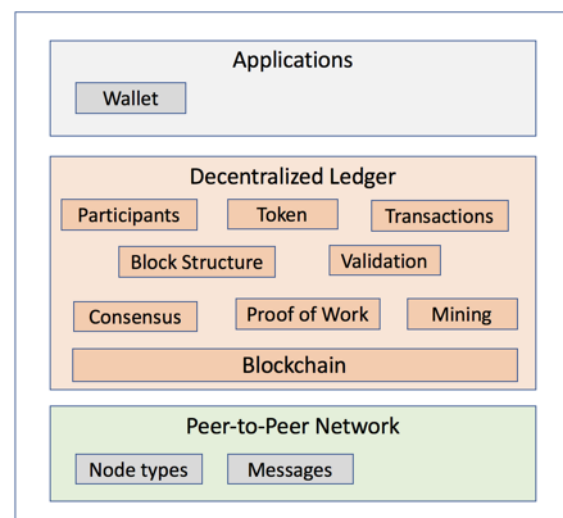
5.3 Architectuur

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. 5.3 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.

De Decentralized Ledger is de kern van de technologie en zorgt ervoor dat de globale blockchain consistent en fraudebestendig blijft. De fundamentele structuur achter de gehele technologie is de blockchain, waar transacties gegroepeerd worden in blokken en elk blok cryptografisch 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 proces uitvoert. Om de Decentralized Ledger bij te werken en te onderhouden communiceren de nodes met elkaar door middel van het versturen van berichten.



Figuur 5.3: Blockchain architectuur

5.4 Gedistribueerd netwerk

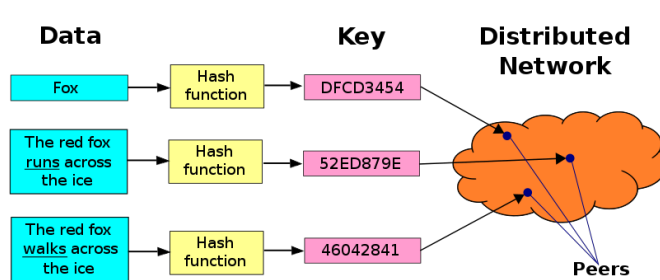
In dit hoofdstuk wordt de vraag "Waaruit bestaat het onderdeel gedistribueerd netwerk binnen Blockchain technologie?" behandeld. Bij deze vraag wordt er gekeken naar de geïdentificeerde onderdelen uit hoofdstuk 5.3. Er wordt een korte introductie gegeven in peer-to-peer netwerken en waarom het een belangrijk 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 gedecentraliseerd 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 optreedt (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).

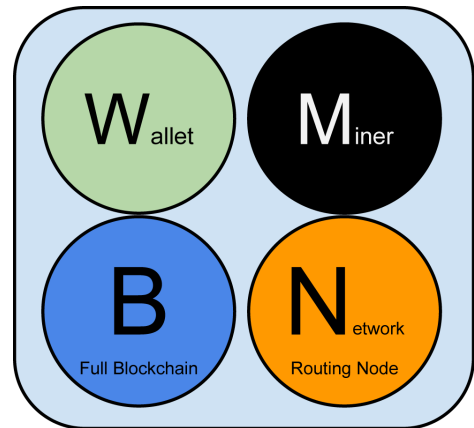
Nodes

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.

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.



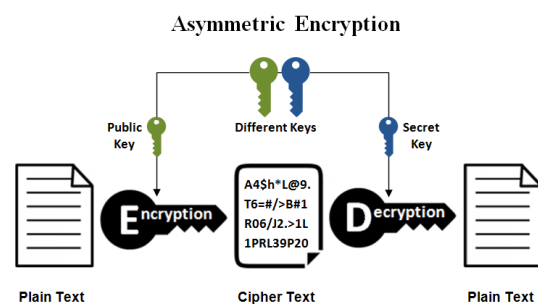
Figuur 5.5: Een bitcoin netwerk node die alle functies bevat: wallet, mining, blockchain database en netwerk routing, (Antonopoulos, 2014, p. 172).

5.5 Identiteit

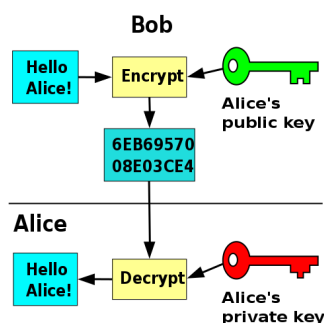
In dit hoofdstuk wordt de vraag “Waaruit bestaat het onderdeel Identity Management binnen Blockchain technologie?” behandeld. Zoals beschreven in hoofdstuk 5.1 zijn anonimiteit en controleerbaarheid belangrijke eigenschappen van een Blockchain implementatie. Allereerst zal er beschreven worden wat identiteit 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.



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

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.

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 wordt 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 voorgestelde 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 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

Een van de overzichten is het maandelijks 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.

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.

#	Name	Symbol	Volume (1d)	Volume (7d)	Volume (30d)
1	 Bitcoin	BTC	\$5,728,630,000	\$47,024,950,272	\$239,837,765,688
2	 Ethereum	ETH	\$1,653,700,000	\$13,056,842,240	\$93,063,570,688
3	 Tether	USDT	\$1,858,830,000	\$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	\$13,445,324,382
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	\$172,823,000	\$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	\$3,060,712,660
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	\$1,879,299,036
25	 Binance Coin	BNB	\$45,055,600	\$312,276,682	\$1,935,435,524

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

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.

6.0.3 Selectie

Aan de hand van deze attributen is een lijst opgesteld, te zien in tabel 1, 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

Literatuur

- Castor, A. . (2017). *A short guide to bitcoin forks - coindesk*. Verkregen van <https://www.coindesk.com/short-guide-bitcoin-forks-explained/>
- 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>
- 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])
- Lamport, L. et al. (1982). The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3), 382–401.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
- Pfitzmann, A. & Köhntopp, M. (2001). Anonymity, unobservability, and pseudonymity—a proposal for terminology. In *Designing privacy enhancing technologies* (pp. 1–9).
- Reid, F. & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks* (pp. 197–223). Springer.
- 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.

Bijlages

I Opdrachtformulering

ONTWIKKELING VAN EEN GEDISTRIBUEERDE BLOCKCHAIN

Bouw een blockchain implementatie zonder gebruik te maken van bestaande blockchain libraries.

Organisatie

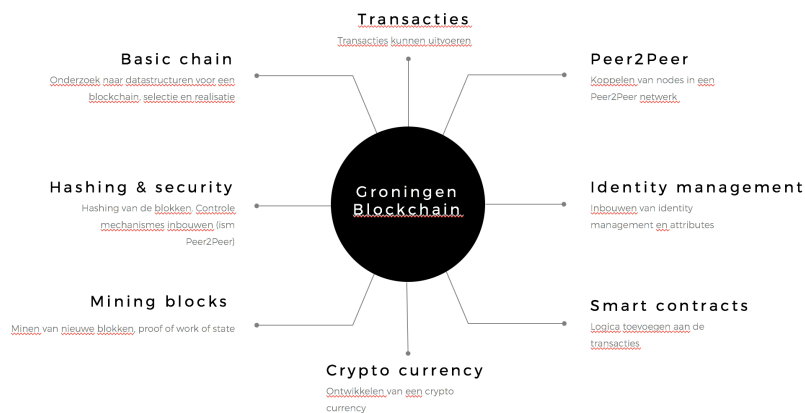
Quintor is een toonaangevend bedrijf op het gebied van Agile software development, Enterprise Java / .NET technologie en mobile development. Wij hebben sinds onze oprichting in 2005 een gezonde groei doorgemaakt en hebben inmiddels 150 personeelsleden. Vanuit onze vestigingen in Amersfoort, Groningen en Den Haag ondersteunen wij onze klanten bij de uitdagingen die grootschalige enterprise projecten met zich meebrengen. Quintor beschikt over een Software Factory waarin wij inhouse projecten voor onze klanten uitvoeren.

Probleemstelling

Voor de ontwikkeling van een blockchain dienen een aantal software componenten te worden ontwikkeld:

1. Een gegevensstructuur voor een node
2. Hashing functionaliteit
3. Mining van blokken
4. Synchronisatie van nodes (peer2peer)
5. Transacties
6. Identity management
7. Eventueel een crypto currency en smart contracts.

GRONINGEN BLOCKCHAIN



Deze opdracht richt zich op het ontwikkelen van een gedistribueerd netwerk(4) en identity management(6).

De overige onderdelen zullen in andere opdrachten gerealiseerd worden.

Aanpak

Allereerst worden in afstemming met de opdrachtgever (Johan Tillema) de uitgangspunten bepaald voor de te ontwikkelen blockchain. Deze gaan over snelheid, beveiligingsniveau en toepassingsmogelijkheden.

Vervolgens worden voor 4) en 6) de verschillende architectuur alternatieven in kaart gebracht. Dit wordt gedaan door het uitvoeren van literatuur onderzoek en door te kijken welke keuzes zijn gemaakt in andere blockchain implementaties zoals Ethereum, Hyperledger of BitCoin.

Samen met de opdrachtgever wordt een keuze gemaakt voor de toe te passen architectuur.

Vervolgens wordt een eerste gedistribueerde blockchain geïmplementeerd in Java of in .NET.

Achtergrond probleemstelling

Blockchains garanderen integriteit van data door gebruikmaking van cryptografische primitieven zoals hash functies en public-private key cryptografie. Door het ondertekenen van berichten wordt authenticiteit gegarandeerd en de hash functies zorgen voor een keten die mutaties van oude data onmogelijk maakt.

Op basis van deze onderzoeksvragen wordt een proof of concept verwacht. Op te leveren producten: een basaal blockchain implementatie die aan de volgende eisen voldoet;

- 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

II Afstudeerplan

Afstudeerplan

Informatie afstudeerder en gastbedrijf *(structuur niet wijzigen)*

Afstudeerblok: 2018-1.1 (start uiterlijk 5 februari 2018)

Startdatum uitvoering afstudeeropdracht:

Inleverdatum afstudeerdossier volgens jaarrooster: 1 juni 2018

Studentnummer: 14068265

Achternaam: van Hoven

Voorletters: J.

Roepnaam: Jeffrey

Adres: Rehobothplantsoen 14

Postcode: 2751BK

Woonplaats: Moerkapelle

Telefoonnummer: 0795932704

Mobiel nummer: 0646157795

Privé emailadres: jeffreyvanhoven@gmail.com

Opleiding: Informatica

Locatie: Zoetermeer

Variant: voltijd

Naam studieloopbaanbegeleider: Renate Vermeij

Naam begeleidend examiner: T. Cocx

Naam tweede examiner: D.R. Stikkolorum

Naam bedrijf: Quintor

Afdeling bedrijf: n.v.t

Bezoekadres bedrijf: Lange Vijverberg 4-5

Postcode bezoekadres: 2513 AC

Postbusnummer:

Postcode postbusnummer:

Plaats: Den Haag

Telefoon bedrijf: 070-2044037

Telefax bedrijf:

Internetsite bedrijf: <https://www.quintor.nl/>

Achternaam opdrachtgever: Tillema

Voorletters opdrachtgever: J.

Titulatuur opdrachtgever:

Functie opdrachtgever:

Doorkiesnummer opdrachtgever:

Email opdrachtgever: jtillema@quintor.nl

Achternaam bedrijfsmentor: dhr. Ooms

Voorletters bedrijfsmentor: B

Titulatuur bedrijfsmentor:

Functie bedrijfsmentor: Java Software Engineer

Doorkiesnummer bedrijfsmentor:

Email bedrijfsmentor: booms@quintor.nl

Doorkiesnummer afstudeerder:

Functie afstudeerder (deeltijd/duaal):

Titel afstudeeropdracht:

Ontwikkelen van een gedistribueerde Blockchain.

Opdrachtschrijving**Bedrijf**

Quintor is een toonaangevend bedrijf op het gebied van Agile software development, Enterprise Java/ .NET technologie en mobile development. Wij hebben sinds onze oprichting in 2005 een gezonde groei doorgemaakt en hebben inmiddels 150 personeelsleden. Vanuit onze vestigingen in Amersfoort, Groningen en Den Haag ondersteunen wij onze klanten bij de uitdagingen die grootschalige Enterprise projecten met zich meebrengen. Quintor beschikt over een Software Factory waarin wij inhouse projecten voor onze klanten uitvoeren.

Probleemstelling

Quintor is een bedrijf die klanten ondersteund bij het realiseren van grootschalige, uitdagende Enterprise projecten. Aangezien de toepassing en adoptie van Blockchain technologie steeds groter wordt wil het bedrijf de toepassingsmogelijkheden en technieken onderzoeken om zo inzicht te kunnen krijgen in hoe het gebruikt kan worden in de aangeboden vraagstukken vanuit klanten.

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.

De focus in deze opdracht ligt op het onderzoeken van de Blockchain onderdelen Identity Management en Distributed Network. Er zullen Blockchain implementaties onderzocht worden die de onderdelen geïmplementeerd hebben om een zo compleet mogelijk technisch overzicht te creëren van de technieken en protocollen die gebruikt zijn om de onderdelen te realiseren. Daarnaast wordt er onderzocht wat de toepassingen en de doelen van de bestaande implementaties zijn. Uiteindelijk zal er een advies uitgegeven worden aan de opdrachtgever, waarbij een keuze gemaakt zal worden op de manier waarop een Proof of Concept gerealiseerd gaat worden met als doel het toetsen van de gekozen technieken.

Doelstelling van de afstudeeropdracht

Het doel van deze opdracht is middels het opstellen van een Proof of Concept van de Blockchain onderdelen Network & Identity Management en Distributed Network, zonder gebruik te maken van bestaande oplossingen, kennis te ontwikkelen voor Quintor op het gebied van Blockchain technologie.

Resultaat

De opdracht zal een Proof of Concept van de Blockchain onderdelen Network & Identity Management en Distributed Network opleveren waarbij er gebruik gemaakt wordt van advies uit het literatuuronderzoek gedaan naar de onderdelen in bestaande Blockchain implementaties.

Uit te voeren werkzaamheden, inclusief een globale fasering, mijlpalen en bijbehorende activiteiten

5 dagen - Plan van Aanpak opstellen met behulp van J. Tillema.

- Opstart

15 dagen - Literatuuronderzoek naar Blockchain waarbij de volgende bekende architecturen worden onderzocht:

- Ethereum
- HyperLedger
- BitCoin.

Eventueel kennis uitwisselen met Blockchain experts van het Blockchain Fieldlab Education in Groningen waarvan Quintor medeoprichter van is.

35 dagen - Ontwikkelen, ontwerpen en testen.

- Waarbij geen gebruik gemaakt wordt van bestaande oplossingen.
- Door middel van Agile Software Development

Hierbij zullen de volgende mijlpalen behaald worden:

- Afronding implementatie Distributed Network.
- Afronding implementatie Network & Identity Management.

10 dagen – Testen.

5 dagen – Overdracht.

Op te leveren (tussen)producten

Product	
Plan van Aanpak	Een document met daarin de planning en de afspraken die gemaakt zijn met de opdrachtgever.
Sprint	Per twee weken zal er een sprintplanning plaatsvinden waarbij nieuwe taken worden ingedeeld. Aan het eind van een sprint zal er een presentatie gegeven worden over de voortgang van het project.
Adviesrapport	Een document met daarin de uitkomst van het literatuuronderzoek naar Ethereum, HyperLedger en BitCoin.
Proof of Concept	Als uiteindelijk resultaat een generieke implementatie van de onderdelen Network & Identity Management en een Distributed Network.

Te demonstreren competenties en wijze waarop

Kerntaak	
1.1	Selecteren, methoden, technieken en tools.
<p>Het juist uitzoeken van een development workflow en de technieken die daarbij te pas komen in overeenstemming met Quintor. Daarnaast zullen er beslissingen gemaakt moeten worden die invloed hebben op de manier waarop de Blockchain technologie geïmplementeerd zal worden:</p> <p>Bijvoorbeeld:</p> <ul style="list-style-type: none"> - Gaat het onderdeel Distributed Network webbased werken of met een ander protocol? <p>Concrete taken:</p> <ul style="list-style-type: none"> - Het opzetten van een OTAP-omgeving en/of DevOps toepassen om dit te simuleren. - Selecteren en adviseren over implementatie van de onderdelen Distributed Network en Network & Identity Management. 	
3.2	Ontwerpen systeemdeel.
<p>Voor het opstellen van een generieke Blockchain zal het nodig zijn om de complexe delen van de te ontwikkelen applicatie met behulp van UML uit te werken.</p> <p>Concrete taken:</p> <ul style="list-style-type: none"> - Een object georiënteerd ontwerp van de onderdelen Distributed Network en Network & Identity Management waarbij er rekening gehouden wordt met de generieke toepassing en samenwerking van de twee onderdelen. - Het identificeren, integreren en ontwerpen van de onderdelen die onderzocht zijn tijdens het literatuuronderzoek. - Rekening houdende met beveiligingseisen gesteld door Quintor. 	
3.3	Bouwen applicatie.
<p>Het ontwikkelen van de onderdelen Distributed Network en Network & Identity Management waarbij gebruikt wordt gemaakt van een object georiënteerde programmeertaal.</p> <p>Concrete taken:</p> <ul style="list-style-type: none"> - Het ontwikkelen van de onderdelen Distributed Network en Network & Identity Management door middel van de programmeertalen Java of C#. - Gebruik makend van de softwaremanagement tools die opgezet zijn voor de OTAP-omgeving en/of de DevOps toepassingen om deze omgeving te simuleren. 	
3.4	Initiëren en plannen testproces.
<p>Om de integriteit van de ontwikkelde software te waarborgen zullen er verschillende testen gemaakt worden. Een belangrijk aspect is het testen van de security bij het implementeren van het Network & Identity Management onderdeel.</p> <p>Concrete taken:</p> <ul style="list-style-type: none"> - Het onderzoeken van test-, soorten en strategieën die gebruikt worden voor een Blockchain implementatie. - Eventueel methodiek hanteren die Quintor gebruikt. 	

III Plan van Aanpak

Quintor

Plan van Aanpak

**Het opzetten van een peer-to-peer netwerk met identiteit
management door middel van Blockchain technologie**

Jeffrey van Hoven
14068265@student.hhs.nl
9 april 2018

Inhoudsopgave

1	Aanleiding	3
2	Probleemanalyse	4
3	Doelstelling	5
4	Resultaten	6
4.1	Adviesrapport	6
4.2	Proof of Concept	6
5	Aanpak	7
5.1	Onderzoeksopzet	7
5.1.1	Dataverzameling	7
5.1.2	Dataomschrijving	8
5.1.3	Analysemethode	8
5.2	Adviesrapport	9
5.3	Proof-of-Concept	9
6	Planning	10

Inleiding

In dit document wordt de aanpak beschreven van de afstudeeropdracht “Ontwikkeling van de Blockchain onderdelen Distributed Network en Identity Management”, aangeboden door Quintor.

De resultaten van het uitgevoerde onderzoek naar de manier waarop Blockchain implementaties de onderdelen Distributed Network en Identity Management heeft als doel het bedrijf te adviseren over de mogelijkheden om een zo generiek mogelijke implementatie te realiseren van waarbij acties beperkt worden door het onderdeel Identity Management.

Hoofdstuk 1

Aanleiding

In 2017 heeft Quintor in samenwerking met DUO/MinOCW, Groningen Declaration Network (GDN), Stichting ePortfolio Support (StePS), TNO en Rabobank, het Blockchain Field-lab Education (BFE) 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 op het gebied van Blockchain. Daarnaast wil het bedrijf in de toekomst Blockchain technologie inzetten om vraagstukken vanuit klanten op te lossen. Door het aanbieden van een doorlopende afstudeeropdracht wil het bedrijf erachter komen wat er voor nodig is om een Blockchain implementatie te creëren.

Hoofdstuk 2

Probleemanalyse

Quintor is een bedrijf die klanten ondersteund bij het realiseren van grootschalige, uitdagende Enterprise projecten. Aangezien de toepassing en adoptie van Blockchain technologie steeds groter wordt wil het bedrijf de toepassingsmogelijkheden en technieken onderzoeken om zo inzicht te kunnen krijgen in hoe het gebruikt kan worden in de aangeboden vraagstukken vanuit klanten.

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 contract-beheer.

De focus in deze opdracht ligt op het onderzoeken van de Blockchain onderdelen Identity Management en Distributed Network. Er zullen Blockchain implementaties onderzocht worden die de onderdelen geïmplementeerd hebben om een zo compleet mogelijk technisch overzicht te creëren van de technieken en protocol-len die gebruikt zijn om de onderdelen te realiseren. Daarnaast wordt er onderzocht wat de toepassingen en de doelen van de bestaande implementaties zijn. Uiteindelijk zal er een advies uitgegeven worden aan de opdrachtgever, waarbij een keuze gemaakt zal worden op de manier waarop een Proof-of-Concept gere-aliseerd gaat worden met als doel het toetsen van de gekozen technieken.

Hoofdstuk 3

Doelstelling

Aangezien de opdracht verspreid is over onderdelen van Blockchain technologie is er een globaal doel en een doel die specifiek voor deze opdracht geldt. Het streven naar het globale doel is het opdoen van kennis omtrent 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 oplossingen, kennis te ontwikkelen voor Quintor op het gebied van Blockchain technologie.

Hoofdstuk 4

Resultaten

4.1 Adviesrapport

Er zal een adviesrapport opgesteld worden die, met behulp van de informatie uit het onderzoek, technieken aanbeveelt om de Blockchain onderdelen Identity Management en Distributed Network te realiseren. Aan de hand van dit adviesrapport zal er in samenwerking met het bedrijf een besluit genomen worden over de technieken die geadviseerd zijn.

4.2 Proof of Concept

Het Proof-of-Concept zal de realisatie van de onderdelen Identity Management en Distributed Network bevatten met daarbij de opgestelde documentatie en ontwerpen. In het Proof-of-Concept worden de geselecteerde technieken uit het adviesrapport getoetst.

Hoofdstuk 5

Aanpak

De uitvoering van dit project zal bestaan uit meerdere delen. Allereerst zal er een literatuuronderzoek gedaan worden naar een selectie van Blockchain implementaties. Uit dit onderzoek zal een adviesrapport komen die aangeboden zal worden aan het bedrijf. Hieruit zal een keuze gemaakt worden op de manier waarop de onderdelen gerealiseerd zullen worden. Om uiteindelijk de geselecteerde technieken te toetsen zal er een Proof of Concept ontwikkeld worden.

5.1 Onderzoeksopzet

In de afstudeeropdracht wordt er een adviesrapport opgesteld waarin advies wordt gegeven over de realisatie van het Proof of Concept dat betrekking heeft tot de implementatie van een Blockchain implementatie met de onderdelen Distributed Network en Identity Management. Door kwalitatieve methodieken toe te passen wordt er een technische beschrijving opgesteld van de verschillende onderdelen in de geselecteerde Blockchain implementaties.

5.1.1 Dataverzameling

Er wordt onderzoek gedaan door middel van 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'. Voor het opdoen van voorkennis zullen er gepubliceerde research papers, wiki's en beschikbare courses doorlopen worden. Hierna zal er een selectie van Blockchain implementaties gemaakt worden die bestudeerd zullen worden in het onderzoek.

5.1.2 Dataomschrijving

Om de scope van het onderzoek te beperken met betrekking tot de beschikbare tijd wordt er een selectie van drie Blockchain implementaties gemaakt. Om tot deze selectie te komen zal er een lijst van de top 20 cryptocurrencies opgesteld worden en onderzocht worden op de beschreven inclusie- en exclusiecriteria.

Inclusie- en exclusiecriteria

De implementaties zijn in eerste instantie geselecteerd op de aanwezigheid van het onderdeel Identity Management. Daarnaast spelen de attributen open-source, of er een technische White paper beschikbaar is en het gebruikte consensus algoritme een rol tijdens de selectie van de vijf implementaties. Om diverse implementaties in kaart te brengen voor het uitbrengen van een zo goed mogelijk advies is het van belang dat de onderdelen Identity Management en Distributed Network op diverse wijze zijn geïmplementeerd. Hiervoor zijn onderstaande criteria vastgesteld.

Hard-forks

Een hard fork ((blockchain), 2010) is in essentie een aftakking van een bestaande blockchain door wijzigingen in de huidige structuur van de blockchain. Dit komt bijvoorbeeld voor als er een fout in de Blockchain ontdekt of misbruikt wordt. Aangezien de implementaties hiervan niet afwijken van de originele Blockchain worden hard forks niet meegenomen in het onderzoek.

Consensus algoritme

Een van de bepalende factoren van de inrichting van het onderdeel Distributed Network is het gebruik van het consensus algoritme. Dit bepaalt in hoe de verschillende verbonden cliënten overeenstemming krijgen over de waarheid van de blockchain (Konstantopoulos, 2017). Om een compleet beeld te schetsen is het nodig om implementaties te selecteren met verschillende consensus algoritmes.

5.1.3 Analysemethode

Om te bepalen welke technieken gebruikt kunnen worden vanuit bestaande Blockchain implementaties zal er deskresearch uitgevoerd worden. Hierbij worden de werkingen van de onderdelen Distributed Network en Identity Management onderzocht en technisch beschreven.

5.2 Adviesrapport

Uit het onderzoek zal een adviesrapport komen over de manieren waarop de onderdelen Identity Management en Distributed Network opgesteld zijn binnen de onderzochte implementaties. Door het overzichtelijk maken van de resultaten uit het onderzoek zal het makkelijker zijn voor het bedrijf om een keuze te maken over de manier waarop de onderdelen gerealiseerd zullen worden.

5.3 Proof-of-Concept

Om de geselecteerde keuze(s) te toetsen zal er uiteindelijk een proof-of-Concept van de onderdelen Identity Management en Distributed Network gerealiseerd worden. Het is belangrijk dat de integriteit van deze onderdelen zo goed mogelijk bewaakt worden, waardoor er veel tijd besteed zal worden aan het testen van de implementaties. Om kennis op te doen voor het testen, ontwikkelen en ontwerpen van een blockchain implementatie zal er een selectie gemaakt worden van de gebruikte methoden, toegepaste technieken en benodigde tools.

Hoofdstuk 6

Planning

Voor de uitvoering van het project is er een globale planning gemaakt die zowel de benodigde documenten en feedback momenten bevat als de werkzaamheden die verricht worden gedurende de opdracht. De planning is hieronder weergegeven in tabel 6.1.

Tabel 6.1: Planning

Mijlpaal	Duur in dagen	
<i>Orientatie</i>	10d	
Opstart	2d	
Vooronderzoek	4d	
Plan van Aanpak	4d	
<i>Onderzoek</i>	25d	
Selectie implementaties	2d	
Theoretisch kader	3d	
Implementatie #1	7d	
Implementatie #2	7d	
Implementatie #3	6d	
<i>Adviesrapport</i>	10d	
Orientatie indeling	2d	
Schrijven	7d	
Voorleggen	1d	
<i>Selecteren methoden</i>	5d	
Selectie taal	1d	
Ontwikkelomgeving	2d	
Testen	2d	
<i>Ontwikkeling</i>	25d	
Distributed Network	12d	
Identity Management	13d	
<i>Testen</i>	5d	
Integratie	5d	
<i>Overdracht</i>	5d	

Literatuur

(blockchain), F. (2010). *Fork (blockchain) wikipedia, the free encyclopedia*. Verkregen van [https://en.wikipedia.org/wiki/Fork\(blockchain\)](https://en.wikipedia.org/wiki/Fork(blockchain)) ([Online; geraadpleegd op 22 februari 2018])

Konstantopoulos, G. (2017). *Understanding blockchain fundamentals, part 2: Proof of work & proof of stake*. Verkregen van <https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of> ([Online; geraadpleegd op 22 februari 2018])

IV Implementatie selectie

V Onderzoeksrapport

Quintor

Onderzoeksrapport

**Het opzetten van een peer-to-peer netwerk met identiteit
management door middel van Blockchain technologie**

Jeffrey van Hoven
14068265@student.hhs.nl
15 mei 2018

Samenvatting

Hoofdstuk 1

Inleiding

Dit adviesrapport is geschreven in het kader van een afstudeeropdracht gedaan in opdracht van Quintor. Het doel van dit document is het adviseren van Quintor hoe de specifieke onderdelen van de Blockchain gerealiseerd kunnen worden. Dit onderzoek is gedaan omdat Quintor kennis wilt opdoen met betrekking tot het Blockchain domein, waarbij er gekeken wordt wat de mogelijkheden zijn tot het gebruik van Blockchain technologie bij haar klanten.

In het onderzoek zijn er vragen beantwoord waarbij de antwoorden hierop bijdragen aan het advies dat gegeven is. Het betreft een onderzoek hoe de onderdelen Distributed Network en Identity Management gerealiseerd zijn in de Blockchain protocollen EOS, Cardano, Bitcoin en Monero.

Inhoudsopgave

1	Inleiding	2
2	Probleemstelling	4
3	Opzet	8
4	Resultaten	9
4.1	Soorten netwerken	9
4.1.1	Proof of Work	10
4.1.2	Proof of Stake	11
4.2	Gevaren	12
4.2.1	Eclipse Attack	12
4.2.2	Majority Attack	12
4.2.3	Denial of Service (DoS)	12
4.2.4	Sybil Attack	12
4.2.5	Double spending	13
4.2.6	Nothing at Stake	13
4.3	Identiteit	14
4.4	Bitcoin	15
4.4.1	Functionaliteit	15
4.4.2	Gevaren	16
4.4.3	Identiteit	17
4.5	Cardano	18
4.5.1	Functionaliteit	18
4.5.2	Gevaren	19
4.5.3	Identiteit	19
4.6	EOS	20
4.6.1	Functionaliteit	20
4.6.2	Gevaren	20
4.6.3	Identiteit	20
5	Conclusie	21
6	Bibliografie	22

Hoofdstuk 2

Probleemstelling

Woordenlijst

0-confirmation double spending . 12

account Een combinatie van public- en private keys waarbij de public key als identificatie gebruikt wordt. 15

block races . 12

bloom filter . 16

bootstrap node . 16

difficulty Een netwerk setting dat beïnvloed hoe moeilijk om het proof-of-work op te lossen. 10

double spending . 15

elector . 11

fork . 13

miner . 16

minting Een benaming voor de manier waarop een nieuw block gegenereerd wordt bij een Proof of Stake algoritme. 11

node . 15, 16, 18

nonce Een 4-byte veld waarvan de waarde ingesteld wordt zodat de hash van een block een reeks van nullen bevat. De rest van de inhoud van een block staat hierdoor vast. 10

peer list . 16

selfish mining . 12

slot leader . 11, 18

stake . 11

token . 11, 13

UTXO-model . 18

voting power . 10, 12

wallet (node) . 16

Afkortingen

BFT Byzantine Fault Tolerance. 9

DHT Distributed Hash Table. 18

DoS Denial of Service. 3, 12, 16

DPoS Delegated Proof of Stake. 11

PoS Proof of Stake. 11, 18

PoW Proof of Work. 10, 11, 12, 16

tx transactie. 16

Hoofdstuk 3

Opzet

Hoofdstuk 4

Resultaten

4.1 Soorten netwerken

In dit hoofdstuk wordt er onderzocht welke verschillende netwerken er gebruikt worden in bestaande implementaties. Hierbij wordt zowel de definitie van soorten en de selectie van implementaties gebruikt uit de resultaten van het vooronderzoek.

"De distributie van informatie en het probleem van wederzijdse overeenstemming over een consistente staat van het netwerk vormt een uitdaging, zeker in de aanwezigheid van zelfzuchtige en/of kwaadwillende deelnemers- en B. Scheuermann (2016). Het is een uitdaging die bekend staat als het Byzantine Generals' Problem, en is beschreven door Lamport et al. (1982). Het stelt 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. In hoeverre een computersysteem hiermee om kan gaan wordt de Byzantine Fault Tolerance (BFT) genoemd en wordt aangeduid als: $f = \lfloor \frac{N-1}{t} \rfloor$ waarbij N componenten van een computersysteem zijn en t de foutieve componenten.

In blockchain implementaties zijn de componenten die onbetrouwbaar zijn de deelnemers van het peer-to-peer netwerk. Het soort netwerk is dan ook verbonden met de manier waarop consensus bereikt wordt tussen de deelnemers van het netwerk en is getypeerd als het consensus protocol dat geïmplementeerd is.

4.1.1 Proof of Work

De originele implementatie van Blockchain technologie is gepresenteerd door Nakamoto (2008) in "*Bitcoin: A peer-to-peer electronic cash system*". Het maakt gebruik van een algoritme genaamd Proof of Work (PoW) om consensus te bereiken. Hierbij gaat het om het oplossen van een wiskundig probleem $Y \in \mathbb{N} < f(X + n)$ waarbij f een hash functie is, n de nonce, X de data en Y de difficulty.

In het geval van Bitcoin is de Y waarde een getal die aangeeft wat de difficulty is om de hash te berekenen en wordt de X waarde incrementeel opgehoogd. Een voorbeeld is gegeven in fig. 4.1. Dit proces zorgt ervoor dat de integriteit van de data in een block op de Blockchain bewaakt wordt. Wanneer een kwaadwillende deelnemer aan het netwerk de data van een block wilt aanpassen die reeds opgenomen is in de Blockchain, kan er via het PoW makkelijk gevalideerd worden of het block invalide is.

```
"Hello, world!0" => 1312af178c253f84028d480
"Hello, world!1" => e9afc424b79e4f6ab42d99c
"Hello, world!2" => ae37343a357a8297591625e
...
"Hello, world!4248" => 6e110d98b388e77e9c6f
"Hello, world!4249" => c004190b822f1669cac8
"Hello, world!4250" => 0000c3af42fc31103f1f
```

Figuur 4.1: Werking Proof-of-Work, van Bitcoin Wiki (2010). Wanneer de eerste vier bits ($Y = 4$) van de hash 0 zijn is de proof opgelost.

Daarnaast beschrijft de bedenker van het protocol, Satoshi Nakamoto, het PoW algoritme als 'one-CPU-one-vote'. Aangezien het gebruikte hashing algoritme geen limitaties stelt tot de zogeheten voting power van een deelnemer in het netwerk creëert het gunstige omstandigheden voor high-end GPU eigenaren tegenover high-end CPU eigenaren (Van Saberhagen, 2013, p. 2).

Monero maakt gebruik van het CryptoNight algoritme (Noether et al., 2014), een implementatie gebaseerd op CryptoNote, waarin gebruik gemaakt wordt van een egalitair Proof of Work (Van Saberhagen, 2013, p. 11). In contrast met het Bitcoin protocol Proof of Work algoritme is het ontworpen om inefficiënt berekenbaar te zijn op een GPU, waardoor er gelijke kansen zijn voor de deelnemers van het netwerk die het mining proces uitvoeren.

4.1.2 Proof of Stake

"Een eerste overweging met betrekking tot de werking van blockchain protocollen gebaseerd op Proof of Work – zoals Bitcoin – is de energie benodigd voor hun uitvoering.- Kiayias et al. (2017). In een onderzoek gedaan door O'Dwyer en Malone in 2014 naar het energieverbruik van het Bitcoin mining netwerk is geschat dat onder redelijke omstandigheden het netwerk gelijk stond met het energiegebruik van Ierland. Om deze reden zijn er onderzoeken en experimenten gedaan naar alternatieve consensus algoritmes. Proof of Stake (PoS) is een consensus algoritme waarbij, in plaats van het verspillen van elektriciteit om zware rekenkundige problemen op te lossen, een deelnemer geselecteerd wordt om het volgende blok te genereren (doorgaans minting genoemd) op basis van willekeurige selectie en rijkdom of leeftijd (i.e., de stake).

Cardano maakt gebruik van PoS waarbij iedere deelnemer van het netwerk met een positief balans (e.g. stake) als stakeholders gezien worden. Om uitgekozen te worden om een nieuw blok te genereren moet een stakeholder geselecteerd worden als slot leader. De implementatie verdeelt de fysieke tijd in tijdvakken en elke tijdvak is verdeeld in slots. Voor elke slot wordt een slot leader verkozen, die verantwoordelijk is voor het produceren van één blok. Niet alle deelnemers van het netwerk, bijvoorbeeld die minder dan 2% van de totale circulatie van tokens hebben, worden geselecteerd om benoemd te worden tot slot leader. Deze groep van deelnemers maken deel uit van de electors groep. Electors kiezen nieuwe slot leaders gedurende het huidige tijdsvak, waarna er een selectie gemaakt wordt en de nieuwe slot leaders vaststaan voor het volgende tijdsvak. Hoe meer stake een deelnemer heeft, hoe groter de kans dat zij uitgekozen wordt om een slot leader te worden in het volgende tijdsvak. De slot leader luistert naar transacties die aangekondigd worden door andere nodes, bundelt ze in een nieuw blok, signeert het met zijn private key en publiceert het blok in het netwerk (Cardano Docs, 2013c).

EOS is een implementatie die gebruik maakt van Delegated Proof of Stake (DPoS) om consensus te bereiken. Het grote verschil tussen DPoS en PoS; in een PoS systeem is elke deelnemer die stake heeft maakt onderdeel uitmaken van het validatie- en consensusproces. Met DPoS kan elke deelnemer die stake heeft andere deelnemers kiezen die onderdeel uitmaken van het validatie- en consensusproces (Roman, K. , 2018). In contrast met het PoW algoritme is er geen competitie voor het produceren van een blok, maar wordt er samengewerkt om een blok te produceren.

4.2 Gevaren

Wanneer deelnemers uitmaken van een grootschalig netwerk die niet gecontroleerd wordt door een centrale autoriteit kan het voorkomen dat deelnemers zich misdragen. In juli 2016 is Ethereum opgesplitst in twee partities die dezelfde valuta hanteren; *Ethereum* en *Ethereum Classic*. Dit is veroorzaakt door een kwaadwillende deelnemer in het netwerk die door een bug in het systeem geld naar zichzelf toe kon sturen. Dit heeft ertoe geleid dat veel gebruikers mogelijk een aanzienlijk verlies geleden hebben, waaronder veel ontwikkelaars van Ethereum. Om dit verlies op te lossen werd er een hard-fork voorgesteld die Ethereums code aanpast waarbij de transacties van de kwaadwillende deelnemer teruggedraaid werden (Kiffer, Levin & Mislove, 2017).

Dit illustreert een van de mogelijke manieren waarop een kwaadwillende gebruiker het systeem kan ondermijnen. Om een duidelijk overzicht te geven van de gevaren binnen een gedecentraliseerd peer-to-peer systeem wordt er onderzocht welke technieken toegepast worden om aanvallen van een kwaadwillende deelnemer van het netwerk tegen te gaan.

4.2.1 Eclipse Attack

Een aanval op het peer-to-peer netwerk waarbij er controle over een deelnemer zijn toegang tot informatie gelimiteerd, of zelfs gemanipuleerd wordt. Met de juiste manipulatie van het peer-to-peer netwerk kan er informatie verduistert worden zodat een goedwillende deelnemer aan het netwerk alleen maar kan communiceren met kwaadwillende deelnemers. Dit kan leiden tot block races, selfish mining en 0-confirmation double spending (Heilman, Kendler, Zohar & Goldberg, 2015).

4.2.2 Majority Attack

Een aanval waarbij één deelnemer de richting van het netwerk bepaald door het bezitten van 51% de voting power. In het geval van Proof of Work betekent dit dat de kwaadwillende deelnemer 51% van de totale rekenkracht nodig heeft om deze aanval uit te voeren. Dit stelt de kwaadwillende deelnemer in staat om het netwerk te manipuleren en kan leiden tot 0-confirmation double spending.

4.2.3 Denial of Service (DoS)

Een algemene benaming voor een collectie van mogelijke oorzaken voor een bewuste verstoring van de services die het peer-to-peer netwerk faciliteert. Dit kan op meerdere manieren optreden, bijvoorbeeld door het invoegen van heel veel transacties in één block, zodat het lang duurt voordat het peer-to-peer netwerk het nieuwe block heeft opgenomen.

4.2.4 Sybil Attack

Een aanval waarbij een deelnemer meerdere virtuele deelnemers creëert in het netwerk waarbij de gecreëerde deelnemers het verkiezingsproces kunnen verstoren door verkeerde informatie door te geven in het netwerk, zoals positief stemmen voor een malafide transactie (Conti, Lal, Ruj et al., 2017).

4.2.5 Double spending

Bij Creditcard-gebaseerde betalingen wordt er eerlijkheid bereikt door het bestaan van een bank of een andere vertrouwde tussenpersoon (e.g. Paypal). Hierbij wordt de tussenpersoon vertrouwd om te controleren dat diegene die een betaling doet aan een derde partij het geld niet al heeft uitgegeven (G. Karame, Androulaki & Capkun, 2012). In gedecentralizeerde systemen, waarbij er geen vertrouwde tussenpersoon aanwezig is, staat dit bekend als het *double spending* probleem, waarbij het mogelijk is om tokens die reeds uitgegeven zijn (i.e. opgenomen in een block) nogmaals gebruikt wordt om een transactie uit te voeren.

4.2.6 Nothing at Stake

Wanneer er een fork ontstaat is de optimale strategie elke replica van de blockchain te valideren, zodat de diegene die het validatie proces uitvoert nog steeds uitbetaald krijgt, ongeacht of de fork geaccepteerd wordt of niet.

4.3 Identiteit

Blockchain kan een zeker mate van privacy garanderen door de public en private keys, wat ervoor zorgt dat een gebruiker niet zijn echte identiteit hoeft te hanteren om met het systeem te interacteren. Echter, Meiklejohn et al. (2013) toont aan dat blockchain niet de transactionele privacy kan waarborgen omdat de waarden van alle transacties en saldo van elke public key openbaar inzichtbaar zijn.

Okamoto (1992) beschrijft zes criteria waaraan de ideale implementatie van elektronisch geld moet voldoen. In het bijzonder worden er twee criteria genoemd:

- **Untraceability:** voor elke inkomende transactie hebben alle mogelijke afzenders gelijke kansen om geïdentificeerd te worden als verstuurder.
- **Unlinkability:** voor elke twee uitgaande transacties moet het onmogelijk zijn om aan te tonen dat ze naar dezelfde persoon verstuurd zijn.

4.4 Bitcoin

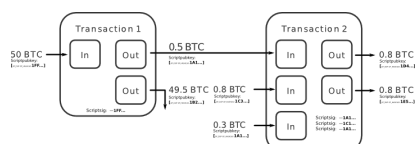
4.4.1 Functionaliteit

Architectuur Bitcoin is een netwerk waarin geen coördinerende rollen zijn. Elke deelnemer van het netwerk heeft een complete replica van alle informatie die benodigd is voor het verifiëren van de validiteit van binnenkomende transacties. Er zijn verschillende services die het netwerk faciliteert die kort toegelicht zijn in ??, twee daarvan zijn met name belangrijk voor de beschrijving van het netwerk: netwerk routing, en het mining proces. In de basis van het netwerk staan de transacties die op abstract niveau bitcoins van een of meer accounts naar een of meer bestemmingsaccounts overmaken. Een account, in de context van het bitcoin netwerk, is een combinatie van een public- en private key, waarbij de public key als identificatie van de account gebruikt wordt. Om een transactie te versturen wordt de transactie gesigneerd met de private key van de account die de transactie wilt uitvoeren.

Transacties bestaan uit een input en output. In plaats van het aggregeren van een balans voor elk account, wordt er bijgehouden wat de output van een transactie is. De balans is hierbij de som van alle openstaande outputs van het desbetreffende account. In fig. 4.2 is te zien hoe dit in zijn werk gaat. Een onderdeel van de services die de nodes binnen het netwerk aanbieden is het valideren van transacties. Hierbij worden drie onderdelen gevalideerd:

- Een output mag maar één keer geclaimd zijn.
- Nieuwe outputs worden alleen gecreëerd door een transactie.
- De som van alle waarden van de geclaimde outputs moet groter zijn als de totale som van de nieuwe gecreëerde outputs.

Wanneer dit het geval is wordt de transactie geaccepteerd en opgenomen in de lokale replica van de blockchain. Over tijd kan het voorkomen dat de replica van verschillende nodes inconsistent worden, waarbij het kan voorkomen dat er twee of meer transacties dezelfde coin meerdere malen uitgeeft. Dit staat bekend als double spending (Decker & Wattenhofer, 2013).



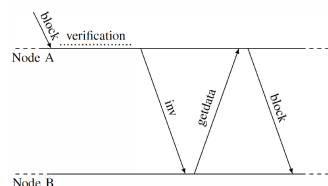
Figuur 4.2: Voorbeeld van het UTXO-model zoals in gebruik bij Bitcoin, bron: <http://news.8btc.com/thoughts-on-bytom-design-extension-of-utxo-structure>.

Een nieuw block wordt gecreëerd door het uitvoeren van het mining proces. Dit wordt uitgevoerd door zogenaamde miners node. Om te bepalen welke node verantwoordelijk is voor het volgende block moet er een oplossing gevonden worden voor het proof-of-work. Dit proces zorgt ervoor dat er een beslissing gemaakt wordt over de volgorde van de transacties, en dat de inhoud van een block niet aangepast kan worden omdat dit in directe verbinding staat met het gedane PoW.

Discovery protocol Om het het netwerk te betreden worden er DNS servers benaderd waarbij gebruik wordt gemaakt van het TCP protocol. Deze DNS servers worden in stand gehouden door vrijwilligers en geven een willekeurige set aan bootstrap nodes terug die actief zijn in het netwerk. Wanneer de node toegetreden is tot het netwerk wordt er een peer list bijgehouden met alle nodes waarmee er connectie is gelegd. Deze peer list wordt gebruikt om connectie te leggen bij een eerstvolgende toetreding tot het netwerk.

Informatie propagatie Voor het updaten en synchroniseren van de blockchain worden er transactie (tx) en block berichten verstuurd. Om tegen te gaan dat tx- en block berichten verstuurd worden naar nodes die al afweten van deze informatie, wordt er een *inv* bericht verstuurd wanneer een transactie of een block volledig geverifieerd is. Het *inv* bericht bevat een lijst van transactie- en block hashes die reeds ontvangen zijn door de verstuurder en die beschikbaar zijn om opgehaald te worden.

Wanneer een node deze informatie wilt ontvangen (bijv. omdat het de informatie nog niet heeft), wordt er een *getdata* bericht verstuurd naar de verstuurder van het *inv* bericht, met daarin de hashes van de informatie die de node wilt hebben. Fig. 4.3 visualiseert dit proces.



Figuur 4.3: Berichten die verzonden worden om informatie over een block uit te wisselen (Decker & Wattenhofer, 2013, p. 4).

4.4.2 Gevaren

Majority Attack Nakamoto (2008) stelt dat het uitvoeren van een majority attack op het netwerk onpraktisch is omdat het uitvoeren ervan niet opweegt tegen de kosten voor de benodigde hardware om de rekenkracht te behalen die hiervoor nodig is. Dit blijkt niet altijd het geval, Eyal en Sirer (2014) beschrijft namelijk een strategie genaamd Selfish Mining waarbij er gevalideerde blocks achtergehouden worden voor het netwerk waardoor er opzettelijk een fork wordt gecreëerd. De eerlijke miners zullen verder werken aan de publiekelijke blockchain terwijl de uitvoerder van het Selfish Mining strategie verder werkt op de achtergehouden blockchain. Als de uitvoerder meer blokken ontdekt ontstaat er een voorsprong op de publiekelijke blockchain en worden de blocks nog steeds achtergehouden. Wanneer de lengte van de publiekelijke blockchain de lengte van de achtergehouden blockchain benaderd, zal de uitvoerder de blockchain publiceren. Dit leidt ertoe dat miners die het Bitcoin protocol volgen hun middelen verspillen aan het minen van cryptopuzzles die er niet toe doen.

Denial of Service Over de jaren heen zijn er kwetsbaarheden in het Bitcoin protocol geïdentificeerd die het mogelijk maken om een DoS aanval uit te voeren.

De meest recente¹ aanval (NIST, 2013) exploiteert een zwakte in de implementatie van een Bloom filter, een filter die onder andere gebruikt wordt door wallets om alleen transacties binnen te halen waarbij de deelnemer betrokken is. Hierdoor was het mogelijk om een sequentie van berichten te sturen die ervoor zorgde dat een volledige node binnen het netwerk overbelast werd.

Eclipse Attack Heilman et al. heeft aangetoond dat Bitcoin's peer discovery mechanisme toegankelijk is voor een *Eclipse attack*. Door de manier waarop het Peer Discovery mechanisme werkt is het mogelijk om de lijst van connecties zo te manipuleren dat nieuwe deelnemers doorgestuurd worden naar kwaadwillende deelnemers.

Double spending G. O. Karame, Androutaki en Capkun toont aan dat het in het beginstadium van het Bitcoin protocol mogelijk was om via zogenaamde 'fast payments' een double spending aanval uit te voeren.

4.4.3 Identiteit

Er zijn drie onderdelen van het Bitcoin systeem die interessant zijn voor het analyseren van het systeem in relatie tot de identiteit van de gebruiker. Ten eerste is de gehele historie van Bitcoin transacties publiekelijk in te zien. Zoals eerder vermeld is dit nodig om zonder centrale autoriteit validatie van de transacties te doen. Het tweede is het UTXO-model dat gebruikt wordt om uitgaves en inkomsten bij te houden. In dit model bestaat een transactie uit meerdere inputs en outputs, waarbij de input een eerdere output van een transactie is geweest. Ten derde zijn de betaler en de ontvanger van een transactie gekoppeld aan de transactie door middel van een public key.

Reid en Harrigan (2013) stelt dat deze drie onderdelen, met name de publieke toegankelijkheid van de Bitcoin transacties en de input-output relatie tussen transacties en public-keys, ingedeeld kunnen worden in twee verschillende netwerken die tezamen opereren, het *transaction network* en het *user network*. Waarbij het *transaction network* de stroom van Bitcoins beschrijft tussen transacties over de tijd, en het *user network* tussen gebruikers over de tijd. Door het analyseren van de structuur van deze twee netwerken aan de hand van de informatie uit het Bitcoin netwerk, is er geconcludeerd dat het mogelijk is om verschillende public keys met elkaar te associëren, en het met de juiste middelen het mogelijk is om de activiteit van een gebruiker gedetailleerd in kaart te brengen.

Hierbij voldoet het bitcoin protocol met name niet aan de de untraceability eis. Alle transacties die gedaan worden tussen de deelnemers van het netwerk zijn publiekelijk in te zien en elke transactie kan herleid worden naar de verstuurder en ontvanger. Ook is het indirect mogelijk om twee uitgaande transacties naar dezelfde persoon aan te tonen binnen het netwerk.

¹Er zijn recentere aanvallen op het Bitcoin protocol geweest waarbij er DoS aanval heeft plaatsgevonden maar deze zijn niet nader gespecificeerd, zie: "Common Vulnerabilities and Exposures - Bitcoin Wiki".

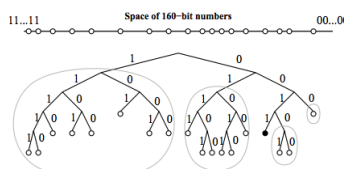
4.5 Cardano

4.5.1 Functionaliteit

Architectuur Net zoals bij Bitcoin zijn de transacties de kern van de implementatie, waarbij er wederom gebruik wordt gemaakt van het UTXO-model zoals beschreven bij de architectuur van Bitcoin. De architectuur van het Cardano netwerk bestaat uit drie soorten nodes die fundamenteel zijn voor de werking van het protocol: *core*, *relay* en *edge* nodes. *Core nodes* zijn de kern van het netwerk. Het zijn de enige nodes die geselecteerd kunnen worden om slot leader te worden, waardoor het de enige nodes zijn die een block kunnen creëren. *Relay nodes* worden gezien als de proxy tussen core nodes en het internet. Ze hebben geen stake in het netwerk, waardoor ze makkelijk te verplaatsen of veranderd kunnen worden. *Edge nodes* zijn de simpele nodes die iedereen kan uitvoeren. Deze nodes kunnen transacties aanmaken binnen het netwerk en aanbieden aan *core* nodes via de *relay* nodes (Cardano Docs, 2013a, Topology).

Discovery protocol Om het netwerk te betreden wordt er gebruik gemaakt van een bestaand protocol genaamd Kademlia, wat gebaseerd is op het gebruik van een Distributed Hash Table (DHT) architectuur. Elke node wordt behandeld als een tak in een Binary Tree waarbij de positie van een node bepaald wordt door een unieke prefix van de identificatie code van een node.

In fig. 4.4 is de positie van een node met de prefix 0011 te zien. Het protocol garandeert dat elke node in verbinding staat met een andere node. Met deze garantie kan elke node een andere node lokaliseren aan de hand van de identificatie code (Maymounkov & Mazieres, 2002, p. 2).



Figuur 4.4: Binary Tree zoals in gebruik bij het Kademlia protocol, Maymounkov en Mazieres (2002).

Informatie propagatie

Berichten worden verstuurd voor het uitwisselen van informatie tussen deelnemers. Hierbij zijn drie abstracte types gedefinieerd: *inv*, *req* en *data*. Net zoals bij Bitcoin wordt de *inv* message gebruikt om aan te geven dat er data beschikbaar is. Het *req* bericht wordt vervolgens gebruikt om beschikbare data op te vragen. De data wordt vervolgens verstuurd via een *data* message. Berichten die bijvoorbeeld een block versturen zijn nader gespecificeerde *data* berichten. Op deze drie types zijn alle berichten in het netwerk gebaseerd, bijvoorbeeld is het *MsgBlock* bericht, die block informatie uitwisselt, gebaseerd op een *data* bericht (Cardano Docs, 2013b). Een bericht kan verstuurd worden naar drie verschillende mediums: het versturen van een bericht naar een node, de burens, en het gehele netwerk. Naar welk medium het bericht wordt verstuurd is opgenomen in de header van een bericht.

4.5.2 Gevaren

Sybil Attack Een fundamenteel probleem bij een implementatie van PoS, zoals beschreven door (Kiayias et al., 2017), is het simuleren van een leiderschapsverkiezing. Om een eerlijke, willekeurige verkiezing onder deelnemers van het netwerk te hebben is het nodig om een zekere mate van wanorde te introduceren. Mechanismes die benodigd zijn om deze wanorde te introduceren zijn gevoelig voor beïnvloedingen van kwaadwillende deelnemers in het netwerk.

Eclipse attack In het Kademlia netwerk is het mogelijk om een eclipse attack uit te voeren, maar wel lastig. In Cardano Docs (2013b) wordt uitgelegd hoe dit mogelijk zou zijn. Door de manier waarop het netwerk ingedeeld is, is het mogelijk, indien het netwerk constant blijft, om door veel nodes in het netwerk aan te maken de IDs rondom een bestaande node te bezitten, waardoor de communicatie met deze node te manipuleren is. Om dit tegen te gaan heeft Monero een uitbreiding gerealiseerd op het Kademlia protocol, waarbij node IDs vervangen worden door HashIds.

Een HashId is een binaire reeks van 32 bytes bestaande uit twee onderdelen. De nonce, een willekeurige 14 reeks aan bytes binaire reeks, en hashing data dat gegenereerd wordt aan de hand van de zogenaamde DerivingKey, een PBKDF2 hash dat gebruik maakt van HMAC (Hash-based Message Authentication Code) en een Salt, een SHA-512 hash (Cardano Docs, 2013a, P2P Layer, Addressing).

4.5.3 Identiteit

TODO

4.6 EOS

4.6.1 Functionaliteit

<https://steemit.com/eos/@trogdor/eos-vs-ethereum-for-dummies>

De blockchain implementatie EOS werkt toe naar een operating systeem speciaal voor blockchain toepassingen. In eerste instantie zal er een Blockchain gerealiseerd worden die dient als proof-of-concept van het ontwerp. In dit proof-of-concept is er een eerste versie gerealiseerd die het mogelijk maakt voor developers om een eigen applicatie op het EOS netwerk te creëren. Hierbij is de focus gelegd het faciliteren van functionaliteiten die betrekking hebben op account permissies, authenticatie en de communicatie tussen het internet en het netwerk. Er wordt gespeculeerd dat EOS een sterke concurrent van Ethereum zal worden als het gaat om Blockchain als een developer platform.

Architectuur EOS maakt gebruik van aanpak waarbij extensies op de basis componenten (e.g. het netwerk, de 'chain', etc.) gerealiseerd worden als plugins. Dit maakt het zodat het protocol makkelijk te wijzigen is in de toekomst.

Discovery protocol

Informatie propagatie

4.6.2 Gevaren

TODO

4.6.3 Identiteit

TODO

Hoofdstuk 5

Conclusie

Hoofdstuk 6

Bibliografie

- 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>
- Bitcoin Wiki. (2010). *Proof of work*. Verkregen van https://en.bitcoin.it/wiki/Proof_of_work ([Online; benaderd op 29 maart, 2018])
- Cardano Docs. (2013a). *Cardano*. Verkregen van <https://cardanodocs.com/technical/protocols/p2p/#addressing>
- Cardano Docs. (2013b). *Csl application-level messaging - cardano*. Verkregen van <https://cardanodocs.com/technical/protocols/csl-application-level/>
- Cardano Docs. (2013c). *Ouroboros proof of stake algorithm - cardano*. Verkregen van <https://cardanodocs.com/cardano/proof-of-stake/>
- Conti, M., Lal, C., Ruj, S. et al. (2017). A survey on security and privacy issues of bitcoin. *arXiv preprint arXiv:1706.00916*.
- Decker, C. & Wattenhofer, R. (2013, Sept). Information propagation in the bitcoin network. In *Ieee p2p 2013 proceedings* (p. 1-10). doi: 10.1109/P2P.2013.6688704
- en B. Scheuermann, F. T. (2016, thirdquarter). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys Tutorials*, 18(3), 2084-2123. doi: 10.1109/COMST.2016.2535718
- 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).
- 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).
- Karame, G., Androuraki, E. & Capkun, S. (2012). Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin. *IACR Cryptology ePrint Archive, 2012*(248).

- 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).
- Kiffer, L., Levin, D. & Mislove, A. (2017). Stick a fork in it: Analyzing the ethereum network partition. In *Proceedings of the 16th acm workshop on hot topics in networks* (pp. 94–100).
- 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).
- Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M. & Savage, S. (2013). A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on internet measurement conference* (pp. 127–140).
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
- NIST. (2013). *Nvd - cve-2013-5700*. Verkregen van <https://nvd.nist.gov/vuln/detail/CVE-2013-5700> ([Online; benaderd op 6 april, 2018])
- Noether, Y. et al. (2014). Monero is not that mysterious. *Technical report*.
- O'Dwyer, K. J. & Malone, D. (2014). Bitcoin mining and its energy footprint..
- Okamoto, K., Tatsuaki en Ohta. (1992). Universal electronic cash. In *Proceedings of the 11th annual international cryptology conference on advances in cryptology* (pp. 324–337). London, UK, UK: Springer-Verlag. Verkregen van <http://dl.acm.org/citation.cfm?id=646756.705374>
- 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*.

Tabel 1: Bekeken implementaties uit de initiële selectie met de onderzochte attributen.

Blockchain	Identity Management	Whitepaper	Open-source	In circulation since	Available Dapps development platform	Notes	Consensus	Website	Repository	Gebruikte talen	Whitepaper url
Bitcoin	No	Yes	Yes	4/27/11	No		Proof of Work	https://bitcoin.org/nl/	https://github.com/bitcoin/	C++	https://bitcoin.org/bitcoin.pdf
Ethereum	Yes	Yes	Yes	7/30/15	Yes		Proof of Work	https://www.ethereum.org/	https://github.com/ethereum/	Go, C++	https://github.com/ethereum/wiki/wiki/White-Paper
Teher	No	Yes	No	2015	Yes	Fork from Bitcoin.	Proof of Reserves	https://www.teher.io/	https://bitbucket.org/teher/		https://teher.io/wp-content/uploads/2016/06/teherwhitepaper.pdf
Ripple	Not sure	Yes	Yes	2012	No	Not really a Blockchain	Ripple Consensus Algorithm	https://ripple.com/	https://github.com/ripple/	C++	https://ripple.com/files/ripple_consensus_whitepaper.pdf
EOS	Yes	Sort of	Yes	1/31/18	Yes		Delegated Proof of Stake	https://eos.io/	https://github.com/eosio/	C++	
Cardano	Not sure	Yes	Sort of	11/29/17	Yes	Only the Settlement layer is open-source available.	Proof of Stake		https://github.com/input-output-hk/cardano-sl	Haskell	
NEO	Yes	No	Yes	2014	Yes		Delegated Byzantine Fault Tolerance	https://neo.org/	https://github.com/neo-project/	Walter in C++	https://aun.org/uploads/files/a272ef64dc81w396d48095b1.pdf
Quum	Yes	Yes	Sort of	11/3/17	Yes	Adopts the UNO model from Bitcoin while utilizing the Ethereum network. Implements PoS 3.0 as sorted by the original Proof of Stake coin Bitcoin. Only the wallet is open-source.	Proof of Stake	https://quum.org/en/	https://github.com/quumproject/		
TRON	No	Yes	Sort of	2017	No	Badly translated whitepaper and web-site.	Proof of Stake	https://tron.network/en.html	https://github.com/tronprotocol/	Java	https://836f9e91.uns1.com/tron/whitebook/TronWhitepaper_en.pdf
Status	Yes	No	Yes		Yes	Identity Management in form of user-names. Mobile client voor Ethereum, een Dapp die het mogelijk maakt om te interfaen met andere Dapps?	Proof of Work	https://status.im/	https://github.com/status-im/	Go	
Stellar	Not sure	Sort of	Yes	2014	Yes	Whitepaper only describes the consensus protocol, initially based on the Ripple protocol.	Stellar Consensus Protocol	https://www.stellar.org	https://github.com/stellar/	C	
Huobi Token	No	No	No		No	Legality Blockchain users can buy but ? are awarded these tokens. Doesnt look like anything's available for this crypto.	?	https://www.huobi.pro			
AMN Coin	Not sure	No	No		No			https://amncoin.com/website/en/ico			https://amncoin.com/content/downloads/amncoin_whitepaper_en-us.pdf
Dash	No	Sort of	Yes	1/6/14	Not sure	Initially named Xeon (XC), renamed to Darkcoin and then rebranded as Dash. Fork from Litecoin. First self-funded blockchain. Transaction fees go to a treasury which funds development.	Proof of Service	https://www.dash.org/	https://github.com/dashpay/	C++	https://github.com/dashpay/dash/wiki/Whitepaper
VeChain	No	No	No	2015	No	Chinese, private blockchain for retail usage in combination with IoT.		https://www.vechain.com/#/			
LSK	Yes	No	Yes	9/22/17	Yes	Technical documentation available at https://lsk.io/documentation , albeit not in depth.	Delegated Proof of Stake	https://lsk.io/	https://github.com/LSK-HQ	JavaScript	https://lsk.io/documentation/
Monero	Yes	Yes	Yes	4/18/14	No	Claims to be one and only fully anon-mized Blockchain implementation.	Proof of Work	https://getmonero.org/	https://github.com/monero-project/	C++	https://download.getmonero.org/whitepaper_a.moredated.pdf
Behave (CON)	Yes	Yes	Yes			Uses black and white addresses.	PoW + PoS	https://nashv/	https://github.com/HeastOrg	C++	
Nano	No	Yes	Yes		Not sure	Previously known as Flabbits, second blockchain that uses a tangle instead of a chain.	Loop Fault Tolerance	https://nano.org/en	https://github.com/con-foundation/		https://con-foundation/resources/whitepaper/CONWhitepaper-EN-Draft.pdf

VI Adviesrapport

Quintor

Adviesrapport

**Het opzetten van een peer-to-peer netwerk met identiteit
management door middel van Blockchain technologie**

Jeffrey van Hoven
14068265@student.hhs.nl
9 mei 2018

Inleiding

Dit adviesrapport is geschreven in het kader van een afstudeeropdracht gedaan in opdracht van Quintor. Het doel van dit document is het adviseren van Quintor hoe de specifieke onderdelen van de Blockchain gerealiseerd kunnen worden. Dit onderzoek is gedaan omdat Quintor kennis wilt opdoen met betrekking tot het Blockchain domein, waarbij er gekeken wordt wat de mogelijkheden zijn tot het gebruik van Blockchain technologie bij haar klanten.

In het onderzoek zijn er vragen beantwoord waarbij de antwoorden hierop bijdragen aan het advies dat gegeven is. Het betreft een onderzoek hoe de onderdelen Distributed Network en Identity Management gerealiseerd zijn in de Blockchain protocollen EOS, Cardano, Bitcoin en Monero.

Inhoudsopgave

1	Onderzoeksopzet	3
2	Alternatieve maatregelen	4
3	Conclusie	5
4	Bronnen	6

1 Onderzoeksopzet

Er is als eerste een vooronderzoek uitgevoerd naar het Blockchain domein, welke als afbakening en informatie gebruikt wordt in het onderzoek. Als eerste is gekeken naar de wat Blockchain is en welke mogelijkheden er zijn tot het toepassen van deze technologie. Vervolgens is er gekeken naar de architectuur van een Blockchain implementatie en is er een afbakening gemaakt van de onderdelen Identity Management en Distributed Network.

Met deze kennis is uiteindelijk het onderzoek uitgevoerd waarbij er vier Blockchain protocollen, EOS, Cardano, Monero en Bitcoin, zijn onderzocht op de onderdelen Distributed Network en Identity Management. Hierbij zijn technieken naar voren gekomen die interessante aanpakken hebben op het gebied van de benoemde onderdelen.

2 Alternatieve maatregelen

Wat gaat de maatregel opleveren of welke bijdrage levert de maatregel aan de oplossing van het probleem of vraagstuk? Binnen hoeveel tijd?

Waaruit blijkt dat de maatregel iets oplevert?

Wat is ervoor nodig (geld, tijd, mensen, organisatie)?

Wat zijn de voor- en nadelen van de maatregel?

3 Conclusie

4 Bronnen

VII Voortgangsverslag

Voortgangsverslag: Afstuderen Quintor Den Haag
28 maart 2018
Jeffrey van Hoven

In dit document wordt de voortgang besproken in het afstudeertraject van Jeffrey van Hoven bij het bedrijf Quintor in Den Haag. Het omvat werkzaamheden van 4 sprints waarin er gewerkt is aan het opstellen van het plan van aanpak, het doen van vooronderzoek, onderzoeksopzet en een start maken aan het uitvoeren van het onderzoek.

Plan van Aanpak

Het opstellen van het plan van aanpak duurde iets langer als ingepland. Uiteindelijk is er veel tijd besteed aan het beschrijven van de aanpak en het scherpstellen van de probleemstelling en doelstelling. Dit is in overleg gebeurd met de begeleider vanuit Quintor, Ben Ooms, en een mede afstudeerder, Kevin Bos, die het lokale onderdeel van de Blockchain onderzoekt. Hier zijn meerdere gesprekken over gehouden en daarom is het opstellen van het plan van aanpak ook een beetje uitgelopen.

Vooronderzoek

Gedurende de tijd die gebruikt werd om het plan van aanpak op te stellen is er ook vooronderzoek gedaan naar de onderdelen die deel uitmaken van mijn afstudeeropdracht, namelijk het Distributed Network en het Identity Management. Hierdoor is er tijds winst geboekt bij het doen van het vooronderzoek terwijl het plan van aanpak uitliep. De beschrijving van de werkzaamheden is hierbij wel achtergelopen voor het afstudeerverslag, wat weer ingehaald is in de afgelopen weken.

Onderzoeksopzet

Aan dit onderdeel is veel tijd besteed waardoor het uitgelopen is. Zo is er veel tijd verloren gegaan aan het opstellen van een selectiemethode voor de te onderzoeken implementaties. Daarnaast bleek het opstellen van de hoofdvraag en deelvragen redelijk lastig, aangezien de scope van het onderzoek niet is beperkt vanuit Quintor. Hier zijn ook meerdere gesprekken over geweest gedurende het project waaruit naar voren kwam dat de toepassing pas gegeven werd na het onderzoek.

Conclusie

In het algemeen loop ik achter op de initiële planning die ik gemaakt heb. Zoals besproken tijdens het bezoek van dhr. T. Cocx bij Quintor, is er ruim de tijd genomen om het adviesrapport op te stellen. Die tijd kan gelijktijdig gebruikt worden om het onderzoek uit te voeren. Over het algemeen ben ik tevreden met de voortgang die ik gemaakt heb, en ik hoop dat de obstakels die ik tegengekomen ben tijdens het opstellen van het plan van aanpak en het onderzoek duidelijk terug te lezen zijn in mijn afstudeerverslag.

VIII Bezoekverslag

Bezoekverslag: Afstuderen Quintor Den Haag
27 maart 2018
Jeffrey van Hoven

Verslag

Op 19 maart 2018 is dhr. T. Cocx langsgeweest voor het benodigde bedrijfsbezoek bij Quintor Den Haag om kennis te maken met het bedrijf en meer inzicht te krijgen in de afstudeeropdracht die uitgevoerd wordt door de student. In dit document worden de belangrijkste afspraken, leerpunten en conclusies besproken.

Afspraken

Tijdens het bezoek is er kort verteld over de mogelijkheden tot het verkrijgen van feedback. Er werd nadruk gelegd op de tussentijdse beoordeling en dat het belangrijk is om deel te nemen aan het feedbackmoment dat beschikbaar is in de 10de week van de afstudeeropdracht. Hierbij is duidelijk verteld dat er verwacht wordt dat de student, indien hij gebruik wilt maken van het feedbackmoment, verwacht wordt om 60% van het verslag afgerond te hebben. Het is ook aan de student om de afspraak te maken indien hij er gebruik van wilt maken.

Leerpunten

Daarnaast is er gesproken over inhoudelijke werkzaamheden in relatie tot het verslag. Hierbij zijn een aantal punten genoemd over de formulering van het onderzoek. Er werd bijvoorbeeld gesproken over "technieken", wat een nogal vage term is en meerdere betekenissen kan hebben. Als suggestie werd er gegeven om het "protocol implementaties" te noemen.

Het tweede onderwerp was de stakeholder relatie met een andere afstudeerder die een onderdeel van de Blockchain gaat realiseren. Dit is totaal niet beschreven in het afstudeerverslag, maar toont wel de complexiteit van de opdracht. Er werd dan ook als tip gegeven om dit wel te beschrijven in het afstudeerverslag.

Conclusies

Uit het gesprek is waardevolle feedback gekomen. Aangezien er veel nadruk werd gelegd op het feedback moment in de 10de week, ook al is er aangegeven dat het niet benodigd is, zal er zeker naar toegewerkt worden om die datum als een deadline neer te zetten.