Onderzoek naar

Gedistribueerde netwerken en identiteits management binnen Blockchain technologie

Jeffrey van Hoven

26 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

Lijst van figuren

Lijst van tabellen

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 | 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.

2.1 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 worden 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 maken van de onderdelen.

2.2 Onderzoek

In de opdrachtomschrijving die aangeleverd is door Quintor zijn er geen duidelijke eisen en specificaties gesteld aan zowel de uitvoering als realisatie van de afstudeeropdracht. Dit heeft ertoe geleid det er een gesprek gehouden is met de Blockchain expert, Pim Otte, en de begeleider, Ben Ooms, over de eisen, afbakening en in welke mate de samenwerking met Kevin Bos 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.

Opzet Om een zo compleet mogelijk technische beschrijving van de werkingen van de gespecificeerde onderdelen te maken wordt er kwalitatief onderzoek uitgevoerd. Dit zal gedaan worden met behulp van deskresearch. De uitvoering van het deskresearch bestaat uit het onderzoeken van bestaande Blockchain protocollen, waarbij er indien mogelijk gebruik wordt gemaakt van wetenschappelijke literatuur.

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.

2.3 Proof of Concept

De uitgekozen technieken zullen gerealiseerd worden in een Proof of Concept. Dit zal in samenwerking zijn met Kevin Bos, 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.

2.4 Planning

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

Literatuur

Bijlages

I Opdrachtformulering

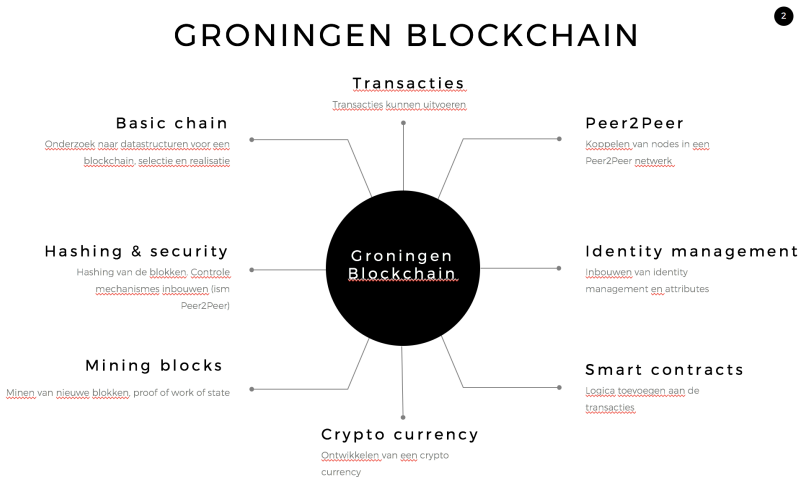
ONTWIKKELING VAN EEN GEDISTRIBUEERDE BLOCKCHAIN

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.



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 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 examinator: T. Cocx
Naam tweede examinator: 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.

Opdrachtomschrijving

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.**
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: Bijvoorbeeld: - Gaat het onderdeel Distributed Network webbased werken of met een ander protocol? Concrete taken: - 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.**
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. Concrete taken: - Een object georiënteerd ontwerp van de onderdelen Distrubuted 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.**
Het ontwikkelen van de onderdelen Distributed Network en Network & Identity Management waarbij gebruikt wordt gemaakt van een object georiënteerde programmeertaal. Concrete taken: - Het ontwikkelen van de onderdelen Distributed Network en Network & Identity Management door middel val 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.**
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. Concrete taken: - 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

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 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.

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 opensource, 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**	
Orientatie	10d	
Opstart	2d	
Vooronderzoek	4d	
Plan van Aanpak	4d	
Onderzoek	25d	
Selectie implementaties	2d	
Theoretisch kader	3d	
Implementatie #1	7d	
Implementatie #2	7d	
Implementatie #3	6d	
Adviesrapport	10d	
Orientatie indeling	2d	
Schrijven	7d	
Voorleggen	1d	
Selecteren methoden	5d	
Selectie taal	1d	
Ontwikkelomgeving	2d	
Testen	2d	
Ontwikkeling	25d	
Distributed Network	12d	
Identity Management	13d	
Testen	5d	
Integratie	5d	
Overdracht	5d	

Literatuur

(blockchain), F. (2010). *Fork (blockchain) wikipedia, the free encyclopedia.* Verkregen van `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

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

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: $f = [\frac{N-1}{t}]$ 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 aanduid 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 proef 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 block 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 verkiezen 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 block, signeert het met zijn private key en publiceert het block 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 verkiezen 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 block, maar wordt er samengewerkt om een block 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 gedecentralizeerd 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 betekend 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 vertrouwe 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:

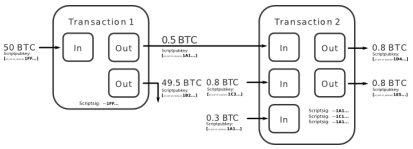
- **Untraceability:** voor elke inkomende transactie hebben alle mogelijke afzenders gelijke kansen om geïdentificeerd te worden als verstuurder.
- **Unlinkability:** voor elke twee uitgaande transacties moet het onmogelijk zijn om aan te tonen dat ze naar dezelfde persoon verstuurd zijn.

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 desbetreffend 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:



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

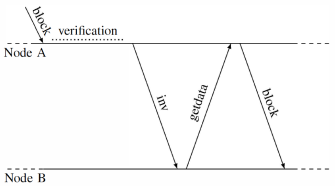
Wanneer dit het geval is wordt de transactie geaccepteerd en opgenomen in de lokale replica van de blockchain. Over tijd kan het voorkomen dat de replica van verschillende nodes inconsistent worden, waarbij het kan voorkomen dat er twee of meer transacties dezelfde coin meerdere malen uitgeeft. Dit staat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

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 inhoudt 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 onstaat 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 leid 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 recente[1] aanval (NIST, 2013) exploiteert een zwakheid 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, Androulaki 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 tesamen 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.

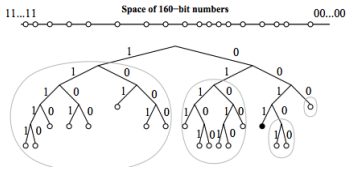
[1] Er zijn recentere aanvallen op het Bitcoin protocol geweest waarbij er DoS aanval heeft plaatsgevonden maar deze zijn niet nader gespecificeerd, zie: "Common Vulnerabilities and Exposures - Bitcoin Wiki".

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 verplaatsten 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.



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

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).

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 buren, 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., Androulaki, 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
Tether	No	Yes	No	2015	Yes	Fork from Bitcoin.	Proof of Reserves	https://www.tether.to/	https://bitbucket.org/tetherto/		https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.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		
Qtum	Yes	Yes	Sort of	11/13/17	Yes	Adopts the UTXO model from Bitcoin while utilizing the Ethereum network. Implements PoS 3.0 as coined by the original Proof of Stake coin Blackcoin. Only the wallet is open-source.	Proof of Stake	https://qtum.org/en/	https://github.com/qtumproject	Wallet in C++	https://qtum.org/uploads/files/a2772efe4dc8ed1100319c6480195fb1.pdf
TRON	No	Yes	Sort of	2017	No	Badly translated whitepaper and website.	Proof of Stake	https://tron.network/en.html	https://github.com/tronprotocol	Java	https://o836fheg1.qnssl.com/tron/whitebook/TronWhitepaper_en.pdf
Status	Yes	No	Yes	-	Yes	Identity Management in form of usernames. Mobile client voor Ethereum, een Dapp die het mogelijk maakt om te interfacen 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 te Ripple protocol	Stellar Consensus Protocol	https://www.stellar.org	https://github.com/stellar	C	
Huobi Token	No	No	No		No	Loyalty Blockchain, users cant buy but are awarded these tokens.	?	https://www.huobi.pro			
ATMCoin	Not sure	No	No	-	No	Doesnt look like anythings available for this crypto.		https://atmcoin.com/website/inicio			https://atmcoin.com/contenidos/documentos/atmcoin_whitepaper_en-us.pdf
Dash	No	Sort of	Yes	1/18/14	Not sure	Initially named Xcoin (XCO), 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/#/			
Lisk	Yes	No	Yes	9/22/17	Yes	Technical documentation available at https://lisk.io/documentation, albeit not in-depth.	Delegated Proof of Stake	https://lisk.io/	https://github.com/LiskHQ	JavaScript	https://lisk.io/documentation/
Monero	Yes	Yes	Yes	4/18/14	No	Claims to be one and only fully anonimized Blockchain implementation	Proof of Work	https://getmonero.org/	https://github.com/monero-project	C++	https://downloads.getmonero.org/whitepaper_annotated.pdf
Hshare	Yes	Yes	Yes			Uses black and white addresses	PoW + PoS	https://h.cash/	https://github.com/HcashOrg	C++	
ICON	Yes	Yes	No		Not sure		Loop Fault Tolerance	https://icon.foundation/?lang=en	https://github.com/icon-foundation/		https://icon.foundation/resources/whitepaper/ICON-Whitepaper-EN-Draft.pdf
Nano	No	Yes	Yes		No	Previously known as Raiblocks. Second blockchain that uses a tangle instead of a chain.		https://nano.org/en			

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

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 tijdswinst 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.