

Automatiseren Claim Process

*Blockchain en Smart contract technologie gebruiken
om een gedistribueerd claim systeem te ontwikkelen*

Door: Calum Iain Munro



Software Development, ICA, VT

HBO bachelorscriptie:

Versie: 1 (Draft)

Datum: 17 mei 2018

Gegevens opdrachtgever:

Bedrijf: HeadForward B.V.

Contactpersonen: Daniël Siahaya

Gegevens opleiding:

Opleiding: HBO bachelor Informatica

School: Hogeschool van Arnhem en Nijmegen

Begeleider: Misja Nabben

Assessor: Rein Harle

Gegevens opdrachtnemer:

Teamlid: Calum Iain Munro (549288)

INHOUDSOPGAVE

1 Versiebeheer	3
2 Inleiding	4
2.1 Aanleiding	4
2.2 Relevantie	4
2.3 Probleemstelling	5
3 De blockchain technologie	6
3.1 Het algemene concept achter de blockchain	6
3.2 Type Blockchain	9
3.2.1 Privé Blockchain	9
3.2.2 Consortium Blockchain	9
3.2.3 Openbare Blockchain	10
4 De architectuur van de blockchain technologie	11
4.1 Blok (block)	11
4.2 Gedecentraliseerd netwerk	11
4.3 Consensus (overeenstemming) algoritmes	11
4.4 Smart contract	12
5 De huidige staat van de blockchain technologie	13
6 Implementatie	14
6.1 User stories en requirements	15
7 Conclusie	19
Bibliografie	19
8 Bijlagen	21
A Smart contract: Claims	22

HOOFDSTUK 1

VERSIEBEHEER

Datum	Versie	Door wie	Aanpassing
12-03-2018	v0	Iain Munro	Eerste opzet

HOOFDSTUK 2

INLEIDING

Allereerst word in dit hoofdstuk het onderwerp van deze scriptie behandeld. Dit word gedaan door eerst in paragraaf 2.1 de aanleiding van het onderzoek te bespreken. Waarna de relevantie in paragraaf 2.2 wordt besproken en aansluitend in paragraaf 2.3 de doel- en vraagstellingen zijn geformuleerd.

Het verdere verslag bestaat uit de resultaten van het onderzoek. Het begint met de eerste deelvraag waar de resultaten van het algemene onderzoek naar een aantal basis technische termen in blockchain-technologie en gerelateerde concepten zoals smart contracts word gedaan. Hierna worden er gekeken naar de implementatie van het proof of concept, door de requirements te onderzoeken zodat er in het laatste gedeelte naar de staat van de blockchain technologie gekeken kan worden en een aantal beslissingen naar de oplossingsrichting gemaakt kunnen worden.

2.1 Aanleiding

Zoals al aangegeven in het plan van aanpak verzekeren verzekeringsmaatschappijen zoals Allianz panden voor miljoenen. Dit type verzekeringen wordengedeeld met meerdere verzekeraars, om zo het risico te verspreiden. Dit principe heet co-insurance en het probleem hiermee en ook gelijk de aanleiding voor dit onderzoek is dat het claimproces te veel tijd kost voordat deze wordt uitgekeerd naar de klant. Waardoor klanten van Allianz ontevreden zijn. Dit komt omdat dit proces door de verschillende instanties op verschillende handmatige manier worden uitgevoerd. Het proces wordt bijvoorbeeld bij Allianz gedaan met Excel bestanden, maar dit verschilt per verzekeringmaatschappij. Een claim kan dus vaak meer dan 3 maanden duren voordat deze werkelijk wordt uitbetaald.

2.2 Relevantie

De relevantie van dit onderzoek is om de laatste technologie op software gebied te onderzoeken om hiermee een proof of concept te ontwikkelen. In dit geval heeft de opdrachtgever aangegeven om in dit onderzoek naar de blockchain en smart contracts te willen kijken.

2.3 Probleemstelling

Het doel van deze scriptie is om aan te tonen hoe blockchaintechnologie en smart contracts gebruikt kunnen worden om informatie over claims van verzekeringen veilig te delen en te controleren tussen partijen die elkaar niet noodzakelijk vertrouwen.

Dit wordt bewezen door een proof-of-concept software applicatie voor de use case van elektronische verzekeringgegevens. De resultaten van het onderzoek kan buiten de scope van dit onderzoek toegepast worden voor andere usecases.

De hoofdvraag van dit onderzoek is (**MRQ**):

MRQ - “Hoe is de blockchain technologie in te zetten om het claimproces van Allianz te automatiseren?” Deze vraag is onderverdeeld in verschillende deelvragen (**SRQ**):

- **SRQ1:** “*Wat is de blockchain en hoe werkt het?*” literatuuronderzoek naar een aantal basis technische termen in blockchain-technologie en gerelateerde concepten zoals smart contracts word gedaan.
- **SRQ2:** “*Wat is de huidige staat van de technologie en hoe kan het worden ingezet voor de claim use cases.*” Om deze vraag te beantwoorden, zal ook een literatuuronderzoek worden uitgevoerd naar de verschillende implementaties van de blockchain technologie en beslissingen worden genomen op basis van eigenschappen die belangrijk zijn voor het ontwikkelen van de Proof of Concept.
- **SRQ3:** “*Uit welke use cases, requirements en concerns bestaat het claim proces van Allianz?*” Om deze vraag te beantwoorden word er samen met de klant Allianz gekeken naar het claim proces en worden er een software architectuur opgebouwd.

Het proof of concept (PoC) in dit verslag zal alleen bestaan uit de code die nodig is voor de smart contracts. De smart contracts maken het grootste deel uit van de core business logica en autorisatie. Aangezien de korte projectduur van 3 maanden en het overvloed aan bestaande blockchain en smart contract implementaties is er gekozen om geen blockchain te programmeren.

HOOFDSTUK 3

DE BLOCKCHAIN TECHNOLOGIE

In dit hoofdstuk wordt er een korte uitleg gegeven over een aantal basis technische termen in cryptografie, blockchain-technologie en gerelateerde concepten zoals smart contracts. Dit zodat we weten waar we het over hebben wanneer we het proof of concept behandelen.

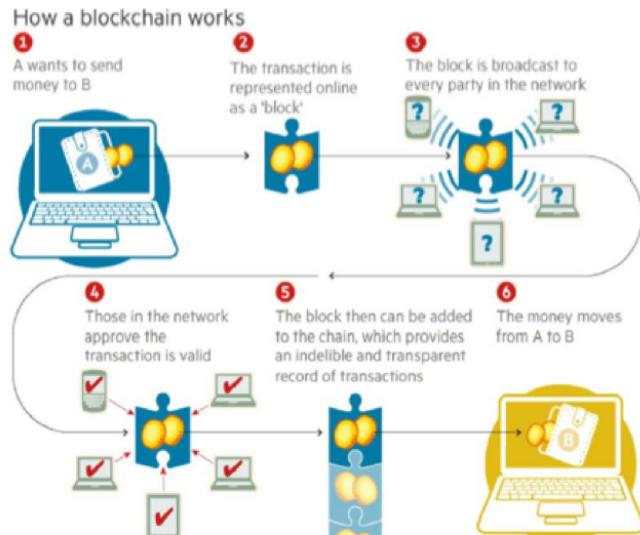
3.1 Het algemene concept achter de blockchain

Blockchain technologie is bekend geworden door de introductie van de digitale valuta bitcoin. De bitcoin werd geïntroduceerd door Satoshi Nakamoto in 2008 door een white paper genaamd Bitcoin: A Peer-To-Peer Electronic Cash System [14]. Hierin legt hij uit hoe in een peer-to-peer omgeving geld overgemaakt kan worden om online betalingen rechtstreeks van de ene partij naar de andere overgemaakt kunnen worden, zonder een financiële instelling. De blockchain is de technologie achter de Bitcoin die het mogelijk maakt.

In dit onderzoek gebruiken we de beschrijving het ICTU¹, die de blockchain beschrijft als: een specifieke databasetechnologie die leidt tot een gedistribueerd autonoom grootboeksysteem [6]. De integriteit van dit gedistribueerd autonoom grootboeksysteem wordt gewaarborgd doordat iedere partij zeggenschap heeft bij de validatie van een transactie. Dit versnelt het proces doordat beheerders en tussenpersonen worden uitgeschakeld. Meningsverschillen worden opgelost door een consensus van een meerderheid van de deelnemers.

Databasetransacties worden gegroepeerd in data blokken die vervolgens achter elkaar in een reeks blokken worden opgeslagen, vandaar de naam blockchain. De koppeling tussen blokken en hun inhoud wordt beschermd door cryptografie en kan niet worden vervalst. Daarom kan informatie die eenmaal in een blockchain is ingevoerd niet worden gewist; In essentie bevat een blockchain een accuraat, tijd gestempeld en verifieerbaar archief van elke transactie die ooit is gemaakt. Figuur 3.1 geeft het algemene idee weer van hoe deze technologie werkt met als bekende use case de bitcoin.

¹<https://www.ictu.nl/>



Figuur 3.1: Illustrert hoe de blockchain werkt [8]

De blockchain technologie lost verschillende problemen op die voorkomen bij het gebruik van traditionele gecentraliseerde database technologieën die in handen zijn van één instantie. Dit soort technologieën vereisen vertrouwen dat de beheerder zorgvuldig omgaat met de toegang of bewerkingen van de data. Verder dat de database toegankelijk is voor de belanghebbenden en dat de instantie er de volgende dag nog is. Deze problemen komen niet voor in een gedecentraliseerde blockchain database. Dit komt omdat een nieuwe dienst, software bedrijf of markten op de blockchain de volgende zes design principes [9] hanteren:

1. Netwerk integriteit

Het systeem bewaakt de data integriteit doordat ieder lid in het netwerk alle transacties kan nalopen en kan controleren. In plaats dat er maar een lid is dit proces uitvoert. Gebruikers op het netwerk kunnen rechtstreeks waarde met elkaar uitwisselen door dit te registeren op een blok. Elk blok heeft een verwijzing naar een voorgaand blok verwijzen, waardoor niemand een transactie kan verbergen of kan vervalsen. Dit omdat er meer andere gebruikers zijn met de juiste realiteit.

2. Gedistribueerd

Het systeem is volledig Gedistribueerd. Dit houdt in dat er geen één punt is van controle. Er is niet een gebruiker of organisatie die het systeem uit kan zetten.

3. Security

In Satoshi's white paper [14], geeft hij aan dat iedere deelnemer van het netwerk vereist zijn om een public key infrastructure (PKI) te gebruiken om het platform veilig te houden. De PKI is een geavanceerde vorm van asymmetrische cryptografie, waar de gebruiker beide een publiek en privé sleutel ontvangt om zichzelf binnen het netwerk te identificeren en berichten kan versleutelen en ontsleutelen.

4. Eigendomsrechten

Eigendomsrechten zijn transparant en afdwingbaar voor iedere gebruiker. Hierdoor dient een blockchain als een publiek register. Door een tool die Proof of Existence (PoE) heet. Deze tool creert en registreert de cryptografische overzichten van akten, licenties en andere rechten van gebruikers. Dit wordt gedaan door een hash te berekenen van de public key van een gebruiker.

5. Privacy

Gebruikers beheren hun eigen data. Er is geen centrale partij die dit doet. Op een blockchain netwerk kunnen gebruikers er zelf voor kiezen wat zij vrij geven aan persoonlijke informatie. Dit kan worden gedaan door persoonlijke gegeven mee te geven in hun public key of in een externe centrale database. Het gehele identificatie en verificatie laag die ervoor weggeeft wie wat naar elkaar stuurt is los van het de transactie laag. Hierdoor kunnen gebruikers op de blockchain anoniem zijn.

6. Valuta als motivatie

Het systeem motiveert deelnemers van het netwerk door ze valuta te geven voor bepaalde acties op het netwerk. In het geval van de bitcoin, krijgen miners bitcoin geld voor het eerst volgende blok te koppelen aan het vorige blok aan data. Dit wordt gedaan door een cryptografische puzzel op te lossen die geleidelijk lastiger word.

3.2 Type Blockchain

Om een geïnformeerd besluit te maken welk type blockchain juist is voor het proof of concept worden de verschillende type blockchain in dit paragraaf behandeld. Dit wordt gedaan vanaf een hoog technisch niveau. In essentie zijn er drie types blockchain: privé, consortium en openbaar. Deze types kunnen daarna weer onderverdeeld worden in twee categorieën: open bevat openbaar en gesloten bevat privé en consortium.

De categorie gesloten, waarin de types privé en consortium zitten zijn bedoelt voor een gelimiteerde omgeving zoals een bedrijf of groepen bedrijven en organisaties. Terwijl een openbare blockchain een open is tot iedereen er geen permissies zijn die mensen of systemen erbuiten houden.

Per type blockchain wordt er ook gelijk gekeken naar de grote projecten die relevant zijn. Zodat in een vervolg hoofdstuk hierover een vergelijking kan worden uitgevoerd.

3.2.1 Privé Blockchain

Voor een volledige private blockchain, moeten de schrijf rechten op een centrale plek staan die beheert wordt vaak door een organisatie. De lees rechten kunnen beide publiekelijk of ook net zo beperkt zijn als de schrijf rechten. Applicaties die gebruik maken van een privé Blockchain zijn interne apps die alleen gebruikt worden binnen een bedrijf of organisatie. Want in andere gevallen wordt publieke lees rechten en controleerbaarheid vereist [7]. Voorbeelden van privé Blockchains zijn MultiChain en Hyperledger:

MultiChain - MultiChain is een platform voor het ontwikkelen en publiceren van privé blockchains. Het lost een aantal schaalbaarheid problemen [James-Lubin] van de blockchain op met een geïnteregeerde gebruiker permissie systeem. Verder biedt het bedrijven de mogelijkheid om zonder software ontwikkelaars een blockchain op te richten [mut].

Hyperledger - Hyperledger is een open source project die ontwikkeld wordt met het doel om een geavanceerd bedrijfstakoverkoepelende blockchain implementatie te ontwikkelen. Het wordt gehost door de Linux Foundation [lin] en wordt gezamenlijk ontwikkeld door grote organisaties in financiëlen, banken, IoT, productie en technologie [hyp].

3.2.2 Consortium Blockchain

Consortium blockchain is gedeeltelijk privé. Het overeenstemmingproces ookwel consensusproces over de integriteit van de data op de blockchain wordt door een aantal vooraf geselecteerde nodes (gebruikers) uitgevoerd. Deze nodes zijn bijvoorbeeld 10 grote financiële instellingen die bij de aanmaak van een nieuwe block aan de blockchain zeggenschap hebben. Andere deelnemers van de blockchain hebben nog steeds het recht om de besluiten van de 10 nodes te controlleren, maar ze hebben verder geen stem in het feit of de volgende block valide is.

Het voordeel van de consortium variant is deze efficiënter zijn en toch voldoende transactie transparantie geven. Ook is het niet een bedrijf die alleen oordeelt over de data. Voorbeelden van dit type zijn Ethereum en R3:

Ethereum - Het Ethereum project beschrijft zich als een gedecentraliseerd platform voor applicaties die precies gedraait worden zoals ze geprogrammeerd worden zonder enige kans van fraude, censuur of

veranderingen van derden ². Applicaties, smart contracts, worden geprogrammeerd in de Solidity taal die voor het Ethereum project is ontwikkeld. Het wordt open-source ontwikkeld en er is een bondgenootschap, de Enterprise Ethereum Alliance ³ dat bestaat uit 315 fortune 500 bedrijven en organisaties, die gezamenlijk werken aan het het enige platform die smart contracts ondersteund op de blockchain.[10]

Het project kan gezien worden als verder uitgewerkte versie van Bitcoin die meer functionaliteiten toevoegt. Zo bestaat de status van Ethereum netwerk net zoals de Bitcoin uit meerdere objecten die 'accounts' worden genoemd, waarbij elke account een adres van 20 bytes en statusovergangen heeft. De staat van deze objecten worden opgeslagen in de blockchain waaruit gelijk afgeleiden kan worden waar valuta naartoe gaat.[Vitalik Buterin]

R3 - Dit is een gedistribueerd database-technologiebedrijf in New York. Het is verbonden met veel van 's werelds grootste financiële instellingen, met als missie om de voordelen van de blockchain te realiseren [Stan Higgins].

3.2.3 Openbare Blockchain

Dit type blockchain is zoals de naam al aangeeft publiek beschikbaar tot iedereen in de wereld. Dit houdt in tegenstelling tot Consortium ook het consensusproces in. Iedere gebruiker op het netwerk heeft zeggenschap op de geldigheid van nieuwe data en kan nieuwe data schrijven.

Een volledig publieke blockchain is een open-source systeem door het gebruik van zogeheten cryptoeconomics gebruikers op economisch doeleinde motiveert om samen te werken. Hierdoor kunnen ontwikkelaars die gebruik maken van zo'n blockchain belangen zoals beschikbaarheid waarborgen. Bijvoorbeeld zorgt een hogere tarief in een transactie resulteren in snellere transacties of convergentie over de nieuwe blokken die toegevoegd worden aan de blockchain. Een voorbeeld van hiervan is het bekende Bitcoin project.

Bitcoin. Bitcoin is het bekendste voorbeeld van een blockchain project. Bitcoin staat vooral bekend als digitale valuta en online betalingssysteem die door gebruik van cryptografie om valuta-eenheden te geneert en reguleert. Verder gebruikt het cryptografie om de overdracht van fondsen te verifiëren zonder een centrale bank.

²<https://www.ethereum.org/>

³<https://entethalliance.org/>

HOOFDSTUK 4

DE ARCHITECTUUR VAN DE BLOCKCHAIN TECHNOLOGIE

Dit hoofdstuk gaat iets verder in op de basis architectuur van de blockchain. Dit zodat tijdens het ontwikkelen van de Proof of Concept we de basis begrippen van de architectuur begrijpen.

4.1 Blok (block)

De blockchain bied een gedistribueerd grootboekssysteem. Gegevens worden permanent opgeslagen in het netwerk via bestanden die blokken worden genoemd. Een blok is een document alle recente transacties die nog moeten worden vastgelegd. Het heeft daarom de naam blockchain, omdat het een reeks van blokken die naar de vorige verwijzen[13].

Een blok in het geval van de Bitcoin bestaat uit een header en een body [11]. De header bestaat uit drie stukken meta gegevens. De eerste is een verwijzing naar een vorige blokhash (Merkle-hash`https://en.wikipedia.org/wiki/Merkle_root`, een datastructuur die wordt gebruikt om alle transacties in het blok efficiënt samenvatten)[4].

4.2 Gedecentraliseerd netwerk

The interactions among user on blockchain principally use a decentralized network in which each user represents a node at which a blockchain client is installed. When a user performing a transaction with another user or when a node receives data from another node, it verifies the authenticity of the data. It then broadcasts the validated data to every other node connected to it [86]. Within such a mechanism, the data spreads across the whole network. The benefit of using this mechanism is the centralization of the human factor is minimized and trust shifts from the human agents of a central organization to an open source code [5].

4.3 Consensus (overeenstemming) algoritmes

Om de werking van de blockchain te begrijpen en te vertrouwen, moet het begrip van Consensus oftewel overeenstemmings algoritmes duidelijk zijn. Deze algoritmes worden gebruikt wanneer een (nieuw) blok aan informatie geverifieerd wordt. Het zorgt voor één historie van transacties waar de geschiedenis geen ongeldige of tegenstrijdige transacties bevat.

Dit is allemaal nodig omdat de blockchain draait in een zelf gereguleerde, wantrouwende omgeving waar het nodig is om meningsverschillen over transacties binnen het netwerk op een lijn te krijgen. Het zorgt er bijvoorbeeld ook voor dat er niet één account is die meer uitgeeft dan dat het heeft, of waar hij of zij twee keer iets overmaakt, dit heet double-spending. De bekende consensus algoritmes zijn proof of work en proof of stake.

1. Proof of Work (PoW)

Het PoW consensus algoritme is het meest voorkomende algoritme in blockchain. Het werd

geïntroduceerd door de Bitcoin en gaat ervan uit dat alle peers met rekenkracht mee stemmen door PoW-instanties, crytografische puzzels op te lossen en hiermee het recht hebben om de volgende blok aan te maken in het netwerk. Zo maakt de Bitcoin gebruik van een hash-gebaseerde PoW, wat inhoudt dat de peers een nonce-waarde¹ proberen te vinden. Hierbij is wel de voorwaarden dat de vorige blokhash kleiner moet zijn dan de huidige doelwaarde die in de blokparameters staat van het vorige blok. Wanneer een dergelijke nonce wordt gevonden, maakt de miner het blok aan en stuurt hij het door naar zijn peers. Deze peers ontvangen dit dan en verifiëren of het klopt aan de hand van het vorige blok [5].

2. Proof-of-Stake (PoS)

Op het moment moet Proof-of-Stake zich nog bewijzen in de crypto valuta gemeenschap. Het is ontwikkeld om bestaande inefficiënte consensus algoritmes zoals PoW te vervangen. Het algemeen begrip van PoS is dat een peer (deelnemer van de blockchain), pas het stemrecht heeft op een nieuwe blok in de blockchain als de peer voldoende heeft ingezet in het netwerk. In het geval van PeerCoin² worden nieuwe blokken gegeneerd door het netwerk op basis van niet gespendeerde valuta en hoe oud deze is [Vasin].

Met deze methode wordt aangenomen dat mensen met meer valuta minder snel het netwerk zullen aanvallen [11]. Dit lost op het gebied van energiebesparing de problemen van PoW op, waar gebruikers miners aan zetten om valuta te ontvangen. Bij PoS wordt de valuta die niet beweegt steeds meer waard.

4.4 Smart contract

De naam smart contract (slimme contracten) is aantoonbaar een verkeerde benaming omdat ze in feite niet slim zijn noch contracten in gezond verstand. Slimme contracten zijn, in de context van blockchain, gewoon logica die op een blockchain wordt gepubliceerd, kan dergelijke transacties ontvangen of uitvoeren elk adres (transacties kunnen worden afgewezen of vereisen speciale argumenten om te functioneren) en dat kan fungeren als een onveranderlijke overeenkomst. Het doel van de slimme contracten is om op te treden als een "geautomatiseerd transactieprotocol dat de voorwaarden van een contract uitvoert" (Szabo, 1994) en werd voor het eerst bedacht door cryptograaf Nick Szabo. Het basisidee, en de bron van het contractdeel in de naam, is dat bepaalde delen van contracten kunnen zodanig in de software worden opgenomen dat de inbreuk daarop ofwel duur is of onmogelijk. Slimme contracten worden vaak verward met Ricardiaanse contracten (Griggs, 2015), de digitale opname en verbinding met andere systemen van een contract op wet. Dit is niet wat met slimme contracten wordt bedoeld, omdat ze niet legaal hoeven te zijn op geen enkele manier, noch verbonden met externe systemen. Men zou zich echter waarde kunnen voorstellen in de koppeling van slimme contracten met Ricardiaanse om de functionaliteit van iuit te besteden" juridische contracten met slimme contracten

¹https://en.wikipedia.org/wiki/Cryptographic_nonce

²<https://peercoin.net/>

HOOFDSTUK 5

DE HUIDIGE STAAT VAN DE BLOCKCHAIN TECHNOLOGIE

Dit hoofdstuk behandelt de huidige staat van de blockchain technologie en beantwoordt de vraag “*Wat is de huidige staat van de technologie en hoe kan het worden ingezet voor de claim use cases.*” (**SRQ2** in paragraaf 2.3). Om deze vraag te beantwoorden splitsen de deelvraag verder op in:

1. Wat zijn de eigenschappen die worden meegenomen in de overwegingen naar een keuze van een blockchain-technologie?
2. Welke blockchain-technologie implementaties zijn die in aanmerking komen?
3. Uit deze blockchain-technologie implementaties welke is hieruit het beste geschikt voor onze use case?

We zullen beginnen met het meer gedetailleerd toelichten van de blockchain-technologie. Er wordt een onderzoeksprotocol gepresenteerd om te laten zien welke informatie verwacht wordt van verschillende implementaties en welke implementaties werden geselecteerd en hoe ze van elkaar verschillen. Hierna wordt elke implementatie in meer detail bekeken en voor elk wordt een conceptueel representatiemodel verschaffen.

HOOFDSTUK 6

IMPLEMENTATIE

In dit hoofdstuk wordt het design van het proof of concept (PoC) die gebruik maakt van smart contracts en blockchain technologie behandeld. Eerst worden de verschillende actors (gebruikers) gedefineerd waarbij de user stories worden vastgesteld, om te voorzien van de functionele requirements van het PoC.

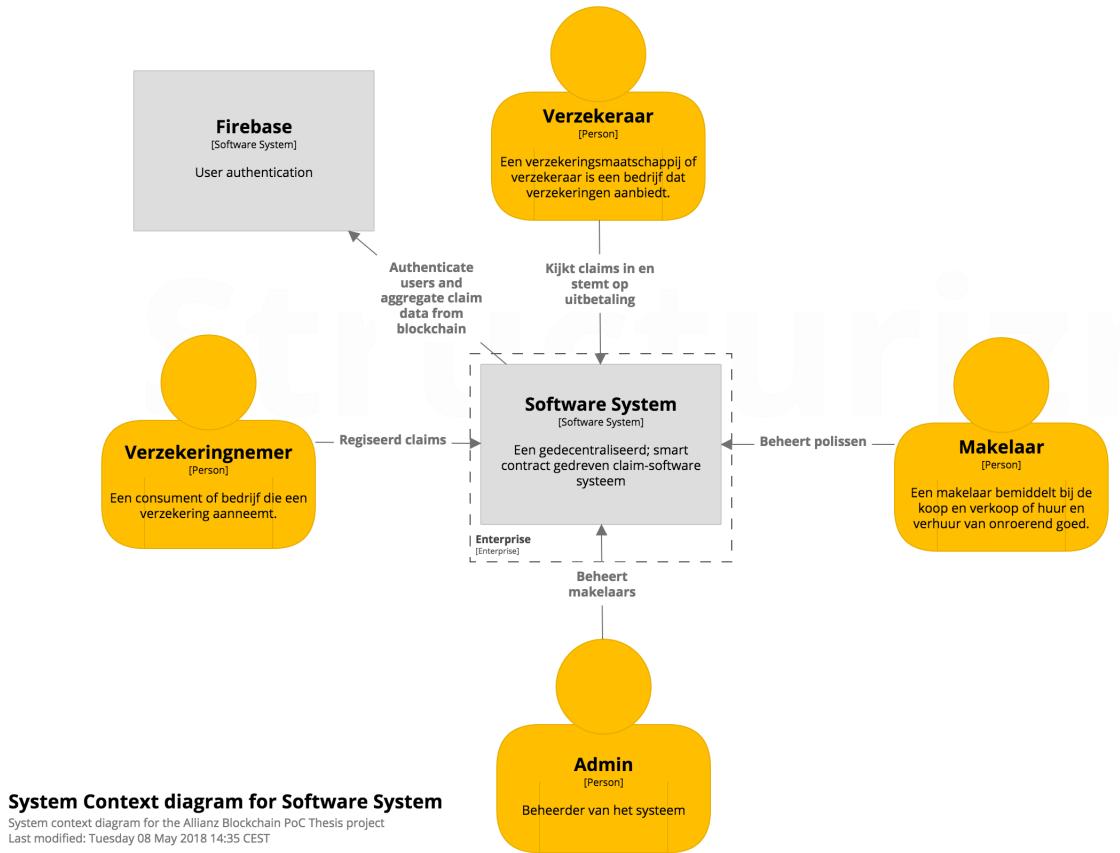
- quality attributes
- c4.

6.1 User stories en requirements

De scope van de implementatie beschreven beperkt zich tot de volgende gebruikers: verzekeraar, verzekerde en makelaar. Om zo compleet mogelijk alle functionele requirements te noteren is in de onderstaande tabel 6.1 de user stories vanuit de verschillende gebruikers perspectief geschreven. De verschillende gebruikerstypes worden daarna meer in detail gedefinieerd. Er is tijdens het opstellen van de requirements gekozen om alleen het essentiële op te schrijven en deze zoveel mogelijk de versimpelen. Te weten dat, het gebruiksgemak en security eisen van de PoC op een rendabel niveau moeten zijn.

Als een ...	Wil ik / moet ik ...	Zodat ...	Nr
Verzekerde	Kunnen zien welke ingediende claims ik heb	Ik de status hiervan kan controleren.	1.1
	Kunnen inloggen met een email en wachtwoord combinatie	Mijn informatie kan inlezen van de blockchain.	1.2
	Een claim aanvraag kunnen indienen	Ik het schadebedrijf uitbetaald krijg	1.3
	Kunnen registreren	Zodat ik kan inloggen	1.4
Verzekeraar	Kunnen zien welke ingediende claims er zijn	Ik de status hiervan kan controleren	2.1
	Mijn stem kunnen registreren op een openstaande claim	Zodat deze vervolgens goedkeuring of afkeuring ontvangt	2.2
Makelaar	Kunnen zien welke polissen er geregistreerd zijn	Zodat verzekerde claims kunnen indienen	3.1
	Een nieuwe polis kunnen registreren	Zodat verzekerde claims kunnen indienen	3.2
Admin	Makelaars registreren	Zodat deze kunnen inloggen op het systeem	4.1

Figuur 6.1: User stories die de functionele requirements defineren en het development van het proof of concept leiden.



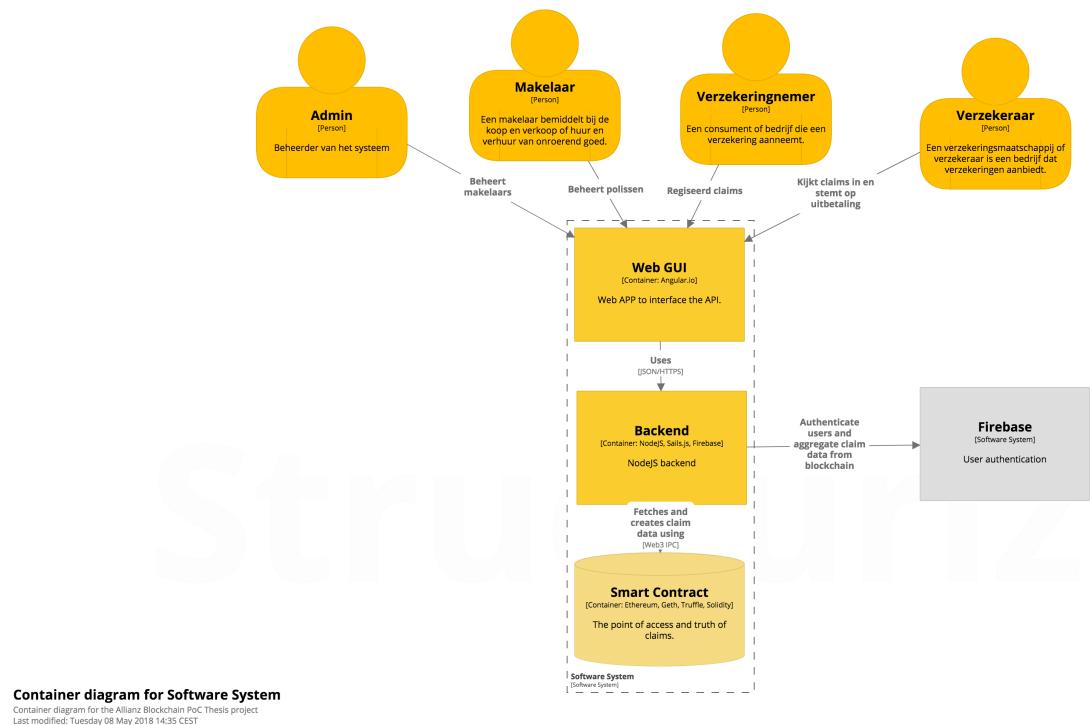
Figuur 6.2: C4 - Context.

Verzeker nemers zijn consumenten of bedrijven die een verzekering heeft en met een polisnummer claims kan aanvragen en de status van kan ophalen. De manier waarop gebruikers via de backend interactie hebben met de smart contract in de Ethereum blockchain word getoond in figuur 6.2.

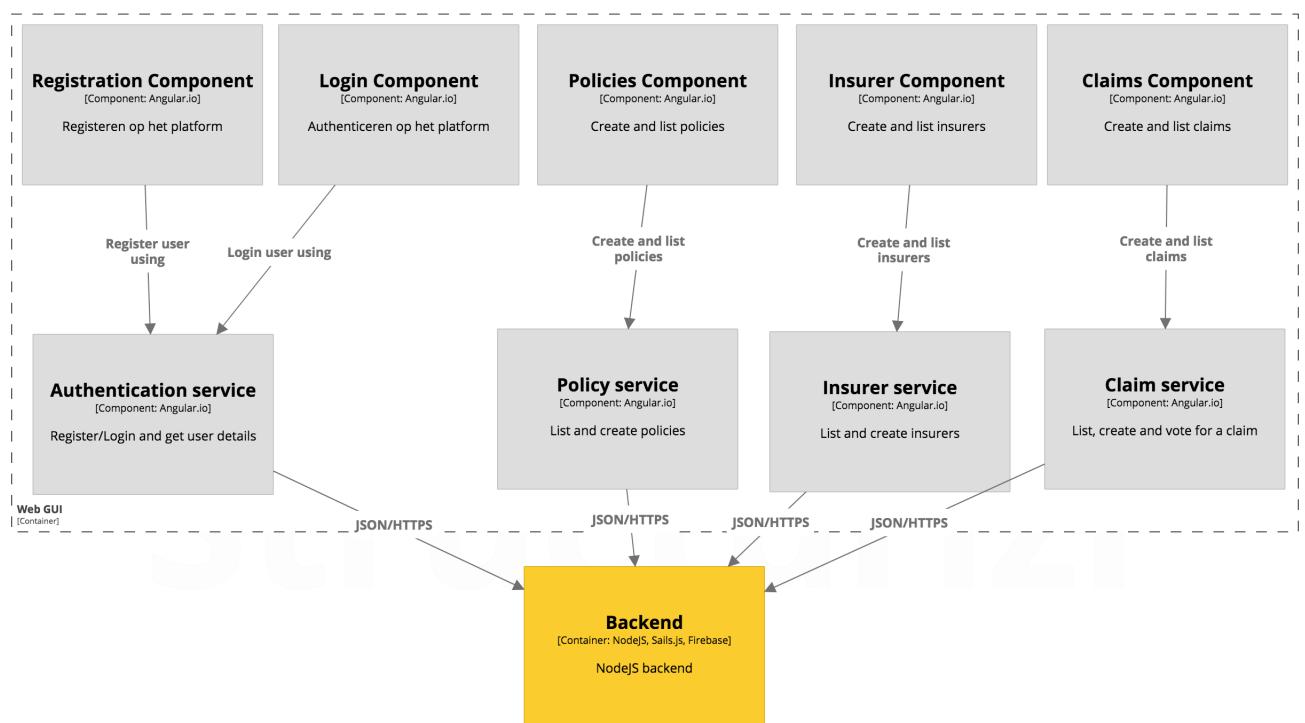
In de onderstaande opsomming staan de non-functinoele requirements die ook aan het PoC worden gesteld.

- **R1.** Het systeem geeft gebruikers toegang op basis van hun email en wachtwoord
- **R2.** Het systeem controleert bij een claim aanvraag van of het polis nummer valide is
- **R3.** Het systeem moet automatisch goedkeuring geven voor een claim als het claimbedrag onder 1000 euro zit en het type diefstal is.
- **R4.** Met gebruik van smart contracts en de blockchain wordt de data integriteit gewaarborgd.
- **R5.** Een verzekeraar kan bij het aanmaken van een nieuwe polis aangeven wat de verdeling is tussen de verzekерingsmaatschappijen.

The design of the final PoC was based on the requirements and user stories mentioned above.



Figuur 6.3: C4 - Containers.



Component diagram for Software System - Web GUI

Components diagram for the frontend of the PoC project.

Last modified: Tuesday 08 May 2018 14:35 CEST

Figuur 6.4: C4 - Containers.

HOOFDSTUK 7

CONCLUSIE

- Ethereum.

BIBLIOGRAFIE

Blockchain technologies for business.

The linux foundation.

Multichain.

Andreas M (2017). *Mastering Bitcoin (Second Edition, Second Print): Programming the Open Blockchain.*

Arthur Gervais (2016). *On the security and performance of proof of work blockchains.*

Bas Kaptijn, Peter Bergman, S. (2016). *Blockchain.*

Buterin, V. (2015). On public and private blockchains.

Dhrubes Biswas, Charlotta Johnsson, T. T. Z. I. (2016). Applied innovation review, issue no. 2 june 2016.

Don Tapscott, A. (2016). *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world.* Portfolio / Penguin.

DR. GAVIN WOOD (2014). *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER.*

Iuon-Chang Lin, T. (2017). *A Survey of Blockchain Security Issues and Challenges.* Department of Photonics and Communication Engineering, Asia University.

James-Lubin, K. Blockchain scalability: A look at the stumbling blocks to blockchain scalability and some high-level technical solutions.

Matthew English, Soren Auer, J. (2016). *Block Chain Technologies The Semantic Web: A Framework for Symbiotic Development.* Computer Science Conference for University of Bonn Students, J. Lehmann, H. Thakkar, L. Halilaj, and R. Asmat, Eds.

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

Stan Higgins. Inside r3cev's plot to bring distributed ledgers to wall street.

Vasin, P. *BlackCoin's Proof-of-Stake Protocol v2.*

Vitalik Buterin. *A NEXT GENERATION SMART CONTRACT DECENTRALIZED APPLICATION PLATFORM.*

HOOFDSTUK 8

BIJLAGEN

BIJLAGE A

SMART CONTRACT: CLAIMS

```
1 pragma solidity ^0.4.15;
2
3 contract Claims {
4
5     // Claim struct
6     struct Claim {
7         bytes32 id;
8         string policyId;
9         ClaimTypes claimType;
10        uint amount;
11        State state;
12        bool exists;
13        bytes32[] insurers;
14    }
15
16    struct Vote {
17        bool value;
18        bool hasVoted;
19        bool canVote;
20    }
21
22    enum State {New, Pending, Approved, Rejected, AutoApproved}
23    enum ClaimVote {Approved, Rejected}
24    enum ClaimTypes {NA, GlasDamage, FireDamage, StormDamage, Theft}
25
26    // Who owns this contract
27    address private authority;
28
29    // Claim[] claims;
30
31    mapping(bytes32 => Claim) claims;
32    mapping(bytes32 => mapping(bytes32 => Vote)) claimVotes;
33
34    // Map of claims for addresses
35    mapping(bytes32 => uint) claimsIndexMapping;
36    mapping(address => bytes32[]) addressClaimsMapping;
37
38    event newClaim(bytes32 id, string policyId, ClaimTypes claimType, uint
39                    amount);
40    event claimApproved(bytes32 id);
41    event claimRejected(bytes32 id);
42    event claimAutoApproved(bytes32 id);
43    event logVote(bool value, bool hasVotes, bool canVote);
```

```

43
44     // Construct me
45     function Claims() public {
46         authority = msg.sender;
47     }
48
49     function createClaim(bytes32 id, string policyId, ClaimTypes claimType, uint
50         amount, bytes32[] insurers) public {
51         require(!hasClaim(id));
52         var claim = Claim(
53             id,
54             policyId,
55             claimType,
56             amount,
57             State.New,
58             true,
59             insurers
60         );
61
61         for (uint i = 0; i < insurers.length; i++) {
62             claimVotes[id][insurers[i]] = Vote(false, false, true);
63         }
64
65         claims[id] = claim;
66         addressClaimsMapping[msg.sender].push(id);
67
68         newClaim(id, policyId, claimType, amount);
69         if (shouldAutoApprove(claim)) {
70             claim.state = State.AutoApproved;
71             claims[id] = claim;
72
73             claimAutoApproved(claim.id);
74         }
75     }
76
77     function getClaim(bytes32 id) public constant returns (
78         string policyId,
79         ClaimTypes claimType,
80         uint amount,
81         uint state
82     ) {
83         require(hasClaim(id));
84         var claim = claims[id];
85
86         policyId = claim.policyId;
87         claimType = claim.claimType;
88         amount = claim.amount;
89         state = uint(claim.state);
90     }
91
92     function vote(bytes32 claimId, bytes32 insurerId, bool vote) public {

```

```

93     require(hasClaim(claimId));
94
95     var claim = claims[claimId];
96     claim.state = State.Pending;
97     claims[claimId] = claim;
98
99     var voteObject = claimVotes[claimId][insurerId];
100    require(!voteObject.hasVoted);
101
102    voteObject.value = vote;
103    voteObject.hasVoted = true;
104    claimVotes[claimId][insurerId] = voteObject;
105
106    if (hasVoteFinished(claimId)) {
107        var approved = true;
108        for (uint i = 0; i < claim.insurers.length; i++) {
109            voteObject = claimVotes[claimId][claim.insurers[i]];
110
111            if (!voteObject.value) {
112                approved = false;
113                i = claim.insurers.length + 1;
114            }
115        }
116
117        if (approved) {
118            claim.state == State.Approved;
119            claimApproved(claimId);
120        } else {
121            claim.state == State.Rejected;
122            claimRejected(claimId);
123        }
124
125        claims[claimId] = claim;
126    }
127 }
128
129 function setClaimState(bytes32 id, State state) internal {
130     var claim = claims[id];
131
132     claim.state = state;
133     claims[id] = claim;
134 }
135
136 function shouldAutoApprove(Claim claim) internal constant returns (bool) {
137     return (
138         (claim.claimType == ClaimTypes.Theft && claim.amount < 1000)
139     );
140 }
141
142 function hasClaim(bytes32 id) internal constant returns (bool) {
143     Claim storage claim = claims[id];

```

```
144     return claim.exists == true;
145 }
146
147 function hasVoteFinished(bytes32 claimId) internal constant returns (bool) {
148     var claim = claims[claimId];
149     uint votes = 0;
150     for (uint i = 0; i < claim.insurers.length; i++) {
151         var vote = claimVotes[claimId][claim.insurers[i]];
152
153         if (vote.hasVoted) {
154             votes++;
155         }
156     }
157
158     return votes == claim.insurers.length;
159 }
160 }
```