

# 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: 8 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

---

<b>1 Versiebeheer</b>	<b>3</b>
<b>2 Voorwoord</b>	<b>4</b>
<b>3 Inleiding</b>	<b>5</b>
3.1 Motivatie . . . . .	5
3.2 Doel en onderzoeksvragen . . . . .	5
3.3 Limitaties . . . . .	6
3.4 Gerelateerd werk . . . . .	6
<b>4 Technische achtergrond</b>	<b>7</b>
4.1 Blockchain-technologie . . . . .	7
4.2 Overeenstemming algoritmes . . . . .	7
4.3 Smart contracts . . . . .	8
<b>5 Implementatie</b>	<b>9</b>
5.1 User stories en requirements . . . . .	10
<b>Bibliografie</b>	<b>11</b>
<b>6 Bijlagen</b>	<b>14</b>
<b>A test</b>	<b>15</b>

# HOOFDSTUK 1

## VERSIEBEHEER

---

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

## HOOFDSTUK 2

### VOORWOORD

---

TODO.

# HOOFDSTUK 3

## INLEIDING

---

### 3.1 Motivatie

Verzekeringsmaatschappijen zoals Allianz verzekeren panden voor miljoenen. Dit type verzekeringen worden in de praktijk gedeeld met meerdere verzekeraars, om zo het risico te verspreiden. Dit principe heet co-insurance en de verzekeringen worden in een bestaand systeem genaamd E-ABS 1 opgeslagen door de verschillende verzekeraars. Het probleem 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 het claimproces buiten E-ABS loopt waardoor een claim door de broker (makelaar) en de verschillende verzekeringsmaatschappijen met handmatige bedrijfsprocessen eerst gevalideerd moeten worden en gezamenlijk uitgekeerd. Het proces wordt momenteel 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.

### 3.2 Doel en onderzoeks vragen

Het doel van dit scriptie is om aan te tonen hoe blockchain technologie 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 verzekering gegevens. De resultaten van het onderzoek kan buiten de scope van dit onderzoek toegepast worden voor andere usecases. Het doel van het onderzoek kan worden opgesplitst in de volgende drie onderzoeks vragen:

- **Onderzoeks vrag 1: Uit welke use cases, requirements en concerns bestaat het huidige proces van Allianz?** Om deze vraag te beantwoorden, zal ook een literatuuronderzoek worden uitgevoerd. Verder zal er een onderzoek worden gedaan naar de bestaande frameworks en technologieën voor data-opslag (met en zonder de blockchain technologie). Het laatste deel zal worden gedaan door een vergelijking uit te voeren op de verschillende technologieën.
- **Onderzoeks vrag 2: Welke kansen & knelpunten bestaan bij het toepassen van de blockchain? -**
- **Onderzoeks vrag 3: Hoe automatiseer je het huidige proces met de blockchain? -**

### **3.3 Limitaties**

This PoC will strictly consist of the code necessary for the smart contracts, which define most of the operational logic and basic permissions management. Considering the time constraints of this thesis (approximately six months) and abundance of existing blockchains, no blockchain will be programmed. However, in Section 3.2.4 and in 2.2.3, there is a discussion of blockchains design considerations for the extension of the PoC. The thesis discusses cryptography used in blockchains and some additional encryption mechanisms are suggested for the PoC. These are however relying on existing technologies and implementations and are not part of the smart contracts code. One could also argue that other parties involved in the economics and regulation of health care such as insurance companies, the Ministry of public health or the medical products agency should be included. Although these types of users are not implemented with their specific requirements, in the PoC, they are considered and discussed in Section 5.2. Another highly relevant subject, important for the application of block-chain technology to handling of personal data such as in the medication plan, are legal considerations. Since this is a technical thesis, most legal requirements are not discussed but the ambition is that data privacy laws shall be honoured.

### **3.4 Gerelateerd werk**

Since the start of this thesis (August 2016), much related work has been done, advances in blockchain technology and large open source efforts in development have been made. (Zyskind et al., 2015), presents ENIGMA, a blockchain-based solution for secure multi-party computations. They suggest using blockchains for permissions management and for storing pointers to encrypted data, while the actual data is hosted by a trusted, blind escrow service. (Kosba, Miller, Shi, Wen, Papamanthou, 2015) lay the groundwork for a project called HAWK, a framework and compiler for writing privacy-preserving smart contracts. (Kish Topol, 2015) Propose in Nature Biotechnology, the use of blockchain technology for managing patient data but do not discuss a specific implementation or technical discussion. (Azaria, Ekblaw, Vieira, Lippman, 2016) design a modular system for storing electronic medical records on a blockchain, they suggest a Proof-of-Work system for incentivising the participation of doctors and hospitals in the system. Med-Vault (“Medical Records Project Wins Top Prize at Blockchain Hackathon,” 2015) were present in the media but have not published any details regarding their blockchain-EMR. To the best knowledge of the author, there have been no functional, electronic medical prescriptions based on blockchain technology built so far

# HOOFDSTUK 4

## TECHNISCHE ACHTERGROND

---

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.

### 4.1 Blockchain-technologie

De blockchain is een specifieke databasetechnologie die leidt tot een gedistribueerd autonoom grootboek-systeem (Kaptijn, B., Bergman, P., Gort, S. Whitepaper block-chain. ICTU, 2016). 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 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.

De technologie lost verschillende problemen op die voorkomen bij het gebruik van traditionele gecentraliseerde database technologieën die in handen zijn van een 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.

### 4.2 Overeenstemming algoritmes

Overeenstemming algoritmes zijn van het grootste belang voor blockchain-technologie, omdat het doel van Bitcoin was om waarde over te dragen in een niet-gereguleerde, wantrouwende omgeving, waar een zekere manier om transacties te valideren nodig was. Het doel van het consensusalgoritme is ervoor te zorgen dat er één historie van transacties bestaat en dat die geschiedenis geen ongeldige of tegenstrijdige transacties bevat. Bijvoorbeeld dat geen account probeert meer uit te geven dan het account bevat, of om hetzelfde token twee keer uit te geven, de zogenaamde double-spending. In tabel 2.2 worden verschillende belangrijke consensusalgoritmen met elkaar vergeleken. Hieronder wordt een korte introductie gegeven van een paar van hen, maar voor meer details wordt de lezer verwezen (Back, 1997), (Nakamoto, 2008), (Fischer, 1983), (Tendermint, 2017).

### **4.3 Smart contracts**

De naam 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 uit te besteden" juridische contracten met slimme contracten

# HOOFDSTUK 5

## 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.

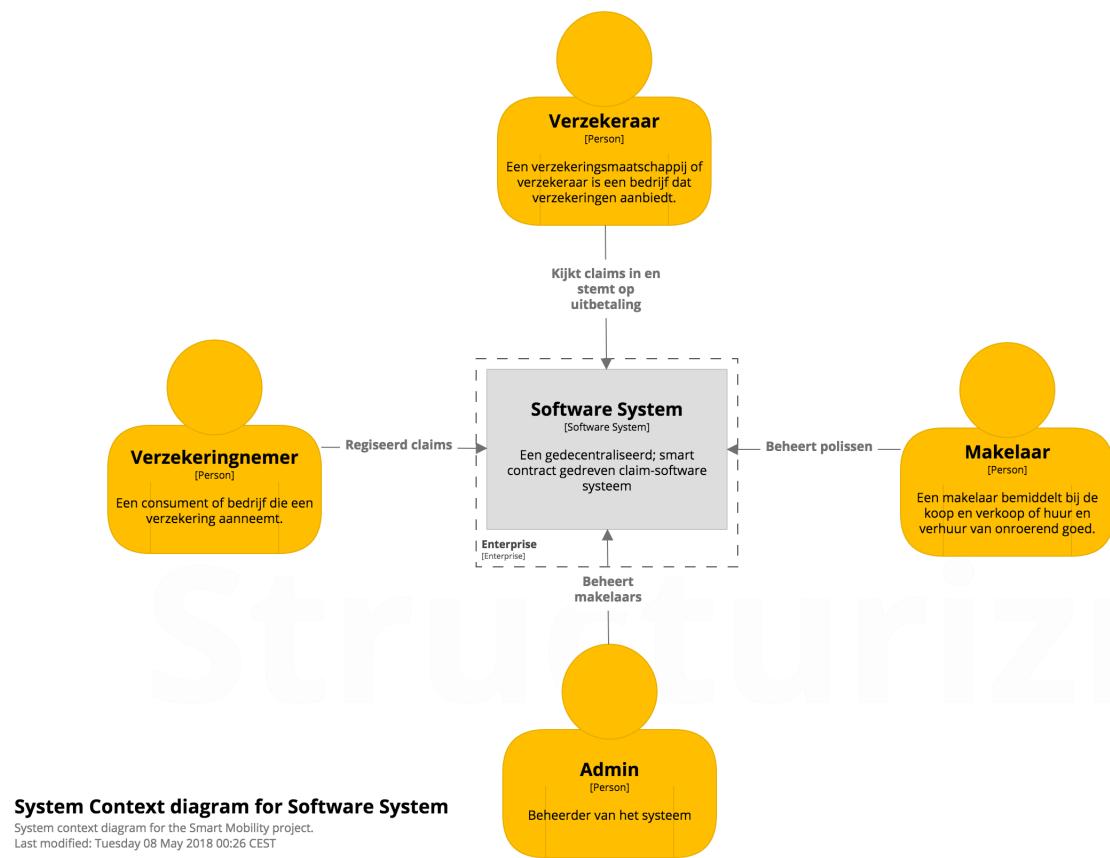
- quality attributes
- c4.

## 5.1 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 (TODO INSERT TABEL NAME) 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. while still keeping the PoC at a viable level of usability and security. (TODO MAKE IT DUTCH)

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



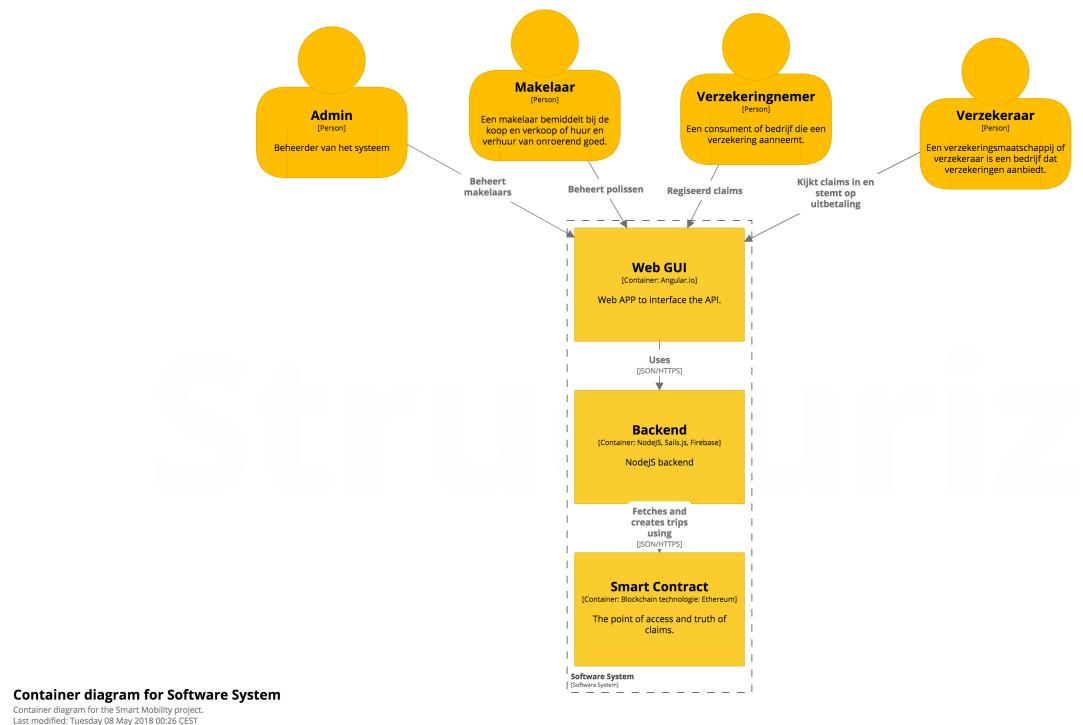
Figuur 5.2: C4 - Context.

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 5.2.

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 verzekeringmaatschappijen.

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



Figuur 5.3: C4 - Containers.

## BIBLIOGRAFIE

---

## HOOFDSTUK 6

### BIJLAGEN

---

# BIJLAGE A

TEST

---

cool