February 19, 2024

Joris Elfferich

Hogeschool rotterdam

Technische Informatica

Hoe beheren we de IHM digitaal in een veilige omgeving?

AfstudeerStage

Contents

[Inleiding 2](#_Toc162268741)

[Wat moet er precies opgeslagen worden? 2](#_Toc162268742)

[Hoe slaan we de IHM op? 3](#_Toc162268743)

[Database: 3](#_Toc162268744)

[Lokaal opslaan: 3](#_Toc162268745)

[Cloud opslaan: 3](#_Toc162268746)

[Github: 3](#_Toc162268747)

[Blockchain: 4](#_Toc162268748)

[Afweging 4](#_Toc162268749)

[Waar slaan we de IHM op? 5](#_Toc162268750)

[Blockchain: private, public of hybride 5](#_Toc162268751)

[Public: 5](#_Toc162268752)

[Private: 5](#_Toc162268753)

[Hybride: 5](#_Toc162268754)

[Conclusie: 5](#_Toc162268755)

[Hoe slaan we de IHM op in de blockchain? 6](#_Toc162268756)

[Hoe beheren we de IHM? 6](#_Toc162268757)

[Conclusie: 7](#_Toc162268758)

[Bronnen 8](#_Toc162268759)

[Changelog 8](#_Toc162268760)

# Inleiding

Door huidige onveiligheden in de Inventory of Hazardous Materials (IHM) gaat de IHM gedigitaliseerd worden. Dit zou het beheren van het IHM een stuk veiliger en overzichtelijker maken. Zo zou het onmogelijk worden om de IHM te vervalsen. We willen de IHM nu dus ergens veilig digitaal opslaan op een manier waar het goed toegankelijk is voor de stakeholders maar ook veilig. Ook moet er goed beheerd worden wie de juiste machtigen hebben. Er wordt onderzocht voor antwoorden op de volgende vragen:  
  
Wat moet er precies opgeslagen worden?  
Waar slaan we de IHM op?  
Hoe slaan we de IHM op?  
Hoe beheren we de IHM?

# Wat moet er precies opgeslagen worden?

De Inventory of Hazardous Materials[1] is een document dat een cruciaal onderdeel is van de maritieme industrie, met name in de context van scheepsrecycling. Het biedt een gedetailleerd overzicht van alle gevaarlijke materialen die aanwezig zijn op het schip. Dit is essentieel voor het waarborgen van veiligheid, milieubescherming en naleving van internationale regelgeving zoals de Hong Kong Conventie en de EU-regelgeving over scheepsrecycling [(Ren Di & Lougridis, 2021).](https://www.semanticscholar.org/paper/THE-INVENTORYING-OF-HAZARDOUS-MATERIALS%2C-RECYCLING-Di-Lougridis/db4cf87f5bb3dac577f72ca38e10abe7a97c006e)

Nauwkeurigheid in de IHM is van het grootste belang. Een incorrecte IHM kan leiden tot veiligheidsrisico's, milieuschade en niet-naleving van regelgeving, wat kostbaar of gevaarlijk kan zijn. Als bijvoorbeeld een gevaarlijk materiaal niet correct wordt geïdentificeerd en gedocumenteerd, kan het onjuist worden behandeld tijdens de scheepsrecycling, wat potentieel schadelijk kan zijn voor werknemers en het milieu.

Beveiliging van de IHM is dus erg belangrijk. Door de gevoeligheid van de informatie, is het cruciaal om ervoor te zorgen dat deze veilig wordt opgeslagen en alleen kan worden aangepast door geautoriseerd personeel. Ongeautoriseerde toegang tot of manipulatie van de IHM-gegevens kan leiden tot onjuiste behandeling van gevaarlijke materialen, met mogelijke veiligheids- en milieugevolgen.

De IHM is nu vaak een pdf-document van veel pagina’s lang met een bestands grootte van ongeveer 10MB.

# Hoe slaan we de IHM op?

Er zijn veel manieren op bestanden op te slaan, hier kijken we naar wat populaire opties en of deze bij de requirements past:

## Database:

Databases zijn de meest gebruikte manier om grote aantallen data op te slaan. Deze database kan zowel lokaal en in de cloud worden opgeslagen. In de cloud opslaan zorgt ervoor dat je overal bij de database kan. Handig maar dat betekent ook dat je kan worden aangevallen door cyberattacks. Lokaal opslaan op een (micro)computer zou veiliger kunnen zijn. Dan zou je echt de data alleen kunnen ophalen of aanpassen op het schip waarvan de IHM is. Dit is veilig maar onhandig voor de stakeholders. Voor zowel een cloud en lokale database zou je een database administrator nodig hebben die deze database beheert en beveiligd. Ook zullen er verschillende user accounts moeten worden gemaakt voor de verschillende autoriteiten die moeten kunnen valideren of aanpassen. De beveiliging bij de database beheerder leggen kan ook voor zwakheden in de beveiliging zorgen. De IHM is ook een document in hetzelfde formaat als een tekstdocument. Als je deze in een database wilt zetten zou je ook nog een nieuwe database moeten maken die lijkt op het oorspronkelijke document.

## Lokaal opslaan:

Vrijwel de meest simpele oplossing aan de software kant. Hier is het idee dat er op het schip een (micro) computer wordt geplaatst. Vervolgens met behulp van een speciaal programma of de ingebouwde OS-beveiliging wordt de IHM beveiligd met een wachtwoord of token (gekoppeld aan een speciale pas). Zo kan deze alleen worden aangepast door mensen met de juiste autorisatie. Deze oplossing is niet schaalbaar, niet superveilig en misschien wat onhandig. Hier zou het IHM een tekstdocument zijn wat makkelijk aan te passen is. Maar dat betekent dat alle aanpassingen gedaan moeten worden op het schip zelf. Dit kan onhandig zijn. In principe hoef je op het schip alleen het versiebeheer van de IHM te moeten kunnen zien. Aanpassingen aan het IHM zouden beter digitaal gemaakt kunnen worden via het internet.

## Cloud opslaan:

Deze optie is vrijwel hetzelfde als ‘lokaal opslaan’, maar dan op een cloud server zodat de IHM makkelijker toegankelijk is. Je kunt je een online filesharing platform voor je zien (zoals google drive of sharepoint) dat al vaak door bedrijven gebruikt wordt. Op dit platform kan je meerdere mensen toevoegen die verschillende rechten hebben. De veiligheid van deze oplossing is redelijk, je weet vrij zeker dat alleen de stakeholders bij de IHM kunnen. Wel is het moeilijk om de aanpassingen van de IHM te beheren. Je kan makkelijk zien wie het bestand aanpast en op welke datum, maar de juiste aanpassing terugvinden is vaak niet mogelijk. Ook lijkt het me moeilijk om dit te koppelen aan de module op het schip, aangezien een cloud platform vaak wordt beheerd door een bedrijf.

## Github:

Github is een online platform wat vooral gebruikt wordt door programmeurs om code met elkaar te delen en op te slaan. Het lijkt een beetje op een cloud file server, maar hierbij ligt de focus op versiebeheer en het overzien van veranderingen. Bij code is het erg belangrijk om terug te kunnen gaan naar vorige versies en het overzien van kleine veranderingen die de werking aanpassen. Voor het beheren van de IHM is GitHub dus best een prima oplossing. Als de IHM zou moeten worden aangepast kan dat gemakkelijk via GitHub. Vervolgens voordat deze versie definitief wordt opgeslagen kunnen de andere stakeholders de ‘push’ verifiëren. Zo kan je dus ook op GitHub de verschillende stakeholder de juiste rechten geven. Als nadeel is GitHub niet zo gebruikersvriendelijk, en kan het moeilijk zijn om te leren gebruiken.

## Blockchain:

Blockchain biedt een gedecentraliseerd en transparant register waarin alle wijzigingen traceerbaar en onveranderlijk zijn[2,3]. Dit zorgt voor betrouwbaarheid en integriteit van de gegevens. Elke wijziging moet worden gevalideerd door meerdere partijen, waardoor frauduleuze manipulatie wordt voorkomen. Elke versie van het IHM kun je zien als een block, die wordt toegevoegd aan de chain. Eenmaal in de chain is het mogelijk om dit bestand te downloaden, maar niet meer om deze aan te passen. Een hash is een vingerafruk van een document, een unieke code voor de data van het document. Als er een aanpassing aan het document wordt gemaakt wordt deze hash volledig anders. Deze hashes van de documenten wordt opgeslagen in de blockchain. Zo is het onmogelijk om data te vervalsen en nog steeds een normale chain te hebben. De chain zal gelijk kunnen aangeven dat een van de hashes niet meer overeenkomt. Deze systeemarchitectuur is erg veilig en maakt het bijna onmogelijk om de IHM te frauderen. De blockchain zal je een opeenvolgend record krijgen van alle aanpassingen van het document, wat erg goed is voor valideren en verifiëren van wijzigingen.

## Afweging

Uit deze opties zijn blockchain en GitHub wel degelijk goede oplossingen. Github heeft een erg goede versie beheer, je kan makkelijk met de andere stakeholders samenwerken en kan altijd bereikt worden via het internet want Github heeft hun eigen servers (die niet altijd immuun zijn voor data breaches). Blockchain wordt vooral gebruikt voor sensitieve informatie, en deze informatie is dan ook onverandelijk als het eenmaal in de blockchain staat. De informatie in de blockchain is vaak erg transparant en daardoor zijn veranderingen goed traceerbaar.  
  
Uiteindelijk is Github goed voor robuust versiebeheer, gezamenlijk bewerken en gemakkelijke toegang. Terwijl blockchain goed is voor gegevensintegriteit, onveranderlijkheid en transparantie voor naleving van de regelgeving. Voor de use case is blockchain wat passender hoewel github een redelijk alternatief is.

# 

# Waar slaan we de IHM op?

Er zijn een paar verschillende types blockchain netwerken. Welk netwerk past het beste bij onze vereisten?

## Blockchain: private, public of hybride

Public:  
In dit netwerk kan iedereen meedoen met het netwerk. Binnen dit netwerk kan iedereen lezen, schrijven en valideren. Bij publieke blockchains, zoals Bitcoin en Ethereum, zijn alle transacties volledig transparant. Dit draagt bij aan de traceerbaarheid en verifieerbaarheid van transacties. Dit maakt het netwerk erg gedecentraliseerd. Binnen een public netwerk willen nieuwe deelnemers meedoen om het te gebruiken binnen hun eigen doeleinden. Hoe meer mensen er deelnemen des te veiliger het is. Blockchain werkt namelijk peer to peer, en hoe meer peers er zijn, hoe veiliger het is. Deelnemers krijgen ook een prijs voor elke validatie ze maken voor andere mensen binnen het netwerk. De prijs die deelnemers krijgen, vaak 'mining reward' genoemd, om mensen te stimuleren voor het onderhouden van de netwerkintegriteit Bij dit valideren komen wel gegevens vrij zoals de inhoud en de adressen, hierdoor kan je anonimiteit verliezen.[4]

### Private:

Deelnemers kunnen alleen deelnemen aan dit netwerk door een uitnodiging, zodat de identiteit van alle deelnemers vast is gesteld. Private blockchains worden vaak gebruikt in bedrijfsomgevingen waar controle over de deelnemers en activiteiten essentieel is. Binnen dit netwerk wordt er gecontroleerd wie mag valideren (minen) en wie meedoet aan de consensus protocollen. Hoewel private blockchains minder gedecentraliseerd zijn, kunnen ze aanzienlijk efficiënter zijn in transactiesnelheid en energieverbruik. Je kan het meer zien als een gesloten database beveilidg met crypto grafische sleutels. Alleen mensen met toestemming in dit netwerk mogen aanpassingen maken en gegevens valideren. Private blockchains geven dus prioriteit aan efficiëntie en onveranderlijkheid. Maar omdat er minder mensen toegang hebben zijn er dus minder validaties wat het netwerk onveiliger maakt met betrekking tot datalekken. Ook is er misschien geen sprake van consensus, maar alleen van de onveranderlijkheid van de ingevoerde gegevens. [4]

Hybride:  
Dit blockchain netwerk is een mix tussen private and public. Iedereen kan deelnemen nadat de identiteit is geverifieerd. Zo krijgen de deelnemers alleen permissies om specifieke activiteiten uit te voeren (lezen, schrijven of invoeren). Hybride blockchains kunnen dus meerdere functies hebben, en wordt vaak gemaakt en verhuurd aan bedrijven die de voordelen van zowel publieke als private netwerken willen benutten, zoals transparantie en controle over bepaalde aspecten van de blockchain. De beveiligingsaspecten van hybride blockchains hangen af van de specifieke architectuur en implementatie. Maar ze zijn over het algemeen veiliger dan publieke netwerken, hoewel het risico op hacking is nog steeds aanwezig, net als bij alle onlinesystemen. [4]

Conclusie:  
Voor onze use-case is het beste om hybride of private blockchain te gebruiken. Een hybride netwerk is meer gedecentraliseerd en maakt het makkelijker om mensen toe te laten tot dit netwerk voor validaties, maar dit zorgt voor een complexere blockchain wat moeilijk valt te integreren. Terwijl de private blockchain efficiënter is met snellere transactie snelheden en lagere kosten. Ook is sensitieve informatie beter beschermd. Alleen is de prive blockchain wel meer gecentraliseerd, wat een minder robuuste systeemarchitectuur is. En hoewel het netwerk schaalbaar is, is deze niet even goed schaalbaar als de hybride of public blockchain. Toch zal voor deze use-case een prive netwerk sneller en makkelijker zijn om te ontwikkelen, en biedt de juiste vereiste voor de opdracht omschrijving.

# Hoe slaan we de IHM op in de blockchain?

De IHM is een vrij groot bestand, hoe slaan we deze op?

De veiligste manier is om een bestand volledig op te slaan in de blockchain. Dit betekent de data van het bestand wordt in de blockchain gezet. Om het bestand te bekijken moet je dan het bestand opnieuw maken met de data uit de blockchain en zo kan je het bestand bekijken. Op deze manier is het bijna onmogelijk om de IHM te aanpassen en frauderen. Wat een simpelere oplossing is om de data van het bestand in te lezen, en deze te hashen en alleen deze hash in het systeem opslaan. Vervolgens sla het u geüploade bestand op in een veilige plaats op de server. Het bestand kan zo makkelijk gedownload worden maar als je het bestand aanpast ziet de blockchain gelijk dat de hashes niet meer overeenkomen. Deze manier is iets simpeler en maakt het nog steeds niet mogelijk om de IHM te frauderen zonder dat dit wordt gezien door de blockchain. Wat wel belangrijk is dat als er gefraudeerd zou worden de data verloren raakt. Terwijl als de data is opgeslagen in de blockchain deze nog kan worden gebruikt als backup. De data opslaan in de blockchain is het veiligste maar zorgt wel voor latency bij het uploaden van bestanden aangezien er een hash moet worden gemaakt wat ook door het hele bestand gaat. Als je dit combineert met een PoW (zie volgend hoofdstuk) kan je wat vertraging hebben (5+ seconden). Aangezien snelheid niet van het uiterste belang is, is het veiliger om de volledige data van het bestand in een block te zetten. Alhoewel de kans vrij klein is dat er in het server gehackt wordt om een aanpassing te maken aan de IHM is het toch goed om een extra maatregel te nemen.

# Hoe beheren we de IHM?

Om de IHM te beheren moeten meerdere stakeholders samenwerken voor aanpassingen aan de IHM. Een consensus mechanisme is een programma dat wordt gebruikt om een overeenstemming te krijgen over de huidige blockchain. In de bitcoin-blockchain wordt er een PoW(Proof of Work) consensus gebruikt [6]. Voordat een block definitief wordt toegevoegd aan de blockchain moet deze eerst geverifieerd worden. Deelnemers krijgen een beloning voor het oplossen van een hash, en zo zullen er vaak meerdere personen bezig zijn met het ontcijferen (minen) van deze hash. Als deze eenmaal is opgelost krijgt deze persoon de prijs en is het block klaar om in de blockchain gezet te worden. De andere personen die bezig waren met het minen, verifiëren dat de informatie klopt en bereiken ze zo dus een consensus. Voor onze use case is dit niet nodig want wij willen een private blockchain netwerk gebruiken. Ook moet er menselijk worden bepaald of de informatie die in de blockchain wordt gezet correct is. Dus wanneer een block wordt toegevoegd aan de chain zal deze eerst in behandeling zijn. De desbetreffende stakeholders zullen een notificatie krijgen. Ze zullen de informatie binnen dit block moeten goedkeuren. Als de informatie volgends alle stakeholders correct is en dus goedgekeurd zal het block definitief gechained worden aan het vorige block. Als een van de stakeholders dit niet goedkeurt zal het block niet worden gechained en moet er overlegd worden over het informatieprobleem. Zo moet binnen het blockchain netwerk een rollensysteem worden gemaakt. Waar verschillende accounts andere rechten hebben(Admin, Alleen lezen, Alleen valideren, Alleen Uploaden). Onze consensus is dus menselijk, maar we kunnen wel het idee lenen van de PoW om ons systeem extra veilig te maken. Zo kunnen we de stakeholders een block laten minen als deze wordt goedgekeurd door de stakeholders. Hier gebruiken we een extra getal in de blockchain om iteratief de hash opnieuw uit te rekenen tot een doel is bereikt. Zo kunnen we binnen het systeem alleen hashes accepteren die beginnen met x aantal nullen. Dit maakt de systeem architectuur nog veiliger.

# Conclusie:

In dit onderzoek is er gekeken naar de IHM, een document dat een gedetailleerd overzicht van alle gevaarlijke materialen die aanwezig zijn op het schip bevat. Door de gevoeligheid van de informatie, is het cruciaal om ervoor te zorgen dat dit document veilig wordt opgeslagen en alleen kan worden aangepast door geautoriseerd personeel. Ongeautoriseerde toegang tot of manipulatie van de IHM-gegevens kan leiden tot onjuiste behandeling van gevaarlijke materialen, met mogelijke veiligheids- en milieugevolgen.   
  
Er is naar meerdere digitaliseringen oplossingen gekeken zoals het gebruik van een database, cloud server, github en blockchain. De oplossing die het beste bij de opgestelde eisen zat was het gebruiken van blockchain. Aangezien blockchain goed is voor gegevensintegriteit, onveranderlijkheid en transparantie voor naleving van de regelgeving. Nu kan een blockchain netwerk op verschillende manieren werken, public, private of een mix. De private blockchain blijkt hieruit efficiënter met snellere transactie snelheden en lagere kosten. Ook is sensitieve informatie hier beter beschermd.   
  
Maar hoe werkt dit private blockchain netwerk precies? De data van het IHM zal direct worden opgeslagen in een block, zodat het onmogelijk is om de data van het bestand aan te passen. Dit zal wat langer duren maar valt binnen de requirements.  
  
Ten slot is er gekeken naar een consensus mechanisme en hoe dat eruit zou zien binnen dit blockchain netwerk. Bovenop het blockchain server moet een interface gemaakt worden waar de stakeholders verschillende accounts krijgen met de desbetreffende rechten (uploaden, verifiëren en valideren). Bij het goedkeuren van een block zal dit ook gemined worden zodat de hash moeilijker is en voldoet aan de vooropgestelde eisen van het systeem.

# Bronnen

[1] Official Journal of the European Union, “Regulation (EU) no 1257/2013 of the European Parliament” <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:330:0001:0020:EN:PDF>

[2] Z. Church, “Blockchain, explained,” MIT Sloan, <https://mitsloan.mit.edu/ideas-made-to-matter/blockchain-explained>

[3] A. Hayes, “Blockchain facts: What is it, how it works, and how it can be used,” Investopedia, <https://www.investopedia.com/terms/b/blockchain.asp>

[4] S. Seth, “Public, private, permissioned blockchains compared,” Investopedia, <https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/>

[5] J. Lintzer, “Storing documents on the blockchain: What, why and how?,” jSign, <https://www.jsign.com/blog/storing-documents-with-blockchain>

[6] J. Frankenfield, “What are consensus mechanisms in Blockchain and cryptocurrency?,” Investopedia, <https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp>

# Changelog

|  |  |  |
| --- | --- | --- |
| Versie | Verandering | Datum |
| 0.1 | Opzet gemaakt | 06/02/24 |
| 0.2 | Opties geschreven | 12/02/24 |
| 0.3 | Blockchain, private, public af | 14/02/24 |
| 0.4 | Hoe slaan we blockchain op | 15/02/24 |
| 0.5 | Hoe beheren we de blockchain | 16/02/24 |
| 1.0 | Conclusie en bronnen klaar | 20/02/24 |