Veiligheid van data op de blockchain technologie en het gebruik van smart contracts

Onderzoeksvoorstel Bachelorproef

Wouter Van Hecke[1]

Samenvatting
Dit onderzoek gaat over de blockchain technologie en een concept dat de blockchain technologie met zich meebrengt: ”smart contracts”. Dit is een concept dat onze manier van omgaan met huidige contracten helemaal kan veranderen. Er zit veel potentieel in (de) blockchain technologie/smart contracts en is daarom ook belangrijk dat dit verder onderzocht wordt, zowel voor jonge programmeurs die zich verder willen verdiepen in smart contracts en voor geavanceerde programmeurs die de huidige problemen verder willen behandelen. In deze bachelorproef wordt onderzocht hoe de blockchain technologie zijn data beveiligd en hoe deze technologie kan toegepast worden in supply chain en voting systems. Het doel van deze bachelorproef is aan te tonen waarom een blockchain heel veilig is en hoe het in de praktijk gebruikt kan worden.

Sleutelwoorden
Onderzoeksdomein. Blockchain — Smart Contracts — Ethereum

Contact: [1] wouter.vanhecke.w9895@student.hogent.be

Inhoudsopgave

1. Introductie

Technologie blijft steeds evolueren. De blockchain technologie is daar een belangrijk voorbeeld van. Deze nieuwe technologie begint meer en meer bekend te worden, kijk maar naar de stijging in waarde van bitcoin het afgelopen jaar. Maar de blockchain technologie is zoveel meer dan alleen maar bitcoin en andere cryptocurrencies. Omdat een blockchain een gedecentraliseerd systeem is, is het van hoog belang om ervoor te zorgen dat data zo beveiligd mogelijk is om de integriteit van het systeem te behouden. Een ander concept dat blockchain met zich mee brengt zijn de ”smart contracts”. Een smart contract is een zelf uitvoerbaar script dat opgeslagen wordt op de blockchain. Hiermee kan je bijvoorbeeld programmeren dat persoon A op een bepaald tijdstip persoon B zal betalen, dit zal op dat exacte tijdstip dan automatisch uitgevoerd worden dankzij het smart contract. Omdat dit nog een relatief nieuwe technologie is, bestaat er nog veel verwarring rond dit concept. Daarom is het belangrijk dat deze technologie verder onderzocht wordt. Het doel van deze bachelorproef is aan te tonen waarom een blockchain heel veilig is en hoe het in de praktijk gebruikt kan worden. De hoofdvraag van deze bachelorproef wordt dus:

Hoe wordt data op de blockchain beveiligd?
Omdat de blockchain technologie een gedecentraliseerde technologie is, kan iedereen het netwerk binnentreden, ongeacht de intentie van de persoon. Daarom is het heel belangrijk dat alle data op de blockchain goed beveiligd wordt. Bij deze vraag wordt er onderzocht hoe de blockchain zijn data precies beveiligd en alleen maar de correcte informatie vrijgeeft aan de huidige eigenaar.

Andere onderzoeksvragen bestaan uit:
Hoe wordt de blockchain technologie gebruikt voor supply chain? De blockchain technologie vindt bij meer en meer industrieën een thuis. Bij deze vraagt wordt er onderzocht hoe de blockchain technologie een thuis heeft gekregen bij supply chain.

Hoe kan de blockchain technologie gebruikt worden als een voting system? Omdat elke gebruiker op de blockchain anoniem is, maar er tegelijkertijd ook geen kennis is over de betrouwbaarheid van de gebruiker, wordt er onderzocht hoe de blockchain toch gebruikt kan worden als een voting system en waarom dit toch een velige keuze kan zijn.

NEO en Ethereum zijn allebei platformen dat smart contracts ondersteunen, maar hoe verschillen ze van elkaar?

Stel nu dat je een applicatie wil schrijven dat gebruik maakt van smart contracts en nu moet je kiezen op welke blockchain technologie je deze applicatie wil maken. In dit deel wordt er onderzocht wat de verschillen zijn tussen de blockchain platformen 'NEO' en 'Ethereum'.

2. State-of-the-art

Er zijn al meerdere artikels en thesissen geschreven over smart contracts. Artikels hebben het vaak over wat een smart conctract nu eigenlijk is, terwijl andere bachelorproeven of thesissen al snel meer gedetailleerd ingaan op een specifieke toepassing met smart contracts.

2.1 A gentle introduction

Het eerste artikel (antonylewis2015, 2016) geeft een kort, maar krachtige introductie over smart contracts. Het geeft een paar basis definities, samen met een paar praktische voorbeelden in verband met banken. Het geeft uitleg over wat een smart contract doet en hoe je het kan gebruiken. Ook vertelt de auteur over zijn visie van de toekomst voor smart contracts.

2.2 Impossible use cases

Het tweede artikel, geschreven door Greenspan (2016), vertelt meer over wat niet mogelijk is met smart contracts op dit moment. Het haalt drie use cases naar boven waar mensen veel over spreken en die op dit moment nog niet mogelijk zijn. Hij geeft een duidelijk, praktisch voorbeeld en bespreekt hoe je dit probleem kan omzeilen.

2.3 Smart contracts in de pharmacy wereld

In deze thesis, geschreven door Bergquist (2017), wordt het probleem met apothekers aangehaald. De auteur spreekt over hoe patiënten soms verkeerde medicatie voorgeschreven krijgen en daardoor nog zieker kunnen worden. Dit ligt in de handen van de dokter die de examinatie heeft afgelegd en hoe al het vertrouwen bij de dokter ligt. De dokter schrijft de medicatie op een prescriptie en zet hier een stempel op als validatie. De auteur heeft geprobeerd om dit om te zetten naar een smart contract dat werk met privacy en validatie.

3. Methodologie

De vragen zullen beantwoord worden aan de hand van literatuurstudies. Er zal onderzocht worden hoe de blockchain technologie zijn data beveiligd en hoe smart contract aspecten kunnen helpen zoals supply chain, voting, kostefficiëntie...

4. Verwachte resultaten

Hoe wordt data op de blockchain beveiligd? Voor deze onderzoeksvraag wordt verwacht dat de data op een blockchain zeer goed beveiligd wordt dankzij encryptie. Het vervalsen van gegevens zal onmogelijk zijn voor mensen met valse intenties omdat de blockchain technologie werkt met een gedecentraliseerd systeem waar je alleen maar gegevens aan kan toevoegen en niet verwijderen/aanpassen.

Hoe wordt de blockchain technologie gebruikt voor supply chain? Voor deze onderzoeksvraag wordt verwacht dat producten succesvol op de blockchain kunnen worden opgeslaan en zorgt voor authenticiteit van producten.

Hoe kan de blockchain technologie gebruikt worden als een voting system? Omdat de blockchain technologie zorgt voor een systeem waar annonimiteit en vertrouwloos vertrouwen topprioriteiten zijn, kan een blockchain technologie als een voting system gebruikt worden. Omdat een blockchain werkt met hash values en een gelinkte list waar constant de hash value van de vorige block wordt opgeslagen, kan vervalsing niet voorkomen, omdat de hash values dan niet meer overeenkomen.

NEO en Ethereum zijn allebei platformen dat smart contracts ondersteunen, maar hoe verschillen ze van elkaar? Om deze vraag te beantwoorden zullen de twee platformen naast elkaar gelegd worden en vergeleken worden op aspecten zoals kosten, transactievermogen, snelheid, gebruikte programmeertaal, toegankelijkheid.

5. Verwachte conclusies

Uit de onderzoeken zal blijken dat er nog veel groeipotentieel is voor blockchain technologieën. Smart contracts zullen in de toekomst als standaard gebruikt worden voor contracten omdat er veel minder logische fouten gemaakt kunnen worden tijdens het uitvoeren van het contract. Blockchain technologie kan opgenomen worden binnen zowel kleine als grote bedrijven. Door het gebruik van blockchain te standaardiseren zal er veel geld bespaard worden op vlak van onkosten / het betalen van derde partijen, omdat hun werk nu geautomatiseerd kan worden.

Referenties

antonylewis2015. (2016). A gentle introduction to smart contracts. Verkregen van https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/

Bergquist, J. H. (2017). *Blockchain Technology and Smart Contracts* (masterscriptie, Uppsala University).

BlockGeeks. (2016). Smart Contracts: The Blockchain Technology That Will Replace Lawyers. Verkregen van https://blockgeeks.com/guides/smart-contracts/

Bokhorst, J. (2016). Smart contracts binnen de blockchain: contracteren 2.0? Verkregen van https://www.ordina.nl/nl-nl/blogs/2016/oktober/smart-contracts-binnen-de-blockchain-contracteren-20/

Greenspan, G. (2016). Why Many Smart Contract Use Cases Are Simply Impossible. Verkregen van https://www.coindesk.com/three-smart-contract-misconceptions/

Hertig, A. (Unknown). How Do Ethereum Smart Contracts Work? Verkregen van https://www.coindesk.com/information/ethereum-smart-contracts-work/