Het verbeteren van de privacy en security in de vierde industriële revolutie door middel van het integreren van blockchain: onderzoek en proof-of-concept

Onderzoeksvoorstel Bachelorproef 2020-2021

Florian Landuyt[1]

Samenvatting

Na de grote veranderingen door de opkomst van de machines op het einde van de 18de eeuw, het intreden van elektriciteit in 1870 en na de adoptie van elektronica in de tweede helft van de 20ste eeuw, zijn we in de vierde industriële revolutie aanbeland. Cyber-fysieke systemen vormen de basis van deze beweging, waar Internet of Things (IoT) een grote rol in speelt. In dit werk start ik met het bespreken van de verschillende uitdagingen die de vierde industriële revolutie met zich meebrengt. Twee van de grootste uitdagingen waarmee Industry 4.0 te kampen heeft, blijken security en privacy te zijn. Een eventuele oplossing voor dit probleem is het integreren van een blockchain. Deze technologie is oorpronkelijk ontworpen voor het gebruik van cryptocurrencies, maar wordt de dag van vandaag overgenomen in heel wat andere projecten. In mijn onderzoek worden de voor- en nadelen van deze methodiek tegenover elkaar gezet. Hierna voer ik een grondig onderzoek uit naar welk soort implementatie van blockchain hier het meest voor geschikt zal zijn. Na het bekomen van een resultaat uit de voorgaande analyse ga ik aan de slag met het creëren van een proof of concept (PoC). In deze PoC zal ik meerdere IoT devices aansluiten op het meest geschikte blockchain ontwerp en aantonen dat de privacy en security beduidend beter is. Op deze manier kan geschetst worden waarom het een slimme zet zou zijn om dit te implementeren op grote schaal. Hierbij wordt verwacht dat de blockchain basis voor een IoT netwerk de security en privacy zal verbeteren.

Sleutelwoorden

Onderzoeksdomein. Blockchain — Industry 4.0 — Internet of Things — IoT — Privacy — Security — Ethereum — Smart contracts

Contact: [1] florian.landuyt.y2414@student.hogent.be;

Inhoudsopgave

1. Introductie

Internet of Things (IoT) bevindt zich overal in het dagelijks leven. In de keuken, rond onze pols, in ziekenhuizen, auto's, op straat, en ga zo maar door.

IoT stelt een netwerk voor waar "things" (koelkasten, auto's, koffiezetapparaten) of apparaten geïntegreerd met kleine sensoren en/of actuoren onderling verbonden zijn met elkaar door een publiek of privaat netwerk. De devices in IoT worden vanop een afstand bestuurd, om zo de gewenste functionalteit uit te voeren. De connectie tussen de verschillende apparaten is een van de centrale pijlers in de vierde industriële revolutie. IoT vormt samen met Cloud computing, Augmented Reality (AR), Big data, Autonome robots, Artificiële Intelligentie (AI), Machine Learning (ML) en nog veel andere technologieën/concepten deze revolutie. Het grote verschil tussen de klassieke manier bij het verbinden en beheren van IoT devices en bij Industry 4.0 is dat er geen tussenpersoon meer bestaat. Je apparaat kan gegevens opslaan, die gegevens analyseren en een beslissing nemen over deze data zonder inbreng van "a human in the loop". Aangezien veel toestellen het gsm-nummer, thuisadres of e-mailadres van hun eigenaar kunnen bevatten, is het vinden van een veilige manier om je toestellen te verbinden met elkaar van reusachtig belang.

In het onderzoek naar het nut van de integratie van blockchain ter verbetering van security en privacy binnen een netwerk van IoT devices, ga ik op zoek naar antwoorden op volgende deelvragen:

- Wat zijn de maatregelen en protocollen die op dit moment gelden voor het verbeteren van de security en privacy bij Industry 4.0?

- Wat zijn huidige valkuilen bij een groot IoT netwerk?
- Wat zijn de voor- en nadelen van het implementeren van blockchain als oplossing voor privacy- en securityproblemen?
- Bij welke toestellen kan blockchain geïmplementeerd worden, indien het een meerwaarde blijkt te bieden?
- Zijn de huidige apparaten en netwerken in staat om geïntegreerd te worden in een blockchain?

2. State-of-the-art

2.1 Industry 4.0

De grote digitale veranderingen in het laatste decennium hebben ervoor gezorgd dat veel experten er vanuit gaan dat Industry 4.0 van start is gegaan. Om deze revolutie volledig te kunnen vatten is het belangrijk om het geheel te zien als een "value-chain". Deze "value-chain" beschikt over de leveranciers (en oorsprong) van het materiaal en componenten die gebruikt worden voor "smart-manufactering", de digitale end-to-end 'supply-chain' en de eindgebruiker. Dit concept wordt onderbouwd door verschillende pijlers: Cloud Computing, Big data, Augmented Reality (AR), Simulation Internet of Things (IoT) en nog vele anderen.

2.2 Internet of Things

Het aantal apparaten verbonden met het internet blijft stijgen. Per seconde worden 127 nieuwe toestellen aangesloten op het internet en tegen 2025 wordt er geschat dat er 75 miljard toestellen verbonden zullen zijn met het internet. Aangezien veel IoT fabrikanten toestellen blijven leveren waar er software- en hardwarefouten in verscholen zitten, blijven IoT apparaten één van de grootste krachten die schuilt achter distributed denial of service (DDoS) aanvallen (Džaferović, Sokol, Almisreb & Mohd Norzeli, 2019). Het aantal DDoS aanvallen blijft gestaag stijgen. Dit door ongeschikte wachtwoorden, de onmogelijkheid om firmware te herstellen en hiaten in de authenticatie en het data transfer ecosysteem. De security en privacy van gebruikers komt met andere woorden in gedrang door verouderde hardware en software, moeilijkheden bij het ontdekken wanneer een toestel is getroffen en problemen bij gecentraliseerde organisaties waarbij de data op één enkele plaats wordt opgeslagen. Meerdere onderzoekers hebben de problemen die te maken hebben met privacy en security bij IoT systemen al eens onderzocht. Zo worden in „IoT Privacy and Security: Challenges and Solutions" (Tawalbeh, Muheidat, Tawalbeh & Quwaider, 2020) reeds verschillende oplossingen aangekaart voor de verschillende uitdagingen die IoT met zich meebrengt. Eén van de oplossingen in dit laatste onderzoek bestaat uit het het gebruiken van een Proposed Layered Cloud-Edge-IoT model. Hier gaan ze mee aan de slag met andere mogelijkheden die het privacy probleem zouden kunnen oplossen. De bestaande onderzoeken rond dit onderwerp zullen mijn werk een stuk vlotter laten lopen.

2.3 Blockchain

Voor het jaar 2008 werd er in de volksmond nog niet gepraat over blockchain, maar daar bracht Satoshi Nakomoto verandering in door zijn whitepaper „Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2008) te publiceren waarin hij Bitcoin aan de wereld voorstelt. In deze paper werd niet enkel de wereldbekende cryptocurrency verduidelijkt, maar werd ook het concept blockchain gepresenteerd. Deze technologie werd ontworpen voor het oplossen van het "double-spend" probleem bij het betalen met een digitale munteenheid. Het "double spend" probleem is het risico dat eenzelfde munt van een bepaalde digitale currency meerdere malen kan gespendeerd worden. Blockchain pakt dit probleem aan met het ontwerp van een publieke digitale ledger waarin elke ooit uitgevoerde transactie wordt opgenomen. Om een transactie op te slaan op de blockchain, worden verschillende transacties gegroepeerd in een blok, die aan elkaar gelinkt worden door elke blok te voorzien van een timestamp en een cryptografische hashfunctie die gemaakt wordt van de informatie dat zich bevindt in de vorige blok. Deze hashfunctie creëert een onveranderlijke ketting aan data doordat elke aanpassing in een willekeurige blok wordt doorgevoerd doorheen de volledige ketting.

Al snel werden de eerste tekortkomingen van het bitcoin blockchain-ontwerp weggewerkt door een nieuw concept, Ethereum. In 2014 slaagde Vitalik Buterin er in om de toenmalige blockchain koploper van zijn troon te stoten door blokchain te voorzien van smart contracts. In „A next generation smart contract and decentralized application platform" (Buterin, 2014) werd er duidelijk gemaakt dat door het gebruik van smart contracts, uitvoerbare code opgeslagen op een blockchain, het concept blockchain bruikbaar wordt voor applicaties en concepten die zich buiten de cryptocurrency atmosfeer bevinden.

Het aantal bedrijven die het gebruik van blockchain verwelkomen in hun onderneming, blijft jaar na jaar gestaag stijgen. Ook bij het vinden van een oplossing voor slecht beveiligde netwerken zijn al verschillende technieken onderzocht. In het onderzoek „Using Ethereum Blockchain in Internet of Things: A Solution for Electric Vehicle Battery Refueling" (H. Sun e.a., 2018) wordt er een oplossing voor privacy en security gegeven door middel van het implementeren van een Ethereum blockchain.

Er is reeds enorm veel onderzoek gedaan naar de technische barrières, voor- en nadelen, en mogelijkheden van een blockchain integratie met IoT. De afwezigheid van klassieke databank methodes en software technieken maakt het enorm moeilijk om grote datasets te verwerken. Een andere challenge waar ik in dit onderzoek te maken mee zal krijgen is de mogelijkheid om componenten met elkaar te laten samenwerken op een zo efficiënt mogelijke manier. Zoals in „Technical aspects of blockchain and IoT" (Atlam & Wills, 2019) aangekaart, zijn er tot op het heden nog enorm veel problemen mee.

Het opzetten van de PoC zal geholpen worden door het onderzoek „Using Ethereum Blockchain in Internet of Things: A Solution for ElectricVehicle Battery Refueling" (H. Sun & Sun, 2018). In dit onderzoek stellen de schijvers een Ethereum blockchain voor bij het ontwikkelen van een mechanisme voor het herladen van de batterij van een elektrische auto. Aangezien ik op dit moment opteer voor een Ethereum blockchain in mijn PoC, kan ik zorgen dat het opzetten van het project op een gelijklopende manier verloopt.

De oplossingen die „Blockchain for the IoT: Privacy-Preserving Protection of Sensor Data" (Chanson, Bogner, Bilgeri, Fleisch & Wortmann, 2019) en „Towards decentralized IoT security enhancement: A blockchain approach" (Qian e.a., 2018) bieden voor de privacy en security van blockchain integratie bij een IoT netwerk, zullen mij zeker op weg zetten bij het beantwoorden van mijn onderzoeksvragen.

Samen met een peer-to-peer connectie, asymetrisch encrypteren van de data, proof-of-work (PoW) consensus, een digitale handtekening en smart contracts, kan blockchain er voor zorgen dat verschillende oorzaken van eerder aangekaartte problemen worden weggewerkt.

3. Methodologie

Dit werk start ik met een diepgaand literatuuronderzoek waarbij ik de verschillende problemen definieer waarmee het huidig netwerk aan IoT apparaten kampt. Hierbij breng ik de verschillende protocollen in kaart waar IoT-apparaten leveranciers de dag van vandaag rekening mee houden en toon ik aan op welke manier er rekening gehouden wordt met de veiligheid en privacy van gebruikersgegevens. Als volgt ga ik verschillende mogelijkheden nagaan waarbij het probleem rond privacy en security kan verbeterd worden. Ik verwacht een drietal mogelijkheden te vinden, waarna ik dieper op de blockchain methode zal ingaan. Vervolgens zal ik een vergelijkende studie voeren tussen de verschillende soorten implementatie van blockchain. Naast de besproken Ethereum, bestaat ook nog de Bitcoin implementatie, de Multichain methode, OpenChain blockchain en nog vele andere. De meest voor de hand liggende blockchain zal ik verder onderzoeken. Hierbij definieer ik de voor- en nadelen van het kiezen van deze blockchain.

Tot slot zal ik aan de slag gaan met een proof-of-concept door het implementeren van de ethereum blockchain waarbij ik meerdere raspberry pi's en smart devices op hetzelfde netwerk zal aansluiten.

4. Verwachte resultaten

Ik verwacht dat mijn onderzoek zal aantonen dat het gebruik van ethereum blockchain een duidelijke verbetering toont op het vlak van veiligheid en privacy. Door de vele artikels die ik reeds heb gevonden, ga ik ervan uit dat ik geen problemen zal ondervinden bij het vergaren van informatie rond dit onderwerp. Ik verwacht dat de kost van het grootschalig uitvoeren en implementeren van dit werk in de toekomst het grootste struikelblok zal zijn. Het zelf implemeneteren van het blockchain netwerk zal volgens mij het meest ingewikkelde deel van dit werk zijn. Ik verwacht dat dit zeker niet zonder moeilijkheden zal verlopen.

5. Verwachte conclusies

De blockchain implementatie om de veiligheid en privacy te verbeteren zal zijn investering zeker waard zijn. De voordelen van deze methode zullen de nadelen ver overstijgen. Aangezien het netwerk van IoT devices alleen maar zal uitbreiden en de gegevens op de toestellen belangrijker zullen worden, verwacht ik dat dit een ideale oplossing zal zijn om deze problemen weg te werken.

Referenties

Atlam, H. F. & Wills, G. B. (2019). Technical aspects of blockchain and IoT.

Buterin, V. (2014). A next generation smart contract and decentralized application platform.

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E. & Wortmann, F. (2019). Blockchain for the IoT: Privacy-Preserving Protection of Sensor Data. Journal of the Association for Information Systems.

Džaferović, E., Sokol, A., Almisreb, A. & Mohd Norzeli, S. (2019). DoS and DDoS vulnerability of IoT: A review. Sustainable Engineering and Innovation, ISSN 2712-0562.

Muhammad Burhan, B. K., Rana Asif Rehman & Ki, B.-S. (2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT.

Qian, Y., Jiang, Y., Jing Chen, Y. Z., Song, J., Zhou, M. & Pustisek, M. (2018). Towards decentralized IoT security enhancement: A blockchain approach.

Ramachandran, G. S. & Krishnamachari, B. (2018). Blockchain for the IoT: Opportunities and Challenges.

Sun, H., Hua, S., Zhou, E., Pi, B., Sun, J. & Yamashita, K. (2018). Using Ethereum Blockchain in Internet of Things: A Solution for Electric Vehicle Battery Refueling.

Sun, H. & Sun, J. (2018). Using Ethereum Blockchain in Internet of Things: A Solution for ElectricVehicle Battery Refueling.

Tawalbeh, L., Muheidat, F., Tawalbeh, M. & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions.

Yang, Y., Wu, L., Yin, G., Li, L. & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet of Things Journal.