BLOCKCHAIN SECURITY:
VEILIGE EN ROBUUSTE SMART CONTRACTS

TNO innovation for life

Blockchain is een onderwerp dat de laatste paar jaren steeds meer aandacht heeft gekregen, waarbij de hype er omheen ook heeft gezorgd voor hoge (deels misplaatste) verwachtingen van de disruptieve kracht van deze technologie. Blockchain technologie zelf past echter wel in een algemene trend van toenemende digitalisering en autonomie van digitale systemen. De digitale munteenheid Bitcoin, waar blockchain technologie zijn oorsprong heeft, is hiervan een voorbeeld.

Blockchain technologie kan gezien worden als een manier om samenwerking te faciliteren tussen verschillende partijen die elkaar maar tot op zekere hoogte vertrouwen. Zij beogen dit vertrouwen te vergroten door afspraken en opdrachten tussen partijen bij te houden in een gedistribueerde, gedeelde database, die de eigenschap heeft dat al hetgeen daarin is vastgelegd, niet meer kan worden herroepen. Sommige blockchain-technologieën voegen hieraan de mogelijkheid toe om kleine taakjes/programmaatjes uit te voeren. Dit kan (op termijn) betekenen dat traditionele "derde partijen" of tussenpersonen die deze taken nu nog moeten uitvoeren, worden weg-geoptimaliseerd.

Zulke programmaatjes (zogenaamde "smart contracts") worden ook in de gedeelde database opgeslagen en zijn dus niet meer (zomaar) aan te passen zodat iedereen kan zien wat ze gaan doen en daar op kan vertrouwen. De smart contracts worden vervolgens autonoom en gedistribueerd uitgevoerd en kunnen zelfstandig wijzigingen aanbrengen in de gedeelde database, wat smart contracts in feite de controle geeft over grote hoeveelheden waarde. Daarbij 'leven' de smart contracts in een open, gedistribueerde omgeving, wat maakt dat fouten in de smart contract code grote (ook: financiële) gevolgen kunnen hebben.

Een voorbeeld van deze gevolgen blijkt uit het "The DAO" incident (op het Ethereum platform): door de onderliggende smartcontract code van "The DAO" te analyseren en een fout daarin te misbruiken, kreeg een aanvaller de controle over meer dan $50M van de ongeveer $150M die in het contract zat.

ONDERZOEK 2017

De genoemde eigenschappen van smart contracts stellen hoge eisen aan hun integriteit: ze moeten doen wat bedoeld is, en niet doen wat niet bedoeld is. Dit project stelt zich dan ook ten doel om gaten die zitten tussen de intentie achter een smart contract (wat het zou moeten doen) en wat een contract uiteindelijk daadwerkelijk doet, te verkleinen. De te ontwikkelen technologie en tooling moet veiliger en robuuster smart contracts mogelijk maken. Specifiek zijn wij van plan de volgende oplossingsrichtingen te verkennen:

- Genereren van smart contracts vanuit gevalideerde business rules.
- Genereren van smart contracts met bewijsbare eigenschappen door toepassing van recente ontwikkelingen op het gebied van formele methoden.
- Ontwikkeling van/uitbreiding van analyse- en/of visualisatie-tools voor bestaande smart contracts om veelgemaakte fouten te detecteren.

OPROEP TOT SAMENWERKING MET STAKEHOLDERS

Binnen dit project zijn wij op zoek naar partners, met name voor het aandragen van use-cases om mee te experimenteren en onze projectresultaten te valideren. Hierbij zijn wij vooral geïnteresseerd in use-cases waarin meerdere partijen (uit verschillende domeinen) belang hebben bij een gezamenlijke waarheid om efficiënte samenwerking te faciliteren.

Stakeholders die hun use-case willen aanbieden voor analyse in het onderzoeksproject zijn van harte uitgenodigd contact op te nemen met Dhr. Dr. M.H. (Maarten) Everts voor nadere informatie.

TNO.NL

WE MAKE CYBER WORK FOR YOU

CONTACT
Dhr. Dr. M.H. (Maarten) Everts
T +31 (0)88 866 31 90
M +31 (0)63 175 70 70
E maarten.everts@tno.nl