Data science and data security, Smart Industries

Blockchain is hot, maar is het ook voor jou?

Imecs beveiligings- en privacy-experten helpen bedrijven op weg met Blockchain.

Intro

Veel artikels in de media schrijven laaiend enthousiast over Blockchain, en volgens specialisten zal de technologie de volgende tien jaar een revolutie ontketenen in de economie. Blockchain biedt op het eerste zicht inderdaad kansen om transacties en processen te optimaliseren, de efficiëntie te verhogen, fraude terug te dringen en kosten te verminderen. Maar veel bedrijven kijken verder dan de hype en vragen zich af hoe zij met Blockchain aan de slag kunnen gaan en hoe hun bedrijfslogica naar die nieuwe technologie kan worden vertaald. “Blockchain staat voor een toolbox en een bepaalde aanpak. Het is geen kant-en-klaar product,” verduidelijken Wouter Joosen en Bart Preneel, directeurs en beveiligingsgoeroes bij imec. “Het is dus essentieel om de talrijke mogelijkheden van de technologie te verkennen, basisregels voor privacy en beveiliging uit te werken en mogelijke juridische implicaties te onderzoeken.”

Veilige en gedeelde registratie

Sinds het allerprilste begin van de handel houden mensen informatie bij over hun transacties en akkoorden. En toen het aantal betrokken partijen begon toe te nemen en de waarde van de transacties steeg, werden er regels afgesproken en kwamen er instellingen om de informatie te registreren. Een eenvoudige geldoverdracht tussen twee bedrijven bv. is slechts mogelijk als twee banken in actie komen en informatie uitwisselen, en gewoonlijk is daar ook nog een interbancaire instelling bij betrokken. Al deze instellingen moeten deze informatie bijhouden, een forse beveiligingsinfrastructuur opzetten en snelle en betrouwbare communicatie garanderen.

Wouter Joosen: “Door de mondialisering van productie en handel is de behoefte aan registratie en controle nog toegenomen. Dit leidt tot een wildgroei aan registratiesystemen en instellingen die fouten, fraude en verkeerde interpretaties moeten voorkomen. Tegenwoordig zit elk bedrijf verweven in diverse netwerken en logistieke ketens en probeert het verwoed om alle registraties correct en up-to-date te houden. Zelfs als particulier heb je bijvoorbeeld alle moeite van de wereld om je online digitale identiteit correct te houden: je wachtwoorden, adressen, loopbaangegevens enz.”

Blockchaintechnologie belooft dat alles grondig te vereenvoudigen met behulp van een geautomatiseerd logboek dat door alle partijen wordt gedeeld en gecontroleerd.

Met andere woorden: meerdere partners kunnen afspraken maken, transacties uitvoeren, en slimme contracten opzetten zonder tussenkomst van een derde partij.

Een voorbeeld uit de handel maakt dit duidelijk. Je overweegt om een diamant te kopen, maar eerst wil je graag weten of die echt is, niet werd gestolen en op een ethische manier gedolven. De verkoper geeft je een certificaat, maar hoe weet jij - en hoe weet zelfs de verkoper - of alles wat op dat certificaat staat ook klopt? Een Blockchaintoepassing zou dit vraagstuk kunnen oplossen. Elke gedolven diamant zou in een elektronisch register terechtkomen, samen met een unieke digitale hogeresolutiefoto en uitleg over de afkomst. Telkens wanneer de diamant in andere handen terechtkomt, zou nieuwe informatie worden toegevoegd. Vóór er informatie in het register wordt opgenomen, controleren diverse partijen of ze wel klopt. Het register moet dus niet centraal worden beheerd; alle partijen hebben een kopie en kunnen volgens bepaalde regels informatie toevoegen. De manier waarop dat gebeurt maakt het vrijwel onmogelijk om ermee te knoeien. Dus wanneer jij uiteindelijk de edelsteen in handen krijgt, zie je alles wat ermee gebeurd is, vanaf het opdelven tot wanneer jij hem in je bezit hebt. En je kunt zeker zijn dat die informatie correct is.

Van Bitcoin tot jouw toepassing

“Veel bedrijven zien wel dat Blockchain voordelen en mogelijkheden biedt, maar weten niet hoe en waar te beginnen,” zegt Joosen.

> *“Blockchain is geen product dat je zonder meer installeert. Het is een technologische toolbox om op een andere manier te gaan werken, een methode om tussen partijen betrouwbare informatie bij te houden zonder dat er een tussenpersoon of centrale overheid aan te pas komt.”*

In essentie is een Blockchaintoepassing - zoals de naam aangeeft - een keten van digitale blokken. Elk blok bevat een aantal geverifieerde transacties, bijvoorbeeld een aantal betalingen of wijzigingen in de eigendomsstatus van een object. Deelnemers hebben toegang tot hun exemplaar van de keten om blokken toe te voegen of informatie in de keten te raadplegen.

De bekendste toepassing van de Blockchaintechnologie is Bitcoin, de digitale munt die door geen enkele instantie wordt uitgegeven of gewaarborgd. Bitcoin laat zien hoe krachtig de technologie is en hoe ze kan gebruikt worden. Maar een aantal aspecten zijn misschien minder interessant voor bedrijfstoepassingen.

Joosen: "Om te beginnen is Bitcoin een publiek register. Iedereen kan meedoen, Bitcoins kopen, ermee betalen of zelfs blokken in de keten verifiëren en toevoegen. Dit laatste is de zogeheten 'mining', een specifiek businessmodel op zichzelf. Maar bij bedrijven gaat het meestal niet om publieke toepassingen: slechts een beperkt aantal partijen wil gegevens delen. Dit heeft belangrijke gevolgen voor de manier waarop de toegang tot de gegevens en de beveiliging worden georganiseerd."

Of neem nu privacy en traceerbaarheid. In principe kan iedereen die een Bitcoinadres in handen krijgt de Blockchain raadplegen en de geschiedenis en eigendomsevolutie van die Bitcoin zien. Zodra je snapt hoe Blockchain in elkaar zit, kan je er heel gedetailleerde informatie uithalen over de werking ervan. Alhoewel er technieken bestaan om de privacy van deelnemers te verhullen, ontbreekt dus een inherente privacybescherming. Dat is misschien niet zo erg in het geval van de Bitcoin of de diamant van ons voorbeeld, maar als jouw toepassing toevallig medische gegevens bevat, dan wil je zeker een strikte toegangscontrole en privacymaatregelen inbouwen.

"Toch is de Bitcoin een mooi voorbeeld," zegt Preneel. "Het is een vrij toegankelijk laboratorium om alle mogelijkheden en uitdagingen van Blockchaintoepassingen te bestuderen. Daarom volgen onze onderzoekers alles wat er met de Bitcoin gebeurt op de voet."

"Wie Bitcoin heeft bedacht, blijft een mysterie, maar het is een heel slim systeem. De uitvinder schreef gedistribueerde, op consensus gebaseerde software die gebruik maakt van bestaande netwerk- en versleutelingstechnologie. Niemand was daar eerder in geslaagd. Tegelijk zijn er nog wel wat uitdagingen. Zo bestaat er discussie over de meest efficiënte grootte van de blokken. Daarbij is het interessant om te zien hoe een netwerk van partijen erin slaagt om het eens te worden over wijzigingen aan het systeem zelf. Wij kijken ook met veel belangstelling naar de privacytechnieken en -strategieën waarmee mensen in dit zeer publieke systeem anoniem proberen te blijven."

"Onze wetenschappers publiceren regelmatig studies over dit onderwerp en wij hebben gemerkt dat één ervan de manier van stemmen bij consensus bij Bitcoin heeft veranderd. Het is razend interessant om te zien hoe een complexe toepassing als Bitcoin functioneert. En we leren er veel uit dat goed van pas komt in andere cases."

Op verkenning

Om bedrijven te helpen met Blockchaintechnologie en te zien hoe ze praktische een toepassing kunnen ontwikkelen, heeft imec een imec.icon-project opgezet met zes bedrijven die de nieuwe technologie op hun specifieke domeinen willen toepassen.

Joosen: “Er is bijvoorbeeld een fintechbedrijf bij dat wil nagaan hoe nuttig Blockchain is om reverse factoring te organiseren en gehypothekeerde facturen bij te houden. Een ander voorbeeld is een technologiebedrijf in de gezondheidssector dat aan gedecentraliseerde patiëntendossiers wil werken. Hiervoor zijn strikte privacyregels natuurlijk onontbeerlijk. En een derde bedrijf werkt met ontwerp- en simulatiegegevens voor voertuig- en vliegtuigonderdelen. Hier gaat het dus eerder om een toepassing van supply chain management. Ten slotte wil een telecombedrijf een systeem opzetten om IoT-data te verhandelen. Al deze voorbeelden hebben één kenmerk gemeen dat ze onderscheidt van Bitcoin: de behoefte om strikte toegang, veiligheids- en privacymaatregelen toe te passen. Die moeten dan worden geselecteerd en geïmplementeerd in het gekozen platform, bijvoorbeeld als plugins of extra softwarelagen.”

Zo’n imec.icon project is bedoeld voor vraaggedreven, coöperatief onderzoek. Over een periode van gemiddeld twee jaar werken multidisciplinaire teams van wetenschappers en industriële partners samen om digitale oplossingen te ontwikkelen. Het programma heeft al meer dan 100 voltooide projecten in een hele reeks ICT-gerelateerde toepassingsdomeinen en markten opgeleverd.

“Naast dit project leveren wij ook industrieel advies,” zegt Preneel.

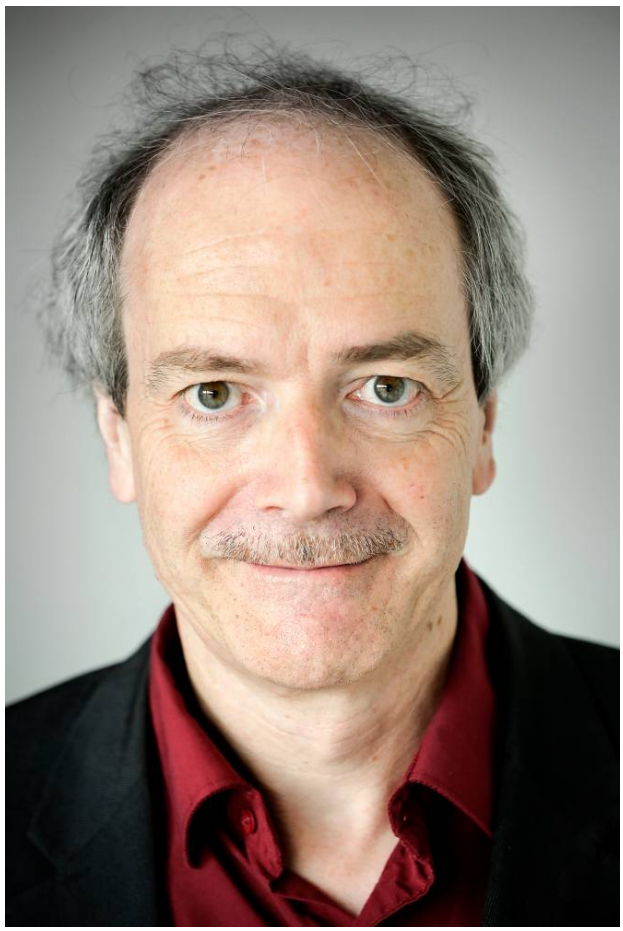
> *“Sommige bedrijven tasten alleen maar de mogelijkheden af, andere zijn al bezig met de ontwikkeling van een toepassing. Ze kunnen daarvoor terecht bij onze onderzoekers, die hen met hun ervaring en expertise kunnen helpen om de juiste beslissingen te nemen, juridische aspecten onder de loep te nemen en privacy- en beveiligingskwesties uit alle mogelijke invalshoeken te bekijken.”*

“Wij merken een grote vraag naar onafhankelijk advies over Blockchain bij bedrijven,” zegt Joosen. “Het nieuws doet de ronde dat Blockchain de wereld gaat veranderen en dat iedereen beter vroeg dan laat in deze technologie investeert. Bedrijven willen dus weten of ze er baat bij kunnen hebben en of ze er nu al in moeten investeren en expertise opbouwen. Wij beschikken over de kennis en de experts om ze met deze vragen te helpen.”

Meer weten?

- Lezing van Bart Preneel waarin hij de grondbeginselen van Bitcoin uitlegt

Biografie Bart Preneel



Bart Preneel leidt de onderzoeksgroep COSIC bij imec – KU Leuven en is ook gewoon hoogleraar aan de KU Leuven (België). Zijn voornaamste onderzoeksdomeinen zijn informatiebeveiliging en privacy, met de nadruk op zowel cryptografische algoritmes en protocollen als op efficiënte en veilige implementaties. Hij levert ook advies aan belangrijke spelers uit de financiële, telecom- en hardwaresector. Bart was een van de medeontwerpers van de Belgische programma's voor eID en e-voting en is actief in internationale standaardiseringsorganisaties. Professor Preneel is een fellow van de International Association for Cryptologic Research (IACR), waarin hij directeur (1997-nu), ondervoorzitter (2002-2007) en voorzitter (2008-2013) was. Hij is lid van de Permanent Stakeholders Group van ENISA (European Network and Information Security Agency) en van Academia Europaea. In 2014 ontving hij de RSA Award for Excellence op het onderzoeksdomein wiskunde.

Biografie Wouter Joosen

Wouter Joosen leidt de DistriNet onderzoeksgroep bij imec – KU Leuven en is daarnaast ook gewoon hoogleraar aan de KU Leuven (België). Zijn onderzoek gaat onder andere over software-engineering en architecturen voor veilige gedistribueerde systemen, security middleware en veilige oplossingen voor het IoT, cloudcomputing, IAM, DevOps, SecDevOps, Privacy-by-Design, en GDPR. Wouter is medeoprichter van de KU Leuven spin-off Ubizen (dat nu deel uitmaakt van Verizon Business Solutions), waarin hij de functie van CTO bekleedde van 1996 tot 2000 en van COO van 2000 tot 2002. Hij was ook betrokken bij de oprichting van een aantal andere KU Leuven spin-offs zoals Inmanta en Elimity.