Is blockchain technologie de heilige graal voor cybersecurity? Een onderzoek naar de impact van blockchain technologie op gebied van cybersecurity in Estland

Verdaasdonk, Mathieu

Is Blockchain technologie de heilige graal voor cybersecurity?

Een onderzoek naar de impact van blockchain technologie op gebied van cybersecurity in Estland

Master scriptie

1 juli 2022

Universiteit Leiden

Mathieu Verdaasdonk

Begeleider: Alex Ingrams

Universiteit Leiden

Inhoud

Voorwoord

Dit onderzoek is tot stand gekomen als onderdeel van het afronden van de master Politiek, Beleid en Management aan de Universiteit Leiden.

Gezien de bestuurskundige achtergrond van de onderzoeker en de interesse naar de nieuwe technologische ontwikkelingen die zich manifesteren werd voor de onderzoeker al vroeg duidelijk welke richting het onderwerp van de scriptie op zou gaan. Gezien de algemene hype rondom blockchain technologie binnen de wereld van tech en gadgets, leek deze technologie zich te lenen voor een onderzoek.

In de vroege stage van het kiezen van onderwerpen heeft de onderzoeker de mogelijke toepassingen van deze nieuwe techniek binnen de eigen kringen besproken. Op dat moment werd vooral de interesse gewekt door het idee dat het ooit mogelijk moest worden om eigendom te registreren met de hulp van deze technologie.

Toen het onderzoeksvoorstel daadwerkelijk vorm begon te krijgen, werd uitgegaan van de mogelijkheid om informatiehuishouding te versterken door het gebruiken van deze nieuwe technologie. Gezien de noodzaak in Nederland voor de overheid om de informatiehuishouding op orde te brengen, leek een comparatieve studie tussen Nederland en Estland een goede keus.

Bij nader inzien bleek een comparatieve studie binnen de tijd die stond voor het onderzoek, niet erg haalbaar. Ook bleek in het vooronderzoek dat een comparatief framework tussen de twee landen erg complex en daarmee wederom te tijdrovend. Daarnaast bleek het meer haalbaar om het onderzoek te richten op het veld van cybersecurity in plaats van informatiemanagement.

Om die redenen is uiteindelijk gekozen om een single-case studie uit te voeren om zo achter de werking en de impact van het implementeren van blockchain technologie te komen.

De onderzoeker wil zijn dank uitspreken aan Dhr. Ingrams voor de prettige begeleiding en de scherpe inzichten.

1. Inleiding en onderzoeksvraag

In de afgelopen decennia hebben veel landen een digitale infrastructuur aangelegd om optimaal te kunnen inspelen op de kansen die nieuwe technologische ontwikkelingen bieden. Waar vroeger alles nog analoog gebeurde, kan tegenwoordig steeds meer digitaal geregeld worden. In het kader van efficiëntie van overheidshandelen is de verregaande digitalisering goed uit te leggen; wanneer er verregaande digitalisering plaatsvindt, zijn er minder verwachte structurele kosten. Hoewel er veel kansen en mogelijke efficiëntiewinst hangen aan digitalisering van een samenleving, zijn er ook nieuwe gevaren. Cyberaanvallen kunnen, door de groeiende afhankelijkheid van de samenleving op de digitale infrastructuur, delen van de samenleving verlammen door in te breken in de systemen en deze plat te leggen of te manipuleren. Daarnaast kan gevoelige informatie worden buitgemaakt zonder sporen achter te laten. Er zijn een aantal gevallen waarin de impact van dergelijke cyberaanvallen duidelijk wordt. Zo werden in 2017 twee containerterminals van de haven van Rotterdam platgelegd (AD, 2017) De haven van Rotterdam is een van de belangrijkste handelshavens van Europa en het platleggen van een deel van deze haven heeft enorm veel geld gekost. Volgens de directeur digitaal & IT van de Rotterdamse haven bestaat er in 2022 ook nog altijd een reële dreiging voor cyberaanvallen op de belangrijke handelshaven (NRC,2022). Ook banken kunnen het doelwit zijn van cyberaanvallen. Zo werden in 2007 aanvallen gepleegd op de websites van banken in Estland. Deze websites werden binnen een korte tijd platgelegd en konden dus niet meer gebruikt worden. Maar hier bleef het niet bij. Ook de communicatiemiddelen van de overheid werden bij deze aanvallen uitgeschakeld en in de chaos werden nog tientallen andere doelwitten in deze samenleving aangevallen (Shackelford, 2010). Deze voorbeelden zijn niet enkele incidenten. Het Center for Strategic & International Studies (CSIS) houd op een website bij welke cyberincidenten er allemaal gerapporteerd worden. Wanneer men deze website bekijkt, ziet hij tal van recente cyberincidenten die zich overal ter wereld voordoen (CSIS, 2022).

Het rapport *Cybersecuritybeeld Nederland* van het Nationaal Coördinator Terrorismebestrijding en Veilgheid (2020) stelt dat Nederland moet uitgaan van een permanente dreiging van cyber attacks en dat de cybersecurity nog lang niet op orde is om het land op alle fronten tegen dergelijke digitale aanvallen te verdedigen. Ook stelt het rapport dat cyberincidenten de ‘achilleshiel’ van de digitale veiligheid zijn.

Het is voor overheden dan ook belangrijk om zich te wapenen tegen het voordoen van cyberincidenten, om het beschadigen, lekken of aanpassen van gevoelige informatie te voorkomen. Het is bijvoorbeeld van belang dat (gevoelige) data efficiënt en veilig opgeslagen wordt (Irion, 2013). Blockchain technologie wordt steeds vaker genoemd als mogelijke oplossing voor de uitdaging van veilige informatiemanagement.

Pilkington (2016) geeft in een overzicht weer dat er verschillende definities van het concept blockchain zijn en dat het probleem van veel definities is dat ze de toepassing van de blockchain in de definitie betrekken. Om deze reden wordt door Pilkinton gesteld dat de definitie van Vitalik Buterin het concept het beste weergeeft (p.229):

‘’a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always visible, and which carries a very strong cryptoeconomically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies.’’

Pilkinton nuanceert deze definitie wel, aangezien ‘magische computers’ geen wetenschappelijk waardevol concept is. Desalniettemin geeft de definitie het concept van blockchain wel weer, zonder de toepassing er van in de definitie te trekken.

Yaga et al. (2018) stellen dat een blockchain gezien kan worden als een gedecentraliseerde gedeelde digitale map waar een groep gebruikers transacties kan registreren en waarbinnen niet zo maar geknoeid kan worden met informatie en eventuele afwijkingen direct detecteerbaar zijn. Zo kunnen er transacties plaatsvinden tussen de gebruikers van de gedeelde map en zodra deze transacties in de map zijn gepubliceerd, kunnen deze niet meer worden aangepast. De onderzoekers spreken hier van een gesimplificeerde definitie, om de complexe materie duidelijker te maken.

Populaire media schetst een beeld waarin blockchain de heilige graal zou moeten zijn voor de toekomst van cybersecurity en informatiemanagement. De vraag is echter hoe deze technologie zich manifesteert in de realiteit.

Bijvoorbeeld is het zo dat een blockchain slechts zo sterk is als de hoeveelheid schakels die tot de ketting behoren. Wanneer een blockchain uit slechts een aantal schakels bestaat, bestaat er nog altijd het risico dat iemand de informatie op enige manier manipuleert (Berawi et al., 2021). Daarnaast maakt blockchain technologie gebruik van zogenaamde sleutels. Er zijn publieke sleutels, die alle ‘normale’ informatie op de blockchain weergeven en er zijn private sleutels die toegang verlenen tot data die afgeschermd is. Alketbi et al. (2018) stellen dat bestaande hack methoden deze sleutels kunnen dupliceren en dat hiermee, zonder dat degene die de sleutel in beheer heeft er van af weet, kan worden ingelogd in het blockchain netwerk. Ook stellen Alketbi et al. (2018) dat het ‘right to be forgotten’ aangetast kan worden wanneer gebruik wordt gemaakt van blockchain technologie in de opslag van informatie door de overheid omdat alle versies van alle informatiebundels (nodes) kunnen worden ingezien door iedereen in het netwerk. Informatie die normaliter dus (na enige tijd) wordt verwijdert, kan binnen dit netwerk niet verwijdert worden.

De theorie lijkt een beeld te schetsen van een toekomst waarin overheden door het gebruik van blockchain technologie grote problemen omtrent cybersecurity kunnen aanpakken, doordat het haast niet te hacken zou zijn en de technologie de transparantie verhoogt. De vraag is echter of deze nieuwe technologie in de praktijk ook echt zo effectief is als de theorie doet lijken. Binnen dit onderzoek zal worden onderzocht wat de impact op de mate van cyberveiligheid is van het gebruiken van blockchain technologie door overheden.

2. Theorie

2.1 Kernbegrippen

2.1.1 Gedeelde gedigitaliseerde map (Distributed Ledger Technology – DLT)

Wanneer binnen dit onderzoek gesproken wordt over een gedeelde map, doelt de onderzoeker op het onderdeel van de blockchain technologie waarbinnen verschillende gebruikers informatie kunnen opslaan en elke vorige versie van de informatie in het systeem ook in te zien is. Wat deze gedeelde map binnen de blockchain technologie onderscheid van mappen in andere technologie is dat de informatie niet kan worden aangepast of worden vervangen, er kan slechts informatie worden toegevoegd. (Alketbi et al. (2018); Yaga et al. (2018); Berawi et al. (2021))

2.1.2 Hash-functie

Yaga et al. (2018) stellen dat gecodeerde hash-functies een belangrijk component zijn van blockchain technologie. Hash-functies zijn computer gegenereerde codes die aan data of datasets worden gehangen wanneer deze binnen het blockchain netwerk worden opgeslagen om zo later, door iedere individuele gebruiker, te kunnen verifiëren of deze data of dataset in originele staat verkeerd. Wanneer iemand de data of dataset invoert en deze opnieuw '*hasht*' moet de output van de hash (ofwel *digest*) exact dezelfde zijn als de output van de hash van het origineel, anders betekend het dat er een verandering in de data heeft plaatsgevonden. Zelfs als de kleinst mogelijke verandering heeft plaatsgevonden, zal de output van de hash volledig anders zijn dan die van het origineel. Belangrijk is hier dat de hash-functie algoritmen los staan van blockchain technologie, maar dat het wel een belangrijk onderdeel is van de werking van blockchain technologie als geheel.

2.1.3 Consensus protocol

Het consensus protocol stamt af van de oude manier van transacties doen. Wanneer twee partijen vroeger een transactie wilden doen, moest er een derde partij worden betrokken om onpartijdig de transactie te bevestigen, zodat geen van de twee partijen fraude kon plegen. Met de komst van globale transacties bleek dit echter lastig, bijvoorbeeld omdat een partij zich kon voordoen als zowel de koper als de onpartijdige partij.

In het geval van blockchain, zijn er verschillende consensus protocollen verschenen, die ieder een eigen werking kent. Het betreft echter altijd een systeem van controle van transacties door meerdere actoren om geknoei met (data) transacties te voorkomen. (Sankar et al.,2017)

Samy et al. (2021) stellen dat het consensus protocol de procedure is die er voor zorgt dat alle schakels in het netwerk dezelfde transacties doorvoert in de 'ledger' bij elke update.

2.1.4 Smart contracts

Cong en He (2019) stellen dat er nog geen algemeen geaccepteerde definitie is van smart contracts, maar dat de aard van de werking er van er voor zorgt dat er een werkende definitie gesteld wordt. Een smart contract is volgens hen een digitaal contract waarbij de bepalingen in dat contract afhangen van een gedecentraliseerde consensus waar niet mee te knoeien is en die normaliter zelf bekrachtigend is doordat deze automatisch uitgevoerd wordt.

2.1.5 Cyberincidenten

Cyberincidenten zijn volgens de Nationaal Coördinator Terrorismebestrijding en Veiligheid (2020, p.11): ‘’alle gebeurtenissen of activiteiten die de beschikbaarheid, integriteit of vertrouwelijkheid aantasten van informatie- en procesbesturingssystemen, daardoor verwerkte en opgeslagen informatie en daarvan afhankelijke diensten en processen.’’ De RIA (2018) stelt grofweg dezelfde definitie. Dergelijke incidenten kunnen veroorzaakt worden door een moedwillige activiteit van een cyberactor, cyberaanvallen of uitval door technisch of menselijk falen. Het grote verschil met het begrip cybersecurity is hier dat cyberincidenten de gebeurtenissen zijn die cybersecurity tracht te voorkomen. Gezien de groeiende mate van invloed van technologie op de maatschappij, is het van belang dat het risico op dergelijke cyberincidenten zo klein mogelijk gemaakt wordt. Toch zijn er nog regelmatig berichtgevingen over bijvoorbeeld dataleks en cyberaanvallen.

2.2 Concepten

2.2.1 Informatiehuishouding (information management)

Binnen dit onderzoek zal informatiehuishouding worden gedefinieerd als de (1) opslag van informatie (2) het beheer van de data en (3) de verstrekking van de opgeslagen informatie (RDDI, 2021).

2.2.2 Typen blockchain technologie

Blockchain technologie is grofweg uit te splitsen in drie typen; de publieke blockchain, de consortium blockchain en de volledig private blockchain (Sankar et al., 2017).

De publieke blockchain kent geen gecentraliseerde macht die boven de rest van de blockchain staat. Iedereen kan zich in het netwerk voegen of het netwerk weer verlaten wanneer hen dat uit komt. Ook kan iedere gebruiker in het netwerk zowel transacties doen als ze verifiëren.

De consortium blockchain kent geen gelijke macht, omdat de actoren die transacties mogen verifiëren van te voren zijn aangewezen. De gebruikers kunnen wel een verificatieproces starten, maar deze moet worden goedgekeurd door de actoren die van te voren zijn aangewezen.

De volledig private blockchain lijkt erg op de consortium blockchain. Dit type blockchain kent wel een gecentraliseerde macht die boven het hele netwerk staat en dus belangrijke beslissingen binnen en over het netwerk kan nemen. Ook het verificatieproces is volledig in handen van de centrale macht.

2.2.3 Cyberveiligheid

Binnen dit onderzoek zal cyberveiligheid worden gedefinieerd als de mate van het voorkomen van cyberincidenten op gebied van gegevensopslag en gegevensdeling. Volgens de Nationaal Coördinator Terrorismebestrijding en Veiligheid (2020) zijn cyberincidenten alle gebeurtenissen of activiteiten die de beschikbaarheid, integriteit of vertrouwelijkheid aantasten van informatie- en procesbesturingssystemen, daardoor verwerkte en opgeslagen informatie en daarvan afhankelijke diensten en processen.

2.3 Theoretisch kader

Het zorgvuldig opslaan van data is van groot belang voor de cyberveiligheid van een overheidsorganisatie. Hill (2014) stelt zelfs dat sterke databeschermingssystemen noodzakelijk zijn voor overheidsorganisaties om de taken en functies die zij wettelijk verplicht zijn uit te voeren veilig te kunnen doen. Whitman en Mattord (2018) stellen dat vertrouwelijke documenten en geclassificeerde informatie van overheidsorganisaties worden gezien als overheidseigendom dat moet worden beschermd ten tijden van het gebruik, de opslag en het communiceren van informatie door het implementeren van beleid, scholing en technologie. Berawi et al. (2021) onderstrepen het belang van sterke systemen om data te beschermen en stellen daarnaast dat deze sterke systemen in het bijzonder belangrijk zijn voor overheidsinstellingen die vertrouwelijke data en informatie kennen in hun documenten. Door de grote hoeveelheid en de waarde van dergelijke documenten, zouden dit soort documenten volgens de onderzoekers beschermd moeten kunnen worden tegen alle mogelijke dreigingen. Berawi et al. stellen vervolgens dat eerder vooral werd ingezet op dataopslag via de 'cloud'. Dit zou echter niet toereikend zijn aangezien er wel een gedeelde toegang is tot de informatie, waardoor het gebruikersgemak groot is, maar het systeem van cloudopslag erg gevoelig is voor cyberaanvallen. Een alternatief zou bijvoorbeeld lokale systeemopslag zijn. Het nadeel hier is dat het datadelingsproces hierbij moeilijker is. Doordat de hoeveelheid data jaarlijks toeneemt, zijn data integratie en data beveiliging cruciale punten van aandacht geworden voor overheidsinstellingen binnen het domein van dataopslag (Irion, 2013).

Binnen het veld van blockchain technologie is een tweedeling ontstaan. Husain (2020) stelt dat er twee kampen zijn die tegenover elkaar staan in de politisering van blockchain technologie; de crypto-anarchisten en de crypto institutionalisten. De eerste groep vind dat blockchain technologie juist disruptief zou moeten zijn ten opzichte van de centrale macht. De andere groep, de crypto-institutionalisten, willen juist dat overheden de potentie van blockchain gebruiken om de overheidsinstellingen te versterken.

Het vooronderzoek lijkt een beeld te schetsen waarin de crypto-institutionalisten vooral de wetenschap lijken te stimuleren, aangezien er steeds meer onderzoeken zijn naar mogelijke toepassingen van blockchain technologie in het sociaal domein. De meest onderzochte velden zijn; gezondheidszorg, gegevensopslag en identiteitsmanagement, de registratie van eigendom, verkiezingen en het Internet of Things.

Gezondheidszorg

Het grootste aantal onderzoeken naar de mogelijke toepassingen van blockchain in het sociaal domein is uitgevoerd op gebied van het thema gezondheidszorg, stelt Stanford Business Center for Social Innovation (Galen et al., 2018).

Hölbl et al. (2018) onderstrepen deze claim en stellen dat blockchain technologie op een aantal vlakken potentiële toepassingen kent binnen de gezondheidszorg. De grootste winst is volgens hen te behalen door blockchain technologie in te zetten op gebied van data management om zo de vele verschillende opzichzelfstaande systemen te kunnen verbinden en digitale gezondheidsdossiers zo meer complementair te maken. Blockchain technologie zou de datadeling kunnen bevorderen maar ook de toegang tot bepaalde data voor bepaalde partijen beter kunnen afschermen. Daarnaast kan deze technologie een positief effect hebben op gebied van; de transparantie van de ervaring van de zorgaanbieder, medische rekeningen, contracteren, het delen van medische dossiers, klinische onderzoeken en het tegengaan van nepmedicijnen. In de praktijk wordt blockchain technologie vooral ingezet op gebied van datadeling, het creëren van een complementair medisch dossier en het controleren van toegang tot de informatie. Hölbl et al. (2018) verwachten dat de technologie in de toekomst ook op de andere gebieden zal worden toegepast.

Het feit dat de toegang tot het medisch dossier door het inzetten van blockchain technologie dus voor bepaalde partijen beter afgeschermd zou kunnen worden, lijkt er voor te zorgen dat deze sector een sterker niveau van cybersecurity kan behalen met betrekking tot het beschermen van gevoelige gegevens.

Gegevens opslag en Identiteitsmanagement

Er zijn een aantal studies gedaan waarin de mogelijke toepassing van blockchain technologie op gebied van gegevens opslag en gegevensdeling wordt uitgediept. Zo zou het gebruik van blockchain technologie kunnen leiden tot meer transparantie (Badzar, 2016), snellere en makkelijkere informatiedeling (Wang et al., 2017), meer betrouwbaarheid (Kshetri, 2018) en makkelijkere en betere traceerbaarheid van data (Wang et al., 2020)

Blockchain technologie zou door de gedecentraliseerde structuur in combinatie met het consensus protocol, waardoor veranderingen in de data door iedere link in de schakel geverifieerd wordt, moeten zorgen voor een sterk beveiligde informatieopslag (Yaga et al. 2018) Door het potentieel effect van blockchain technologie op gebied van transparantie, cyberveiligheid en het tegengaan van corruptie wordt deze technologie steeds vaker benoemd als waardevol voor overheden om de uitdagingen met betrekking tot gegevensopslag aan te pakken (Alketbi et al.,2018; Berawi et al., 2021).

Ook identiteitsmanagement zou volgens de theorie een volgende stap kunnen zetten door het toepassen van blockchain technologie. Volgens Mattila (2016) heeft het gebruik van blockchain technologie bij online identiteitsmanagement twee grote voordelen. Het eerste voordeel is dat het gebruik van deze technologie geen onafhankelijke derde partij meer nodig heeft om een transactie tussen twee partijen te voltooien. Dit komt omdat de blockchain technologie het anoniem vertrouwen verwezenlijkt door het gebruik maken van een consensus protocol. Bij het doen van transacties zorgt het kunnen weglaten van een derde partij voor minder transactiekosten. Daarnaast hoeven de partijen niet onnodig veel persoonlijke informatie te bieden bij het doen van deze transacties, in principe kan dit anoniem.

Het tweede voordeel is dat blockchain technologie veel meer toepassingen voor de digitale identiteit toelaat. In principe kan de digitale identiteit met blockchain in iedere dienst worden geïntegreerd, mits de gebruiker dit wenst. Wanneer de digitale identiteit op meerdere platformen wordt gebruikt, kan dit in potentie de online reputatie van een individu versterken en daarmee wordt het vertrouwen tussen vreemden op het internet versterkt.

Rathee en Singh (2021) stellen echter dat hoewel er potentie is om identiteitsmanagement te verbeteren met blockchain technologie, er ook keerzijden zijn. De belangrijkste mogelijke valkuil is het privacy vraagstuk, wat volgens hen meer aandacht behoeft. Andere mogelijke zwakten van de technologie zijn schaalmogelijkheden, interoperabiliteit, kosten aangaande transacties, databeveiliging en data authenticatie, data opslag en het tekort aan (cyber)vaardigheden bij werknemers.

De theorie lijkt een beeld te schetsen waarin implementaties van blockchain technologie op gebied van gegevensopslag voor winst kunnen zorgen met betrekking tot het versterken van de cybersecurity aangaande dit onderwerp. Ook zouden online transacties en andere toepassingen van een online identiteit op een veilige en snelle manier kunnen worden gefaciliteerd door de technologie.

Registratie van eigendom

Sinds 2013 zijn er projecten met het gebruiken van blockchain technologie om eigendom te registreren (EVRY, 2020). Dit gebeurt door de documenten die het eigendom beschrijven in te laden in de blockchain en te ‘bestempelen’. Vervolgens volgt het de ‘normale’ weg in de blockchain en wordt de data zo gevalideerd. Om vervolgens eigenaar van het eigendom te worden in de blockchain, wordt een transactie gecreëerd waarbij gerefereerd wordt naar het fysieke object. Vervolgens krijgt de eigenaar een crypto grafische ‘sleutel’, waarmee eigenaarschap van het object wordt vastgesteld.

In het vooronderzoek zijn vooral stukken literatuur gevonden die onderzoek doen naar de mogelijkheid om vastgoed op een dergelijke manier vast te leggen (Castellanos en Benbunan-Fich, 2018; Wouda en Opdenakker, 2019).

Deze manier van het registreren van eigendom zou volgens de theorie toekomstbestendig moeten zijn en het opslaan van de data in de blockchain zou de veiligheid van de documenten moeten garanderen. Ook zouden bevoegde partijen gemakkelijk eerdere documenten aangaande hetzelfde goed gemakkelijk kunnen inzien, wat getuigt van meer transparantie.

Verkiezingen

Mattilla (2016) stelt dat een online stem systeem moet beschikken over een aantal eigenschappen om de onpartijdigheid van verkiezingen te kunnen waarborgen. Zo moet een dergelijk systeem anoniem zijn maar tegelijkertijd controleerbaar en moet het systeem niet te manipuleren zijn maar tegelijkertijd ook niet onder beheer staan (van een natuurlijk persoon). Volgens Mattila heeft blockchain technologie de eigenschappen om een dergelijk systeem te creëren.

Hjalmarsson et al. (2018) hebben een systeem ontworpen waarbij, met het gebruik van een blockchain technologie en smart contracts, uitdagingen op het gebied van elektronisch stemmen zouden moeten worden kunnen overwonnen. De nuance hierbij is dat dit systeem nog puur theoretisch is en is opgesteld voor landen met een klein inwonersaantal.

Garg et al. (2019) hebben bij hun comparatief onderzoek naar diverse e-voting systemen de conclusie getrokken dat blockchain technologie op dit moment een sterk alternatief is in vergelijking met de bestaande digitale stem systemen maar dat het niet alle uitdagingen en problemen oplost en daarmee dus niet waterdicht is, wat de maatschappij wel verwacht van stem systemen.

Volgens de theorie is het inzetten van blockchain technologie om te stemmen dus een sterk alternatief voor de bestaande stem-systemen. Dit omdat de blockchain technologie een sterk niveau van cyberveiligheid garandeert en er dus niet gesjoemeld kan worden met stemmen.

Internet of Things

Het Internet of Things (IoT) kan worden gezien als een netwerk van slimme systemen dat data verzameld en intelligente beslissingen kan maken (Panarello et al., 2018). Steeds meer fysieke dingen kunnen data verzamelen en delen met het overkoepelende netwerk, om zo betere beslissingen te maken. Dit is bijvoorbeeld terug te zien in de trend van smart cities. In plaats van dat iedere organisatie zijn eigen systemen bouwt en gebruikt, zou het IoT moeten zorgen dat alle platformen kunnen draaien binnen het IoT systeem.

Mattila (2016) stelt dat er bij het opstellen van een dergelijk netwerk een inherente wrijving is tussen economische belangen van de organisaties binnen de private sector en het belang van een IoT netwerk. Private organisaties geven immers niet graag de autonomie uit handen en maken vaak liever zelf een systeem dan dat ze binnen het systeem van een ander bedrijf moeten opereren. En zelfs als dit gebeurt, kan het zo zijn dat het bedrijf die de systemen ontwerpt voorrang verleent aan webverkeer naar de eigen producten of diensten. Dit wantrouwen zorgt er voor dat het IoT moeilijk van de grond komt. Blockchain technologie zou hier een uitkomst kunnen bieden, aangezien het een gedecentraliseerd en neutraal platform kan bieden waar iedere gebruiker over dezelfde rechten en autonomie beschikt, aldus Mattila.

Panarello et al. (2018) stellen tevens dat blockchain technologie een aantal fundamentele problemen van IoT, bijvoorbeeld problemen aangaande privacy, data integriteit en vertrouwelijkheid, kan oplossen. Dit komt doordat blockchain technologie in essentie de eigenschappen kent waar het IoT mee worstelt. Zo zorgt blockchain technologie voor authenticiteit, integriteit en, door het gebruik maken van smart contracts, het zorgvuldig managen van autorisatie en transacties.

De blockchain technologie kan volgens de theorie dus belangrijke vraagstukken die opkomen bij het ontwerpen en implementeren van IoT oplossen. Vooral op gebied van veilige dataopslag, ethische vraagstukken en het tegengaan van corruptie van de data.

Hoewel er meerdere studies een aantal velden van mogelijke implementatie binnen het sociaal domein veronderstellen, kent de implementatie van blockchain technologie ook uitdagingen. Een aantal van deze uitdagingen bij het implementeren van blockchain technologie die worden omschreven in de literatuur zijn de schaalmogelijkheden, systeemintegratie en de complexiteit van de technologie.

Prewett, Prescott en Phillips (2020) stellen dat een grote uitdaging bij het implementeren van blockchain technologie in overheidshandelen is dat er vaak al veel bestaande systemen gebruikt worden door overheden. Daarom zou vaak worden gezocht naar een manier om de blockchain complementair aan deze systemen te laten functioneren, in plaats van een volledig nieuw netwerk van IT systemen op te bouwen.

Mohanta et al. (2019) stellen dat schaalmogelijkheden een van de uitdagingen van blockchain technologie is. Dennis, Owenson en Aziz (2016) stellen zelfs dat dit een fundamentele limitatie van blockchain technologie is. Dit komt omdat de traditionele blockchain zo is ingericht dat iedere gebruiker alle informatie moet kunnen opslaan om deel te nemen aan de blockchain. Door de publieke aard van de technologie is het aantal data echter enorm gegroeid en kunnen gebruikers met weinig opslagcapaciteit deze data niet opslaan en dus niet deelnemen aan het netwerk.

Prewett, Prescott en Phillips (2020) stellen dat de complexiteit van blockchain technologie er voor kan zorgen voor een aantal knelpunten bij het implementeren van de technologie. Naast dat het door de complexiteit van de technologie veel kosten met zich meebrengt om een eigen blockchain systeem te bouwen, stellen de onderzoekers dat de complexiteit zelf ook kan zorgen voor minder interesse in de toepassing van de technologie. Wanneer leiders van bedrijven of overheden immers niet weten wat het systeem is en hoe het werkt, zullen zij het minder snel implementeren. Daarnaast moet het ook overzichtelijk zijn voor de mensen die er mee moeten gaan werken én moet er genoeg geschoold personeel zijn die achter de schermen van de blockchain werken.

De theorie veronderstelt een aantal mogelijke terreinen waar het gebruik van blockchain technologie kan zorgen voor een sterker niveau van cybersecurity. De meeste studies naar de mogelijke toepassingen van blockchain technologie in het sociaal domein zijn echter uitgevoerd op gebied van theorievorming en dus is het belangrijk dat de praktische implementatie en de risico’s van het gebruiken van (hybride) blockchain technologie in toepassingen door overheden onderzocht wordt. Dit wordt onderstreept door verschillende wetenschappers (Lindman et al., 2017; Alketbi et al., 2018; Zhong et al., 2020; Barawi et al., 2021).

3. Onderzoeksopzet en dataverzameling

3.1 Onderzoeksbenadering en -design

Dit onderzoek betreft een enkele case study waarbij de ervaringen van Estland op het gebied van het implementeren van blockchain technologie bestudeert worden om het effect van deze technologie op een aantal vlakken te meten. Allereerst zal een 'nulmeting' worden gedaan om de situatie vóór de implementatie van blockchain technologie te meten, vervolgens zal worden vergeleken of de situatie is verbeterd, verslechterd of is gestagneerd.

3.1.1 Deelvragen

Binnen dit onderzoek zal worden getracht antwoord te geven op de volgende vragen:

- Wat was de situatie met betrekking tot cyberveiligheid in Estland vóór de implementatie van blockchain technologie?

- Wat is de situatie met betrekking tot cyberveiligheid in Estland ná de implementatie van blockchain technologie?

- Wat zijn de risico's van het implementeren van blockchain technologie ter behoeve van de cyberveiligheid van digitale processen (in het algemeen)?

3.2 Analyse-eenheid en casusselectie

De analyse-eenheden binnen dit onderzoek is de (technologie achter de) versterking van cyberveiligheid binnen overheden.

De case die geselecteerd is de toepassing van blockchain technologie in Estland. Deze case is geselecteerd omdat Estland in de top drie staat van de UN e-government survey (2020). Dit laat zien dat Estland gezien wordt als een van de leidende landen op gebied van e-governance onder de 193 lidstaten van de UN. Dit zou kunnen wijzen op een best-practice case en dus is het van belang dat de precieze werking en onderdelen van het e-governance beleid en de digitale infrastructuur van Estland worden onderzocht. Daarnaast is Estland een interesting case, aangezien het land sinds haar onafhankelijkheid in 1991 in grote mate toegespitst lijkt te zijn op e-governance en digitale infrastructuur (Semenzin, Rozas en Hassan, 2022), in contrast met veel andere landen in de periode voor het nieuwe millenium. Het vroeg inzetten op digitalisering en e-governance, maakt het dat Estland als een unieke case kan worden gezien en daardoor waarde kan hebben bij het toetsen of verrijken van bestaande theorieën over het gebruik van blockchain technologie door overheden.

3.3 Operationalisering

3.3.1 Informatiehuishouding

De onderzoeker veronderstelt een sterke informatiehuishouding wanneer data veilig en gemakkelijk kan worden opgeslagen en alleen beschikbaar is voor mensen die bevoegd zijn die data te gebruiken. De onderzoeker veronderstelt een zwakkere informatiehuishouding wanneer data niet veilig kan worden opgeslagen, niet gemakkelijk kan worden opgeslagen of beschikbaar is voor onbevoegden.

Informatie over de veiligheid, het gebruikersgemak en de mogelijkheid om bepaalde data sets af te sluiten zal worden verzameld door de bestaande wetenschappelijke literatuur en evaluaties van projecten die gebruik maken van blockchain technologie (bijvoorbeeld in Estland) te analyseren middels een deskresearch.

3.3.2 Cyberveiligheid

De onderzoeker verondersteld een sterk niveau van cyberveiligheid wanneer het aantal cyberincidenten laag is. De onderzoeker verondersteld een zwak niveau van cyberveiligheid wanneer het aantal cyberincidenten hoog is.

Cijfermatige weergaven van het aantal cyberincidenten en de aard van deze incidenten zijn tijdens het vooronderzoek gevonden door publicaties van de Estonian Information System Authority (RIA). De rapporten van deze organisatie zullen voornamelijk gebruikt worden om inzicht te verschaffen in mogelijke trends met betrekking tot aantallen cyberincidenten door de jaren heen en de impact van eventuele incidenten op het informatiemanagement systeem.

3.3.3 Weergave operationalisering

Op de volgende pagina is de operationalisering in een tabel weergegeven. Belangrijk is dat de concepten die worden onderzocht allen op een eigen manier invloed hebben op het niveau van cyberveiligheid. Zo heeft ieder type blockchain bijvoorbeeld zijn eigen voor- en nadelen ten opzichte van cyberveiligheid, heeft de aanwezigheid van de implementatie risico's ook een mogelijk effect op dat vlak en heeft de manier waarop data wordt opgeslagen en gedeeld (informatiemanagement) ook een invloed op de mate van cyberveiligheid.

In de kolom 'verwachte observaties' maakt de onderzoeker duidelijk wat het precies is dat de onderzoeker wil meten per onderdeel van een concept.

In de kolom 'databronnen' worden de verschillende soorten documenten of andere informatiebronnen die de onderzoeker verwacht te gebruiken specifiek gemaakt.

In de kolom 'locaties' wordt weergegeven waar de onderzoeker de documenten of databronnen die gevonden zijn in het vooronderzoek vandaan heeft. Hier worden dan ook de trefwoorden genoemd die de onderzoeker heeft gebruikt. Ook worden in deze kolom de zoekmachines genoemd waar de onderzoeker gebruik van heeft gemaakt.

Concepten	Verwachte observaties	Databronnen	Locaties
Informatiehuishouding **Definitie:** De opslag van informatie, het beheer van de data en de verstrekking van de opgeslagen informatie.	Een verandering in hoe de informatie wordt opgeslagen in de perioden vóór en - na de implementatie van blockchain technologie in Estland.	Websites van e-estonia en guardtime, rapporten van organisaties en wetenschappelijke literatuur	e-estonia.com, guardtime.com, zoekopdrachten in google.com onder trefwoorden; 'cloud storage in Estonia' en 'information storage in Estonia' en zoekopdrachten naar literatuur in de databases google.scholar.com en de bibliotheek van Universiteit Leiden onder trefwoorden; 'Blockchain in Estonia' en 'Estonia before blockchain'.
	Een verandering in de wijze waarop data beheert wordt in de perioden vóór en – na de implementatie van blockchain technologie in Estland.	Websites van e-estonia en guardtime, rapport van PWC en wetenschappelijke literatuur	e-estonia.com, guardtime.com, rapport van PWC, gevonden via google.com door te zoeken op 'blockchain in Estonia' en zoekopdrachten naar literatuur in de databases google.scholar.com en de bibliotheek van Universiteit Leiden onder trefwoorden; 'Blockchain in Estonia', 'Private blockchains' en 'Estonia before blockchain'
	De verwachting is dat er zowel in de periode vóór als na de invoering van blockchain technologie in Estland geen informatie wordt verstrekt aan onbevoegden.	Website van e-estonia, wetenschappelijke literatuur en/of evaluaties van de RIA	e-estonia.com, evaluaties (perioden tussen 2012-2021) via Ria.ee en zoekopdrachten naar literatuur in de databases google.scholar.com en de bibliotheek van Universiteit Leiden onder trefwoorden; 'Estonia before blockchain', 'Blockchain in Estonia' en 'Cyber security in Estonia'

Private blockchain technologie **Definitie:** Type blockchain technologie waar een centrale macht boven het netwerk staat en keuzes kan maken over het netwerk en de data in het netwerk.	De verwachting is dat er bewijs wordt gevonden dat de blockchain technologie zoals deze is geïmplementeerd in Estland, een private blockchain betreft.	Websites van e-estonia en guardtime, wetenschappelijke literatuur en een rapport van het PWC	e-estonia.com, guardtime.com, een rapport van het PWC, gevonden door 'Blockchain in Estonia' in te voeren in zoekmachine Google.com en zoekopdrachten naar literatuur in de databases google.scholar.com en de bibliotheek van Universiteit Leiden onder trefwoorden; 'Blockchain in Estonia', 'Blockchain casestudy' en 'types of blockchain'.
Cyberveiligheid **Definitie:** De mate van het voorkomen van cyberincidenten op gebied van gegevensdeling en gegevensopslag	De verwachting is dat er na de implementatie van blockchain technologie in Estland een daling is in het aantal cyberincidenten	Jaarlijkse evaluatierapporten van de RIA	Ria.ee
Implementatie risico's	De verwachting is dat de literatuur een aantal implementatierisico's veronderstelt ten opzichte van het gebruiken van blockchain technologie door overheden	Wetenschappelijke literatuur	Zoekopdrachten naar literatuur in de databases google.scholar.com en de bibliotheek van Universiteit Leiden onder trefwoorden; 'Blockchain implementation risks', 'Blockchain risks', 'Blockchain challenges' en 'Blockchain case study'

Tabel 1: Overzicht operationalisering

3.4 Dataverzameling

Dit onderzoek zal inzichten gebruiken die verschaft zijn uit wetenschappelijke bronnen. Dit betreft onderzoeken naar informatiemanagement, cyberveiligheid, cyberincidenten, blockchain, toepassingen van blockchain en onderzoek gericht op de casus (blockchain in Estland). Daarnaast zal er gebruik gemaakt worden van zowel kwalitatieve als kwantitatieve data aangaande cyberincidenten zowel binnen het domein van de casus als in het algemeen. Dit kan gaan om berichtgeving over ingrijpende cyberincidenten of cijfermatige weergaven van aantallen cyberincidenten in een gebied. In het vooronderzoek zijn evaluatierapporten van de Republic of Estonia Information System Authority (RIA) gevonden over de jaren na het implementeren van de blockchain technologie, deze zullen worden gebruikt om het succes van de implementatie te meten en eventuele onvoorziene impact te duiden. Ook kunnen deze documenten de algemene trends binnen het cyber beleid van Estland weergeven. Een meer uitgebreide weergave van de dataverzameling – en selectie, met een overzicht van de trefwoorden die zijn gebruikt om bronnen te vinden, is te vinden in de bijlagen.

3.5 Analysekader

Allereerst zal er een nulmeting worden gehouden om te bepalen in welke mate het niveau van cyberveiligheid vóór de implementatie van blockchain technologie in de casus problemen ondervond met betrekking tot de aantallen – en de aard van cyberincidenten of andere problemen omtrent cyberveiligheid. Vervolgens zullen een aantal jaren na de implementatie onderwerp zijn van de analyse om eventuele trends met betrekking tot de aantallen en de aard van cyberincidenten of andere problemen in de periode ná de implementatie van blockchain technologie te kunnen vaststellen. Hierbij worden meerdere jaren onderwerp van de analyse omdat eventuele uitschieters zo kunnen worden geïdentificeerd en er dus uitspraken gedaan kunnen worden over de algemene trend die zich voordoet binnen het gebied van de casus. De eventuele trends die worden vastgesteld binnen de twee perioden (vóór en nà de implementatie van blockchaintechnologie in Estland) zullen vervolgens naast elkaar worden gehouden om te bepalen in welke mate het gebruik van blockchain technologie impact heeft gehad op het niveau van cyberveiligheid van Estland. Aangezien het doel van dit onderzoek is om de discussie over het gebruik van blockchaintechnologie voor het bevorderen van de cyberveiligheid van overheden aan te zwengelen, zal er ook kwalitatief materiaal worden gebruikt, wat vaak onderhevig is aan interpretatie. Tot slot zal er gebruikt worden gemaakt van literatuur die reeds beschikbaar is aangaande dit onderwerp.

4. Resultaten

4.1 Wat was de situatie met betrekking tot cyberveiligheid in Estland vóór de implementatie van blockchain technologie?

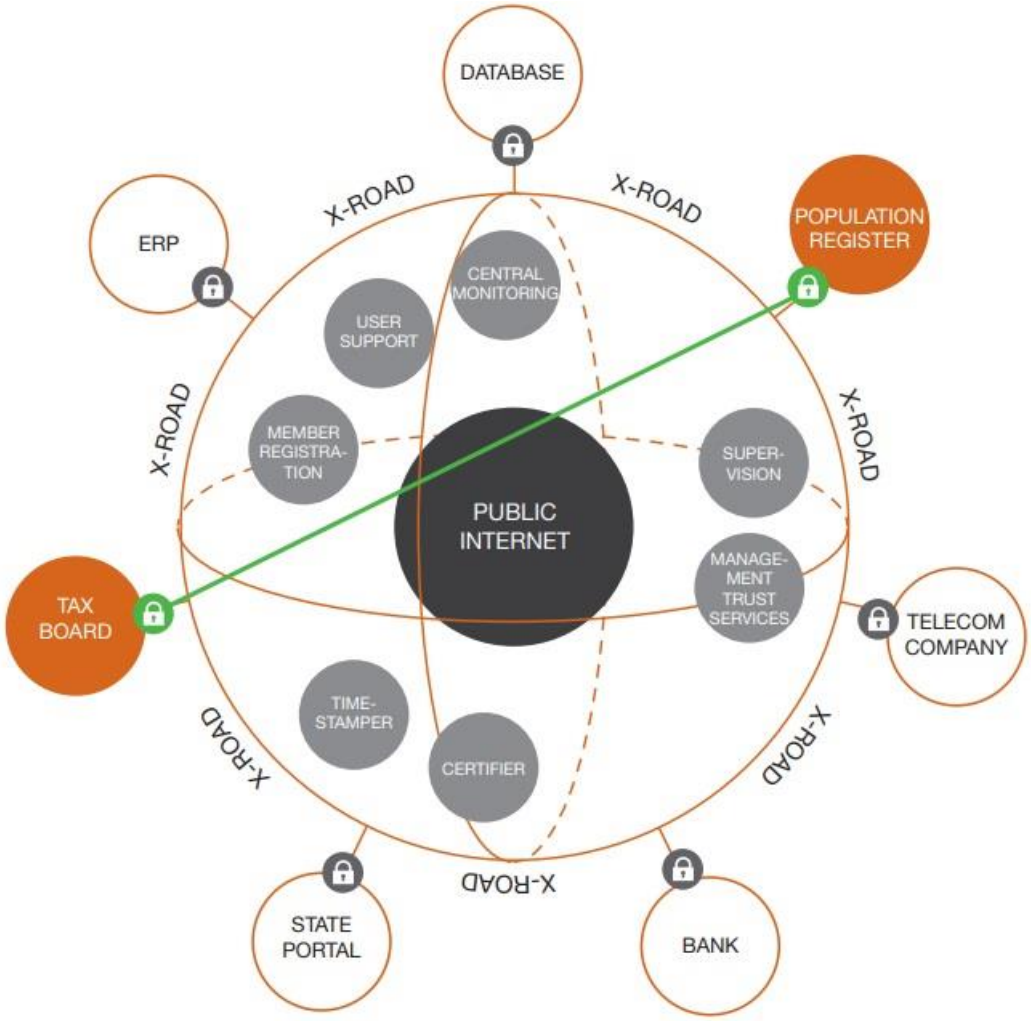
4.1.1 Algemeen

Nadat Estland in 1991 onafhankelijk werd verklaard, bleken de bestuurders het besef te hebben dat het land, waar haast geen voorzieningen aanwezig waren, de unieke kans hadden om het land op te bouwen en in te richten naar een toekomstvisie waarin efficiëntie en technologie centraal staan (e-estonia, 2022). In de eerste jaren werd een infrastructuur aangelegd waardoor IT mogelijkheden steeds makkelijker konden worden geïntegreerd in de maatschappij. Hierop volgend kwamen er diverse initiatieven door de overheid om de nieuwe digitale wereld te omarmen. Zo werden computervaardigheden bijvoorbeeld een prioriteit gemaakt in het onderwijs vanaf het jaar 1996. In de periode hierna werden diverse (overheids)diensten gedigitaliseerd. Zo kon men bijvoorbeeld vanaf het jaar 2000 de belastingaangifte volledig online aangeven (e-estonia, 2022). Er bleken zich echter problemen voor te doen in de vorm van de kosten van data deling en het voordoen van cyberincidenten. Met name dataleks door onvoldoende beschermde databases deden zich vaak voor. Om deze redenen werd de 'X-Road' ontworpen. Om er voor te zorgen dat onbevoegden minder makkelijk toegang konden krijgen tot gevoelige – of persoonlijke informatie, werd in 2002 een e-ID ingevoerd. Dit wil zeggen dat de persoonlijke identiteit gekoppeld is aan een ID-kaart, waarmee men zich zowel in het dagelijks leven als in de digitale sfeer moet kunnen legitimeren. Zo weet het systeem wie er welke data probeert te openen en kan het voorkomen dat iemand zich voordoet als een ander om zo toegang te krijgen tot bepaalde datasets. In de jaren hierna werden steeds meer diensten digitaal geregeld. Tot in 2007 grootschalige georganiseerde cyberaanvallen plaatsvonden waarvan Estland het doelwit was. Deze gebeurtenis zorgde er voor dat Estland en een groot deel van de internationale gemeenschap zich meer ging focussen op cyberveiligheid (e-estonia, 2022). In 2009 werd een deel van de opslagcapaciteit van Estland geoutsourcet naar de cloud van grote multinationals (Kotka & Liiv, 2015). Kort hierna, in 2012, werd blockchaintechnologie geïntegreerd in de digitale infrastructuur van Estland (PWC, 2019).

4.1.2 X-Road

Aangezien Estland geen centrale database heeft (e-estonia, 2022) wordt data opgeslagen op de plaats waar het ingevoerd wordt. Omdat organisaties echter wel vaak informatie nodig hebben die op andere plaatsen is opgeslagen moet er dagelijks een grote hoeveelheid data tussen organisaties gedeeld worden. Hierbij zijn drie dingen van groot belang; de data die is opgeslagen moet niet in te zien zijn door onbevoegden maar wel makkelijk beschikbaar zijn voor bevoegden, de data moet integer zijn (derden moeten het niet aan kunnen passen) en de informatie moet afgeschermd blijven voor onbevoegden op het moment dat het gedeeld wordt.

De X-Road is ontwikkeld om al deze opgaven in één keer aan te kunnen pakken. Met het gebruik van deze technologie wordt alle nieuwe data meteen gesynchroniseerd met andere databasis, zodat informatie maar een keer op een locatie hoeft te worden opgeslagen en vervolgens beschikbaar is voor alle relevante partijen. De X-Road is breed inzetbaar doordat het toepasbaar is op bijna alle andere verschillende systemen die worden gebruikt. Estland claimt dat deze manier van datadeling zorgt voor een jaarlijkse besparing van 1345 jaar aan werktijd (e-estonia, 2022), die anders door verschillende organisaties zou moeten worden gebruikt om data te verkrijgen, delen of bundelen. Estland noemt de X-Road dan ook de '*ruggengraat*' van e-Estland.



Figuur 1: Weergave van hoe het X-Road netwerk organisaties verbind (PWC, 2019. pp. 5)

4.1.3 e-ID

Een belangrijke ontwikkeling binnen het informatiemanagement van Estland was de koppeling van persoonsbewijzen aan een digitale code waarmee men online te identificeren is. Priisalu en Ottis (2017) stellen dat Estland bij het inrichten van de digitale overheid steunden op drie ‘pilaren’. De eerste van deze pilaren was het koppelen van de identiteit aan de digitale code. De tweede pilaar was vervolgens om de burger in staat te stellen op een veilige manier gebruik te maken van de online service van de overheid. Dit werd gedaan door een persoonlijke versleuteling van data te koppelen aan de persoonlijke digitale code, om de privacy van gegevens van de burger te waarborgen. Daarnaast werd er een soort digitale handtekening ontworpen, waarmee online identiteitsfraude moest worden voorkomen. Al deze digitale ontwikkelingen werden samengebracht in de ID-kaart die de burger fysiek bij zich moet dragen.

4.1.4 de cyberaanvallen van 2007

In 2007 ontstond er onrust in Estland doordat verschillende bevolkingsgroepen tegen over elkaar kwamen te staan omdat er tumult was ontstaan over de locatie van een standbeeld van een soldaat in een Sovjet-Unie uniform. Toen de overheid na een periode van protesten en anti-protesten besloot het standbeeld te verplaatsen naar een militaire begraafplaats, kwam de onrust tot een hoogtepunt en begonnen Russisch sprekende Estlanders zich digitaal te bewapenen met allerlei malware om de digitale infrastructuur van Estland te verlammen (Priisalu & Ottis, 2017). Vooral websites van de overheid en communicatiemiddelen van de overheid werden aangevallen en werden aangepast of platgelegd (Shackleford, 2010). Hoewel de systemen van Estland tegen de meeste van de manieren die werden gebruikt om de cyberaanvallen te plegen waren getest en sterk genoeg waren geacht, bleek door de enorme omvang van de hoeveelheid aanvallen toch dat de cyberveiligheid onvoldoende op orde was om alle aanvallen te keren (Priisalu & Ottis, 2017). Estland beweert dat dit de grootschaligste cyberaanval tot op heden is (e-estonia, 2022).

4.1.5 na de cyberaanvallen van 2007

Door de cyberaanvallen van 2007 ontstond er wantrouwen binnen de bevolking van Estland, die zich afvroeg of een verregaande digitale overheid wel wenselijk was als het zo kwetsbaar bleek voor kwaadwillende mensen. De overheid reageerde hierop door volledige openheid te geven over wat voor impact de cyberaanvallen hadden gehad. De schade leek erg mee te vallen. Persoonsgegevens van burgers waren niet in het gedrang gekomen en de systemen werden hersteld. Ook liet de overheid zien dat ze bezig waren om in de toekomst dergelijke aanvallen te weren. Door deze transparantie en de wil van de overheid om hun cybersecurity beter op orde te brengen, zorgden voor een herstel van vertrouwen bij de burgers (Priisalu & Ottis, 2017). Niet alleen in Estland zorgde de cyberaanvallen van 2007 voor actie richting sterkere cyberveiligheid (e-estonia, 2022) maar ook internationaal kwam cyberveiligheid meer op de kaart te staan.

4.2 Wat is de situatie met betrekking tot cyberveiligheid in Estland ná de implementatie van blockchain technologie?

4.2.1 Algemeen

Estland kent in de jaren na de implementatie van de KSI blockchain technologie een opbloeiende IT sector. Zo zijn in deze periode bijvoorbeeld de NATO Cooperative Cyber Defence Centre of Excellence en het EU Agency voor grootschalige IT systemen gevestigd in het land (Republic of Estonia Ministry of Foreign Affairs, 2021). Dit schetst een beeld waarbij Estland wordt gezien als expert op het gebied van digitalisering en cyber security.

4.2.2 X-Road

In de jaren na de implementatie van blockchain technologie bleef de X-Road erg belangrijk voor Estland. Het bleef de basis vormen waarop informatie werd opgeslagen en gedeeld. Het verschil met hoe de X-Road voor de implementatie van blockchain technologie werkte is dat het nu verbonden is met de KSI-blockchain om te zorgen dat de informatie niet te veranderen is en niet beschikbaar is voor onbevoegden.

De X-Road zelf maakt in deze periode een opmars op het internationaal toneel. In 2013 werd het eerste digitaal getekende internationaal verdrag getekend tussen Estland en Finland, om het onderhouden en verder uitbreiden van de X-Road technologie in samenwerking voort te zetten. Later zou Finland deze technologie dan ook implementeren (x-road.global, 2022).

4.2.3 KSI Blockchain

Keyless Signature Infrastructure (KSI) blockchain technologie is een blockchain die is ontworpen door een bedrijf genaamd Guardtime. Het verschil met een ‘normale’ blockchain is dat deze blockchain gebruik maakt van een ander soort autorisatie dan de doorsnee blockchain. Doordat de KSI blockchain geen cryptografische sleutels genereerd, maar een hash-functie cryptografie gebruikt om samen met de DLT het verificatieproces te realiseren (Guardtime, 2022). Guardtime stelt dat de KSI blockchain technologie twee grote zwakten van de gemiddelde blockchain oplost; de opschaalmogelijkheden en de afwikkelingstijd.

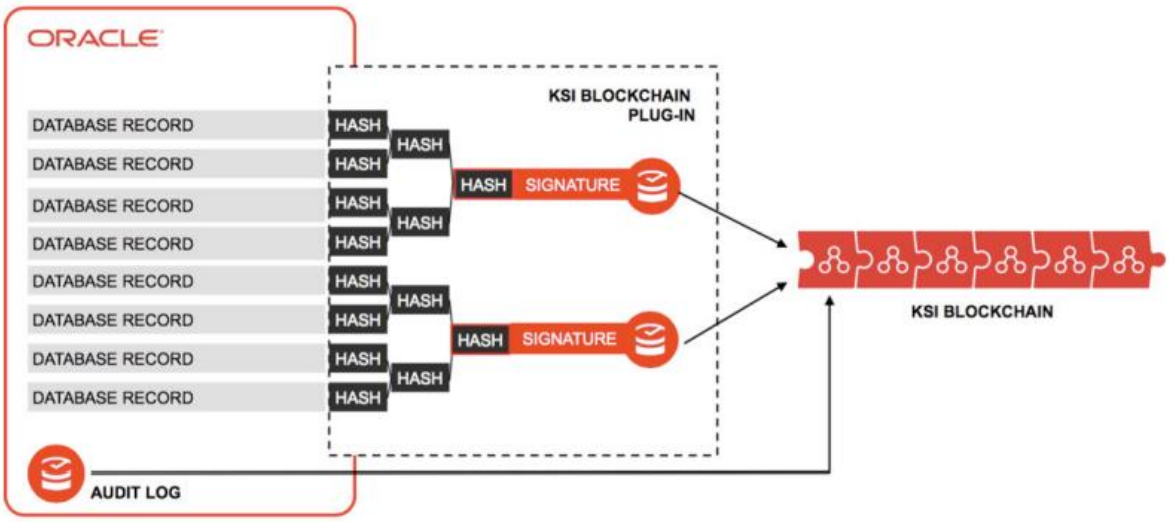
De zwakte van eerdere benaderingen van blockchain technologie op gebied van opschaalmogelijkheid is dat deze benaderingen opschalen aan de hand van een lineaire formule waarbij de variabele die de trend van de lijn bepaald, staat voor het aantal transacties. De KSI blockchain schaalt echter op door een lineaire formule waarbij de variabele die de trend van de lijn bepaald staat voor tijd. De opschaling is hier dus niet afhankelijk van het aantal transacties maar van de verlopen tijd. De zwakte van eerdere benaderingen van blockchain aangaande de afwikkelingstijd schuilt in het publieke aspect van veel benaderingen van blockchain technologie. Door de publieke aard moet het mogelijk zijn voor iedereen om toegang te krijgen tot de blockchain. Het verifiëren van data in een publieke blockchain duurt echter relatief lang, omdat er een Proof of Work (PoW) opgehaald moet worden die er voor zorgt dat de data juist is en door andere schakels geverifieerd en opgenomen kan worden. PoW is een vorm van een consensus protocol waarbij de computer een puzzel moet oplossen om te laten zien aan andere gebruikers van de blockchain dat een nieuw blok met data geverifieerd is en dus in de ketting kan worden toegevoegd, het antwoord van de puzzel kan hierbij snel worden geverifieerd door de andere gebruikers (Yaga et al., 2018). Doordat de KSI blockchain een private blockchain betreft, kan het aantal deelnemers in de blockchain worden gecontroleerd, waardoor de PoW niet meer nodig is en de data direct gesynchroniseerd kan worden (Guardtime, 2022). Tot slot stelt de ontwikkelaar van de KSI blockchain dat deze bestand is tegen ‘quantum computing’, een nieuw soort technologie waarbij met veel grotere aantallen data tegelijk kan worden gewerkt en dus ook met meer kracht kan worden gehackt.

4.2.4 KSI blockchain in Estland

Nu duidelijk is wat de KSI blockchain is en hoe het zich verhoud tot andere benaderingen van blockchain technologie is het van belang om de werking er van binnen de systemen van e-governance van Estland vast te stellen.

Zoals eerder genoemd, wordt de X-Road als de ruggengraat van het e-governance systeem van Estland gezien (e-estonia, 2022). Zelfs na de invoering van de KSI-blockchain technologie blijkt de X-Road nog altijd de belangrijkste schakel binnen het systeem te zijn. De data van Estland blijft in de X-Road en wordt dus niet opgeslagen in de KSI-blockchain zelf (PWC, 2019). In plaats daar van, wordt de KSI-blockchain gebruikt als plug-in en wordt de data gestempeld en worden de hashes opgeslagen binnen de KSI-blockchain (Semenzin, Rozas en Hassan, 2022). Wanneer een document of ander stuk data wordt aangepast, verandert deze hash ook, waardoor meteen zichtbaar is dat er een verandering heeft plaatsgevonden. Ook de originele data inclusief de originele hash blijven inzichtelijk binnen het blockchain systeem. Op deze manier kunnen veranderingen in datasets meteen worden gespot, waar het daarvoor gemiddeld zeven maanden duurde voor veranderingen in datasets ontdekt werden (PWC, 2019, pp. 7).

De KSI-blockchain is tevens niet over de hele breedte van het e-governance systeem in Estland uitgerold. De KSI-blockchain is actief in; de registratie van de gezondheidszorg, de eigendomsregistratie, de bedrijfsregistratie, de erf-registratie, het digitale rechtssysteem en de staatskrant (PWC, 2019; Semenzin, Rozas en Hassan, 2022).



Figuur 2: De werking van de Guardtime KSI-Blockchain als plug-in (Lõhmus, 2017, pp. 16.)

4.2.5 E-governance door de jaren

Om te bepalen welke trends omtrent cyberincidenten er spelen of gespeeld hebben binnen het e-governance beleid van Estland sinds het implementeren van de KSI-blockchain, zal overzichtelijk moeten worden gemaakt wat er per jaar is gebeurt binnen dit domein. Hierbij zal worden uitgegaan van incidenten aangaande de publieke sector. Hiervoor zullen vooral de evaluaties van de RIA worden gebruikt.

4.2.5.1 2012

In 2012, het jaar dat de KSI-blockchain op verschillende vlakken is geïmplementeerd, zijn er geen kritieke cyberincidenten gerapporteerd in Estland. Wel zijn er 41 significante incidenten door overheidsorganisaties gerapporteerd. Deze incidenten worden echter niet als kritiek beschouwd, aangezien deze incidenten niet tot serieuze veiligheidsproblemen hebben geleid (RIA, 2013).

Verder rapporteert de RIA een stagnering van de aantallen (pogingen tot) cybercriminaliteit en het opstellen van aanvullende wetgeving en maatregelen omtrent gedigitaliseerde processen.

4.2.5.2 2013

In het jaar 2013 zijn in totaal door de autoriteit 1164 meldingen in Estland (RIA, 2015). Daarvan zijn er 135 meldingen door overheidsorganisaties gerapporteerd, waarvan een kwart als moedwillige cyberaanvallen zijn bestempeld (RIA, 2014). 17% procent van alle meldingen zijn door de melders zelf geclassificeerd als kritiek, 15 procent van de meldingen als significant. Van de 135 meldingen, zijn er 116 geclassificeerd als daadwerkelijke cyberincidenten. Deze incidenten werden vaak veroorzaakt door aanvallen (25%), administratieve fouten (18%) en tekortkomingen in zowel hardware (16%) als software (15%).

De gerapporteerde aanvallen bestonden vooral uit georganiseerde ‘denial of service’ aanvallen (DDOS), geïsoleerde inbraken in informatiesystemen, geïsoleerde overnamen van service accounts en geïsoleerde gevallen van phishing e-mails.

De nuance bij deze rapportage is dat vanaf januari 2013 een wet is ingegaan waarbij overheidsorganisaties verplicht zijn cyberincidenten te rapporteren aan de RIA, waardoor het aantal meldingen naar verwachting is gestegen. Er kwamen 73 rapportages en meldingen binnen.

4.2.5.3 2014

In 2014 zijn door de autoriteit in totaal 1151 meldingen behandeld in Estland (Ria, 2015). Hiervan zijn 486 meldingen van cyberincidenten door overheidsorganisaties gerapporteerd. 20% van deze incidenten werd als kritiek geclassificeerd, ongeveer 30% als significant (RIA, 2015). 22% van alle gerapporteerde incidenten betreft aanvallen. 21% van de gerapporteerde incidenten werd als ‘overig’ geclassificeerd, de RIA stelt hierbij dat dit vaak ging om het uitvallen van stroom in bepaalde gebieden. 15% van de gerapporteerde incidenten werd geclassificeerd als administratieve fout. De andere incidenten werden geclassificeerd onder problemen met; software (19%), hardware (10%) en externe service providers (13%).

De aanvallen worden meer frequent en tevens meer divers, stelt de RIA. Daarom geeft het aan in 2015 een 24-uurs cybersecurity team te willen samenstellen om zo ook buiten kantoortijden in te kunnen grijpen bij calamiteiten.

4.2.5.4 2015

In 2015 zijn 5809 meldingen door de autoriteit in Estland behandeld. Hiervan zijn 402 meldingen van cyberincidenten door overheidsorganisaties gerapporteerd. 27% van deze incidenten werd als kritiek geclassificeerd (RIA, 2016). De overige distributie van de incidenten op gebied van zowel niveau van kritiek als de aard van de incidenten worden niet gerapporteerd door de RIA. Ze doen echter wel een aantal uitspraken. Zo zijn de vier vaakst voorkomende gevallen van cyberincidenten aanvallen, software problemen, externe service provider problemen en administratieve fouten.

De vier grootste cyber gevaren voor Estland zijn volgens de RIA (2016): cybercriminaliteit, cyber spionage, het gebruik van cyber tools in oorlogsvoering en het gebrek aan cybersecurity kennis, skills en gewaarwording bij gebruikers van digitale platformen. De RIA stelt zelfs dat menselijke fouten de grootste veroorzaker is bij de meeste serieuze cyber incidenten.

4.2.5.5 2016

De RIA (2017) stelt dat in 2016, 9135 meldingen door de autoriteit zijn behandeld in Estland. 20 tot 30 procent van alle meldingen over cyberincidenten werden door de melders gelinkt aan overheidsinstellingen. In totaal werden 1687 meldingen over zaken aangaande cyberspace tot de overheidssector gerekend. De RIA geeft hier voor de reden dat er vooral meer ingezet is door de organisaties om incidenten te melden. Veel van deze meldingen zou over mogelijke dreiging gaan en zijn dus niet geclassificeerd als cyberincident.

Naast technische mankementen en menselijke fouten, zijn de meeste cyberincidenten geclassificeerd als cyberaanvallen. Echter zijn deze aanvallen niet de voornaamste veroorzaker van kritieke incidenten. Deze zijn toe te schrijven aan menselijke fouten.

In de gezondheidszorg rapporteert de RIA meerdere randsomware gevallen. Dit houdt in dat een virus zich in een systeem nestelt, de data cryptisch opsluit en vervolgens gijzelt. De eigenaar van het systeem moet dan een geldbedrag betalen om de data weer in te kunnen zien. De grootste reden hiervoor is het gebrek aan kundige IT'ers binnen de gezondheidssector, aldus de RIA.

4.2.5.6 2017

De RIA (2018) rapporteert dat er in 2017, 10923 meldingen door de autoriteit zijn behandeld in Estland. Hiervan is in 3162 gevallen vastgesteld dat cyberincidenten hebben plaatsgevonden, waarvan 122 gevallen een hoge prioriteit hadden. Echter is niet gerapporteerd hoe veel van deze cyberincidenten in de publieke sector plaatsvonden. De distributie van cyberincidenten bij de overheidsinstellingen is wel gerapporteerd. Zo waren verschillende gevallen van het uitvallen van bepaalde diensten de grootste veroorzaker van cyberincidenten (59%), gevolgd door digitale inbraken (18%). Het aandeel van cyberincidenten door administratieve fouten bedraagt in 2017 vier procent.

De RIA stelt dat de grootste problemen voor cyberincidenten bij overheidsinstellingen worden veroorzaakt door het uitvallen van diensten door het niet naar behoren werken van IT voorwerpen of menselijke fouten.

In de sector gezondheidszorg rapporteert de RIA een groeiende trend van incidenten door aanvallen. Hoewel er geen cijfers worden genoemd, melden ze wel dat er meer gevallen zijn. Daarom pleit de RIA voor meer ondersteuning voor deze sector.

4.2.5.7 2018

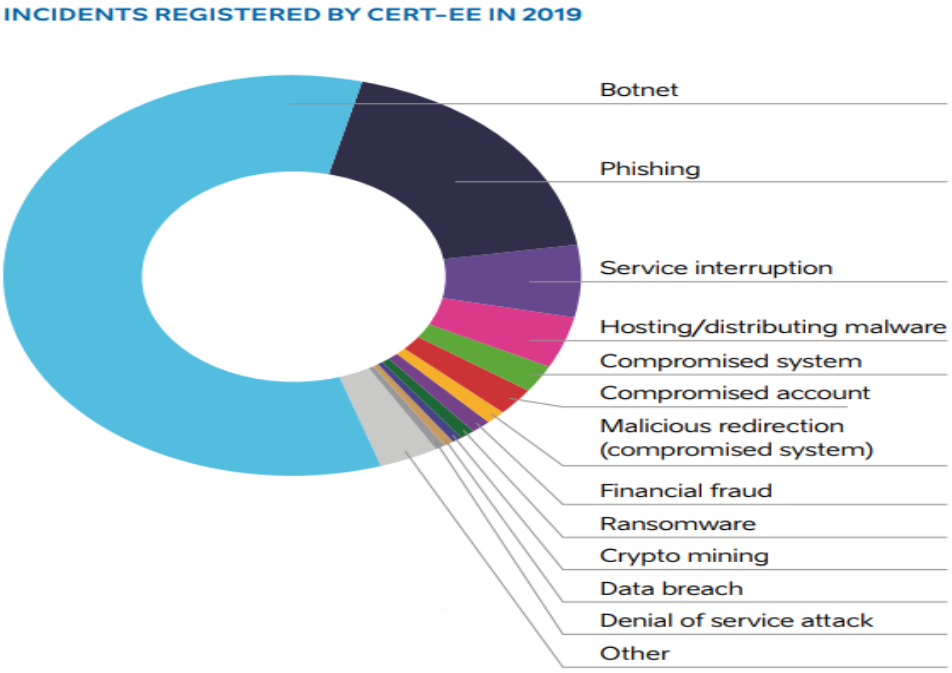
De RIA (2019) stelt in het rapport over 2018 dat er 17440 meldingen door de autoriteit zijn behandeld in Estland. Er worden geen uitspraken over het aandeel van de gemelde incidenten dat toebehoort aan de overheidsinstellingen. Ook de distributie van de cyberincidenten toegeschreven aan overheidsinstellingen is niet gerapporteerd.

De algemene trend laat bijna een verdubbeling van het aantal meldingen zien, waarvan er 3390 zijn bestempeld als incidenten. De meeste hiervan zijn geclassificeerd als malware en botnets.

4.2.5.8 2019

De RIA (2021) stelt dat de autoriteit in 2019, 24369 meldingen heeft behandeld in Estland. Hiervan werden 3164 meldingen geclassificeerd als cyberincident. In het rapport over 2019 (RIA, 2020) is wederom niet uitgesplitst wat het aandeel van cyberincidenten was die te maken hadden met overheidsinstellingen. Ook is de distributie van incidenten die betrekking hadden op de overheid niet weergegeven.

De algemene distributie van cyberincidenten is grafisch weergegeven, zonder vermelding van de statistiek. Zie figuur 3.



Figuur 3: Algemene distributie van cyberincidenten in Estland in 2019. (RIA, 2020, pp. 9)

4.2.5.9 2020

In het rapport van de RIA (2021) over het jaar 2020, wordt gesteld dat er dat jaar 22896 meldingen zijn behandeld door de autoriteit in Estland. Hiervan zijn er 2722 als cyberincidenten bestempeld, waarvan de meeste geclassificeerd zijn als botnet (28%) of phishing (26%) incidenten. Dit jaar zijn er ook veiligheidssystemen in werking gesteld die geautomatiseerde meldingen maken aan de autoriteit, dat waren er dit jaar 55635 (RIA, 2022).

Verder is wederom geen uitspraak gedaan over het aantal cyberincidenten die betrekking hadden op de overheidsinstellingen van het land. Ook niet over de distributie hier van.

Het rapport (RIA, 2021) schetst wel een beeld van een aantal aanvallen die gericht zijn op overheidsinstellingen, zo werden drie ministeries slachtoffer van cyberaanvallen, hierbij werd gevoelige informatie (gezondheidszorg) buitgemaakt. Ook werden meerdere pc's van overheidsinstellingen geïnfecteerd met Emotet, een virus. Ook vielen een aantal keer diensten die door overheidsinstellingen worden gebruikt om data te communiceren uit.

De gezondheidssector kende dertien incidenten waarbij diensten uitvielen.

4.2.5.10 2021

In 2021 zijn er 20077 meldingen door de autoriteit in Estland behandeld. Hiervan zijn er 2237 als cyberincidenten geclassificeerd(RIA, 2022). Het grootste deel hier van betreft phishing incidenten (ongeveer 35%). Het aantal geautomatiseerde meldingen was in dat jaar 73826.

Het rapport geeft niet weer wat het aantal cyberincidenten is dat zich in de publieke sector heeft gemanifesteerd. Ook de distributie hiervan is niet weergegeven.

Wel stelt het rapport vast dat in het algemeen het jaar 2021 grote zwakten van het e-governance systeem zijn blootgelegd. Zo werd bij de RIA zelf ingebroken en werden er bijna 300.000 foto's van medewerkers gestolen. Ook werd wereldwijd bekend dat Log4j, een IT-programma dat ook in Estland gebruikt wordt, door verouderde java-scripten erg kwetsbaar is geworden. In Estland werd deze zwakte uitgebuit door crypto miners te installeren op kwetsbare computers. Volgens RIA zijn deze miners opgespoord en verwijdert. Wel stelt de RIA dat er later eventueel wordt vastgesteld of er andere uitbuitingen van de zwakte heeft plaatsgevonden, bijvoorbeeld in de vorm van dataleks.

Ook heeft Estland vijftig procent meer DDOS aanvallen waargenomen. Ze spreken van een trend die zich al enkele jaren voordoet, maar de stijging in aantallen was nog niet eerder zo groot.

Een interessante opmerking in het rapport is dat de RIA probeert hackers de mogelijkheid te geven om de systemen te testen en ze te betalen wanneer ze kwetsbaarheden in de systemen communiceren met de RIA.

4.3 Wat zijn de risico's van het implementeren van blockchain technologie ter behoeve van de cyberveiligheid van digitale processen (in het algemeen)?

Het implementeren van nieuwe technologische tools brengt vaak niet alleen kansen met zich mee, maar ook knelpunten en valkuilen. Het is van belang om deze in kaart te brengen om verantwoord beleid gericht op het utiliseren van nieuwe technieken te kunnen opstellen. Om deze reden zullen de risico's van het implementeren van blockchain technologie in kaart worden gebracht.

Een van de risico's van de implementatie van blockchain technologie is het design risico. Berawi et al. (2021) stellen dat een blockchain slechts zo sterk is als zijn zwakste schakel. Daarnaast moet de hoeveelheid schakels hoog genoeg zijn, want in theorie kan het systeem gehackt worden als er een poging plaatsvind waarbij de kracht van de computers die de hack doen minimaal 51% van de kracht heeft van de computers binnen de blockchain (Dennis, Owenson en Aziz, 2016). Er moet dus goed worden nagedacht over hoe het blockchain systeem in elkaar dient te steken.

Een ander risico bij de implementatie van blockchain is de veiligheid en de toegang tot data. Wanneer blockchain technologie gebruikt wordt door organisaties, is het goed denkbaar dat niet alle informatie voor alle gebruikers beschikbaar dient te zijn. Hoe meer schakels er binnen een systeem zijn, hoe minder veilig het werken met privé 'sleutels' wordt. Zelfs als documenten worden opgeslagen via het hash-systeem, blijft er metadata aan de hashes hangen waardoor derden de aard van de opgeslagen data en degene die betrokken zijn bij de data achterhaald worden (Prewett, Prescott en Phillips, 2020).

Nog een risico van het implementeren van blockchain technologie is het opslaan van data. In principe is het zo dat in een blockchain, alle versies van alle data bewaard worden (Dennis, Owenson en Aziz, 2016). Deze grote hoeveelheid data dient ergens te worden opgeslagen. In een traditionele blockchain gebeurt dit in iedere schakel. Maar er zijn ook modellen waarbij blockchain en andere manieren van opslag, bijvoorbeeld cloud-based opslag, worden gebruikt (Berawi et al, 2021). Hoewel het probleem van de fysieke opslag hierdoor worden opgelost, dienen zich andere problemen aan. Zo stellen Alketbi et al. (2018) dat, bij opslag van informatie door overheden, er een 'right to be forgotten' bestaat. Dit houdt in dat bepaalde documenten na verloop van tijd worden verwijdert, om de privacy van burgers of medewerkers te beschermen. Dit kan verholpen worden door een 'temperol' blockchain model op te stellen, waarbij oude datasets uit de blockchain worden verwijdert (Dennis, Owenson en Aziz, 2016). Dit zorgt op zijn beurt echter weer voor een afbreuk aan de transparantie, een van de grootste selling-points van blockchain technologie.

Een ander risico van het implementeren van blockchain technologie is de afhankelijkheid van aanbieders (White, King en Holladay, 2020). Omdat blockchain technologie zo nieuw en zo complex is, wordt het vaak uitbesteed. Echter is het zo dat veel van de aanbieders nog in de start-up fase zijn en dat er daarnaast afspraken gemaakt dienen te worden over bijvoorbeeld het onderhoud van de blockchain.

Het laatste risico dat zal worden besproken is het sleutel management. Het consensus protocol van een blockchain zorgt er voor dat de data gebundeld en beschermd wordt opgeslagen. Deze data moet vervolgens worden geopend met een sleutel. De sleutel kan publiek of privé zijn. Wanneer de sleutel publiek is, kan iedereen de data inzien. Wanneer de sleutel privé is, kan alleen degene die de sleutel heeft, de data inzien (Alketbi et al., 2018; Prewett, Prescott en Phillips, 2020). Wanneer de sleutel echter kwijtraakt of gestolen wordt, kan de originele eigenaar van de sleutel helemaal niets meer en heeft de dief of iemand die de sleutel vind, toegang tot alle data. Daarnaast zou de sleutel gedupliceerd kunnen worden en kan met de neppe sleutel toegang tot de data worden verkregen (Alketbi et al., 2018).

4.4 Analyse

4.4.1 Wat was de situatie met betrekking tot cyberveiligheid in Estland vóór de implementatie van blockchain technologie?

In de periode voor de implementatie van blockchaintechnologie in Estland was het land al een van de toonaangevende landen met betrekking tot e-governance. Met het invoeren van de X-Road is een grote stap gezet naar een goed functionerende digitale overheid. Echter is gebleken dat deze verregaande digitalisering niet alleen kansen met zich meebrengt, ook zwakten. Met als impactvolle gebeurtenis de cyberaanvallen van 2007, werd duidelijk dat het land zichzelf beter moest gaan wapenen tegen cyberincidenten om de samenleving te beschermen tegen dergelijke disruptieve incidenten. Het niveau van cyberveiligheid moest dus worden verhoogd.

4.4.2 Wat was de situatie met betrekking tot cyberveiligheid in Estland ná de implementatie van blockchain technologie?

Estland heeft gekozen om de KSI-Blockchain te implementeren. Dit is een private blockchain die als een plug-in functioneert. Data wordt niet opgeslagen binnen de blockchain zelf, maar in de databases die Estland zelf kiest. Wel wordt data gehasht en de hashes worden opgeslagen in de blockchain. Dit zou er voor moeten zorgen dat de data slechts door bevoegden kunnen worden ingezien en niet ongezien aangepast kunnen worden, daarmee zou de cyberveiligheid van deze datasets sterker moeten zijn. De blockchain is echter niet overal geïmplementeerd, slechts in een aantal velden. De verzamelde data (zie bijlage 1) laat een verhoging zien in het aantal meldingen dat jaarlijks gedaan wordt. De data laat in de laatste jaren een vermindering in het totaal aantal cyberincidenten in het land zien. Estland wordt echter regelmatig getroffen door kritische cyberincidenten, ook in de sectoren waar de KSI-blockchain actief is.

Interessant aan de verzamelde data is dat de RIA in geen enkel van de evaluaties uitspraken doet over de daadwerkelijke effectiviteit van de KSI blockchain. Het woord ‘blockchain’ wordt zelfs in alle documenten samen slechts twee maal genoemd.

4.4.3 Wat zijn de risico’s van het implementeren van blockchain technologie ter behoeve van de cyberveiligheid van digitale processen (in het algemeen)?

De implementatie risico’s die geïdentificeerd zijn in het onderzoek zijn; het design risico, de veiligheid van en de toegang tot data, het opslaan van data, de afhankelijkheid van aanbieders en het sleutelmanagement.

5. Conclusie en discussie

5.1 Conclusie

Allereerst is het van belang te melden dat binnen dit onderzoek is getracht uitsluitend te meten wat de impact van blockchain technologie is geweest op gebied van cybersecurity in Estland, andere factoren die wellicht invloed hebben gehad op het niveau van cybersecurity zijn binnen dit onderzoek niet uitgelicht.

De hoofdvraag van dit onderzoek is de vraag wat de impact van blockchain technologie op gebied van de cyberveilgheid in Estland is. De resultaten van dit onderzoek wijst op twee mogelijke gebieden van impact; de snellere opsporing van cyberincidenten en de publiciteit die het gebruik van de technologie met zich meebrengt.

Het hashing systeem van de KSI-blockchain zorgt er voor dat de autoriteit die verantwoordelijk is voor cybersecurity in Estland bijna tegelijk met een incident kan identificeren welke data is getroffen. Dit lijkt echter alleen te gelden voor incidenten waarbij daadwerkelijk data wordt veranderd of ontvreemd.

De publiciteit die Estland heeft verkregen door zich te profileren als blockchain pionier, kan hebben bijgedragen aan de status die Estland heeft verworven binnen het veld van cybersecurity. Die status heeft op zijn beurt weer een mogelijk effect gehad op het binnenhalen van de organisaties van de NATO en de EU aangaande cyberveiligheid en grootschalige IT projecten. Deze link is echter niet empirisch bewezen.

Deze twee mogelijke gebieden van impact staan in contrast met de literatuur, waar van een grotere impact wordt uitgegaan. De onderzoeker deelt de mening van de crypto anarchisten dat de KSI-blockchain niet gezien kan worden als een volwaardige blockchain. Dit omdat deze toepassing louter gebruikt maakt van het hashing systeem. Daarom zou, in de mening van de onderzoeker, eerder gesproken moeten worden van een hashing plug-in dan van een blockchain. Daarnaast wordt de plug-in slechts gebruikt in een aantal velden.

Met betrekking tot de cyberveiligheid is in de laatste jaren waarover data verzameld is een vermindering van het totaal aantal cyberincidenten in Estland waargenomen. Deze daling is echter op basis van deze data niet toe te schrijven aan het gebruik van blockchain technologie, omdat de data in deze jaren niet meer per beleidsveld wordt gecommuniceerd. Hierdoor is onderlinge vergelijking met de situatie in andere velden niet mogelijk. Daarnaast hebben in deze jaren de beleidsvelden waar de KSI-blockchain actief is zich een aantal kritische cyberincidenten voorgedaan, waardoor kan worden aangenomen dat de KSI-blockchain niet alle cyberincidenten heeft kunnen stoppen.

De implementatie uitdagingen die vastgesteld zijn in het theoretisch kader lijken door de ontwikkelaars van de KSI-blockchain goed te zijn bestudeerd. Alle drie lijken ze in acht te zijn genomen bij het ontwerpen van de plug-in. Echter lijken ze daarbij de effectiviteit van de blockchain uit het oog te zijn verloren, want dit onderzoek wijst op een gering effect van de KSI-blockchain.

Een positief effect van het design van de KSI-blockchain toepassing lijkt te zijn dat het een aantal van de vastgestelde implementatierisico's ontwijkt. Zo kan de toepassing erg sterk worden opgeschaald, behoeft het geen gegevensopslag door derden, wordt er geen gebruik gemaakt van sleutels en kan een gebruiker zelf bepalen welke data het behoud en welke data niet. Andere risico's blijven bestaan, zo is Estland bij het gebruik van de KSI-blockchain nog altijd afhankelijk van de aanbieder, Guardtime. Ook blijft het risico bestaan dat de oudere, soms kwetsbare systemen nog altijd de basis vormen van de digitale infrastructuur in Estland, omdat de KSI-blockchain als plug-in functioneert.

Al met al concludeert de onderzoeker dat de blockchain technologie zoals deze is toegepast in Estland een geringe impact heeft gehad.

5.2 Discussie

Dit onderzoek kent een aantal beperkingen. Zo was niet alle data beschikbaar die de onderzoeker ter beschikking dacht te krijgen. In het vooronderzoek zijn een aantal evaluaties van de RIA bekeken en hier werd de distributie van het aantal – en de aard van – cyberincidenten per veld gemaakt. Echter bleek dit later niet in ieder evaluatie rapport te gelden. Hierdoor kon in de laatste periode die onderdeeldeel was van het onderzoek niet worden uitgesplitst wat de situatie met betrekking tot cyberincidenten specifiek voor overheidsinstellingen was. Hierdoor konden met betrekking tot die perioden louter uitspraken gedaan worden over de algemene situatie in Estland in plaats van een sterke vergelijking per jaar. Er werd in de documenten wel gesproken over ingrijpende cyberincidenten die zich voordeden binnen bepaalde beleidsterreinen die onderdeel waren van het onderzoek, waardoor toch enige uitspraak gedaan kon worden over eventuele trends.

Er lijkt binnen de literatuur geen algemeen geaccepteerde definitie van blockchain technologie te gelden. Waar bij de opzet van dit onderzoek werd uitgegaan van een toepassing van blockchain technologie in haar traditionele vorm, bleek de aard van de blockchain toepassing in Estland wezenlijk anders. Hierdoor waren een aantal, volgens de literatuur kenmerkende eigenschappen van blockchain technologie, niet aanwezig en dit kan invloed hebben gehad op de generaliseerbaarheid van dit onderzoek.

Tot slot is de impact van een technologie vaak breder dan de daadwerkelijke output en de theoretische verbanden. Echter zijn, door de omvang van dit onderzoek en de tijd die de onderzoeker had om dit onderzoek uit te voeren, niet alle mogelijke elementen van impact onderzocht.

5.2.1 Verder onderzoek

Allereerst is het van belang dat de wetenschap een algemeen geaccepteerde werkbare definitie van blockchain technologie vast weet te stellen. Aangezien er een groot deel elementen zijn binnen de technologie die elk los van elkaar kunnen worden geütiliseerd door diverse sectoren, is het van belang dat duidelijk is voor eenieder wanneer er gesproken kan worden over een blockchain technologie en wanneer er gesproken dient te worden over een technologisch aspect van deze technologie.

Daarnaast zijn er nog erg weinig wetenschappelijke onderzoeken naar de praktische werking van blockchain technologie in de publieke sector, hoewel de literatuur uitwijst dat er in verschillende landen mee wordt geëxperimenteerd. Een framework om de onderzoeken naar de praktische werking van de verschillende vormen van blockchain mee te analyseren zou hierbij kunnen helpen, deze moet echter eerst worden ontwikkeld.

Literatuurlijst

Alketbi, A., Nasir, Q., Talib, M.A., 2018. Blockchain for Government Services-Use Cases, Security Benefits and Challenges. *In:* 2018 15th Learning and Technology Conference (L&T), pp. 112–119, Jeddah, Saudi Arabia

Badzar, A. (2016). *Blockchain for securing sustainable transport contracts and supply chain transparency.* [Masters Thesis, Lund University]. Lund University Publications. https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8880383&fileOId=8880390

Berawi, M. A., Sari, M., Addiani, F. A. F., & Madyaningrum, N. (2021). Developing a Blockchain-based Data Storage System Model to Improve Government Agencies' Organizational Performance. *International Journal of Technology*, *12*(5), 1038. https://doi.org/10.14716/ijtech.v12i5.5237

Castellanos, A., & Benbunan-Fich, R. (2018, 13 december). *Digitalization of Land Records: From Paper to Blockchain*. ResearchGate.Net. Geraadpleegd op 15 mei 2022, van https://www.researchgate.net/publication/329222337_Digitalization_of_Land_Records_From_Paper_to_Blockchain

Center for Strategic and International Studies. (2022). *Significant Cyber Incidents*. Geraadpleegd op 19 april 2022, van https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Cong, L. W., & He, Z. (2019). Blockchain Disruption and Smart Contracts. *The Review of Financial Studies*, *32*(5), 1754–1797. https://doi.org/10.1093/rfs/hhz007

Dennis, R., Owenson, G., & Aziz, B. (2016). A Temporal Blockchain: A Formal Analysis. *2016 International Conference on Collaboration Technologies and Systems (CTS)*. https://doi.org/10.1109/cts.2016.0082

EVRY. (2020). *Blockchain: Powering the Internet of Value*. Finyear. https://www.finyear.com/attachment/637653/

Galen, D., Brand, N., Boucherle, L., Davis, R., Do, N., El-Baz, B., Kimura, I., Wharton, K., & Lee, J. (2018). *Blockchain for Social Impact Moving beyond the hype*. Stanford Business Center for Social Innovation. https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/study-blockchain-impact-moving-beyond-hype.pdf

Garg, K., Saraswat, P., Bisht, S., Aggarwal, S. K., Kothuri, S. K., & Gupta, S. (2019, April). A comparitive analysis on e-voting system using blockchain. In *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)* (pp. 1-4). IEEE.

Guardtime. (2022). *KSI data sheet*. guardtime.com. Geraadpleegd op 16 mei 2022, van https://m.guardtime.com/files/KSI_data_sheet_201509.pdf

Hill, J.F., 2014. The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders. In: The Hague Institute for Global Justice, Conference on the Future of Cyber Governance

Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018, July). Blockchain-based e-voting system. In *2018 IEEE 11th international conference on cloud computing (CLOUD)* (pp. 983-986). IEEE.

Hölbl, M., Kompara, M., Kamišalić, A., & Nemec Zlatolas, L. (2018). A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry*, *10*(10), 470. https://doi.org/10.3390/sym10100470

Husain, S. O. (2020, mei). (De)coding a technopolity Tethering the civic blockchain to political transformation. Wageningen University. https://doi.org/10.18174/514268

Irion, K. (2013). Government Cloud Computing and National Data Sovereignty. *Policy and Internet*, *4*(3–4), 40–71. https://doi.org/10.1002/poi3.10

Kotka, T., & Liiv, I. (2015). Concept of Estonian Government Cloud and Data Embassies. *Electronic Government and the Information Systems Perspective*, 149–162. https://doi.org/10.1007/978-3-319-22389-6_11

Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, *39*, 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

KSI Blockchain. (2021, 15 november). E-Estonia. Geraadpleegd op 15 mei 2022, van https://e-estonia.com/solutions/cyber-security/ksi-blockchain/

Lindman, J., Tuunainen, V. K., & Rossi, M. (2017). Opportunities and risks of Blockchain Technologies–a research agenda.

Lõhmus, I. (2017). *Securing Public Services with Blockchain* [Presentatieslides]. Guardtime. https://www.maaamet.ee/pcc2017/docs/PCC_11_Lohmus_Estonia_Blockchain_Guardtime.pdf

Mattila, J. (2016). *EconStor: The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures*. Econstor.Eu. Geraadpleegd op 15 mei 2022, van https://www.econstor.eu/handle/10419/201253

Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy Challenges. *Internet of Things*, *8*, 100107. https://doi.org/10.1016/j.iot.2019.100107

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2020). *Cybersecuritybeeld Nederland 2020*. https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020

Nordic Institute For Interoperability Solutions. (2022). *X-Road® History*. X-Road.Global. Geraadpleegd op 15 mei 2022, van https://x-road.global/xroad-history

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT Integration: A Systematic Survey. *Sensors*, *18*(8), 2575. https://doi.org/10.3390/s18082575

Pilkington, M., (2016). Blockchain technology. Olleros, F., Zhegu, M.,(Reds.), *Research Handbook on Digital Transformations* (pp. 225-251). Edward Elgar Publishing. 10.4337/9781784717766

Prewett, K. W., Prescott, G. L., & Phillips, K. (2020). Blockchain adoption is inevitable—Barriers and risks remain. *Journal of Corporate Accounting & Finance*, *31*(2), 21–28. https://doi.org/10.1002/jcaf.22415

Priisalu, J., & Ottis, R. (2017). Personal control of privacy and data: Estonian experience. *Health and Technology*, *7*(4), 441–451. https://doi.org/10.1007/s12553-017-0195-1

PWC. (2019). Estonia - the Digital Republic Secured by Blockchain. https://www.pwclegaltech.com/wp-content/uploads/2018/10/Estonia-the-Digital-Republic-Secured-by-Blockchain.pdf

Rathee, T., & Singh, P. (2021). A systematic literature mapping on secure identity management using blockchain technology. *Journal of King Saud University - Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2021.03.005

Republic of Estonia Ministry of Foreign Affairs. (2021). *Cyber Security*. vm.ee. Geraadpleegd op 15 mei 2022, van https://vm.ee/en/cyber-security

Riigi Infosüsteemi Amet. (2013). *Summary of the Estonian Information System's Authority on ensuring cyber security in 2012*. https://www.ria.ee/en/information-system-authority/publications.html

Riigi Infosüsteemi Amet. (2014). *2013 Annual Report Cyber Security Branch of the Estonian Information System Authority*. https://www.ria.ee/en/information-system-authority/publications.html

Riigi Infosüsteemi Amet. (2015). *2014 Annual Report Cyber Security Branch Of the Estonian Information System Authority*. https://www.ria.ee/en/information-system-authority/publications.html

Riigi Infosüsteemi Amet. (2016). *2015 Annual Report of the Estonian Information System Authority's Cyber Security Branch*. https://www.ria.ee/en/information-system-authority/publications.html

Riigi Infosüsteemi Amet. (2017). *Annual Cyber Security Assessment 2017 Estonian Information System Authority*. https://www.ria.ee/en/information-system-authority/publications.html

Riigi Infosüsteemi Amet. (2018). *Estonian Information System Authority Annual Cyber Security Assessment 2018*. https://www.ria.ee/en/information-system-authority/publications.html

Riigi Infosüsteemi Amet. (2019). *Estonian Information System Authority Annual Cyber Security Assessment 2019*. https://www.ria.ee/en/information-system-authority/publications.html

Riigi Infosüsteemi Amet. (2020). *Cyber Security In Estonia 2020*. https://www.ria.ee/en/information-system-authority/publications.html

Riigi Infosüsteemi Amet. (2021). *Cyber Security in Estonia 2021*. https://www.ria.ee/en/information-system-authority/publications.html

Riigi Infosüsteemi Amet. (2022). *Cyber Security in Estonia 2022*. https://www.ria.ee/en/information-system-authority/publications.html

Rijksprogramma Duurzaam Digitale Informatiehuishouding. (2020, 12 oktober). *Rijksprogramma Duurzaam Digitale Informatiehuishouding*. Digitale Overheid. Geraadpleegd op 1 april 2022, van https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/leren-en-ontwikkelen/rijksprogramma-duurzaam-digitale-informatiehuishouding/#:%7E:text=De%20informatiehuishouding%20omvat%20de%20opslag,zelfs%20een%20bierviltje%20met%20afspraken.

Samy, H., Tammam, A., Fahmy, A., & Hasan, B. (2021). Enhancing the performance of the blockchain consensus algorithm using multithreading technology. *Ain Shams Engineering Journal*, *12*(3), 2709–2716. https://doi.org/10.1016/j.asej.2021.01.019

Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017). Survey of consensus protocols on blockchain applications. *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*. https://doi.org/10.1109/icaccs.2017.8014672

Semenzin, S., Rozas, D., & Hassan, S. (2022). Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia. *Policy and Society*. https://doi.org/10.1093/polsoc/puac014

Shackelford, S. J. (2010). Estonia Two-and-A-Half Years Later: A Progress Report on Combating Cyber Attacks. *Journal of Internet Law*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1499849

Story. (2022, 2 februari). E-Estonia. Geraadpleegd op 15 mei 2022, van https://e-estonia.com/story/

United Nations. (2020). *E-Government Survey 2020*. https://publicadministration.un.org/en/Research/UN-e-Government-Surveys

Van Heel, L. (2017, 26 december). *Cyberaanval ontwrichtte haven: "Het blijft niet bij deze hack"*. AD.nl. Geraadpleegd op 19 april 2022, van https://www.ad.nl/rotterdam/cyberaanval-ontwrichtte-haven-het-blijft-niet-bij-deze-hack~a9df8631/?referrer=https%3A%2F%2Fwww.google.com%2F

Wang, M., Wu, Y., & Chen, B., & Evans, M. (2020). Blockchain and Supply Chain Management: A New Paradigm for Supply Chain Integration and Collaboration. *Operations and Supply Chain Management: An International Journal*, 14(1), 111-122.

Wang, J., Wu, P., Wang, X., & Shou, W. (2017). The outlook of blockchain technology for construction engineering management. *Frontiers of Engineering Management*, *4*(1), 67. https://doi.org/10.15302/j-fem-2017006

Wassens, R. (2022, 24 maart). *'Kans op gerichte cyberaanval op Rotterdamse haven is reëel'*. NRC. Geraadpleegd op 19 april 2022, van https://www.nrc.nl/nieuws/2022/03/24/roep-de-haven-maar-uit-tot-crisisgebied-a4104937

White, B. S., King, C. G., & Holladay, J. (2020). Blockchain security risk assessment and the auditor. *Journal of Corporate Accounting & Finance*, *31*(2), 47-53.

Whitman, M. E., & Mattord, H. J. (2018). *Management of Information Security*. Cengage Learning.

Wouda, H. P., & Opdenakker, R. (2019). Blockchain technology in commercial real estate transactions. *Journal of Property Investment & Finance*, *37*(6), 570–579. https://doi.org/10.1108/jpif-06-2019-0085

X-Road. (2021, 15 november). E-Estonia. Geraadpleegd op 15 mei 2022, van https://e-estonia.com/solutions/interoperability-services/x-road/

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview. *National Institute of Standards and Technology Internal Report*. https://doi.org/10.6028/nist.ir.8202

Zhong, B., Wu, H., Ding, L., Luo, H., Luo, Y., & Pan, X. (2020). Hyperledger fabric-based consortium blockchain for construction quality information management. *Frontiers of Engineering Management*, *7*(4), 512–527. https://doi.org/10.1007/s42524-020-0128-y

Bijlagen

Bijlage 1: Overzicht van meldingen van cyberincidenten volgens de RIA

	Automatische meldingen	Handmatige Meldingen	Cyberincidenten algemeen	Cyberincidenten overheid	Verschil in cyberincidenten in het algemeen t.o.v. het jaar er voor	Verschil in cyberincidenten in de publieke sector t.o.v. het jaar er voor
2012	-	-	-	41	-	-
2013	-	1164	-	116	-	+ 75
2014	-	1151	-	-	-	-
2015	-	5809	-	-	-	-
2016	-	9135	-	-	-	-
2017	-	10923	3162	-	-	-
2018	-	17440	3390	-	+ 228	-
2019	-	24369	3164	-	- 226	-
2020	55635	22896	2722	-	- 442	-
2021	73826	20077	2237	-	- 485	-

Bijlage 2: Literatuurlijst van wetenschappelijke bronnen die zijn gebruikt bij de beantwoording van de deelvragen

Alketbi, A., Nasir, Q., Talib, M.A., 2018. Blockchain for Government Services-Use Cases, Security Benefits and Challenges. *In:* 2018 15th Learning and Technology Conference (L&T), pp. 112–119, Jeddah, Saudi Arabia

Berawi, M. A., Sari, M., Addiani, F. A. F., & Madyaningrum, N. (2021). Developing a Blockchain-based Data Storage System Model to Improve Government Agencies' Organizational Performance. *International Journal of Technology*, *12*(5), 1038. https://doi.org/10.14716/ijtech.v12i5.5237

Dennis, R., Owenson, G., & Aziz, B. (2016). A Temporal Blockchain: A Formal Analysis. *2016 International Conference on Collaboration Technologies and Systems (CTS)*. https://doi.org/10.1109/cts.2016.0082

Prewett, K. W., Prescott, G. L., & Phillips, K. (2020). Blockchain adoption is inevitable—Barriers and risks remain. *Journal of Corporate Accounting & Finance*, *31*(2), 21–28. https://doi.org/10.1002/jcaf.22415

Priisalu, J., & Ottis, R. (2017). Personal control of privacy and data: Estonian experience. *Health and Technology*, *7*(4), 441–451. https://doi.org/10.1007/s12553-017-0195-1

Semenzin, S., Rozas, D., & Hassan, S. (2022). Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia. *Policy and Society*. https://doi.org/10.1093/polsoc/puac014

Shackelford, S. J. (2010). Estonia Two-and-A-Half Years Later: A Progress Report on Combating Cyber Attacks. *Journal of Internet Law*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1499849

White, B. S., King, C. G., & Holladay, J. (2020). Blockchain security risk assessment and the auditor. *Journal of Corporate Accounting & Finance*, *31*(2), 47-53.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview. *National Institute of Standards and Technology Internal Report*. https://doi.org/10.6028/nist.ir.8202