Blockchain voor SURFnet en aangesloten instellingen

Een technologieverkenning

Utrecht, november 2017
Versienummer: 1.0

Colofon

Blockchain voor SURFnet en aangesloten instellingen
Een technologieverkenning

SURF
Postbus 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

Auteurs
Willem Noort (Innovalor), Maarten Wegdam (Innovalor)

Reviewers
Joost van Dijk (SURFnet), Martijn Oostdijk (Innovalor), Timothy Sealy (Saxion Enschede / InnoValor), Bas Zoetekouw (SURFnet), Frans Ward (SURFnet), Arnout Terpstra (SURFnet), Wladimir Mufty (SURFnet)

SURF is de ICT-samenwerkingsorganisatie van het Nederlandse hoger onderwijs en onderzoek.
Deze publicatie is digitaal beschikbaar via de website van SURF: www.surf.nl/publicaties

Inhoudsopgave

Management Summary

Blockchain is ‘hot’, een nieuwe technologie die volgens velen een grote impact kan hebben op hoe vertrouwen online werkt. Aandacht gaat met name uit naar Bitcoin en de financiële sector, maar ook voor SURFnet en haar achterban in het onderwijs en onderzoek zou de impact groot kunnen zijn. Deze whitepaper is het resultaat van een technologieverkenning die InnoValor voor en met SURFnet heeft gedaan naar blockchain. Doel van de whitepaper is SURFnet te helpen om te bepalen waar eventuele mogelijkheden van blockchain liggen voor SURFnet en haar instellingen. Een tweede doel is om op basis van deze verkenning de discussie met haar achterban over blockchain aan te kunnen gaan.

Blockchain kan gerust een hype genoemd worden. In negatieve zin een hype omdat de impact overdreven wordt; in positieve zin omdat veel mensen grote impact verwachten. In deze whitepaper proberen we hier nuance in aan te brengen door niet alleen de mogelijkheden van Blockchains te beschrijven, maar criteria te definiëren voor welke problemen blockchain kan worden ingezet. Ook werken we gebruik makend van deze criteria een aantal use cases uit om te illustreren hoe blockchain wel of niet gebruikt kan worden voor SURFnet en haar achterban.

Onze aanpak voor deze technologieverkenning bestond uit literatuuronderzoek, een analyse van een groot aantal blockchain-initiatieven en diverse sessies met, met name, SURFnetters om onze bevindingen te toetsen en input te krijgen over de toepassingen voor SURFnet en haar achterban. Gezien de hoeveelheid aandacht voor en rapporten over blockchain bleek dit niet triviaal, we pretenderen dan ook niet compleet en volledig actueel te zijn.

Wat is blockchain?

Blockchain is een nieuwe decentrale databasetechnologie die volgens sommigen een deel van de diensten van onder andere banken, notarissen of zelfs overheden overbodig zou kunnen maken. Technisch gezien is een blockchain letterlijk een lange keten van virtuele blokken die regelmatig wordt aangevuld met een nieuw blok waarin de recentste veranderingen van de database als een lijst van transacties is opgenomen. Hiermee is het niet zomaar mogelijk om blokken uit het verleden aan te passen. Blockchain is decentraal, elke deelnemer die gebruik maakt van een blockchain heeft de beschikking over een eigen kopie van alle blokken. Hierdoor is er ook een hoge mate van transparantie voor alle geïnteresseerden. Blockchains hebben een relatief lage capaciteit om data in op te slaan, waardoor het slecht vergelijkbaar is met een reguliere database. Belangrijk aan blockchain is dat de blockchain protocollen ervoor zorgen dat er consensus ontstaat over welke informatie in de blockchain mag worden opgenomen. Eenvoudig gezegd bepaalt de meerderheid van de deelnemers daardoor wat de ‘waarheid’ is.

De bekendste blockchain implementatie is Bitcoin, maar er bestaan veel andere implementaties waarvan Ethereum een bekende en na bitcoin waarschijnlijk meest volwassen is. Een generalisatie van blockchain is distributed ledger technologie, in deze whitepaper blijven we bewust weg van de nuances tussen blockchain en distributed ledgers omdat dit voor deze verkenning niet relevant is.

Wanneer is blockchain een geschikte oplossing?

Hieronder definiëren we vijf belangrijke criteria waaraan een toepassing zou moeten voldoen wil blockchain een geschikte oplossing zijn. Deze zijn niet uitputtend en hoeven niet alle vijf altijd te gelden, maar als ze niet, of maar heel beperkt, gelden dan is het wel de vraag of blockchain de juiste oplossing is:

1. **Wantrouwen** – Een uitgangspunt van blockchains is dat er sprake is van wantrouwen tussen partijen over de informatie opgeslagen in een gezamelijke database en de veranderingen daarvan. Om dit wantrouwen weg te nemen worden er gebruik gemaakt van complexe wiskundige berekeningen en protocollen om de integriteit te van de data te beschermen.
2. **Geen Trusted Third Party** – De traditionele oplossing van een meer centralistische TTP is ongewenst vanwege kosten of wantrouwen. Specifiek is blockchain geschikt als de TTP niet wordt vertrouwd met het correct uitvoeren van databasemutaties.
3. **Transparantie** – Transparantie is een doel, of zo niet, dan is het in ieder geval geen bezwaar. Alle informatie die is opgeslagen in een blockchain is inzichtelijk voor alle deelnemers. Aangezien er alleen blokken kunnen worden toegevoegd aan de keten, kan er ook geen informatie uit een blockchain verdwijnen. Dit is bijvoorbeeld een probleem bij het verwerken van persoonlijke data, *right to be forgotten* is erg lastig te implementeren of zelfs onmogelijk. Overigens zijn er wel maatregelen mogelijk om identiteiten op de blockchain te pseudonimiseren, zodat transparantie daarvoor geen vereiste is.
4. **Meerdere schrijvers** – Om een blockchain meerwaarde te laten bieden boven een TTP, is het noodzakelijk dat er meerdere onafhankelijke partijen zijn die de blokken maken (miners).
5. **Werkend businessmodel voor mining** – 'Traditionele' blockchains zoals bitcoin brengen hoge investeringen en operationele kosten met zich mee om voldoende rekenkracht te krijgen. Dit is bovendien belastend voor het milieu. Er moet daarom wel een businessmodel bestaan waarin het voor de deelnemers aantrekkelijk is om deze investeringen te doen.

Use cases voor SURFnet en haar achterban

Ons onderzoek naar blockchain use cases die relevant zijn voor SURFnet en/of haar achterban en die verder gaan dan een pilot, heeft geen concrete resultaten opgeleverd. Blijkbaar wordt blockchain op dit moment nog niet toegepast in (hoger) onderwijs en onderzoek. Wel zijn er gebruikmakend van bovenstaande criteria een aantal relevante use cases geïdentificeerd waarin blockchain mogelijk een rol kan gaan spelen, en die hiermee ook de mogelijkheden en onmogelijkheden illustreren:

- **Attribute ledgers.** Federaties van identity providers kunnen de blockchain op verschillende manieren inzetten. Het opslaan van persoonlijke gegevens op de blockchain is niet zonder meer mogelijk vanwege privacyaspecten, maar in combinatie met off-chain opslag en privacy-enhancing technology kunnen blockchains wel ingezet worden.
- **Certificate transparency.** Bij Certificate Transparency gaat het erom dat er een log is van alle uitgereikte digitale 'public key' certificaten, om illegaal uitreiken hiervan te kunnen detecteren. Het huidige ontwerp van Certificate Transparency maakt geen gebruik van blockchain, maar met blockchain kan de integriteit van een log beter worden bewaakt dan nu het geval is.
- **DNS.** Naming systems zijn populaire toepassingen van blockchain, en kan DNS robuuster maken.
- **Onderwijscertificaten / micro credentials.** Om de beschikbaarheid en bruikbaarheid in andere toepassingen van onderwijscertificaten te vergroten zou gebruik gemaakt kunnen worden van de blockchain.

Conclusie

Ook voor SURFnet en haar achterban zijn er vele toepassingen waar blockchain-technologie impact op kan hebben. Voor een concrete roadmap, of een beslissing hier zwaar op in te zetten, is het ons inziens te vroeg, de technologie is te onvolwassen en de toepassingen zijn nog niet concreet genoeg. Het is echter wel te overwegen om de technologie verder te leren kennen door Proof-of-Concepts te doen, en om samen met de achterban verder op zoek gaan naar toepassingen. Voor deze Proof-of-Concepts moeten de verwachtingen niet te hoog gespannen zijn; ze zijn er primair om de technologie te leren kennen. De impact zal de komende periode (in ieder geval de komende twee à drie jaar) verder waarschijnlijk laag zijn. Voor toepassingen zal te allen tijde gelden dat er, naast de meerwaarde van blockchain, ook de vergelijking gemaakt zal moeten worden met andere oplossingsrichtingen, zoals het inzetten van Trusted Third Parties, en dat de benodigde standaardisatie meegewogen moeten worden evenals het business model..

1. Introductie blockchain

Blockchain is een nieuwe databasetechnologie die volgens sommigen traditionele Trusted Third Parties (TTP's) zoals banken, notarissen of zelfs overheden zou kunnen vervangen[1]. Blockchain is letterlijk een lange keten van virtuele blokken die regelmatig wordt aangevuld met een nieuw blok waarin de recentste veranderingen van de database als een lijst van transacties is opgenomen. Geïnteresseerden kunnen eenvoudig met elkaar synchroniseren door alle updates in de vastgelegde volgorde toe te passen. Aan dit mechanisme ontleent blockchain zijn decentrale karakter.

Succes van Bitcoin
De meeste mensen kennen blockchain vooral van de eerste toepassing: Bitcoin. Deze munt is in 2008 ontwikkeld door een onbekend perso(o)n(en) met pseudoniem Satoshi Nakamoto. De afgelopen jaren is de waarde van Bitcoins explosief gestegen, met ook flinke dalen. Nog steeds geldt Bitcoin als voorbeeld en inspiratie voor veel andere initiatieven die gebruik maken van blockchains.

1.1. Eigenschappen

De belangrijkste eigenschap van blockchains is dat het partijen die elkaar niet vertrouwen toch in staat stelt om een eenduidige toestand van een database te krijgen. Met andere woorden: blockchains zijn tegelijk organisatorisch gedecentraliseerd en logisch gecentraliseerd. Elke partij heeft hierdoor dezelfde versie van de 'waarheid' of convergeert daar in ieder geval snel naartoe.

Blockchains bevatten niet de toestand van de database zelf, maar de volledige geschiedenis van updates van de database. Alle deelnemers repliceren de gehele database door alle transacties in de juiste volgorde toe te passen. Een gevolg hiervan is dat de inhoud van een blockchain volledig transparant is voor alle deelnemers. Het is dus niet mogelijk om deelnemers slechts toegang te geven tot een deel van de database.

Blockchains zorgen voor een strikte handhaving van de regels rondom transacties. Deze regels zijn vastgelegd in software, zodat automatisch wordt bepaald welke transacties geldig zijn en welke niet. Een aanvaller die valse informatie wil laten plaatsen in de blockchain bereikt niets met het aanpassen van zijn software, omdat ongeldige transacties alsnog zullen worden geweigerd door de andere deelnemers. Dit kan zowel als een voordeel als een nadeel worden gezien: het voordeel is dat er geen vertrouwen nodig is voor het uitvoeren van de regels en een nadeel is dat ongewenste gebeurtenissen niet kunnen worden tegengehouden. Is voor sommige toepassingen een menselijke hand misschien gewenst? Een concreet voorbeeld hiervan is een hack waarbij iemand zijn sleutels verliest en de hacker daarmee iemands tegoeden steelt. Op de blockchain is deze gebeurtenis zichtbaar, maar de transacties zelf zijn geldig en belanden dus in een blok. Er bestaat geen mechanisme om deze transacties tegen te houden zonder de regels met terugwerkende kracht te veranderen.

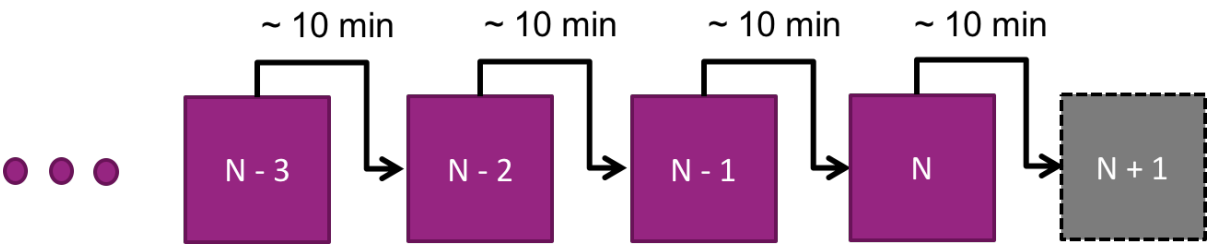
Blockchains zijn onveranderlijk in de zin dat transacties niet achteraf meer kunnen worden gewijzigd of ongedaan gemaakt. Er kunnen alleen nieuwe transacties worden toegevoegd. Als de regels het dus toelaten kan het effect van een transacties wel ongedaan worden gemaakt met een nieuwe transactie, maar de oude transactie blijft altijd bestaan en zichtbaar voor de andere deelnemers.

[1] FD Opinie, Nederland moet koploper in blockchain-technologie worden, 2 januari 2017, Vermeend en De Bruin, https://fd.nl/opinie/1181379/nederland-moet-zich-inspannen-om-koploper-op-gebied-blockchain-technologie-te-worden

Voor het correct functioneren van een blockchain moeten alle deelnemers (eventueel indirect) met elkaar kunnen communiceren, zodat alle nieuwe transacties ook door alle deelnemers verwerkt kunnen worden. Om dit te bereiken wordt er over het algemeen gekozen voor een decentrale (peer-to-peer) manier van communiceren tussen deelnemers om transacties te verspreiden. Het uitvallen van een deel van het netwerk kan hierdoor nauwelijks verstorend werken, wat het netwerk als geheel robuust maakt tegen verstoringen en opzettelijke aanvallen.

1.2. Werking

De transacties van een bepaalde periode worden gebundeld in een 'block' om ze definitief te maken. Ieder block bevat een referentie naar het vorige block zodat er een keten van blokken (blockchain) ontstaat (zie ook Afbeelding 1). Die referentie werkt door een zogenaamde (cryptografische) hash[2] van het vorige blok op te nemen in het nieuwe blok. Hierdoor kan een block niet worden aangepast zonder ook alle volgende blocks aan te passen.



Afbeelding 1 Een blockchain met elke 10 minuten een nieuw block

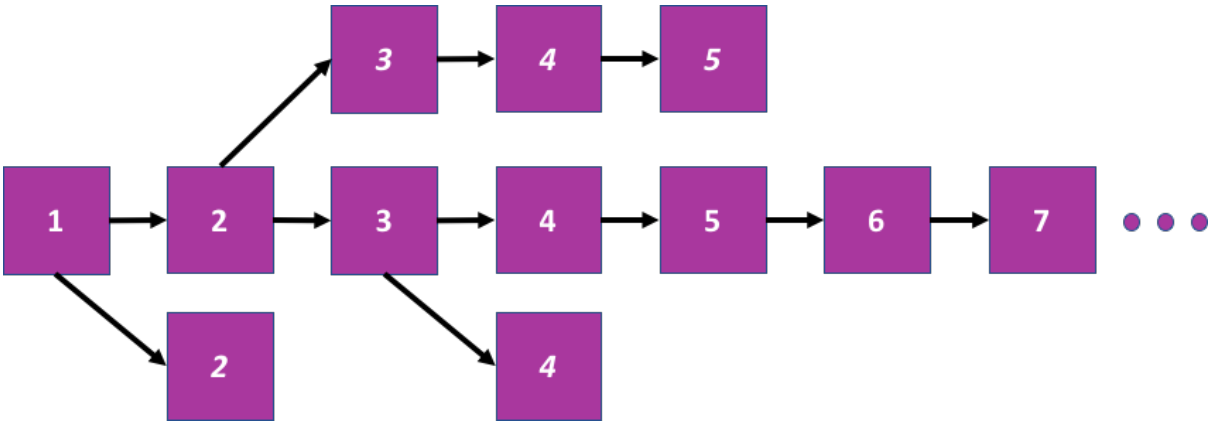
Om te zorgen dat een block achteraf niet meer kan worden aangepast of ongedaan gemaakt, heeft een *miner* het block verzegeld met de oplossing van een complex wiskundig probleem over de inhoud van het block ('Proof-of-work'). Het vinden van een dergelijke oplossing vergt een behoorlijke investering aan hardware en stroomkosten. Hoe 'ouder' het block, hoe langer de keten van blocks die naar het block refereert. Het wordt dus steeds duurder om een block aan te passen, omdat opeenvolgende blocks ook moeten worden aangepast. Het vinden van geldige blokken door Proof-of-work wordt ook wel 'minen' genoemd en dit wordt gedaan door miners. Miners ontvangen dus continu nieuwe transacties die worden gevalideerd en opgenomen in een kandidaat-block waarbij een geldig proof-of-work wordt gezocht. Een block is alleen geldig als alle individuele transacties en het proof-of-work geldig zijn. De snelheid waarmee nieuwe blokken worden gemined, is dus beperkt door de gezamenlijke rekenkracht van de miners. Bij Bitcoin wordt er gemiddeld elke 10 minuten een block gemined en verspreid onder de deelnemers in het netwerk. Als de gezamenlijke rekenkracht van alle miners toe- of afneemt wordt periodiek de moeilijkheidsgraad van het proof-of-work aangepast zodat de snelheid waarmee nieuwe blokken worden gemined gelijk blijft.

Voor het democratisch functioneren van een blockchain is het van groot belang dat miners onafhankelijk van elkaar opereren en niet een meerderheid van de totale rekenkracht in het netwerk in handen kunnen krijgen door samen te werken. In praktijk blijkt echter vaak dat miners wel gaan samenwerken voor schaalvoordelen[3].

Als een aanvaller achteraf een transactie wil verwijderen of aanpassen, moet hij dus het blok waarin die transactie is opgenomen vervangen én alle blokken die daarna zijn gemaakt. Dit kan alleen als de aanvaller sneller nieuwe blokken vindt dan de rest van het netwerk. Dit wordt de 51%-aanval genoemd, omdat deze aanval alleen gegarandeerd slaagt indien de aanvaller meer dan de helft van alle

[2] https://www.byte.nl/kennisbank/item/gegevens_beveiligen_met_encryptie_en_hashing - Hashing
[3] zie https://blockchain.info/pools voor de huidige distributie van rekenkracht van de verschillende miningpools. Hier wordt duidelijk dat een aantal grote pools kunnen collaboreren om een meerderheid van rekenkracht te krijgen.

rekenkracht van het netwerk bezit. Transacties zijn dus nooit helemaal definitief, aangezien er altijd een theoretische mogelijkheid bestaat dat een aanvaller dit doet. De kans hierop neemt wel af als de transactie langer geleden heeft plaatsgevonden tot, als het goed werkt, vrijwel nul.



Afbeelding 2 Conflict over geldigheid van een block: een fork

Als er een conflict optreedt over de geldigheid van een transactie of block, zal dat zich uiten in een zogenaamde 'fork'. Er kunnen verschillende redenen zijn voor het ontstaan van een dergelijk conflict: wellicht is een bepaalde transactie niet geldig, maar het kan ook zijn dat er conflicten ontstaan als niet iedereen de software updatet of een bug ergens. Bij een fork bestaan er meerdere blokken die naar hetzelfde vorige blok verwijzen, zoals gevisualiseerd in Afbeelding 2. Als er een fork optreedt, zullen de miners dus moeten kiezen op basis van welk block ze een nieuw block willen maken. Het block dat op deze manier de meeste rekenkracht achter zich krijgt zal dan vanzelf onderdeel worden van de langste keten. Aangezien er in de langste keten ook de grootste investering aan rekenkracht is gedaan, zal deze keten als de 'juiste' worden beschouwd. Het andere block (of de kortere keten) zal dus worden genegeerd. Je zou ook kunnen zeggen dat er in het geval van een conflict (fork) wordt gestemd op basis van de rekenkracht van de miners met welk block er verder moet worden gegaan. De andere forks sterven als het ware uit.

1.3. Categorieën van blockchains

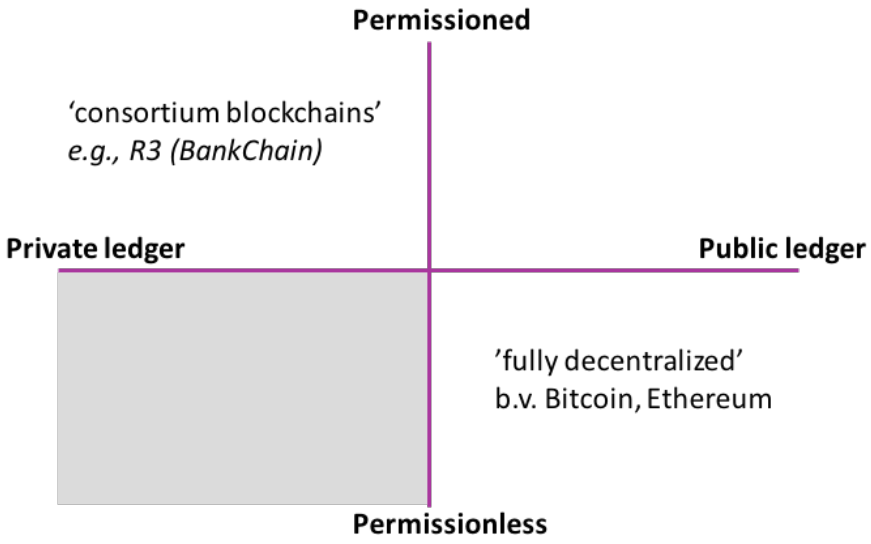
Uit de vorige stukken kan worden afgeleid dat er verschillende interacties worden aangegaan met blockchains, namelijk het maken van blokken en transacties en het ophalen van informatie uit de blockchain. Blockchains zijn dan ook te categoriseren op basis van (de)centraliteit van ieder van deze interacties (zie ook Afbeelding 3):

- **Permissioned versus permissionless**: Deze as gaat over wie er blocks mogen toevoegen aan de chain. In een permissionless model is hier niets over vastgelegd en mag iedereen nieuwe blokken minen. In een permissioned model is er wel vastgelegd wie de miners zijn. Permissioned blockchain zullen over algemeen efficienter zijn.
- **Public versus private ledger**: Deze as gaat over wie er toegang hebben tot de informatie die is opgeslagen in de blockchain. Ofwel alle informatie is publiek, ofwel de informatie wordt alleen in beperkte kring gedeeld (private).

Traditionele blockchains zoals die van Bitcoin en Ethereum[4] vallen allemaal in de categorieën public en permissionless ledger, dus de meest decentrale variant. Maar er bestaan ook voorbeelden van

[4] https://www.ethereum.org/

permissioned, private blockchains, zoals R3[5]. Dit is een een private, permissioned blockchain die ingezet kan worden voor interbancaire transacties. Een private permissionsless blockchain is geen reeele optie, immers om te minen moet er toegang zijn tot de transacties. Een volwassen voorbeeld van een permissioned, publieke blockchain zijn we niet tegengekomen, maar dit zou er wel kunnen zijn of komen, bijvoorbeeld als transparantie belangrijk is.



Afbeelding 3 Categorieën van blockchains

Er is al uiteengezet dat blocks worden beveiligd door Proof-of-work: een ingewikkeld wiskundig probleem oplossen over het block, maar er wordt ook onderzoek gedaan naar een andere vorm van beveiliging, genaamd Proof-of-stake. Hierbij wordt het recht om een nieuw block toe te voegen aan de blockchain verloot onder de deelnemers naar ratio van hun belang in het systeem. Voor cryptocurrencies is dit typisch gerelateerd aan het saldo van de deelnemers. Het idee hierachter is dat in geval van fraude het vertrouwen in de cryptocurrency afneemt en daarmee ook de wisselkoers. De aanname is dat de rijksten hier geen belang bij hebben. Op dit moment kan dit mechanisme als experimenteel worden beschouwd en heeft het zich nog niet bewezen met een succesvolle toepassing.

1.4. Soorten transacties

De inhoud van een transactie is helemaal afhankelijk van de toepassing waarvoor de blockchain wordt ingezet. Veel transacties zijn financieel van aard en bevatten (condities voor) een verhandeling van een geld of goed. Andere transacties bevatten verwijzingen (cryptografische hashes) naar data die niet op de blockchain zelf zijn opgeslagen, bijvoorbeeld vanwege de gevoeligheid van de data of omdat de hoeveelheid gerefereerde data te groot is om in een blockchain te worden opgeslagen. Typisch wordt een transactie ook cryptografisch ondertekend om de authenticiteit aan de tonen.

Een bijzondere categorie van transacties heeft te maken met smart contracts. Een smart contract is in principe niets anders dan programmacode en kan (bijvoorbeeld in Ethereum) worden geüpload naar een blockchain door middel van een transactie. Het smart contract functioneert vervolgens als een zelfstandige entiteit op de blockchain, volgens het vooraf geprogrammeerde gedrag. Verdere transacties kunnen worden gebruikt voor interactie met het smart contract. Een voorbeeld van een smart contract is voor crowdfunding, dat bijvoorbeeld net als Kickstarter alleen uitbetaalt als er een van tevoren

[5] http://www.r3cev.com/

bepaalde hoeveelheid funding aanwezig is binnen een bepaalde tijd[6]. Als het streefbedrag niet op tijd wordt gehaald, worden de bedragen die wel ingelegd zijn automatisch teruggestort op de rekeningen van de donateurs. Doordat het gedrag van het smart contract vooraf al vastligt op de blockchain, kunnen donateurs er zeker van zijn, dat hun donatie alleen daadwerkelijk wordt uitbetaald als aan alle voorwaarden zijn voldaan of anders hun donatie terugkrijgen. Omgekeerd kunnen donateurs hun toezegging niet ongedaan maken als er wel aan de voorwaarden zijn voldaan. Dit alles dus volledig decentraal, zonder vertrouwde tussenpartij.

[6] Dit voorbeeld is op dit moment al eenvoudig te realiseren met Ethereum: https://www.ethereum.org/crowdsale

2. Criteria voor toepassen blockchain

In dit hoofdstuk definieren we een vijftal criteria die helpen om te bepalen of een use case geschikt is voor het toepassen van blockchain. Deze criteria zijn bepaald op basis van desktoponderzoek (onder andere [7,8,9,10]), een workshop met SURFnetters en eigen ervaringen. De eerste drie criteria hebben meer te maken met de problemen die opgelost moeten worden voor die specifieke toepassing, en de laatste twee criteria hebben meer te maken met hoe het opgelost wordt. We beweren niet dat als een use case niet aan alle criteria voldoet, dat het geen zin heeft dit met blockchain op te lossen. We zien deze criteria meer als richtinggevend om dit te bepalen.

Als laatste maken we in dit hoofdstuk een aantal algemene beperkingen van blockchains expliciet, aangezien die ook relevant zijn in het bepalen of blockchain een geschikte technologie is voor een specifieke use case.

Wantrouwen tussen partijen over de state van een database
Zonder wantrouwen tussen partijen over de state van een database is er zelden een reden voor het gebruik van blockchain. Immers zonder wantrouwen tussen de deelnemers zijn er veel meer en vaak simpelere manieren om data beschikbaar te maken tussen deelnemers. Denk hierbij bijvoorbeeld aan distributed hashtables[11], of gecentraliseerde traditionele relationele databases, websites, etc. Vanwege de hoge kosten van het minen van nieuwe blocks zouden blockchains pas moeten worden overwogen als deze andere manieren niet voldoen. Blockchains zijn bovendien pas goed in te zetten als alle deelnemers de geldigheid van een transactie kunnen controleren aan de hand van objectieve (uit te drukken in programmacode) regels, maar dit niet is vast te stellen zonder de toestand van de database te kennen. Cryptocurrencies zijn goede voorbeelden waarbij er aan dit criterium is voldaan. De geldigheid van een transactie is hier namelijk afhankelijk van het saldo van degene die geld overmaakt. Een ander goed voorbeeld gaat over naming systems zoals NameCoin[12] (DNS op blockchain), waarbij een claim op een (domein)naam (transactie) alleen geldig is als het nog niet eerder is geclaimd (state). Een voorbeeld waarbij niet duidelijk aan dit criterium wordt voldaan is het uploaden van diploma's naar een blockchain. In dit geval is de geldigheid van een transactie namelijk alleen afhankelijk van het vertrouwen in de instelling die het diploma heeft afgegeven. Er moet in dit geval goed worden nagedacht over wat de meerwaarde van blockchain is boven het verspreiden van door de instelling (digitaal) ondertekende documenten.

Een traditionele oplossing met een Trusted Third Party (TTP) is ongewenst
Een toepassing waarbij er sprake is van wantrouwen tussen partijen kan op de 'klassieke' manier met een TTP opgelost worden. Blockchain kan gezien worden als een alternatief hiervoor. Er moet dan wel een goede reden bestaan om geen TTP te gebruiken en moet in de uiteindelijke blockchainoplossing de rol van de TTP ook daadwerkelijk verdwijnen of worden verminderd.

Vaak is de reden om TTP's te vervangen door blockchains het ontbreken van een partij die door iedereen wordt vertrouwd, of te hoge kosten. Een goed voorbeeld van een TTP is een notaris, die in sommige gevallen mogelijk kan worden vervangen door een blockchain in combinatie met smart contracts, of banken die niet meer nodig zijn bij cryptocurrencies. In de praktijk verwachten we dat de rol van TTP vaak niet helemaal zal verdwijnen, maar wel minder wordt. Bijvoorbeeld bij een herbruikbare

[7] http://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/
[8] http://www.coindesk.com/want-use-blockchain/
[9] https://www.quora.com/What-are-non-Bitcoin-applications-of-blockchain-technology
[10] http://itsblockchain.com/2016/12/19/when-to-use-blockchain/
[11] http://www.cs.princeton.edu/courses/archive/spr11/cos461/docs/lec22-dhts.pdf
[12] https://namecoin.org/

identiteitsoplossing kan een attributenleverancier gezien worden als een TTP. Als de attributen op een blockchain worden opgeslagen, verdwijnt de TTP echter niet. Immers, de TTP blijft noodzakelijk voor vertrouwen in verifiëren van die identiteitsgegevens (de assertions).

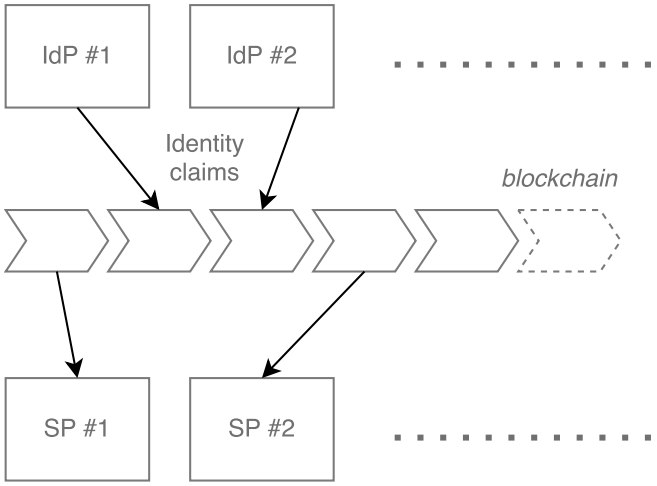
Transparantie nodig
Een criterium is dat er transparantie nodig is (over de transacties, over de database), of als dit niet nodig is dat het in ieder geval niet erg is dat er transparantie is. Aangezien de gehele state van de blockchain inzichtelijk is voor alle deelnemers, is er typisch meer transparantie bij gebruik van blockchains dan zonder. Vanzelfsprekend is het belangrijk of het hierbij om een public of een private ledger gaat. Transparantie kan een voordeel zijn, maar dit is niet per se het geval. Bijvoorbeeld als er persoonlijke gegevens moeten worden verwerkt, is de transparantie van blockchain juist een nadeel. Als vuistregel kan worden aangehouden om geen blockchains in te zetten voor de verwerking van persoonlijke gegevens[13]. Als blockchain toch is gewenst, dan moeten er extra maatregelen worden getroffen om de gegevens te beschermen. Dit is vaak wel mogelijk, bijvoorbeeld door gebruik te maken van encryptie en off-chain functionaliteit, maar kan erg omslachtig worden. Of anders gesteld, het middel kan erger zijn dan de kwaal. Het is bovendien beperkend voor welke regels er gesteld kunnen worden aan de geldigheid van transacties. Ook in praktijk blijkt het vaak lastig om persoonlijke data te beschermen. Veel cryptocurrencies maken gebruik van pseudoniemen om de identiteiten achter transacties te beschermen, maar desondanks kan er toch vaak informatie worden achterhaald van de identiteit(en) achter een transactie[14,15].

Meerdere miners
Het maken van nieuwe blokken moet door meerdere onafhankelijke partijen gebeuren. Als dit niet het geval is, dan is de blockchainoplossing feitelijk toch gecentraliseerd en kunnen alternatieven net zo geschikt, of zelfs geschikter (want goedkoper) zijn.

Werkend businessmodel voor mining
Mining met proof-of-work, zoals dat gebeurt bij ‘traditionele’, publieke, blockchains brengt hoge investeringen en operationele kosten met zich mee en is belastend voor het milieu. Er moet dan wel een businessmodel bestaan waarin het voor de miners aantrekkelijk is om deze investeringen te doen. Bij cryptocurrencies kan dit eenvoudig door de miner van een block te belonen met een bepaalde hoeveelheid van de valuta, maar voor toepassingen anders dan cryptocurrencies kan het lastiger zijn om de miners te belonen. De Ethereum blockchain neemt dit probleem grotendeels uit handen van de ontwikkelaars door handel te creeëren in ‘brandstof’. Brandstof wordt door gebruikers betaald aan de miners naar mate gebruik wordt gemaakt van de Ethereum blockchain. Als het gebruik van een publieke blockchain zoals Ethereum echter geen optie is, moet er goed worden nagedacht over een businessmodel voor miners, of een ander consensusmechanisme worden gebruikt zoals Proof-of-Stake.

[13] Van Doorne, Privacy, security en blockchain, Oktober 2016,
[14] http://cointel.eu/
[15] https://www.elliptic.co/

2.1. Beperkingen



In de praktijk blijkt dat de strenge handhaving van de vastgestelde regels omtrent transacties niet altijd wenselijk is. Als gevolg van computercrashes kunnen gebruikers hun private keys kwijtraken en daarmee toegang verliezen tot bijvoorbeeld geld of andere bezittingen als die op een blockchain worden vastgelegd. Dit probleem is niet uniek voor blockchains, maar in tegenstelling tot blockchains is er bij andere systemen vaak wel een TTP voor re-issuing. Een andere beperking is dat er ook juridische problemen kunnen ontstaan, wanneer bijvoorbeeld bepaalde wetgeving niet kan worden nageleefd. Een voorbeeld hiervan is dat er verwijzingen naar kinderporno kunnen worden opgenomen in de blockchain van Bitcoin, maar dat deze op geen enkele manier nog kunnen worden verwijderd[16]. Een ander recent voorbeeld heeft zich afgespeeld op de blockchain van Ethereum, waar hackers erin zijn geslaagd om een grote hoeveelheid geld te stelen uit een smart contract (zie [17] en kader 'Ethereum en de DAO hack').

Gerelateerd aan bovengenoemde criterium over transparantie, maar hier ook nog apart genoemd omdat we het expliciet willen maken is dat de privacy van gebruikers van blockchains maar in beperkte mate kan worden beschermd. Traditionele vormen van encryptie schieten bijvoorbeeld tekort als er persoonlijke gegevens moeten worden verwerkt. Omdat er alleen gegevens kunnen worden toegevoegd aan de blockchain, is het gebruik van blockchaintechnologie ook mogelijk in strijd met de vergeet-mij-wetgeving in de GDPR[18].

Vanwege de manier waarop blockchains zijn opgebouwd, het opslaan van de volledige geschiedenis van veranderingen, kan een blockchain alleen maar groeien. De hele transactiegeschiedenis moet dan ook beschikbaar blijven zodat nieuwe deelnemers de database kunnen reproduceren. Dit beperkt de hoeveelheid informatie die kan worden opgeslagen op een blockchain, de snelheid waarmee nieuwe data kan worden toegevoegd[19] en daarmee dus de schaalbaarheid van blockchainoplossingen.

[16] http://money.cnn.com/2013/05/02/technology/security/bitcoin-porn/index.html
[17] http://www.coindesk.com/ethereum-dao-hacker-getting-away-classic/
[18] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-erasure/
[19] Om de periodieke kosten van opslag niet te laten toenemen, mag de omvang van een blockchain niet sneller groeien dan dat de kosten voor opslag afnemen.

3. Use cases

Gedurende het onderzoek naar toepassingen van blockchain voor SURFnet en haar achterban zijn er geen relevante en volwassen initiatieven gevonden. Dit betekent niet dat er geen relevantie toepassingen zullen komen, dit kan ook te maken hebben het de onvolwassenheid van de blockchain technologie of simpelweg dat er meer tijd nodig is om goede toepassingen te bedenken. Om wel de (on)mogelijkheden van blockchain technologie voor SURFnet en haar achterban verder te verkennen, schetsen we in dit hoofdstuk een aantal mogelijke use cases die in ieder geval deels aan de eerder beschreven criteria voldoen of extra aandacht hebben gekregen tijdens het onderzoek vanwege de extra hoge relevantie voor SURFnet.

3.1. Attribute ledger in plaats van identity federation

De blockchain kan worden ingezet voor de gefedereerde opslag van identiteitsattributen. Vergeleken met de SAML-gebaseerde identity federations is de opslag van de identiteitsattributen dan decentraal en gerepliceerd, in plaats van bij de identity provider. De identity providers, of aparte attribuutproviders, zetten de attributen dus, na verificatie, op een blockchain.
De rol van de identity provider komt hierdoor niet te vervallen. De identity provider blijft verantwoordelijk voor het vaststellen van de identiteitsinformatie, inclusief de bijbehorende processen om dit betrouwbaar te kunnen doen, maar de identity provider is niet meer verantwoordelijk voor de opslag en het is transparant welke attributen er over wie zijn vastgesteld. De meeste federaties kennen ook een centrale rol voor het vaststellen en controleren van afspraken rondom vertrouwen, levels of assurance, privacy etc., vaak de federatie trust provider genoemd. Deze rol blijft ook nodig, want die bepaalt of de identity provider wel goed hun verificatieprocessen etc. uitvoeren. Toegepast op SURFconext, de identiteitsfederatie van SURFnet, wordt de technische infrastructuur[20] drastisch anders, onder andere is er geen hub meer nodig en zijn de identiteitsproviders (de instellingen) geen onderdeel meer van elke opvraag van een attribuut.

Voordelen
- Omdat er allemaal lokale kopieën zijn, is de attribute ledger altijd beschikbaar.
- Transparantie voor alle partijen, met name voor de gebruiker die kan zien welke attributen er opgeslagen zijn.
- Schaalbaarheid voor leesoperaties, immers dit kan op elke kopie gebeuren.
- Specifiek voor hub-and-spoke federaties zoals SURFconext is er geen manipulatie van attributen op de centrale hub mogelijk, dus is er geen (of minder) technische trusted third party nodig. Het minimaliseren van data moet dan wel op de end-points gebeuren.

Nadelen
- Transparantie van de persoonlijk attributen is slecht voor de privacy. Er zullen significante aanvullende maatregelen nodig zijn (encryptie van attributen, off-chain opslag etc).
- De schaalbaarheid voor wijzigen of toevoegen van attributen is beperkt t.o.v. huidige oplossingen.
- Afhankelijk van de specifieke blockchain technologie, treedt er een vertraging op bij schrijfoperaties, namelijk de tijd tot het volgende block wordt gevonden. Bij Ethereum is dit bijvoorbeeld gemiddeld ongeveer 15 seconden[21] en bij Bitcoin zelfs 10 minuten[22].

[20] SURFconext is een zogenaamde hub-and-spoke federatie, waarin er een centrale hub is die SAML en andere berichten doorzet. Deze hub, maar ook de software bij de verschillende identity providers (universiteiten etc.) zal flink 'dunner' worden of zelfs verdwijnen.
[21] https://etherchain.org/
[22] https://en.bitcoin.it/wiki/Block - What_is_the_maximum_number_of_blocks.3F

- Functies die op dit moment door de hub worden vervuld (protocol vertaling, attribuutmanipulaties) zijn niet meer mogelijk.
- Schaalbaarheid van de opslag van de attributen, op een blockchain kunnen die maar beperkt opgeslagen worden, er zal snel een off-chain oplossing gezocht moeten worden, die complexiteit toevoegt en mogelijk een deel van de voordelen tenietdoet.
- Geen transparantie over wie attributen gekregen heeft omdat de attributen van elke lokale kopie gelezen kunnen worden

Samengevat is er een duidelijke potentie voor een soort attributen ledger door de toegenomen transparantie en minder afhankelijkheid van trusted third parties, maar een rechttoe-rechtaan oplossing zal blockchain niet bieden vanwege gebrek aan schaalbaarheid en de significante aanvullende en off-chain technologie die nodig is vanwege onder andere privacy issues. En er zullen trusted third parties nodig blijven voor o.a. het vaststellen van attributen.

Hier verder niet uitgewerkt, maar beperkter gebruik van blockchain in de context van identiteitsfederaties is ook mogelijk[23], bijvoorbeeld voor het opslaan van meta informatie over welke identiteitsproviders onderdeel zijn van een federatie, of voor opslaan van gebruikers-consent.

3.2. Certificate transparency op de blockchain

Mede naar aanleiding van het Diginotar incident in 2011[24] waarbij een verstrekker van digitale 'public key' certificaten (voor het 'slotje' in browsers etc.) werd gehackt, is Certificate transparancy[25] ontstaan. Het idee is dat elke verstrekker van certificaten, ook wel Certificate Authority genoemd, in een log publiceert welke certificaten hij verstrekt. Dit kunnen domeineigenaren, maar ook anderen, dan controleren. Bijvoorbeeld de Rabobank kan controleren of er niet iemand stiekem een certificaat op naam van de Rabobank aanvraagt om daarmee phishingaanvallen te doen.

Critici[26] van Certificate transparency stellen dat de gemiddelde domeineigenaar niet de capaciteit heeft om alle logs te monitoren (immers elk Certificate Authority heeft zijn eigen log) of de middelen heeft om in te grijpen bij onregelmatigheden. Bovendien beschermt Certificate transparency niet tegen de mogelijkheid dat een log kwaadwillend (of gehackt) is. Blockchain zou een verbetering kunnen zijn.

Een oplossing is om logs samen een (permissioned) blockchain te laten draaien om zo een gezamenlijke log bij te houden. Dit kan veel lijken op wat verschillende banken van plan zijn met R3, maar dan wel publiekelijk in te zien. Deze oplossing maakt het monitoren van logs een stuk eenvoudiger omdat er een centrale plaats is om de logs te doorzoeken. Ook wordt het veiliger omdat Certificate Authorities bij een gezamenlijke oplossing ook de integriteit van elkaars documenten beschermen. De Certificate Authorities een gezamenlijke log laten draaien op een bestaande (permissionless) blockchain met bijvoorbeeld een Ethereum smart contract is waarschijnlijk niet haalbaar vanwege de grote benodigde opslagcapaciteit.
Een andere oplossing is om alleen de *headers* van alle periodieke updates van een log op een blockchain vast te leggen. Dit heeft als voordeel dat een bestaande blockchain i.c.m. een smart contract gebruikt kan worden. Deze optie is geen oplossing voor het eenvoudig monitoren van de diverse logs, maar maakt het voor een kwaadwillende Certificate Authority wel onmogelijk om zijn eigen audit log achteraf nog te vervalsen. Immers, de headers zijn opgeslagen op een blockchain en kunnen daardoor niet meer veranderen.

[23] Bijvoorbeeld Sovrin https://www.sovrin.org lijkt distribute ledger technology te gebruiken voor bepaalde aspecten van haar user centric identity oplossing.
[24] Zie bijvoorbeeld https://nl.wikipedia.org/wiki/Hack_bij_DigiNotar
[25] https://www.certificate-transparency.org/
[26] https://blog.okturtles.com/2014/09/the-trouble-with-certificate-transparency/

Een neveneffect van een Certificate transparency-achtige oplossing op de blockchain is dat er discussie zal ontstaan over wie erop mag schrijven, oftewel, wie zijn eigenlijk de Certificate Authorities? Hier is nu geen autoritatieve bron, er is bijvoorbeeld geen trusted third party die dit vaststelt voor de hele wereld. Er zijn wel allerlei informele samenwerkingsverbanden (bijvoorbeeld CA/Browser forum[27]), belangrijke partijen (bijvoorbeeld browser en OS aanbieders) en nationale regels, maar die zijn het niet altijd eens[28]. Of dit als voordeel of nadeel gezien wordt laten we in het midden, maar opvallend is om te constateren dat in dit geval blockchain een meer centrale benadering is dan het alternatief van Certificate transparency.

Voordelen
- Meer centrale benadering, dus eenvoudigere monitoring.
- Achteraf aanpassen van logs niet meer mogelijk.

Nadelen
- Alle Certificate Authorities zover krijgen hun log op die blockchain te zetten

Samengevat biedt het opslaan van verstrekte certificaten op de blockchain een voordeel qua transparantie, maar zijn er wel problemen die geïntroduceerd worden (wie zijn de Certificate authorities, hoe die allemaal overtuigen mee te doen) die met de meer decentrale Certificate transparency vermeden worden.

3.3. DNS op de blockchain

Naming systems zoals DNS worden gebruikt voor het beheren van domeinnamen zoals bijvoorbeeld nos.nl of google.com. Traditioneel hebben dit soort systemen te maken met de volgende uitdagingen:
- *Leesbaarheid* – De namen moeten eenvoudig lees- en herkenbaar zijn voor mensen.
- *Security* – Namen mogen niet te stelen zijn van de rechtmatige eigenaar: alle deelnemers moeten de informatie krijgen die de eigenaar aan een naam heeft gekoppeld.
- *Decentraliteit* – Het systeem mag geen single point of failure hebben en enkele (collaborerende) partijen mogen niet te veel invloed hebben op het systeem.

Traditioneel kan een systeem hooguit twee van de drie eigenschappen hebben[29]. Zo biedt DNS leesbare namen en veiligheid (i.c.m. DNSsec[30]), maar heeft het wel centrale elementen, zoals IANA[31] en ICAN[32]. Het gebruik van blockchain technologie wordt regelmatig aangedragen[33] als oplossing voor dit probleem en zou daarom geschikt kunnen zijn om te gebruiken als alternatief voor DNS. Transacties op een dergelijke blockchain omvatten dan het claimen van een domeinnaam, het updaten van de gekoppelde informatie en eventueel het verhandelen en vernieuwen van claims op een domeinnaam. Blockchain biedt een decentrale oplossing die daardoor in dagelijks gebruik complexer is dan DNS. Vooral het opzoeken van informatie over een domein wordt complexer. Dit is echter vooral een tradeoff tussen decentraliteit en complexiteit waarin mogelijk nog keuzes gemaakt kunnen worden.

Voordelen
- Mogelijke oplossing waardoor een naming system zowel leesbare namen, security als decentraliteit biedt.

[27] https://cabforum.org/
[28] https://www.thales-esecurity.com/blogs/2012/may/harmonising-european-audit-standards-for-certification-authorities
[29] https://conceptdraw.com/a1092c3/preview
[30] https://www.dnssec.nl/
[31] https://www.iana.org/
[32] https://www.icann.org/
[33] https://namecoin.org/

- Offline opslag van DNS records maakt het internet robuuster en heeft privacy voordelen voor de gebruikers[34].
- Een blockchain hoeft DNS niet helemaal te vervangen. Er zijn allerlei hybride oplossingen denkbaar, wat een transitie kan vereenvoudigen. Subdomeinen kunnen bijvoorbeeld door een traditionele DNSserver worden beheerd terwijl het domein zelf wordt beheerd op een blockchain.
- Het is transparent(er) wie er welke wijzigingen gemaakt heeft in de DNS records.

Nadelen
- Onmogelijk om merknamen te beschermen. Een centrale autoriteit zou hier juist op kunnen toezien en uitspraak doen als er een dispuut optreedt.
- De totale DNS database is erg veel data (10TB+). Het is niet haalbaar om alles naar een blockchain te migreren. Er zal dus veel off-chain gedaan moeten worden.

Samenvattend bestaan er goede mogelijkheden om naming systems al dan niet gedeeltelijk op een blockchain te plaatsen. Specifiek voor DNS zijn er veel interessante ontwerpkeuzes te maken wat betreft de mate waarin DNS wordt verplaatst naar een blockchain en regels omtrent verstrekking, verloop en verlenging van domeinnamen.

3.4. Studievoortgang op de blockchain

In het hoger onderwijs worden behaalde diploma's opgeslagen in het diplomaregister van de Dienst Uitvoering Onderwijs (DUO). Via het portal van DUO kan een gebruiker zijn behaalde certificaten uit het diplomaregister inzien. Dit diplomaregister is niet publiek en het is niet mogelijk voor een gebruiker om derden toestemming te geven zijn of haar gegevens in te zien in het diplomaregister. Wel is het mogelijk voor een gebruiker om een uittreksel te maken van zijn gegevens in het register. Dit uittreksel kan zowel digitaal als op papier. Om de echtheid van het digitaal uittreksel te borgen wordt de pdf voorzien van een certificaat dat bewijst dat het document afkomstig is van DUO. Als het gaat om certificaten van minder formele cursussen, of voor kleinere cursussen is momenteel nog weinig geregeld.

Middels blockchain technologie is het mogelijk om het echtheidsbewijs op te slaan in een publiekelijk beschikbaar decentraal systeem.

Voordelen
- Geen centrale partij voor opslag die vertrouwd moet worden, en die mogelijk ook ooit verdwijnt.
- Mogelijkheden voor het meer fijnmazig opslaan van behaalde vakken of studiepunten, bijvoorbeeld een blockchain versie van Open Badges[35].

Nadeel
- De daadwerkelijke diploma's opslaan op de blockchain zal waarschijnlijk niet schalen, er zal met off-chain opslag in combinatie met hashing gewerkt moeten worden. Hiervoor kan worden gedacht aan technologieën zoals IPFS[36]
- Het bekende nadeel van persoonlijke data die inzichtelijk is buiten wat de persoon wenselijk vindt.
- Het probleem van wat een geaccrediteerde instelling is voor de diploma's is hiermee niet opgelost, evenmin als de semantiek van het diploma.

[34] Door DNS queries te monitoren kan bepaald worden welke websites een gebruiker bezoekt.
[35] Open Badges zijn digitale bewijzen dat iemand vaardigheid, vak etc gehaald heeft, zie https://openbadges.org/
[36] https://ipfs.io/

4. Conclusie

Blockchains, of distributed ledgers, krijgen erg veel aandacht. Het is een nieuwe technologie die volgens sommigen een grote impact kan hebben op hoe vertrouwen online werkt en trusted third parties niet, of minder, nodig kan maken. Tegelijk is gebleken dat blockchain nog een onvolwassen technologie is; in deze technologieverkenning hebben we eigenlijk geen volwassen toepassingen gevonden die relevant zijn voor SURFnet en haar achterban. Ook is het duidelijk dat bij mogelijke use cases er de nodige off-chain en andere aanvullende technologie nodig is voor het succesvol toepassen van blockchain technologie. Of anders gesteld, blockchain kan meer gezien worden als een mogelijk onderdeel van een oplossing, dan als ‘de’ oplossing.

Voor een concrete roadmap voor SURFnet rond de toepassing van blockchains, of een beslissing hier zwaar op in te zetten, is het ons inziens nog te vroeg. Verder de technologie leren kennen door Proof-of-Concepts uit te voeren, aangevuld met samen met de achterban verder op zoek gaan naar toepassingen, is echter zeker wel te overwegen. Voor deze Proof-of-Concepts moeten de verwachtingen niet te hoog gespannen zijn; ze zijn er primair om de technologie te leren kennen en de impact zal de komende tijd waarschijnlijk laag zijn, in ieder geval de komende twee à drie jaar. De in deze verkenning beschreven criteria kunnen helpen bij het selecteren van toepassingen waar blockchain een meerwaarde kan hebben.