Privacy & Identity Lab

Het gebruik van blockchain technologie in het verkiezingsproces

Datum:

12 april 2018

Auteur:

dr. Jaap-Henk Hoepman (Radboud Universiteit)

Reviewers:

prof. Bart Jacobs (Radboud Universiteit)
dr. Oskar van Deventer (TNO)

Dit onderzoek is uitgevoerd door het Privacy & Identity Lab (http://www.pilab.nl/), hierbij juridisch vertegenwoordigd door de Radboud Universiteit Nijmegen.

Hoofdstuk 1

Samenvatting

De blockchain — de technologie achter de Bitcoin — is (in theorie althans) een decentrale, onweerlegbare, en onveranderbare database van transacties. Het ligt daarom voor de hand te denken dat blockchain technologie de betrouwbaarheid en eventueel efficiëntie van het verkiezingsproces in Nederland zou kunnen verhogen. Dit rapport onderzoekt of dit in de praktijk ook het geval zou kunnen zijn.

Om deze vraag te beantwoorden bevat dit rapport een uitgebreide, voor leken begrijpbare, beschrijving van wat een blockchain is, hoe die werkt, en wat de voor- en nadelen van een blockchain zijn.

Vervolgens gaat het rapport in op de vraag of, en zo ja hoe, blockchain technologie gebruikt zou kunnen worden om het verkiezingsproces op een betrouwbare wijze te digitaliseren. We gaan hierbij uit van de acht waarborgen waaraan een verkiezingsproces moet voldoen zoals die 2008 zijn opgesteld door de commissie Korthals Altes. En we richten ons daarbij op een aantal specifieke onderdelen van het verkiezingsproces, zoals het bepalen van de kiesgerechtigdheid in het stemlokaal, internetstemmen, stemmen in het stemlokaal, het tellen van de stemmen, en het plaatsonafhankelijk stemmen in heel Nederland.

We stellen vast dat het uitgangspunt is en blijft dat in het verkiezingsproces het papier leidend is. Daar verandert blockchain technologie niets aan. We constateren dat de ideale blockchain niet bestaat, en dat in de praktijk een blockchain (afhankelijke van het type) een aantal grote nadelen kent. Voor alle typen blockchains geldt dat deze in de praktijk veel minder decentraal zijn dan men doet voorkomen. Daarmee vervalt hun belangrijkste voordeel, zeker omdat het huidige verkiezingsproces ook al in hoge mate decentraal is. Bovendien is het waarborgen van de vertrouwelijkheid problematisch als alle transacties in de voor iedereen toegankelijke blockchain worden bijgehouden.

We concluderen dat het toepassen van blockchain technologie in het verkiezingsproces niet wenselijk is.

Hoofdstuk 2

Inleiding

Na ophef over de onbetrouwbaarheid van stemcomputers werd in 2007 de commissie Korthals Altes [9] ingesteld, om te adviseren over de inrichting van het verkiezingsproces. Deze commissie stelde een achttal waarborgen op, en toetste alle belangrijkste tot dan toe bekende vormen van stemmen (zoals stemmen met papier en potlood, elektronisch stemmen, etc.) aan deze acht waarborgen.

Omdat blockchain technologie aan belang wint, maar destijds niet als mogelijk ondersteunende technologie in de analyse is meegenomen, rijst de vraag of het gebruik van blockchain technologie in het verkiezingsproces kan helpen. Concepten zoals Votebook [10], en bedrijven als Voatz[1], Follow My Vote[2], en VoteWatcher[3] spelen hier op in.

2.1 Het verkiezingsproces

Het verkiezingsproces bestaat uit een aantal verschillende stappen, die onder de verantwoordelijkheid van verschillende partijen worden uitgevoerd. We schetsen hier kort het proces dat doorlopen wordt bij landelijke verkiezingen voor de Tweede Kamer.

In de eerste fase stelt de Kiesraad vast welke partijen meedoen aan de verkiezingen. Zij stelt de kandidatenlijsten vast, en onder welk lijstnummer een partij aan de verkiezingen deelneemt. Hiermee ligt de verkiezing, d.w.z. datgene waaruit gekozen kan worden, vast.

Vervolgens moet bepaald worden wie er mogen stemmen. Dit is de verantwoordelijkheid van de gemeenten. Zij bepalen de kiesgerechtigdheid van hun inwoners op basis van de Basisregistratie Personen (BRP), en voorzien kiezers van stempassen een aantal weken voor de verkiezingen. Hiermee ligt vast wie er mogen stemmen.

De colleges van burgemeester en wethouders van gemeenten zijn verantwoordelijk voor de organisatie van Tweede Kamerverkiezingen, zoals het aanwijzen van stembureaus, het inrichten van stembureaus en het benoemen van stembureauleden.

Ook het stemproces zelf, op de dag van de verkiezingen, valt onder de verantwoordelijkheid van de gemeente. Kiezers brengen, nadat bijvoorbeeld op basis van een stempas op het stemburo bepaald is of ze inderdaad kiesgerechtigd zijn, hun stem uit.

Na het sluiten van de stembus worden de stemmen geteld. De uitslagen worden handmatig per stembureau geteld. Gemeenten totaliseren deze uitslagen op het niveau van partijen en kandidaten. Daarna tellen de hoofdstembureaus de uitslagen van gemeenten op tot een uitslag voor hun kieskring. Tot slot brengen de hoofdstembureaus deze kieskring-uitslagen over naar het centraal stembureau (Kiesraad). Deze stelt op basis van de uitslagen van de hoofdstembureaus de landelijke uitslag vast. In alle stappen na het handmatig tellen van de stemmen wordt gebruik gemaakt van ondersteunende software (OSV), die in opdracht van de Kiesraad is ontwikkeld.

2.2 De acht waarborgen

De commissie Korthals Altes heeft de volgende acht waarborgen opgesteld waarvan zij vindt dat het verkiezingsproces in Nederland moet voldoen [9].

Transparantie Het verkiezingsproces moet zo zijn ingericht, dat het helder van structuur en opzet is, zodat in beginsel iedereen inzicht in de structuur ervan kan hebben. Er zijn in het verkiezingsproces geen geheimen. Vragen moeten beantwoord kunnen worden; de antwoorden moeten controleerbaar en verifieerbaar zijn.

Controleerbaarheid Het verkiezingsproces moet objectief controleerbaar zijn. De controle- instrumenten kunnen, afhankelijk van de vorm van stemmen waartoe wordt besloten, verschillen.

Integriteit Het verkiezingsproces moet correct verlopen en de uitkomst mag niet beïnvloedbaar zijn anders dan door het uitbrengen van rechtmatige stemmen.

[1] https://voatz.com
[2] https://followmyvote.com
[3] http://votewatcher.com.

Kiesgerechtigdheid Alleen kiesgerechtigde personen mogen aan de verkiezing deelnemen.

Stemvrijheid Iedere kiesgerechtigde moet bij het uitbrengen van zijn of haar stem zijn of haar keuze in alle vrijheid, vrij van beïnvloeding, kunnen bepalen.

Stemgeheim Het moet onmogelijk zijn om een verband te leggen tussen de identiteit van de persoon die de stem uitbrengt en de inhoud van de uitgebrachte stem. Het proces moet zodanig zijn ingericht, dat het onmogelijk is de kiezer te laten aantonen hoe hij of zij gestemd heeft[4].

Uniciteit Iedere kiesgerechtigde mag, gegeven het Nederlandse kiesstelsel, één stem per verkiezing uitbrengen, die bij de stemopneming precies één keer meegeteld mag en moet worden.

Toegankelijkheid Kiesgerechtigden moeten zoveel mogelijk in de gelegenheid gesteld worden om direct deel te nemen aan het verkiezingsproces. Indien dat onmogelijk is, moet de mogelijkheid openstaan om indirect – door het verlenen van een volmacht – aan de verkiezing deel te nemen.

De commissie heeft destijds alle belangrijkste tot dan toe bekende vormen van stemmen (zoals stemmen met papier en potlood, elektronisch stemmen, etc.) aan deze acht waarborgen getoetst. Zij concludeerde dat het stemmen met potlood en papier het best aan deze acht voorwaarden voldeed. Maar ook was in haar ogen een vorm van elektronisch stemmen haalbaar, mits de papieren stem nog steeds leidend is. Dit systeem op basis van een elektronische stemmenprinter en een elektronische stemmenteller is vervolgens door de commissie van Beek nader geanalyseerd [13].

2.3 Vraagstelling

De centrale onderzoeksvraag luidt als volgt.

> Kan blockchain technologie van betekenis zijn om op een betrouwbare wijze (onderdelen van) het verkiezingsproces te digitaliseren?

Ter beantwoording van deze vraag zal worden onderzocht of blockchaintechnologie kan helpen om de volgende onderdelen van het verkiezingsproces op een verantwoorde manier te digitaliseren.

- Bepalen in het stemlokaal van de kiesgerechtigdheid door een elektronische controle van de stempas die de kiezer aanbiedt aan het stembureau.
- Internetstemmen (kiezers in het buitenland);
- Elektronisch stemmen in het stemlokaal met een stemprinter;
- Elektronisch tellen van (papieren) stembiljetten in het stemlokaal;
- Plaatsonafhankelijk stemmen in heel Nederland. Dat wil zeggen het realiseren van een landelijk raadpleegbaar kiezersregister (LKR) dat op de dag van stemming door alle stembureaus (ca 10.000) wordt geraadpleegd als een kiezer in een stemlokaal komt stemmen.

Hierbij zal voor elk van deze vier onderdelen gekeken worden of blockchain technologie al dan niet nadere invulling kan geven aan de waarborgen van de commissie Korthals Altes zoals die hierboven beschreven zijn.

Daarnaast wordt gevraagd om een beschrijving van blockchain technologie in een voor leken begrijpelijke taal. Deze beschrijving moet de leek in staat stellen de analyse van het gebruik van blockchain technologie in het verkiezingsproces te begrijpen.

2.4 Leeswijzer

We beginnen het rapport met een uitgebreide, informele, beschrijving van blockchain technologie in hoofdstuk 3. In dit hoofdstuk gaan we ook in op de voor- en nadelen van blockchain technologie. In hoofdstuk 4 maken we een eerste grove analyse ten aanzien van het gebruik van blockchain technologie in het verkiezingsproces op basis van de acht waarborgen, waarna we in hoofdstuk 5 de hierboven opgesomde onderdelen van het verkiezingsproces in meer detail analyseren wat betreft de (on)toepasbaarheid van blockchain technologie. Hoofdstuk 6 vat onze conclusies samen, waarna het rapport afsluit met een overzicht van gebruikte bronnen.

[4] En waarbij het ook niet mogelijk moet zijn om te bepalen óf een kiezer gestemd heeft.

Hoofdstuk 3

Over blockchain technologie

Traditioneel houden organisaties al hun transacties bij in een *grootboek* (in het Engels een *ledger* genoemd). Zo leggen ze de volgorde van alle transacties vast, in een (min of meer) onveranderbaar register. Eenmaal in het grootboek bijgeschreven kan een transactie niet meer veranderd of verwijderd worden.

Een *blockchain* is een digitale equivalent van zo'n grootboek. Letterlijk is een blockchain een keten van blokken (zie figuur 3.1). Ieder blok bevat een aantal transacties, en is daarmee te vergelijken met een pagina uit een grootboek. Daarnaast bevat een blok een 'onveranderbare verwijzing'[1] naar het vorige blok in de keten; naar analogie met het grootboek is dat dus een verwijzing naar de vorige pagina in het grootboek. De onveranderbare verwijzing is als een soort miniatuurfoto van het vorige blok, de vorige pagina in het grootboek[2]. Dit creëert een soort Droste effect, met als gevolg dat het meest recente blok in feite alle informatie over alle voorgaande blokken vastlegt. Net zoals het kaft en de binding van een grootboek ervoor zorgen dat je niet zomaar pagina's kunt toevoegen en verwijderen, zorgt deze 'onveranderbare verwijzing', deze foto van het vorige blok, ervoor dat de volgorde van de blokken in de blockchain vast ligt.

De doorbraak van Satoshi Nakamoto[3] was dat hij zich realiseerde dat je een blockchain kunt gebruiken om een *gedistribueerd* grootboek (distributed ledger) bij te houden [12]. In plaats van een grootboek dat wordt bijgehouden op één centrale locatie door één vertrouwde boekhouder, werken hierbij meerder boekhouders samen om gezamenlijk het grootboek bij te houden. Iedere boekhouder[4] heeft een lokale kopie van de blockchain (het grootboek), en iedere boekhouder mag transacties aan de blockchain (het grootboek) toevoegen. Zo ontstaat er een voor iedereen te raadplegen historisch overzicht van alle transacties, waarbij transacties die in het verleden zijn gedaan niet kunnen worden teruggedraaid. Merk op dat de voor de hand liggende oplossing om meerdere boekhouders een gedeeld grootboek te laten bijhouden in zeg een Google docs spreadsheet nog steeds gecentraliseerd is: Google zou de inhoud zomaar kunnen wijzigen.

We onderscheiden twee soorten blockchains: *permissionless* blockchains en *permissioned* blockchains. Bij een permissionless blockchain is *iedereen* boekhouder: iedereen heeft toegang tot de blockchain en kan transacties aan de blockchain toevoegen. Bitcoin en Ethereum zijn permissionless. Dit type blockchain is (in theorie althans) volledig gedecentraliseerd.

Bij een permissioned blockchain is toegang tot de blockchain beperkt en kan maar een (zeer) kleine groep vooraf geselecteerde boekhouders transacties aan de blockchain toevoegen, hetzij voor zichzelf, hetzij in opdracht van anderen. Voorbeelden van persmissioned blockchains zijn Hyperledger Fabric of Tendermint. Banken en bedrijven maken vaak gebruik van persmissioned blockchains. Dit type blockchain is slechts in beperkte mate gedecentraliseerd. Merk op dat het prima mogelijk is dat een permissioned blockchain *openbaar* is, dat wil zeggen dat iedereen de transacties op de blockchain kan inzien. Permissioned betekent slechts dat het aantal partijen dat de blockchain beheert beperkt is. Permissionless blockchains zijn per definitie altijd openbaar.

Het toevoegen van transacties aan een blockchain moet op een gecoordineerde manier gebeuren zodat alle boekhouders ook inderdaad dezelfde blokken en dezelfde transacties in die blokken zien. Hiervoor zorgt het zogenaamde *consensus* mechanisme[5] [1]. Het blijkt

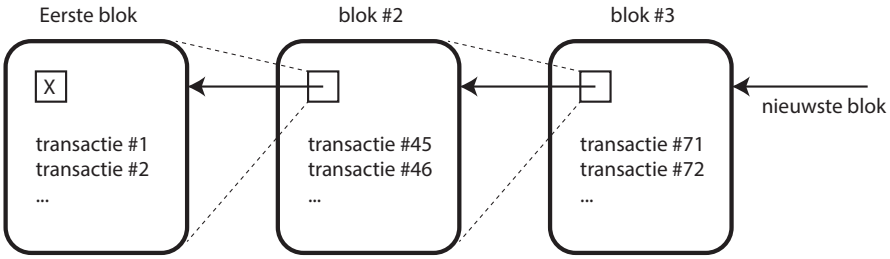
[1] Deze onveranderbare verwijzing is de cryptografische hash van de inhoud van het blok waarnaar verwezen wordt. Zo'n hash is onomkeerbaar: hij is makkelijk uit te rekenen, maar niet te inverteren. Een hashfunctie h berekent voor willekeurige data d een samenvatting $h(d)$ van *vaste lengte* zodanig dat: 1) als de data verschilt, i.e. $d \neq d'$, dan is de samenvatting ook verschillend, i.e. $h(d) \neq h(d')$, en 2) gegeven een samenvatting $h(d)$ is het onmogelijk om de invoer d te achterhalen.

[2] http://www.govtech.com/data/GT-OctoberNovember-Securing-the-Vote.html (23-03-2018).

[3] Satoshi Nakamoto is het pseudoniem van de onbekende uitvinder(s) van Bitcoin.

[4] In dit rapport spreken we consequent over boekhouders, daar waar in de literatuur de vagere termen 'members' of 'nodes' wordt gebruikt. Iedere boekhouder heeft of is een computer die alle noodzakelijke berekeningen en administratieve handelingen verricht.

[5] Historisch gezien maken permissionless blockchains gebruik van een fundamenteel ander consensus mechanisme (proof-of-work) dan permissioned blockchains. Dat onderscheid begint tegenwoordig



Figuur 3.1: *De blockchain*

dat de mate van ge(de)centraliseerdheid van een blockchain veel invloed heeft op (of afhangt van) het consensus mechanisme.

Laten we daarom eens kijken hoe het consensus mechanisme werkt bij een permissionless blockchain, zoals Bitcoin dat gebruikt.

3.1 Permissionless blockchains: consensus op basis van proof-of-work

Bitcoin is een vorm van virtueel geld, een zogenaamde crypto currency. Bitcoin is permissionless: iedereen met een computer of smartphone kan meedoen. Je hoeft alleen maar wat software te installeren en je wordt automatisch lid van het bitcoin netwerk. Dit bitcoin netwerk is een zogenaamd peer-to-peer (P2P) netwerk waarin leden onderling met elkaar bitcoin transacties verwerken zonder tussenkomst van een centrale partij. Met de bitcoin software kun je bitcoins kopen of verkopen. Iedereen die lid is van het netwerk kan een verzoek voor een nieuwe transactie indienen (als je voldoende bitcoins hebt, natuurlijk). En iedereen die lid is kan ook boekhouder zijn (maar dat hoeft niet).

De transactieverzoeken worden over alle boekhouders van het bitcoin netwerk verspreid. Niet alle verzoeken komen echter bij alle boekhouders aan, en zeker niet allemaal in dezelfde volgorde. Om ervoor te zorgen dat er uiteindelijk wel *overeenstemming* (*consensus*) wordt bereikt over welke transacties in welke volgorde zijn uitgevoerd wordt de blockchain block voor block opgebouwd.

Zoals al eerder gezegd, je zou zo'n block als één bladzijde uit het grootboek kunnen zien. Op gezette tijden wordt een willekeurig boekhouder gemachtigd om nieuwe transacties op een nieuwe pagina van het grootboek te schrijven. Daarin schrijft deze boekhouder dus de nieuwe transacties die hij ontvangen heeft, en in de volgorde waarin hij ze ontvangen heeft. De boekhouder moet wel controleren of de transacties kloppen met andere transacties eerder in het grootboek. Anders zullen de andere boekhouders (die deze controle ook uitvoeren) de nieuwe bladzijde in het grootboek, het nieuwe blok, niet accepteren. Vervolgens voegt hij het blok aan de blokchain toe en stuurt het nieuwe blok aan alle andere boekhouders.

Een cruciale vraag is nu: hoe kies je uit een groep onbekende boekhouders één iemand echt willekeurig uit (om te voorkomen dat te vaak een kwaadwillende boekhouder gekozen wordt die er voor kan zorgen dat de informatie in de blockchain alsnog verandert).

Satoshi's tweede uitvinding was *proof of work* als een mechanisme om op een volledig gedecentraliseerde manier een willekeurig boekhouder in het bitcoin netwerk te machtigen om een nieuw blok te maken. Proof of work laat iedere boekhouder een lastige rekenkundige puzzel oplossen[6]. De eerste die de oplossing vindt is de winnaar en mag het eerstvolgende blok aan de blokchain toevoegen. Het oplossen van de puzzel heet *minen*, en de boekhouders heten daarom ook wel *miners*. De winnaar ontvangt een beloning (in bitcoin) voor het minen van het blok. Dat moet ook wel, want minen kost geld (zie verderop). Zonder beloning zou niemand willen minen en dan zou de blockchain uit elkaar vallen.

De puzzel is zo geconstrueerd dat er geen slimmigheidjes zijn om snel de oplossing te vinden. Het enige dat werkt is één voor één alle mogelijke oplossingen te proberen. Vandaar dat hoe sneller de computer is waarmee een boekhouder probeert de puzzel op te lossen, hoe groter de kans is dat hij wint. De moeilijkheidsgraad van de puzzel is zo ingesteld dat gemiddeld gesproken iedere 10 minuten een nieuwe winnaar gevonden

enigszins te vervagen, maar voor dit rapport houden we ons aan deze traditionele classificatie.

[6] Ook deze puzzel maakt gebruik van hashfuncties. Om precies te zijn wordt gevraagd om voor het nieuwe blok met inhoud b een nonce n te vinden zodanig dat de hash $h(b, n)$ kleiner is dan een bepaalde drempelwaarde. Hoe kleiner die drempel, des te moeilijker de puzzle. Voor vaste b is de enige optie om willekeurig alle mogelijke nonce n één voor één te proberen totdat de uitvoer van de hashfunctie aan de eisen voldoet.

wordt. Als er meer mensen lid worden van het bitcoin netwerk, of als de rekenkracht van de miners omhoog gaat, wordt de puzzel automatisch moeilijker gemaakt.

Mining kost heel veel stroom, en snelle mining hardware is duur. De kans dat een boekhouder een blok mined is bovendien heel erg klein. Het kan dus erg lang duren voordat een boekhouder zijn eerste beloning voor het succesvol minen van een blok ontvangt en zo zijn investeringen terugverdient. Vandaar dat boekhouders samenwerken in zogenaamde *mining pools* om het risico te verdelen. De opbrengsten van het minen van een blok worden over de leden van de pool verdeelt naar rato van de rekenkracht die ze inbrengen in de pool.

3.2 De voor en nadelen van permissionless blockchains (op basis van proof of work)

Het grote voordeel van een permissionless blockchain is dat er (in het ideale geval) geen enkele centralisatie plaatsvind. Alles is decentraal. Iedereen kan meedoen en bijdragen aan de stabiliteit en veiligheid van de blockchain door ook als boekhouder mee te doen. Die bijdrage is enkel afhankelijk van de hoeveelheid ingebrachte rekenkracht[7]. Iets wat eenmaal aan de blockchain is toegevoegd kan er (in theorie) door niemand anders meer afgehaald worden. Dit vergroot de transparantie en accountability aanzienlijk.

Helaas bestaat de ideale blockchain niet, en zijn er in de praktijk een groot aantal nadelen.

- Er is (nog) geen volledig wiskundig bewijs van de **veiligheid en stabiliteit** van blockchains die gebruik maken van proof of work[8] (zoals bitcoin en vele andere blockchains doen) [3]. Het argument dat zo'n blockchain veilig en stabiel is als ten minste 51 % van de rekenkracht in handen is van eerlijke boekhouders, houdt enkel stand onder zeer versimpelende aannames in de zogenaamde speltheorie. In de praktijk blijkt dat al een aanzienlijk kleinere fractie van de miners het Bitcoin netwerk kan destabiliseren [6]. Onder de aanname dat de groep van miners nooit verandert, en slechts een derde van hen kwaadwillend is, is er een bewijs dat het bitcoin netwerk stabiel en veilig is [8, 7].
- Permissionless blockchains **schalen slecht**. Het aantal transacties dat de Bitcoin blockchain kan verwerken is bijvoorbeeld een tiental per seconde. Ter vergelijking: creditcardmaatschappijen verwerken normaal gesproken tienduizend transacties per seconde. Dit lijkt inherent te zijn aan permissionless blockchains, dwz. een noodzakelijk gevolg van volledige decentralisatie[9].
- **Transaction finality**. Bij permissionless blockchains is niet meteen duidelijk of een transactie ook echt verwerkt is en door het netwerk geaccepteerd is. De zekerheid groeit naarmate er nieuwe blokken aan zo'n blockchain zijn toegevoegd. In Bitcoin is die zekerheid er pas na ongeveer een uur.
- Het **energiegebruik** van proof-of-work is kolossaal, en groeit (kwadratisch) met het aantal gebruikers. Huidige schattingen zijn dat één Bitcoin transactie net zoveel energie kost als het electriciteitsgebruik van vijf en een half Amerikaanse gezinnen gedurende een dag in 2017[10]. Proof of work is niet duurzaam.
- Blockchains slaan noodzakelijkerwijs alle transacties op die ooit zijn uitgevoerd. Iedere boekhouder moet een volledige kopie van de blockchain lokaal bijhouden. Dit lijdt tot **excessief geheugengebruik**: op dit moment (maart 2018) is de Bitcoin blockchain 160 GB groot[11], en neemt zij met 50 GB per jaar in grootte toe.
- Permissionless blockchains staan of vallen met de bereidheid van de leden om ook inderdaad als boekhouder op te treden. Vandaar dat permissionless blockchains een **beloning structuur** nodig hebben. Voor een cryptocurrency als Bitcoin ligt zo'n beloning structuur voor de hand. Voor andere toepassingen die niet direct financieel van aard zijn, is dat niet het geval.
- In de praktijk zijn permissionless blockchains veel **gecentraliseerder** dan in theorie bedoeld is. Sinds 2016 hebben telkens vier Bitcoin mining pools meer dan 53% van de totale mining power in handen [5] (en daarmee dus controle over de blockchain). Daarnaast hebben ook de ontwikkelaars van de software veel macht, en zijn in de praktijk in het verleden transacties wel degelijk teruggedraaid[12]
- Transacties in een permissionless blockchain zijn openbaar en voor iedereen in te zien. Dat maakt permissionless blockchains inherent **privacy** onvriendelijk. Er zijn wel voorstellen om de privacy

[7] We focussen hier op permissionless blockchains met proof-of-work als consensus mechanisme. Dit mechanisme wordt het meest gebruikt. Het is ook het enige mechanisme waarvoor een enigzins solide argumentatie voor de stabiliteit bestaat; maar zie verderop.

[8] Dit geldt in veel sterkere mate ook voor andere consensus mechanismen zoals proof-of-stake.

[9] https://www.coindesk.com/decentralization-vs-scale-studies-explore-cryptos-growing-struggle/ (12-3-2018).

[10] https://digiconomist.net/bitcoin-energy-consumption (25-08-2017).

[11] https://blockchain.info/charts/blocks-size (13-03-2018).

[12] In Ethereum is dit gebeurd na de zogenaamde DAO hack, waarbij een hacker een fout in de een smart contract (de DAO genaamd) misbruikte om 55 miljoen dollar te stelen. In een Ethereum software update werd het vervolgens de hacker onmogelijk gemaakt zijn buit uit te geven.

impact te verminderen, bijvoorbeeld door gebruik te maken van zero-knowledge technieken, door de echte gegevens te versleutelen, of ergens anders te bewaren en enkel de hash van de gegevens op een blockchain op te slaan. In de laatste twee gevallen is dan wel de vraag wie de sleutels beheerd, of wie de externe opslagruimte beheerd. Als privacy een belangrijke eigenschap is, ligt het daarom meer voor de hand om een inherent privacy-vriendelijkere technologie toe te passen.

3.3 Permissioned blockchains: Consensus op basis van BFT

In een permissioned blockchain is er een kleine groep (hooguit enkele tientallen) vooraf aangewezen boekhouders die verantwoordelijk zijn voor het bijhouden van het grootboek. Dat maakt het grootboek veel minder gedecentraliseerd, en daardoor is het mogelijk om gebruik te maken van een totaal andere consensus mechanisme, gebaseerd op *Byzantine Fault Tolerance (BFT)* [3].

Het gebruikt van woord Byzantine is ontstaan uit de informele beschrijving van het oorspronkelijke probleem, waarbij een aantal divisies van het Byzantijnse leger, elk met zijn eigen generaal, een dorp omsingeld hebben. Een aanval op het dorp is alleen succesvol als voldoende generaals tegelijk besluiten het dorp aan te vallen. Helaas zijn niet alle Byzantijnse generaals te vertrouwen. Sommige zijn verraders die actief zullen proberen de verovering van het dorp tegen te werken [11]. Dergelijk kwaadaardig gedrag wordt sindsdien Byzantine genoemd (om het te onderscheiden van minder kwaadaardige fouten, zoals een (passieve) systeemcrash).

Byzantine Fault Tolerance (BFT) is een klassiek probleem uit de informatica, waar formeel geanalyseerde oplossingen voor bestaan, onder de aanname dat ten hoogste een derde van de computers in het netwerk kwaadwillend is [4]. Het grootste nadeel van deze oplossingen is dat ze een uitzonderlijk groot aantal berichten onderling moeten uitwisselen, wat ze ongeschikt maakt voor grote netwerken. Vandaar dat BFT enkel van toepassing is in een permissioned setting met een klein aantal (enkele tientallen) boekhouders.

3.4 De voor en nadelen van permissioned blockchains (op basis van BFT)

Het belangrijkste voordeel van permissioned blockchains op basis van BFT is dat er wiskundige bewijzen zijn dat ze veilig en stabiel zijn (zolang aan de aanname is voldaan dat ten hoogste een derde van de boekhouders onbetrouwbaar is). Dit is veel sterker dan het oppervlakkige argument waarop de veiligheid van proof of work in permissionless blockchains is gebaseerd. Ook is de veiligheid en stabiliteit van permissioned blockchain niet afhankelijk van aannames over 'rationeel' gedrag van de boekhouders.

Daarnaast zijn er nog een aantal voordelen. Als een blockchain niet openbaar is (en of dat zo is hangt af van de opzet van de permissioned blockchain) is er een beperkter privacy risico. In zijn algemeenheid geldt dat met een permissioned blockchain met een beperkt aantal boekhouders een of meer verantwoordelijken voor de verwerking aangewezen kunnen worden. Permissioned blockchains kunnen hoge transactie volumes verwerken, en er is ook meteen duidelijk of transacties al dan niet verwerkt zijn. Tenslotte gebruiken permissioned blockchains een 'normale' hoeveelheid energie; er is geen speciale hardware nodig die continue staat te rekenen.

Permissioned blockchains hebben ook nadelen. Het grootste nadeel is de hoge mate van **gecentraliseerdheid** van permissioned blockchains. Vooraf wordt een klein aantal vaste boekhouders aangewezen. Vaak door één partij, dan wel door een groep aan elkaar gelieerde partijen. Andere gebruikers hebben geen invloed op deze keuze. Voor hen is er in de praktijk dan ook amper verschil tussen een situatie waarin een permissioned blockchain wordt gebruikt in plaats van een centrale server.

Daarnaast wisselen in BFT gebaseerde blockchains de boekhouders onderling **veel berichten** uit om de verschillende kopieën van het grootboek consistent te houden. Dit heeft uiteindelijk ook een beperkend effect op het maximaal te verwerken transactievolume. Daarnaast geldt ook hier dat de volledige blockchain door alle boekhouders bewaard moet worden, en er dus een significante hoeveelheid **geheugen gebruikt** wordt (overigens wel minder dan in permissionless blockchains omdat een permissioned blockchain veel minder boekhouders heeft)[13].

3.5 Afsluitende opmerkingen

Dé blockchain bestaat niet. De twee voorbeelden die hier geschetst zijn, zijn wel de twee benaderingen die op dit moment het meest in zwang zijn, en geven de eigenschappen en mogelijkheden van blockchains in de praktijk goed weer. Proof-of-work is

[13] Waarbij wel aangetekend moet worden dat als er gebruik gemaakt wordt van BFT er minder reden is om de volledige transactie geschiedenis bij te houden omdat je niet terug in de tijd hoeft te kunnen. Efficiëntere strategieën om de huidige toestand bij te houden zijn dan mogelijk.

het dominante consensus mechanisme voor permissionless blockchains. Andere opties (bijvoorbeeld proof-of-stake) zijn slecht onderbouwd. Byzantine Fault Tolerance is het dominante mechanisme voor permissioned blockchain. Dit ligt ook voor de hand vanwege het veel kleinere aantal boekhouders in een permissioned blockchain.

Naast het verwerken van eenvoudige transacties, kunnen blockchains ook gebruikt worden voor het decentraal en voor iedereen controleerbaar uitvoeren van zogenaamde *smart contracts*. Ethereum is het bekendste blockchain platform hiervoor [2, 18]. De naam smart contract is enigszins misleidend: een contract is voornamelijk een juridisch begrip. Een smart contract is in werkelijkheid gewoon een willekeurig stukje software[14] dat invoer verwerkt en uitvoer produceert, op basis van in de software geprogrammeerde regels. De invoer van een smart contract zou een financiële transactie kunnen zijn, en de uitvoer het overdragen van een eigendomsrecht. Met zo'n soort contract zou je een kadaster kunnen modelleren, of de verkoop van kunst of grondstoffen traceerbaar kunnen maken. Door een blockchain te gebruiken is de werking van alle smart contracts transparant en voor iedereen te verifiëren: de uitvoer is, ook later, niet aan te passen.

Behalve deze automatische transparantie, verifieerbaarheid en onweerlegbaarheid is er verder niets magisch of slim aan deze smart contracts. Net als alle andere software kan een smart contract bugs bevatten, met soms desastreuze gevolgen.

Als we, in functionele zin, de (ideale) blockchain zouden willen beschrijven, dan is het een *decentrale*, *onweerlegbare*, en *onveranderbare* database van *transacties* die, als deze openbaar is, voor iedereen toegankelijk is. Een blockchain is nodig als tegelijkertijd aan twee voorwaarden is voldaan:

- er is niet één te vertrouwen centrale partij, én
- de volgorde van de te verwerken transacties is van belang.

Dat betekent dus ook dat als er wél ene te vertrouwen centrale partij is, of als de volgorde van transacties niet van belang is, een blockchain niet noodzakelijk is. Een blockchain is nadrukkelijk *niet* een vertrouwensmachine of een waarheidsmachine. Het gebruik van een blockchain verplaatst en verandert vertrouwensrelaties. Een blockchain zorgt er voor dat alle boekhouders dezelfde transacties zien, niet noodzakelijkerwijs dat al deze transacties waar zijn of overeenkomen met de werkelijkheid. Daar moet de toepassing die gebruik maakt van een blockchain zelf voor zorgen, zoals Bitcoin dat bijvoorbeeld doet.

We merken afsluitend op dat, gezien de voorgaande analyse, de ideale blockchain, die volledig gedecentraliseerd is, en waarin transacties echt niet teruggedraaid kunnen worden, in werkelijkheid helaas niet bestaat.

[14] Je zou het kunnen vergelijken met een software agent; een technologie die een twintigtal jaar geleden in zwang was.

Hoofdstuk 4

Verkiezingen en blockchains: een eerste grove analyse

4.1 Papier is leidend

Eerder onderzoek naar nieuwe (digitale) inrichtingen van het verkiezingsproces, door de commissies Korthals Altes [9] en Van Beek [13] spreekt een grote voorkeur uit voor een systeem waarin het papieren proces leidend[1] is. Zoals het rapport van de commissie Korthals Altes stelt:

> Het stemmen met voorgedrukte papieren stembiljetten in een stemlokaal is transparant, controleerbaar en integer. Het proces is voor iedere kiezer te begrijpen en gade te slaan. Het is objectief vast te stellen welke stemmen er zijn uitgebracht en hoe ze zijn geteld. Hertellen is mogelijk door de papieren stembiljetten opnieuw te tellen. Doordat er geen technische middelen worden gebruikt, doet zich niet het risico voor dat de uitslag van de verkiezing beïnvloed zou kunnen worden door iets anders dan de uitgebrachte stemmen.

Ditzelfde geldt, min of meer, voor een systeem met stemmenprinters en stemmenscanners zoals voorgesteld door de commissie Van Beek [13], met dien verstande dat het gebruik van stemmenprinters het (theoretische) risico van het doorbreken van het stemgeheim met zich mee draagt, en een te grote vertrouwen in de correctheid van de stemmen scanner (en teller) uiteindelijk de controleerbaarheid en integriteit aantast. Steekproefgewijze controletellingen zijn daarom essentieel.

Verkiezingen zijn een complex proces met een unieke combinatie van waarborgen die zeer lastig allemaal in voldoende mate te vervullen zijn. Aan de ene kant worden zeer strikte betrouwbaarheidseisen en controleerbaarheidseisen gesteld, terwijl aan de andere kant stemvrijheid en stemgeheim essentieel zijn. In essentie moet een proces voor verkiezingen betrouwbaar en controleerbaar zijn, maar tegelijkertijd een 'harde knip' realiseren tussen aan de ene kant de kiezer wiens kiesgerechtigdheid op basis van zijn identiteit moet worden vastgesteld, en zijn anonieme, doch controleerbare, stem aan de andere kant.

Ieder systeem waarin het papieren proces *niet* leidend is, en waarin een uitgebrachte stem digitaal wordt geregistreerd, maakt dat de kiezer op technologie moet vertrouwen om te controleren of de stem die hij of zij wil uitbrengen ook inderdaad correct geregistreerd is[2]. En het maakt in essentie hertellingen onmogelijk, en daarmee het systeem minder controleerbaar en integer[3]. We gaan er in de rest van het rapport dus van uit dat het papieren proces leidend is.

4.2 Ondersteunt een blockchain de acht waarborgen?

Met dat gegeven als uitgangspunt rijst de vraag in hoeverre blockchain technologie ondersteunend aan of versterkend voor de acht waarborgen van de commissie Korthals Altes kan zijn.

Als we een blockchain zien als een decentrale, onweerlegbare, en onveranderbare database van transacties die voor iedereen toegankelijk is, dan ligt het voor de hand dat de waarborgen *transparantie* (vanwege de openbaarheid), *controleerbaarheid* (vanwege

[1] Papier is leidend als formeel gesproken de uitslag van de verkiezingen uiteindelijk bepaald wordt door de op papier vastgelegde stemmen. Dit is het geval als de stemmen op papier worden uitgebracht en geteld. Maar ook als bij een gedigitaliseerd stemproces uiteindelijk voor een hertelling toch de papieren bewijzen van uitgebrachte stemmen worden geteld om de uitslag te controleren en officieel vast te stellen.

[2] http://www.govtech.com/data/GT-OctoberNovember-Securing-the-Vote.html (23-03-2018).

[3] https://www.washingtonpost.com/opinions/we-need-to-hack-proof-our-elections-an-old-technology-can-help/2018/02/14/27a805bc-0c4b-11e8-95a5-c396801049ef_story.html?utm_term=.247609a98e5f (15-3-2018).

de onweerlegbaarheid) , en *integriteit* (vanwege de onveranderbaarheid) mogelijk geholpen zijn met de toepassing van blockchain technologie[4]. We gaan hier in de volgende hoofdstukken, voor elk van de te beoordelen verkiezings-proces-stappen, nader op in. Vraag is wel of hier echt een blockchain voor nodig is, aangezien de transacties zelf vanuit één (in zekere zin centrale, want de overheid) bron komen, en de volgorde van deze transacties niet van belang is. Ook moeten we niet vergeten dat, als het gaat om de integriteit, de boekhouders veel invloed hebben en dat we er op moeten vertrouwen dat (in de permissionless setting) de boekhouder die een blok mag toevoegen aan een blockchain daadwerkelijk uitgebrachte stemmen toevoegt, en niet zijn eigen voorkeuren laat prevaleren. Correctheid van uitgebrachte stemmen controleren is namelijk veel lastiger dan controleren of een Bitcoin transactie valide is. Een Bitcoin transactie is simpelweg valide als de handtekening klopt en er niet teveel bitcoins verstuurd worden. Controleren of een stem is uitgebracht door iemand die kiesgerechtigd is, is lastig als tegelijkertijd het stemgeheim bewaard moet worden.

Op basis van datzelfde (ideaal)beeld van een blockchain ligt het ook voor de hand dat juist de waarborgen *stemvrijheid* en *stemgeheim* niet, of althans niet direct, geholpen zijn met het toepassen van een blockchain. Stemvrijheid vereist dat een kiezer zijn of haar stem zonder beïnvloeding kan uitbrengen. Dit betekent dat de ruimte waarin de stem uitgebracht wordt dergelijke beïnvloeding moet voorkomen. Hierop heeft een blockchain geen invloed. Stemgeheim vereist dat niemand, ook de kiezer zelf, een koppeling kan maken tussen kiezers en de stem die ze hebben uitgebracht. Iedere vorm van registratie van stappen in het verkiezingsproces op een blockchain (of deze nu permissioned of permissionless is) ondermijnt deze waarborg. Het toepassen van blockchain technologie schaadt het stemgeheim daarom eerder dan dat het het stemgeheim helpt waarborgen.

Ook *uniciteit* is niet gegarandeerd bij het toepassen van een blockchain[5]. Het probleem is dat de boekhouders beslissen welke transacties al dan niet in het volgende blok worden meegenomen. Het is niet duidelijk hoe je, in een blockchain toepassing voor digitaal stemmen, af kunt dwingen dat boekhouders alle uitgebrachte stemmen op de juiste wijze op een blockchain registreren, en hoe je bijvoorbeeld kunt voorkomen dat een malafide boekhouder bepaalde kiezers toe staat meerdere keren te stemmen.

Voor de waarborg *kiesgerechtigheid* is de (on)toepasbaarheid van blockchain technologie minder evident. We bespreken de issues in het volgende hoofdstuk.

Ten aanzien van *toegankelijkheid* geldt in eerste instantie dezelfde argumentatie als voor stemvrijheid: de waarborg richt zich voornamelijk op de manier waarop een stem kan worden uitgebracht, en of deze manier voldoende open is voor allerlei verschillende mensen met een bepaalde handicap, bijvoorbeeld. Maar hier valt ook de groep expats onder die niet in staat zijn in Nederland zelf te stemmen. De vraag rijst dan of blockchain technologe kan helpen het proces van 'kiezen op afstand' te verbeteren. Hier gaan we nader op in in sectie 5.2. Diezelfde vraag rijst ook als het gaat om het verlenen en controleren van volmachten, of de mogelijkheid om plaatsonafhankelijk te stemmen, zie sectie 5.5.

[4] https://freedom-to-tinker.com/2017/09/12/blockchains-and-voting/ (23-03-2018).

[5] http://www.govtech.com/data/GT-OctoberNovember-Securing-the-Vote.html (23-3-2018).

Hoofdstuk 5

Gedetailleerde analyse van het gebruik van blockchains binnen het verkiezingsproces

Na de grove analyse uit het vorige hoofdstuk gaan we nu nader onderzoeken of blockchain technologie kan helpen om de volgende onderdelen van het verkiezingsproces op een verantwoorde manier te digitaliseren.

- Bepalen in het stemlokaal van de kiesgerechtigdheid door een elektronische controle van de stempas die de kiezer aanbiedt aan het stembureau.
- Internetstemmen (kiezers in het buitenland);
- Elektronisch stemmen in het stemlokaal met een stemprinter;
- Elektronisch tellen van (papieren) stembiljetten in het stemlokaal;
- Plaatsonafhankelijk stemmen in heel Nederland. Dat wil zeggen het realiseren van een landelijk raadpleegbaar kiezersregister (LKR) dat op de dag van stemming door alle stembureaus (ca 10.000) wordt geraadpleegd als een kiezer in een stemlokaal komt stemmen.

5.1 Bepalen kiesgerechtigdheid

Een belangrijke stap in het verkiezingsproces is het bepalen, in het stemlokaal, van de kiesgerechtigdheid van een kiezer. Dit wordt gedaan door een de stempas die de kiezer aanbiedt aan het stembureau te controleren. Hiertoe beschikt elk stembureau over een register van ongeldig verklaarde stempassen (ROS). Bij binnenkomst wordt de stempas van de kiezer (met stempasnummer) op het stembureau ingenomen en gecontroleerd tegen dit register. De ingenomen stempassen worden op het stembureau in pakken verzameld en verzegeld, bewaard door de gemeente, en na drie maanden vernietigd.

De vraag is of blockchain technologie dit proces van verbeteren, door de controle betrouwbaarder te maken, en door onweerlegbaar vast te leggen hoeveel mensen in een bepaald stemlokaal hebben gestemd. Dit richt zich dan met name op het verbeteren van de waarborgen *kiesgerechtigheid*, *uniciteit* en *controleerbaarheid*.

Een beperkte toepassing van een blockchain, die niet vastlegt hoeveel mensen hebben gestemd, zou zijn om het register van ongeldig verklaarde stempassen (ROS) op een blockchain vast te leggen, en op basis daarvan stempassen te controleren. Dat kan, maar dat is overkill, omdat het hier gegevens uit één betrouwbare bron (de gemeente) betreft [19], die dus net zo goed in een digitaal ondertekend bestand kunnen worden geregistreerd, waarbij de digitale handtekening het document tegen veranderingen beschermt. Bovendien is de vraag of een dergelijk register openbaar moet zijn: stempasnummers zijn, omdat ze te herleiden zijn tot personen, persoonsgegevens.

Een verdergaande toepassing van blockchain technologie[1] is om na controle de valide, gebruikte, stempassen te registreren op een blockchain. Hiermee wordt vastgelegd hoeveel mensen hebben gestemd, en wordt voorkomen dat een eventuele kopie van een stempas meer dan één keer gebruikt wordt. Er zijn verschillende manieren om deze registratie te doen, bijvoorbeeld door een 'salted hash'[2] van het stempasnummer op te slaan. Zolang de salt maar geheim is, is naderhand niet meer te controleren of een opgeslagen hash overeenkomt met een bepaald stempasnummer.

[1] Deze is bij het referendum over de Wiv in Groningen getest, zie https://www.gemeente.nu/dienstverlening/e-overheid/groningen-houdt-proef-digitaal-tellen-stemmen/ (20-3-2018).

[2] Zoals eerder al gezegd, is een hashfunctie h een functie die makkelijk uit te rekenen is, maar niet te inverteren is. Met andere woorden: gegeven een hash $x = h(d)$ van een stempasnummer d is het stempasnummer niet meer terug te herleiden. Maar, gegeven zo'n hash x en een vermoeden dat het de hash van d is, is dit wel eenvoudig te controleren. Reken simpelweg $h(d)$ en kijk of $h(d) = x$. Deze mogelijkheid om stempasnummers te controleren wordt voorkomen door een 'salt' toe te voegen. Deze salt is een willekeurig geheim nummer dat aan het te hashed stempasnummer wordt toegevoegd. Dus in plaats van $h(d)$ bereken je $h(d,s)$ waarbij s de salt is. Zonder de salt te weten kun je dan een vermoeden voor een stempasnummer d niet meer controleren

Merk op dat het stempasnummer onder meer de volgende zaken bevat: een code die aangeeft welke verkiezingen het betreft, het stemlokaal en een volgnummer. Dit is dus een uniek nummer dat voor iedere kiezer anders is. Bovendien bezit de gemeente een registratie die het stempas nummer aan een persoon koppelt. Deze registratie is nodig om, bijvoorbeeld, voor kiezers die zeggen geen stempas te hebben ontvangen het oude stempas nummer ongeldig te maken en een nieuwe stempas uit te kunnen geven[3].

Zodra de salt wel bekend is, kan de lijst met uitgegeven stempas nummers gebruikt worden om te achterhalen welke stempassen gescand zijn, en dus (via het door de gemeente beheerde register van stempas nummers) wie er bij bijvoorbeeld bij een referendum gestemd hebben. Omdat de stempassen per stembureau gescand worden, en de uitslagen ook per stembureau gepubliceerd worden, zou bij een extreme uitslag op een stembureau (veel voor of veel tegenstemmers) dus een goede inschatting gemaakt kunnen worden of iemand voor of tegen de wet heeft gestemd. In ieder geval is te achterhalen wie de wet überhaupt belangrijk genoeg vond om voor of tegen te stemmen

Omdat de salt in ieder geval gebruikt wordt door de apparatuur waarmee stempassen gescand worden en de hash van de stempasnummers op de blockchain gezet worden, is het risico dat de salt alsnog bekend wordt significant. Dit levert een bedreiging op van het *stemgeheim*.

5.2 Internetstemmen voor kiezers in het buitenland

Bij het huidige papieren verkiezingsproces moeten kiezers in het buitenland hun stem per post opsturen. Een belangrijk probleem voor deze kiezers is dat zij hun stembiljet niet of te laat ontvangen[4]. Ook is er onzekerheid of een stembiljet dat in het buitenland op de post is gedaan uiteindelijk ook in Nederland wordt meegeteld. Internetstemmen zou hiervoor een oplossing kunnen bieden.

Het fundamentele probleem van Internetstemmen voor kiezers in het buitenland is dat de omgeving waar de stem wordt uitgebracht, dat wil zeggen de PC, laptop of tablet van de kiezer, ongecontroleerd is. De PC kan malware bevatten, de laptop kan gehackt zijn. Dit betekent dat er allerlei manieren zijn waarop de uitgebrachte stem gemanipuleerd kan worden.

[3] Merk op dat dit een zwakheid in het huidige papieren proces laat zien, omdat de gemeente de stempassen (weliswaar verzegeld) bewaard maar in theorie dus kan zien wie er wel dan niet gestemd hebben.

[4] https://nos.nl/artikel/2163145-stemmen-vanuit-buitenland-blijft-probleem.html (12-4-2018).

Daarnaast is het zo dat er geen toezicht is op de manier waarop de kiezer zijn stem uitbrengt. (Dit is overigens ook een probleem bij het huidige, papieren, verkiezingsproces voor kiezers in het buitenland.) Daar waar in het stemlokaal het verboden is om met iemand mee te gaan in het stemhokje, kan de kiezer in het buitenland best samen met zijn of haar partner een stem uitbrengen. Daarmee is het risico van beïnvloeding hoog. En ook creëert dat mogelijkheden om aan te tonen wat er gestemd is, en zo de stem te verkopen.

Dit zijn geen problemen waar een blockchain een oplossing voor kan bieden.

5.3 Het uitbrengen van een stem in het stemlokaal

Zoals in hoofdstuk 4 is uitgelegd, gaan we er in deze analyse van uit dat het papieren proces leidend is, eventueel ondersteund door elektronisch stemmen in het stemlokaal met een stemprinter. Zoals in het rapport van de commissie van Beek [13] wordt besproken is het (vanwege de privacy risico's en vanwege het feit dat het papieren proces leidend moet zijn) niet gewenst dat zo'n stemprinter ook alvast de stemmen telt. In deze setting lijkt daarom geen rol weggelegd voor een blockchain.

5.4 Het tellen van de stemmen

Ook hier is het uitgangspunt dat het papier leidend is. Wel zijn er verschillende mogelijkheden om op papier uitgebrachte stemmen te tellen: dat kan volledig met de hand, of met een stemmenscanner. Het met de hand tellen kan in het stembureau zelf plaats vinden. Tellen met een stemmenscanner kan, uit kosten en beheersoverwegingen, op één centrale locatie in een gemeente plaatsvinden.

Het tellen van de stemmen en het uiteindelijk bepalen van de uitslag is een getrapt, en in eerste instantie grotendeels gedecentraliseerd proces, zoals geschetst in sectie 2.1. In dit proces wordt bij iedere stap een tussenresultaat (de uitslag van een stembureau, gemeente of kieskring) zowel op paper (in een proces verbaal, voorzien van handtekeningen) als digitaal (in een XML bestand op een USB stick) doorgegeven aan de volgende verwerker in de keten.

Het proces van tellen, het bepalen van tussenresultaten en het bepalen van de uiteindelijke uitslag is gebaat bij zo veel mogelijk transparantie. Fouten of moedwillige beïnvloeding komen op die manier aan het licht. Zo heeft Fox-IT [16] in haar analyse van OSV, de software die gebruikt wordt voor het optellen van de stemmen

en het bepalen van de uitslag, onder andere aanbevolen om de transparantie van het verkiezingsproces te verhogen, door het "op een toegankelijke wijze publiceren van de volledige digitale en de papieren gegevensstromen". Daar kun je in theorie een blockchain voor gebruiken [10]. Maar als de bronnen van deze informatie toch al vast liggen, is het voldoende om deze informatie op een openbare website te publiceren, voorzien van een digitale handtekening van de bron (bijv. het stembureau, het kiesdistrict of het centrale stembureau). Zo'n website is sowieso toegankelijker dan een blockchain, omdat je speciale software nodig hebt om de inhoud van een blockchain in te zien, terwijl een standaard browser volstaat om de website te bezoeken.

5.5 Plaatsonafhankelijk stemmen in heel Nederland

De laatste vraag is of er een rol is voor het gebruiken van blockchain technologie op plaatsonafhankelijk stemmen in heel Nederland mogelijk te maken. Dat wil zeggen het realiseren van een landelijk raadpleegbaar kiezersregister (LKR) dat op de dag van stemming door alle stembureaus (ca 10.000) wordt geraadpleegd als een kiezer in een stemlokaal komt stemmen.

Deze vraag is vergelijkbaar met de vraag of blockchain kan helpen bij het bepalen van de kiesgerechtigdheid in het stemlokaal, zoals besproken in sectie 5.1. Aan een oplossing gebaseerd op blockchain technologie kleven daarom dezelfde bezwaren als daar reeds besproken zijn.

We moeten ons hierbij bovendien realiseren dat uiteindelijk de overheid bepaalt of iemand kiesgerechtigd is, en dus de vertrouwde bron is voor de informatie in zo'n landelijk raadpleegbaar kiesregister [15]. De vraag is dan of het zinvol is om deze informatie vervolgens, met veel moeite, te decentraliseren door middel van een blockchain. Wat ons betreft is het antwoord daarop ontkennend. Een centraal te raadplegen kiesregister is makkelijker op te zetten, maar zelfs dan is de vraag hoe je het stemgeheim (met name de vraag óf iemand gestemd heeft) afdoende kunt beschermen.

Hoofdstuk 6

Conclusies

Blockchain is een nieuwe technologie die nog volop in ontwikkeling is. De ideale blockchain (die niet bestaat overigens) kan gezien worden als een decentrale, onweerlegbare, en onveranderbare database van transacties.

Grofweg kunnen we drie soorten blockchain onderscheiden. *Permissionless* blockchains (zoals Bitcoin die gebruikt), waarbij iedereen toegang heeft tot de blockchain en transacties kan inzien of toevoegen. *Permissioned maar publieke* blockchains, waar iedereen transacties op de blockchain kan inzien, maar waarbij enkel een kleine groep vooraf aangewezen boekhouders transacties aan de blockchain kan toevoegen. En tenslotte *Permissioned en gesloten* blockchains waar alleen de kleine groep vooraf aangewezen boekhouders toegang heeft tot de blockchain.

Permissionless blockchains (met een consensus mechanisme gebaseerd op proof-of-work) zijn inefficiënt, niet schaalbaar, in de praktijk slechts beperkt gedecentraliseerd, en de veiligheid en betrouwbaarheid ervan is nog niet 100% vastgesteld. Permissioned blockchains (met een consensus mechanisme gebaseerd op Byzantine Fault Tolerance protocollen) zijn veel efficiënter en wel schaalbaar, maar zijn per definitie niet echt decentraal omdat de groep boekhouders klein is en vooraf bepaald wordt. Alle blockchains vormen, zonder tegenmaatregelen, een inbreuk op de privacy als ze persoonsgegevens verwerken. In het geval van permissionless blockchains is dan ook nog eens de vraag wie de verantwoordelijke (in de zin van de Algemene Verordening Gegevensbescherming) is.

Gezien deze bezwaren is een belangrijke vraag wanneer gebruik van een blockchain noodzakelijk is, d.w.z. wanneer het echt wat toevoegt. We constateren dat een blockchain alleen noodzakelijk is als tegelijkertijd aan twee voorwaarden is voldaan: er is niet één te vertrouwen centrale partij, én de volgorde van de te verwerken transacties is van belang. Dit geeft al aan dat het gebruik van blockchain technologie in het verkiezingsproces minder voor de hand ligt dan op het eerste gezicht lijkt: de volgorde van transacties is niet van belang.

In het verkiezingsproces is het uitgangspunt dat het papier leidend is. Traditioneel is het verkiezingsproces in hoge mate gedecentraliseerd. Daarnaast worden alle stappen om tot een uitslag te komen uitgebreid gedocumenteerd en gecontroleerd, en zijn deze stappen voor iedere burger waarneembaar, met de publicatie van de processen verbaal, zoals pas sinds kort gebeurt

Het gebruik van een permissioned blockchain om het verkiezingsproces te verbeteren ligt, vanwege het zeer beperkte decentrale karakter van dergelijke blockchains, niet voor de hand. Een essentiële afhankelijkheid van het verkiezingsproces van een dergelijke blockchain zou betekenen dat een beperkt aantal entiteiten (enkele tientallen) de uitslag zouden kunnen beïnvloeden, of op zijn minst het vertrouwen in de uitslag kunnen ondermijnen.

Helaas is een keuze voor de (in theorie) zeer decentrale permissionless blockchain in de praktijk niet aan te bevelen: ook die zijn behoorlijk gecentraliseerd, hebben daarnaast nog een aantal andere grote nadelen, en bovendien is de veiligheid van dit type blockchains nog niet formeel aangetoond.

We concluderen dat, in ieder geval bij de huidige stand der techniek, het toepassen van blockchain technologie in het verkiezingsproces niet wenselijk is. We verwachten overigens niet dat die situatie, door technologische ontwikkelingen, snel zal veranderen: een echt decentrale blockchain lijkt per definitie niet schaalbaar en niet duurzaam te zijn.

Bibliografie

[1] Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn, and George Danezis. Consensus in the age of blockchains. *CoRR*, abs/1711.03936, 2017.

[2] Vitalik Buterin. Ethereum: A next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper, 2013.

[3] Christian Cachin and Marko Vukolic. Blockchain consensus protocols in the wild. *CoRR*, abs/1707.01873, 2017.

[4] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance and proactive recovery. *ACM Trans. Comput. Syst.*, 20(4):398–461, 2002.

[5] A. Efe Gencer, S. Basu, I. Eyal, R. van Renesse, and E. Gün Sirer. Decentralization in Bitcoin and Ethereum Networks. *ArXiv e-prints*, January 2018.

[6] Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In *Financial Cryptography and Data Security - 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers*, pages 436–454, 2014.

[7] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. Cryptology ePrint Archive, Report 2014/765, June 2017. https://eprint.iacr.org/2014/765.

[8] Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II*, pages 281–310, 2015.

[9] Adviescommissie inrichting verkiezingsproces (commissie Korthals Altes). *Stemmen Met Vertrouwen*. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, September 2007.

[10] Kevin Kirby, Antony Masi, and Fernando Maymi. Votebook. A proposal for a blockchain-based electronic voting system. Technical report, New York University, September 2016.

[11] Leslie Lamport, Robert E. Shostak, and Marshall C. Pease. The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 4(3):382–401, 1982.

[12] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. October 31 2008.

[13] Commissie onderzoek elektronisch stemmen in het stemlokaal (commissie Van Beek). *Elke Stem Telt. Elektronsich stemmen en tellen.* Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, December 2013.

[14] Ryan Osgood. The future of democracy: Blockchain voting. Tufts University, December 2016.

[15] Morgan E. Peck. Do you need a blockchain? *IEEE Spectrum*, 54(10):38–39,60, oct 2017.

[16] Paul Pols, Daniël Niggebrugge, and Francisco Dominguez. Onderzoek OSV en proces; rapportage. Technical Report PR-160624, Fox IT, March 2017.

[17] Gijs van de Water. Blockchain ballot. Electoral enhancement or danger to democracy? Master's thesis, Tilburg University, December 2017.

[18] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. EIP-150 Revision. (The Ethereum Yellow Paper), 2017.

[19] Karl Wüst and Arthur Gervais. Do you need a blockchain? *IACR Cryptology ePrint Archive*, 2017:375, 2017.