Blockchain: Identity Management en Distributed Network

Onderzoeksrapport

Jeffrey van Hoven

31 mei 2018

Samenvatting

Inhoudsopgave

Lijst van figuren

Woordenlijst

Symbolen

o-confirmation double spending . 7

A

account Een combinatie van public- en private keys waarbij de public key als identificatie gebruikt wordt. 10

B

block races . 7
bloom filter . 12
bootstrap node . 11

D

difficulty Een netwerk setting dat beïnvloed hoe moeilijk om het proof-of-work op te lossen. 5
double spending . 10

E

elector . 6

F

fork . 8

M

miner . 11
minting Een benaming voor de manier waarop een nieuw block gegenereerd wordt bij een Proof of Stake algoritme. 6

N

node . 10, 11, 14, 18
nonce Een 4-byte veld waarvan de waarde ingesteld wordt zodat de hash van een block een reeks van nullen bevat. De rest van de inhoud van een block staat hierdoor vast. 5

P

peer . 18
peer list . 11

S

selfish mining . 7, 20
slot leader . 6, 14
stake . 6

T

token . 6, 8
tunnel . 17, 18, 19, 21

U

UTXO-model . 14, 17

V

voting power . 5, 7

W

wallet (node) . 12

Afkortingen

B

BFT Byzantine Fault Tolerance. 4

D

DHT Distributed Hash Table. 14
DoS Denial of Service. ii, 7, 12
DPoS Delegated Proof of Stake. 6

I

I2NP I2P Network Protocol. 18, 19
I2P The Invisible Internet Project. 17, 18, 21

P

PoS Proof of Stake. 6, 15, 20
PoW Proof of Work. 5, 6, 7, 11

T

tx transactie. 11

1 Inleiding

Dit onderzoeksrapport is opgesteld in het kader van een afstudeeropdracht gedaan in opdracht van Quintor. Het betreft een onderzoek naar de Blockchain onderdelen Identity Management en Distributed Network. Het document betreft de resultaten van een onderzoek naar hoe de onderdelen Distributed Network en Identity Management gerealiseerd zijn in de Blockchain protocollen EOS, Cardano, Bitcoin en Monero.

2 Probleemstelling

Aangezien de toepassing en adoptie van Blockchain technologie steeds groter wordt wil Quintor de toepassingsmogelijkheden en technieken onderzoeken om zo inzicht te kunnen krijgen in hoe het gebruikt kan worden in de aangeboden vraagstukken vanuit klanten. Dit brengt zich tot het probleem, namelijk dat Quintor onvoldoende kennis heeft van het Blockchain domein om de toepassing ervan te kunnen adviseren in vraagstukken vanuit klanten.

3 Opzet

4 | Resultaten

4.1 Soorten netwerken

In dit hoofdstuk wordt er onderzocht welke verschillende netwerken er gebruikt worden in bestaande implementaties. Hierbij wordt zowel de definitie van soorten en de selectie van implementaties gebruikt uit de resultaten van het vooronderzoek.

"De distributie van informatie en het probleem van wederzijdse overeenstemming over een consistente staat van het netwerk vormt een uitdaging, zeker in de aanwezigheid van zelfzuchtige en/of kwaadwillende deelnemers- en B. Scheuermann (2016). Het is een uitdaging die bekend staat als het Byzantine Generals' Problem, en is beschreven door Lamport et al. (1982). Het stelt dat het essentieel is voor een betrouwbaar computersysteem om te kunnen gaan met fouten die optreden in een of meer van de componenten, waardoor het kan voorkomen dat er conflicterende informatie verstuurd wordt naar de andere componenten van het systeem. In hoeverre een computersysteem hiermee om kan gaan wordt de Byzantine Fault Tolerance (BFT) genoemd en wordt aangeduid als: $f = [\frac{N-1}{t}]$ waarbij N componenten van een computersysteem zijn en t de foutieve componenten.

In blockchain implementaties zijn de componenten die onbetrouwbaar zijn de deelnemers van het peer-to-peer netwerk. Het soort netwerk is dan ook verbonden met de manier waarop consensus bereikt wordt tussen de deelnemers van het netwerk en is getypeerd als het consensus protocol dat geïmplementeerd is.

4.1.1 Proof of Work

De originele implementatie van Blockchain technologie is gepresenteerd door Nakamoto (2008) in *"Bitcoin: A peer-to-peer electronic cash system"*. Het maakt gebruik van een algoritme genaamd Proof of Work (PoW) om consensus te bereiken. Hierbij gaat het om het oplossen van een wiskundig probleem $Y \in \mathbb{N} < f(X + n)$ waarbij f een hash functie is, n de nonce, X de data en Y de difficulty.

In het geval van Bitcoin is de Y waarde een getal die aanduid wat de difficulty is om de hash te berekenen en wordt de X waarde incrementeel opgehoogd. Een voorbeeld is gegeven in fig. 4.1. Dit proces zorgt ervoor dat de integriteit van de data in een block op de Blockchain bewaakt wordt. Wanneer een kwaadwillende deelnemer aan het netwerk de data van een block wilt aanpassen die reeds opgenomen is in de Blockchain, kan er via het PoW makkelijk gevalideerd worden of het block invalide is.

```
"Hello, world!0" => 1312af178c253f84028d480
"Hello, world!1" => e9afc424b79e4f6ab42d99c
"Hello, world!2" => ae37343a357a8297591625e
...
"Hello, world!4248" => 6e110d98b388e77e9c6f
"Hello, world!4249" => c004190b822f1669cac8
"Hello, world!4250" => 0000c3af42fc31103f1f
```

Figuur 4.1: Werking Proof-of-Work, van Bitcoin Wiki (2010). Wanneer de eerste vier bits ($Y = 4$) van de hash 0 zijn is de proef opgelost.

Daarnaast beschrijft de bedenker van het protocol, Satoshi Nakamoto, het PoW algoritme als 'one-CPU-one-vote'. Aangezien het gebruikte hashing algoritme geen limitaties stelt tot de zogeheten voting power van een deelnemer in het netwerk creëert het gunstige omstandigheden voor high-end GPU eigenaren tegenover high-end CPU eigenaren (Van Saberhagen, 2013, p. 2).

Monero maakt gebruik van het CryptoNight algoritme (Noether et al., 2014), een implementatie gebaseerd op CryptoNote, waarin gebruik gemaakt wordt van een egalitair Proof of Work (Van Saberhagen, 2013, p. 11). In contrast met het Bitcoin protocol Proof of Work algoritme is het ontworpen om inefficiënt berekenbaar te zijn op een GPU, waardoor er gelijke kansen zijn voor de deelnemers van het netwerk die het mining proces uitvoeren.

4.1.2 Proof of Stake

"Een eerste overweging met betrekking tot de werking van blockchain protocollen gebaseerd op Proof of Work – zoals Bitcoin – is de energie benodigd voor hun uitvoering.- Kiayias et al. (2017). In een onderzoek gedaan door O'Dwyer en Malone in 2014 naar het energieverbruik van het Bitcoin mining netwerk is geschat dat onder redelijke omstandigheden het netwerk gelijk stond met het energiegebruik van Ierland. Om deze reden zijn er onderzoeken en experimenten gedaan naar alternatieve consensus algoritmes. Proof of Stake (PoS) is een consensus algoritme waarbij, in plaats van het verspillen van elektriciteit om zware rekenkundige problemen op te lossen, een deelnemer geselecteerd wordt om het volgende blok te genereren (doorgaans minting genoemd) op basis van willekeurige selectie en rijkdom of leeftijd (i.e., de stake).

Cardano maakt gebruik van PoS waarbij iedere deelnemer van het netwerk met een positief balans (e.g. stake) als stakeholders gezien worden. Om uitgekozen te worden om een nieuw block te genereren moet een stakeholder geselecteerd worden als slot leader. De implementatie verdeelt de fysieke tijd in tijdvakken en elke tijdvak is verdeeld in slots. Voor elke slot wordt een slot leader verkozen, die verantwoordelijk is voor het produceren van één blok. Niet alle deelnemers van het netwerk, bijvoorbeeld die minder dan 2% van de totale circulatie van tokens hebben, worden geselecteerd om benoemd te worden tot slot leader. Deze groep van deelnemers maken deel uit van de electors groep. Electors verkiezen nieuwe slot leaders gedurende het huidige tijdsvak, waarna er een selectie gemaakt wordt en de nieuwe slot leaders vaststaan voor het volgende tijdsvak. Hoe meer stake een deelnemer heeft, hoe groter de kans dat zij uitgekozen wordt om een slot leader te worden in het volgende tijdsvak. De slot leader luistert naar transacties die aangekondigd worden door andere nodes, bundelt ze in een nieuw block, signeert het met zijn private key en publiceert het block in het netwerk (Cardano Docs, 2013c).

EOS is een implementatie die gebruik maakt van Delegated Proof of Stake (DPoS) om consensus te bereiken. Het grote verschil tussen DPoS en PoS; in een PoS systeem is elke deelnemer die stake heeft maakt onderdeel uitmaken van het validatie- en consensusproces. Met DPoS kan elke deelnemer die stake heeft andere deelnemers verkiezen die onderdeel uitmaken van het validatie- en consensusproces (Roman, K. , 2018). In contrast met het PoW algoritme is er geen competitie voor het produceren van een block, maar wordt er samengewerkt om een block te produceren.

4.2 Gevaren

Wanneer deelnemers uitmaken van een grootschalig netwerk die niet gecontroleerd wordt door een centrale autoriteit kan het voorkomen dat deelnemers zich misdragen. In juli 2016 is Ethereum opgesplitst in twee partities die dezelfde valuta hanteren; *Ethereum* en *Ethereum Classic*. Dit is veroorzaakt door een kwaadwillende deelnemer in het netwerk die door een bug in het systeem geld naar zichzelf toe kon sturen. Dit heeft ertoe geleid dat veel gebruikers mogelijk een aanzienlijk verlies geleden hebben, waaronder veel ontwikkelaars van Ethereum. Om dit verlies op te lossen werd er een hard-fork voorgesteld die Ethereums code aanpast waarbij de transacties van de kwaadwillende deelnemer teruggedraaid werden (Kiffer, Levin & Mislove, 2017).

Dit illustreert een van de mogelijke manieren waarop een kwaadwillende gebruiker het systeem kan ondermijnen. Om een duidelijk overzicht te geven van de gevaren binnen een gedecentralizeerd peer-to-peer systeem wordt er onderzocht welke technieken toegepast worden om aanvallen van een kwaadwillende deelnemer van het netwerk tegen te gaan.

4.2.1 Eclipse Attack

Een aanval op het peer-to-peer netwerk waarbij er controle over een deelnemer zijn toegang tot informatie gelimiteerd, of zelfs gemanipuleerd wordt. Met de juiste manipulatie van het peer-to-peer netwerk kan er informatie verduistert worden zodat een goedwillende deelnemer aan het netwerk alleen maar kan communiceren met kwaadwillende deelnemers. Dit kan leiden tot block races, selfish mining en 0-confirmation double spending (Heilman, Kendler, Zohar & Goldberg, 2015).

4.2.2 Majority Attack

Een aanval waarbij één deelnemer de richting van het netwerk bepaald door het bezitten van 51% de voting power. In het geval van Proof of Work betekend dit dat de kwaadwillende deelnemer 51% van de totale rekenkracht nodig heeft om deze aanval uit te voeren. Dit stelt de kwaadwillende deelnemer in staat om het netwerk te manipuleren en kan leiden tot 0-confirmation double spending.

4.2.3 Denial of Service (DoS)

Een algemene benaming voor een collectie van mogelijke oorzaken voor een bewuste verstoring van de services die het peer-to-peer netwerk faciliteert. Dit kan op meerdere ma-

nieren optreden, bijvoorbeeld door het invoegen van heel veel transacties in één block, zodat het lang duurt voordat het peer-to-peer netwerk het nieuwe block heeft opgenomen.

4.2.4 Sybil Attack

Een aanval waarbij een deelnemer meerdere virtuele deelnemers creëert in het netwerk waarbij de gecreëerde deelnemers het verkiezingsproces kunnen verstoren door verkeerde informatie door te geven in het netwerk, zoals positief stemmen voor een malafide transactie (Conti, Lal, Ruj et al., 2017).

4.2.5 Double spending

Bij Creditcard-gebaseerde betalingen wordt er eerlijkheid bereikt door het bestaan van een bank of een andere vertrouwde tussenpersoon (e.g. Paypal). Hierbij wordt de tussenpersoon vertrouwd om te controleren dat diegene die een betaling doet aan een derde partij het geld niet al heeft uitgegeven (G. Karame, Androulaki & Capkun, 2012). In gedecentraliseerde systemen, waarbij er geen vertrouwe tussenpersoon aanwezig is, staat dit bekend als het *double spending* probleem, waarbij het mogelijk is om tokens die reeds uitgegeven zijn (i.e. opgenomen in een block) nogmaals gebruikt wordt om een transactie uit te voeren.

4.2.6 Nothing at Stake

Wanneer er een fork ontstaat is de optimale strategie elke replica van de blockchain te valideren, zodat de diegene die het validatie proces uitvoert nog steeds uitbetaald krijgt, ongeacht of de fork geaccepteerd wordt of niet.

4.3 Identiteit

Blockchain kan een zeker mate van privacy garanderen door de public en private keys, wat ervoor zorgt dat een gebruiker niet zijn echte identiteit hoeft te hanteren om met het systeem te interacteren. Echter, Meiklejohn et al. (2013) toont aan dat blockchain niet de transactionele privacy kan waarborgen omdat de waarden van alle transacties en saldo van elke public key openbaar inzichtbaar zijn.

Okamoto (1992) beschrijft zes criteria waaraan de ideale implementatie van elektronisch geld moet voldoen. In het bijzonder worden er twee criteria genoemd:

- **Untraceability:** voor elke inkomende transactie hebben alle mogelijke afzenders gelijke kansen om geïdentificeerd te worden als verstuurder.

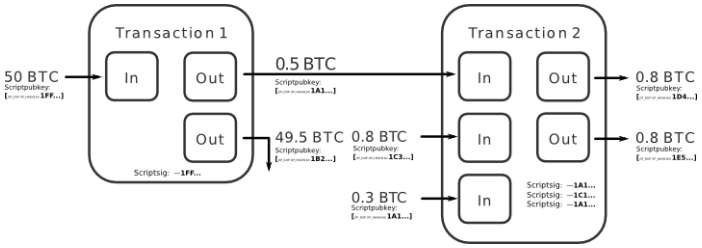
- **Unlinkability:** voor elke twee uitgaande transacties moet het onmogelijk zijn om aan te tonen dat ze naar dezelfde persoon verstuurd zijn.

4.4 Bitcoin

4.4.1 Functionaliteit

Architectuur Bitcoin is een netwerk waarin geen coördinerende rollen zijn. Elke deelnemer van het netwerk heeft een complete replica van alle informatie die benodigd is voor het verifiëren van de validiteit van binnenkomende transacties. Er zijn verschillende services die het netwerk faciliteert die kort toegelicht zijn in **??**, twee daarvan zijn met name belangrijk voor de beschrijving van het netwerk: netwerk routing, en het mining proces. In de basis van het netwerk staan de transacties die op abstract niveau bitcoins van een of meer accounts naar een of meer bestemmingsaccounts overmaken. Een account, in de context van het bitcoin netwerk, is een combinatie van een public- en private key, waarbij de public key als identificatie van de account gebruikt wordt. Om een transactie te versturen wordt de transactie gesigneerd met de private key van de account die de transactie wilt uitvoeren.

Transacties bestaan uit een input en output. In plaats van het aggregeren van een balans voor elk account, wordt er bijgehouden wat de output van een transactie is. De balans is hierbij de som van alle openstaande outputs van het desbetreffend account. In fig. 4.2 is te zien hoe dit in zijn werk gaat. Een onderdeel van de services die de nodes binnen het netwerk aanbieden is het valideren van transacties. Hierbij worden drie onderdelen gevalideerd:



Figuur 4.2: Voorbeeld van het UTXO-model zoals in gebruik bij Bitcoin, bron: http://news.8btc.com/thoughts-on-bytom-design-extension-of-utxo-structure.

- Een output mag maar één keer geclaimd zijn.
- Nieuwe outputs worden alleen gecreëerd door een transactie.
- De som van alle waardes van de geclaimde outputs moet groter zijn als de totale som van de nieuwe gecreëerde outputs.

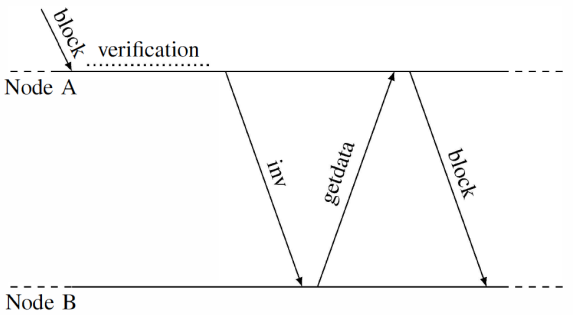
Wanneer dit het geval is wordt de transactie geaccepteerd en opgenomen in de lokale replica van de blockchain. Over tijd kan het voorkomen dat de replica van verschillende nodes inconsistent worden, waarbij het kan voorkomen dat er twee of meer transacties dezelfde coin meerdere malen uitgeeft. Dit staat bekend als double spending (Decker & Wattenhofer, 2013).

Een nieuw block wordt gecreëerd door het uitvoeren van het mining proces. Dit wordt uitgevoerd door zogenaamde miners node. Om te bepalen welke node verantwoordelijk is voor het volgende block moet er een oplossing gevonden worden voor het proof-of-work. Dit proces zorgt ervoor dat er een beslissing gemaakt wordt over de volgorde van de transacties, en dat de inhoudt van een block niet aangepast kan worden omdat dit in directe verbinding staat met het gedane PoW.

Discovery protocol Om het het netwerk te betreden worden er DNS servers benaderd waarbij gebruik wordt gemaakt van het TCP protocol. Deze DNS servers worden in stand gehouden door vrijwilligers en geven een willekeurige set aan bootstrap nodes terug die actief zijn in het netwerk. Wanneer de node toegetreden is tot het netwerk wordt er een peer list bijgehouden met alle nodes waarmee er connectie is gelegd. Deze peer list wordt gebruikt om connectie te leggen bij een eerstvolgende toetreding tot het netwerk.

Informatie propagatie Voor het updaten en synchroniseren van de blockchain worden er transactie (tx) en block berichten verstuurd. Om tegen te gaan dat tx- en block berichten verstuurd worden naar nodes die al afweten van deze informatie, wordt er een *inv* bericht verstuurd wanneer een transactie of een block volledig geverifieerd is. Het *inv* bericht bevat een lijst van transactie- en block hashes die reeds ontvangen zijn door de verstuurder en die beschikbaar zijn om opgehaald te worden.

Wanneer een node deze informatie wilt ontvangen (bijv. omdat het de informatie nog niet heeft), wordt er een *getdata* bericht verstuurd naar de verstuurder van het *inv* bericht, met daarin de hashes van de informatie die de node wilt hebben. Fig. 4.3 visualiseert dit proces.



Figuur 4.3: Berichten die verzonden worden om informatie over een block uit te wisselen (Decker & Wattenhofer, 2013, p. 4).

4.4.2 Gevaren

Majority Attack Nakamoto (2008) stelt dat het uitvoeren van een majority attack op het netwerk onpraktisch is omdat het uitvoeren ervan niet opweegt tegen de kosten voor de benodigde hardware om de rekenkracht te behalen die hiervoor nodig is. Dit blijkt niet altijd het geval, Eyal en Sirer (2014) beschrijft namelijk een strategie genaamd Selfish Mining waarbij er gevalideerde blocks achtergehouden worden voor het netwerk waardoor er opzettelijk een fork wordt gecreëerd. De eerlijke miners zullen verder werken aan de publiekelijke blockchain terwijl de uitvoerder van het Selfish Mining strategie verder werkt op de achtergehouden blockchain. Als de uitvoerder meer blokken ontdekt onstaat er een voorsprong op de publiekelijke blockchain en worden de blocks nog steeds achtergehouden. Wanneer de lengte van de publiekelijke blockchain de lengte van de achtergehouden

blockchain benaderd, zal de uitvoerder de blockchain publiceren. Dit leid ertoe dat miners die het Bitcoin protocol volgen hun middelen verspillen aan het minen van cryptopuzzles die er niet toe doen.

Denial of Service Over de jaren heen zijn er kwetsbaarheden in het Bitcoin protocol geïdentificeerd die het mogelijk maken om een DoS aanval uit te voeren. De meest recente[1] aanval (NIST, 2013) exploiteert een zwakheid in de implementatie van een Bloom filter, een filter die onder andere gebruikt wordt door wallets om alleen transacties binnen te halen waarbij de deelnemer betrokken is. Hierdoor was het mogelijk om een sequentie van berichten te sturen die ervoor zorgde dat een volledige node binnen het netwerk overbelast werd.

Eclipse Attack Heilman et al. heeft aangetoond dat Bitcoin's peer discovery mechanisme toegankelijk is voor een *Eclipse attack*. Door de manier waarop het Peer Discovery mechanisme werkt is het mogelijk om de lijst van connecties zo te manipuleren dat nieuwe deelnemers doorgestuurd worden naar kwaadwillende deelnemers.

Double spending G. O. Karame, Androulaki en Capkun toont aan dat het in het beginstadium van het Bitcoin protocol mogelijk was om via zogenaamde 'fast payments' een double spending aanval uit te voeren.

4.4.3 Identiteit

Er zijn drie onderdelen van het Bitcoin systeem die interessant zijn voor het analyseren van het systeem in relatie tot de identiteit van de gebruiker. Ten eerste is de gehele historie van Bitcoin transacties publiekelijk in te zien. Zoals eerder vermeld is dit nodig om zonder centrale autoriteit validatie van de transacties te doen. Het tweede is het UTXO-model dat gebruikt wordt om uitgaves en inkomsten bij te houden. In dit model bestaat een transactie uit meerdere inputs en outputs, waarbij de input een eerdere output van een transactie is geweest. Ten derde zijn de betaler en de ontvanger van een transactie gekoppeld aan de transactie door middel van een public key.

Reid en Harrigan (2013) stelt dat deze drie onderdelen, met name de publieke toegankelijkheid van de Bitcoin transacties en de input-output relatie tussen transacties en publickeys, ingedeeld kunnen worden in twee verschillende netwerken die tesamen opereren, het *transaction network* en het *user network*. Waarbij het *transaction network* de stroom van Bitcoins beschrijft tussen transacties over de tijd, en het *user network* tussen gebruikers over de tijd. Door het analyseren van de structuur van deze twee netwerken aan de hand

[1] Er zijn recentere aanvallen op het Bitcoin protocol geweest waarbij er DoS aanval heeft plaatsgevonden maar deze zijn niet nader gespecificeerd, zie: "Common Vulnerabilities and Exposures - Bitcoin Wiki".

van de informatie uit het Bitcoin netwerk, is er geconcludeerd dat het mogelijk is om verschillende public keys met elkaar te associëren, en het met de juiste middelen het mogelijk is om de activiteit van een gebruiker gedetailleerd in kaart te brengen.

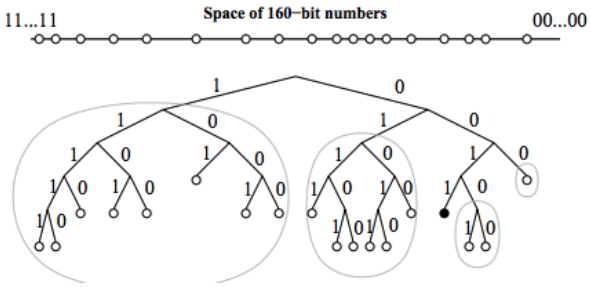
Hierbij voldoet het bitcoin protocol met name niet aan de de untraceability eis. Alle transacties die gedaan worden tussen de deelnemers van het netwerk zijn publiekelijk in te zien en elke transactie kan herleid worden naar de verstuurder en ontvanger. Ook is het indirect mogelijk om twee uitgaande transacties naar dezelfde persoon aan te tonen binnen het netwerk.

4.5 Cardano

4.5.1 Functionaliteit

Architectuur Net zoals bij Bitcoin zijn de transacties de kern van de implementatie, waarbij er wederom gebruik wordt gemaakt van het UTXO-model zoals beschreven bij de architectuur van Bitcoin. De architectuur van het Cardano netwerk bestaat uit drie soorten nodes die fundamenteel zijn voor de werking van het protocol: *core*, *relay* en *edge* nodes.*Core nodes* zijn de kern van het netwerk. Het zijn de enige nodes die geselecteerd kunnen worden om slot leader te worden, waardoor het de enige nodes zijn die een block kunnen creëren. *Relay nodes* worden gezien als de proxy tussen core nodes en het internet. Ze hebben geen stake in het netwerk, waardoor ze makkelijk te verplaatsten of veranderd kunnen worden. *Edge nodes* zijn de simpele nodes die iedereen kan uitvoeren. Deze nodes kunnen transacties aanmaken binnen het netwerk en aanbieden aan *core* nodes via de *relay* nodes (Cardano Docs, 2013a, Topology).

Discovery protocol Om het netwerk te betreden wordt er gebruik gemaakt van een bestaand protocol genaamd Kademlia, wat gebaseerd is op het gebruik van een Distributed Hash Table (DHT) architectuur. Elke node wordt behandeld als een tak in een Binary Tree waarbij de positie van een node bepaald wordt door een unieke prefix van de identificatie code van een node. In fig. 4.4 is de positie van een node met de prefix 0011 te zien. Het protocol garandeert dat elke node in verbinding staat met een andere node. Met deze garantie kan elke node een andere node lokaliseren aan de hand van de identificatie code (Maymounkov & Mazieres, 2002, p. 2).



Figuur 4.4: Binary Tree zoals in gebruik bij het Kademlia protocol, Maymounkov en Mazieres (2002).

Informatie propagatie

Berichten worden verstuurd voor het uitwisselen van informatie tussen deelnemers. Hierbij zijn drie abstracte types gedefinieerd: *inv*, *req* en *data*. Net zoals bij Bitcoin wordt de *inv* message gebruikt om aan te geven dat er data beschikbaar is. Het *req* bericht wordt vervolgens gebruikt om beschikbare data op te vragen. De data wordt vervolgens verstuurd

via een *data* message. Berichten die bijvoorbeeld een block versturen zijn nader gespecificeerde *data* berichten. Op deze drie types zijn alle berichten in het netwerk gebaseerd, bijvoorbeeld is het *MsgBlock* bericht, die block informatie uitwisselt, gebaseerd op een *data* bericht (Cardano Docs, 2013b). Een bericht kan verstuurd worden naar drie verschillende mediums: het versturen van een bericht naar een node, de buren, en het gehele netwerk. Naar welk medium het bericht wordt verstuurd is opgenomen in de header van een bericht.

4.5.2 Gevaren

Sybil Attack Een fundamenteel probleem bij een implementatie van PoS, zoals beschreven door (Kiayias et al., 2017), is het simuleren van een leiderschapsverkiezing. Om een eerlijke, willekeurige verkiezing onder deelnemers van het netwerk te hebben is het nodig om een zekere mate van wanorde te introduceren. Mechanismes die benodigd zijn om deze wanorde te introduceren zijn gevoelig voor beïnvloedingen van kwaadwillende deelnemers in het netwerk.

Eclipse attack In het Kademlia netwerk is het mogelijk om een eclipse attack uit te voeren, maar wel lastig. In Cardano Docs (2013b) wordt uitgelegd hoe dit mogelijk zou zijn. Door de manier waarop het netwerk ingedeeld is, is het mogelijk, indien het netwerk constant blijft, om door veel nodes in het netwerk aan te maken de IDs rondom een bestaande node te bezitten, waardoor de communicatie met deze node te manipuleren is. Om dit tegen te gaan heeft Monero een uitbreiding gerealiseerd op het Kademlia protocol, waarbij node IDs vervangen worden door HashIds.

Een HashId is een binaire reeks van 32 bytes bestaande uit twee onderdelen. De nonce, een willekeurige 14 reeks aan bytes binaire reeks, en hashing data dat gegenereerd wordt aan de hand van de zogenaamde DerivingKey, een PBKDF2 hash dat gebruik maakt van HMAC (Hash-based Message Authentication Code) en een Salt, een SHA-512 hash (Cardano Docs, 2013a, P2P Layer, Addressing).

4.5.3 Identiteit

De cardano implementatie is een public Blockchain waarbij alle transacties inzichtbaar zijn en iedereen mee kan doen aan het consensus proces. Het maakt gebruik van public- en private keys om pseudonimiteit te waarborgen, waarbij de elliptic curve cryptografie implementatie Curve25519 toegepast wordt om de public- en private key te genereren. Binnen Cardano worden er verschillende adressen gebruikt om transacties van een bestemming te voorzien (Cardano Docs, 2013a, "Addresses in Cardano SL"):

1. **public key address**
   Een base58 gecodeerde string van de public key dat gebruikt wordt als bestemming van een transactie.

2. **script address**
   Wordt gebruikt voor het Pay to Script Hash principe, waarbij er in plaats van de public key gebruikt wordt als bestemming, een validatie script verstuurd wordt die gebruik maakt van een zogenaamde redemption script. Om de waarde van de transactie te claimen dient het validatie script positief uit te vallen.

3. **redeem address**
   Wordt gebruikt voor het Pay to Public Key Hash principe, waarbij er een hash gecreëerd wordt wat ervoor zorgt dat de public key alleen publiekelijk geregistreerd wordt wanneer de output van een transactie wordt uitgegeven.

4.6 EOS

4.6.1 Functionaliteit

https://steemit.com/eos/@trogdor/eos-vs-ethereum-for-dummies

De blockchain implementatie EOS werkt toe naar een operating systeem speciaal voor blockchain toepassingen. In eerste instantie zal er een Blockchain gerealiseerd worden die dient als proof-of-concept van het ontwerp. In dit proof-of-concept is er een eerste versie gerealiseerd die het mogelijk maakt voor developers om een eigen applicatie op het EOS netwerk te creëren. Hierbij is de focus gelegd het faciliteren van functionaliteiten die betrekking hebben op account permissies, authenticatie en de communicatie tussen het internet en het netwerk. Er wordt gespeculeerd dat EOS een sterke concurrent van Ethereum zal worden als het gaat om Blockchain als een developer platform.

Architectuur EOS maakt gebruik van aanpak waarbij extensies op de basis componenten (e.g. het netwerk, de 'chain', etc.) gerealiseerd worden als plugins. Dit maakt het zodat het protocol makkelijk te wijzigen is in de toekomst.

Discovery protocol

Informatie propagatie

4.6.2 Gevaren

TODO

4.6.3 Identiteit

EOS is een consortium Blockchain waarin de identiteit van een gebruiker vastgelegd wordt in een account model, waarbij een account identificeerbaar is door een unieke naam van maximaal twaalf karakters. Handeling zijn geresticteerd door middel van een Role Based Permissie systeem. Om dit mogelijk te maken dient een gebruiker allereerst geautoriseerd te zijn alvorens deel te kunnen nemen aan het netwerk. Centraal in de implementatie staat de notie van Actions & Handlers. Elk account (i.e. deelnemer) heeft een eigen database die alleen toegankelijk is door gedefinieerde action handlers. Dit systeem is soortgelijk aan smart contracts zoals in gebruik bij Ethereum.

4.7 Monero

4.7.1 Functionaliteit

Architectuur Monero maakt gebruik van The Invisible Internet Project (I2P) protocol. Het I2P protocol stelt het netwerk in staat om deelnemers te beschermen tegen een zekere mate van verkeer; waarbij de identiteit van de verstuurder en ontvanger verborgen wordt, terwijl er gebruik gemaakt wordt van encryptiestandaarden om de inhoud van berichten te verbergen en te garanderen dat het bericht aankomt (Zantout & Haraty, 2011). Het protocol ondersteund zowel TCP/IP als UDP/IP communicatie, waarbij de Transport laag in het network van Monero gelimiteerd is aan de mogelijkheden die I2P ondersteund (Monero, 2017b). De transport laag faciliteert de connectie tussen de verschillende deelnemers in het netwerk. Om vervolgens te kunnen communiceren wordt er gebruik gemaakt van een tunnel. Elke deelnemer in het netwerk heeft minimaal twee Tunnels, een voor uitgaand- en inkomend verkeer. Wanneer er communicatie plaatsvind tussen twee deelnemers zullen er vier tunnels aangemaakt worden; twee voor uitgaand verkeerd en twee voor inkomend verkeer (Monero, 2017d). Ook Monero maakt gebruik van het UTXO-model, waarbij er bij iedere transactie twee keys aanwezig zijn; een spend key en een view key. Beide keys zijn onderdeel van een account, waarbij de spend key gebruikt wordt om geld uit te geven, en de view key gebruikt wordt om permissie te geven om de transacties in te zien van een deelnemer. De keys spelen een belangrijke rol in de privacy van de deelnemer omtrent transacties (Monero, 2017a).

Discovery protocol Het discovery protocol in gebruik bij Monero is soortgelijk aan de manier waarop Bitcoin het discovery proces uitvoert. Om het netwerk te bootstrappen wordt er gebruik gemaakt van nodes die vastgelegd zijn in de broncode, waarna er een lijst van peers wordt teruggegeven aan de deelnemer en de centrale node vergeten wordt. Het is ook mogelijk om zelf deelnemers vast te leggen waarna geprobeerd wordt om connectie te maken.

Informatie propagatie Alles binnen het I2P netwerk wordt gecommuniceerd via berichten. In het onderdeel architectuur is er kort gesproken over Tunnel en de functionaliteiten die ermee gerealiseerd wordt. Er zijn twee soorten berichten die verzonden worden: Tunnel berichten en I2P Network Protocol (I2NP) berichten[2]. Het proces, zoals beschreven in Monero (2017c):

- De Tunnel verzameld I2NP berichten en verwerkt ze naar Tunnel berichten. Hierbij kan het voorkomen dat I2NP berichten gefragmenteerd worden omdat ze van variabele grootte zijn, terwijl Tunnel berichten een vaste grootte hebben.

[2]Zie "I2NP Specifiation - I2P | Overview" voor de verschillende types.

- De Tunnel encrypt de verwerkte data en stuurt het door in de vorm van Tunnel berichten.
- De deelnemer, en andere deelnemers die deel uitmaken van de Tunnel, pakken een laag van de encryptie uit en verifiëren dat het bericht geen duplicaat is en sturen het vervolgens door naar een volgende deelnemer.
- Met de tijd zullen de Tunnel berichten het eindpunt bereiken waarna ze terug worden gezet naar de originele I2NP berichten.

4.7.2 Gevaren

TODO

4.7.3 Identiteit

TODO

5 Conclusie

In dit onderzoek is er gezocht naar een antwoord op de vraag: "Welke protocol implementaties kunnen toegepast worden om de onderdelen Distributed Network en Identity Management te realiseren voor een Blockchain implementatie?". Hiervoor is kwalitatief onderzoek uitgevoerd naar de Blockchain implementaties, EOS, Cardano, Monero en Bitcoin.

1. **"Welke soorten gedistribueerde netwerken worden er gebruikt in de implementaties?"**
   Een gedistribueerd netwerk binnen Blockchain is getypeerd aan het consensus protocol dat gebruikt wordt. In het onderzoek zijn er twee soorten geïdentificeerd, netwerken die gebruik maken van Proof of Stake of van Proof of Work.

2. **"Hoe werken de gedistribueerde netwerken van de implementaties en tegen welke gevaren zijn ze bestendig?"**
   In het onderzoek is de functionaliteit beschreven die ondersteund wordt door een gedistribueerde netwerk van een implementatie en is er aandacht besteed aan de oplossingen die het netwerk gebruikt om aanvallen tegen te gaan.

   - **Bitcoin**
     Het netwerk van Bitcoin communiceert via TCP/IP en maakt gebruik van bootstrap nodes waarmee connectie wordt gemaakt op het moment dat een nieuwe deelnemer het netwerk wilt toetreden. Informatie wordt verstuurd door een voorafgedefinieerde set aan berichttypes: *inv*, *tx*, *block*, *getdata*, waarbij een *inv* bericht gebruikt wordt ter inventarisatie over de beschikbaarheid van data, *tx* bericht om een transactie te versturen, *block* bericht om een block te versturen, *getdata* bericht om data op te vragen.

     Op het Bitcoin netwerk zijn meerdere aanvallen in de loop der jaren uitgevoerd en geïdentificeerd, een studie uit 2015 gedaan door Heilman et al. (2015) toont aan dat het Peer Discovery mechanisme vatbaar is voor een Sybil Attack. Nakamoto (2008) stelt dat de voordelen van het uitvoeren van een majority attack niet opweegt tegen de kosten voor de benodigde hardware om de rekenkracht te behalen. Eyal en Sirer (2014) beschrijft dat het niet nodig is om een merendeel van de rekenkracht te bezitten en introduceert de aanval selfish mining.

   - **Cardano**
     Het netwerk van Cardano communiceert via TCP/IP en maakt gebruik van het

Kademlia protocol waardoor het maar nodig is om één bootstrap node te gebruiken om het netwerk toe te treden. De achterliggende structuur van Kademlia is een Binary Tree waarbij de positie van een deelnemer in de Binary Tree bepaald wordt door een unieke prefix van de identificatiecode. Het protocol garandeert dat een deelnemer in verbinding staat met ten minste één andere deelnemer. Informatie wordt uitgewisseld door drie abstracte berichttypes: *inv*, *req*, en *data*. Het *inv* bericht wordt gebruikt om aan te geven dat er data beschikbaar is, het *req* bericht wordt gebruikt om beschikbare data op te vragen en het *data* bericht wordt vervolgens gebruikt om de data te versturen.

Implementaties die gebruik maken van PoS zijn afhankelijk van de manier waarop een leiderschapsverkiezing wordt gesimuleerd, waarbij er grote kans is dat het gevoelig is voor beïnvloedingen van kwaadwillende deelnemers in het netwerk in de vorm van een Sybil Attack. Cardano heeft een zwak punt in het Kademlia netwerk geïdentificeerd waardoor het mogelijk zou zijn om Eclipse Attack uit te voeren.

- **Monero**
  Het netwerk van Monero maakt gebruik van het The Invisible Internet Project (I2P) protocol, dat zowel UDP/IP als TCP/IP ondersteund. Om het netwerk toe te treden wordt er gebruik gemaakt van bootstrap nodes die vastgelegd zijn in de broncode. Communicatie wordt gedaan door middel van Tunnels, waarbij elke deelnemer twee Tunnels, een inkomende en een uitgaande, heeft voor elke connectie.

- **EOS**
  TODO

3. **"Hoe wordt er omgegaan met de identiteit van de gebruiker binnen de implementatie?"**

Literatuur

Roman, K. . (2018). *Understanding eos and delegated proof of stake — steemit.* Verkregen van https://steemit.com/eos/@eosgo/understanding-eos-and-delegated-proof-of-stake

Bitcoin Wiki. (2010). *Proof of work.* Verkregen van https://en.bitcoin.it/wiki/Proof_of_work ([Online; benaderd op 29 maart, 2018])

Cardano Docs. (2013a). *Cardano.* Verkregen van https://cardanodocs.com/technical/protocols/p2p/#addressing

Cardano Docs. (2013b). *Csl application-level messaging - cardano.* Verkregen van https://cardanodocs.com/technical/protocols/csl-application-level/

Cardano Docs. (2013c). *Ouroboros proof of stake algorithm - cardano.* Verkregen van https://cardanodocs.com/cardano/proof-of-stake/

Conti, M., Lal, C., Ruj, S. et al. (2017). A survey on security and privacy issues of bitcoin. *arXiv preprint arXiv:1706.00916*.

Decker, C. & Wattenhofer, R. (2013, Sept). Information propagation in the bitcoin network. In *Ieee p2p 2013 proceedings* (p. 1-10). doi: 10.1109/P2P.2013.6688704

en B. Scheuermann, F. T. (2016, thirdquarter). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys Tutorials*, *18*(3), 2084-2123. doi: 10.1109/COMST.2016.2535718

Eyal, I. & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security* (pp. 436–454).

Heilman, E., Kendler, A., Zohar, A. & Goldberg, S. (2015). Eclipse attacks on bitcoin's peer-to-peer network. In *Usenix security symposium* (pp. 129–144).

Karame, G., Androulaki, E. & Capkun, S. (2012). Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin. *IACR Cryptology ePrint Archive*, *2012*(248).

Karame, G. O., Androulaki, E. & Capkun, S. (2012). Double-spending fast payments in bitcoin. In *Proceedings of the 2012 acm conference on computer and communications security* (pp. 906–917).

Kiayias, A. et al. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual international cryptology conference* (pp. 357–388).

Kiffer, L., Levin, D. & Mislove, A. (2017). Stick a fork in it: Analyzing the ethereum network partition. In *Proceedings of the 16th acm workshop on hot topics in networks* (pp. 94–100).

Lamport, L. et al. (1982). The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, *4*(3), 382–401.

Maymounkov, P. & Mazieres, D. (2002). Kademlia: A peer-to-peer information system based on the xor metric. In *International workshop on peer-to-peer systems* (pp. 53–65).

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M. & Savage, S. (2013). A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on internet measurement conference* (pp. 127–140).

Monero. (2017a). *Account | moneropedia | monero - secure, private, untraceable.* Verkregen van `https://getmonero.org/resources/moneropedia/account.html`

Monero. (2017b). *Kovri | moneropedia | monero - secure, private, untraceable.* Verkregen van `https://getmonero.org/resources/moneropedia/kovri.html`

Monero. (2017c). *Message | moneropedia | monero - secure, private, untraceable.* Verkregen van `https://getmonero.org/resources/moneropedia/message.html`

Monero. (2017d). *Tunnel | moneropedia | monero - secure, private, untraceable.* Verkregen van `https://getmonero.org/resources/moneropedia/tunnel.html`

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

NIST. (2013). *Nvd - cve-2013-5700.* Verkregen van `https://nvd.nist.gov/vuln/detail/CVE-2013-5700` ([Online; benaderd op 6 april, 2018])

Noether, Y. et al. (2014). Monero is not that mysterious. *Technical report*.

O'Dwyer, K. J. & Malone, D. (2014). Bitcoin mining and its energy footprint..

Okamoto, K., Tatsuaki en Ohta. (1992). Universal electronic cash. In *Proceedings of the 11th annual international cryptology conference on advances in cryptology* (pp. 324–337). London, UK, UK: Springer-Verlag. Verkregen van `http://dl.acm.org/citation.cfm?id=646756.705374`

Reid, F. & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks* (pp. 197–223). Springer.

Van Saberhagen, N. (2013). *Cryptonote v 2. 0.*

Zantout, B. & Haraty, R. (2011). I2p data communication system. In *Proceedings of icn* (pp. 401–409).