Allianz Hogeschool van Arnhem en Nijmegen

Onderzoeksverslag

De blockchain technologie

Door: Calum Iain Munro

ICA INFORMATICA COMMUNICATIE ACADEMIE

Software Development, ICA, VT

HBO bachelorscriptie:
Versie: 1 (Definitief)
Datum: 15 juni 2018

Gegevens opdrachtgever:
Bedrijf: HeadForward B.V.
Contactpersonen: Daniël Siahaya

Gegevens opleiding:
Opleiding: HBO bachelor Informatica
School: Hogeschool van Arnhem en Nijmegen
Begeleider: Misja Nabben
Assessor: Rein Harle

Gegevens opdrachtnemer:
Teamlid: Calum Iain Munro (549288)

Inhoudsopgave

HOOFDSTUK 1

Inleiding

Dit onderzoeksverslag is geschreven tijdens het afstudeerproject van Iain Munro voor het Claim proces van Allianz. Allereerst wordt in dit hoofdstuk het onderwerp van dit onderzoeksverslag behandeld. Dit wordt gedaan door in paragraaf 1.1 de aanleiding van het onderzoek te bespreken. Waarna de relevantie in paragraaf 1.2 wordt besproken en aansluitend in paragraaf 1.3 de doel- en vraagstellingen worden geformuleerd.

Het verdere verslag bestaat uit de resultaten van het onderzoek naar de blockchain-technologie en gerelateerde onderwerpen zoals smart contracts. Verder behandeld dit onderzoek ook de verschillende types blockchain. Hierna volgt de conclussie in paragraaf 4.

1.1 Aanleiding

De aanleiding voor dit onderzoek is dat er een proof of concept ontwikkeld wordt voor Allianz. Echter zijn de onderwerpen nog niet bekend. De aanleiding hiervoor is aangeven in het plan van aanpak [8].

1.2 Relevantie

De relevantie van dit onderzoek is om een aantal basis technische termen in cryptografie, blockchain-technologie en gerelateerde onderwerpen duidelijk te krijgen. Hiermee weet ik waar ik het over heb wanneer ik het proof of concept ontwikkel en hierover besluiten maak.

De relevantie van het onderzoek naar smart contracts is dat dit een term is die wordt gebruikt bij het ontwikkelen van een gedecentraliseerde blockchain applicatie.

1.3 Probleemstelling

Het doel van dit onderzoeksverslag is om duidelijk te krijgen wat blockchain technologie en smart contracts zijn en hoe ze gebruikt kunnen worden om informatie over claims van verzekeringen veilig te delen en te controleren, vooral tussen partijen die elkaar niet noodzakelijk vertrouwen.

Dit wordt in het afstudeerproject bewezen door een proof of concept softwareapplicatie voor de use case van elektronische verzekeringsgegevens te maken. Hierdoor liggen andere use-cases buiten de omvang van dit onderzoek.

De hoofdvraag (**MRQ**) van dit onderzoek is:

"*Wat is de blockchain en hoe werkt het?*"

Om deze vraag te beantwoorden wordt er een literatuuronderzoek uitgevoerd naar een technische basis termen rondom de blockchain-technologie en gerelateerde onderwerpen.

HOOFDSTUK 2

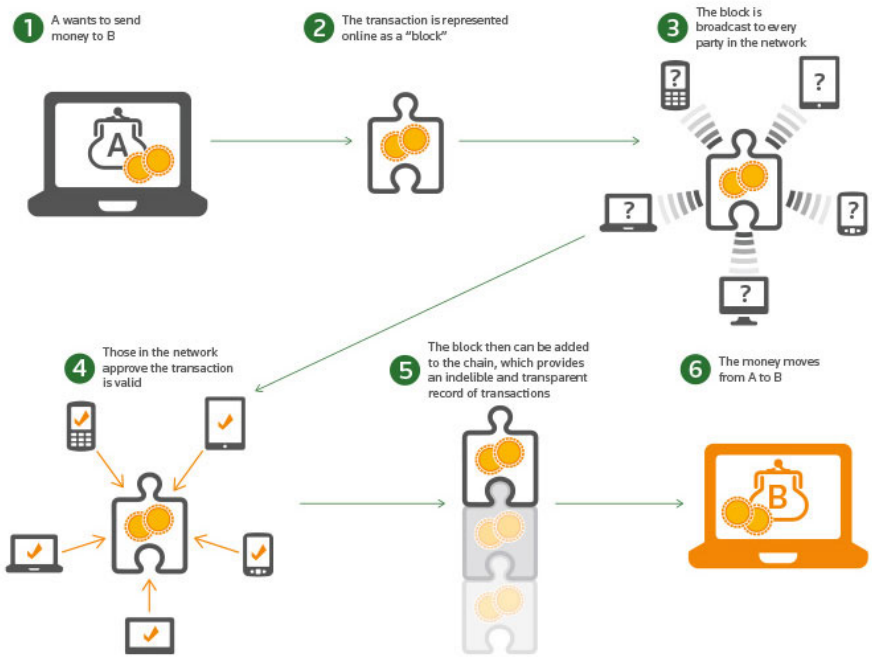
De blockchain technologie

In dit hoofdstuk wordt er een korte uitleg gegeven over een aantal basis technische termen in cryptografie, blockchain-technologie en gerelateerde onderwerpen zoals smart contracts. Hiermee wordt er een duidelijk begrippenkader gemaakt voor de proof of concept.

2.1 Het algemene concept achter de blockchain

De Blockchain technologie is wereldwijd bekend geworden door de introductie van de digitale valuta genaamd Bitcoin. De Bitcoin werd geïntroduceerd in 2008 door Satoshi Nakamoto in een white paper "Bitcoin: A Peer-To-Peer Electronic Cash System"[16]. Hierin legt hij uit hoe in een gedecentraliseerde softwareomgeving (zie paragraaf 3.2), geld veilig overgemaakt kan worden. Denk hierbij aan een online betaling, waar de een partij rechtstreeks naar een andere partij geld kan overmaken zonder de verschillende financiële instellingen die normaal gesproken de transactie faciliteert.

Database transacties worden gegroepeerd en opgeslagen in blokken van data die vervolgens achter elkaar in een reeks wordt vastgelegd. Iedere deelnemer van het netwerk beschikt over deze blokken en een nieuwe deelnemer downloadt altijd eerst de gehele en recente historie van het netwerk. Hieruit krijgt de technologie de naam Blockchain [15]. De koppeling tussen blokken en hun inhoud wordt beschermd door cryptografie en kan niet worden vervalst. Daarom kan informatie die eenmaal in een blockchain is ingevoerd niet worden gewist; in essentie bevat een blockchain een accuraat, tijd gestempeld en verifieerbaar archief van elke transactie die ooit is gemaakt. Figuur 3.1 geeft het algemene idee weer van hoe deze technologie werkt met als bekende use case de bitcoin.



Figuur 2.1: Illustreert hoe de blockchain werkt [9]

In dit onderzoek gebruiken we de beschrijving van het ICTU [1], die de blockchain beschrijft als: een specifieke databasetechnologie die leidt tot een gedistribueerd autonoom grootboeksysteem [6]. De integriteit van dit gedistribueerd autonoom grootboeksysteem wordt gewaarborgd doordat iedere partij zeggenschap heeft bij de validatie van een transactie. Dit versnelt het proces doordat beheerders en tussenpersonen worden uitgeschakeld. Meningsverschillen worden opgelost door een cryptografisch consensus algoritme (zie paragraaf 3.3).

De blockchain technologie lost verschillende problemen op die voorkomen bij het gebruik van traditionele gecentraliseerde database technologieën die in handen zijn van één instantie. Dit soort technologieën vereisen vertrouwen dat de beheerder zorgvuldig omgaat met de toegang of bewerkingen van de data. Verder dient de database toegankelijk te zijn voor de belanghebbende en dat hij erop kan vertrouwen dat de instantie er de volgende dag nog is. Deze problemen komen niet voor in een gedecentraliseerde blockchain database. Dit komt omdat een nieuwe dienst, softwarebedrijf of markten op de blockchain de volgende zes designprincipes [10] hanteren:

1. Netwerk integriteit
   Het systeem bewaakt de data integriteit doordat ieder lid in het netwerk alle transacties kan nalopen en kan controleren, in plaats van een enkel lid die dit proces uitvoert. Gebruikers op het netwerk kunnen rechtstreeks waarde met elkaar uitwisselen door dit te registeren op een blok. Elk blok heeft een verwijzing naar een voorgaand blok, waardoor niemand een transactie kan verbergen of kan vervalsen. Dit omdat er meer andere gebruikers zijn met de juiste realiteit.

[1] https://www.ictu.nl/

2. Gedistribueerd

   Het systeem is volledig Gedistribueerd. Dit houdt in dat er geen één punt is van controle of falen. Er is niet een gebruiker of organisatie die het systeem uit kan zetten.

3. Security

   Satoshi's white paper [16] vereist dat het systeem beveiligd is door een public key infrastructure (PKI) [2]. De PKI is een geavanceerde vorm van asymmetrische cryptografie, waar de gebruiker zowel een publiek en privé sleutel ontvangt om zichzelf binnen het netwerk te identificeren en berichten kan versleutelen en ontsleutelen.

4. Eigendomsrechten

   Eigendomsrechten over valuta en andere data zijn transparant in het netwerk en dus beschikbaar voor iedere gebruiker van het netwerk. Hierdoor dient een blockchain als een publiek register door middel van een tool genaamd Proof of Existence (PoE) [3]. Deze tool creëert en registreert de cryptografische overzichten van akten, licenties en andere rechten van gebruikers.

5. Privacy

   Gebruikers beheren hun eigen data. Er is geen centrale partij en gebruikers op het netwerk geven zelf aan wat ze aan informatie vrijgeven. Dit is echter allemaal optioneel en een gebruiker op de blockchain hoeft in de meeste implementaties alleen een publieke en private key te hebben. De gehele identificatie- en verificatie laag zijn los van elkaar waardoor gebruikers op de blockchain de mogelijkheid hebben om anoniem te zijn.

6. Valuta als motivatie

   Het systeem motiveert deelnemers van het netwerk door ze valuta te geven voor bepaalde acties op het netwerk. In het geval van de bitcoin, krijgen miners bitcoin geld voor het eerstvolgende blok te koppelen aan het vorige blok aan data. Dit wordt gedaan door een cryptografische puzzel op te lossen die geleidelijk lastiger wordt.

[2] https://en.wikipedia.org/wiki/Public_key_infrastructure
[3] https://en.wikipedia.org/wiki/Proof_of_Existence

2.2 Type Blockchain

Om een geïnformeerd besluit te maken welk type blockchain juist is voor het proof of concept worden de verschillende type blockchain in dit paragraaf behandeld. Dit wordt gedaan vanaf een hoog technisch niveau. In essentie zijn er drie types blockchain: privé, consortium en openbaar. Deze types kunnen daarna weer onderverdeeld worden in de open en gesloten categorieeën blockchain. Per type blockchain wordt er ook gelijk gekeken naar de grote projecten die relevant zijn. Zodat in een vervolg hoofdstuk hierover een vergelijking kan worden uitgevoerd.

De categorie gesloten, waarin de types privé en consortium zitten zijn bedoeld voor een gelimiteerde omgeving zoals één of meerdere bedrijven en organisaties. Terwijl een openbare blockchain volledig open is en geen permissies zijn die mensen of systemen erbuiten houden.

2.2.1 Privé Blockchain

Voor een volledige private blockchain, moeten de schrijfrechten op een centrale plek staan die beheerd worden door een organisatie. De leesrechten kunnen zowel publiekelijk of ook net zo beperkt zijn als de schrijfrechten. Applicaties die gebruik maken van een privé Blockchain zijn interne applicaties die alleen gebruikt worden binnen een bedrijf of organisatie. Want in andere gevallen wordt publieke leesrechten en controleerbaarheid vereist [7]. Voorbeelden van privé Blockchains zijn MultiChain en Hyperledger:

MultiChain - MultiChain is een platform voor het ontwikkelen en publiceren van privé blockchains. Het lost een aantal schaalbaarheid problemen [13] van de blockchain op met een geïntegreerde gebruiker permissie systeem. Verder biedt het bedrijven de mogelijkheid om zonder software ontwikkelaars een blockchain op te richten [3].

Hyperledger - Hyperledger is een open source project. Het wordt ontwikkeld met als doel om een geavanceerd bedrijfstak overkoepelende blockchain implementatie te realiseren. Het wordt ondersteund door de Linux Foundation [2] en wordt gezamenlijk ontwikkeld door grote organisatie in financiën, banken, IoT, productie en technologie [1].

2.2.2 Consortium Blockchain

Het consortium blockchain type is gedeeltelijk privé. Het onderscheidt zich in het consensus (zie paragraaf 3.3) proces waar alleen een aantal vooraf geselecteerde peers (gebruikers) de integriteit van de data op de blockchain waarborgen. Deze nodes zijn bijvoorbeeld 10 grote financiële instellingen die bij de aanmaak van een nieuwe block aan de blockchain zeggenschap hebben. Andere deelnemers van de blockchain hebben nog steeds het recht om de besluiten van de 10 nodes te controleren, maar ze hebben verder geen stem over het feit of de volgende block valide is.

Het voordeel van de consortium variant is dat deze efficiënter is en toch voldoende transactie transparantie geeft. Ook is het niet een bedrijf die alleen oordeelt over de data. Voorbeelden van dit type zijn Ethereum en R3:

Ethereum - Het Ethereum project beschrijft zichzelf als een gecentraliseerd platform voor applicaties die precies uitgevoerd worden zoals ze geprogrammeerd zijn. Dit allemaal zonder enige kans van fraude, censuur of veranderingen van derden [4]. Applicaties, smart contracts, worden geprogrammeerd in de Solidity taal die voor het Ethereum project is ontwikkeld. Het wordt open-source ontwikkeld en er is een bondgenootschap, de Enterprise Ethereum Alliance[5] dat bestaat uit 315 fortune 500 bedrijven en organisaties, die gezamenlijk werken aan het het enige platform die smart contracts ondersteunt op de blockchain.[11]

Het project kan gezien worden als een verder uitgewerkte versie van Bitcoin die meer functionaliteiten toevoegt. Zo bestaat de status van Ethereum netwerk net zoals de Bitcoin uit meerdere objecten die 'accounts' worden genoemd, waarbij elk account een adres van 20 bytes en statusovergangen heeft. De staat van deze objecten worden opgeslagen in de blockchain waaruit gelijk afgeleid kan worden waar valuta naartoe gaat.[20]

R3 - Dit is een gedistribueerd database-technologiebedrijf in New York. Het is verbonden met veel van 's werelds grootste financiële instellingen, met als missie om de voordelen van de blockchain te realiseren. Het is momenteel nog enorm in ontwikkeling en het bedrijf voert vooral onderzoek uit[18].

2.2.3 Openbare Blockchain

Dit type blockchain is zoals de naam al aangeeft publiek beschikbaar tot iedereen in de wereld. Dit houdt in tegenstelling tot Consortium ook het consensus (zie paragraaf 3.3) proces in. Iedere gebruiker op het netwerk is gelijk en heeft zeggenschap op de geldigheid van nieuwe data blokken.

Een volledig publieke blockchain is een open-source systeem die gebruikers met economisch doeleinde motiveert om samen te werken. Dit principe heet crypto economics en hierdoor kunnen ontwikkelaars belangen zoals beschikbaarheid waarborgen. Zo zal een transactie met een hoger tarief resulteren in snellere conversie. Een voorbeeld hiervan is het bekende Bitcoin project.

Bitcoin. Bitcoin is het bekendste voorbeeld van een blockchain project. Bitcoin staat vooral bekend als digitale valuta en online betalingssysteem die door gebruik van cryptografie om valuta-eenheden te geneert en reguleert. Verder gebruikt het cryptografie om de overdracht van fondsen te verifiëren zonder een centrale bank.

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

HOOFDSTUK 3

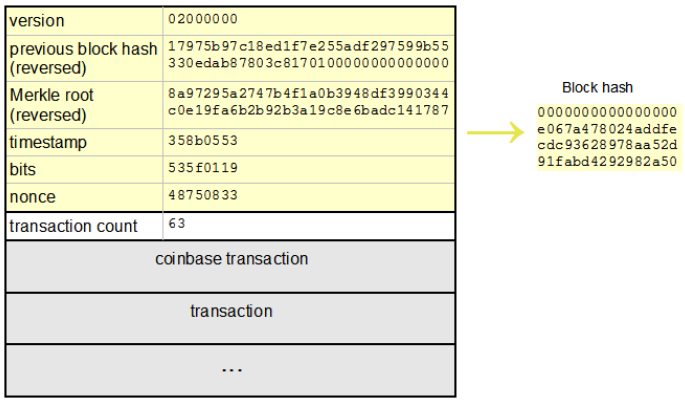
De architectuur van de blockchain technologie

Dit hoofdstuk gaat verder in op de basisarchitectuur van de blockchain. Zodat tijdens het ontwikkelen van het Proof of Concept, de basisbegrippen van de technologie correct worden begrepen.

3.1 Blok (block)

Zoals al eerder was aangegeven is de blockchain een gedistribueerd grootboeksysteem. Gegevens worden permanent opgeslagen in het netwerk via bestanden die blokken worden genoemd. Een blok is een document waarin recente transacties van een bepaald moment zijn vastgelegd. Het heeft daarom de naam blockchain, omdat het een reeks van blokken zijn die steeds maar naar de vorige verwijst. Een nieuwe blockchain database begint daarom met een zogenaamd genesis blok [15].

Een blok in het geval van de Bitcoin bestaat uit een header en een body [12]. De header bestaat uit drie stukken metagegevens. De eerste is een verwijzing naar een vorige blockhash (Merkle-hash [1]). Hierdoor verbindt het blok met de vorige uit de blockchain. De tweede set van metagegevens is moeilijkheidsgraad, tijdstempel en nonce[2]. Het laatste stuk metadata is de Merkle-tree root, een datastructuur die wordt gebruikt om alle transacties in het blok efficiënt samen te vatten [4].



Figuur 3.1: Illustreert de structuur van een block in de bitcoin blockchain.
Bron: http://www.righto.com/2014/09/mining-bitcoin-with-pencil-and-paper.html

[1] https://en.wikipedia.org/wiki/Merkle_tree
[2] https://en.wikipedia.org/wiki/Cryptographic_nonce

3.2 Gedecentraliseerd netwerk

Interacties tussen gebruikers op de blockchain gebeuren hoofdzakelijk gedecentraliseerd. Dit betekent dat iedere gebruiker een punt vertegenwoordigt van het netwerk. Iedere gebruiker heeft dezelfde blockchain software geïnstalleerd en is direct verbonden met een aantal andere gebruikers van het netwerk. Wanneer een gebruiker een transactie uitvoert met een andere gebruiker dan ontvangen de andere gebruikers deze informatie ook. Deze gebruikers valideren ze dan eerst en sturen het vervolgens door als het klopt [21].

Het voordeel van een gedecentraliseerd netwerk, is dat geen centraal punt is die kan falen of de beheerdersrol kan hebben. Hierdoor wordt de menselijke factor geminimaliseerd en het vertrouwen verschuift van centrale organisatie naar vertrouwen in de open source code waaraan meerdere auteurs aan werken[14].

3.3 Consensus (overeenstemming) algoritmes

Om de werking van de blockchain te begrijpen en te vertrouwen, moet het begrip van Consensus oftewel overeenstemming algoritmes duidelijk zijn. Deze algoritmes worden gebruikt wanneer een (nieuw) blok aan informatie geverifieerd wordt. Het zorgt voor één historie van transacties waar de geschiedenis geen ongeldige of tegenstrijdige transacties bevat.

Dit is allemaal nodig omdat de blockchain draait in een zelf gereguleerde, wantrouwende omgeving waar het nodig is om meningsverschillen over transacties binnen het netwerk op een lijn te krijgen. Het zorgt ervoor dat er niet één account is die meer uitgeeft dan dat het heeft, of waar hij of zij twee keer iets overmaakt, dit heet double-spending. De bekende consensus algoritmes zijn proof of work en proof of stake:

1. Proof of Work (PoW)
   Het PoW consensus algoritme is het meest voorkomende algoritme in blockchain. Het werd geïntroduceerd door de Bitcoin en gaat ervan uit dat alle peers met rekenkracht mee stemmen door PoW-instanties, cryptografische puzzels op te lossen en hiermee het recht hebben om de volgende blok aan te maken in het netwerk. Zo maakt de Bitcoin gebruik van een hash-gebaseerde PoW, wat inhoudt dat de peers een nonce-waarde[3] proberen te vinden. Wanneer een dergelijke nonce wordt gevonden, maakt de miner het blok aan en stuurt hij het door naar zijn peers. Deze peers ontvangen dit dan en verifiëren of het klopt aan de hand van het vorige blok [5].

2. Proof-of-Stake (PoS)
   Op het moment moet Proof-of-Stake zich nog bewijzen in de crypto valuta gemeenschap. Het is ontwikkeld om bestaande inefficiënte consensus algoritmes zoals PoW te vervangen. Het algemeen begrip van PoS is dat een deelnemer van de blockchain, pas het stemrecht heeft op een nieuwe blok in de blockchain als de peer zich voldoende heeft ingezet in het netwerk. In het geval van PeerCoin[4] worden nieuwe blokken gegeneerd door het netwerk op basis van niet gespendeerde valuta en hoe oud deze is [19].

   Met deze methode wordt aangenomen dat oude deelnemers van het netwerk minder snel het netwerk zullen aanvallen [12]. Dit lost op het gebied van energiebesparing de problemen van PoW op, waar gebruikers miners aanzetten om valuta te ontvangen. Bij PoS wordt de valuta die niet beweegt steeds meer waard.

[3] https://en.wikipedia.org/wiki/Cryptographic_nonce
[4] https://peercoin.net/

3.4 Smart contract

Het idee achter smart contracts is een "geautomatiseerd transactie protocol dat de voorwaarden van een contract uitvoert"[17] en werd voor het eerst bedacht door cryptograaf Nick Szabo. Dit idee is door de opkomst van de blockchain populair geworden. Dit komt doordat de blockchain gedecentraliseerd is en daardoor de tussenpersonen bij een gecentraliseerde smart contracts applicatie eruit haalt. Smart contracts is, in de context van blockchain, gewoon software die op een blockchain wordt gepubliceerd en die transacties kan ontvangen of uitvoeren. Iedere transactie heeft een adres en kan worden gevolgd.

HOOFDSTUK 4

Conclusie

Het type privé blockchain kan voor het proof of concept direct uitgesloten worden. Dit omdat het hele idee van het proof of concept gaat om het feit dat alle transacties transparant zijn voor alle deelnemers van het netwerk. Zodat bijvoorbeeld verzekeraars een transactie kunnen verifiëren voordat ze hem uitbetalen.

Hierna houden we alleen nog het Consortium en openbaar type blockchain over. Hierbij is gekozen voor consortium omdat deze efficiënter is in het verwerken van transacties. Daarnaast zit in de consortium variant het project Ethereum, die momenteel de enige is die smart contracts biedt op de blockchain.

Verder is de conclusie dat de technologie om de blockchain en hoe deze werken nu duidelijk en kan er ontwikkeld worden aan het proof of concept.

Bibliografie

[1] Blockchain technologies for business. URL https://www.hyperledger.org/.

[2] The linux foundation. URL https://www.linuxfoundation.org/.

[3] Multichain. URL https://www.multichain.com/.

[4] Andreas M. *Mastering Bitcoin (Second Edition, Second Print): Programming the Open Blockchain*. June 2017. URL https://github.com/bitcoinbook/bitcoinbook/blob/develop/book.asciidoc.

[5] Arthur Gervais. *On the security and performance of proof of work blockchains*. 2016.

[6] Steven Gort Bas Kaptijn, Peter Bergman. *Blockchain*. 2016. URL https://www.ictu.nl/sites/default/files/documents/ICTU_Whitepaper_Blockchain.pdf.

[7] Vitalik Buterin. On public and private blockchains, 2015. URL https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

[8] Calum Iain Munro. *Plan van Aanpak - Afstudeerproject: Allianz*. 2018.

[9] Tim Minshall Thas Nirmalathas Zoran Perunovic Ikhlaq Sidhu Dhrubes Biswas, Charlotta Johnsson. Applied innovation review, issue no. 2 june 2016. 2016.

[10] Alex Tapscott Don Tapscott. *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Portfolio / Penguin, 2016.

[11] DR. GAVIN WOOD. *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER*. 2014. URL https://bravenewcoin.com/assets/Whitepapers/Ethereum-A-Secure-Decentralised-Generalised-Transaction-Ledger-Yellow-Paper.pdf.

[12] Tzu-Chun Liao Iuon-Chang Lin. *A Survey of Blockchain Security Issues and Challenges*. Department of Photonics and Communication Engineering, Asia University, 2017. URL http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf.

[13] Kieren James-Lubin. Blockchain scalability: A look at the stumbling blocks to blockchain scalability and some high-level technical solutions. URL https://www.oreilly.com/ideas/blockchain-scalability.

[14] Marcella Atzori. *Blockchain technology and decentralized governance: Is the state still necessary?* 2015.

[15] John Domingue Matthew English, Soren Auer. *Block Chain Technologies The Semantic Web: A Framework for Symbiotic Development*. Computer Science Con- ference for University of Bonn Students, J. Lehmann, H. Thakkar, L. Halilaj, and R. Asmat, Eds, 2016. URL `https://pdfs.semanticscholar.org/2fd3/7fed17e07c4ec04caefe7dcbcb16670fa2d8.pdf`.

[16] Nakamoto, Satoshi. *Bitcoin: A peer-to-peer electronic cash system*. 2008.

[17] Nick Szabo. Smart contracts, 1994. URL `http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html`.

[18] Stan Higgings. Inside r3cev's plot to bring distributed ledgers to wall street. URL `https://www.coindesk.com/r3cev-distributed-ledger-wall-street/`.

[19] Pavel Vasin. *BlackCoin's Proof-of-Stake Protocol v2*. URL `http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf`.

[20] Vitalik Buterin. *A NEXT GENERATION SMART CONTRACT DECENTRALIZED APPLICATION PLATFORM*. URL `http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf`.

[21] Zibin Zheng. *Blockchain Challenges and Opportunities: A Survey*. 2016.