Blockchain Technology for Governmental Services:
Dilemmas in the Application of Design Principles

Paulus A. Corten

Abstract — Blockchain is rapidly developing and experiences increasing popularity. The technology is a peer-to-peer broadcasted transaction network with transparent and cryptographic secured information that enables smart contracts. These automatic executed contracts can significantly improve many services from both the public as the private sector by replacing the middleman in many processes. However, the rapid development of blockchain is hampered by a lack of knowledge, empirical research and skilled developers. Hardly any research has a focus on blockchain for governmental services. Neither are the dilemmas that need to be addressed during the design of smart contract implementations analyzed. This causes project teams to lack guidelines to support them in the implementation of smart contracts in governmental services. We used the design science approach to answer the research question: Which design dilemmas occur when applying design principles for smart contract implementation in governmental services? Based on a literature review, four case studies and six expert interviews we formulated 36 design principles for the implementation of smart contracts in governmental services. We discovered and analyzed seven dilemmas that can occur when applying these principles. The findings offer project teams that implement smart contracts valuable insights into which design actions are recommended and which dilemmas possibly occur. We recommend further research that strengthens the generalizability of these dilemmas. We also recommend further research into strategies to cope with the seven dilemmas we formulated.

Keywords — Governmental Services, Blockchain Technology, Design Science Approach, Design Principles, Design Dilemmas

I. Introduction

The interest in blockchain technology, the fundament of Bitcoin and other cryptocurrencies, has grown since the last months of 2017 (Gaggioli, 2018). The valuation of cryptocurrencies is over 385 billion dollars (Coinmarketcap.com, n.d.), main stream media are publishing articles about blockchain (Financial Times, 2018; CNN, 2018; BBC, 2018) and blockchain startups are raising billions of dollars with the blockchain equivalent of the initial public offering (IPO): the initial coin offering (ICO) (Zetsche et al., 2017, p.3). Some even call blockchain technology the biggest invention since the internet (Drescher, 2017).

Blockchain started in 2008 when the pseudonym Nakamoto published a paper describing the theory behind the digital currency Bitcoin (Nakamoto, 2008). Transactions between individuals are secured by cryptography, broadcasted peer-to-peer, verified by nodes in a network and the history of transactions are distributed to all nodes in the network (Tapscott & Tapscott, 2016). There is no longer a need for an intermediary that verifies the correctness of the transaction, such as a bank, because the blockchain is designed to automate this verification (Swan, 2015).

Blockchain also enables smart contracts. The smart contract was first described in 1994 by Nick Szabo as being a *"computerized transaction protocol that executes the terms of a contract"* (Szabo, 1994, p.1). Ethereum is the first platform that enables the use of blockchain powered smart contracts, enabling applications such as financial derivatives, hedging contracts, wills, employment contracts, identity systems, decentralized file storage, voting, peer-to-peer gambling, prediction markets and many more (Buterin, 2013). Many firms deal with contracts every day. Intermediaries such as lawyers, accountants and managers currently function as trusted third parties. Smart contracts can radically change their roles (Iansati & Lhakani, 2017, p.10),

because smart contracts can be used to authorize, verify and approve transactions (Ølnes, Ubacht, & Janssen, 2017, p.363). Blockchain enables a decentralized peer-to-peer network that disables the need for a trusted intermediary (Bahga & Madisetti, 2016, p.534), such as the above mentioned.

Potential benefits and promises of blockchain are amongst others: transparency, avoiding fraud and manipulation, reducing corruption, increased trust, auditability, reduced costs, reducing human errors, access to information, privacy, reliability and security (Ølnes, Ubacht, & Janssen, 2017, p.359). Though many of these benefits lack empirical evidence (Ølnes, Ubacht, & Janssen, 2017, p.359), it shows the potential disruptive effects in the private sector (Drescher, 2017, p.24). Moreover, blockchain has the potential to disrupt and improve many facets of governments as well (Tapscott & Tapscott, 2016, p.140). Smart contracts can decrease costs, improve efficiency (Swan, 2015, p.27), and improve governmental services to be "more personal, immediate and efficient" (Government Office for Science, 2016, p.9).

However, blockchain is a nascent technology: Bitcoin was first described in 2008 and the first smart contract platform Ethereum was developed in 2013. Only a few developers and people with in-depth knowledge exist in the blockchain ecosystem (DApp.Design interview, 2018) and blockchain powered smart contracts lack academic research (Yli-Huumo et al., 2016). There is especially a lack of empirical knowledge on the implementation of smart contracts in governmental services. An overview of guidelines to assist project teams is non-existent (Corten, forthcoming), hampering the project development. Such guidelines, so called *design principles*, could greatly benefit project teams with the implementation process and would accelerate the creation of more use cases and empirical knowledge. In this article we are the first to address this knowledge gap by defining design principles for smart contract implementation in governmental services and analysing the dilemmas that occur when applying those principles. Our leading research question is: Which design dilemmas occur when applying design principles for smart contract implementation in governmental services?

This paper is structured as follows. In section II we present our research approach: the design science approach. Within this approach we used a literature review, four case studies and six expert interviews to explore and categorize design principles for smart contracts in the domain of governmental services. In section III we present a comprehensive overview of the 36 design principles we retrieved. Additionally, we discuss seven dilemmas that exist between those design principles and present the characteristics of those dilemmas. Finally, we offer conclusions and suggestions for further research in section IV.

II. Research approach

We used a design science approach as described by Hevner et al. (2004) in order to derive design principles. Considering that this approach is especially applicable in developing information systems such as blockchain, we deemed this research method as appropriate for our research. The design science approach enables the creation of new empirical knowledge and consists of multiple steps where information is observed, applied, assessed and refined by using several research methods. This research consists of six steps of the design science approach: applying knowledge with a literature review, building the first version of design principles, observing data with six case studies in Dutch municipalities, assessing and refining the design principles, evaluating with six expert interviews, and assessing and refining the design principles to form the final version. We discuss these steps in more detail in the paragraphs below.

A. A*pply knowledge: literature review*

In the first phase of our design science approach we conducted a literature review in order to apply knowledge by finding design principles in the literature. We consulted Scopus for the keywords '*blockchain*', '*principles*', '*design*' and '*government*', with the exact search term: ALL ("blockchain" AND "principles" AND "design" AND "government"). A selection of the result of 26 publications was made on basis of the following criteria: freely accessible in English, offers design principles, focusses on blockchain powered smart contracts and focusses on implementation in governmental services. This narrowed down the list to four publications (Ølnes & Jansen, 2017; Sharma, Moon & Park, 2017; Eshuis, Norta & Roulaux, 2016; Pilkington, 2016). In grey literature we found three additional publications with design

principles from a more practical point of view, which we added to the selection (Government Office for Science, 2016; NASCIO, 2017; Blockchainpilots.nl, 2016).

B. Build: first version of design principles

The total of seven publications were coded in the software program ATLAS.ti. We used the coded quotations to build the first version of design principles, which were initially divided into four categories: political, economic, social and technological. We used these categories, because there is not yet a categorization for such design principles. These categories were used as sensitizing concepts that provided us "*a general sense of reference and guidance in approaching empirical instances"* (Blumer, 1954, p.7). The categorization was assessed and refined in later stages of the research.

C. Observe data: case studies

We conducted four case studies in order to observe data from the environment and assess the first version of the design principles. The cases concern four Dutch municipalities that can be considered as early adopters in the implementation of smart contracts and were conducted as national coordinated pilots, where the results are used to retrieve and share empirical knowledge, research the potential impact of specific use cases and start building blockchain applications (Blockchainpilots.nl, 2016). The cases were the Gelrepas (municipality of Arnhem), debt assistance (municipality of Schiedam), waste processing (municipality of Utrecht) and the disabled parking permit (municipalities of Schiedam and Drechtsteden). The information for the case studies was retrieved by means of secondary background information and primary information from face-to-face interviews with various roles in the project teams: advisor process management, advisor business intelligence, program manager, data scientist and business consultant. The following four sub paragraphs offer an introduction to the four smart contract implementation projects that were used for the case studies.

C.1 Case study 1: Gelrepas

The municipality of Arnhem offers a physical card, the Gelrepas, to citizens with a low income of several neighboring municipalities in order to receive discounts on several sportive and cultural activities (VNG/KING, 2017, p.8). Currently, a citizen has to apply through a physical form. An employee of the municipality checks if the applicant applies to the requirements, such as the maximum monthly income and the citizenship of participating municipalities. The employee sends the physical Gelrepas by mail to the applicant along with physical discount coupons. The citizen pays at the participating organizations by demonstrating his Gelrepas and giving the coupons. The organization needs to send the coupons to the municipality, which will transfer money to the organization as compensation (VNG/KING, 2017, p.10). The process can be eased by applying blockchain. The municipality holds a database with citizens that fulfill the requirements. Citizens do not have to apply through a physical form anymore, but can install an application with a QR-code. The participating organization scans the citizens' code, which automatically verifies in the blockchain whether or not the citizen has the right to claim the discount and registers the transaction. (VNG/KING, 2017, p.11). Expected benefits of the new process are: reduced costs, improved transparency and auditability, avoiding fraud and manipulation, and improved access to information (Corten, forthcoming).

C.2 Case study 2: budget assistance

The organization Stroomopwaarts in the municipality of Schiedam currently assists citizens with financial problems with the help of a budget manager that takes control of the citizens' financial administration. This could for example be that the budget manager pays the bills, taking over the financial control from the citizen. The budget assistance is currently not a municipal service, but the municipality pays for the costs. The expenses of the citizen can also be restricted with smart contracts, for example by programming how much money can be spent on rent, energy and free expenses. The budget manager is no longer necessary, as his actions are replaced by the smart contract's restrictions. By using the blockchain it is also possible to early detect citizens that are heading to financial problems and signal the municipality to intervene (Pomp & Hartog, 2017). Expected benefits of the new process are: reduced costs, increased trust, transparency and increase of predictive capability (Corten, forthcoming).

C.3 Case study 3: waste processing

Waste of citizens in the municipality of Utrecht is collected and processed by multiple organizations. They need a permit from the ILT (Dutch Human Environment and Transport Inspectorate) to be allowed to collect waste. The municipality and his citizens currently cannot directly access the details and validity of the permits. Those permits can be deployed by the ILT as a smart contract on the blockchain, which contains the details and validity of each permit. The municipality can then automatically validate the permit of an organization each time a transaction is registered in the blockchain (Pomp & Hartog, 2017). Expected benefits of the new process are: improved access to information, increased trust, reduced costs, reduced process time, improved transparency, avoiding fraud and manipulation, and persistency and irreversibility of data (Corten, forthcoming).

C.4 Case study 4: disabled parking permit

The disabled parking permit is a physical card that allows citizens of European Union countries to park at disabled parking spots. Disabled citizens apply for the card through the municipality, which verifies at the GGD (Dutch Public Health Service), the RDW (Netherlands Vehicle Authority) and the European Union if the citizen is eligible to receive the card. Drechtsteden (a cooperation between the municipalities of Alblasserdam, Dordrecht, Hendrik-Ido-Ambacht, Papendrecht, Sliedrecht and Zwijndrecht) deploy the disabled parking permit on a blockchain by using smart contracts to prevent fraud and theft. The license plate of the vehicle of the disabled citizen is registered in a smart contract and the physical card is replaced by a mobile application. The citizen confirms that he parked through the application, that registers the action on the blockchain. Parking inspectors scan the license plate of the vehicle. The system automatically verifies the parking permit through the blockchain. The card is not physical anymore and thus cannot be stolen or misused (Pomp & Hartog, 2017). Expected benefits of the new process are: reduced costs, reduced process time, avoiding fraud and manipulation, and increased privacy (Corten, forthcoming).

D. Assess and refine: second version of design principles

The interviewees from the four case studies read and discussed the first version of principles. We refined the principles based on that information. In addition, we discussed possible design dilemmas with the interviewees. This led to an adapted overview of the design principles from literature, based on empirical experiences from the cases.

E. Evaluate: expert interviews

We interviewed six experts in the field of smart contract implementation from a diversity of backgrounds and roles in this domain in order to evaluate the second version of design principles. Experts can be defined as *"people who possess special knowledge of a social phenomenon which the interviewer is interested in"* (Gläser & Laudel, 2009, p.117). The experts were the project manager of Dutch blockchain pilots (Blockchainpilots.nl), blockchain developers from DApp.Design that cooperated with the municipality of Schiedam, a data scientist for the Dutch government (ICTU), a law firm with smart contract expertise (Pels Rijcken), the project leader of the Stadjerspas (municipality of Groningen) and blockchain developers from Forus that cooperated with the municipality of Zuidhorn. The experts validated the design principles and offered their opinions on possible dilemmas.

F. Assess and refine: final version of principles

We coded the transcripts from the expert interviews in ATLAS.ti. The second version of the design principles were assessed and refined using the coded quotations from the interviews. This led to the final version of design principles and dilemmas.

III. Results

A. Overview of design principles

The application of the six described steps from the design science approach resulted in the final version of design principles for the implementation of smart contracts in governmental services, that are listed in table 1. The 36 design principles are divided into five categories: political (one principle), economic (three principles), social (eleven principles), technological (fifteen principles) and legal (six principles). The initial categorization (see section

II) was expanded with the category legal on the basis of the expert validation.

Based on the case study and the experts interviews we discovered seven design dilemmas between pairs of design principles:

1. Allocate budget & profitability;
2. Communicate significance & examine impact on jobs;
3. Security & open source coding;
4. Privacy & decide ledger type;
5. Scalability & transaction speed;
6. Consider back-ups & decide ledger type;
7. Define responsibilities & decide ledger type.

In the next paragraphs we elaborate on each of these dilemmas in full.

B. Allocate budget & profitability

Smart contract implementations demand the allocation of budget (Blockchainpilots.nl, 2016; Arnhem interview, 2017; Utrecht interview, 2017; Schiedam interview, 2017), while managers will also determine the profitability of each project, because governmental organizations are financially steered (Arnhem interview, 2017; Schiedam interview, 2017; Drechtsteden interview, 2018). This can be a dilemma, because smart contract implementations will not necessarily lead to costs savings. The disabled parking permit for example will not lead to cost savings, but can improve the life of disabled citizens, because they are protected from theft of the permit and can view free parking spaces in an application: *"The parking permit for disabled is not something that has a valid business case directly, but is the town council prepared to invest money to ease the life of a disabled citizen?"* (Drechtsteden interview, 2018). Another example is the implementation of smart contracts in Zuidhorn. This Dutch municipality has a system, the Kindpakket, that offers discounts to children in families with a low budget (Municipality of Zuidhorn, 2017). Experts recognize the dilemma: *"There is much investing in Zuidhorn I would say. It is a relatively large investment. And if you would only look what it would mean for the Kindpakket and what do we save with it, I think it is currently not balanced"* (Forus interview, 2018). The interviewees confirm that blockchain innovation demands budget, whereas the profitability cannot be retrieved in the short term.

This dilemma is not unique for blockchain technology, but characteristic for the public sector. The main difference with the private sector is that the private sector has profitability as main motivation for innovation, whereas the public sector aims at other goals, such as the quality of services or fighting poverty (Mulgan & Albury, 2003, p.6). Public sector organizations lack funds for innovation, while private sector organizations have venture capitalists (Borins, 2001, p.311).

Allocation of budget and profitability is a dilemma that is not unique for smart contract implementations, but it is characteristic for innovation in governmental services. It will therefore remain a dilemma in the future as well.

C. Communicate significance & examine impact on jobs

Implementing smart contracts can improve many processes, but has a potential impact on jobs and functions as well (Arnhem interview, 2017; Utrecht interview, 2017). From the interviews it became clear that it is important that the benefits of the implementation are communicated with stakeholders (Government Office for Science, 2016; Arnhem interview, 2017; Utrecht interview, 2017; Drechtsteden interview, 2018). However, explaining that the implementation is beneficial is hampered by the possibility of someone losing their job or changing their function: *"You have to cooperate, but you will lose your job. You cannot convince with that, but that is how it works"* (Arnhem interview, 2017). The blockchain developers from DApp.Design acknowledge this dilemma: *"My experience is that people want to know: What is in it for me? If they sense that it will impact their job in the future, you have a problem. I did a project where people really needed to be educated about the added value of the project. I think that it is important to communicate." ... "I would not start with that too early, you do not want to cause commotion"* (DApp.Design interview, 2018). It is clear that the interviewees see the dilemma as a sensitive issue that needs to be handled with care.

Table 1 – Design principles for the implementation of smart contracts in governmental services [Corten, forthcoming].

Cat	Name	Statement	Rationale	Implication	Source(s)
Political	1. Define a vision	Define a vision for blockchain based government	There has to be a shared vision for what blockchain can bring stakeholders	Stakeholders share the same vision for what blockchain will do	(Blockchainpilots.nl, 2016); (Government Office for Science, 2016); (Arnhem interview, 2017); (Schiedam interview, 2017)
Economic	2. Invest in blockchain knowledge	Invest in blockchain knowledge	The field is new and much specific knowledge is necessary	Specific knowledge increases	(Blockchainpilots.nl, 2016); (NASCIO, 2016); (Government Office for Science, 2016); (Arnhem interview, 2017); (Utrecht interview, 2017); (Schiedam interview, 2017); (Drechtsteden interview, 2018)
	3. Allocate budget	Allocate budget for research and development	Research and development are costly and need to be financially stimulated	Research and development increases	(Blockchainpilots.nl, 2016); (Arnhem interview, 2017); (Utrecht interview, 2017); (Schiedam interview, 2017)
	4. Determine profitability	Determine economic and social profitability	Successful projects are profitable in terms of educational, economic or social effects	Prevention of waste of resources	(Arnhem interview, 2017); (Schiedam interview, 2017); (Drechtsteden interview, 2018)
Social	5. Find experts	Find relevant experts from different fields	The field is new and much specific knowledge is necessary from different domains	Experts have more specific knowledge and experience	(Blockchainpilots.nl, 2016); (Arnhem interview, 2017); (Drechtsteden interview, 2018)
	6. Cooperate with other organizations	Cooperate with other public and private organizations and universities	There are many parties who can share knowledge and cooperate	Knowledge and best practices are shared	(Blockchainpilots.nl, 2016); (Pilkington, 2016); (NASCIO, 2016); (Government Office for Science, 2016); (Arnhem interview, 2017); (Utrecht interview, 2017); (Schiedam interview, 2017); (Drechtsteden interview, 2018)
	7. Involve stakeholders	Involve the right stakeholders at the right moment	Stakeholders can have different requirements and goals, but they need to be involved at the right time to prevent slowing down the process	Requirements are discussed and broadly accepted	(Blockchainpilots.nl, 2016); (NASCIO, 2016); (Arnhem interview, 2017); (Utrecht interview, 2017); (Schiedam interview, 2017)
	8. Share results	Share the results of each project	Parties can learn from each other	Project results share knowledge amongst each other	(Blockchainpilots.nl, 2016); (NASCIO, 2016); (Arnhem interview, 2017); (Utrecht interview, 2017)
	9. Compose multidisciplinary team	Compose a multidisciplinary team	Blockchain demands a team with different backgrounds, which can scale up during time	The project has experts on different fields to address different issues	(Blockchainpilots.nl, 2016); (Government Office for Science, 2016); (Arnhem interview, 2017); (Schiedam interview, 2017)
	10. Communicate significance	Communicate significance of smart contract projects to others	Due to the new character of the field, others need to be convinced of the significance	Broad audience is aware of the possibilities of smart contracts	(Government Office for Science, 2016); (Arnhem interview, 2017); (Utrecht interview, 2017); (Drechtsteden interview, 2018)
	11. Examine impact on jobs	Examine the impact on current jobs and tasks	Blockchain can cause certain jobs and tasks to be superfluous, but it depends on the process	Employees can be better prepared for a change of their job or task	(Arnhem interview, 2017); (Utrecht interview, 2017)

	12. Involve supervisor	Involve supervisor in the process	Supervisors can decide on resources that are available for the project	More support from the supervisor and more resources	(Arnhem interview, 2017); (Schiedam interview, 2017)
	13. Examine shifting role of the government	Examine the possible change of government roles	Smart contract projects can drastically change the role of the government, which needs to be examined prior to implementation	A better understanding of how smart contracts can change the role and tasks of governmental institutions	(Arnhem interview, 2017); (Drechtsteden interview, 2018)
	14. Define responsibilities	Define responsibilities in the new process	As blockchain develops, the responsibilities for certain tasks can change as well	Clarity about responsibilities	(Schiedam interview, 2017)
	15. Define project goals	Define project goals	Projects are hard to evaluate when project goals are not defined beforehand	Clear preset goals	(Schiedam interview, 2017); (Drechtsteden interview, 2018)
Technological	16. Account for security	Prioritize security and execute penetration testing	Blockchain and smart contracts demand strict security attention	Security becomes a priority and the system becomes safer	(Sharma et al., 2017); (Ølnes & Jansen, 2017); (Government Office for Science, 2016); (Arnhem interview, 2017); (Utrecht interview, 2017); (Schiedam interview, 2017)
	17. Code open source	Code in open source	Shared code spreads knowledge, but can limit security in the short term. Strive for full open source coding in the long term	Knowledge is efficiently shared	(Blockchainpilots.nl, 2016); (Pilkington, 2016); (Arnhem interview, 2017); (Utrecht interview, 2017); (Schiedam interview, 2017); (Drechtsteden interview, 2018)
	18. Select process and scope of the project	Select the process and scope of the project	It is necessary to select the correct process and to clearly communicate how far the scope reaches	The focus of implementation is clear	(Blockchainpilots.nl, 2016); (NASCIO, 2016); (Arnhem interview, 2017); (Utrecht interview, 2017); (Schiedam interview, 2017); (Drechtsteden interview, 2018)
	19. Map the process	Map the current process	Implementation builds on the prior process	It is clear how the current process works	(Blockchainpilots.nl, 2016); (Eshuis et al., 2016); (Arnhem interview, 2017); (Utrecht interview, 2017); (Schiedam interview, 2017)
	20. Build a prototype	Build a working and testable prototype	Testing is necessary before the old process can be completely replaced	Viability of implementation can be tested	(Blockchainpilots.nl, 2016); (Arnhem interview, 2017); (Utrecht interview, 2017); (Schiedam interview, 2017); (Drechtsteden interview, 2018)
	21. Start small projects	Start development with small projects	There is a lack of experience and knowledge, so small projects are the safest option	Knowledge develops with low effort and low threats	(Blockchainpilots.nl, 2016); (Government Office for Science, 2016); (Arnhem interview, 2017); (Utrecht interview, 2017); (Schiedam interview, 2017)
	22. Assess risks	Assess the risks per use case	New technology can bring new risks that need to be assessed	Clear view of risks per case	(Government Office for Science, 2016); (Schiedam interview, 2017); (Drechtsteden interview, 2018)
	23. Learn from prior development	Learn about prior projects and development, and build upon it	Prior projects show opportunities and threats, and prevents building from scratch	Proven technology can be learned from and used	(Ølnes & Jansen, 2017); (NASCIO, 2016); (Government Office for Science, 2016); (Arnhem interview, 2017); (Utrecht interview, 2017); (Schiedam interview, 2017)

	24. Decide ledger type	Decide on the type of ledger	There are different ledger types with different opportunities and threats	Ledger type fits the case	(Government Office for Science, 2016); (Arnhem interview, 2017); (Utrecht interview, 2017); (Schiedam interview, 2017); (Drechtsteden interview, 2018)
	25. Consider back-ups	Consider offline back-ups when using a private ledger	Private ledgers need back-ups, but public ledgers do not	Better protection against system failure	(Government Office for Science, 2016); (Utrecht interview, 2017); (Drechtsteden interview, 2018)
	26. Design for scalability	Make project scalable	Projects can be scaled up later if needed	Option to scale up easily	(Drechtsteden interview, 2018)
	27. Determine desired transaction speed	Define the desired minimum transaction speed	Many blockchain platforms have a low maximum transaction throughput	Understanding of the speed of the application	(Drechtsteden interview, 2018)
	28. Design good UI/UX	Design a good user interface and user experience	Blockchain technology is not visible for users, so UI/UX is important for their experience	Good user experience	(Drechtsteden interview, 2018)
	29. Determine authorizations	Determine data view and edit authorizations	Blockchain demands new definitions for who can view, edit and delete data	Clear authorization management	(Utrecht interview, 2017)
	30. Assess applicability of blockchain	Assess if blockchain is applicable for the process	Blockchain can benefit many processes, but is not applicable to each process	Good assessment of the applicability of blockchain	(Forus interview, 2018); (DApp.Design interview, 2018)
Legal	31. Research legal implications	Research legal implications and enforceability	There are possible legal issues	Possible legal issues are addressed in advance. Note that these should not limit the thinking process	(Blockchainpilots.nl, 2016); (Government Office for Science, 2016); (Utrecht interview, 2017); (Arnhem interview, 2017); (Drechtsteden interview, 2018)
	32. Define clear policies and legislation	Define clear policies and legislation regarding blockchain and smart contracts	The legislative framework was made when blockchain did not yet exist	The policies and legislation address opportunities and threats of blockchain	(Blockchainpilots.nl, 2016); (NASCIO, 2016); (Government Office for Science, 2016); (Drechtsteden interview, 2018)
	33. Define contract types	Define different contract types	Certain smart contracts have legal meaning that imply application of legislation	Clear overview of contract types and applicable laws	(Pels Rijcken interview, 2018)
	34. Define participants	Define participants when using private blockchains	Participants in private blockchains can have legal meaning and need to be trusted	Clear definition of participants and applicable legislation	(Pels Rijcken interview, 2018)
	35. Translate code to language	Translate application code to understandable language	Legislation demands certain decisions under public law to be translate to natural language	Text that explains how the application code comes to a decision	(Pels Rijcken interview, 2018)
	36. Account for privacy	Prioritize privacy	Blockchain and smart contracts demand strict privacy attention	Possible privacy risks are known and addressed	(Sharma et al., 2017); (Government Office for Science, 2016) (Arnhem interview, 2017); (Drechtsteden interview, 2018)

This dilemma was also noticed by the developers of the Kindpakket in Zuidhorn. Before smart contracts were implemented, the employee managed coupons by hand. Smart contracts automate the management of the coupons, but allow the position of the employee to change into someone who manages the program: *"In our case it was pleasant she does not lose her job, but her function changes." ... "On a large scale we should accept that people will lose their job." ... "For the lady who keeps the coupons it was scary at first, she did everything manually. Now there is a CSV-parser that automatically scans the file. She has a program on her computer now, with which she is very happy. You take something from her, but also give something back. Because we involved everyone, there was less resistance"* (Forus interview, 2018). This example shows that involving the employees can decrease resistance.

This dilemma is not new and certainly not unique for smart contract implementation. Throughout history there are many examples of technologies where some hailed the significance of implementation, while others feared the impact on jobs: the textile artisans and the automation of textile production in the 19th century (David, 2015, p.1), the automation of agriculture in the 20th century (David, 2015, p.5), the automation of the automobile belt (David, 2015, p.5) and the automation of many activities in the workplace (Chui, Manyika & Miremadi, 2015, p.3).

The communication of the significance and the impact on jobs is a dilemma that will be different for each process: some implementations will have a major impact on jobs and some will not. Involving the employees who will see their job affected can decrease resistance.

D. Security & open source coding

Academic researchers as well as practitioners agree that smart contract implementations should focus on a high level of security (Sharma et al., 2017; Ølnes & Jansen, 2017; Government Office for Science, 2016; Arnhem interview, 2017; Utrecht interview, 2017; Schiedam interview, 2017). On the other hand, sharing results and derived knowledge is also essential in order to learn from each other (Blockchainpilots.nl, 2016; NASCIO, 2016; Arnhem interview, 2017; Utrecht interview, 2017). By making the source code open for every party to see and use, knowledge is easily shared (Blockchainpilots.nl, 2016; Pilkington, 2016; Arnhem interview, 2017; Utrecht interview, 2017; Schiedam interview, 2017; Drechtsteden interview, 2018). Making the code open source has two potential effects on the security of the application. On the one hand, malicious individuals can find vulnerabilities in the code and misuse them. On the other hand, benevolent individuals can find vulnerabilities as well and report or improve them (Payne, 2002). Open source coding improves the security in the long term (Hoepman & Jacobs, 2007), but experts foresee threats in the short term: *"We want complete open source, but Kindpakket is not open source because of security." ... "You need enough eyes to look at the code, before giving it to the community. And the community has to be strong enough to do that." ... "It also involves users having a wallet with money on it and that needs a high level of security." ... "We are working each day to make it open source. In the long term I believe that open source coding is safe"* (Forus interview, 2018). ICTU however disagrees with that point of view: *"I completely disagree. There is only one secure option and that is radically transparent and open source without compromises"* (ICTU interview, 2018). These two viewpoints show the controversy of the dilemma that can be found in the literature as well. However, arguments for either viewpoint are often not strengthened with quantative data (Schryen & Kadura, 2009).

This dilemma is not unique for smart contract implementations. Many computer programs that are closed source have an open source equivalent: Internet Explorer (closed) and Firefox (open), Adobe Photoshop (closed) and Gimp (open), and Microsoft Office (closed) and OpenOffice.org (open) (Pfaffman, 2007, p.42). Admittedly, the closed source examples are also closed source to protect their revenue model, but the open source programs embrace the possibility of everyone to find and improve bugs (Pfaffman, 2007, p.38).

Open source coding is thus not unique for smart contract implementations, but can hamper the security in the short term. Experts expect that the dilemma will be less important in the long term, when a strong community has been built. The open source coding will then be less of a threat to the security. However, the dilemma is still

controversial in the literature and amongst practitioners.

E. Privacy & decide ledger type

Blockchain offers two main different ledger types. The public ledger is a transparent copy of all transactions and the balances of each address, which is distributed between many nodes (Swan, 2015, p.1). The private ledger runs between one or a few organizations, where the transactions are only transparent for a few selected nodes (Zheng et al., 2017). The transparency of the public ledger decreases the privacy of users (He et al., 2017, p.16), which can be undesirable when handling personal data. The private blockchain does not have these issues: only certain trusted parties are allowed to have a copy of the transaction history and thus increases the privacy (Janssen et al., 2017, p.1). However, the private blockchain has disadvantages over the public blockchain, such as the possibility of tampering and centralized consensus (Zheng et al., 2017, p.6). The choice for a ledger type strongly impacts the privacy. Experts acknowledge this design dilemma: "*We see that also with Kindpakket. We want to use a public blockchain, but cannot do so due to privacy problems. That is why we are actively researching zero knowledge solutions, which enables privacy on the blockchain"* (Forus interview, 2018).

Thus, the dilemma is important at the moment, but solutions are expected. The dilemma is unique for blockchain technology as it relies on specific characteristics of public and private blockchains. The potential solution that the experts mention is zero-knowledge proof of knowledge. The theory of zero-knowledge proofs is that one party possesses knowledge (the *prover*) and wants to prove that he possesses this knowledge to another party (the *verifier*). In order for this verification to be zero-knowledge proof, the verifier needs to verify that the prover possesses knowledge, without the verifier to see any of the information (Feige, 1988). This method does not reveal the information of the prover and increases his privacy (De Santis, Micali & Persiano, 1987, p.58). A specific application of this theory, called zk-SNARK, disables the transparency of transactions in the blockchain, which is already functioning in the blockchain application Zcash (Z.cash, n.d.). The most popular smart contract platform Ethereum is currently developing this application on their blockchain too (Sharma, 2017).

The importance of privacy limits the choice for a ledger type and is an unique dilemma that does not appear in other applications. However, the development of the zero-knowledge proof of knowledge is expected to address this dilemma.

F. Scalability & transaction speed

Each of the smart contract applications needs a certain transaction speed, but most blockchain based platforms are limited by their lack of scalability (Drechtsteden interview, 2018). Ethereum for example currently only allows approximately fifteen transactions per second worldwide (Etherscan.io, n.d.). This implies that if there is one single application that requires fifteen transactions per second, all other applications in the world could not use the Ethereum platform. The developers of Forus, that implemented the Kindpakket in Zuidhorn, explain that they currently have no problems with their transaction speed, but would see this dilemma as their application scales: *"We have approximately 200 children in the system and until now there have been around 500 financial transactions in a few months' time." ... "That is not a problem now, but you should account for it when you apply Kindpakket in for example Amsterdam or five municipalities"* (Forus interview, 2018). The developers of DApp.Design acknowledge the problem as well, but are optimistic: "*If I see the developments at the moment, this is one of the major problems in blockchain. They are developing this full speed. This will be solved, this year. But not now. You can do fifteen transactions per second, which is too slow. I have an example in which two or three transactions per day are necessary, it is not a problem for that process"* (DApp.Design interview, 2018).

The main solution that improves the transaction speed and scalability is called *sharding*. Ethereum is developing this solution under the project name Plasma, where it applies the MapReduce framework to the blockchain (Poon & Buterin, 2017). Currently, every transaction is validated by the entire network of nodes. Sharding will create subsets of nodes that each act as their own network of nodes. This increases the number of transactions that can be validated and thus increases the transaction speed and scalability (Buntinx, 2017).

The MapReduce framework was designed for high-performance, massively-scalable distributed systems (Rohloff & Schantz, 2010) and not for blockchain, which shows that this dilemma is not unique for blockchain. The dilemma is important until a solution is implemented, but it is expected that development of solutions such as sharding will stop this dilemma.

G. Consider back-ups & decide ledger type

Choosing between a public and private ledger also determines the need for a back-up. The fundament of blockchain technology is that a copy of the blockchain is distributed amongst all nodes in the network (Iansati & Lhakani, 2017). In a public blockchain many copies exist as there is an unlimited amount of nodes that may participate. A private blockchain however limits the number of nodes and thus the number of participants that hold a copy of the blockchain (Tapscott & Tapscott, 2016). Parties agree that a backup of data is important (Government Office for Science, 2016; Utrecht interview, 2017; Drechtsteden interview, 2018). When the number of nodes with a copy of the data is large, a back-up can be considered unnecessary, but a private blockchain only has a handful of nodes, which decreases the security of the backup function (Matanović, 2017, p.4). The interviewees acknowledge this dilemma: *"I assume it is not necessary. At least if we use a public ledger. With a private ledger we will have to"* (Drechtsteden interview, 2018). Also Zuidhorn is currently obliged to use back-ups due to the choice for a private ledger: *"The nice thing about a public chain is that it is a back-up." … "We have that with Kindpakket at the moment. Because of the trade-offs we are still on a private blockchain"* (Forus interview, 2018).

The backup characteristic of the blockchain makes this dilemma unique for smart contract implementations. The reliability of the backups depends on the number of nodes. Hence, the necessity for back-ups is inherent to private blockchains, whereas public blockchains make backups superfluous. This dilemma will therefore continue to exist.

H. Define responsibilities & decide ledger type

The prior dilemma showed that a small amount of nodes keep a record of the data in the case of a private blockchain. The responsibility for that data is for those who keep it and thus for those nodes. However, it is not clear who is responsible for the data in a public blockchain, where thousands of nodes have a back-up. Developers from the expert interviews address this dilemma: *"If you use a private ledger, the one who uses the private ledger carries responsibility for the technology and you can adapt things if you would like to. You can fork internally and no one would notice. With a public ledger, the miners carry responsibility and the consensus algorithm guarantees that responsibility"* (Forus interview, 2018). So the responsibility of data verification lies at the handful of nodes in a private ledger and with many nodes in a public ledger. Note that in a private blockchain it is easier to tamper and alter information, while this is nearly impossible in a public blockchain (Zheng et al., 2017, p.6). The division of responsibilities is different from standard IT solutions, which makes it especially important to define responsibilities in a private blockchain: "*it is necessary to clarify the responsibilities of each participating organization*" (Hou, 2017, p.4). Concluding, choosing between a public and a private ledger has a great impact on how responsibilities are divided between participants of the network.

This dilemma is inherent to the characteristics of the blockchain and thus both unique for blockchain as a permanent feature.

IV. Conclusion

The field of blockchain lacks academic research and empirical knowledge. An overview of design principles to aid project teams that implement smart contracts in governmental services and design dilemmas they encounter was non-existent, hampering the implementation of smart contracts. We used the design science approach in order to create the first overview of 36 principles with empirical knowledge from four case studies. This overview can support project teams in accelerating the implementation process, which can lead to more actual implementations. Furthermore, we found the following seven dilemmas that force project teams to make design choices:

1. Allocate budget & profitability;
2. Communicate significance & examine impact on jobs;
3. Security & open source coding;
4. Privacy & decide ledger type;
5. Scalability & transaction speed;

6. Consider back-ups & decide ledger type;
7. Define responsibilities & decide ledger type.

Three dilemmas are unique for smart contract implementations and are not yet seen in other IT projects: privacy & decide ledger type, consider backups & decide ledger type, and define responsibilities & decide ledger type. Their uniqueness comes from the new characteristics that blockchain offers when choosing between a public and private ledger, which therefore were not yet known from other IT projects. These dilemmas demand extra attention as research on their effects and coping strategies is non-existent. The other four dilemmas are known from other IT projects, which makes it interesting to assess if existing coping strategies for these dilemmas are applicable in smart contract implementation projects as well.

Two dilemmas are expected to be solved in the short term due to the developments of blockchain technologies themselves: privacy & decide ledger type can be solved with *zero-knowledge proof* solutions and scalability & transaction speed can be solved with *sharding*. Project teams will have to cope with these dilemmas for now, but it is expected that these will be solved by future technological improvements. Five of the dilemmas are considered to be permanent, which means that project teams will need to account for them in the future as well. Table 2 provides an overview of the characteristics per dilemma.

Table 2 - Characteristics of the design dilemmas.

Dilemma	**Unique**	**Solution expected**
Allocate budget & profitability	No	No
Communicate significance & examine impact on jobs	No	No
Security & open source	No	No
Privacy & decide ledger type	Yes	Yes
Scalability & transaction speed	No	Yes
Consider back-ups & decide ledger type	Yes	No
Define responsibilities & decide ledger type	Yes	No

Further research is essential to describe the characteristics of these dilemmas more in-depth, as we used a limited amount of cases and experts in order to derive a first overview. More case studies and expert interviews can be conducted to derive more information about these dilemmas and to assess if these dilemmas exist in all governmental services that implement smart contracts. Another recommendation is to study the coping strategies of these dilemmas. We derived a first overview of the dilemmas and described some potential coping strategies, but these strategies can be researched more in-depth. Further research can assess the applicability of existing strategies on our overview of design dilemmas on the one hand and can find new strategies for the dilemmas on the other hand.

References

Bahga, A., & Madisetti, V. K. (2016). *Blockchain Platform for Industrial Internet of Things.* Journal of Software Engineering and Applications, 9(10), 533.

BBC (2018). *What Is Blockchain and how Does It Work?* Retrieved online on the 8th of February 2018 from http://www.bbc.com/news/av/business-38932854/what-is-blockchain-and-how-does-it-work.

Blockchainpilots.nl (2017). *Blockchain Pilots: A Brief Summary.* Retrieved online on the 15th of December 2017 from https://docs.wixstatic.com/ugd/df1122_3de6de424d3b4f618af9e768e12d0ca0.pdf.

Blumer, H. (1954). *What Is Wrong With Social Theory?.* American Sociological Review, 19(1), 3-10.

Borins, S. (2001). Encouraging Innovation in the Public Sector. Journal of Intellectual Capital, 2(3), 310-319.

Buntinx, J. P. (2017). *What Is Sharding?* Retrieved online on the 7th of February 2018 from https://themerkle.com/what-is-sharding/.

Buterin, V. (2013). *Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform.* Retrieved online on the 8th of February 2018 from http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

Chui, M., Manyika, J., & Miremadi, M. (2015). *Four Fundamentals of Workplace Automation.* McKinsey Quarterly, 29(3), 1-9.

CNN (2018). *European Banks Could Soon Hold Bitcoin, Admits ECB President.* Retrieved online on the 8th of February 2018 from https://www.ccn.com/european-banks-soon-hold-bitcoin-admits-ecb-president/.

Coinmarketcap.com (n.d.). *Cryptocurrency Market Capitalizations.* Retrieved online on the 8th of February 2018 from https://coinmarketcap.com/.

Corten, P.A. (Forthcoming). Implementation of Blockchain Powered Smart Contracts in Governmental Services (Complex System

Engineering and Management, Master Thesis), Delft University of Technology, Delft. Retrieved from repository.tudelft.nl.

David, H. (2015). *Why are There Still So Many Jobs? The History and Future of Workplace Automation.* Journal of Economic Perspectives, 29(3), 3-30.

De Santis, A., Micali, S., & Persiano, G. (1987). *Non-Interactive Zero-Knowledge Proof Systems.* In Conference on the Theory and Application of Cryptographic Techniques (pp. 52-72), Santa Barbara, August 16-20, 1987. Berlin: Springer.

Drescher, D. (2017). *Blockchain Basics: A Non-Technical Introduction in 25 Steps.* New York: Apress.

Eshuis, R., Norta, A., & Roulaux, R. (2016). *Evolving Process Views.* Information and Software Technology, 80, 20-35.

Etherscan.io (n.d.). *Ethereum Transaction Chart.* Retrieved online on the 7th of February 2018 from https://etherscan.io/chart/tx.

Feige, U., Fiat, A., & Shamir, A. (1988). *Zero-Knowledge Proofs of Identity.* Journal of Cryptology, 1(2), 77-94.

Financial Times (2018). *Blockchain Explainer: A Revolution Only in its Infancy.* Retrieved online on the 8th of February 2018 from https://www.ft.com/content/6c707162-ffb1-11e7-9650-9c0ad2d7c5b5.

Gaggioli, A. (2018). *Blockchain Technology: Living in a Decentralized Everything.* Cyberpsychology, Behavior, and Social Networking, 21(1), 65-66.

Gläser, J., & Laudel, G. (2009). On Interviewing "Good" and "Bad" Experts. In *Interviewing Experts* (pp. 117- 137). Basingstoke: Palgrave Macmillan UK.

Government Office for Science (2016). *Distributed Ledger Technology: Beyond Block Chain.* Retrieved online on the 8th of February 2018 from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

He, D., Leckow, R., Haksar, V., Mancini-Griffoli, T., Jenkinson, N., Kashima, M., ... & Tourpe, H. (2017*). Fintech and Financial Services: Initial Considerations.* International Monetary Fund Staff Discussion Note, 17(05).

Hevner, A., Von Alan, R. H., March, S. T., Park, J., & Ram, S. (2004). *Design Science in Information Systems Research.* MIS Quarterly, 28(1), 75-105.

Hoepman, J. H., & Jacobs, B. (2007). *Increased Security Through Open Source.* Communications of the ACM, 50(1), 79-83.

Hou, H. (2017). *The Application of Blockchain Technology in E-Government in China.* In the 26th International Conference on Computer Communications and Networks (ICCCN 2017), (pp. 1-4), Vancouver, July 31-August 3, 2017. Washington: IEEE.

Iansiti, M., & Lakhani, K. R. (2017). *The Truth About Blockchain*. Harvard Business Review, 95(1), 118-127.

Janssen, R. T. J. M., Stam, P., Visser, J., de Vries, D., & Wijnker, J. (2017). Blockchaintechnologie in de Gezondheidszorg. ESB, 102(4752), 394-397.

Matanović, A. (2017). *Blockchain/Cryptocurrencies and Cybersecurity, Threats and Opportunities*. In the 9th International Conference on Business Information Security (BISEC-2017), (pp. 11-15), Belgrade, October 18. Belgrade: Belgrade Metropolitan University.

Mulgan, G., & Albury, D. (2003). *Innovation in the Public Sector.* Strategy Unit, Cabinet Office, 1(40).

Municipality of Zuidhorn, 2017. *Innovatieve Uitvoering Kindpakket met Belangrijke Eerste Stap Blockchain Technologie.* Retrieved online on the 7th of 2017 from https://www.zuidhorn.nl/bestuur-en-organisatie/nieuws_3800/item/innovatieve- uitvoering-kindpakket-met-belangrijke-eerste-stap-blockchain-technologie_6490.html.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Unpublished manuscript. Retrieved online on the 5th of September 2017 from https://bitcoin.org/bitcoin.pdf.

NASCIO (2017). *Blockchains: Moving Digital Government Forward in the States.* Retrieved online on the 8th of February 2018 from https://www.nascio.org/Portals/0/Publications/Documents/2017/NASCIO%20Blockchains%20in%20State%20Government.pdf.

Ølnes, S., & Jansen, A. (2017). *Blockchain Technology as s Support Infrastructure in e-Government. In International Conference on Electronic Government* (pp. 215-227), St. Petersburg, September 4-7, 2017. Cham: Springer.

Ølnes, S., Ubacht, J., & Janssen, M. (2017). *Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing.* Government Information Quarterly 34(3), 355-364.

Payne, C. (2002). *On the Security of Open Source Software.* Information Systems Journal, 12(1), 61-78.

Pfaffman, J. (2007). It's Time to Consider Open Source Software. TechTrends, 51(3), 38-43.

Pilkington, M. (2016). Blockchain Technology: Principles and Applications. In *Research Handbook on Digital Transformations* (pp.225-253). Cheltenham: Edward Elgar

Pomp, M. & Hartog, K. (2017). Blockchain Magazine. Retrieved online on the 14th of October 2017 from http://hostedby.frogjump.nl/blockchain-magazine#!/Blockchain magazine.

Poon, J. & Buterin, V. (2017). *Plasma: Scalable Autonomous Smart Contracts. Unpublished manuscript.* Retrieved online on the 7th of February 2017 from http://plasma.io/plasma.pdf.

Rohloff, K., & Schantz, R. E. (2010). *High-Performance, Massively Scalable Distributed Systems Using the MapReduce Software Framework: The SHARD Triple-Store.* In The SPLASH Workshop on Programming Support Innovations for Emerging Distributed Applications (PSI EtA - ΨH 2010), (pp. 4.1-4.5), Reno, October 17, 2010. New York: ACM.

Schryen, G., & Kadura, R. (2009). *Open Source Vs. Closed Source Software: Towards Measuring Security*. In The 2009 ACM Symposium on Applied Computing (pp. 2016-2023), Honolulu,

March 8-12, 2009. New York: ACM.
Scopus (n.d.). *Document Results.* Retrieved online on the 15th of December 2017 from https://www.scopus.com.
Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). *Block-VN: A Distributed Blockchain Based Vehicular Network Architecture in Smart City.* Journal of Information Processing Systems, 13(1), 84.
Sharma, R. (2017). *'Zero Knowledge Proofs' Could Boost Blockchain Adoption on Wall Street.* Retrieved online on the 7th of February 2018 from https://www.investopedia.com/news/zero-knowledge-proofs-could-boost-blockchain-adoption-wall-street/.
Swan, M. (2015). *Blockchain: Blueprint for a New Economy.* Sebastopol: O'Reilly Media.
Szabo, N. (1994). *Smart Contracts.* Unpublished manuscript. Retrieved online on the 5th of September 2017 from http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.
Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.* New York: Penguin.
VNG / KING (2017). *Gemeentelijke Blockchainpilots 2017.* Retrieved online on the 9th of January 2018 from https://depilotstarter.vng.nl/sites/default/files/project_bestand/gemeentelijke_blockchainpilots_20171_0.pdf.
Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). *Where Is Current Research on Blockchain Technology?—A Systematic Review.* PloS one, 11(10).
Z.cash (n.d.). *Internet Money*. Retrieved online on the 7th of February 2018 from https://z.cash/technology/index.html.
Zetzsche, D. A. and Buckley, R. P., Arner, D. W. & Föhr, L. (2017). *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators.* Unpublished manuscript, University of Luxembourg. Retrieved on the 5th of March 2018 from: https://ssrn.com/abstract=3072298.
Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.* In Big Data (BigData Congress), 2017 IEEE International Congress, (pp. 557-564), Honolulu, June 25-30, 2017. Washington: IEEE.

Appendix A: List of interviewees

Table 3. Details of the interviews

Date	Organization	Interviewee role(s)
December 20, 2017	Municipality of Arnhem	Advisor Process & Advisor Business Intelligence
December 21, 2017	Municipality of Schiedam	Program Manager Social Infrastructure
December 22, 2017	Municipality of Utrecht	Data Scientist
January 4, 2018	Municipalities of Drechtsteden	Business Consultant
January 23, 2018	Blockchainpilots.nl	Project Manager National Blockchain Pilots
January 25, 2018	DApp.Design	Blockchain Developers
January 22, 2018	ICTU	Data Scientist for the Dutch Government
January 22, 2018	Pels Rijcken	Law Expert
January 26, 2018	Municipality of Groningen	Project Leader Stadjerspas
January 29, 2018	Forus	Blockchain Developers