Aligning stakeholder interests, governance requirements and blockchain design in business and government information sharing

van Engelenburg, S.H.; Rukanova, B.D.; Hofman, Wout; Ubacht, J.; Tan, Y.; Janssen, M.F.W.H.A.

DOI
10.1007/978-3-030-57599-1_15

Publication date
2020

Document Version
Final published version

Published in
Electronic Government - 19th IFIP WG 8.5 International Conference, EGOV 2020, Proceedings

Citation (APA)
van Engelenburg, S. H., Rukanova, B. D., Hofman, W., Ubacht, J., Tan, Y., & Janssen, M. F. W. H. A. (2020). Aligning stakeholder interests, governance requirements and blockchain design in business and government information sharing. In G. V. Pereira, M. Janssen, H. Lee, I. Lindgren, M. P. R. Bolívar, H. J. Scholl, & A. Zuiderwijk (Eds.), *Electronic Government - 19th IFIP WG 8.5 International Conference, EGOV 2020, Proceedings* (pp. 197-209). (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Vol. 12219 LNCS). Springer. https://doi.org/10.1007/978-3-030-57599-1_15

Aligning Stakeholder Interests, Governance Requirements and Blockchain Design in Business and Government Information Sharing

Sélinde van Engelenburg[1](✉), Boriana Rukanova[1], Wout Hofman[2], Jolien Ubacht[1], Yao-Hua Tan[1], and Marijn Janssen[1]

[1] Delft University of Technology, Delft, The Netherlands
{S.H.vanEngelenburg,B.D.Rukanova,J.Ubacht,Y.Tan,
M.F.W.H.A.Janssen}@tudelft.nl
[2] TNO, The Hague, The Netherlands
wout.hofman@tno.nl

Abstract. Governance requirements for systems supporting information sharing between businesses and government organisations (B&G) are determined by a high variety of stakeholders with often conflicting interests. These conflicting interests can hamper the introduction and scaling-up of ICT-innovations that change their roles and authorities. We address one such innovation: the introduction of blockchain technologies in the B&G context. Who can govern data and the system depends on several elements of the design of a blockchain-based system, particularly the data structure, consensus mechanism and network topology. Design choices regarding these elements affect who can make decisions and hence we call them blockchain control points. These control points require an explicit and well-understood relationship between the design decisions and the interests of stakeholders. Yet, the literature on blockchain technology and governance does not offer such insight. Therefore, we developed a framework to assess the alignment between stakeholders interest and blockchain design choices. This framework consists of three views and their interrelationships, 1) a stakeholder view providing insight into the tensions between stakeholder's interests and governance requirements, 2), a governance view on the rights concerning the data and the system, and 3) a blockchain control view describing how design decisions on the control points affect whether governance requirements are met and how parties can exercise their rights. Making these links explicit enables an understanding of how technical design choices can trigger organizational dynamics from the stakeholder view and vice versa. Based on the framework we formulate a research agenda concerning blockchain design choices and governance.

Keywords: Blockchain technology · Distributed ledger technology · Governance · Business · Government · Information sharing · Access control · Consensus mechanism

Published by Springer Nature Switzerland AG 2020
G. Viale Pereira et al. (Eds.): EGOV 2020, LNCS 12219, pp. 197–209, 2020.
https://doi.org/10.1007/978-3-030-57599-1_15

1 Introduction

The literature on information sharing between businesses and/or government organisations (B&G information sharing) describes various blockchain-based systems, ranging from supply chain management to information sharing to improve safety and security, and to e-government (e.g., [1–5]). In these domains, various stakeholders are involved, with often conflicting interests. For example, it might be in the interest of businesses in a supply chain to share information to reduce the bullwhip effect and reduce costs [6, 7]. Furthermore, the government might want to reuse the same data for risk assessment [8]. However, businesses might only want to share data if it is secure and can only be controlled and accessed by the appropriate and identifiable parties [9–11]. Parties like IT providers also have their interests. Hence, we view blockchain-based systems as complex socio-technical systems in which many stakeholders with divergent interests are involved.

In 2009, Satoshi Nakamoto [12] combined several existing technologies to solve the double-spending problem for the cryptocurrency Bitcoin without an intermediary. He created the first example of what was later called blockchain or distributed ledger technology. Later on, blockchain technology was generalised to other application domains. Blockchain technology (BCT) has several features that can make it also useful for B&G information sharing: a high level of transparency, immutability and reliability.

In contrast to the more simple case of cryptocurrencies in which a transaction takes place between two parties that send and receive the currency, in the case of B&G information sharing, a diversity of types of transactions can occur in which multiple stakeholders are involved. Stakeholders that can play a diversity of roles and have different types of relationships. This leads to a complicated context that requires different technological design choices. For example, if BCT is used to support cryptocurrencies, usually all nodes can view and verify transactions and are anonymous [12]. But when businesses want to reduce the bullwhip effect in supply chains, the data needs to be accessible only to a select number of identifiable parties to avoid disclosure of sensitive business data.

In the literature, some solutions in the domain of blockchain technology are provided that can help to deal with the different governance needs for B&G information sharing, e.g. the use of private networks or proof of authority as a consensus mechanism [1]. However, no framework exists that helps to assess the relationship between the design of the blockchain-based system on the needs for governance in the B&G information sharing domain and vice versa. Simultaneously, it requires looking at the entire technical design of the system to assess whether these needs are met and aligned with stakeholder interests. In this paper, we present a framework to provide insight into the relationship between blockchain design choices and governance for B&G information sharing. This insight can enable adaptive government and contribute to an agile government [13, 14].

First, we provide an overview of the framework in Sect. 2. Next, in Sect. 3, we present the stakeholder view of the framework which provides insight into the complexities and dynamics of B&G information sharing. We illustrate this by a case of B&G information sharing in international trade. In Sect. 4, we introduce the concept of governance requirements to make the rights of stakeholders explicit. In Sect. 5, we present the blockchain control points and how different design choices affect which rights parties can exercise. In Sect. 6, we show the use of the framework based on the case of TradeLens. Based on

this, in Sect. 7, we outline our research agenda for further research into the relationship between blockchain design choices and governance.

2 A Governance Framework for Blockchain-Based B&G Information Sharing

In this section, we present an overview of the proposed framework. The framework allows for systematically analysing the relationships between the stakeholder context of parties involved in B&G information sharing, the governance requirements stemming from this context and the blockchain design choices (see Fig. 1). Here, we present the relationships between the views of the framework.

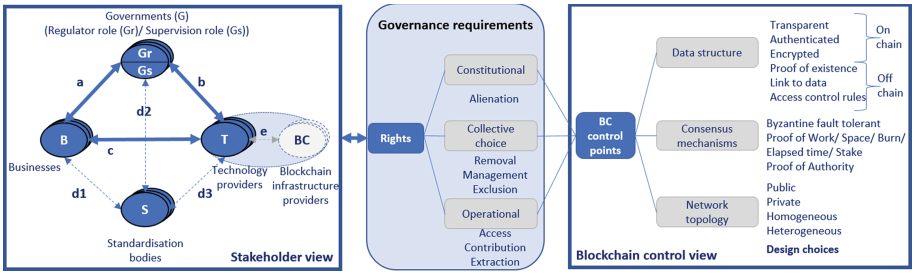

Fig. 1. Overview of the proposed framework for systematically analyzing the relationship between governance in B&G information sharing and design choices in blockchain technology.

Governance as an abstract concept can be seen as all processes of social organization and social coordination [15]. We use the term governance in the broad sense as processes of social organization and coordination that relate to blockchain-based B&G information sharing. We use the term governance requirements, as discussed later in this paper, in a more narrow sense as decision rights that parties should be able to exercise based on stakeholder dynamics and the design choices.

The first view of our framework is the stakeholder view where we classify the stakeholders in B&G information sharing and discuss their interests and potential tensions between them. The blockchain control view refers to blockchain control points. Control points enable parties to exercise power over other actors in a sociotechnical system and are often domain-specific [16, 17]. We identified several control points for blockchain-based systems that are subject to design choices. By making design choices, different ways of governing the data and the system are enabled. Therefore, changes in configurations of design choices for these blockchain control points can also lead to a change in the power dependencies among the stakeholders involved.

It is difficult to systematically translate high-level dynamics between stakeholders into blockchain design choices, and vice versa. The needs for governance in B&G information sharing of the stakeholder view are complicated and often described based on high-level concepts. While considering governance in this way helps to reveal the high-level dynamics at play, it is difficult to translate to and from more low-level design choices for the information-sharing system.

Therefore, to allow for a systematic analysis of the interaction between design choices at blockchain control points and the stakeholder interests, we introduce another view of the framework, which relies on the concept of governance requirements. The governance requirements act as an intermediary between high-level governance considerations and low-level technical design choices. Governance requirements describe decision rights that parties should be able to exercise explicitly. The determination of the rights for the stakeholders involved starts in the stakeholder view and leads to agreements (e.g., specified in contracts). On the other hand, what rights parties can exercise depends on the technological design choices made. The framework shows this relationship by placing the governance requirements between the stakeholder and the blockchain control view.

The framework can be used in two ways: 1) a. analyze the stakeholder dynamics to come to an agreement and determine what governance requirements should be met and then b. identify the design choices that allow for meeting these requirements, and 2) a. determine the effect of certain design choices on the meeting of governance requirements, and b. determine the effects on the tensions between the stakeholders involved. The framework could be used at different stages of the design process. For example, relationships and interests among stakeholders can change, or external factors can force different design choices, e.g., in the case of new laws or regulations.

3 Stakeholders and Complexity in the B&G Information Sharing Domain

The B&G domain is fundamentally different from the cryptocurrency domain. To develop blockchain-based systems, the complexities and specificities of the B&G domain are key for understanding the design options. As indicated in Fig. 1, we identify four main stakeholder groups on a high level of abstraction (labelled by multiple ovals) that are relevant in the context of B&G information sharing:

1. *Businesses* (B), such as supply chain partners, are in the business stakeholder group. Their motivation to use blockchain technology is usually driven by a strive for competitive gains and economic benefits, and increasingly by social responsibility.
2. *Government agencies* (G) can act in different roles, e.g. as a regulator (Gr) or as a body supervising the activities of businesses (Gs). In their regulatory role, government agencies can issue laws and regulations or can adopt policies to stimulate developments by e.g. providing public funding. In their role of government supervision, governments are interested in receiving additional information from businesses to perform their supervision processes, such as customs risk assessment or compliance management.
3. *Technology providers* (T) refer to infrastructure and platform providers. These are providers of technical solutions to businesses and government and they are driven by their business model. Recently, this group also includes new actors (BC) that specifically provide blockchain infrastructures such as Hyperledger.
4. *Standardization bodies* (S) also play a role in the B&G domain. The growth in multiple blockchain-enabled solutions requires standardization for interoperability of blockchain-based systems and services.

Figure 1 shows that these actors are interrelated. We show the primary relationship between government, business and technology providers as solid arrows labelled with *a*, *b*, and *c* respectively. The dotted arrows labelled *d* denote the secondary link of each of these stakeholders with standardization organizations. We also explicitly depict the link between technology providers and blockchain providers (arrow labelled *e*) as there can be conflicting and mutual interests between these parties as well. All of these links can be used to identify potential tensions.

While the model is quite general and would apply to other cases as well, we illustrate it by using the example of international trade. Here, we see the complexity of the international supply chains that link many business actors. When goods are moved on a global scale, a diversity of governing authorities (e.g., customs) are involved when the goods cross national borders. Especially in a global setting, multiple levels of government, ranging from national, supranational (e.g., EU) to global (e.g., World Customs Organization) are involved. These governmental organisations exchange information with other governments and businesses.

In B&G information sharing, standardization plays a key role. International standardization bodies such as UN CEFACT play a crucial role in standardizing business documents and data sets. The World Customs Organization developed the World Customs Data Model. Currently, these standards focus on older means of information sharing, such as messaging and declarations. This means that innovative implementations take a lot of time before actual adoption.

The B&G information-sharing world is quite fragmented. Over the last decades, efforts have been made on the side of both businesses and governments to overcome such fragmentation and to allow for better information sharing. Recently, global digital trade infrastructures enabled by blockchain have emerged that allow government agencies to access (additional) business information from the supply chains, which is provided voluntarily [18]. While technically it is becoming increasingly easy to share information in the B&G domain, information sharing remains a complex issue [19]. Businesses and governments are extremely careful that key information is not accessible to parties that are not authorized to see it. In the B&G domain, parties are rarely anonymous, as is often the case with cryptocurrencies. For example, in purchasing contracts and subcontracting contracts, different parties will need to be named. Government agencies need to know which parties are filing import and export declarations, so these parties need to be registered to perform these operations. Linking these stakeholder dynamics to blockchain design choices directly is difficult. In the next section, we introduce the governance requirements as a way to link the two.

4 Governance Requirements

We now turn to the governance requirements in our framework. These have two dimensions: 1) which parties should have control, and 2) the extent to which parties should have control. For the first, we turn to the work of Constantinides [20]. He relies on work from the field of natural resource commons arrangements. This viewpoint is relevant, as the distributed nature of blockchain with the complexities of B&G information sharing will rarely lead to simple centralised governance arrangements. Constantinides [20]

views infrastructure resources, such as a database containing data, in a way analogous to natural resources, such as a forest containing trees. In our case, the main resource is the blockchain on which different types of data are stored. These can include transactions, smart contracts, events or documentation.

In some cases, the data in B&G information sharing is not stored in the blockchain itself, but the blockchain stores only hashes of the data, links to the data, or rules for controlling access to the data. This turns the databases that store the actual data into resources as well. Furthermore, if the data on the blockchain is encrypted, then the system for generating and sharing keys is also a resource, for example.

Table 1. Different types of rights in blockchain-based B&G information sharing systems (adapted from [20, 21])

Rights		**Rights in a blockchain-based system for B&G information sharing**
Constitutional rights	Alienation	Right to determine who has what collective rights
Collective choice rights	Removal	Right to remove parts of the blockchain-based system
	Management	Right to determine how, when, and where parts of the blockchain-based system can be used and choices on control points may be changed
	Exclusion	Right to determine who has what operational and removal rights and how these can be transferred
Operational rights	Access	Right to access parts of the blockchain-based system (i.e., nodes, external databases or key management system)
	Contribution	Right to store, revise or delete data shared using blockchain.
	Extraction	Right to obtain access to data shared using blockchain

Constantinides [20], based on the work of Ostrom [21], describes three types of rights, namely constitutional, collective choice and operational rights. Constitutional rights refer to who may or may not participate in making collective choices for the system [20]. Collective choice refers to rights concerning users and components within the information system, and operational rights refer to those related to access to the information system and the data [20]. In Table 1, we describe how these types of rights can be applied in the case of a blockchain-based B&G information sharing system. It is important to note here that 'data shared using blockchain' can refer to data that is directly stored in the blockchain, as well as data that is stored elsewhere.

A governance requirement is a description of to what extent certain parties should have what rights. As the domain of B&G information sharing is complex due to multiple stakeholders with various interests, parties will often need to share rights and there will not be a single party that can make all decisions by themselves. For example, a consortium of parties might need to share the right to decide who can be a node in the network. The consortium in that case then shares exclusion rights concerning access to the system. The consortium might also decide that a carrier should have extraction rights, which is a governance requirement. To fulfil this requirement, the system needs

to be designed such that the carrier can prevent or permit others to extract data. Whether this is the case, depends on the design choices described in the next section.

5 The Blockchain Control View

The blockchain control view connects design choices and governance requirements. First, we identify control points that can be used to control who can exercise what rights in the system. Then, we identify possible design choices for those control points. Next, we relate the effects of the design choices to the rights presented in Table 1. Table 2 shows the control points and each design choice we identified.

Table 2. Overview of control points and design choices in the framework

Control point	Design choice	Description
Data structure	Transparent	The data to be shared is stored on the blockchain without encryption
	Authenticated	The data to be shared is stored on the blockchain. The party that adds the data encrypts it to authenticate it. Others can decrypt and verify their identity.
	Encrypted	The data to be shared is stored on the blockchain. The party that adds the data encrypts it to keep it confidential from others. Only parties provided with a key can view the data.
	Proof of Existence	A hash of the data to be shared is stored on the blockchain to prove it existed when it was added and make it possible to determine whether the data changed afterwards. The data itself is stored elsewhere.
	Link to data	A link to the data to be shared is stored on the blockchain. The link can be used to find the data stored elsewhere.
	Access control rules	Rules for controlling access to the data that needs to be shared is stored on the blockchain. Parties are allowed to extract the data stored elsewhere based on these rules.
Blockchain network topology	Public	Anyone can be a node in the network.
	Private	Only some parties can be a node in the network and have certain rights.
	Homogeneous	All nodes store the same data and link in the same way to other nodes.
	Heterogeneous	Nodes differ in the data that they store and/or the links they have to other nodes.
Consensus mechanism	Byzantine fault-tolerant	Relies on 'good' nodes not forwarding malicious messages to the rest of the network. Requires the network not to be public to avoid Sybil attacks.
	Proof of work/ space/ stake/ …	Relies on nodes performing a certain task or having a certain property and the rest of the network checking this before accepting the blocks they add.
	Proof of Authority	Only authorized nodes control who can add blocks to the blockchain.

Some design choices can be combined, such as authenticated and encrypted data. The data structure control point refers to the form of the data stored in the blocks and whether the data that is to be shared is stored in the blockchain itself, or whether the blockchain is only used to share data stored elsewhere. An important effect of the choice of encrypting data is that someone with extraction rights requires a key to be able to exercise their rights. When only proofs of existence, links, or access control rules are stored for the data, then not only the rights over the blockchain components and the data in the blockchain will need to be considered, but also over the additional databases and the data that is stored there. Storing the actual data elsewhere, however, does provide new opportunities, for example, to remove the data.

The blockchain network topology control point refers to the arrangements concerning who can be a node in the blockchain network and how nodes are linked. Public and private refers to whether the network is publicly accessible or not. Of course, the main effect of design choices for the blockchain network topology is in the access rights to nodes. Whether a party can be a node, in turn, determines whether they can exercise other rights, such as contribution rights. Whether the network is homogeneous or heterogeneous can play a role in who has extraction rights as it affects what data they can store or receive.

The consensus mechanism also affects different rights. The consensus mechanism determines how a consensus is reached between parties about what blocks should be in the chain and who can add them and under which conditions. The choice for consensus mechanism thus directly affects contribution rights. For example, the parties that provide Proof of Work (PoW) can exercise contribution rights, while for Byzantine Fault Tolerance (BFT) all nodes that do not send messages that are considered malicious by the other nodes can do so. Furthermore, the consensus mechanism determines who can decide who should be able to exercise contribution rights. In the case of BFT, this is 2/3 of the nodes and for PoW this is the nodes with 51% of CPU power [12, 22].

6 Demonstration of the Framework: The TradeLens Case

We use an empirical case to demonstrate the use of the framework. In-depth knowledge of the development of TradeLens was gained by participatory research as part of the PROFILE[1] Horizon 2020 EU project. TradeLens[2] is a global blockchain-enabled infrastructure driven by IBM and Maersk, that allows for sharing events and documents in international trade. Initial development and piloting started in 2015. In 2018, it was rolled out as a global commercial infrastructure. The goal of TradeLens is digitizing global trade [18]. Digitization and development of digital trade infrastructures such as data pipelines are aimed at overcoming fragmentation of the information passed through systems of supply chain partners and authorities, and overcoming inefficiencies in the exchange of paper documents [8, 23, 24].

Stakeholder View: The stakeholder group for TradeLens includes various network partners and client groups, such as carriers, government authorities, shippers, and providers of financial services. TradeLens is intended to be open to other industry parties. But,

[1] https://www.profile-project.eu/.
[2] https://www.tradelens.com/.

carriers are competitors and therefore they do not want to provide their data to each other. Authorities are interested in access to business data to perform their customs risk assessment and to cross-validate the customs declaration data against business data.

Governance Requirements: Considering the governance requirements, TradeLens is owned by IBM and MAERSK and, therefore, they hold the constitutional rights. As TradeLens is intended to be open to other industry parties, the collective choices are made by the TradeLens board, which includes IBM, Maersk and additional carriers. Businesses and government authorities who interact with TradeLens are granted operational rights. The operational rights are defined in data sharing specifications agreed upon by stakeholders. For example, TradeLens has access rights to be a node to provide its services, but by default does not have extraction rights to the data. Authorities only have extraction rights to relevant data. Also, it is required that carriers cannot extract each other's data.

Blockchain Control View: For TradeLens, design choices were made to provide the parties involved with the ability to exercise their rights and to allow for scaling up the system. Regarding the network topology, the choice was made to rely on Hyperledger. The network consists of several private networks called channels. As a carrier can be a node, they can exercise their access right. Other parties that have access rights can become one as well. To meet the governance requirement that carriers cannot extract each other's data, the channels are reserved for single carriers in a private network. TradeLens has a node in each of these private networks, and the network is thus heterogeneous.

Regarding the data structure, initially, the design choice was to store documents on the blockchain and encrypt them to ensure that only the appropriate parties can extract them. Later, to enhance scalability, documents were stored off-chain and a link to the document plus a hash of the content of the document is stored on the chain. Authorities can use the link to determine where the data is stored and the hash of the retrieved document will be compared with the hash stored on the chain, to prove the document's content has not changed.

Several issues propagate from the stakeholder view through the governance requirements to the blockchain control view and vice-versa. We illustrate the interdependency between the views with two examples. The government has extraction rights to some documents. When the data was stored on-chain, they exercised that right by obtaining data from the blockchain and by obtaining a decryption key. However, when the data was stored off-chain, the documents need to be stored in an external document storage where they need to obtain them from. This triggers additional complexity in the stakeholder view. In particular, the question becomes who will provide the document store and how to ensure that the documents will not be deleted. In principle, TradeLens, other technology providers or the businesses themselves can host a document store. Momentarily, complexity is reduced by TradeLens offering the document storage themselves, with the agreement of the other parties. If in the future parties prefer to arrange their own document storage, this will trigger additional stakeholder dynamics, as additional negotiations and agreements on how the data storage would be handled would need to be made between TradeLens and these other actors.

One more example is related to illustrating the dynamics among different technology providers (represented with multiple (T) ovals in our framework in Fig. 1). In this case, we take a specific example of the creation of value-added services by other technology providers. TradeLens is a node but only has access rights and no extraction rights. This is similar to the role of a Port Community Systems (PCSs) for its members in the Netherlands (i.e. facilitating data sharing without extraction rights). TradeLens collaborates with the PCS in Rotterdam. The PCS has information about the container when the container arrives at the Port of Rotterdam. TradeLens has information about the route of the container and possible rerouting before it arrives at the port of Rotterdam. TradeLens and PortBase are collaborating to link their systems. An independent company which provides services for the planning of pick-up slots for barges arriving at the port of Rotterdam was able to arrange extraction rights to the data of the PCS and TradeLens to offer value-added services. They approached the relevant businesses that own the data that is held in TradeLens and the PCS and requested permission to see their data. Once the businesses gave permission, the independent company could access the data and provide the value-added services. This example shows how technology providers like third-party app providers can make use of platforms like TradeLens to create value-added services on top of the blockchain-based system. Therefore by detailing the technology (T) stakeholder group from the stakeholder view we can reason about the dynamics of actors involved in this group and how this relates to the blockchain design choices.

7 Directions for Further Research

The examples in Sect. 6 illustrate how our framework enables manoeuvering back and forth from an abstract understanding of the domain and stakeholders to a detailed understanding of the dependencies between governance requirements, blockchain control points and design choices. This interplay allows us to gain insight into the dependencies within complex socio-technical systems based on a blockchain-based system.

We demonstrated the framework in a case from the global trade logistics domain. We identified examples of interdependencies between the components of the framework. As the relationship between the stakeholder interests, the governance requirements and the control points in the blockchain architecture were not addressed in the extant literature, we consider the framework as a starting point for future research. The framework provides a structured approach to identify interdependencies in other complex sociotechnical blockchain-based systems. Table 3 provides an initial overview of future research topics based on the interactions that we identified in the framework.

Table 3. Future research topics based on interactions between views in the framework

Interactions	Topics for further research
Stakeholders → governance requirements → blockchain control points	Detailing the technology stakeholders into blockchain infrastructure, blockchain solution and app providers and investigating: - possible scenarios regarding the distribution of rights among the technology providers and how they impact their business models; - the effects of the scenarios on user rights; - what the different scenarios are for adding value-added services (e.g. smart contracts or off-chain apps relying on blockchain data) and how these can affect the business models of technology providers and the user stakeholder group; - what are complexities for determining the true ownership of data in the stakeholder view and how does it affect the distribution of rights.
Design choices → governance requirements	Investigating the effects of design choices on management and alienation rights; The effect of combinations of design choices on governance requirements (i.e. encrypted data and BFT); For what governance requirements do we need to develop different architectures, because they cannot be met?
Blockchain control points → design choices	Which are additional control points and design choices? Which are additional effects of the current design choices?

8 Conclusions

This paper presents a novel framework that provides a broad understanding of the link between governance and blockchain design choices. The key elements of this framework are considering various stakeholders and their conflicting and mutual interests in B&G information sharing, governance requirements and blockchain control points. Control points are important, but often not considered in the information system's design, whereas blockchain often is used to improve control and thereby creating trust.

The framework can be used to analyse the effect of design decisions. We demonstrate how technical design choices can trigger organizational dynamics at the stakeholder level and vice versa. The tensions and opposing interests of stakeholders result in blockchain design choices that influence how data is shared and rights can be exercised. The framework draws attention to relevant elements to analyse this interaction. Although requirements like transparency and access control are clear, they can be realized in different ways, which influences design and governance. We demonstrate how they can be accounted for simultaneously when designing blockchain applications.

Our intention is not to present a complete framework. New control points and design choices that affect governance requirements might be found or developed and a lot of research still needs to be performed to get full insight into the relationship between the control points and governance. Rather, we present a framework that links control points and design choices to rights. This also can help to identify gaps in knowledge, for example by looking at what relationships are unknown or what governance requirements stakeholders have that cannot be met with the current design choices. Additionally, embedding new knowledge in the framework systemizes it and helps to translate it

into a form that can be applied directly in B&G information sharing. Evaluation of the framework using empirical cases in other B&G domains is part of future research. This will lead towards the development of a robust conceptual framework that supports the design of blockchain architectures that align the stakeholder interests, the governance requirements and the blockchain control points.

Acknowledgements. This research was partially funded by the PROFILE Project (nr. 786748), which is funded by the European Union's Horizon 2020 research and innovation program. Ideas and opinions expressed by the authors do not necessarily represent those of all partners.

The authors would like to also thank Norbert Kouwenhoven for his contribution to demonstrating the framework in the TradeLens examples.

References

1. Ølnes, S., Ubacht, J., Janssen, M.: Blockchain in government: benefits and implications of distributed ledger technology for information sharing. Gov. Inf. Q. **34**, 355–364 (2017). https://doi.org/10.1016/j.giq.2017.09.007
2. Korpela, K., Hallikas, J., Dahlberg, T.: Digital supply chain transformation toward blockchain integration. In: Proceedings of the 50th Hawaii International Conference on System Sciences, pp. 4182–4191 (2017). https://doi.org/10.24251/HICSS.2017.506
3. van Engelenburg, S.: Designing context-aware architectures for business-to-government information sharing (2019). https://doi.org/10.4233/uuid:d25fd4fd-02d7-4811-b675-615badbb3c05
4. Segers, L., Ubacht, J., Rukanova, B., Tan, Y.H.: The use of a blockchain-based smart import declaration to reduce the need for manual cross-validation by customs authorities. In: ACM International Conference Proceeding Series, pp. 196–203 (2019). https://doi.org/10.1145/3325112.3325264
5. Tian, F.: An agri-food supply chain traceability system for China based on RFID & blockchain technology. In: 13th International Conference on Service Systems and Service Management (ICSSSM), pp. 1–6 (2016). https://doi.org/10.1109/ICSSSM.2016.7538424
6. Lee, H.L., Padmanabhan, V., Whang, S.: Information distortion in a supply chain: the bullwhip effect. Manag. Sci. **43**, 546–558 (1997). https://doi.org/10.1287/mnsc.43.4.546
7. Bray, R.L., Mendelson, H.: Information transmission and the bullwhip effect: an empirical investigation. Manag. Sci. **58**, 860–875 (2012). https://doi.org/10.1287/mnsc.1110.1467
8. Hesketh, D.: Weaknesses in the supply chain: who packed the box. World Cust. J. **4**, 3–20 (2010)
9. Fawcett, S.E., Osterhaus, P., Magnan, G.M., Brau, J.C., McCarter, M.W.: Information sharing and supply chain performance: the role of connectivity and willingness. Supply Chain Manag. Int. J. **12**, 358–368 (2007). https://doi.org/10.1108/13598540710776935
10. Lee, H.L., Whang, S.: Information sharing in a supply chain. Int. J. Manuf. Technol. **1**, 79–93 (2000). https://doi.org/10.1504/IJMTM.2000.001329
11. Hart, P., Saunders, C.: Power and trust: critical factors in the adoption and use of electronic data interchange. Organ. Sci. **8**, 23–42 (1997). https://doi.org/10.1287/orsc.8.1.23
12. Nakamoto, S.: bitcoin: a peer-to-peer electronic cash system (2008)
13. Janssen, M., van der Voort, H.: Adaptive governance: towards a stable, accountable and responsive government. Gov. Inf. Q. **33**, 1–5 (2016). https://doi.org/10.1016/j.giq.2016.02.003
14. Mergel, I., Gong, Y., Bertot, J.: Agile government: systematic literature review and future research. Gov. Inf. Q. **35**, 291–298 (2018). https://doi.org/10.1016/j.giq.2018.04.003

15. Bevir, M.: What is governance? In: Key Concepts in Governance, pp. 2–11. SAGE (2008)
16. Elaluf-Calderwood, S., Eaton, B., Herzhoff, J., Sorensen, C.: Mobile platforms as convergent systems – analysing control points and tussles with emergent socio-technical discourses. In: Maícas, J.P. (ed.) Recent Developments in Mobile Communications: A Multidisciplinary Approach, pp. 97–112 (2011). Books on Demand
17. Rukanova, B., de Reuver, M., Henningsson, S., Nikayin, F., Tan, Y.H.: Emergence of collective digital innovations through the process of control point driven network reconfiguration and reframing: the case of mobile payment. Electron. Mark. (2019). https://doi.org/10.1007/s12525-019-00352-z
18. Tan, Y.-H., Rukanova, B., Engelenburg, S. van, Ubacht, J., Janssen, M.: Developing large scale B2B blockchain architectures for global trade lane. In: 6th Innovation in Information Infrastructures (III) Workshop, University of Surrey (2019)
19. Eckartz, S.M., Hofman, W.J., Van Veenstra, A.F.: A decision model for data sharing. In: Janssen, M., Scholl, H.J., Wimmer, M.A., Bannister, F. (eds.) EGOV 2014. LNCS, vol. 8653, pp. 253–264. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-44426-9_21
20. Constantinides, P.: Perspectives and implications for the development of information infrastructures. IGI Global (2012). https://doi.org/10.4018/978-1-4666-1622-6
21. Ostrom, E.: How types of goods and property rights jointly affect collective action. J. Theor. Polit. **15**, 239–270 (2003). https://doi.org/10.1177/0951692803015003002
22. Lamport, L., Shostak, R., Pease, M.: The byzantine generals problem. ACM Trans. Program. Lang. Syst. **4**, 382–401 (1982). https://doi.org/10.1145/357172.357176
23. Klievink, B., et al.: Enhancing visibility in international supply chains: the data pipeline concept. Int. J. Electron. Gov. Res. **8**, 14–33 (2012). https://doi.org/10.4018/jegr.2012100102
24. Rukanova, B., Henningsson, S., Henriksen, H.Z., Tan, Y.-H.: Digital trade infrastructures: a framework for analysis. Complex Syst. Inform. Model. Q., 1–21 (2018). https://doi.org/10.7250/csimq.2018-14.01