A Blockchain Architecture for Reducing the Bullwhip Effect

Sélinde van Engelenburg(✉), Marijn Janssen, and Bram Klievink

Faculty of Technology, Policy and Management, Delft University of Technology, Jaffalaan 5, Delft, The Netherlands
{S.H.vanEngelenburg, M.F.W.H.A.Janssen, A.J.Klievink}@tudelft.nl

Abstract. Supply chain management is hampered by a lack of information sharing among partners. Information is not shared as organizations in the supply chain do not have direct contact and/or do not want to share competitive and privacy sensitive information. In addition, companies are often part of multiple supply chains and trading partners vary over time. Blockchains are distributed ledgers in which all parties in a network can have access to data under certain conditions. Private blockchains can be used to support parties in making their demand data directly available to all other parties in their supply chain. These parties can use this data to improve their planning and reduce the bullwhip effect. However, the transparency that blockchain technology offers makes it more difficult to protect sensitive data. The dynamics between these properties are not well understood. In this paper, we design and evaluate a blockchain architecture to explore its feasibility for reducing information asymmetry, while at the same time protecting sensitive data. We found that blockchain technology can allow parties to balance their need for inventory management with their need for flexibility for changing partners. However, measures to protect sensitive data lead either to reduced information, or to reduced speed by which the information can be accessed.

Keywords: Blockchain · Blockchain technology · Supply chain management
Information sharing · Information asymmetry · Bullwhip effect
Distributed ledger

1 Introduction

The availability of timely information is crucial for operations in supply chains. If information lags behind the "Bullwhip Effect" (BWE) might occur [1, 2]. The BWE is the effect of the amplification of the demand in the supply chain when there is no good overview of the demand expected in the supply chain. Each node has only information and forecasting based on the demand of the next node, but not an overview of the end-customer demand. The more nodes are between the end-user demand and the supply chain party, the larger the bullwhip effect can be [3]. The final customer demand might be fairly even, but due to the use of batches when ordering, the demand

B. Shishkov (Ed.): BMSD 2018, LNBIP 319, pp. 69–82, 2018.
https://doi.org/10.1007/978-3-319-94214-8_5

fluctuates. This results in having larger stocks than needed, excessive production, non-optimal scheduling of production and large warehouses. The risks of having stock are not only that it needs capital, but stock might also become obsolete.

Numerous studies show that addressing BWE requires better information sharing about the demand between supply chain partners [4]. The BWE effect can be avoided by overcoming information asymmetry in the supply chain. Forecasts are based on the information available. By collaboration and sharing the end-customer demand with all parties in the chain, each party will be able to make a more realistic planning of the use of their capacity and the orders that will be produced [5]. By looking at the end-customer demand, variations of forecasts caused by batch orders can be avoided.

Blockchain was originally conceptualized by Nakamoto [6] to store and share transactions of the cryptocurrency Bitcoin. Blockchain technology could be used to share other data instead of transactions, including the demand data that supply chain parties can use to avoid the BWE. Blockchain technology allows for distributed information sharing without requiring an intermediary. Blockchain technology can thus allow parties in a supply chain to directly share data with parties further downstream in the supply chain and thereby reduce information asymmetry. It is possible to limit the parties that can be part of the network and have reading rights, for instance in a private or consortium blockchain [7, 8]. Additionally, once data is stored in a blockchain, it becomes hard to change it and therefore it can be a trusted way to share information among supply chain partners. This makes blockchain an interesting candidate for supporting information sharing to reduce the BWE.

The straightforward access to data that blockchain technology offers has a downside as well. The demand data can be sensitive as sharing of customer data or demand data might harm the negotiation and competitive positions of companies. Sharing that data with a large number of parties, without protecting it, might harm businesses' interests. This might mean that businesses are not willing to share the data required to reduce the BWE via a blockchain, without a form of access control. One solution is to only include parties in the network that are in a specific supply chain. However, this would mean that if parties decide to change supply chains, they have to change blockchain networks as well. This reduces their flexibility and makes it harder to access the data from the new supply chain.

A balance between data accessibility and data protection is required to support information sharing to reduce data asymmetry in supply chains. Without accessibility, there is no reduction of information asymmetry. Without the protection of sensitive data, it is unlikely that businesses will be willing to share data [9]. However, the dynamics between the transparency offered by blockchain technology and the protection of sensitive data are not well understood. Therefore, it is unclear whether blockchain technology will in fact be feasible for reducing information asymmetry in supply chains. This work provides an initial exploration of these dynamics.

In the next section, we discuss the related work. In Sect. 3, we describe the research approach. In Sect. 4, we establish the requirements for an architecture that supports the sharing of demand data to reduce the BWE based on literature. Establishing these requirements helps to get deeper insight into the needs for data accessibility and data protection. In Sect. 5, we provide a design for a blockchain architecture in which we attempt to balance accessibility with the protection of data. Section 6 provides an

illustration of the architecture. In Sect. 7, we provide an evaluation of the architecture. In this evaluation, we reflect on how well we could balance data accessibility with data protection and what are the difficulties in striking a balance.

2 Related Work

Research on using blockchain technology to store and share other types of data than transaction data is on the rise in a variety of domains. Blockchain is proposed to support different processes in the domains of supply chain management and business process management as well [10–18]. Examples are tracing goods throughout their lifecycle [10, 12], conflict resolution in supply chains [14], crowd lending [15], business-to-government information sharing [11] and supply chain integration [13].

The literature mentions various benefits of blockchain technology. Mentioned particularly often is that blockchain allows for transparency and traceability and thereby provides trust without requiring an intermediary party [10, 12, 13, 16, 18]. Examples of other benefits ascribed to blockchain technology are robustness by decentralization, practical immutability of stored data, anonymity of nodes, and high data integrity [10, 12, 13, 15, 16]. The disadvantages mentioned in literature are the difficulty of changing data once it is stored, scalability issues, privacy and confidentiality issues, the unclear legal status of smart contracts, and wasted resources [12, 14–16].

Access control and protecting sensitive data is a recurrent theme in the related literature on blockchain technology. The proposed blockchain designs often incorporate some form of access control. Usually this involves encryption to protect sensitive data or making the blockchain network private (see e.g., [10, 11, 13, 14, 16]). However, rarely, an analysis is made of the impact of the chosen form of access control on the perceived benefits of using blockchain technology. Yet, such impact is likely, especially as data protection is at odds with the transparency offered by blockchain technology. Insight into the dynamics between solutions for protecting sensitive data and data accessibility is required to establish whether blockchain technology can provide a balance that is suitable for a proposed application.

3 Research Approach

Blockchain technology relies on distributed ledgers, encryption, Merkle tree hashing and consensus protocols [19]. While these technologies themselves are not new, their specific combination in blockchain technology is. As discussed in the previous section, due to the novelty of blockchain technology, there is no existing knowledge on the dynamics between solutions for protecting sensitive data and data accessibility that we could use as a starting point for our investigations. Therefore, this work is of an explorative nature.

In this work, we design a blockchain architecture for the sharing of demand data in supply chains to support the reduction of the BWE. We focus on balancing access control with data accessibility in our design. The tensions between the need for access

control and data accessibility are especially important in this domain, as on the one hand the demand data is sensitive. On the other hand, however, to make reduction of the BWE possible, high data accessibility is required.

As there is a clear tension between requirements for access control and data accessibility when sharing demand data in supply chains, it is interesting to look at the extent to which they can be met in a design based on blockchain technology. More specifically, the difficulties we come across when making design decisions and the extent to which we are able to strike a balance can provide an initial insight into the dynamics that play a role. For the evaluation of the architecture, we thus focus on the considerations taken into account in the design decisions and the extent to which we are able to provide the appropriate level of access control and transparency.

4 Requirements

The architecture for supporting information sharing to reduce the BWE, should ensure the accessibility of demand data and at the same time protect sensitive data. The demand data needs to be accessible, as this accessibility reduces information asymmetry. Protecting sensitive data is necessary, as businesses otherwise might not be willing to share [9]. To determine what the requirements are for reaching this objective, it needs to be known what type of information needs to be shared. Additionally, we need to know what data is sensitive to businesses and how it should be protected.

Requirement 1 for the architecture is that it should support the sharing of inventory levels, work in progress levels, order data and demand data. The BWE is prevalent in traditional supply chains in which parties can base their forecasts only on purchase orders from the previous party in the supply chain [5, 20, 21]. Various studies show that the BWE is reduced when additional information is shared [5, 21, 22]. Sharing market demand data reduces the BWE [5]. The BWE can be further mitigated when inventory levels and work in progress levels are shared as well [5]. This should be done in such a way that information asymmetry is diminished and that all parties in the supply chain can base their forecasts on the same data.

Requirement 2 is that demand data and inventory and work in progress levels should only be accessible to parties in the same supply chain and identities should be anonymized where possible. Demand data can be sensitive. First of all, the identity of parties (like customer names) can be sensitive when information is shared vertically, i.e., with other parties in the same supply chain upstream or downstream. A party that shares data about the identity of their buyer might be bypassed in the supply chain when their producer starts selling directly to their buyer [23, 24].

In addition, information can be shared horizontally, i.e. with parties at the same level in the same supply chain or with other supply chains. Many companies operate in multiple supply chains which complicates information sharing. Other businesses might be competitors that could use this data to their advantage or be used by others to approach customers.

Finally, because of competition law not all information can be shared as this might result in cartel formation. For instance, a business could have a strategy for dealing

with their inventory that reduces costs. This might provide them with a competitive advantage. If another business has their inventory levels, they could learn from this, causing the competitive advantage to be reduced or lost. In addition, while it is beneficial for a business to share data to reduce the BWE vertically, there is no clear benefit of sharing it horizontally. Considering the risks, this should thus be avoided.

5 A Blockchain Architecture for Reducing the Bullwhip Effect

In this section, we present a blockchain architecture for diminishing the bullwhip effect. We focus on balancing the requirements in the previous section. We illustrate and evaluate the architecture in subsequent sections.

A blockchain is a distributed ledger in which data is stored in a series of blocks. Nodes in a blockchain network each have a copy of the blockchain [6]. New data that is added to the blockchain is distributed throughout the network [6]. It is then collected into blocks and added to the blockchain by linking the new block to the last block in the chain [6]. Parties in the network can accept the new block according to a consensus mechanism [6]. They express acceptance by adding new blocks on top [6].

The overall architecture presented here consists of several elements: (1) a blockchain network consisting of nodes operated by supply chain members, (2) a data architecture for the format of data in the blockchain, (3) a data sharing architecture for the sharing of data among supply chain partners, and (4) a data access architecture for providing supply chain partners access to certain data.

5.1 The Blockchain Network

The right to read, write or contribute to consensus of nodes can be restricted. The difference between open, consortium and private blockchains is that respectively everybody, a limited set of parties or one centralized organization can control the consensus process and write new data to the blockchain [7]. For all types, it is possible to have public reading rights [7]. However, for private blockchains, it is also a possibility to restrict who can be a node and read the data and thus make the reading rights private [7].

For our design, we are concerned with data accessibility and data protection. In other words, with who can read what data. As a simplification, consortium and private blockchains are sometimes both called “private” (see e.g., [7]). Since our main concern is who has reading rights, and not who controls the consensus process, we will use the term private for our blockchain in this sense as well.

In our design, we will limit what parties can be a node and have reading rights to the data in the blockchain. As we will further discuss in the evaluation, limiting access to the network to parties in a supply chain might be too restrictive. Therefore, in the design, businesses in a certain industry can be part of the network for that industry.

5.2 Data Architecture

In a blockchain, each block consists of a header and a body [6]. In the body, the actual data is stored. The header contains a Merkle root that is unique to the data that is stored in the body [6]. This means that if the data in the body is (maliciously) changed, the Merkle root does not match the data in the body anymore. Furthermore, the header contains a unique hash of the header of the previous block in the chain [6]. Thus, if the header of the previous block is changed, the hash of the header in the next block does not match anymore. Consequently, changing data that is stored in a block requires its header and the header of all subsequent blocks to be changed to avoid detection. This makes it harder to modify data that is stored in a blockchain.

In the case of our design, the data that should be in the body of the block is order data, market demand data, data on the inventory level and on the work in progress level of businesses. These types of data are different, as orders can be viewed as an interaction between businesses. Conversely, inventory and work in progress levels signify internal statuses of businesses.

To store an order in a block, at least the following data elements are required: (1) ID of the retailer, (2) ID of the supplier, (3) type of goods that are ordered, (4) the quantity of goods that are ordered, (5) the date at which the goods will be delivered, and (6) a unique order number. Purchases could be arranged in long-term contracts as well. Such a contract can be stored in a similar manner as a simple order, with added data elements with information from the contract that is relevant for forecasting, such as agreements on repetitive orders. Furthermore, the date that is stored for a contract will signify the end of the contract instead of the date of delivery.

To improve the reliability of the data both businesses can sign the order or contract with their private key. Just as in the case of the wallet of users in Bitcoin, the ID of the businesses can be used as a corresponding public key. Other parties can check whether the parties have indeed signed the agreement using this public key as part of the consensus mechanism (see Sect. 5.3).

Not all data in a purchase order or contract is required to be added as data elements for businesses to base their forecasts on. For instance, data on pricing does not seem to provide an additional benefit for reducing the BWE and is highly sensitive. Hence, such data should not be stored in the blockchain. However, businesses could benefit from storing a proof of existence of the full purchase order and contract in the blockchain. For such proof of existence, merely a unique hash of the document is stored and signed by parties and not the document itself. This can provide businesses with a proof of what was agreed upon, which might improve trust. This benefit could incite businesses to add their orders and contracts at an early stage, which allows other parties to have the data at an earlier stage and to start forecasting earlier in the process.

The inventory levels and work in progress levels can be added to the blockchain as well. For this, at least the following data elements need to be added: (1) ID of the business, and (2) inventory or work in progress level. The party that adds the data can sign it to signify that they added the data themselves.

The data that parties add to the blockchain can be encrypted, with the exception of the ID's of parties and the end-dates of contracts. The latter data elements are necessary to determine who is in what supply chain. This, in turn, is needed to determine what

data is relevant to parties and whether they should have access. While not being encrypted, it is not necessary to link the actual businesses to an ID.

5.3 Data Sharing Architecture

Nakamoto [6] describes 6 steps for running a blockchain network. Some of these can be left out when other data than transactions are shared. Most notably, the steps necessary to provide proof of work might not be required [11].

Based on this, the sharing of data via the blockchain can be as follows:

1. A party collects data on orders, contracts and inventory and work in progress levels.
2. The party encrypts all data elements, except for their own ID's and the dates of the end of contracts.
3. The party and other parties involved sign the data.
4. The data is distributed throughout the network.
5. A node adds the data to a block and they add the block to the chain.
6. The new block is distributed throughout the network.
7. Parties check whether the data is actually signed by the appropriate parties using their ID's (public key).
8. If they accept the data, they add a new block on top.

5.4 Data Access Architecture

As data is encrypted in the design, the appropriate parties need to be able to decrypt it in order to access it. To obtain a key, a party has to request it from a key distribution component. This request should contain the ID of the party that shared the data via the blockchain and specify what data access is requested to. The key distribution component will determine whether the data requested is from a party downstream the goods flow of the party requesting the key in the same supply chain. Only if this is the case, it will provide a key. Data access is thus flexible and depends on the context of what parties are in a supply chain with each other at a certain moment.

Who is in the same supply chain depends on the contracts between parties. The current supply chain a business is in can be viewed as a chain of businesses that have contracts with each other that have not ended yet. All data to determine this is available without encryption, viz, the ID's of parties and the end dates in the contracts. The key distribution component should thus have its own copy of the ledger.

Figure 1 provides an example of businesses in an industry that are connected via contracts that have not ended yet. In this example, all businesses, except for retailer A2, are in the supply chain of business D. A2 is not in their supply chain, as there is no path of contracts from D to A2. This means that D can get access to data from all parties, except for A2. For instance, business B1 is downstream in the same supply chain of C1 and thus C1 can have access to data from B1. Businesses C2 and C3 are in the same supply chain, but not downstream from each other.

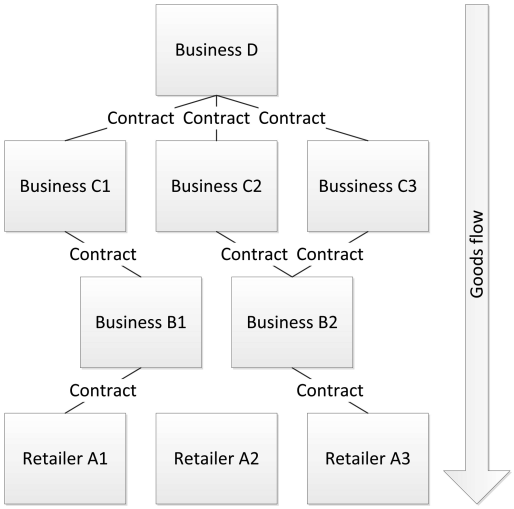

Fig. 1. Businesses in an industry connected via (still in force) contracts in supply chains

To determine who is in a supply chain downstream of a certain business, the key distribution component can do the following:

1. Determine the ID of the business.
2. Search the blockchain for contracts that have not ended yet where the business with this ID is the supplier.
3. List the IDs of the businesses that are purchasing goods in these contracts. These parties are in the supply chain.
4. Determine what parties are in the supply chain of the purchasers (induction).
5. Continue until you arrive at a set of businesses that do not have contracts.

6 Illustration

For the illustration, we consider a scenario with a typical user activity. In this scenario, business A manufactures cars. They use an audio system in their cars produced by business B. Business A has closed a contract with business B in which they agree to buy the audio systems from business B for a certain price. Business C is a retailer that actually sells the cars to consumers. They are in a contract with business A. Each of these parties is a node in the blockchain network via which they share data, as described in Sect. 5.1.

For the illustration we assume that the data about the contracts is already stored in the blockchain by business A. An activity diagram for the scenario is shown in Fig. 2. The storing of the contract by business A is left out here as well to improve clarity.

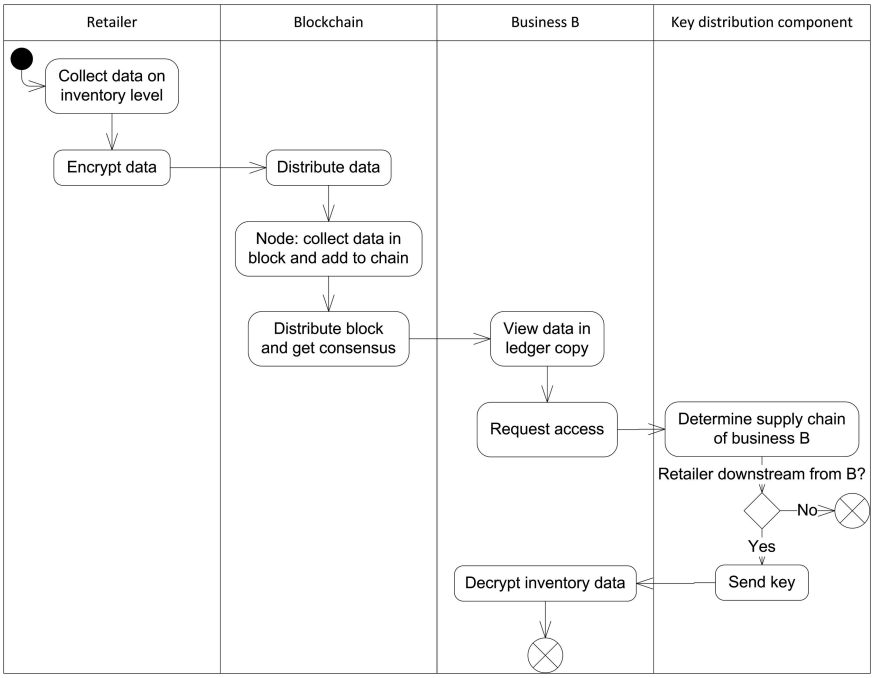

Fig. 2. UML activity diagram for the blockchain architecture

In the scenario, the retailer first collects new data about their inventory level and put it in the format described in Sect. 5.2. They then encrypt the data and sign it with their signature. Subsequently, they insert the data to the blockchain together with their ID. The inventory level data is then distributed throughout the blockchain network and shared via the steps provided in Sect. 5.3.

Business B receives the data in a new block in their copy of the blockchain. They want access to this data and they request access from the decision control component. The decision control component then tries to decide whether the retailer is in the supply chain downstream from business B according to the steps provided in Sect. 5.4. The retailer is indeed downstream in the supply chain from B. As the contracts are stored in the blockchain, the key distribution component can establish this. Then, the key distribution component provides a key to business B for decrypting the data on the inventory level. Business B can use the data to determine their inventory strategy.

7 Evaluation

In Sect. 4, we established two requirements for the architecture, (1) it should support the sharing of inventory levels, work in progress levels, order data and demand data such that all parties in the supply chain base their forecasts on the same data, and (2) that demand data and inventory and work in progress levels should only be

accessible to parties in the same supply chain and identities should be anonymized where possible. Here we discuss the extent to which we were able to meet each of the requirements, and more importantly, what are the difficulties in balancing them. Based on this analysis, we derive what are the dynamics between data accessibility and data protection when using blockchain technology to reduce the BWE.

In the design, parties have access to the data that they require to reduce the bullwhip effect. Demand data, inventory levels and work in progress levels can be accessed via the blockchain from parties downstream. These are exactly the parties that the data should be obtained from. When a party downstream the supply chain adds new data, all parties upstream have the same level of access to it, regardless of the number of parties that are in between. This is a clear advantage of using a blockchain.

In addition, when parties enter into a new contract with businesses, they can add the contract to the blockchain. Based on this, they can determine who is downstream in their supply chain in the same way as the key distribution component does. This allows them to determine what data is relevant to them. In addition, as the end dates of contracts are stored in the blockchain, parties can determine when others leave their supply chain. Data from these parties is no longer relevant. The ability to determine what data is relevant, further improves accessibility. In this way the context is taken into account.

By sharing their data via the blockchain, parties know that it can be accessed by all parties upstream in their supply chain. This means that parties do not have to make information sharing arrangements with individual parties. This makes accessing the appropriate data easier as well.

There thus is an advantage to storing data about contracts in the blockchain. Another advantage of blockchain technology is that everybody can have equal access to the data necessary to establish what parties are in a contract, namely their IDs and the end date of the contract. In the architecture, the consensus mechanism is based on checking whether parties have signed the data. Once data is accepted, it is hard to change. This property might provide an incentive to store the contract information, possibly together with a signed proof of existence of the full contract. Namely, storage in the blockchain could provide businesses with a certain amount of proof that they are in fact in an agreement with another business. So, not only is it beneficial to store contract information in the blockchain to improve accessibility, the blockchain technology also provides an incentive to do so.

Thus, access is provided to the data required to diminish the BWE. However, the data is encrypted and a key should be obtained. This reduces the speed and ease with which the data can be accessed.

Parties downstream can choose not to get into long term contracts with others, but to only work with single orders or switch contracts often. In this way, they might block access to data from parties downstream. This might mean that parties that want to share the data and benefit from the data sharing cannot do so, due to this other party. This might impact the relationships between businesses. They depend on each other to make their data available and to benefit from sharing. Businesses could deal with this by looking at the duration of contracts in the supply chain of a business that they are considering getting into a contract with and taking this into account in their decision.

The easiest way to ensure that only parties in the same supply chain can access data, is by only allowing members of the same supply chain to be part of the blockchain network. However, if a party wants to change supply chains, this would mean that they need to change blockchains as well. Having to change from information sharing system can have a quite negative impact on accessibility of data as well.

On the other hand, purchasing flexibility is viewed by some businesses as part of their competition strategy and can be a reason that they still are involved in a traditional supply chain, despite the risk of BWE [20]. As such, supply chain partners change as old parties might disappear and new ones might enter the supply chain. A solution allowing for more flexibility is the one in the architecture, namely making the blockchain only available to parties in the same industry. This allows them to change supply chains, without having to change the system that they use to share data.

In the architecture, confidentiality is guarded by encrypting the data and only allowing parties downstream in the same supply chain access. These are exactly the only parties that should have access to protect the sensitive data according to requirement 2. The extent to which an appropriate level of protection is offered thus depends on the security of the key distribution component and the quality of the encryption.

In Sect. 4, we discussed that identities of businesses should be protected, to prohibit parties to be bypassed in the supply chain or to know each other's trading partners and agreements. In the design, businesses will know the ID of other businesses that they are in direct contact with, but they do not need to know who is behind the ID's of the other parties in their supply chain, or even the blockchain. To a certain extent, it might be possible to derive this from looking at the number of purchase orders, or contracts that certain IDs have with each other. This issue will be bigger when it is, for instance, known that there are only a couple of parties that make certain product in an industry. Conversely, when there is a high number of small businesses involved, it is much harder to determine what party is behind a certain ID.

In addition, if businesses frequently change their ID, accessing data for other parties becomes limited, or even impossible. The IDs are necessary to establish in what supply chains businesses are and thus what data is relevant to them and what data they should have access to. When a party changes ID, it cannot be established in what supply chain they are and their data cannot be accessed. For instance, when a party uses different IDs for a contract and for data on their inventory level, they make the data on the inventory level inaccessible for the party that they are in a contract with, as now it is not possible to establish that they are in the same supply chain. We thus cannot fully protect the identities of the parties in the supply chains without severely reducing accessibility.

In the end, there is not a single party that controls access to the data, but the access is controlled by all parties downstream in the goods flow from the party that wants access. A party can provide parties upstream with access by adding the data and their contracts. However, they might not know who the parties upstream are exactly and they cannot provide one party upstream with access, while not the other. This means that they need to trust businesses that they do not know to keep their data confidential.

8 Conclusions and Suggestions for Further Research

In this paper, we investigated the feasibility of blockchain technology for reducing the BWE. In an exploratory effort, we focused on balancing data accessibility with data protection. We first established the requirements for a blockchain architecture for reducing the BWE. We then used the design and evaluation of a blockchain architecture for reducing the BWE as an analytical tool to obtain the required insight.

We found that information sharing using a blockchain has some clear advantages when it comes to providing businesses with access to data. First of all, as data sharing is distributed, parties in a supply chain can have equal access to data from other parties, even when they are further downstream. Blockchain also allows for storing contract data that parties can use to establish what data is relevant to them, without intermediacy of others. There is a clear incentive for parties to store these contracts in a blockchain as well.

Blockchain thus can offer high transparency. However, in the supply chain management domain, it is of paramount importance to only provide access to data to the appropriate parties. We were unable to find a design in which all sensitive data was fully protected, in particular the IDs of the businesses. The reason for this is that the IDs are necessary to identify the data that is relevant to businesses and to arrange access control. Further research could focus on finding other strategies that do not require sharing the IDs of the businesses. In addition, the level of protection of the other sensitive data depends on the quality of the encryption used.

If businesses' data is not adequately protected, they could respond with strategies that reduce data accessibility, e.g., not sharing certain sensitive data at all or frequently changing IDs. In addition, protecting sensitive data requires that parties perform additional steps to get access. This reduces the speed by which data can be accessed.

The fundamental conflict between data accessibility and data protection seems to be magnified when using blockchain technology. To reduce information asymmetry and to benefit from the improved reliability everybody in a network should have equal access to data. Equal access for all parties is in direct conflict with providing different parties in the network with different levels of access. Currently, the way to solve this seems to be by either sharing some additional data not via the blockchain, such as keys or the actual contracts, or by making it only include parties that can have the same level of access. Both possibilities reduce data accessibility. Furthermore, both solutions require additional 1-on-1 connections outside of the blockchain or a third party intermediating after all to distribute keys or establish identities of parties. This could result in the usual disadvantages of intermediation and having various 1-on-1 connections that blockchain seems to avoid at first sight.

Further research is necessary to determine whether there are other solutions that do not harm data accessibility in this way and that avoid relying on additional connections and relying on third parties. In addition, further study is needed to determine what balance between data accessibility and data protection are acceptable to businesses. Additional practical insight might be gained as well by evaluating the architectures in practice.

References

1. Lee, H.L., Padmanabhan, V., Whang, S.: Information distortion in a supply chain: the bullwhip effect. Manag. Sci. **43**, 546–558 (1997)
2. Lee, H.L., Padmanabhan, V., Whang, S.: The bullwhip effect in supply chains. Sloan Manag. Rev. **38**, 93–102 (1997)
3. Fiala, P.: Information sharing in supply chains. Omega **33**, 419–423 (2005)
4. Bray, R.L., Mendelson, H.: Information transmission and the bullwhip effect: an empirical investigation. Manag. Sci. **58**, 860–875 (2012)
5. Cannella, S., Ciancimino, E.: On the bullwhip avoidance phase: supply chain collaboration and order smoothing. Int. J. Prod. Res. **48**, 6739–6776 (2010)
6. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008). https://bitcoin.org/bitcoin.pdf
7. Buterin, V.: On public and private blockchains. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
8. Pilkington, M.: Blockchain technology: principles and applications. In: Olleros, F.X., Zhegu, M. (eds.) Research Handbook on Digital Transformations, pp. 227–253. Edward Elgar Publishing, Cheltenham (2016)
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)
10. Abeyratne, S.: Blockchain ready manufacturing supply chain using distributed ledger. Int. J. Res. Eng. Technol. **5**, 1–10 (2016)
11. van Engelenburg, S., Janssen, M., Klievink, B.: Design of a software architecture supporting business-to-government information sharing to improve public safety and security. J. Intell. Inf. Syst. (2017)
12. Tian, F.: An agri-food supply chain traceability system for china based on RFID & blockchain technology. In: 2016 13th International Conference Service System and Service Management, pp. 1–6 (2016)
13. 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)
14. Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., Mendling, J.: Untrusted business process monitoring and execution using blockchain. In: La Rosa, M., Loos, P., Pastor, O. (eds.) BPM 2016. LNCS, vol. 9850, pp. 329–347. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-45348-4_19
15. Schweizer, A., Schlatt, V., Urbach, N., Fridgen, G.: Unchaining social businesses - blockchain as the basic technology of a crowdlending platform. In: 38th International Conference Information System, pp. 1–21 (2017)
16. Mendling, J., Weber, I., van der Aalst, W., vom Brocke, J., Cabanillas, C., Daniel, F., Debois, S., Di Ciccio, C., Dumas, M., Dustdar, S., Gal, A., Garcia-Banuelos, L., Governatori, G., Hull, R., La Rosa, M., Leopold, H., Leymann, F., Recker, J., Reichert, M., Reijers, H.A., Rinderle-Ma, S., Rogge-Solti, A., Rosemann, M., Schulte, S., Singh, M.P., Slaats, T., Staples, M., Weber, B., Weidlich, M., Weske, M., Xu, X., Zhu, L.: Blockchains for business process management - challenges and opportunities. arXiv:1704.03610, vol. 9, pp. 1–16 (2017)
17. López-Pintado, O., García-Bañuelos, L., Dumas, M., Weber, I.: Caterpillar: a blockchain-based business process management system. In: CEUR Workshop Proceedings, vol. 1920, pp. 1–5 (2017)

18. van der Aalst, W.M.P., De Masellis, R., Di Francescomarino, C., Ghidini, C.: Learning hybrid process models from events: process discovery without faking confidence. In: International Conference on Business Process Management (2017)
19. Tasca, P., Tessone, C.J.: Taxonomy of blockchain technologies. Principles of identification and classification. arXiv Preprint arXiv:1708.04872
20. Matthias, H., Stephen, D., Jan, H., Johanna, S.: Supply chain collaboration: making sense of the strategy continuum. Eur. Manag. J. **23**, 170–181 (2005)
21. Dejonckheere, J., Disney, S.M., Lambrecht, M.R., Towill, D.R.: The impact of information enrichment on the bullwhip effect in supply chains: a control engineering perspective. Eur. J. Oper. Res. **153**, 727–750 (2003)
22. Chatfield, D.C., Kim, J.G., Harrison, T.P., Hayya, J.C.: The bullwhip effect-impact of stochastic lead time, information quality, and information sharing: a simulation study. Prod. Oper. Manag. **13**, 340–353 (2004)
23. Klievink, B., van Stijn, E., Hesketh, D., Aldewereld, H., Overbeek, S., Heijmann, F., Tan, Y.-H.: Enhancing visibility in international supply chains: the data pipeline concept. Int. J. Electron. Gov. Res. **8**, 14–33 (2012)
24. van Stijn, E., Hesketh, D., Tan, Y.-H., Klievink, B., Overbeek, S., Heijmann, F., Pikart, M., Butterly, T.: The data pipeline. In: Global Trade Facilitation Conference 2011, pp. 27–32 (2011)