Blockchain usability within supply chains

Blockchain usability within supply chains

Novelty solutions and consumer benefits?

Abstract

Blockchains receive a lot of attention these days. However, whereas conceptual models and proof-of-concepts are reasonably obtainable, real-world implementations are scarce. This is no different in the field of supply chains. This research takes a theoretical and practical (qualitative) approach to find out what the usability of blockchain technology is, what experts and practitioners expect from it, what hurdles are to overcome and what the possibilities for end-consumers are; all this specifically within supply chains. We find that most setups divert far from the original blockchain concept, and thus also from its potential strengths and drawbacks. Our interviewees are expecting (data) integration, possibly in solutions spanning a whole industry. In terms of hindrances, the technological maturity, its case specificity and a lack of examples come forward as main reasons.

keywords: blockchain, supply chain, trust, data integration, provenance

1 Introduction

Thanks to globalization and global outsourcing, contemporary supply chains consist of many members who are geographically dispersed; this leads to highly complex and opaque supply chains. Supplier mistakes, unethical behavior or fraud, require fast and reliable determination of the origins of products. Not only is this valuable information for all supply chain members, also end-consumers are (just as much as regulators) interested in the quality, origins (e.g. biological products) and safety of their food and products.

Many believe that blockchain technology, of which Bitcoin and Ethereum are the most famous ones, could be the key to support further B2B integration in a cost-effective and flexible way (Korpela, Hallikas, & Dahlberg, 2017), and has as main advantages its durability, transparency, immutability and process integrity (Abeyratne & Monfared, 2016).

However, decentralized, rather slow, fully transparent and pseudonymous networks are arguably not what organizations search for neither. IT providers have come up with workarounds for these issues, but these tend to divert far from the original philosophy and strengths of the blockchain (Peterson, Deeduvanu, Kanjamala, & Boles, 2016). The corporate implementation we tend to evolve towards, raises the question whether blockchain is a real technological solution for existing problems, more than just a 'new, trendy package'. If blockchain is indeed the long-awaited game changer within the supply chain domain, in whatever hybrid implemented form, then we need to understand the underlying reasons for managers and technicians to adopt this technology.

As such, the generalized problem statement of this work becomes:

Blockchain usability within supply chains: What novelty solutions are being sought after and how can end-consumers benefit?

More in detail, we will be researching (1) what insights or visibility into the supply chain do partners want today but cannot get, (2) what are typical applications of blockchain in current practice, (3) whether these motives benefit substantially from blockchain as a technology (and/or how they should) and (4) how the end-consumer can benefit from the blockchain evolution.

1.1 Research method

For a good understanding, this research will first of all introduce some concepts, and clarify some assumptions. Hereafter, we will be looking at the theoretical usability of blockchains by conducting a literature review. For the practical grounding, we will be conducting semi-structured interviews with experts, (supply chain) managers and consultants.

Capturing a multitude of implementations spanning different industries, future-oriented concepts, visions and extensions (such as end-consumer benefits) will require the use of interactive interviews and case studies, in a qualitative research setup. Especially in this case, the outcome of the research strategy will be less biased by the investigators' preconceptions, as constrained questions in a survey might favor a specific outcome, based on the approach and deduction made (Eisenhardt, 1989).

1.2 A chain of blocks

A block in a blockchain essentially consists of a reference (a hash) to its previous block and a number of transactions or state changes. The fact that each block contains a reference to its predecessor, makes it representing a 'chain of blocks' or a *blockchain* (Figure 1).

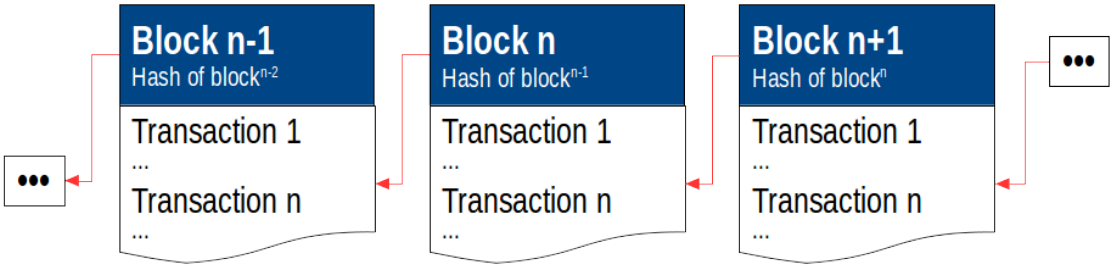

Figure 1: Graphical representation of a blockchain

The hash of a block is a hash of the block in its *completeness*. Therefore, if anyone (later on) would alter the data within any block in the chain, its hash would change, breaking the (block)chain. This should make it difficult to tamper with any data in a blockchain, once it is (officially) recorded. A *consensus algorithm* exists, whereby multiple blockchain nodes agree on whether a block and its contents is valid and allowed to be included in the chain. As long as an honest majority (typically) exists, by consensus about validity, fraudulent participants are prevented to add a self-constructed (counterfeit) block.

1.3 Smart contracts

In a blockchain context, smart contracts represent a piece of software, a set of 'logic' written in a computer programming language. The smart contract itself and its execution state

(such as the content of variables) are stored onto the blockchain, and it is executed by the network, upon invocation. If the network is immutable, then the logic of a certain contract cannot be altered anymore; its state can only be changed by executing the contract, using well-defined, known in advance (programmatic) rules.

1.4 Blockchain types

In the literature, one will encounter different types of blockchain being mentioned, carrying varying and overlapping names. Researchers rarely make their interpretation explicit, and tend to use it 'as most convenient'. For transparency, we firstly want to clarify our assumptions. Throughout this work we will consistently use these naming conventions and their associated definitions.

- **Public blockchains**
  A fully public and possibly transparent network, where nodes can freely join and cooperate in the consensus reaching process. This typically involves an incentive, a compensation in the form of a cryptocurrency, for partaking.
- **Consortium blockchains**
  Nodes in the network are mainly or exclusively hosted by the participants. Eventually, (although seemingly uncommon) external nodes may join, but not participate in the consensus (for risk of 51% attacks). Typically no reward is foreseen.
- **Private blockchains**
  The network is fully shielded (private), and typically hosted by a single provider that is paid for the service offering. Sometimes, the network is distributed (like in a cloud solution).

Note that a node is not necessarily a participant, and a participant is generally not obliged to be a node. In a public setup, nodes are frequently as well called *miners*.

Blockchains are frequently as well called *permissioned*, eventually as an alias of one of the above types. However, being permissioned, the fact of requiring some authorization to *participate* in the blockchain, is clearly a property (not a type): permissioning is imaginable for any of the three blockchain types. Hence as well our explicit distinction between a node and a participant.

2 Literature review

2.1 Bitcoin

An important accomplishment of the Bitcoin whitepaper (Nakamoto, 2008) is that it solves the 'double-spending' problem without a "centralized trustworthy arbitrator or third party" (Cong & He, 2018). The absence of such *centralized, trusted party* allows for low transaction fees, no charge-backs (Bamert, Decker, Elsen, Wattenhofer, & Welten, 2013), fast settlement (Dilley et al., 2016) and is by design censorship-free (Simser, 2015).

Bitcoin solves the dependence upon a centralized and trusted third party by broadcasting all transactions on the peer-to-peer network, where they are processed by (virtually all) nodes. Miners reach *decentralized consensus* by performing Proof-of-Work; the miner who is the first to find a new block, is rewarded (Cong & He, 2018; Bonneau et al., 2015).

Bitcoin users are identified by a hash of their public key: (Bit)coin ownership essentially

means knowing the private key that can redeem them (Bonneau et al., 2015). Any user can own as many key pairs as deemed necessary (typically kept in wallets); because these are not immediately linkable to a real-world identity, users are said to be *pseudonymous* (i.a. Decker & Wattenhofer, 2013).

However, since the Bitcoin network is fully transparent, clustering (Meiklejohn et al., 2013) and traffic analysis (Koshy, Koshy, & McDaniel, 2014) are possible. This transparency is required for Bitcoin to function, allowing for public verification, block validation and inspection (i.a. Yli-Huumo, Ko, Choi, Park, & Smolander, 2016).

2.2 The purpose of cryptocurrencies

Bitcoin and many of its alternatives have (currently) no other purpose than representing and transferring *virtual money*, thus being a simple *cryptocurrency*. Indeed, Bitcoin's scripting language is severely limited to some arithmetic, logical and cryptographic functions (Cong & He, 2018). Extensions have been suggested, such as "Colored coins" (Rosenfeld, 2012), or "Pegged sidechains" (Back et al., 2014).

While cryptocurrencies will help in providing an understanding of the global concepts, this research will focus on blockchain setups that offer more flexibility (like smart contracts with a generic programming language), and may be used in supply chain contexts.

The best known alternative to date was presented by Vitalik Buterin and is called *Ethereum* (Buterin, 2014). Ethereum offers Turing complete (Turing, 1937) *smart contracts* (Hirai, 2017). Now, arbitrarily complex code can be executed on a decentralized platform, and blocks are generated every 12 seconds instead of 10 minutes in Bitcoin (greatly improving transaction speed) (Kiayias & Panagiotakos, 2015).

2.3 Blockchain advantages

2.3.1 Decentralized

While most blockchain authors refer to *decentralized* as being advantageous, few make explicit why this is the case. In the case of blockchains, decentralization's convenience will be mostly the absence of a Single Point of Failure and the fact that the network is not *controlled* by any single party (or only a few). In contrast, centralization typically has advantages of efficiency (less overhead, scale effects, ease of control). Likewise, there is ease of coordination, communication and consensus (Atzori, 2015).

2.3.2 Trustless

Trust is commonly mandatory when some kind of agreement ('consensus') needs to be reached between participants; a common and straightforward solution is then to use a *trusted, central authority* to do the intermediation, regularly based on reputation. In a trustless blockchain environment, any node may join the network and none can be trusted upfront. However, as long as an honest majority exists, the entire network can be considered safe. A system that reaches agreement despite faulty components is a solution to the *The Byzantine Generals Problem* (Lamport, Shostak, & Pease, 1982).

2.3.3 Immutable

Immutability comes with a number of different names, such as being 'tamper-proof' or having 'data integrity'. The immutability in blockchains comes from the fact that blocks refer to their predecessors. If an attacker would attempt to modify or remove a certain block,

that will change its hash or break the chain (respectively), making this change detectable by looking at subsequent blocks (Fanning & Centers, 2016).

2.3.4 Auditable

Being auditable in terms of blockchain, means that it is possible for a legitimate party to verify its correctness (Xu et al., 2016). Transparency is generally considered to be public auditability, where anyone can verify all blocks (and transactions), such as in Bitcoin (Dilley et al., 2016). The property of being auditable is a strong enabler of (public) trust, and essential for the immutability claim: without a possibility to check the correctness, one could still change the blockchain or double-spend value while remaining undetected.

This fundamental auditability (transparency) makes blockchains ideal candidates to track goods and steps throughout (complex) supply chains (Manski, 2017). This might not only be beneficial for supply chain members, but as well for end-consumers: they could now be enabled to verify the history of a product found in the supermarket or a shop. This is generally referred to as *provenance*. This leads us to formulate our first proposition:

> **P1**: End-consumers are not immediately targeted within supply chain blockchain applications, but would be interested in a convenient way to track reliable information about the components/origins concerning the product of their interest.

2.4 A cooperative platform

Blockchain is first of all a *distributed, shared ledger* with some important added conveniences as described earlier. Given the importance of information sharing (and product tracking), such common platform might be a solution supply chains are looking for; this brings us to suggest a second proposition:

> **P2**: Supply chain members are looking for a global, integrated and transparent overview of information coming from all involved chain partners.

2.5 Long(er)-term blockchain issues

2.5.1 Scalability

Scalability refers to the behavior and performance of the network over time, especially in the case of increased volumes. One component of scalability is latency and throughput (which are inversely proportional). Blockchains typically perform significantly less than centralized systems, because of the overhead and latency introduced by the consensus process (Xu et al., 2016). Another limiting parameter is blockchain's storage requirements. One of the basic assumptions of blockchains is that blocks are never removed, let alone old data ever being purged or cleaned. Obviously, over time, any blockchain will only grow by appending blocks (containing transactions or state transitions).

2.5.2 Data privacy

We discusses earlier how the vast majority of contemporary public blockchains requires information to be stored transparently, for auditability purposes. This lack of privacy is a major hindrance in the broad acceptance of decentralized smart contracts (Kosba, Miller, Shi, Wen, & Papamanthou, 2016). One can easily imagine that it is difficult to accept for organizations or individuals that their (financial) transactions, contracts, stock levels,... are fully disclosed, online available. We noted earlier that the naive acceptance of being pseudonymous, is insufficient.

2.5.3 Governance

Contrary to the fact that blockchains such as Bitcoin are broadly accepted to be fully decentralized, some observations show that they are increasingly drifting towards some forms of centralization. This is for example the case when miners organize themselves in mining *pools*, where eventually only a few big pools remain as miner consortia (Gervais, Karame, Capkun, & Capkun, 2014). Another concern is that governance decisions are taken by a limited amount of developers, outvoting the majority of computational power, and thus without acquiring broad network consensus (Gervais et al., 2014). The lead developers have become the *de facto* governance body (Kroll, Davey, & Felten, 2013).

2.5.4 Price volatility

The execution of smart contracts or transactions requires a fee to be paid to the miners (i.a. Kroll et al., 2013). Since this fee is paid in the related cryptocurrency, large fluctuations in their intrinsic value make it difficult to foresee the cost of execution. Dwyer (2015) looked at the economics of Bitcoin and similar private digital currencies, and found the price (for at least some time) to be much more volatile than gold.

At the current price level (around 500 USD), storing only 1MiB in Ethereum costs around 16.000 USD[1] (about 14.000 EUR).

2.6 Towards better blockchains

As can easily be understood, a platform that lacks data privacy and has difficulties to scale (among others), makes its use difficult in a business environment (i.a. Zyskind, Nathan, & Pentland, 2015). Giving up on blockchain's trustless property and making compromises in its decentralized character, effectively work around these prevalent drawbacks; this is what is being done in private and consortium blockchains.

Building further on this, in a generalized way, we can state a third proposition:

> **P3**: Organizations will divert further from textbook blockchain implementations, the more they are concerned/affected by the issues we have identified.

Nonetheless, future technological advances still have the ability to overthrow this prevailing paradigm. 3 notable approaches, popularly as well referred to as 'Blockchain 2.0'-implementations are Enigma (Zyskind et al., 2015), Cardano (Kiayias, Russell, David, & Oliynykov, 2017) and IOTA (Tennant, 2017). However, the latter one is actually not a blockchain data structure, but a directed acyclic graph (a *Tangle*).

3 Methodology

3.1 Research design

In the introduction it was already mentioned that this research would be using the methods of a qualitative research. For this study, (semi-structured) interviews will be our preferred source of evidence. The questions were prepared in advance and to capture the full complexity, follow-up questions were extensively used.

[1] The storage of a 256bit (32 byte) word costs 20.000 gas. The price for one mebibyte is thus (20.000 * 32 * 1.024) = 655,36mio of gas. The average gas price is around 5Gwei (= 0,00000005 ETH), or in total 32,77 ETH. At the current price of one ETH, one mebibyte of data storage in Ethereum costs a bit less than 16.000 USD.

Special effort was made not to overfocus on specific industries (such as [maritime] logistics); this additionally led to the inclusion of a sufficiently documented case study that was found online. Purely financial implementations were left out of consideration, since they target a different type of blockchain concept and divert from traditional supply chains.

3.2 Data collection

The data collection process consisted mainly out of the conduction of interviews. We reached out to 33 potential interviewees that had an affiliation with blockchains, in a multitude of domains but all related to supply chains. This resulted in 6 interviews (of which 1 had to be discarded) in a variety of domains; an overview is given in table 1.

Domain	**Total number**	**Interviews**
Supply chains general	17	1 (+1)
Blockchain general	3	
Maritime Logistics	3	2
Logistics	3	
Provenance	2	
Retail	1	1
Agriculture	1	
Aviation	1	1
Public sector	1	
Energy	1	
	33	5 (+1)

Table 1: Interviewee domain

Potential interviewees were found in the researchers' network and through an extensive search on the internet using Google. Keywords used were combinations of *blockchain*, *supply chain* and the negative filters *-finance* and *-financial*; follow-up queries were used to gather more details about projects and interviewees as found on company websites, online media articles and general webpages. No geographical restriction was imposed.

The novel nature of the topic yielded only a modest number of contacts. However, 4 of the 6 dialogues should be considered as expert interviews, allowing for a broad perspective. Moreover, our dialogues converged towards similar responses: this makes us conclude that we managed to cover a substantial and representative part of the 'population'.

3.3 Operationalization

Intuitively, every project revolves around 3 main phases: a planning phase, an implementation phase and a check/feedback phase. We used these phases to construct our operationalization variables around, and subsequently our semi-structured interview questions. They are detailed in appendix **??**.

3.4 Data analysis

The data has been *coded*, a rigorous and structural method for sorting and organizing it. We used the software RQDA (R-based Qualitative Data Analysis) (HUANG, 2016).

Codes and categories have been dynamically added during the process of interpretation of the data, keeping in mind the dimensions and variables we determined in the previous

section. As required or deemed useful along the way, different codes have been splitted and/or merged together, allowing for an incremental refinement of the coding scheme.

4 Results

As described earlier, the interviews have been coded using the software framework RQDA, allowing for rigor and methodology in the processing, and the effortless retrieval of codings over the different information afterwards.

Data coding requires traversing of all data multiple times, because it is a dynamic process: new codes emerge, they are assigned code categories,... *Pattern matching* was a manual effort: since different interviewees may use a diverse wording to explain similar concepts (≅ codes), a human interpretation helps to extract a representative view.

4.1 Data coding results

Our coding resulted in 20 codes, which were organized in 5 groups. 3 codes were shared between a maximum of two categories, and 3 separate clusters of codes and categories appeared. These codes with their respective categories are visualized in figure 2 using the codes' IDs. This is further detailed in table 2.

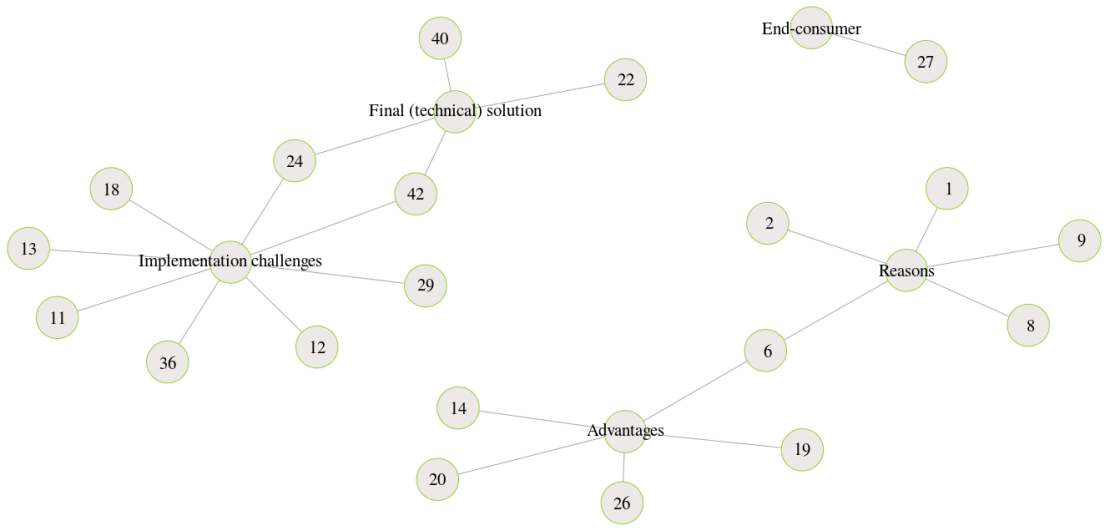

Figure 2: Second coding result: graphical representation

Any IDs come from the tables in the database as used for storage by the RQDA framework. If any ordering may seem to appear, this is coincidental. At most, the IDs may indicate the order in which the new codes were encountered within the information and have been added (since the database will assign incremental IDs for new rows). However, splitting, merging and reuse (after deletion) of codes disturbs this ordering. As such, these IDs have no other significance than to be unique identifiers.

Some text sections (or subsets of each other) might have been assigned overlapping codes. These are called *code crossings*. Our coding did not result in a lot of code crossings, despite heavy grouping, although some could be identified. An overview is presented in table 3. Codes without crossings were left out in favor of a good overview, and crossings were marked

in a different color. The absence of a lot of code crossings implies good practice: codes are well-chosen and mutually distinct (otherwise, merging could be needed).

Code category	**Code ID**	**Code**	**Incidence**
Reasons	1	Outdated technology	10
	2	Efficiency or overhead	11
	6	Use of common platform	35
	8	Risk of fraud	12
	9	Lack of trust	23
Implementation challenges	11	Issues with external cause	8
	12	Complexity	8
	13	Collaboration between members	17
	18	Lack of examples	12
	24	Business model	8
	29	Technological maturity	25
	36	No magical solution	8
	42	Only compliant, specific cases	12
Advantages	6	Use of common platform	35
	14	Automation	5
	19	Transparency	13
	20	Information security	12
	26	Ease / possibility of interface	13
Final (technical) solution	22	Off-chain data storage	8
	24	Business model	8
	40	Blockchain technical specifics	17
	42	Only compliant, specific cases	12
End-consumer	27	Provenance	11

Table 2: Codes and their categories, with incidence

	6	8	9	14	20	24	27	29	36	42	40
Use of common platform(6)	0	0	0	0	0	0	1	0	0	2	0
Risk of fraud(8)		0	1	0	0	0	0	0	0	0	0
Lack of trust(9)			0	0	0	0	0	0	0	0	1
Automation(14)				0	1	0	0	0	0	0	0
Information security(20)					0	0	0	0	0	0	0
Business model(24)						0	0	1	0	0	0
Provenance(27)							0	0	0	0	0
Technological maturity(29)								0	0	0	0
No magical solution(36)									0	2	0
Only compliant, specific cases(42)										0	0
Blockchain technical specifics(40)											0

Table 3: Overview of code crossings

5 Discussion, conclusion and recommendations

We will structure the discussion around our 3 propositions using the results per code category. We continue by recapitulating our research objectives. This will lead to our conclusion, recommendations for practitioners and suggestions for future research.

5.1 Discussion

5.1.1 Proposition P1: opportunities for end-consumers

> **P1**: End-consumers are not immediately targeted within supply chain blockchain applications, but would be interested in a convenient way to track reliable information about the components/origins concerning the product of their interest.

Specifically for end-consumers, at this point, the data analysis pointed only towards provenance applications. A graphical representation is given in Figure 3. This is in line with current research's suggestions and conceptual models: not only are food tracking scenarios envisioned (i.a. Tian, 2017; Tse, Zhang, Yang, Cheng, & Mu, 2017), as well authentication and anti-counterfeit solutions (i.a. McConaghy, McMullen, Parry, McConaghy, & Holtzman, 2017; Crosby, Pattanayak, Verma, & Kalyanaraman, 2016).

Figure 3: Code category detail: end-consumer interest

But however trustworthy the blockchain framework may be, one of the remaining questions is the underlying trustworthiness of the source data (Apte & Petrovsky, 2016), or as Kevin O'Sullivan rightfully pointed out in the interview: "the incorrect assumption that a lot of people have, once data is on the network, you can trust it. The reality is, all you can trust is the fact that it has not been tampered with.".

It should be noted however, that blockchain's immutability and auditability properties may have a preventing character: if fraudulent data is recorded, it should be easy to detect it still afterwards as a control mechanism.

5.1.2 Proposition P2: a global, integrated and transparent view

> **P2**: Supply chain members are looking for a global, integrated and transparent overview of information coming from all involved chain partners.

The outcome of the data collection very clearly showed an interest in the use of blockchains as a common and shared platform, eventually benefiting from the technology's perceived ease of interfacing (see Figure 4). Again indeed, this view is shared with a multitude of different authors (i.a. Milani, García-Bañuelos, & Dumas, 2016; Abeyratne & Monfared, 2016). Moreover, data stored in such a platform is supposed to be secure.

However, whereas the proposition only assumed the platform to be used *within* a supply chain, the data shows opportunities for blockchains to be used *across* supply chains, spanning an entire industry. That is obviously tightly related to blockchain's (observed, perceived) properties of information security in environments where there can exist even a severe lack of trust (Figure 5). This can be observed in several researchers' models (i.a. Gausdal, Czachorowski, & Solesvik, 2018; Mattila et al., 2016), but will undoubtedly take acceptation time (Iansiti & Lakhani, 2017).

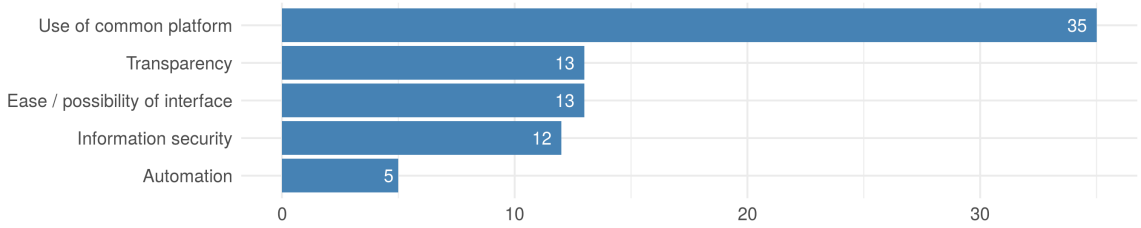

Figure 4: Code category detail: blockchain (perceived) advantages

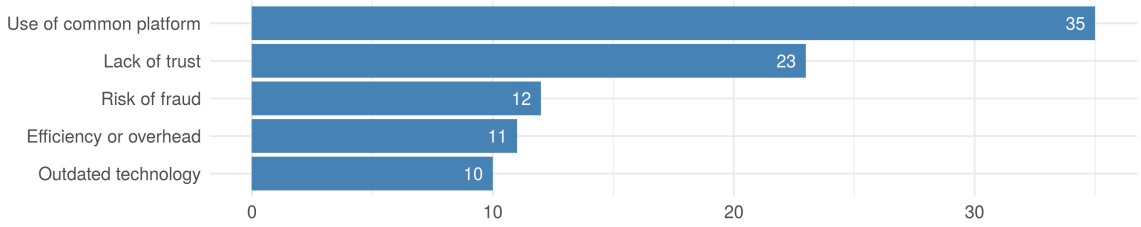

Figure 5: Code category detail: blockchain reasons

To a much lesser extent, our results showed automation benefits by using blockchain. Nevertheless, we argued during the literature review that automation is not essential nor typical for blockchains.

5.1.3 Proposition P3: blockchain issues impose workaround solutions

P3: Organizations will divert further from textbook blockchain implementations, the more they are concerned/affected by the issues we have identified.

The data itself showed only less significant evidence for this proposition. Certainly, the vast majority of our interviewees saw no use for cryptocoins within business applications (excluding public blockchains), and referred to the use of private or consortium blockchains themselves. This corresponds to the many concepts found in the contemporary literature, using permissioning in a non-public blockchain (i.a. Cachin, 2017) or a (currently) 'hypothetical' framework such as Enigma (i.a. Frey, Wörner, & Ilic, 2016).

How the final blockchain solution should look like, is presented in figure 6.

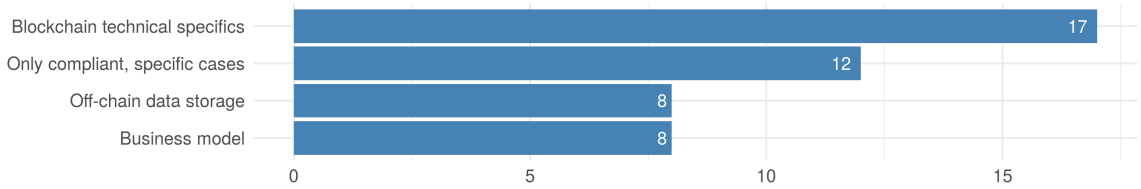

Figure 6: Code category detail: technical solutions in reality

A lot of codes with low frequency were grouped into a code for 'technical specifics', such as the type of blockchain used. Respondents tend to stress that blockchain can only be used in compliant, very specific cases. A non-ignorable number refers to off-chain data storage in response to (data) scalability issues, and the viability of the solution and its maintenance is as well brought up (incentivization, revenue models,...).

As such, despite its benefits, broad adoption cannot be noticed yet; major hurdles are

found in the maturity of the technology and a persistent lack of (good, successful) examples (Figure 7). Other researchers suggest similarly indeed "Logisticians have difficulties getting a clear idea of the benefits and use cases, while consultants and scientists worry about the technological maturity of Blockchain" (Hackius & Petersen, 2017).

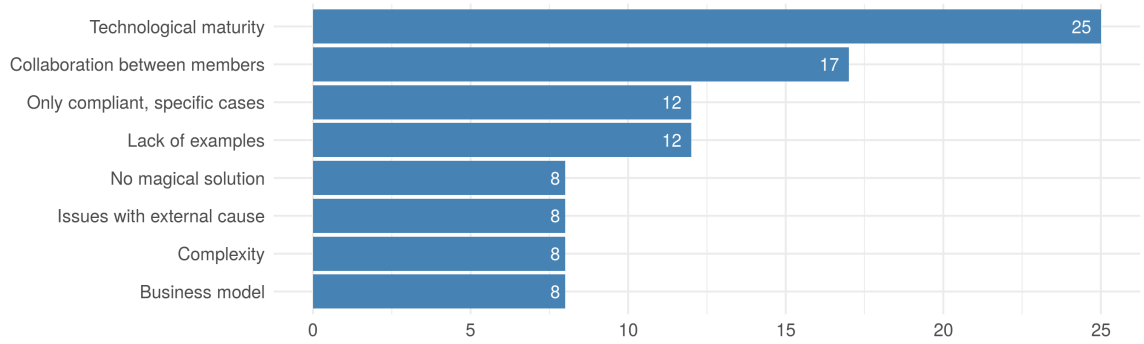

Figure 7: Code category detail: technical challenges

Besides that, the technology alone can only go so far, it still requires participants to collaborate e.g. for the governance of the network, congruent with other research's observations (de la Rosa et al., 2017). Michiel Valee described this as follows: "in a business context there will be governance anyway, it is in practice not feasible otherwise".

Moreover, our literature study earlier pointed out that the absence of coins and the use of private or consortium blockchain types in itself, is already a huge leap away from the original blockchain idea. What is very unclear, despite as well our respondents' assumptions, is in how far the original strengths hold whenever the concept is thoroughly changed. This duality may be reflected in the fact that even practitioners doubt about blockchain's practical usability, and are awaiting each other to come up with a good example.

5.1.4 Research objective

Looking back at this study's research objectives, what clearly stood out from the results was the fact that supply chain partners primarily are expecting (data) integration, as was discussed in and confirmed by proposition P2. This quest for integration is certainly not new nor was it hindered by technological barriers in the recent past.

We are unsure if this integration motive, whether within a supply chain or across supply chains, substantially benefits from blockchain as a technology. The central question actually becomes "what is blockchain?": is it a setup with its advantages and drawbacks like we overviewed it in our literature study, or is a private / consortium hybrid compliant as well? This was similar to the thoughts in proposition P3.

Proposition P1 was very straightforward about the end-consumers' benefits: as far as those are concerned, they lie in the availability of transparent and secure data, made accessible through a provenance application.

5.2 Conclusion

We found that almost no applications exist yet today, further than some in the financial domain (transaction oriented) or further than (eventually advanced) proof-of-concepts. Many reasons could be identified, but technological maturity was the most prevalent one.

Supply chains are mainly interested in blockchain's promise of integration, to be used as a shared platform. However, the data analysis does as well point out that some collaboration will still be required, and so it is unclear whether blockchain really has distinct properties in that sense, or is merely seen as a facilitator. This work observed (and partially invoked) a strong tension field between the original blockchain concepts, a decentralized, trustless, immutable and auditable environment, and the majority of applications as they are being developed today in a business context and particularly within supply chains.

End-consumers seem no immediate beneficiaries of the blockchain evolution, apart from a plenitude of blockchain-powered provenance initiatives. However, trust issues at the source of the data remain to be solved.

Blockchain solutions for use in supply chains do not seem to be as straightforward as anticipated, advertised or commonly assumed. Preliminary to a broad adoption, the current set of paradigms may firstly need an appropriate (technological) solution.

5.3 Recommendations for practitioners

To start with, the business process itself should be critically assessed. What are the underlying causes for the current inefficiencies? If the issue is more fundamental, like lack of digitization or difficulties to collaborate, then no technological framework will present a solution in itself; first of all, the underlying concerns need to be appropriately handled.

The second part of the assessment should be about (1) what the current technological obstacles are, (2) what potential one sees in the use of blockchain, (3) if blockchain is still the right candidate and (4) a thorough look at whether the blockchain solution as advertised (by third-parties or internal IT staff) will truly deliver on all of these points.

Main caveats for practitioners are: Who owns the network? What happens if one of the stakeholders stops? How is trust managed? How will the governance be organized?

5.4 Future research suggestions

These are a multitude of questions that we did not find to be appropriately answered today, each of them separately worthy of a specific research objective. However, we think that these are key inquiries to be tackled, as we experience that practitioners and potential (interested) users today are struggling with these.

Fruitful research around blockchains within supply chains might come in particular from:

- Good governance (structures). What is acceptable for blockchain participants as governance (structure), especially in environments with competitors?
- The development of sustainable blockchain business (or revenue) models.
- What are trust-enablers for enterprises and end-consumers?
- How should blockchain legal frameworks be constructed?
- How can archivation of data be obtained in blockchains? In the case of off-chain data, can we verify the existence of this data without revealing it?

References

Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology*, *05*(09), 1–10. Retrieved from https://dspace.lboro.ac.uk/2134/22625 doi: 10.15623/ijret.2016.0509001

Apte, S., & Petrovsky, N. (2016). Will blockchain technology revolutionize excipient supply chain management? *Journal of Excipients and Food Chemicals*, *7*(3), 910.

Atzori, M. (2015). *Blockchain technology and decentralized governance: Is the state still necessary?* (Mimeo, Available at SSRN: https://ssrn.com/abstract=2709713) doi: 10.2139/ssrn.2709713

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., ... Wuille, P. (2014). *Enabling blockchain innovations with pegged sidechains* (Tech. Rep.). Retrieved 2018-07-01, from https://www.blockstream.ca/sidechains.pdf

Bamert, T., Decker, C., Elsen, L., Wattenhofer, R., & Welten, S. (2013). Have a snack, pay with bitcoins. In *Peer-to-peer computing (p2p), 2013 ieee thirteenth international conference on* (pp. 1–5). Retrieved from https://doi.org/10.1109/P2P.2013.6688717 doi: 10.1109/P2P.2013.6688717

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *2015 ieee symposium on security and privacy (sp)* (pp. 104–121). doi: 10.1109/SP.2015.14

Buterin, V. (2014). *Ethereum white paper: A next generation smart contract & decentralized application platform* (Tech. Rep.). Retrieved 2018-07-01, from https://whitepaperdatabase.com/ethereum-eth-whitepaper/

Cachin, C. (2017). Blockchain - From the Anarchy of Cryptocurrencies to the Enterprise (Keynote Abstract). In P. Fatourou, E. Jiménez, & F. Pedone (Eds.), *20th international conference on principles of distributed systems (opodis 2016)* (Vol. 70, pp. 2:1–2:1). Retrieved from http://drops.dagstuhl.de/opus/volltexte/2017/7071 doi: 10.4230/LIPIcs.OPODIS.2016.2

Cong, L. W., & He, Z. (2018). *Blockchain disruption and smart contracts* (Working Paper No. 24399). National Bureau of Economic Research. Retrieved 2018-07-01, from http://www.nber.org/papers/w24399 doi: 10.3386/w24399

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*, 6–10.

Decker, C., & Wattenhofer, R. (2013). Information propagation in the bitcoin network. In *2013 ieee thirteenth international conference on peer-to-peer computing (p2p)* (pp. 1–10). doi: 10.1109/P2P.2013.6688704

de la Rosa, J. L., Torres-Padrosa, V., el Fakdi, A., Gibovic, D., Hornyák, O., Maicher, L., & Miralles, F. (2017). A survey of blockchain technologies for open innovation. In *4rd annual world open innovation conf. woic* (pp. 14–15).

Dilley, J., Poelstra, A., Wilkins, J., Piekarska, M., Gorlick, B., & Friedenbach, M. (2016). *Strong federations: An interoperable blockchain solution to centralized third party risks.* (Mimeo, Available at arXiv: http://arxiv.org/abs/1612.05491)

Dwyer, G. P. (2015). The economics of bitcoin and similar private digital currencies. *Journal of Financial Stability*, *17*(Supplement C), 81–91. Retrieved from http://www.sciencedirect.com/science/article/pii/S1572308914001259 doi: 10.1016/j.jfs.2014.11.006

Eisenhardt, K. M. (1989). Building theories from case study research. *The Academy of Management Review*, *14*(4), 532-550. Retrieved from http://www.jstor.org/stable/258557 doi: 10.2307/258557

Fanning, K., & Centers, D. P. (2016). Blockchain and its coming impact on financial services. *Journal of Corporate Accounting & Finance*, *27*(5), 53–57. doi: 10.1002/jcaf.22179

Frey, R., Wörner, D., & Ilic, A. (2016). Collaborative filtering on the blockchain: A secure recommender system for e-commerce. In *Amcis 2016 proceedings: Information systems security and privacy (sigsec).* Retrieved from `http://aisel.aisnet.org.ezproxy.elib10.ub.unimaas.nl/amcis2016/ISSec/Presentations/36/`

Gausdal, A., Czachorowski, K., & Solesvik, M. (2018). Applying blockchain technology: Evidence from norwegian companies. *Sustainability*, *10*(06). doi: 10.3390/su10061985

Gervais, A., Karame, G., Capkun, S., & Capkun, V. (2014). Is bitcoin a decentralized currency? *IEEE security & privacy*, *12*(3), 54–60. doi: 10.1109/MSP.2014.49

Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain : trick or treat? In *Proceedings of the hamburg international conference of logistics (hicl), 2017.* Retrieved from `http://hdl.handle.net/11420/1447`

Hirai, Y. (2017). Defining the ethereum virtual machine for interactive theorem provers. In M. Brenner et al. (Eds.), *Financial cryptography and data security* (pp. 520–535). Springer International Publishing. doi: 10.1007/978-3-319-70278-0_33

HUANG, R. (2016). *Rqda: R-based qualitative data analysis. r package version 0.2-8.* Retrieved 2018-07-01, from `http://rqda.r-forge.r-project.org`

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, *95*(1), 118–127.

Kiayias, A., & Panagiotakos, G. (2015). Speed-security tradeoffs in blockchain protocols. *Cryptology ePrint Archive, Report 2015/1019*, *2015*, 1019. Retrieved from `https://eprint.iacr.org/2015/1019`

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. In J. Katz & H. Shacham (Eds.), *Advances in cryptology – crypto 2017* (pp. 357–388). Springer International Publishing. doi: 10.1007/978-3-319-63688-7_12

Korpela, K., Hallikas, J., & Dahlberg, T. (2017). *Digital supply chain transformation toward blockchain integration.* (Mimeo, Available at ScholarSpace: http://hdl.handle.net/10125/41666) doi: 10.24251/HICSS.2017.506

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 ieee symposium on security and privacy (sp)* (pp. 839–858). Retrieved from `doi.ieeecomputersociety.org/10.1109/SP.2016.55` doi: 10.1109/SP.2016.55

Koshy, P., Koshy, D., & McDaniel, P. (2014). An analysis of anonymity in bitcoin using p2p network traffic. In N. Christin & R. Safavi-Naini (Eds.), *Financial cryptography and data security* (pp. 469–485). Berlin, Heidelberg: Springer Berlin Heidelberg.

Kroll, J. A., Davey, I. C., & Felten, E. W. (2013). The economics of bitcoin mining, or bitcoin in the presence of adversaries. In *Proceedings of weis* (Vol. 2013). Retrieved from `http://weis2013.econinfosec.org/papers/KrollDaveyFeltenWEIS2013.pdf`

Lamport, L., Shostak, R., & Pease, M. (1982). The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, *4*(3), 382–401. doi: 10.1145/357172.357176

Manski, S. (2017, 9). Building the blockchain world: Technological commonwealth or just more of the same? *Strategic Change*, *26*(5), 511–522. doi: 10.1002/jsc.2151

Mattila, J., Seppl, T., Naucler, C., Stahl, R., Tikkanen, M., Bdenlid, A., & Seppl, J. (2016). *Industrial blockchain platforms: An exercise in use case development in the energy industry* (Tech. Rep. No. 43). Retrieved from `https://ideas.repec.org/p/rif/wpaper/43.html`

McConaghy, M., McMullen, G., Parry, G., McConaghy, T., & Holtzman, D. (2017). Visibility and digital art: Blockchain as an ownership layer on the internet. *Strategic Change*, *26*(5), 461–470.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: Characterizing payments among men with no names. In *Proceedings of the 2013 conference on internet measurement conference* (pp. 127–140). doi: 10.1145/2504730.2504747

Milani, F., García-Bañuelos, L., & Dumas, M. (2016). Blockchain and business process improvement. *BPTrends (October 2016)*.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system* (Tech. Rep.). Retrieved 2018-07-01, from `http://bitcoin.org/bitcoin.pdf`

Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (2016). A blockchain-based approach to health information exchange networks. In *Proc. nist workshop blockchain healthcare* (Vol. 1, pp. 1–10). Retrieved from `http://kddlab.zjgsu.edu.cn:7200/research/blockchain/huyiyang-reference/A%20Blockchain-Based%20Approach%20to%20Health%20Information%20Exchange.pdf`

Project Provenance Ltd. (2018). *About.* Retrieved 2018-07-01, from `https://www.provenance.org/about`

Rosenfeld, M. (2012). *Overview of colored coins* (Tech. Rep.). Retrieved 2018-07-01, from `https://bitcoil.co.il/BitcoinX.pdf`

Simser, J. (2015). Bitcoin and modern alchemy: in code we trust. *Journal of Financial Crime*, *22*(2), 156-169. doi: 10.1108/JFC-11-2013-0067

SITA. (2018). *Who we are.* Retrieved 2018-07-01, from `https://www.sita.aero/about-us/who-we-are`

Tennant, L. (2017). Improving the anonymity of the iota cryptocurrency.. Retrieved from `https://www.semanticscholar.org/paper/Improving-the-Anonymity-of-the-IOTA-Cryptocurrency-Tennant/490d38d18dea9a61570ce4bc4cb8b1a3a7d527f2`

Tian, F. (2017). A supply chain traceability system for food safety based on haccp, blockchain & internet of things. In *Service systems and service management (icsssm), 2017 international conference on* (pp. 1–6).

Tse, D., Zhang, B., Yang, Y., Cheng, C., & Mu, H. (2017). Blockchain application in food supply information security. In *2017 ieee international conference on industrial engineering and engineering management (ieem)* (pp. 1357–1361).

Turing, A. M. (1937). On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society*, *s2-42*(1), 230–265. doi: 10.1112/plms/s2-42.1.230

VIL. (2018). *Blockchain in supply chains.* Retrieved 2018-07-01, from `https://vil.be/project/blockchain-supply-chains`

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016). The blockchain as a software connector. In *2016 13th working ieee/ifip conference on software architecture (wicsa)* (pp. 182–191). doi: 10.1109/WICSA.2016.21

Yin, R. (2009). *Case study research: Design and methods.* SAGE Publications.

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), e0163477. doi: 10.1371/journal.pone.0163477

Zyskind, G., Nathan, O., & Pentland, A. (2015). *Enigma: Decentralized computation platform with guaranteed privacy.* (Mimeo, Available at arXiv: http://arxiv.org/abs/1506.03471)