A silver bullet? Trust and Transparency in Blockchain Applications for Accounting

Claudia Negri Ribalta
Centre de Recherche en Informatique, Université Paris 1 Pantheon-Sorbonne
Be-Almerys, France
contact author: claudia.negri@almerys.com

Rose Esmander
Department of Management Control, École Supérieure de Commerce de Paris (ESCP)
Be-Optilys, Paris, France

Marius Lombard-Platet
Département d'informatique de l'ENS, École normale supérieure, CNRS, PSL Research University, Paris, France
Be-Studys, Geneva, Switzerland

Manuel Parra Yagnam

Pascal Lafourcarde
Université Clermont Auvergne, LIMOS CNRS UMR 6158, Aubière, France

Abstract

This exploratory paper intends to drive preliminary insights on the implementation of blockchain for accounting. Based off the question of whether blockchain applications for accounting could be revolutionary, this paper employs a ground theory methodology based on semi-structured interviews and concept analysis to highlight the challenges, gaps and the potential effects of this technology. Although deeper studies are needed, the conclusions highlight the socio-technical nature of accounting; the disconnect between the accounting requirements and “faith” in the technology by computer scientists; the relevance and changes of the concepts of trust and transparency when marrying both disciplines; and the real relevance of this technology for the processes of auditing and accounting.

Keywords: accounting, blockchain, transparency, trust

A silver bullet? Trust and Transparency in Blockchain Applications for Accounting

Introduction

Blockchain was first introduced by anonymous author(s) (Nakamoto, 2008). In their paper, they exposed the first application of their technology, the cryptocurrency Bitcoin. Bitcoin's main innovation is its decentralization feature: there is no bank and no authority to authorize or forbid any payment. Hence, the currency gained popularity amongst privacy-oriented people, as well as in the illegal world. In recent years, however, Bitcoin has gained popularity outside these circles, and its now known and used by a wide range of people.

For many, the word blockchain has become synonymous with Bitcoin. In addition it has become a buzzword that has made headlines in all forms of scientific research and social media. Moreover, its applicability is being tested in a wide range of fields, including finance (A. Tapscott & Tapscott, 2017) Healthcare (Agbo, Mahmoud, & Eklund, 2019), Supply chain Management (Blossey, Eisenhardt, & Hahn, 2019) and more.

In many cases, blockchain has been advertised as the pinnacle of transparency and trust, and as a solution to many problems in those fields, including accounting. Yet there appears to be little evidence to support these claims, most of them being simple iterations on the fact that blockchain is tamper-resistant. However, there has also been this vision of the blockchain as trust-less, given that all the information is present and there is no need to trust a central authority such as banks.

Given the perspective of a company that develops and implements blockchain solutions in a multitude of settings, including multiple European H2020 projects, in the fields of healthcare, security and risk assessment, a unique perspective is provided considering the development, implementation and adoption of this technology for accounting. An interdisciplinary approach, heavy on the technical and accounting perspective is provided to outline and exploratory research: (1) how blockchain technology changes our definition of trust and transparency; and (2) whether blockchain applications could be revolutionary or merely a fashion-fad.

Methodology

The objective of this study is to carry out an exploratory research on the relationship between transparency, trust, accounting and blockchain. As specified before, it particularly aims to start understanding:

1. how blockchain technology may change our definition of trust and transparency;
2. whether blockchain applications for accounting could be revolutionary or merely a "fashion-fad".

Trust and transparency are two unclear concepts, that are usually employed without careful thought on what they mean. Some scholars have already noticed this use of both words as buzzwords, even before the invention of blockchain (Beckmann et al., 2012; Raiser, 1999). With the current trend about blockchain, it is natural to fear that at least some of the hype around this new technology is overrated. For instance, it has been proposed that blockchain will eliminate intermediary jobs, and will replace the jobs of, for example, accountants, bookkeepers and auditors (Gordijn, Wieringa, Ioniță, & Kaya, 2019; D. Tapscott & Tapscott, 2017).

Through our experience in working H2020 project related to blockchain, we have experienced that blockchain acts more as a tool, that helps with the efficiency of data management. Our experience when building H2020 projects has provided an insightful experience of creating, designing and implementing blockchain system. We address that there have been attempts to create blockchain-based accounting systems however, most of them haven't been as successful as expected, with some of the better known project shutting down (like Balanc3). It seems, at a first glance, that blockchain does not solve complicated socio-technical problems. Thus, we theorize that blockchain will not change our definition of trust and transparency, nor will it revolutionize the accounting practices.

Essentially, we believe that a blockchain infrastructure for accounting (given the right parameters and characteristics) can, even with its failures, act as a support for accountants and auditors, enabling them to substantially minimize the issue of accessing a truthful source for accounting entries metadata (e.g. who input the data, when, under which pretenses, etc). However, since accounting is essentially a human process, blockchain based accounting will definitely not solve all human mistakes (intentional or otherwise) in the accounting entries or the financial reports produced. Furthermore, the creation of blockchain system for accounting, requires the participation of all stakeholders from the beginning of the software creation process. This means that developers should elicit and gather the requirements from accountants, lawyers and tax experts, in order to deliver a software that fulfills the expectations, complies with regulations and international standards, and fulfills its usability purpose.

We have undertaken a grounded theory methodology approach to begin understanding the phenomena selected. Firstly, as outlined by Strauss and Corbin (1990) theoretical sensitivity comes from literature review, professional experience and analytic processes that help the understanding of the phenomena. Therefore, in order to carry out this research and given the nature of the subject, an extensive literary review on the subject of transparency, trust, accounting and security in smart contracts and effect of blockchain in accounting is carried out. This literary review is done before the interviews were carried out.

Building up on our experience in H2020 projects, we decided to carry out semi-structured interviews to accountants and blockchain developers, based on the theoretical sampling method, in which "researchers seek and sample data that informs their theoretical categories" (Strauss & Corbin, 1994, p. 375) "Theoretical sampling is a tool that allows the researcher to generate theoretical insights by drawing on comparisons among samples of data" (Given, 2008, p.874) This method requires opening the survey sample to diverse groups. In this vein, we have identified these two group of actors as our groups of interest. We seek to compare their views on transparency, trust and blockchain, to better understand why it is being suggested that trust and transparency will evolve as concepts. Also, we seek to compare how they think blockchain might affect the accounting realm and whether if there is an agreement on the potentials of blockchain.

We have developed a set of questions that were asked to both groups. These questions where carefully designed, as to avoid any bias or have underlying suggestions. The interviews were recorded and transcribed with interviewees having no chance to prepare their answers beforehand. Moreover, we created a list of core questions for both groups to answer and we then added specific questions for accountants and blockchain developers. Questions can be consulted in Appendix A . We were careful not to guide respondents on their answers, and not make them feel uncomfortable while answering (Leech, 2002).

The interviews were then anonymized to prevent any biases during analysis. The transcribed text was afterwards analyzed by the authors, to identify key words that appear repeatedly through the interviews, main message, outliers, concepts, among others. This is was grounded theory method identifies the open coding stage on the 3 stage of coding (Strauss & Corbin, 1990) Through the open coding process, we kept a open mind regarding the concepts that the interviewees used and we were constantly comparing the transcripts with the other transcripts. In addition, the interviews were also analyzed and coded through an qualitative analysis software (NVivo) to get more robust results about our analysis. In detail, as outlined by Scott and Usher (Scott & Usher, 2011, p. 89) we are utilizing coding and classifying our interview transcripts by inferring concept's significance, patterns and repetitions that develop. Once we have the codes from the interviews, we proceed to axial coding - the second stage of coding - were we combine and relate the codes identified through our open code to categorize them. Then we will make these patterns explicit and we will elaborate a set of categories that hold firm in the setting being examined; the third stage - selective coding - of grounded theory method of coding approach by Strauss and Corbin 1990. We relate how the informant's terms associate to the theoretical ideas that we have developed, and how the same categories (i.e. transparency) have different codes between accountants and blockchain developers. In other words, how transparency is linked to different concepts depending if the intervewee is an accountant or blockchain developer.

When selecting the sample of accountants, we defined that we were going to interview accountants from different sectors: financial, forensic, junior and senior, *interalia*. This implies a trade-off that gives us a better insight and saturation (Strauss and Corbin, 1990; Bleich and Pekkanen, 2013) on the accountant group's perception towards the subject of study at the expense of explanatory power.

From a developer perspective, the rarity of blockchain developers is a challenge. As a consequence, to compensate the possible low levels of confidence and to achieve partial levels of saturation, we also interviewed blockchain project managers and security professors involved in blockchain projects.

Given the shortage of research and academics that work on blockchain outside the field of computer science and information systems, this article's conclusions should not be taken as conclusive findings. The idea of this research is to validate certain hypotheses about the possible effect that blockchain might have in concepts such as transparency, trust and accounting. It aims in opening the field and start understanding the blockchain effects on socio-technical issues.

For mode details on the methodology, you can resort to Appendix A - Methodology. A table with the meta-data of the interviewee and unsuccessful interviewees is also included in Appendix B - Interview Results .

Transparency and Trust in Blockchain

Transparency

As it is the case with numerous others words, transparency is a concept that does not have a unified definition. There is vast academic research on its meaning and operationalization, yet no consensus on what it specifically means (Michener & Bersch, 2013; Schnackenberg & Tomlinson, 2016). It has been recognized that given the different conceptualizations of transparency, there has been an abuse of conceptual stretching (Bauhr & Grimes, 2017; Michener & Bersch, 2013; Sartori, 1970). It is thus important to clearly define transparency and recognize the flaws of the selected framework.

There is unanimity that transparency is related to information and its disclosure. Throughout different languages, transparency is commonly described as an adjective to describe something can be "seen through". Combining both conceptualization of transparency, it is possible to conclude that at the very least transparency is about disclosure or access to information (Ball, 2009; Bauhr & Grimes, 2017; Michener & Bersch, 2013; Schnackenberg & Tomlinson, 2016).

However, the availability of information without an objective, context or substance, does not necessarily enable inferability about the object in question; i.e. it does not necessarily allow to "see through" the object being described by the information. That's why various authors have proposed that one key variable for transparency is information quality (Granados, Gupta, & Kauffman, 2010; Michener & Bersch, 2013; Nicolaou & McKnight, 2006; Schnackenberg & Tomlinson, 2016). As identified by Schnackenber and Tomlinson (2014) there is a research gap on a canonical definition of information quality, with divergent views between academics on whether this concept is tied to disclosure, clarity or accuracy of information.

We drawn upon this theoretical framework of transparency, to define the working concept for this paper. In other words, we take "a three-dimensional model of transparency" that identifies it as a "perception of the quality of intentionally shared information from a sender and emphasizes that transparency is a function of information disclosure, clarity and accuracy" (Schnackenberg & Tomlinson, 2016). Disclosure means that the information available is relevant and shared in a timely way (Schnackenberg & Tomlinson, 2016), available and accessible (Granados et al., 2010; Michener & Bersch, 2013). By clarity, we refer to the inferability of the information (Granados et al., 2010; Michener & Bersch, 2013), being comprehended by the receiver (Schnackenberg & Tomlinson, 2016), without industry terms (Nicolaou & McKnight, 2006) and understandable (McGaughey, 2002 in Schnackenberg & Tomlinson, 2016). Finally accuracy means that the information is reliable, meaning that is hasn't been tampered with (Granados et al., 2010; Schnackenberg & Tomlinson, 2016).

These definitions provide enough intention and generality to travel enough through different cases - and also is applicable to blockchain - without falling into conceptual stretching (Sartori, 1970). It also allows for a clear analysis of transparency in accounting practice and blockchain implementations, as its focus is on the information itself, rather than solely on the means on how the information is distributed. It facilitates an analysis of blockchain transparency from a technical level (for example, accuracy and reliability) and also, from a conceptual/legal perspective based on the information available (such as the accuracy and disclosure).

Finally, the aforementioned concepts are intrinsically related and similar to the CC5 and CC19 definitions of relevance, faithful representation, comparability, verifiability, opportunity and comprehensibility (International Financial Reporting Standards Foundation, 2018). We have decided to work with a broader definition for trust and transparency since blockchain applications are not contained solely within the realm of accounting. Therefore, restricting trust and transparency to the IFRS' conceptual framework will force us to overlook some of the issues with this technological application. Moreover, as we will see in the next chapters, even with blockchain being able to enable full verification, faithful representation and opportunity there are social, legal and institutional features that play a role in the application of this technology. It can therefore be argued that blockchain will not enable trust on the full system but rather that it will displace the transparency and trust issues to other parts of the accounting chain.

If the technology meets all these criteria of transparency then there will be no need for trust in the technology at least, but based on the next section we can see that even with a fully transparent system, technological, social and institutional features play a role in the acceptance adoption and use of blockchain, therefore in this case it can be argued that transparency does not beget trust but it rather displaces it; it is not increasing it. In addition, as we see in the later section, algorithms might don't necessarily meet the accuracy and disclosure, which leads one to the question, why are companies eager to adopt this kinds of technologies?

Trust

Trust is a very intuitive sentiment that is heavily leveraged in organizational systems, yet proves to be a complicated concept to define (Gambetta et al., 1988; Yamagishi & Yamagishi, 1994). This is mainly the case because there are different forms of trust, which depends on the context, where each discipline devises its distinct definition of it (Lewicki & Bunker, 1995). In addition most definitions of trust are based upon specific empirical testing rather than conceptual analysis (McKnight & Chervany, 2000).

In accounting literature, few similar yet different definitions of trust seem to exist. In many cases, trust is defined as "a psychological state compromising the intention to accept vulnerability based upon positive expectations of the intention of the behavior of another" (Chenhall & Langfield-Smith, 2003; Dekker, 2004). Similarly Tomkins (2001) examines the interaction between accounting information and trust in inter-organizational relationships and concludes that trust is:

> the adoption of a belief by one party in a relationship that the other party will not act against his own interests... with the absence of detailed information about the actions of the other party

According to Neu (1991) trust is defined as:

> social and constitutive expectations common to all exchange participants and consists of process based, character based, and institutional based

Trust in Systems. Many researchers draw upon concepts of Giddens' work on trust in abstract systems (1979, 1984, 1990, 1991). According to Giddens, lack of information is a prime requirement for trust, and therefore trust becomes confidence in the reliability of a person or system, regarding a given set of outcomes or events, where that confidence expresses a faith in the correctness of abstract principles (technical knowledge) (Giddens, 1991). According to Giddens (1991) in the area of system trustworthiness, notions of competence and integrity are likely to be applicable.

Trust and Blockchain. Based on these definitions, blockchain can be defined as a trust-free technology, given that all the required information is present, therefore there is no need to rely on, have faith in, or take any risks. This concept of blockchain being trust-free was introduced and discussed by Greiner and Wang 2015, and later challenged by Lustig and Nardi 2015 as well as Fröwis and Böhme 2017. Most of this work demonstrates that the need for trust will not be eliminated entirely using blockchain, but it would rather shift from trust in centralized authorities to trust in the algorithm (Maurer, Nelms, & Swartz, 2013).

We observe that other definitions of trust are given by the computer science literature, especially in security. Given a protocol, it is assumed that one or several users will participate, and can have diverging interests. The concept of "trusted user", or rather of "honest" user is defined as someone who will strictly follow the protocol, and not try to take advantage of the data they receive: they can be given a secret, and will not make malicious usage of that secret. On the other hand, a "malicious" user can deviate from the protocol as much as they like, for instance by changing values or impersonating other users (Dolev & Yao, 1981). Between these two extremes, a variety of attackers has been described. Probably the most common one is the honest-but-curious adversary, also called passive adversary: it is usually defined as "a legitimate participant in a communication protocol who will not deviate from the defined protocol but will attempt to learn all possible information from legitimately received messages" (Paverd, Martin, & Brown, 2014). While other adversaries exist (fail-stop, semi-malicious, covert...), honest-but-curious adversaries are the most common in the literature. Hence, cryptographic protocols do not necessarily require a full amount of trust in the participating parties: they rather defined what amount of trust they are willing to concede, and build attack-proof protocols on top of these assumptions. In this context, anonymity is not guaranteed in Bitcoin against a honest but curious adversary, even though solutions exist (Heilman, Baldimtsi, & Goldberg, 2016; Jawaheri & Basil, 2017).

Another area where trust is a prerequisite is the adoption phase. Trust is defined as an essential requirement for the adoption of blockchain by all stakeholders (Sas & Khairuddin, 2015). Some identified trust facilitating factors for Bitcoin users were the decentralized system, de-regulation, miner's expertise, transparency, easy and low cost transactions. In addition, a distinction between technological, social and institutional trust was proposed, where institutional trust was seen as one of the leading determiners of adoption and application of blockchain based payment systems (Ahangama & Poo, 2016; Lustig & Nardi, 2015; Zarifis, Cheng, Dimitriou, & Efthymiou, 2015). Reliance on third parties to feed the system with data and support it is another requirement for the blockchain to function, therefore a closed ecosystem is required as a trust facilitating quality (Glaser, 2017). Many of the current blockchain systems do not possess that quality, as they still rely on data from sensors and input from human created data bases, to connect the real world and the digital world.

Most of the literature about blockchain focuses on its application and its impact on traditional economy where very little attention is given to the concept of trust in the blockchain itself (Hawlitschek, Notheisen, & Teubner, 2018). When trust is discussed it mainly concerns the benefits of using a blockchain and its impacts on existing systems.

In this vein, the use of the blockchain can be a cause of issues in trust. Notably, new blocks are added to the blockchain via what is called a consensus phase. While consensus rules may vary according to each blockchain system (Wang et al., 2018), all of them have in common the unavoidable fact that each new block has to be proposed by one network member. The proposer of a block, therefore, is free to choose the transactions or data they want to include, and as such are also free to choose the transactions they will exclude, hence trust and control will be shifted to people proposing the blocks. Moreover, at a broader level, the user must trust that at least 50% (or 66% depending on the consensus used) of the people (or apparented[1]) in the network are honest. While this trust is weaker than the amount of trust one needs to put in a centralised system, it is still an important requirement, and has been violated several times in popular blockchains in the recent years, resulting in high monetary losses (Attah, 2019).

[1] For instance, in *proof-of-work* consensus algorithms, the 50% threshold is placed on the network computing power. Hence one or several users can gather more than 50% of the network computing power without representing 50% or more of the number of users.

Trust and Security in Smart Contracts

Bitcoin, the first blockchain, has been implemented as a ledger supporting simple transactions, and subsequent blockchains have followed suit. Hence, complex logic handling is most times relegated to smart contracts. Smart contracts (programs whose execution does not rely on a trusted authority) were first proposed by Szabo (1997) 20 years before the invention of blockchain. Though Bitcoin proposes a small set of nontrivial operations such as multisignature wallets, the first and most iconic blockchain with implementation of smart contracts is Ethereum (Wood, 2014). Because the code is publicly available on the blockchain, people can get an idea of what a program (or smart contract) does. Also, as the code can be locally executed by anyone, the correctness of the execution is trivially attainable. Hence, smart contracts are often used as a solution for increasing transparency (Francisco & Swanson, 2018; Nugent, Upton, & Cimpoesu, 2016). As such, smart contracts have been tested in a wide variety of applications, such as finance, notary procedures, or even gaming (Bartoletti & Pompianu, 2017).

However, it remains unclear of what kind of transparency is brought by smart contracts. Especially, open-source does not imply that the code is certified to work as expected, thus contradicting the underlying criterion of accuracy. For instance, because of results about undecidability of most programming languages[2], it is impossible to build an algorithm certifying the behavior of every possible smart contract (Rice, 1953; Turing, 1936). Incorrect execution can spawn from three different causes: a genuine bug in the code, a malicious payload inserted by the developer, or a correct smart contract, but following bad or ambiguous specifications.

While, to the best of our knowledge, there is no evidence of malicious smart contracts for the moment, the risk cannot be excluded. For instance, in the open-source community, there are many examples of code containing malicious payloads (Adam-npm, 2018; AKKUŞ, 2019; ceejbot, 2017; Mihajlov, 2018; Perica & Zekić, 2019; Wenceslas, 2018). Sometimes, the vulnerability is a hidden weakness in the protocol, making it hard to even detect the presence of said vulnerability. For instance, it is widely assumed (Bernstein, Lange, & Niederhagen, 2016) that the cryptosystem DUAL_EC_DBRG has been crafted by the NSA to embed such a vulnerability. Bugs in open-source code can also have critical repercussions. In 2014, it was revealed that OpenSSL, a software used to implement HTTPS security on web pages, had been majorly malfunctioning for 16 years, effectively cancelling all protections against a hacker familiar with the vulnerability, which was present on 25%-50% of popular websites (Durumeric et al., 2014). Worse, the attack was undetectable by the targeted server. Similarly in the world of blockchain, the DAO vulnerability, as Dhillon et al. (2017) sum up, caused a breach of 3 million Ether (worth 54 million Euros at that time) because of an undetected bug.

We also remark that open-source does not equal transparency. As a matter of fact, code obfuscation (hiding the behaviour of a source code) is an active field of research in cryptography, following seminal work (Barak et al., 2001). These ideas are also in line with our concept of transparency, as it lacks clarity (inferability on the behaviour of the smart contract). More pragmatically, reverse engineering is a popular activity amongst white-hat hackers, and smart contracts do not qualify as an exception (@icchyr, 2018), which proves that some pieces of code are obscure by design.

On a similar note, some open-source code is precisely designed to achieve maximal pri-

[2] More specifically, the result concern Turing-Complete languages, a very wide set of programming languages. Turing-completeness is strongly suspected to be the exact mathematical transposition of what an algorithm is. Almost all programming languages, except a few very specific ones, are Turing-Complete.

vacy, hence lowering information disclosure to its bare minimum: this is the domain of zero-knowledge cryptography. ZCash (Sasson et al., 2014) is a pioneering cryptocurrency in that domain, and has successfully implemented a blockchain in which all transactions are private (meaning that only the sender and receiver can learn the amount of the transaction, and by default the receiver cannot learn the sender's identity), but anyone can check a transaction validity, thanks to zero-knowledge proofs. We remark that while we get the accuracy (a user can deduce that all transactions are valid), we do not get any information disclosure (we know nothing else that the validity of the transfers), nor the clarity (zero-knowledge proofs are not made to be human readable).

Therefore, the notion of transparency in code cannot be immediately deduced by presence of open-source algorithms, even in blockchain. An effort to characterize the qualities that a smart contract should have in order to be considered as 'trustless' is made in (Fröwis & Böhme, 2017). Notably, they examine how the flow of execution must be protected, what guarantees must be held to certify integrity over time, and so on.

Effects into accounting

Blockchain can be a very powerful tool for storing data that is required to last over time. As it is has already been explained, blockchain is a distributed ledger. In other words, it can be a very reliable method to store data, so that it can't be changed without the other parties noticing it. However, as the tool is, it won't eliminate or completely revolutionize the auditing process, nor will magically solve the broader problems of trust and transparency in accounting.

From an industry perspective, various professional services have reflected on how blockchain technology may impact different industries (Billinghurst, 2018; Deloitte, 2016; Deloitte, Canada, AICPA, & UWCISA, 2017; Ernst and Young Global, 2018; Financial Executive International, 2018). Yet, academia has reacted slower to the phenomena. Only recently have other areas of study, apart from cryptography and computer science, started researching blockchain's impact. Some notable examples are Dai and Miklos (2017) and Yermack (2017), who have researched the potential impact of blockchain in financial services. The conclusions from both authors are similar: blockchain enables faster, cheaper and autonomous financial activities that are normally associated with a high time investment, such as balance sheets, fraud detection, storage of the data, *interalia*. This reflection coincides with the conclusion that professional services have on blockchain.

On a more granular level – given specific system characteristic – blockchain could potentially enable real-time accounting (Dai & Vasarhelyi, 2017; Financial Executive International, 2018; Yermack, 2017). For example, auditors will be able to check every transaction made by a company and thus replace the current random sampling technique (Ernst and Young Global, 2018). It could also allow for daily accounting data aggregation, creation and reporting, lowering risks for potential investors. Furthermore, given a proper architecture design of a blockchain system, it is also possible to embed more certainty about the integrity of the data into the accounting ecosystem (Financial Executive International, 2018).

However, it is paradoxical how the promises of blockchain have been portrayed, the interest in the technology and its real implementation. For example, PWC Global Blockchain Survey (2018) got results from over 600 executives in 15 countries and "found that 62% of the respondents have some blockchain project in development" (Billinghurst, 2018). Yet, the same survey also highlighted that the three mains barriers to adopting blockchain are regulatory compliance, lack of trust from users and the ability of bringing networks together (each barrier being a preoccupation for more than 45% of the respondents). In fact, there are real concerns on how to build blockchain systems that are compliant with current regulations and laws.

On another note, having built-in smart contracts to carry out the jobs that auditors were carrying before - such as cash flows or balance sheet - doesn't necessarily imply that the results are going to be lawful or trusted by other parties. It can't be assumed that - because an actor is using blockchain - the data that has been input into the ledger is accurate, that the source code of smart contracts is reliable, and that the system is secure, among others. As expressed by the Deloitte report of blockchain (Deloitte et al., 2017), blockchain-based accounting systems will still require auditing to ensure that the system is working properly, to verify the accuracy of the data written in the blocks (and very possibly, evidence of it too), the structure of the blockchain system, the smart-contract code and even manually carry out management estimates. For example and as previously mentioned, although it might be possible to see the (open) source code of the smart contract, it isn't always plausible to infer the behaviour. This situation also applies for data oracles, data input and, security, *etc*. Not only due to regulatory compliance, but because it can't be trusted that the data written in a blockchain system is truthful, nor that it provides the security properties of blockchain.

This lead us to support the idea that blockchain will not eliminate auditing professional jobs - a key idea behind Bitcoin proposal and blockchain ideology is that intermediaries will cease to exist - but rather its implementation will shift the focus from financial accounting, into a more technologically oriented approach. If blockchain is implemented, there is a high likelihood of a shift of the accountant's jobs into verifying that the data is truthful, that the systems have been implemented correctly, into the validation and verification of smart contracts, legal compliance, etc. In other words, accountants will be required not only to have knowledge of financial regulations, but also of technology and security - adding an additional layer to an already complex activity. However, methodologies like sampling which lead to many auditing oversights will likely change as auditors and accountants will now be able to check the full trace of the data input into the system.

Furthermore, from our literary review, it seems that blockchain systems on their own will not solve the broader transparency or trust problems through its implementation. From a transparency perspective, blockchain does allow for a higher level of transparency, as there is confidence that the information has not been tampered with. Also, it makes traceability and metadata easier to query. Regardless, transparency is not limited to one variable and also depends on the information available in the block, the access to it, among others.

Essentially, our hypothesis is that a blockchain infrastructure for accounting (given the right parameters and characteristics) can, even with its failures, act as a support for accountants and auditors, enabling them to substantially minimize the issue of accessing a truthful source for accounting entries metadata (e.g. who input the data, when, under which pretenses, etc). However, since accounting is essentially a human process, blockchain based accounting will definitely not solve all human mistakes (intentional or otherwise) in the accounting entries or the financial reports produced. Furthermore, the creation of blockchain system for accounting, require the participation of all stakeholders from the beginning of the software creation process. This means that developers should elicit and gather the requirements from accountants, lawyers and tax experts, in order to deliver a software that fulfills the expectations, complies with regulations and international standards, and fulfills its usability purpose. We expect, however, that this technology might enable new, algorithmically based, alternatives that will change the role of the accountant and might lead to a higher automatization of certain activities.

Interview results

First, we recognize we lack high levels of saturation from both interviewed groups. The more accountants we interviewed, the less we were finding new information and we could anticipate what most of the answer would include, achieving high level but not complete saturation. This situation was partially achieved with developers, meaning we achieved partial saturation, as we could still discover new information for every new interviewee. To surmount this problem in future research that follows this path, a larger sample of interviews and more diverse cohorts would be needed to draw more robust conclusions. Also, other source of data like meta-studies and analysis of real world projects might be interesting to explore. In addition, we recognize that there might be some biases in the answers, once again given the small number of respondents. Being aware of these issues, we tried to avoid to the maximum to snowball interviews, to avoid further biases and interview respondents from different knowledge networks. This is not the case for developers 1, 2 and 4, who work in the same company and were part of our original sampling. This implies that their answers might be biased towards the same conceptual base.

We have carried out the coding process both manually and using NVivo. As expressed on the methodology section, we first carried out an open coding process which we then processed in axial coding. While doing the axial coding, we noticed that terms used in the definitions of transparency and trust in the accountant group had a high frequency. However, this was not the case for the blockchain developers, who appeared to have more divergent views on these topics.

Through the NVivo software, we were able to visualize more clearly which codes tended to repeat themselves, under what circumstances and the frequency they appeared in the interviews. This facilitated a constant comparison between the interest groups.

In this section, we share our general results. Given the scope of this study and the variance of concepts introduced in the interviews, not all codes can be shared and only the highlights from this qualitative analysis are shared.

Trust

Accountants. When it came to their definition of trust, or what thoughts the word trust triggers in them, the accounts gave elaborate descriptions and defined it as something that is more process based that was situated in relation to a client or to a market or to an organization. To accountants, trust was not simply quantitative in nature but there was a qualitative dimension that to them was the key determiner of their judgement to whether or not the quantitative nature is reliable. There was a significant emphasis on the role of accountants and auditors in building this trust through their professional judgement, critical view, and their knowledge about the standards and context. Two major themes that emerged when discussing the topic of trust with accountants and auditors were reliability and accuracy.

The word reliability was used by 5 out of the 8 accountants interviewed when defining trust (see table 6). When asked to elaborate, many of them said they view trust as a historical analysis of the object we are trying to trust. Much of it is based on previous relational experiences and historical data as well as reputation. According to our results, trust is not something that happens spontaneously, it is something one builds over time.

One of the biggest determiners of reliability according to accountants is reputation (see table 6). This was determined based on the context in which the object of trust is situated. Factors such as the country in which a company exists, the management, previous audits, who audited the company as well as previous history of fines or unfaithful representation of financial situation of the company are some of the variables that accountants take into account to assess reliability.

As mentioned above, accountants, when discussing trust in information, used the word accuracy with high frequency. When asked to elaborate about what accuracy means to them, 3 out of the 8 accountants interviewed included the presentation of complete information (see table 6). Confirmation of complete information was determined by the accountants based on their understanding of the standards and regulations, knowledge about the market and on their critical perspective that they apply to ensure that the data is compliant and provides a good representation of the company.

The remaining accountants highlighted traceability as important: being able to track back where the information came from, who entered it into the system, when was it changed, when and who audited it etc. One accountant mentioned the word transparency when talking about trust, but none of the others did.

When asked about the relationship between trust and blockchain adoption, many accountants mentioned the need for blockchain to be first adopted by the more influential companies (see table 4). In addition, the blockchain itself had to be audited and certified for accountant to trust it's validity. Exposure and regular interaction with the blockchain in their practices was essential for accountants to trust and adopt it in their practice.

Some accountants saw the fact that the blockchain is tamper-proof as a problem (see table 3), as for them accounting practices are about revising data when new information is made available, questioning the data and updating it based on new regulations and standards, therefore that contributed little to their level of trust in the data. On the other hand, the need for a lower level of human intervention was mentioned by 2 accountants, to ensure reliability and therefore trust.

Developer. Unlike accountants, when asked about their definition of trust 4 out of the 7 interviewed developers distinguished between trust in a person and trust in a system (see table 12). When it came down to their trust in a person it was quite similar to what accountants said, historical experiences, perceptions and reputation.

Just like accountants for developers reliability was an important concept of trust, but what contributes to their conception of reliability is different. When talking about trust, all 7 developers discussed the concept of consensus in a decentralized system in one way or another (see table 12). For a developer, reliability was a property of the system rater than the participants. While it is important to verify the source of the data verifying the authenticity of the participants was less important, because even if the participant were not honest, they system will not allow them to act in malicious ways. Therefore, the trust of the developers is on the system, more specifically the code and the protocol. An interesting finding is that most developers associate this with control over one's data, privacy, and security.

Based on this, it is then not a surprise that 5 out of the 7 developers placed a significant importance on the functionality of the system to execute a task and transmit information reliably from a sender to a receiver, in order to determine reliability and trust. It is not possible to know if the system is actually doing this, a developer has to trust that it is. The developer's trust stems from the system's conformity to standards and certification by external parties. In addition, transparency and traceability based on information management were mentioned by 4 out of the 7 developers as an important aspect of trusting the system. For all this information see (see table 12)

Transparency

Accountants. When asked about transparency, the accountant cohort responded that it was related to information. In comparison, developers didn't relate this concept directly to information. The four main codes that accountants identified to be linked to transparency were: availability of the information, traceability of information and actions, inferability or meaningfulness of the information (i.e. that the information can actually tell some message) and that it can be "see through" (concept coded into openness). In fact, these patterns and tendencies can be seen in Table 1.

Accountants' definition of transparency falls in line with our literary review and theory about transparency. Specifically, 6 accountants defined transparency with the codes "openness" or "not having information hidden" or "see through"; all being expressions that fall under the category of openness. All the accountants, except accountants 1 and 3, gave us a definition that relates to the inferability of the information. It is important to highlight that none used the exact same word. Specifically, 6 accountants explained that information should be meaningful and another one explained that the information should refer to "how the algorithm works". This is highlighted in Table 1, where we also share other codes that accountants manifested when talking about transparency. Particularly, accountant 1 seemed very certain that transparency was linked with knowing how the systems and algorithms works.

Following the same line of thought, 4 accountants talked about being able to infer "financial statements" or another type of information, when presented the question about transparency (coded under *meaningful information*). 5 accountants talked about traceability of the information, with 1 directly saying "traceability" more than 7 times in the answer (accountant 2) and the 4 others talking about how the blockchain gives an "instant picture" of when, why the information was input, and by whom (and then further explaining that it is access to the "metadata").

All accountants except one, never linked trust to transparency - directly or indirectly - nor saw a direct relation between both concepts. A small table with other codes that were linked with transparency is provided. In addition, in all our notes from most of the interviews, we noticed that accountants gave lengthy and detailed definitions of transparency.

Developers. In comparison with the accountants, the blockchain developers manifested more divergent views on what transparency means. Some developers manifested to have similar views on the definition of transparency that we we theorized (for example developers 1 and 3) others expressed definitions that relate transparency to trust (developers 5 and 7). In fact, most developers added elements of trust in their definition of trust (see table 7).

3 of the developers mentioned several times that transparency can be provided based on the technical aspect of the system in use. Codes such as the system design, the protocol in usage, the knowledge on how the system works and even smart contracts, appeared in 3 of the developers. 2 other developers expressed how the blockchain can allow from transparency without any trust (see table 8).

From our notes, the definitions of trust of most developers (except developer 1 & project manager), were straightforward, short and concise. When asked to further explain the concept, they would repeat the same, use very direct concept (such as "open", "see through", "the system design" or "the protocol in use") when prompted to further explain their position.

Effects of blockchain into accounting

Accountants. The area that accountants perceive that can change the most when using blockchain based accounting systems, is in the traceability of the information. All the accountant's that answered the questions about the impacts of blockchain in accounting, agreed that this area will be the most impacted. In addition, 6 accountants explained that a blockchain based system would probably act more as a tool for their work. In other words, it will be a tool that will allow accountants to easily trace the information back. This is the second area where accountants agree the most. (see table 3)

Another area were accountants agree that blockchain will impact, is on the availability and reliability of information. 6 accountants identified this variable as possibly being affected by blockchain based system. Remembering our transparency definition, information availability and reliability are key concepts.

Other areas that were mentioned, but in less frequency and magnitude were: efficiency and speed of information processing, tamper-proof information and a shift of trust towards technology.

One key finding was that most accountant's has basics notions of blockchain and most of them related it to cryptocurrency. Indeed accountant 2, who was the most informed of all on blockchain, predicted this situation and accountant 4 said it was difficult to teach about blockchain because it "is not easy to understand". Moreover, by reviewing Tables 4 and 5, it is possible to appreciate that accountant 6 never answered a question about blockchain and their answers are more related to technology. Additionally, accountants 3 and 4 told us they knew very little if almost nothing of blockchain.

Regarding the challenges on adoption of such systems, some accountants directly talked about blockchain and others were more general, referring to technology. Although our main focus is on blockchain, we find that it is useful to also include those answered that were more general on technology, as they give an insight to the accountant's perspective.

Without a doubt, the area that concerned the most to accountants is the information that is going to be inside the blockchain. That is, in other words, how the parametrization of the information will be. As seen in Table 4, 4 accountants expressed that this was going to be one of the key elements for a successful widespread adopting blockchain system.

In addition, two other crucial ideas were expressed by the accountants as challenges for the adoption of blockchain: the requirements of the system and trust issues on the system itself. Although requirements were mentioned by two accountants, it highlights itself by the magnitude and importance given by accountant 2. It expressed the importance of blockchain system being different ERP system, that developers work with accountants to see what they need, the importance of how the information is parametrized and a certification process (which was also expressed by accountant 4). In trust issues and testing, accountants expressed they would be skeptical of the system (explicitly said by accountant 6), that it would require testing by other companies and it should be adopted "by the big 4".

Developers. From a developers perspective, there was no agreement in which area the blockchain based system would impact the most. None of the areas identified present more than 3 developers (which represent less than a 50%) agreeing on it. (see table 10)

As per (see table 10) the two concepts with the highest frequency - and also mentioned by 3 accountants - are, one that blockchain solves problems of trust and will be the future of it, and, two, that it will allow natively for traceability of information. In summary, blockchain developers consider that given the architectural design of blockchain, problems of trust will be solved with a blockchain system.

Other concepts, that were discussed but less frequently mentioned, are that blockchain will have impact as a tool, will help with automatization of the accountancy and will allow better information availability and reliability.

The challenges that blockchain system will have to overcome to become a widespread tool, are - compared to what accountants identified - mostly technical obstacles (see table 11). Every developer acknowledged at least one challenge, with technical (or technology) challenges being the most identified by developers (5 developers mentioned this aspect when being interviewed). For example, some of these challenges were the interaction with other systems, the consensus algorithms or developing a "fully fledged solution" (developer 7 quote). Other obstacles relate to the security of blockchain system and data management (recognized by 3 developers), regulations and privacy issues and trust problems with blockchain. As we can see, developers singled out most challenges from the techincal realm of the blockchain technology, rather than from a human optic.

Finally, all the developers have expressed that it is difficult to explain the blockchain technology to non-blockchain enthusiast (see table 9). 4 developers said that people don't understand the technology, particularly the decentralization nature of it and that there are a lot of misconceptions surrounding the technology. Frequency wise, the code that appeared the most and expressed by 3 accountants, is that people tend to overfantasize about the potential of blockchain and what it can actually achieve. Lastly, 3 developers said that non-blockchain enthusiasts tend to link blockchain to cryptocurrencies.

Results discussion

Trust

In comparison to developers who made distinctions between trust in systems and trust in humans, accountants trust in systems was a byproduct of trust in human relations and other variables that were not directly related to the system itself. Both accountants and developers stated reliability as a requirement for trust. This aligns with the definition of trust provided by Giddens (1979, 1984, 1990, 1991), but each group had different requirements for reliability. Accountants trusted organizations to provide complete and faithful representations of the company. In order for them to trust that full information was provided, they rely on their knowledge and on standards as well as qualitative data such as historical relations and reputation of organizations to make judgements. On the other hand, developers reliability was embedded in the system itself to manage relationships between participants and ensure accurate communication between the different parties. For developers, their reliability was based on the functionality of the protocol and code to ensure that the system is doing what it is expected to do. The byproduct of this is a decentralized systems that enables consensus in a decentralized control environment. Based on this view, unlike accountants who place high importance on relational trust, developers view authenticity of involved parties as secondary.

Seal *et al.* (1999) view good personal relations at the individual level as facilitating sustainable trust levels between organisations. The accounting practice is seen to serve two functions, one is governance and control and the second is trust building (Vosselman & Van der Meer-Kooistra, 2009). This was reflected in the accountants' emphasis on vitality of their role in analysing and critiquing the data presented to them in order for them to deem it trustworthy. This aspect of interpreting data and telling a story could lead to another set of challenges which is the subjectivity of the accountant shaped by their own perceptions. While Porter (1996) states that quantification is an important determiner of modernity and reproducibility of evidence and facts, and therefore trust, Fligstein (1998) argues that quantification is embedded in political and economic arrangements that could lead to multiple interpretations of the same set of data based on the subjectivity of those telling the story using this data. In the accounting practices this is the case, accountants are not just presenting numbers, they are telling a story using those numbers, and therefore they become controllers and producers of trust. It is no surprise then that the accountant's definition of reliability and therefore trust is based on non quantitative and more subjective measures such as reputation, historical interactions and standards. This also explains their need to have control and the ability to change the data when new information is made present.

While developers did point out the importance of certifying the data that is entered into the system, which is done based on reputation of organizations feeding this data to the system, they viewed this as just one step of the trust building mechanism. Once the data is entered into the blockchain, trust is reduced to ability of the system to transmit this information from a sender to a receiver. In this sense, building trust through relationships is no longer necessary, because the system manages them in such a way that encourages good behavior and makes it very difficult for one party to influence the system. This is problematic because as mentioned before, trust in the accounting world is based on the interpretation of data and the context in which this interpretation takes place: how is this data collected, how is it presented, power relations, social structures etc. By reducing the concept of trust to a simple automatic process of data sharing, a big part of the picture is overlooked, furthermore, the system is limited in the sense that it can only deliver data that can be quantified, and through this process of quantification, we miss a lot of qualitative information that is necessary for decision making.

In conclusion, both accountants and developers place a significant importance on reliability when deciding whether to trust or not but each generate their reliability differently. Accountants place their trust on the organizations to provide full information and use external factors such as personal relations, reputation and standards to shape their trust, whereas developers place their trust on the systems and their ability to properly execute functions and run protocol. Accounting practices are about more than just representing quantitative data, they are about telling a story using this data and other non quantitative variables (Fligstein, 1998). In addition, besides being tools of control, accounting practices serve as trust building technologies (Vosselman & Van der Meer-Kooistra, 2009). Developers of the blockchaine differentiate between trust in persons and trust in systems, and place higher importance on trust in systems. In this sense trust is reduced to a protocol's ability to securely execute transaction between different parties, by doing this they reduce the essence of the accounting practices to sharing of quantified data, and they overlook the role of accountants as trust builders and byproducts social, political and economic factors.

Transparency

Based on our analysis and interviews, from a transparency point of view, it seems that blockchain isn't expected to change the concept of transparency. None of the respondents from the accountant category indicated that they thought blockchain might directly affect transparency, 3 respondents of the accountants groups talked briefly about how blockchain might relate to transparency and only 4 respondents from the developers group talked about blockchain and transparency. In the case of the developers that linked transparency and blockchain, the link relates to the idea of traceability of the information, rather than the blockchain itself providing transparency.

In other words, only a small part of accountants shared the opinion that a blockchain system would provide a higher level of traceability. Moreover they insisted on saying that blockchain will not provide higher levels of transparency *per se* but rather its protocols and usage will be the defining point on whether the technology has an impact on transparency or not. At the same time, they hold the view that transparency is linked to traceability of information: they are of the opinion that blockchain based tools will help to improve one of the variables of transparency. On the other hand, developers expressed that technical means on its own could provide transparency regardless, specially in the cases of developer 7 and 5. Overall, there seems to be an agreement between most accountants and blockchain developers that accuracy and traceability of information is an important factor for transparency.

All accountants manifested that their concern with the fact that transparency is intimately linked to the inferability of the information. Specifically, related to the idea of information quality. In fact, the sole access to information isn't a sufficient condition for inferability as the information must convey a message. This is highly related to our three-dimensional theorization of transparency, with the clarity on information variable (Granados et al., 2010; Michener & Bersch, 2013; Nicolaou & McKnight, 2006; Schnackenberg & Tomlinson, 2016). In addition, accountants 5 and 6 expressed that the clarity of information is also affected by the comprehensibility of such information. These ideas were not present in the developers answers, as only 1 of them related transparency to the quality of the information.

This is a critical problem. Accountants are expecting certain types of information from accounting systems - in this case, it would be from a possible blockchain-based system. However, blockchain developers don't put the same emphasis on information clarity or meaningfulness as accountants. Thus, the parametrization of information is one of the key areas where blockchain developers and auditors are in misalignment. As accountant 2 highlighted, parametrization of the information that will be available in the blockchain is the most important variable for the success of such systems. To emphasise the importance of this, if the blockchain system isn't created without eliciting what type of information, in which format and - possibly - which standard to follow, auditors will find blockchain based tools of little help. As accountant 2 stressed: "Blockchain is going to be the future of reliability, to the extent that you parameterize and style the information, and gives you the requirements necessary for you to trust this type of information".

Finally, there is an agreement that transparency also depends on the disclosure of the information. Particularly, for both blockchain developers and accountants, transparency is deeply linked to information being available and "open" (or "not hidden" as some interviewees expressed). Based on the answers given, it also seems that blockchain can prove to be helpful in the area of disclosure of information given its decentralized nature.

Thus, three working conclusions become apparent. Firstly, for accountants, transparency is related both to the openness of information and what that information is conveying. The definition accountants gave us is related to our theorized three-dimensional transparency definition. Secondly, parametrization of the information inside the blockchain will be one of the core issues when adopting those systems. It seems that this is one of the most important issues when adopting certain systems, though this conclusion requires further research. Which leads to the third conclusion: blockchain developers should elicit and understand the requirements from the accountants. If the blockchain system fails to provide the type and format of information that accountants require, it might be difficult for blockchain-based systems to be adopted successfully. Moreover, accountants hint that blockchain - in their views - might increase the level of transparency based on how the information has been parametrized, indicating how important is for developers to understand the auditors' expectations.

Although the importance of gathering, specifying and understanding the requirements of all the stakeholders involved in a system is well known in the area of software engineering, further research should be done in requirement engineering and its relation to blockchain based systems as the standardization of parametrization and legal compliance shows to be an added challenge.

Blockchain's impact of accounting

While it appears that blockchain is unlikely to change the concept of transparency on its own, consensus about the impact of blockchain on accounting is not a clear cut. As a matter of fact, all accountants except for one (accountant 6) reported that they believe that their field will be affected by blockchain. As previously mentioned, accountant 6 explained they didn't know about blockchain - and thus has been excluded from this discussion.

As it happens, all developers raised that it was difficult for them to explain blockchain to non blockchain enthusiast. The reasons that developers expressed more frequently, was that people overfantasize about blockchain, they don't understand the technologies way of functioning (such as decentralization) and that they relate all blockchain technology to cryptocurrency. We discovered through our interviews that accountants have a lot of misconceptions of blockchain and the ones that had some knowledge of it, overfantasized. For example, accountant 5 expressed that "I don't know much about blockchain, but I know it's kind of.. tell me if I am right. It's the kind of data that you cannot erase". Although accountant 5 knows one of the most important features of blockchain, which is immutability, they don't seem to know anything else about blockchain, such as consensus algorithms, decentralized nature, permissioned and permissionless networks, *interalia*. Accountant 2 confused legal smart contracts with smart contracts codes. This poses a challenge when gathering the requirements of stakeholders. This will be further discussed in this section.

One of the most popular expected changes by accountants is traceability, with 16 explicit mentions. It is interesting to note that one of the core features of blockchain is tamper-resistance, which improves traceability. This might be the reason why they mention that the traceability of records will be the most impacted area, as it is where blockchain and accounting intersect. Certainly, one of the key issues of accounting is finding the evidence, documentation, approval criteria, among other features. For example, auditing is normally carried out via a sampling technique, which is time-consuming and also leads to potential blindspots. Blockchain could potentially eliminate this task, by providing all available information on the system.

Furthermore, with the traceability of the correct data, accountants will be able to determine and deduce other types of information, such as compliance or even detect anomalies (such as fraud). In other words, accountants recognize the nature of blockchain as a distributed database, which will act as a tool to access the history of a transaction, to have the traceability of a process.

Accountants also frequently highlighted blockchain as a tool that would act as an extra aid to their process. As mentioned, it would help them with the traceability of a process, but it also will improve the availability and reliability of the data and, the efficiency of the data gathering process. As accountant 2 explains it “open the record like this [click] and you’re going to have all the data. You’ll be able to understand immediately”. Hence, the accountant’s views are that, blockchain will not bring "automatization" of the accountant’s job, nor replace its’ role, given that accountancy - as it has already been emphasized - it’s bringing human value and interpretation to raw data.

However, it is of paramount importance to realize that availability and reliability is not guaranteed by blockchain per se, but rather by the technology. Databases, and more generally computers, are available at any time, and communicate with extreme efficiency. The need of a blockchain in a system is not always required, and its inherent complexity can even be a drawback. Especially, when data does not come from multiple sources, or that responsibility of the ownership of data is not disputed, then blockchain is not the best tool to use (Wüst & Gervais, 2017; Yaga, Mell, Roby, & Scarfone, 2019). The flowchart from Yaga et al. is reproduced in Appendix C.

Interestingly, developers have also pointed out that the implementation of the blockchain for accounting will simplify and automate some of the work that both accountants and auditors have to do. However, they didn’t seem to realize that most of the features they mentioned already exist and are widely implemented through ERP software. Developers tend to believe that blockchain will revolutionize the field without having studied which software implementations and automatizations are already out there.

While blockchain is hailed by accountants as a promising tool, interviewees also insisted on the fact that blockchain must prove its resilience before being widely adopted in the public. This conservative stance about new technologies stems from a precaution principle, as information reliability is one of the most important topics for accountants. It thus seems that before blockchain is adopted by the accounting ecosystems, two things must happen. The first one is a clarification of the role of blockchain and its possible use cases, in order to dissipate any misconception that accountants may have. The second one is the trial of time, where a blockchain based system must prove its efficiency and reliability before being handled any critical data.

This view differs dramatically from the one hold by developers, whose main concern relating to blockchain is mainly focus on the programming process, regulations and security. This perspective from blockchain developers emerges as a natural differences from accountants, as their role in the software construction process is rather centered on the technical aspect of system.

In addition, accountants highlighted that they land on a key roadblock that blockchain based system will have to overcome: information that is hosted inside this system must be useful and allow them to draw appropriate conclusions. The parametrization of the information in the system seems to be one of the most important issues for accountants. Given that the core of accountancy is data analysis, it doesn’t come as a surprise that accountants express their concerns over the nature of the data that will be recorded on the blockchain systems. The features that could potentially make blockchain attractive to accountants, such as traceability, availability and reliability of information, will matter very little if the information recorded on the blockchain doesn't represent anything, isn't in the correct format, doesn't comply with legal requirements or in fact, the accountants don't trust it is truthful.

These requirements from accountants need to be carefully understood and dealt with by developers. Gathering what the stakeholders expect, their requirements, is pivotal for the correct construction of the software and should be done from the early stages of the construction of system. In this case, we can conclude that what accountants expectations from a blockchain system isn't shared or understood by the blockchain developers. By reviewing the answers from the blockchain developers, on what they think will be the challenges on adopting blockchain system, none of them mentioned the parametrization of the information or information issues. In fact only developer 1 briefly touches on the parametrization of the information. For example, when querying the word information in NVivo, none of the other developers discuss the importance that information is going to have inside the blockchain, the format, *interalia*. Their focus seems to be on the questions of privacy and/or the tamper-proof nature of blockchain.

Conclusion

This analysis has shown two main outcomes: one, preliminary research results related to the understanding of blockchain technology in accounting and understood effects on the main concepts of trust and transparency; and two, it has highlighted the importance requirement gathering and co-creation, and difficulties in compliance and parametrization.

In terms of other relevant outcomes, firstly, it seems that perception of transparency and trust aren't going to be greatly modified by the implementation of blockchain for accounting. There might be some evolution on these concepts, but the core of them will remain the same.

Secondly, through our analysis of the interviews, we came across that the main concern of accountants regarding blockchain system was the information that would be hosted inside the blockchain: how to minimize the issue of accessing an untruthful source for accounting entries metadata (e.g. who input the data, when, under which pretenses, etc)? This is a socio-technical issue which is directly related to requirement engineering, a process that we had not foreseen to be one of the key issues for blockchain implementation.

Moreover this means that developers should elicit and gather the requirements from accountants, lawyers and tax experts, in order to deliver a software that fulfills their expectations, complies with regulations and international standards, and fulfills its usability purpose. In fact, for requirement gathering, although there are globalizing efforts such as xBRL (XML implementation to define and exchange financial information) and the IFRS (International Financial Reporting Standards), the diversity of legal and technical requirements for integration into current systems is a topic that should be further reflected upon, in particular with the role of smart contracts.

To conclude, further research should be carried out about blockchain implementation, accountancy and software engineering. In this context, we propose some future research questions and reflections that we believe will prove useful for this endeavor:

- What type of model is the best suited to gather requirements from all stakeholders if they do not have previous knowledge of the technology and developers say that it is difficult to explain?

- How do you build robust and reliable systems if the technology is still immature and unexplored in certain aspects?
- How do we surmount the challenge of building blockchain based accounting systems that comply with international standardization efforts (IFRS) and local laws simultaneously?
- How does trust developed in accountancy? What have been the key variables for the adoption of new technologies in accountancy?

References

Adam-npm. (2018, May). Reported malicious module: getcookies. Retrieved August 19, 2019, from https://blog.npmjs.org/post/173526807575/reported-malicious-module-getcookies

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019, April). Blockchain Technology in Healthcare: A Systematic Review. *Healthcare (Basel)*, *7*(2).

Ahangama, S. & Poo, D. C. C. (2016). Credibility of algorithm based decentralized computer networks governing personal finances: the case of cryptocurrency. In *International conference on hci in business, government, and organizations* (pp. 165–176). Springer.

AKKUŞ, Ö. M. (2019, August). CVE-2019-15107. Retrieved August 19, 2019, from https://pentest.com.tr/exploits/DEFCON-Webmin-1920-Unauthenticated-Remote-Command-Execution.html

Attah, E. (2019, May). Five most prolific 51% attacks in crypto: verge, ethereum classic, bitcoin gold, feathercoin, vertcoin. Retrieved August 21, 2019, from https://cryptoslate.com/prolific-51-attacks-crypto-verge-ethereum-classic-bitcoin-gold-feathercoin-vertcoin/

Ball, C. (2009). What is transparency? *Public Integrity*, *11*(4), 293–308. doi:10.2753/PIN1099-9922110400. eprint: https://www.tandfonline.com/doi/pdf/10.2753/PIN1099-9922110400

Barak, B., Goldreich, O., Impagliazzo, R., Rudich, S., Sahai, A., Vadhan, S., & Yang, K. (2001). On the (im)possibility of obfuscating programs. In J. Kilian (Ed.), *Advances in cryptology — crypto 2001* (pp. 1–18). Berlin, Heidelberg: Springer Berlin Heidelberg.

Bartoletti, M. & Pompianu, L. (2017). An empirical analysis of smart contracts: platforms, applications, and design patterns. In M. Brenner, K. Rohloff, J. Bonneau, A. Miller, P. Y. Ryan, V. Teague, . . . M. Jakobsson (Eds.), *Financial cryptography and data security* (pp. 494–509). Cham: Springer International Publishing.

Bauhr, M. & Grimes, M. (2017, November). Transparency to curb corruption? concepts, measures and empirical merit. *Crime, Law and Social Change*, *68*(4), 431–458. doi:10.1007/s10611-017-9695-1

Beckmann, P., Gombert, K., Hoppe, A., Jautz, K., Lindner, M., Roome, J., . . . Theunissen, A. (2012, July). Transparency – more than a buzzword? *MaRBLe*, *1*. doi:10.26481/marble.2012.v1.117

Bernstein, D. J., Lange, T., & Niederhagen, R. (2016). Dual ec: a standardized back door. In P. Y. A. Ryan, D. Naccache, & J.-J. Quisquater (Eds.), *The new codebreakers: essays dedicated to david kahn on the occasion of his 85th birthday* (pp. 256–281). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-662-49301-4_17

Billinghurst, S. (2018, September). "pwc global study shows four out of five executives (84%) surveyed report blockchain initiatives underway". Retrieved from https://www.pwc.com/im/en/media-room/articles/executives-have-blockchain-initiatives-underway.html

Blossey, G., Eisenhardt, J., & Hahn, G. (2019). Blockchain technology in supply chain management: an application perspective. In *Proceedings of the 52nd hawaii international conference on system sciences*.

ceejbot. (2017, August). ‘crossenv‘ malware on the npm registry. Retrieved August 19, 2019, from https://blog.npmjs.org/post/163723642530/crossenv-malware-on-the-npm-registry

Chenhall, R. H. & Langfield-Smith, K. (2003). Performance measurement and reward systems, trust, and strategic change. *Journal of management accounting research*, *15*(1), 117–143.

Dai, J. & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems*, *31*(3), 5–21. doi:10.2308/isys-51804. eprint: https://doi.org/10.2308/isys-51804

Dekker, H. C. (2004). Control of inter-organizational relationships: evidence on appropriation concerns and coordination requirements. *Accounting, organizations and society*, *29*(1), 27–49.

Deloitte. (2016). "blockchain technology. a game-change in accounting?" Retrieved from https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%5C%20game-changer%5C%20in%5C%20accounting.pdf

Deloitte, Canada, C. P. A., AICPA, & UWCISA. (2017). "blockchain technology and its potential impact on the audit and assurance profession". Retrieved from https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain - technology - and - its - potential - impact - on - the - audit - and - assurance - profession.pdf

Dhillon, V., Metcalf, D., & Hooper, M. (2017). The dao hacked. In *Blockchain enabled applications: understand the blockchain ecosystem and how to make it work for you* (pp. 67–78). Berkeley, CA: Apress. doi:10.1007/978-1-4842-3081-7_6

Dolev, D. & Yao, A. C. (1981). On the security of public key protocols. In *Proceedings of the 22nd annual symposium on foundations of computer science* (pp. 350–357). SFCS '81. Washington, DC, USA: IEEE Computer Society. doi:10.1109/SFCS.1981.32

Durumeric, Z., Li, F., Kasten, J., Amann, J., Beekman, J., Payer, M., ... Halderman, J. A. (2014). The matter of heartbleed. In *Proceedings of the 2014 conference on internet measurement conference* (pp. 475–488). IMC '14. Vancouver, BC, Canada: ACM. doi:10.1145/2663716.2663755

Ernst and Young Global. (2018). How blockchain will revolutionize finance and auditing. Retrieved from https://www.ey.com/en_gl/digital/blockchain-why-finance-and-auditing-will-never-be-the-same

Financial Executive International. (2018). Blockchain for financial leaders: opportunity vs. reality. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-fei-blockchain-report-future-hr.pdf

Fligstein, N. (1998). The politics of quantification. *Accounting, Organizations and Society*, *23*(3), 325–331.

Francisco, K. & Swanson, D. (2018). The supply chain has no clothes: technology adoption of blockchain for supply chain transparency. *Logistics*, *2*(1). doi:10.3390/logistics2010002

Fröwis, M. & Böhme, R. (2017). In code we trust? In *Data privacy management, cryptocurrencies and blockchain technology* (pp. 357–372). Springer.

Gambetta, D. et al. (1988). *Trust: making and breaking cooperative relations*. B. Blackwell New York, NY.

Giddens, A. (1979). *Central problems in social theory: action, structure, and contradiction in social analysis*. Univ of California Press.

Giddens, A. (1984). *The constitution of society*. Cambridge: Polity Press.

Giddens, A. (1990). *The consequences of modernity polity*. Cambridge.

Giddens, A. (1991). *Modernity and self-identity: self and society in the late modern age*. Stanford university press.

Given, L. (2008). *The sage encyclopedia of qualitative research methods: a-l ; vol. 2, m-z index*. A Sage Reference Publication. SAGE Publications. Retrieved from https://books.google.ie/books?id=IFrb6IPLISEC

Glaser, F. (2017). Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis.

Gordijn, J., Wieringa, R., Ioniță, D., & Kaya, F. (2019). Towards a sustainable blockchain use case.

Granados, N., Gupta, A., & Kauffman, R. J. (2010, June). Research commentary—information transparency in business-to-consumer markets: concepts, framework, and research agenda. *Info. Sys. Research*, *21*(2), 207–226. doi:10.1287/isre.1090.0249

Greiner, M. & Wang, H. (2015). Trust-free systems-a new research and design direction to handle trust-issues in p2p systems: the case of bitcoin.

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: a literature review on blockchain technology and trust in the sharing economy. *Electronic commerce research and applications*, *29*, 50–63.

Heilman, E., Baldimtsi, F., & Goldberg, S. (2016). Blindly signed contracts: anonymous on-blockchain and off-blockchain bitcoin transactions. In *International conference on financial cryptography and data security* (pp. 43–60). Springer.

@icchyr. (2018, December). Real world ctf 2018 finals. Retrieved August 21, 2019, from https://blog.tonkatsu.info/ctf/2018/12/17/realworldctf-finals.html

International Financial Reporting Standards Foundation. (2018, March). Conceptual framework for financial reporting. Retrieved from https://www.ifrs.org/issued-standards/list-of-standards/conceptual-framework/#about

Jawaheri, A. & Basil, H. (2017). *Deanonymizing tor hidden service users through bitcoin transactions analysis* (Master's thesis).

Leech, B. L. (2002). Asking questions: techniques for semistructured interviews. *PS: Political Science & Politics*, *35*(4), 665–668. doi:10.1017/S1049096502001129

Lewicki, R. J. & Bunker, B. B. (1995). Trust in relationships. *Administrative Science Quarterly*, *5*(1), 583–601.

Lustig, C. & Nardi, B. (2015). Algorithmic authority: the case of bitcoin. In *2015 48th hawaii international conference on system sciences* (pp. 743–752). IEEE.

Maurer, B., Nelms, T. C., & Swartz, L. (2013). "when perhaps the real problem is money itself!": the practical materiality of bitcoin. *Social semiotics*, *23*(2), 261–277.

McKnight, D. H. [D Harrison] & Chervany, N. L. (2000). What is trust? a conceptual analysis and an interdisciplinary model. *AMCIS 2000 Proceedings*, 382.

Michener, G. & Bersch, K. (2013, July). Identifying transparency. *Info. Pol. 18*(3), 233–242. doi:10.3233/IP-130299

Mihajlov, A. (2018, July). Virus in eslint-scope? Retrieved September 19, 2019, from https://github.com/eslint/eslint-scope/issues/39

Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. Retrieved from http://www.bitcoin.org/bitcoin.pdf

Neu, D. (1991). Trust, impression management and the public accounting profession. *Critical Perspectives on Accounting*, *2*(3), 295–313.

Nicolaou, A. I. & McKnight, D. H. [D. Harrison]. (2006). Perceived information quality in data exchanges: effects on risk, trust, and intention to use. *Information Systems Research*, *17*(4), 332–351. Retrieved from http://www.jstor.org/stable/23015810

Nugent, T., Upton, D., & Cimpoesu, M. (2016). Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research*, *5*(2541). doi:10.12688/f1000research.9756.1

Paverd, A., Martin, A., & Brown, I. (2014). Modelling and automatically analysing privacy properties for honest-but-curious adversaries. *University of Oxford, Tech. Rep.*

Perica, R. & Zekić, A. (2019, July). Suppy chain malware - detecting malware in package manager repositories. Retrieved August 19, 2019, from https://blog.reversinglabs.com/blog/suppy-chain-malware-detecting-malware-in-package-manager-repositories

Porter, T. M. (1996). *Trust in numbers: the pursuit of objectivity in science and public life*. Princeton University Press.

Raiser, M. (1999). *Trust in transition*.

Rice, H. G. (1953). Classes of recursively enumerable sets and their decision problems. *Transactions of the American Mathematical Society*, *74*(2), 358–366.

Sartori, G. (1970). Concept misformation in comparative politics. *The American Political Science Review*, *64*(4), 1033–1053. Retrieved from http://www.jstor.org/stable/1958356

Sas, C. & Khairuddin, I. E. (2015). Exploring trust in bitcoin technology: a framework for hci research. In *Proceedings of the annual meeting of the australian special interest group for computer human interaction* (pp. 338–342). ACM.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014, May). Zerocash: decentralized anonymous payments from bitcoin. In *2014 ieee symposium on security and privacy* (pp. 459–474). doi:10.1109/SP.2014.36

Schnackenberg, A. K. & Tomlinson, E. C. (2016). Organizational transparency: a new perspective on managing trust in organization-stakeholder relationships. *Journal of Management*, *42*(7), 1784–1810. doi:10.1177/0149206314525202. eprint: https://doi.org/10.1177/0149206314525202

Scott, D. & Usher, R. (2011). *Researching education: data, methods and theory in educational enquiry*. Continuum Research Methods. Bloomsbury Academic.

Seal, W., Cullen, J., Dunlop, A., Berry, T., & Ahmed, M. (1999). Enacting a european supply chain: a case study on the role of management accounting. *Management Accounting Research*, *10*(3), 303–322.

Strauss, A. & Corbin, J. (1990). *Basics of qualitative research: grounded theory procedures and techniques*. Thousand Oaks, CA, US: Sage Publications, Inc.

Strauss, A. & Corbin, J. (1994). Grounded theory methodology: an overview. In N. Denzin & N. Lincoln (Eds.), *Handbook of qualitative research* (Chap. 17). London: Sage Publications, Inc.

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, *2*(9). doi:10.5210/fm.v2i9.548

Tapscott, A. & Tapscott, D. (2017). How blockchain is changing finance. *Harvard Business Review*, *1*(9), 2–5.

Tapscott, D. & Tapscott, A. (2017). How blockchain will change organizations. *MIT Sloan Management Review*, *58*(2), 10–13. Copyright - Copyright Â© Massachusetts Institute of Technology, 2015. All rights reserved; Last updated - 2018-10-09; CODEN - SMRVAO. Retrieved from https://search.proquest.com/docview/1875399260?accountid=47520

Tomkins, C. (2001). Interdependencies, trust and information in relationships, alliances and networks. *Accounting, organizations and society*, *26*(2), 161–191.

Turing, A. M. (1936). On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, *2*(42), 230–265.

Vosselman, E. & Van der Meer-Kooistra, J. (2009). Accounting for control and trust building in interfirm transactional relationships. *Accounting, Organizations and Society*, *34*(2), 267–283.

Wang, W., Hoang, D. T., Xiong, Z., Niyato, D., Wang, P., Hu, P., & Wen, Y. (2018). A survey on consensus mechanisms and mining management in blockchain networks. *CoRR*, *abs/1805.02707*. arXiv: 1805.02707. Retrieved from http://arxiv.org/abs/1805.02707

Wenceslas, Q. (2018, July). Acroread package compromised. Retrieved August 19, 2019, from https://lists.archlinux.org/pipermail/aur-general/2018-July/034151.html

Wood, G. (2014). Ethereum: a secure decentralised generalised transaction ledger.

Wüst, K. & Gervais, A. (2017). Do you need a blockchain? Cryptology ePrint Archive, Report 2017/375. Accessed: 2017-06-29. Retrieved from http://eprint.iacr.org/2017/375.pdf

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

Yamagishi, T. & Yamagishi, M. (1994). Trust and commitment in the united states and japan. *Motivation and emotion*, *18*(2), 129–166.

Yermack, D. (2017, January). Corporate Governance and Blockchains*. *Review of Finance*, *21*(1), 7–31. doi:10.1093/rof/rfw074. eprint: http://oup.prod.sis.lan/rof/article-pdf/21/1/7/26322010/rfw074.pdf

Zarifis, A., Cheng, X., Dimitriou, S., & Efthymiou, L. (2015). Trust in digital currency enabled transactions model. In *Mcis* (p. 3).

Accountants' tables

Table 1

Codes relating to transparency, by frequency

Accountant	Accuracy of information				Clarity of information			Disclosure of information			
	Standard	Third party role	Traceability	Sub.T	Comprehensible info	Meaningful info	Sub.T	Relevant	Available	Open	Sub.T
#1	0	0	0	0	0	0	0	0	0	1	1
#2	0	0	7	7	0	4	4	0	2	0	2
#3	0	0	1	1	0	0	0	0	2	1	3
#4	0	0	0	0	0	3	3	1	1	2	4
#5	0	0	3	3	1	2	3	0	0	0	0
#6	1	3	0	4	1	1	2	0	0	2	2
#7 and #8	1	2	0	3	0	2	2	1	1	1	3
Sub total	2	5	11	**18**	2	12	**14**	2	6	7	**15**

Table 2

Other codes related to transparency, by proof of existence

Accountant	Technical issues	N: knowing how the system works
#1	X	X
#2	-	-
#3	-	-
#4	-	-
#5	-	-
#6	-	-
#7 and #8	X	-

Table 3

Accountant's perception on how blockchain might affect accounting, by code frequency

Accountant	Efficiency and speed	Information availability, reliability	Less human errrors	Real-time accounting	Shift of trust towards technology	Tamper-proof	Tool	Traceability	Total
#1	0	1	0	1	3	0	1	2	8
#2	3	3	0	0	0	1	5	6	18
#3	3	3	1	2	0	4	1	1	15
#4	0	0	0	1	3	0	0	1	5
#5	2	1	2	0	2	0	2	3	12
#6	0	0	0	0	0	0	0	0	0
#7 and #8	0	5	0	0	1	2	3	3	14
Total	8	13	3	4	9	7	12	16	**72**

Table 4

Accountant's perception on the challenges when adopting blockchain based accounting systems, by frequency

Accountant	Cost problems	Information inside the BC (req.)	Requirements	Tools already exist	Trust issue and testing	Total
#1	0	0	0	0	0	0
#2	0	6	6	0	0	12
#3	0	0	0	0	0	0
#4	1	2	2	0	1	6
#5	0	0	0	1	2	3
#6	0	2	0	0	2	4
#7 and #8	0	1	0	1	0	2
Total	1	11	8	2	5	**27**

Table 5

Accountants' perception of what will not change with blockchain, by frequency

Accountant	Accounting is information	Human analysis	Human value	No change of trust	No shift	Total
#1	0	0	0	1	0	1
#2	0	4	2	0	0	6
#3	1	0	0	0	0	1
#4	0	3	0	1	0	4
#5	0	0	1	0	1	2
#6	0	0	0	0	0	0
#7 and #8	0	2	0	1	1	4
Total	1	9	3	3	2	**18**

Table 6

Accountants' definition of trust or concepts that contribute to trust, by frequency

Accountant	Accuracy	Complete information	Critical analysis	Standarisation	Personal trust	Reliability	Reputation	Tamper proof	Total
#1	0	0	0	1	0	1	0	1	3
#2	0	0	0	1	0	0	0	0	1
#3	0	0	0	0	0	2	0	1	3
#4	0	1	1	0	0	0	1	0	3
#5	1	2	2	2	0	0	1	0	8
#6	0	1	1	0	1	2	2	0	7
#7 and #8	0	0	2	1	0	1	0	0	4
Total	1	4	6	5	1	6	4	2	**29**

Developers' tables

Table 7

Identified codes that developers expressed when defining transparency, by frequency

Developer	Accuracy of information				Clarity of information			Disclosure of information			
	Standard	Third party role	Traceability	Sub.T	Comprehensible info	Meaningful info	Sub.T	Relevent	Availability	Openness	Sub.T
#1 (and PM)	0	0	1	1	4	2	6	0	0	1	1
#2	0	0	0	0	0	1	1	1	1	1	3
#3 (and PM)	0	0	3	3	0	0	0	0	0	1	1
#4	0	0	3	3	0	0	0	0	0	1	1
#5 (and PM)	0	0	0	0	0	0	0	0	1	1	2
#6 (and PM)	0	0	2	2	0	0	0	0	0	0	0
#7	0	1	0	1	0	0	0	0	0	0	0
Sub total	0	1	9	**10**	4	3	**7**	3	4	5	12

Table 8

Other codes related to transparency from developers, by proof of existence

Developer	Other topics			Technical aspect providing transparency					Trust and transparency					
	Trust	Decentralization	Sub.T.	Knowledge on how it works	Smart contracts	System design (blockchain)	Protocol	Sub.T.	Trust w/o transparency	Techn. trust that allows transparency	Transparency by trustless systems	Trust protocol for transparency	Trust on system	Sub.T.
#1	-	-	0	-	-	-	-	0	-	-	-	-	-	0
#2	-	-	0	-	-	-	-	0	-	-	-	-	-	0
#3	-	-	0	-	-	X	X	2	-	-	-	-	-	0
#4	-	-	0	-	-	-	-	0	X	-	-	-	-	1
#5	-	X	1	X	-	-	X	2	-	-	-	X	X	2
#6	-	-	0	-	-	-	-	0	-	-	-	-	-	0
#7	X	-	1	-	X	-	-	1	X	-	X	-	-	2
Sub total	1	1	**2**	1	1	1	2	**5**	2	0	1	1	1	**6**

Table 9

Developer's difficulties when explaining blockchain, by frequency

Developer	Blockchain = cryptocurrency	Difficult for technical to explain to non-tech	Overfantasize	People don't understand	Skeptical	Smart contract misunderstanding	Total
#1	0	0	5	0	0	1	6
#2	2	2	0	2	0	0	6
#3	2	0	0	1	2	0	5
#4	0	1	3	2	0	0	6
#5	1	1	0	2	0	0	4
#6	0	0	0	0	1	0	1
#7	0	0	2	0	0	0	2
Total	5	4	10	7	3	1	**30**

Table 10

Developer's opinion on how blockchain might affect accounting

Developer	Automatization	Control over data	Decentralization	Efficiency and faster	Facilitate auditing	Improvement	Information availability, reliability	Solve transparency	Solve future trust	Tool	Traceability	Total
#1	0	0	2	0	0	0	2	1	0	0	5	10
#2	1	0	1	0	0	0	0	0	0	0	0	2
#3	3	0	0	1	1	0	0	2	3	2	2	14
#4	0	0	0	0	0	0	0	0	4	1	0	5
#5	1	0	0	2	1	2	3	0	0	2	2	13
#6	0	2	1	0	0	0	0	0	3	0	0	6
#7	0	1	1	0	0	0	0	0	0	0	0	2
Total	5	3	5	3	2	2	5	3	10	5	9	**52**

Table 11

Developers' perceptions of the challenges linked to the adoption of blockchain, by frequency

Dev	Fashion fad (no objective)	Privacy and legal	Security	Technical challenges	Trust on the BC	Total
#1	1	3	0	1	0	5
#2	1	0	0	1	2	4
#3	0	0	0	1	2	2
#4	0	0	1	0	0	1
#5	0	0	1	2	0	3
#6	0	0	2	0	1	3
#7	2	2	2	1	1	8
Total	4	5	6	6	6	**26**

Table 12

Developers' definition of trust or concepts that contribute to trust, by frequency

Developer	Certification of input	Consensus	Correct transmission	Functionality	Reliability	Traceability	Total
#1	0	1	1	0	0	1	3
#2	1	1	1	0	1	0	4
#3	0	1	0	2	0	1	4
#4	0	1	0	2	0	0	3
#5	2	1	0	2	2	1	8
#6	0	1	0	2	0	0	3
#7	1	1	1	1	2	1	7
Total	4	7	3	9	5	4	**32**

Annex A
Methodology

The core questions that where asked to both groups where the following:

- **What is your definition of trust?** The objective of this question was to discover the definition of trust of the intervewees. Furthermore, it gives us insight of the attitude of the respondants towards this issue.
- **"Blockchain isn't the end of trust, it is the future of trust". What is your opinion on that phrase?** This question is for further eliciting the definition of trust of respondants, in an indirect way. At the same time, we can also start gathering the perception on how blockchain might affect trust.
- **What is the link between blockchain and trust?** The goal is to understand directly if intervewees perceived there will be a change in the concept of trust due to blockchain
- **What issues can blockchain address? How and why?** Gather what are the areas or challenges that interviewees think blockchain might address, either in a positive or negative fashion.
- **What does the word transparency mean to you?** Same as first question.

The aforementioned questions were created to understand the three main areas of research of this study.

To blockchain developer, we added the following questions:

- **What has been your experience with non-blockchain people, when implementing blockchain systems?** Discover possible challenges when building blockchain system.
- **What have been your problems when implementing blockchain systems?** Discover what are the current issues when building the blockchain system, extrapolate them to accounting system. Reinforcement of the previous question.

For accountants we added the following questions:

- **Do you think blockchain will affect accounting? Why? If so, how?** Gather what accountants are expecting from blockchain systems (requirements) and what are the important elements to consider when building such systems.
- **What are the problems that the blockchain could address in the field of accounting? How?** Same as above.

Annex B
Interview Results

Interviewee	Status	Source	Saturation	Format	Length	Recording	Transcript
Blockchain Developer			**Partial**				
Developer 1 and project manager	Conducted in person 23/10/19	Sample frame		Semi-structured	25 mins	Audio recording, concurrent notes	Confidentiality required
Developer 2	Conducted in person 27/10/19	Sample frame		Semi-structured	22 mins	Audio recording, concurrent notes	Confidentiality required
Developer 3 and project manager	Conducted in person 27/10/19	Sample frame		Semi-structured	29 mins	Audio recording, concurrent notes	Confidentiality required
Developer 4	Conducted in person 18/11/19	Sample frame		Semi-structured	24 mins	Audio recording	Confidentiality required
Developer 5 and project manager 19/11/19	Conducted in person	Sample frame		Semi-structured	27 mins	Audio recording, concurrent notes	Confidentiality required
Developer 6 and professor	Conducted by skype 19/11/19	Sample frame		Semi-structured	20 mins	Audio recording	Confidentiality required
Developer 7 and post-doc student	Conducted by skype, 21/11/19	Referred by Developer 6 and professor		Semi-structured	25 mins	Audio recording	Confidentiality required
Developer 8	Refused 14/11/19	Sample frame					

Table B1

Developers interview modalities

Interviewee	Status	Source	Saturation	Format	Length	Recording	Transcript
Chartered Accountants			**High**				
Accountant 1	Conducted in person, 04/11/19	Sample frame		Semi-structured	17 mins	Audio recording, concurrent notes	Confidentiality required
Accountant 2 and professor	Conducted by skype, 07/11/19	Sample frame		Semi-structured	35 mins	Audio recording, concurrent notes	Confidentiality required
Accountant 3	Conducted by phone 14/11/19	Sample frame		Semi-structured	28 mins	Audio recording	Confidentiality required
Accountant 4 and professor	Conducted in person 14/11/19	Sample frame		Semi-structured	21 mins	Audio recording	Confidentiality required
Accountant 5	Conducted in person 13/11/19	Sample frame		Semi-structured	26 mins	Audio recording	Confidentiality required
Accountant 6	Conducted by phone 15/11/19	Sample frame		Semi-structured	37 mins	Audio recording	Confidentiality required
Accountant 7 and 8	Conducted by phone 21/11/19 and in conjuction	Sample frame		Semi-structured	23 mins	Audio recording	Confidentiality required

Table B2

Accountants interview modalities

Annex C
DHS's flowchart

This annex reproduces the flowchart made by the US Department of Homeland Security (DHS) Science & Technology Directorate, about the need of a blockchain in a system. This flowchart was published by the DHS, then republished by Yaga et al. (2019), which we reproduce here.

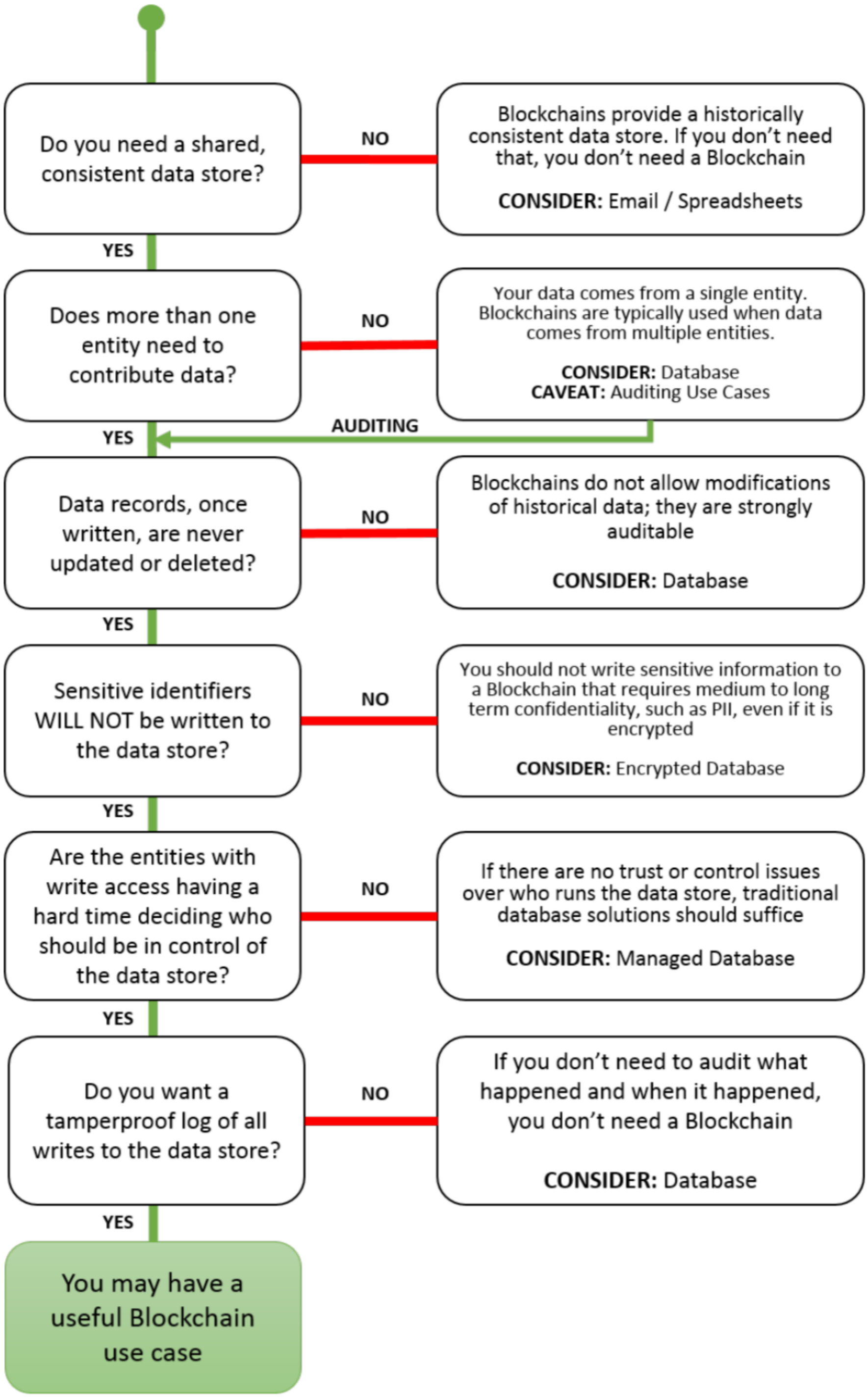
Do you need a shared, consistent data store?
NO
Blockchains provide a historically consistent data store. If you don't need that, you don't need a Blockchain
CONSIDER: Email / Spreadsheets
YES
Does more than one entity need to contribute data?
NO
Your data comes from a single entity. Blockchains are typically used when data comes from multiple entities.
CONSIDER: Database
CAVEAT: Auditing Use Cases
AUDITING
YES
Data records, once written, are never updated or deleted?
NO
Blockchains do not allow modifications of historical data; they are strongly auditable
CONSIDER: Database
YES
Sensitive identifiers WILL NOT be written to the data store?
NO
You should not write sensitive information to a Blockchain that requires medium to long term confidentiality, such as PII, even if it is encrypted
CONSIDER: Encrypted Database
YES
Are the entities with write access having a hard time deciding who should be in control of the data store?
NO
If there are no trust or control issues over who runs the data store, traditional database solutions should suffice
CONSIDER: Managed Database
YES
Do you want a tamperproof log of all writes to the data store?
NO
If you don't need to audit what happened and when it happened, you don't need a Blockchain
CONSIDER: Database
YES
You may have a useful Blockchain use case

Figure C1. DHS' flowchart about the need of a blockchain