Technology in Society 62 (2020) 101298

Contents lists available at ScienceDirect

Technology in Society

journal homepage: www.elsevier.com/locate/techsoc

Blockchain for trustworthy provenances: A case study in the Australian aquaculture industry

Robert Garrard [*,1], Simon Fielke[1]

CSIRO, Land & Water, EcoSciences Precinct, GPO Box 2583, Brisbane, 4001, Qld, Australia

ARTICLE INFO

Keywords:
Blockchain
Provenance
Traceability
Trust
Aquaculture

ABSTRACT

We explore the potential for a blockchain ledger to record supply chain provenances in an inherently trustworthy manner. The use of blockchain in this setting may allow for traceability of products through the supply chain without fear that an item's provenance is fraudulent or has been tampered with. We compare the desirable properties of a blockchain ledger to those of a traditional database. We also consider challenges to the trustworthiness of a provenance idiosyncratic to the context of supply chains. We present a case study in which we conduct a series of semi-structured interviews with members of the prawn aquaculture industry in Australia. This industry was chosen as it stands to gain from robust provenances due to international competition. We find that blockchain based technology is unlikely to deliver substantial gains to the industry when compared to alternatives. Rather, most gains are likely to arise from the industry becoming digitalized, which would be a precondition for any blockchain technology to be operational.

1. Introduction

Consumer sovereignty is an economic doctrine in which the consumer is able to affect which goods and services are produced by way of voting with their dollars [1]. Those goods and services which the consumer finds preferable attract higher expenditure, which incentivizes producers to shift production towards that which is most desired. Common knowledge regarding the characteristics of a good or service, such as its quality, price, and other relevant attributes, is an essential precondition for consumer sovereignty to successfully promote the welfare of the consumer. Situations in which relevant information is concealed from consumers can lead to lower overall consumer welfare; or in extreme cases, market failures [2]. For some consumers, information regarding the provenance, or origin and journey through the supply chain, of certain goods is particularly important. This may be for concerns regarding food safety [3] or for preferences aligning with a consumer's view of ethical environmental and social practices [4–7]. Producers themselves may be incentivized to promote traceability for the purposes of branding and product differentiation, communication of certifications from consumer advocates, and to increase responsiveness to biosecurity threats [8–10].

The issue surrounding supply chain provenances is fundamentally one of trust. Certain products may be considered as having valuable qualities that are not directly observable to the consumer; such as a work of art being the original composition, or food grown without the use of particular pesticides. Since the consumer is unable to verify these qualities personally, they are forced to rely either on the honesty of the vendor, who may have considerable economic motivation to defraud the consumer [11], or on certifications attached to the object. Current solutions for improving traceability, at least partially through the supply chain, include QR barcodes [12], RFID tagging [13–15], DNA barcoding [16], or a combination thereof [17]. While some traceability applications allow for provenance data to be given directly to the end consumer, others only track a product through a subset of agents in the supply chain, requiring consumers to maintain an element of trust. It has been suggested that blockchain may be the technology instrumental in securing traceability throughout the supply chain [18–20] as well as being a disruptive and transformational technology in general [21–27].

A blockchain is a type of distributed ledger; a record of transactions not administered by a trusted central authority. Rather, each user within the blockchain network has a personal copy of the ledger, which they may modify freely, and for which a protocol is in place for updating these ledgers so that all agents within the network may come to consensus on the same ledger. Blockchain was proposed by Nakamoto [28] to overcome a problem faced by purely digital currencies that have a distributed ledger; namely, that users may attempt to repeatedly re-spend the same piece of currency. The key to preventing a user from double-spending their currency is that it must be extraordinarily difficult for that user to convince others in the network to modify old

[*] Corresponding author.
E-mail address: robert.garrard@csiro.au (R. Garrard).
[1] Both authors contributed equally in all aspects of the paper.

https://doi.org/10.1016/j.techsoc.2020.101298
Received 18 September 2019; Received in revised form 3 June 2020; Accepted 17 June 2020
Available online 20 June 2020

entries in their ledgers, while still being comparatively easy to append new transactions to the ledger. For the Bitcoin ledger, this is achieved through "mining"; a process in which a difficult mathematical problem must be solved in order to add a block to the blockchain.

This feature gives a blockchain ledger properties which may be considered desirable. Once a transaction has been recorded, it is virtually impossible to remove, modify, or obscure. This transparency and immutability allows such a ledger to perform its function in an environment that is free of the need to trust a potentially corruptible third-party to execute their stewardship of the ledger honestly. Blockchains are not limited to storing only transaction data for digital currencies, but may also serve as an alternative to any shared database in general. With such a ledger storing the set of transactions in a supply chain, a consumer, or any other agent along the supply chain, could potentially know the entire history of a product's movements in a way which is fundamentally trustworthy by design.

In this article we explore the value proposition for the use of blockchain ledgers in the context of supply chains. We consider blockchain applications as being partitioned into two types: those where a cryptocurrency is an integral feature, such as blockchains used for financial transactions and the execution of smart contracts; and those where the blockchain is used only as a store of information and features no cryptocurrency. Here we consider the latter type. Throughout the article we focus on the use of blockchains specifically to store supply chain provenances, but the analysis extends to information in general; such as sensor data, life cycle analysis data, news articles, video, etc.

We argue that although a blockchain ledger may be appropriate in many settings, the storage of supply chain transactions in a public blockchain ledger is unlikely to lead to significant value added due to gains from trust. Rather than being a disruptive and transformational technology in this setting, we see blockchain as offering at most incremental benefits. To measure the potential value of a blockchain solution it is necessary to compare it not to the status quo, but to the *next best alternative* solution. We compare the potential benefits of a blockchain ledger to those of a traditional centralized database for storing provenances. Furthermore, we examine some issues surrounding traceability within supply chains not present for other settings, such as provenances for online data sets. There are as yet unanswered questions surrounding the visibility of transactions and the honesty of data to be potentially entered into a blockchain. The potential for non-entry, or entry of fraudulent data presents a bottleneck to the trustworthiness of a provenance irrespective of the robustness of the ledger in which it is stored.

We present a case study regarding prawn aquaculture in Australia. A series of interviews were conducted with members of the prawn value chain with the explicit objective of understanding the nature of trust within the supply chain as well as exploring the possibility for a blockchain solution to add value to the industry. A common theme throughout the interviews is that the most urgent need for progress is in the areas of biosecurity and productivity. While trust and traceability were presented as important elements of the supply chain, low cost solutions appear to have already emerged. With respect to trust, the overall trend appears to be towards the tightening of social circles and the concentration of business interactions to within a small set of central players. Traceability within the supply chain appears to have been partially solved by a barcoding system, with provenance information being fragmented at the prawn farm. As biosecurity threats are a major hazard to the prawn industry, one would expect that members of the supply chain would be well incentivized to trace the origin of their products. Prawn farmers express the desire to inform the end consumer of their product's provenance for the purpose of branding, but any attempt to differentiate their product would be undone by the retailer, as fresh prawns from many farms are pooled together before being sold to the consumer. An especially interesting result is that many of the interviewees appear to be aware of blockchain and held attitudes towards blockchain that were overwhelmingly positive. However, participants were unclear on precisely what a blockchain ledger does and what the implications for financial privacy of producers might be.

This paper attempts to make the assumptions underlying blockchain technology explicit by discussing, in concert with prawn aquaculture supply chain stakeholders, what the actual technology entails and therefore shedding light on potential drawbacks in application of such new and hyped technologies. [29] For example, responsible innovation frameworks have been argued to address some of the ethical concerns relating to new technologies, previous work in the precision health domain has highlighted the challenges of such distributed innovation processes in our modern world [30]. It is critical that the development of technological hype alongside technologies (such as those referred to as 'blockchain') is not seen as separate from the systems (societies, communities and individuals) that will be influenced by the development of such technologies [31]. As such we examine, utilizing in-depth qualitative methods, the influence of technological development and associated underlying values in the nascent stage of development as it contributes to industry perceptions in this case study [32].

In Section 2 we explore the differences between blockchain ledgers and traditional databases for storing provenance information. Section 3 considers issues related to obtaining trustworthy provenance data idiosyncratic to the supply chain setting. Section 4 describes a case study undertaken in the prawn supply chain, and Section 5 concludes.

2. Ledgers and traceability

Assuming that a set of trustworthy provenance data is available, in what fashion ought this data be stored? In particular, who may *read* the data, and who may *write* new data to the data set. If the objective is to provide information to the consumer, then the data must be stored in such a way that it is readable by the general public. An important difference between a blockchain ledger and a standard database is how the ability to write entries to the data is managed. A standard database is typically stored in one location and controlled by an administrator who may grant privileges to read and write data to users at their discretion. A blockchain ledger, on the other hand, has multiple identical copies stored across a network of computers. By design, a blockchain ledger is not administered by any one agent and any member of the network may read the ledger and write to it. However, to ensure that each of the disparately stored copies of the ledger remain identical, writing new data to the ledger must be done through a 'consensus mechanism', which usually involves the requirement that users wanting to submit new blocks to the chain must first perform a difficult task which may be verified by the rest of the network. Additionally, blockchain ledgers are 'append only', in that new data may be added to the ledger, but existing data in the ledger may not be modified or deleted. This is in contrast to standard databases which typically allow for entries to be overwritten with updated information.

We next provide a brief description of blockchain ledgers and compare them to a typical relational database.

2.1. Blockchain

Nakamoto [28] developed the blockchain mechanism in order to establish the cryptocurrency Bitcoin. Digital currencies require a record of transactions to be kept in a ledger in order to determine how much currency each agent has, and hence how much they are able to spend. This is in contrast to cash, which is a bearer instrument; you may spend any currency that is in your physical possession. Transactions that use non-physical currency, such as deposits at banking institutions, require the validity of the transaction to be checked against a ledger. This ledger is administered by a third-party, usually a banking institution, who has the sole privilege of reading from and writing to the ledger. A blockchain ledger, on the other hand, is not administered by any third-party. Each agent participating in the Bitcoin network may read the entire history of transactions and may propose new additions to the ledger. This ability for any agent to propose changes to the ledger poses a double-spending problem; an agent may submit a transaction transferring a Bitcoin to one person, and then submit another transaction attempting to transfer that same Bitcoin to a different person. For a distributed digital currency to avoid double-spending, it must solve two problems: (a) transactions must be stored in order, and (b) everybody must agree to update their copy of the ledger in the same way.

Ordering the transactions establishes a line of succession for the possession of each Bitcoin. When somebody attempts to spend a Bitcoin, the ledger may be consulted to verify that they *currently* possess that Bitcoin and have not already spent it in the past. If they have already spent that Bitcoin, the transaction may be deemed invalid and not added to the ledger. The natural way to order a set of transactions is to simply use the *time* at which the transactions occurred. However, timestamps are easily forged, so it is not reliable to order transactions by times self-reported by the agent submitting the transaction. The novelty behind blockchain is that transactions may be ordered without having to appeal to the concept of time. Rather than storing the entire history of transactions in a simple list, small sets of transactions are grouped together into *blocks* which are then chained together in sequence. In this setup, one transaction comes "before" another transaction if it is stored in a previous block.[2] In fact, Nakamoto [28] did not coin the phrase blockchain to refer to this setup; they referred to it as a "timestamp server" using a "chain of blocks".

In order for everybody to possess an identical copy of the ledger, there needs to be a mechanism for establishing consensus regarding whether or not to add a proposed block. Nakamoto [28] exploits a mechanism called *proof-of-work* [33–35], which requires the agent proposing a new block to perform a mathematical task that's difficult to achieve, but easy to verify.[3] If an agent wants to convince other members of the network to attach a block to the blockchain, they must perform a proof-of-work on characteristics of the block. This process is referred to as *mining*. That block gets transmitted to other members of the network who attach it to their blockchain if the proof-of-work is valid. This mechanism is what endows a blockchain with immutability. No data in older blocks may be tampered with or removed otherwise it would invalidate the proof-of-work for those, and all subsequent blocks.

Blockchain has garnered much admiration due to its many desirable properties. It is immutable, data entered can never be changed or removed[4]; auditable, anybody may observe the entire history of transactions; and decentralized, no one party must be trusted to honestly administer the ledger. Additionally, the data stored in the blockchain need not be currency transactions; any data may be stored in the blocks, including supply chain provenances.

2.2. Proof-of-work and energy consumption

Performing the proof-of-work to create a new block is costly to individuals in the network. They must dedicate electricity and compute time to solving the proof-of-work, but the probability that they will be the first person in the network to solve it, and hence be the one to create the next block, it is quite low. In order to incentivize the mining of new blocks, a reward of newly created Bitcoin is awarded to the person who successfully solves the proof-of-work first. At the time of writing, 12.5 Bitcoin (the current reward) is worth approximately US $120,000, which offers a substantial incentive to mine blocks. The reward for mining a block halves every 210,000 blocks, ultimately leading to a maximum creation of 21 million Bitcoins. As the reward decreases (eventually to zero), mining will be incentivized through transaction fees equipped to each Bitcoin transaction.

Rather than using standard CPUs in a desktop computer to perform the proof-of-work, a typical Bitcoin mining rig will likely use Application Specific Integrated Circuits (ASICs). While CPUs are very versatile processors, that versatility comes at the price of being relatively slow. ASICs are processors specifically designed to perform a particular task quickly and efficiently. Despite the relative efficiency of the hardware used to mine Bitcoin, O'Dwyer and Malone [36] estimated that the total energy used by the Bitcoin system is comparable to that used by Ireland as a whole at the time of their study.

The price of Bitcoin, and hence return to mining, has increased dramatically since that estimate was produced. The website digiconomist.net estimates the current energy consumption of the Bitcoin network to be 57 tera-watt hours per year, approximately what is consumed by Bangladesh, and estimate the annual global cost of Bitcoin mining to be $2.8 trillion. They frame this estimate in a rather startling way: the electricity required to mine a single Bitcoin transaction could power 19 US households for a day, and releases 270 kg of carbon dioxide into the atmosphere (27 megatons annually). Stoll et al. [37] finds a similar figure of 22 megatons per year as of 2019.

Alternative consensus algorithms that do not consume as much electricity, such as proof-of-stake and proof-of-space, have been proposed. However, all consensus protocols require that mining new blocks be a costly process for the miner. For a supply chain to operate any kind of public blockchain, block miners must be compensated to incentivize the mining of new blocks.

2.3. Private blockchains

The Bitcoin blockchain, described above, is an example of a public blockchain; anybody may join the network, read from the ledger, or write transactions to it. Private, or permissioned, blockchains on the other hand are usually administered by a single entity, such as a business, or a consortium of entities, which may grant reading and writing privileges to whomever they choose. This type of blockchain is more conducive to maintaining privacy, and since it is administered by a central authority, no proof-of-work is necessary to achieve consensus. However, without the consensus mechanism that makes blockchain novel, this system is not remarkably different from a typical "shared database", whether or not it happens to be stored as a chain of blocks. Furthermore, if the goal is to elucidate provenances in a way which is fundamentally trustworthy by design, a private blockchain defeats the purpose of considering a blockchain solution to begin with. The value of considering a blockchain-like distributed ledger is that no central authority is required to be trusted not to tamper with the ledger. The nature of the proof-of-work mechanism allows for the ledger to be trusted *without* a central authority and *despite* attackers actively trying to modify it.

As well as fully centralized or decentralized blockchains, the ledger may be partially centralized/decentralized with, for example, permissionless reading of the ledger but only a subset of agents able to write (mine) blocks. See Xu et al. [38] for a comparison of the various blockchain architectures.

In the following subsection we compare features of a traditional database to those of a fully decentralized (public) blockchain. We do not explore partially centralized blockchains, which can produce a mixture of the properties below, because of the large number of possible architectures. However, one can broadly categorize partially centralized blockchains into those where entries are written by a single authority (either through sole write permission or having at least 50% of the network's compute power), which are more similar to the traditional database; and those where entries are written through a consensus algorithm, which are more similar to the fully decentralized blockchain.

[2] Note that there is no ordering between the transactions *within* each block, and so it must be verified that no two transactions within a block conflict with each other.

[3] As a very simple example, suppose you're asked to find two numbers which multiply to 143. Finding those numbers may be time consuming, but being asked to verify that 11 and 13 multiply to 143 can be done relatively quickly.

[4] Strictly speaking, it will not be changed or removed with very high probability.

Table 1
Comparison of public blockchains and relational databases against a set of desirable characteristics. Scale of one to three stars, unfilled stars represent half-stars.

	Blockchain	Relational database
Decentralization	★★★	☆
Immutability	★★★	★
Confidentiality	★	★★★
Write Speed	☆	★★★
Robustness	★★★	★☆
Querying	★☆	★★★

2.4. Comparison of blockchain and traditional databases

If the provenance data were not to be stored in a blockchain, how else might it be stored? A common database architecture is the *relational database* [39]. Relational databases store data in a row/column format, similar to a spreadsheet or table. Each row corresponds to an item and columns represent a set of attributes to which the item is related. For example, a row could be a transaction that takes place in the supply chain and its columns may include the actor transferring an object, the actor receiving it, the type of object being exchanged, the payment amount, etc. As a common architecture that is cheap to administer, we use this as a point of comparison to blockchains. Table 1 provides a summary against a set of desirable characteristics for a database to possess.

Decentralization. Blockchains are maximally decentralized for both storage and read/write permissions. Every actor in the blockchain network stores a copy of the ledger locally.[5] Every actor in the network may read from the ledger freely and may attempt to write new blocks to the ledger. No actor in the network is treated preferentially to any other actor. Relational databases tend to be administered by one centralized authority who may grant read/write privileges at their discretion, though they typically retain sole write privileges. Furthermore, the database tends to be stored centrally on a server owned by the administrator.

Immutability. For a proposed block to be attached to the blockchain a valid proof-of-work must be performed. For a given block, the time to perform this proof-of-work may be very long or relatively quick. Many actors in the network are continually forming blocks and attempting to perform the proof-of-work, so there is no guarantee that a particular block a miner is working on will make it into the blockchain, since somebody else may perform their proof-of-work faster. If a bad actor wanted to modify old entries in the blockchain, that modification would invalidate the proof-of-work for the block the entry is contained in, as well as all subsequent blocks. The actor would have to recompute the proof-of-work for that block, and all subsequent blocks, in order to have a valid chain that would be accepted by other agents in the network, and compute the proof-of-work for a new block in order to make the chain longer. While this is not technically impossible to do, the hardness of the proof-of-work is set so that the rate of new block creation easily out-paces the ability of an attacker to recompute the proofs-of-work with *very high probability*.[6] Once an entry has been in the blockchain for sufficient time there is effectively zero chance of it being modified in any way. This is in contrast to a typical relational database, for which the administrator may modify, delete, or amend entries at will. However, some degree of immutability may be built into more traditional databases, such as Google Cloud.[7]

Confidentiality. The ability of an agent to read from a relational database is at the discretion of the administrator. The administrator has the capacity to allow the database to be read by the general public, a select few agents, or retain sole read privileges for themselves. Furthermore, the administrator may grant read privileges to an agent temporarily and then revoke them at a later date. Public blockchain ledgers are readable to everybody, since everybody in the network may have a copy of the complete ledger. It is possible for an agent to submit data to the blockchain in an encrypted form so that only those who possess the decryption key may read it. The agent may then distribute that key to whomever they wish to have access. However, once access is granted it cannot be revoked. Furthermore, if the key is made public, such as through accident or theft, then anybody in the network may read the encrypted data. By the immutability of the blockchain ledger, that data cannot be removed. This is in contrast to a relational database, in which the administrator may remove compromised data.

Write Speed. Once data has been designated for storage in the ledger/database, how long does it take to be recorded? Relational databases can have large amounts of data be written to them extraordinarily quickly. The agent wishing to write data to the database connects to the server and their identity is authenticated. Once the connection is open, they may write as much data as they like without having to be constantly re-authenticated. For each submission an agent wishes to write to a blockchain, they must use a cryptographic signature to authenticate their identity and may be limited in the amount of data that may stored in a block.[8] The data submitted to the network must be bundled into a block by a miner, and a valid proof-of-work successfully found before it may be transmitted through the network and attached to each agent's blockchain. For public blockchains, the proof-of-work needs to be sufficiently hard to prevent attackers from tampering with the blockchain, but this restricts the rate at which new blocks may be found. The Bitcoin network recalibrates every 2016 blocks to maintain a block discovery rate of approximately one block every ten minutes. The speed of block creation does *not* depend on the quantity of traffic attempting to be written to the blockchain. Therefore there may be large lags between when data is submitted and when data finally makes it into the blockchain. Bitcoin transactions often include transaction fees which incentivize miners to group some transactions into blocks more promptly than others.

Robustness. Blockchains have an extraordinary amount of redundancy since each agent in the network possesses a copy of the ledger. If one agent loses their copy of the blockchain it is extremely easy to obtain another copy from any of the agents in the network. Furthermore, it is robust to errors in transmission of the data due to its use of cryptographic hash functions. These allow miners to check for corrupted data, which if detected will cause the transaction to be rejected and need the uncorrupted data to be resent. Relational databases are typically stored in localized servers, which are susceptible to faults which may cause data to be permanently lost. Since this is well known, redundancy can be engineered into the storage of important information, such as by having multiple servers store identical copies of the data at different locations.

Querying. Once the data is stored it is usually necessary to be able to access relevant data conveniently. The data desired to be accessed may follow a complex rule, such as "all transactions after January but before April that involve wheat or cattle". Manipulating the data in this way is relatively easy for relational databases which usually may be queried using a language akin to the Structured Query Language (SQL). Blockchain ledgers are more difficult to query efficiently as such languages are not yet widespread, although they are currently being researched [40]. However, blockchain storage does make it extremely easy to determine the history of possession of an object, since transaction entries must point to the previous entry in which the object was transferred to its current owner.

[5] Note that actors in the blockchain network may be either full nodes or partial nodes. A full node stores the blockchain ledger in its entirety. Partial nodes store the ledger in a compressed form, keeping the chain of blocks but not retaining all of the transactions contained within them.

[6] This is with the caveat that the attacker controls less than 50% of the total compute power in the network.

[7] https://cloudplatform.googleblog.com/2016/08/building-immutable-entities-into-Google-Cloud-Datastore.html.

[8] For the Bitcoin blockchain this limit is 1 megabyte.

The key differences are that public blockchains are fully decentralized, immutable, and robust to a wide variety of failures, whereas traditional databases are easy to query, can have large amounts of data written to them quickly, and if necessary can be made confidential. Partially decentralized blockchains meet somewhere in the middle, trading off some decentralization and immutability for gains in confidentiality and the speed of writing. Fully decentralized public blockchains require no trust in some third-party to administer the ledger honestly, whereas traditional databases and partially decentralized blockchains require some faith that the agents administering them will not compromise the data or exploit their stewardship over it for personal gain.

3. Supply chain provenances

Aside from the question regarding which architecture is appropriate for the ledger/database, there are also issues idiosyncratic to the context of supply chains and securing traceability therein. In this section we examine some of the challenges that need to be addressed for obtaining trustworthy provenances which exist independently of how these provenances will be stored.

3.1. Coordination

Before a transaction may be submitted to a database, it must first be recorded in a form that permits such a submission. Digitizing transaction data is entirely feasible, for example, through the use of RFID tags, barcodes, and scanners [41,42]. However, in order for an object to be completely traceable through the supply chain, such recording would have to take place each time possession of the object is transferred to another member of the supply chain. Since the ultimate goal is to have each transaction recorded in a database viewable by both the supply chain itself and the end consumer, supply chain actors would need to coordinate at least on the format in which they record transactions, and likely also on the hardware with which they are recorded. Such coordination becomes more difficult the larger and more complex the supply chain becomes [43].

3.2. Transaction monitoring

Supposing that a supply chain manages to coordinate on a set of standards for collecting and storing relevant information, how does that information come to be stored in the distributed ledger? Specifically, must agents in the supply chain *voluntarily* transmit the information to be entered? If so, then agents could choose to withhold data. Furthermore, if the costs of such monitoring are non-trivial, then it becomes difficult to discern whether an agent is withholding information for nefarious reasons or if that agent is just unwilling to bear the cost of monitoring transactions. Even in the event that transactions are monitored and uploaded throughout the supply chain, what mechanism guarantees that the data being submitted is truthful? It may well be plausible that fraudulent entries may be argued to simply be mistakes.

Blockchain ledgers for recording data provenances, such as Liang et al. [44], Zhang et al. [45], Ramachandran and Kantarcioglu [46], typically have a mechanism for monitoring changes made to the data without the permission of the agent modifying it. In these cases, the data are stored on a cloud computing platform and all actions on the data are directly visible to the platform itself. Thus changes made to data become automatically and involuntarily submitted to a blockchain ledger.

3.3. Product identification

A provenance for an object cannot be reliably secured unless that object has a trait or characteristic which makes it uniquely identifiable. That trait must also be very difficult to unnoticeably remove, modify, or transfer to another object. A serial number etched into the object provides a good example. The blockchain platform Everledger is able to provide reliable provenances for the diamond industry.[9] Once the quality of each diamond is graded, a serial number is laser inscribed on its girdle, allowing it to be uniquely identified upon which its grading report may be accessed on the Gemological Institute of America's website. Branding objects with a permanent serial number is not feasible for many goods, particularly those where provenance information may be most valuable, such as for fresh foods. Furthermore, such identifying characteristics may necessarily be absent from the final product, preventing the consumer from matching the good they possess with its provenance data. While cattle may be identified with an iron brand and an ear tag, these typically do not end up on the steak.

In cases where attaching a tag, serial number, or barcode to an item is not feasible, as can be the case for fresh food, alternative technologies may be available to identify a product or detect adulteration. These include DNA barcoding [16] and the use of mass spectroscopy for either the targeted detection of certain stable isotopes [47], or non-targeted fingerprinting using statistical models [48]. See [49] and [50] for recent surveys of these methods. These biological fingerprints could be entered into a ledger at the beginning of the supply chain and validated by consumers or wholesalers at the end, similar to the serial number and physical characteristics stored in the aforementioned diamond blockchain.

4. Case study

In this section we explore the potential for blockchain technology in a case study supply chain involving the domestic production of prawns in Australian aquaculture enterprises. As one component of a broader research program examining the integration of digital technologies in agricultural supply chains, a qualitative analysis of the prawn aquaculture supply chain was undertaken. The prawn aquaculture supply chain was chosen as it is a relatively simple in terms of actors involved and stands to gain from traceability by differentiating their product from international competitors.

We gathered supply chain stakeholders contact details through industry contacts in a purposive manner [51–53]. The authors conducted all the interviews and snowballing (asking about links forward and backward in the supply chain) was used to obtain the perceptions of both researchers and members of the chain – inputs, production, and post farm-gate [54].

We undertook a total of 8 interviews to explore an in-depth and highly focused qualitative study within a small industry catering to domestic markets following previously reported research protocols [55–57]. The Australian prawn farming industry consists of approximately 300 full time equivalent jobs across 900 hectares of farm, 95% of which is in the state of Queensland due to the requirement that farm temperatures be above 25 degrees centigrade. Despite its relatively small size, this industry generates annual revenue in excess of $80 million.[10]

Stakeholders were interviewed with enquiry garnering their perceptions of trust, fraud, traceability, innovation, digitalization, and when relevant (stakeholders had heard of it) specifically the relevance of blockchain technology. Fig. 1 represents the supply chain stakeholders that were interviewed, with the number proceeding their description utilized as a reference in the results that follow.

[9] See https://diamonds.everledger.io/.

[10] https://apfa.com.au/prawn-farming/.

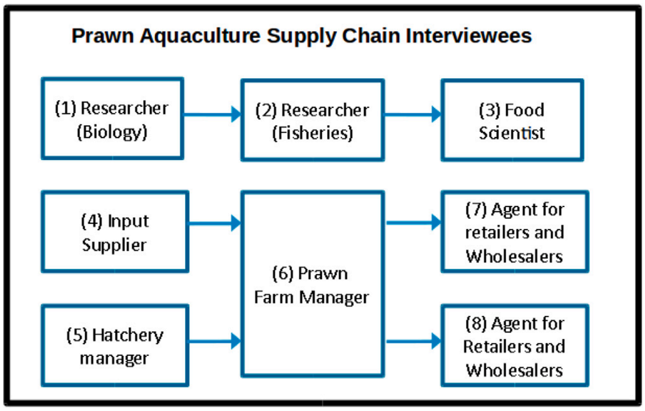
Prawn Aquaculture Supply Chain Interviewees
(1) Researcher (Biology)
(2) Researcher (Fisheries)
(3) Food Scientist
(4) Input Supplier
(6) Prawn Farm Manager
(7) Agent for retailers and Wholesalers
(5) Hatchery manager
(8) Agent for Retailers and Wholesalers

Fig. 1. Interviewees positioned along the prawn aquaculture supply chain.

4.1. Results

Results from the interviews are presented in this section. Firstly, interviewee discussion of blockchain technology specifically, before existing systems that are in place to overcome barriers are examined, more pertinent areas for investment in the prawn aquaculture value chain follow, then underlying assumptions that would have to be broken down are highlighted, and an exploration is made into the existing components of trust in the supply chain.

4.2. Discussing blockchain technology

Discussion of blockchain with interviewees helped develop their understanding of what was involved with such a technology. For instance, the following conversation between one of the interviewees and an interviewer indicates the immediate learning, and an associated change in perception, regarding how useful (or not) blockchain technology might be in the prawn aquaculture supply chain:

> *Interviewer (I): have you heard of blockchain technology?*
>
> *(3) I have. I'm starting to get my head around it. I kind of get it…*
>
> *I: Do you think that that could be used somehow?*
>
> *(3) I think it probably could… it would actually be highly suitable to that blockchain stuff because it wouldn't be that difficult to implement.*
>
> *I: Do you think farmers or anyone along the supply chain would be on board with making the history of all of their transactions and every transaction they make publicly available for anyone in the supply chain to see? Do you think they'd be okay with it?*
>
> *(3) It depends what you mean by every transaction. I'd generally say no.*
>
> *I: For example, when a feed supplier sells feed to a farm, when that money changes hands, that transaction gets listed on a public ledger for anybody to basically look up and observe it.*
>
> *(3) That's true isn't it? So, no, it wouldn't be their first option, I wouldn't think. But they're very open with each other and they interact farm to farm and discuss the operations and all that sort of stuff pretty well, but of course they are competitive.*

Similar discussions were had with many of the interviewees, with uncertainty regarding the actual implications of such a technology being deployed:

> *The blockchain idea got forwarded to me while I was the R&D [Research and Development] chair. I must admit I had to Google it… I still don't fully get it but I think I understand the basics. I probably don't understand enough to give an intelligent, informed answer but certainly if I understand it; it essentially makes data more real-time and transparent to all the different stakeholders… but then produces barriers to things happening. (5)*
>
> *It's getting media attention and it looks interesting but to be honest I don't really truly understand what it is and what it's capable of. From all the articles I've read I don't think that most people do… I know about Bitcoin but the concept of having that decentralised system that's not able to change and everyone can access I understand but I don't understand knowing a little bit about how complicated the supply chain is how we intend to get such a broad range of different businesses to plug into that. It's going to be a bit of a challenge… I've been thinking about it in the last couple of weeks and I don't even know what we would put in that blockchain. We're developing this customer portal that's got information like when the feeds being made, where it is on the truck, when it's going to be delivered and stuff like that… yeah you can have what's the source of the ingredients I suppose… you could see that that packet of fish meal would trace right back to fishing boat X in South America but I don't know what the value of that is… so I don't today know how it would benefit us I guess. (4)*

As the discussions developed interviewees began to link existing endeavours to the hype of blockchain applications, whilst also recognizing challenges that could arise in terms of interoperability:

> *The little bit I understand about blockchain in the research I've done, I think a lot of businesses around the world, not just aquaculture people, are starting to go down that pathway with their own systems… Our customers can submit orders electronically to us that should then be read by our accounting system and create an order. But the way that the units and the products are set up and the codes are different… there's too many things that aren't compatible, it's almost more trouble than it's worth. So there's a major challenge with getting different companies information onto a single system in the correct format. Because let's say we were wanting to tie into a blockchain system, we can present using information like this… but someone else is going to present it in a different way, so how does that all link up and make sense at the end, I think that's going to be the challenge. (4)*

Interviewees, while recognizing that they were not experts on blockchain technology, seemed rather optimistic about the application of blockchain technology in the prawn aquaculture supply chain.

4.3. Traceability

Exploration of existing mechanisms through the supply chain revealed that some of the potential benefits of a blockchain technology already exist in alternative forms. For example barcoding systems to enable traceability of inputs:

> *There's traceability for everything, everything has got batch numbers. For every feed that's batched there's a batch number which relates back to all the ingredients that have been put in it. They all have batch numbers that link to that batch so we can trace it right back to the supplier. (4)*
>
> *So we have a product tracing program so everything's barcoded and scanned and stored and the same when it goes out so that when it goes to the customer, everything's traceable, digitally. (6)*
>
> *Probably that is sufficient, with respect to, you can go right back to the farm, and you've got the day, the batch number and all the records can be available if you need to query something. (3)*

Along with barcoding, systems were in place (or being developed) to allow relevant members of the supply chain to have visibility regarding inputs, outputs and the product credentials through certification:

Everything runs through an accounting system, we sell our hatchery feeds through our website. We're looking at the solutions for a customer portal essentially. Where people log in and are able to see where it's at, we're working on a lot of those kind of things but it's a slow process. (4)

We're in the final stages of getting what's called ASC certification, Aquaculture Stewardship Council. It's the equivalent of the MSC, Marine Stewardship Council, one for the wild fisheries. So it's an independent international certification program... So they come and do audits on the farm. We had three auditors here for five days and they look at environmental and social aspects of the business... they go around the local community, randomly interviewing the local community to ensure there's no issues with the business. [They] interview all the staff to make sure there's no issues there and have to provide an extensive suite of documents for them to review. There's a list of standards that they have to cross check against. They then do a report to the ASC Board, which is based internationally and provide their recommendations against the standards and then the Board either gives the certification or it doesn't and that's communicated to us and then we provide that to [the retailer].. (6)

Importantly, one interviewee explains transparency through the supply chain, leading to questions of what the added value proposition of blockchain technology would be:

I mean maybe there's practical issues but again I'm a big fan of transparency so the old days of doing business was cloak and dagger and you withheld information and you kept that close to your chest because that generated you your money and there's still - that's the old way of doing business in the seafood industry. But in my opinion, it shouldn't be that way anymore. There's no reason for it at all. I mean I know what margin the wholesalers is, I know what margins retailers put on their product, they all know what margins we charge, what commission we charge. We know what the profitability of the farms are... I'm pretty aware of the profitability throughout the supply chain, I mean I can tell you what percentage most people in the supply chain are making and I think there's nothing wrong with that. (7)

In addition to the possible positive impacts on traceability, increased transparency has the potential to create privacy issues and have implications for taxation:

Simply the fact that you have got farms that have got one or two sites or more and if you have got a public view on all of that, including the ATO [Australian Taxation Office], and the guys go "I'm delivering it here" but I didn't use it all and then they're going to take it up here, it will make one farm look like he's (sic) made an enormous profit and a loss on the other one isn't going to be connected at all... It is still farming and to have that sort of visibility I think would be quite dangerous, to be honest, from their point of view. It doesn't help me and it won't help [the retailer] because, going back to the trust side of it, we all have to trust each other to do the right thing by each other and those that we finally found we couldn't really trust in the end, we had to drop. (8)

4.4. Other priority areas for investment

It is important to consider the opportunity cost of any investment in blockchain technology in the prawn aquaculture supply chain. Resources utilized (time, money, or energy) in initiating or developing blockchain could be used to accomplish other things. To that end, interviewees were asked how important innovation was to them and what they saw as the most important areas for investment in the prawn aquaculture supply chain in the future. Responses involved genetic improvement, feed/input improvements, modelling, real-time data, automation and online access improvement. Improvements in prawn biology were a popular example of an area whereby investment would improve productivity and minimize risk:

There would be significant improvements in feed quality, both in the hatchery and on the farm. Significant improvements in [the] pond management side of things. (1)

We've come a long way... what I would say though is, it's still very early days. If we were to compare ourselves to other industry like pork, chicken, beef. They're quite mature industries that are effectively at the top end of their exponential curve in terms of innovation and growth. Even though we've had those advances in the last 20 years we're certainly at the bottom end of that curve. (6)

The following comments indicate that more could be done to monitor, track and model prawn production through the supply chain in an effort to automate aspects of growth and movement through the chain:

If we can use real-time monitoring to measure eight, nine, different parameters and then have some quite good advanced modelling to interpret all those data and the trends, I think that can be extremely powerful and certainly be one of those quantum leaps forward in really understanding the fine relationships between all the different water body parameters that might be otherwise overlooked through lack of time or from the complexity of the data. (5)

I'd love to be able to have real time access to - I'm just fantasising here - being able to track a consignment of fresh prawns that have left [prawn farm] this afternoon and being able to know where that is the whole way down in real time, that would be just tremendous. Because there's a continual bugbear because when you're dealing with a product with a short shelf life, and it's two to three to five days to a market place, and it's only got a 12 day shelf life, or 15 day shelf life nowadays, that would be just tremendous for the customers to be able to look on their mobile phone and go okay, well it hasn't turned up at 6 am but I know it's just an hour out of Sydney and it will be here in an hour's time. (7)

I guess the next step going forward is to automate and be able to trust those systems that can do the more, I guess the human things like analyse the pond water quality parameters and know what actions to take and be able to analyse the relationships of the water quality parameters and prawn health and perhaps more speedy real-time information or predictive tools about the way prawn health or animal's health is heading to make more speedy decisions. That's what I think will happen in the next five to ten years or ten to 15 years. (5)

There was also recognition that producers would need access to internet connections that were reliable and met the perquisite criteria of digital technologies:

I mean communication, the NBN [National Broadband Network] at the farm, I mean not that the NBN has really worked that well, but better internet back at the producer's level would be beneficial. The more reliant we are, it's sometimes hard for them to keep up. And mobile phone systems and stuff like that. (7)

4.5. The existing trust context

In describing the prawn aquaculture supply chain, trust was obviously important to interviewees. Importantly, the relationships between individuals and organizations at different points of the supply chain were explicitly recognized:

I make sure that I'm getting, if it says 98 percent sodium nitrate I make sure that it is 98 percent. So I certainly deal with the bigger companies and develop good relationships. Feed is another really important one, I use the bigger companies or bigger, highly recognised brands in hatchery feeds... [and] tend to shy back from smaller companies [with less] rigorous quality control. (5)

But today, I mean, after doing it for nearly 27 years it is really a lot less effort these days because the guys that we deal with know what they are

> *doing, care about what they are doing and there is only a couple of guys that have survived that really shave every corner. (8)*

> *I think trust is critical right along the supply chain... with respect to trust I know that it does occur and is relevant at each step of the supply chain. It is not so much the direct proof that they need, it's actually built from relationships. (3)*

> *We're not always privy to what diets our farms are using. We have a rough idea, in relationships with the main companies but that's not to say that individual farmers don't get tempted by cheaper prices and go and buy it direct from other producers' off-shore. I suppose we lose visibility on that. Freight companies, we often lose visibility in that process between leaving the farm and getting to the customer. We have direct contacts with the freight companies but the difference between being delivered at 6 am at the Sydney Fish Markets to 8 am is a huge difference. (7)*

There was also recognition, however, that the potential abuse of trust can and does occur. In particular, examples of blatant food fraud or product substitution were described:

> *We knew that the guys [at a fresh seafood market] were putting 'Product of Australia' on stuff that was imported. They have got in December some extra-large [prawns], and back in those days it was a struggle to get a large prawn, let alone an extra-large or a jumbo size out. So we knew what they had out on display and calling them 'Australian' was absolute crap. The guys [at a fresh seafood market] were blatantly proud of the fact they were able to get away with this sort of crap. (8)*

> *I think the [supply chain] thing has become a lot more robust and it's not through monitoring per se, it's more through the trust relationship. But yes, the opportunity for doing that [food fraud] is absolute. And there's been a couple of court cases on that exact thing. (3)*

> *The wholesalers, because they don't sell their product as branded product, you go to their retail outlets and it's just prawns sitting in a window, so it's very easy for them to substitute [the prawns with others] (6)*

> *I've seen cases where there's major retailers down at the fish markets and you know they're not buying Australian prawns from any of the farms. [They are] clearly imported prawns in frozen boxes in the freezer and you know full well, and they know you know too, that the prawns in their window are imported from Thailand and being sold as Australian prawns. But they will buy five boxes or 100 boxes, or 100 kilos of Australian prawns just so they can carry the receipt. There's ways you can detect the origins [for example if prawns] come from Thailand but is there the resources if you do that? So there's tremendous fraud goes on. (7)*

Importantly, however, interviewees had systems in place to attempt to reduce the risk of product substitution:

> *It [the input] can be printed as a Chinese product but packed in New Zealand and it's an easier pathway into Australia. Some of the squid I saw, so the cold water squid are higher in cholesterol and so not all New Zealand squid is New Zealand squid. I certainly research the company, look them up on the internet, I look up foreign companies where they actually list their fishing grounds and usually they have an FAO number or the UN number where they actually fish. So I make sure that I do all my checks to minimise the risk. (5)*

> *We check everything that comes in but you're relying upon your supplier to provide you with the right materials all the time, sometimes you can't check everything... you put a lot of trust in these suppliers to do that because you have to work with someone reliable. But we've had instances in the past where it's not that they've been untrustworthy but they've been supplying us something and then a few months down the line going, "Oh [expletive] the specification of the stuff you've been getting is actually this". They've figured it out and a good supplier will come and say, "Oh look guys we [expletive] up, this is the situation". We'll go back and see what damage that caused or what we need to do to rectify it. But sometimes it's not that the suppliers untrustworthy but it's just for some of these specifications the tools and stuff to test accurately and quickly don't exist... So you rush to do it yourself and that's when you've got to work with a good or a bad supplier, an honest one or a dishonest one and hope that it all works out. So that's why we check everything because even with a multi-national company who should be very reliable sometimes there [are] errors. (4)*

Due to the cost in the event of an issue being incurred by the producers and associated reputational cost of betrayal in such a small industry, it was recognized that in most transactions there was no real incentive for fraudulent behaviour. Rather, there were incentives to monitor and track products closely to avoid increased costs:

> *If they [prawn farmers] do a week's production and have it all under one use by date, which would be stupid for a start, and there is an issue then they have got a whole week of product that they are going to have to recall, withdraw, credit, whatever, because they didn't identify it and micro manage it. (8)*

> *Now, I don't even really think there's too much fraud or that stuff going on in Australia because as I said before, there's only two or three major aquaculture suppliers and they usually deal with the big aquaculture supplier companies that everyone knows or they're certainly known globally. But, ideally, we have a lot of smaller different players who are competing for a massive market and, you know, Australia is usually quite stringent. There's not - I don't think there's too much fraud that happens in the supply chain. (5)*

This section has reported results from the perspective of the interviewees in the prawn aquaculture supply chain. Blockchain technology, existing systems, other priorities, underlying assumptions and existing trust structures were deliberated upon and provide the basis for the following managerial implications and conclusions.

5. Conclusion

In this article we have explored the potential role for blockchain technology in establishing trustworthy provenances for goods in a supply chain. Much hype and speculation surround blockchain technology, especially in relation to its potential to disrupt and fundamentally transform industries. We have suggested that in order to accurately evaluate the utility of a blockchain solution, it ought to be compared not to the *status quo* within an industry, but to the *next best* technology that would be available; namely, storing data in a traditional database rather than a blockchain. When compared to a solution involving a traditional database, the *net* value added from blockchain appears to be significantly reduced. Since widespread digitalization within an industry is a necessary precondition for a distributed database, blockchain or otherwise, this is likely where the highest gains are to be realized.

We considered difficulties in securing trustworthy provenances for goods in a supply chain that may exist independently of how the provenance data is stored. There must be a robust way to uniquely identify the product being tracked in order to match the good to its provenance data. The data being recorded must itself be trustworthy to begin with, which may be called into question if the data are obtained by voluntary self-reporting by the supply chain actors.

It should be noted that blockchain is a relatively young technology with applications still currently under development. In the future, solutions may ultimately be found that produce a substantial value add for a blockchain ledger over a traditional database. On the other hand, blockchain is surrounded by considerable hype and many of the proposed applications may not be feasible.

We explored a case study of the Australian prawn aquaculture supply chain in which we attempted to identify the key barriers to trustworthy provenances as well as identify the capacity for a potential blockchain solution to facilitate provenance. There were several recurrent themes in the interview responses of case study participants.

The areas of highest immediate value were in farm productivity and biosecurity. Traceability is important, especially for biosecurity, but has only been partially solved. Retailers can trace a batch of prawns back to the prawn farm from which they originated, but only the prawn farm may then trace the feedstock and broodstock of that batch. The businesses of some agents are highly digitalized, whereas others still use paper records. Food fraud is a concern but difficult to prove, since the prawns themselves cannot be tagged and uniquely identified, only the containers in which they are shipped. And finally, the notion of a blockchain ledger is relatively well known and looked upon positively, though its precise application to the supply chain remains unclear.

Acknowledgements

The authors would like to thank Stu Arnold, Aysha Flemming, Raj Gaire, Russell Gorddard, Tung Hoang, Emma Jakku, Lilly Lim-Camacho, Mark Staples, and Bruce Taylor for helpful comments and input.

References

[1] W.H. Hutt, The concept of consumers' sovereignty, Econ. J. 50 (197) (1940) 66–77, (ISSN 00130133, 14680297) http://www.jstor.org/stable/2225739.
[2] George A. Akerlof, The market for "lemons": Quality uncertainty and the market mechanism, Q. J. Econ. 84 (3) (1970) 488–500, (ISSN 00335533, 15314650).
[3] Myo Min Aung, Yoon Seok Chang, Traceability in a food supply chain: Safety and quality perspectives, Food Control (ISSN: 0956-7135) 39 (2014) 172–184, http://dx.doi.org/10.1016/j.foodcont.2013.11.007.
[4] Amrou Awaysheh, Robert D. Klassen, The impact of supply chain structure on the use of supplier socially responsible practices, Int. J. Oper. Prod. Manage. 30 (12) (2010) 1246–1268, http://dx.doi.org/10.1108/01443571011094253.
[5] Christian Coff, Michiel Korthals, David Barling, Ethical traceability and informed food choice, in: Christian Coff, David Barling, Michiel Korthals, Thorkild Nielsen (Eds.), Ethical Traceability and Communicating Food, Springer Netherlands, Dordrecht, ISBN: 978-1-4020-8524-6, 2008, pp. 1–18, http://dx.doi.org/10.1007/978-1-4020-8524-6_1.
[6] Samuel Brody, Himanshu Grover, Arnold Vedlitz, Examining the willingness of americans to alter behaviour to mitigate climate change, Clim. Policy 12 (1) (2012) 1–22, http://dx.doi.org/10.1080/14693062.2011.579261.
[7] Lilly Lim-Camacho, Anoma Ariyawardana, Gemma K. Lewis, Steven J. Crimp, Simon Somogyi, Brad Ridoutt, Stuart Mark Howden, Climate adaptation of food value chains: The implications of varying consumer acceptance, Reg. Environ. Change J. (ISSN: 1436-378X) 17 (1) (2017) 93–103, http://dx.doi.org/10.1007/s10113-016-0976-5.
[8] Brian L. Buhr, et al., Traceability and information technology in the meat supply chain: Implications for firm organization and market structure, J. Food Dist. Res. 34 (3) (2003) 13–26.
[9] Miranda PM Meuwissen, Annet GJ Velthuis, Henk Hogeveen, Ruud BM Huirne, et al., Traceability and certification in meat supply chains, J. Agribusiness 21 (2) (2003) 167–182.
[10] Wim Verbeke, Market differentiation potential of country-of-origin, quality and traceability labeling, Estey Centre J. Int. Law Trade Policy 10 (1) (2009) 20–35, Copyright - (c) Copyright 2009 The Estey Journal of International Law and Trade Policy; Last updated - 2010-06-20; SubjectsTermNotLitGenreText - Europe.
[11] John Spink, Douglas C. Moyer, Defining the public health threat of food fraud, J. Food Sci. (ISSN: 1750-3841) 76 (9) (2011) R157–R163, http://dx.doi.org/10.1111/j.1750-3841.2011.02417.x.
[12] Laslo Tarjan, Ivana Šenk, Srdjan Tegeltija, Stevan Stankovski, Gordana Ostojic, A readability analysis for QR code application in a traceability system, Comput. Electron. Agric. (ISSN: 0168-1699) 109 (2014) 1–11, http://dx.doi.org/10.1016/j.compag.2014.08.015.
[13] Thomas Kelepouris, Katerina Pramatari, Georgios Doukidis, RFID-enabled traceability in the food supply chain, Ind. Manag. Data Syst. 107 (2) (2007) 183–200, http://dx.doi.org/10.1108/02635570710723804.
[14] Guillermo Azuara, José Luis Tornos, José Luis Salazar, Improving RFID traceability systems with verifiable quality, Ind. Manag. Data Syst. 112 (3) (2012) 340–359, http://dx.doi.org/10.1108/02635571211210022.
[15] Alfredo Parreño-Marchante, Alejandro Alvarez-Melcon, Mira Trebar, Piero Filippin, Advanced traceability system in aquaculture supply chain, J. Food Eng. (ISSN: 0260-8774) 122 (2014) 99–109, http://dx.doi.org/10.1016/j.jfoodeng.2013.09.007.
[16] Andrea Galimberti, Fabrizio De Mattia, Alessia Losa, Ilaria Bruni, Silvia Federici, Maurizio Casiraghi, Stefano Martellos, Massimo Labra, DNA Barcoding as a new tool for food traceability, Food Res. Int. (ISSN: 0963-9969) 50 (1) (2013) 55–63, http://dx.doi.org/10.1016/j.foodres.2012.09.036.
[17] Jian-Ping Qian, Xin-Ting Yang, Xiao-Ming Wu, Li Zhao, Bei-Lei Fan, Bin Xing, A traceability system incorporating 2D barcode and RFID technology for wheat flour mills, Comput. Electron. Agric. (ISSN: 0168-1699) 89 (2012) 76–85, http://dx.doi.org/10.1016/j.compag.2012.08.004.
[18] Saveen A. Abeyratne, Radmehr P. Monfared, Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger, © The Authors. Published by eSAT, 2016.
[19] H.M. Kim, M. Laskowski, Towards an ontology-driven blockchain design for supply chain provenance, ArXiv e-prints (2016) arXiv:1610.02922.
[20] Yu-Pin Lin, Joy R. Petway, Johnathen Anthony, Hussnain Mukhtar, Shih-Wei Liao, Cheng-Fu Chou, Yi-Fong Ho, Blockchain: The evolutionary next step for ICT e-agriculture, Environments (ISSN: 2076-3298) 4 (3) (2017) http://dx.doi.org/10.3390/environments4030050.
[21] Melanie Swan, Blockchain: Blueprint for a New Economy, " O'Reilly Media, Inc.", 2015.
[22] Don Tapscott, Alex Tapscott, Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world, Penguin, 2016.
[23] Bruce Pon, Blockchain will usher in the era of decentralised computing, LSE Bus. Rev. (2016).
[24] Guillermo Jesús Larios-Hernández, Blockchain entrepreneurship opportunity in the practices of the unbanked, Bus. Horizons (ISSN: 0007-6813) 60 (6) (2017) 865–874, http://dx.doi.org/10.1016/j.bushor.2017.07.012.
[25] Boyd Cohen, José Ernesto Amorós, Lawrence Lundy, The generative potential of emerging technology to support startups and new ecosystems, Bus. Horizons (ISSN: 0007-6813) 60 (6) (2017) 741–745, http://dx.doi.org/10.1016/j.bushor.2017.06.004.
[26] Jun Dai, Miklos A. Vasarhelyi, Toward blockchain-based accounting and assurance, J. Inf. Syst. 31 (3) (2017) 5–21, http://dx.doi.org/10.2308/isys-51804.
[27] Theodosis Mourouzis, Chrysostomos Filipou, The blockchain revolution: Insights from top-management, 2017, CoRR abs/1712.04649. http://arxiv.org/abs/1712.04649.
[28] Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008, http://bitcoin.org/bitcoin.pdf.
[29] Mark Coeckelbergh, Technology and the good society: A polemical essay on social ontology, political principles, and responsibility for technology, Technol. Soc. (ISSN: 0160-791X) 52 (2018) 4–9, http://dx.doi.org/10.1016/j.techsoc.2016.12.002, http://www.sciencedirect.com/science/article/pii/S0160791X16301191, Technology and the Good Society.
[30] Anne Kerr, Rosemary L. Hill, Christopher Till, The limits of responsible innovation: Exploring care, vulnerability and precision medicine, Technol. Soc. (ISSN: 0160-791X) 52 (2018) 24–31, http://dx.doi.org/10.1016/j.techsoc.2017.03.004, http://www.sciencedirect.com/science/article/pii/S0160791X16301282, Technology and the Good Society.
[31] Cristina Voinea, Designing for conviviality, Technol. Soc. (ISSN: 0160-791X) 52 (2018) 70–78, http://dx.doi.org/10.1016/j.techsoc.2017.07.002, http://www.sciencedirect.com/science/article/pii/S0160791X17300908, Technology and the Good Society.
[32] Charla Griffy-Brown, Brian D. Earp, Omar Rosas, Technology and the good society, Technol. Soc. (ISSN: 0160-791X) 52 (2018) 1–3, http://dx.doi.org/10.1016/j.techsoc.2018.01.001, http://www.sciencedirect.com/science/article/pii/S0160791X18300010, Technology and the Good Society.
[33] Markus Jakobsson, Ari Juels, Proofs of work and bread pudding protocols(extended abstract), in: Bart Preneel (Ed.), Secure Information Networks: Communications and Multimedia Security IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS'99) September 20–21, 1999, Leuven, Belgium, Springer US, Boston, MA, ISBN: 978-0-387-35568-9, 1999, pp. 258–272, http://dx.doi.org/10.1007/978-0-387-35568-9_18.
[34] Cynthia Dwork, Moni Naor, Pricing via processing or combatting junk mail, in: Ernest F. Brickell (Ed.), Advances in Cryptology — CRYPTO' 92: 12th Annual International Cryptology Conference Santa Barbara, California, USA August 16–20, 1992 Proceedings, Springer Berlin Heidelberg, Berlin, Heidelberg, ISBN: 978-3-540-48071-6, 1993, pp. 139–147, http://dx.doi.org/10.1007/3-540-48071-4_10.
[35] Adam Back, Hashcash-a denial of service counter-measure, 2002, http://www.hashcash.org/papers/hashcash.pdf.
[36] K.J. O'Dwyer, D. Malone, Bitcoin mining and its energy footprint, in: 25th IET Irish Signals Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014), 2014, pp. 280–285, http://dx.doi.org/10.1049/cp.2014.0699.
[37] Christian Stoll, Lena Klaaben, Ulrich Gallersdorfer, The carbon footprint of bitcoin, Joule (ISSN: 2542-4351) 3 (7) (2019) 1647–1661, http://dx.doi.org/10.1016/j.joule.2019.05.012, http://www.sciencedirect.com/science/article/pii/S2542435119302557.
[38] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, P. Rimba, A taxonomy of blockchain-based systems for architecture design, in: 2017 IEEE International Conference on Software Architecture (ICSA), 2017, pp. 243–252, http://dx.doi.org/10.1109/ICSA.2017.33.
[39] E.F. Codd, A relational model of data for large shared data banks, Commun. ACM (ISSN: 0001-0782) 13 (6) (1970) 377–387, http://dx.doi.org/10.1145/362384.362685.

[40] Yang Li, Kai Zheng, Ying Yan, Qi Liu, Xiaofang Zhou, Etherql: A query layer for blockchain system, in: Selçuk Candan, Lei Chen, Torben Bach Pedersen, Lijun Chang, Wen Hua (Eds.), Database Systems for Advanced Applications, Springer International Publishing, Cham, ISBN: 978-3-319-55699-4, 2017, pp. 556–567.

[41] Charles D. Emery, The use of portable barcode scanners in collections inventory, Collect. Manag. 13 (4) (1991) 1–17, http://dx.doi.org/10.1300/J105v13n04_01.

[42] Rebecca Angeles, RFID Technologies: supply-chain applications and implementation issues, Inf. Syst. Manag. 22 (1) (2005) 51–65.

[43] Gerhard Schiefer, New technologies and their impact on the agri-food sector: An economists view, Comput. Electron. Agric. (ISSN: 0168-1699) 43 (2) (2004) 163–172, http://dx.doi.org/10.1016/j.compag.2003.12.002.

[44] Xueping Liang, Sachin Shetty, Deepak Tosh, Charles Kamhoua, Kevin Kwiat, Laurent Njilla, Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability, in: Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, in: CCGrid '17, IEEE Press, Piscataway, NJ, USA, ISBN: 978-1-5090-6610-0, 2017, pp. 468–477, http://dx.doi.org/10.1109/CCGRID.2017.8.

[45] Y. Zhang, S. Wu, B. Jin, J. Du, A blockchain-based process provenance for cloud forensics, in: 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 2017, pp. 2470–2473, http://dx.doi.org/10.1109/CompComm.2017.8322979.

[46] Aravind Ramachandran, Murat Kantarcioglu, Smartprovenance: A distributed, blockchain based dataprovenance system, in: Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy, in: CODASPY '18, ACM, New York, NY, USA, ISBN: 978-1-4503-5632-9, 2018, pp. 35–42, http://dx.doi.org/10.1145/3176258.3176333.

[47] Hilmar Förstel, The natural fingerprint of stable isotopes—use of IRMS to test food authenticity, Anal. Bioanal. Chem. (ISSN: 1618-2650) 388 (3) (2007) 541–544, http://dx.doi.org/10.1007/s00216-007-1241-z.

[48] Stefanie Gerbig, Stephan Neese, Alexander Penner, Bernhard Spengler, Sabine Schulz, Real-time food authentication using a miniature mass spectrometer, Anal. Chem. (ISSN: 0003-2700) 89 (20) (2017) 10717–10725, http://dx.doi.org/10.1021/acs.analchem.7b01689.

[49] David I. Ellis, Victoria L. Brewster, Warwick B. Dunn, J. William Allwood, Alexander P. Golovanov, Royston Goodacre, Fingerprinting food: Current technologies for the detection of food adulteration and contamination, Chem. Soc. Rev. 41 (2012) 5706–5727, http://dx.doi.org/10.1039/C2CS35138B, http://dx.doi.org/10.1039/C2CS35138B.

[50] Janet Riedl, Susanne Esslinger, Carsten Fauhl-Hassek, Review of validation and reporting of non-targeted fingerprinting approaches for food authentication, Anal. Chim. Acta (ISSN: 0003-2670) 885 (2015) 17–32, http://dx.doi.org/10.1016/j.aca.2015.06.003, http://www.sciencedirect.com/science/article/pii/S0003267015007527.

[51] Alan Bryman, Social Research Methods, Oxford university press, 2008.

[52] LE Redding, FK Barg, G Smith, DT Galligan, MZ Levy, S Hennessy, The role of veterinarians and feed-store vendors in the prescription and use of antibiotics on small dairy farms in rural Peru, J. Dairy Sci. 96 (11) (2013) 7349–7354.

[53] Andrew Sayer, Method in social science: Revised 2nd edition, Routledge, 2010.

[54] H.R. Bernard, Social Research Methods: Qualitative and Quantitative Approaches, Sage, 2000.

[55] Simon J. Fielke, Geoff A. Wilson, Multifunctional intervention and market rationality in agricultural governance: A comparative study of England and south Australia, GeoJournal (ISSN: 1572-9893) 82 (5) (2017) 1067–1083, http://dx.doi.org/10.1007/s10708-016-9729-8.

[56] Barbara King, Simon Fielke, Karen Bayne, Laurens Klerkx, Ruth Nettle, Navigating shades of social capital and trust to leverage opportunities for rural innovation, J. Rural Stud. (ISSN: 0743-0167) 68 (2019) 123–134, http://dx.doi.org/10.1016/j.jrurstud.2019.02.003, http://www.sciencedirect.com/science/article/pii/S0743016718303127.

[57] J.A. Turner, A. Horita, S. Fielke, L. Klerkx, P. Blackett, D. Bewsell, B. Small, W.M. Boyce, Revealing power dynamics and staging conflicts in agricultural system transitions: Case studies of innovation platforms in New Zealand, J. Rural Stud. (ISSN: 0743-0167) 76 (2020) 152–162, http://dx.doi.org/10.1016/j.jrurstud.2020.04.022, http://www.sciencedirect.com/science/article/pii/S074301671630660X.