Journal of Industrial Information Integration xxx (xxxx) xxx

Contents lists available at ScienceDirect

Journal of Industrial Information Integration

journal homepage: www.sciencedirect.com/journal/journal-of-industrial-information-integration

Garbage in garbage out: The precarious link between IoT and blockchain in food supply chains

Warwick Powell, Marcus Foth *, Shoufeng Cao, Valéri Natanelov

Queensland University of Technology (QUT), QUT Design Lab, 2 George Street, Brisbane QLD 4000, Australia

ARTICLE INFO

Keywords:
Blockchain
Data quality
Distributed ledger technology
Meat industry
Internet of things
Food supply chains

ABSTRACT

The application of blockchain in food supply chains does not resolve conventional IoT data quality issues. Data on a blockchain may simply be immutable garbage. In response, this paper reports our observations and learnings from an ongoing beef supply chain project that integrates Blockchain and IoT for supply chain event tracking and beef provenance assurance and proposes two solutions for data integrity and trust in the Blockchain and IoT-enabled food supply chain. Rather than aiming for absolute truth, we explain how applying the notion of 'common knowledge' fundamentally changes oracle identity and data validity practices. Based on the learnings derived from leading an IoT supply chain project with a focus on beef exports from Australia to China, our findings unshackle IoT and Blockchain from being used merely to collect lag indicators of past states and liberate their potential as lead indicators of desired future states. This contributes: (a) to limit the possibility of capricious claims on IoT data performance, and; (b) to utilise mechanism design as an approach by which supply chain behaviours that increase the probability of desired future states being realised can be encouraged.

1. Introduction

Food supply chains have attracted research on improving food traceability and provenance by integrating IoT with blockchain [1]. While these studies have proposed pairing architecture and analytical models to show the competence of integration, theoretical explorations are required to explain how to couple these two technologies, which is critical for going beyond pilots and use cases. Existing blockchain-based food supply chain projects predominantly focus on food traceability and seek to deliver something resembling absolute truth, and thereby 'solving' traceability challenges of the grander claims [2,3] . There also appears to be a widely popularised myth surrounding features of 'safe' and 'secure,' which can be achieved by simply deploying blockchain to food supply chains.

In the IoT and big data era, the old adage of 'garbage in, garbage out' (GIGO, or rubbish in, rubbish out – RIRO in the UK) usually describes the challenge that flawed or corrupt input data produces nonsensical output or 'garbage' [4] . If IoT is used as a data gathering tool and the blockchain is used for distributed data storage [5], this does not necessarily prove that the food item itself has any of the attributes claimed by the data. IoT devices may be faulty or inappropriately deployed; they may be tampered with; communications may be intercepted and data veracity compromised. These are well known security problems, which has occasioned an extensive literature in itself [6]. In this way, the issue of GIGO in blockchain-based food supply chains would be exacerbated when making sense of the tracking and tracking of a large bath of real-time data which is manifold and diverse, and often unstructured. Simply speaking, data on a blockchain may just be immutable, that is, *very secure, garbage*.

In response to the GIGO issues in blockchain-based food supply chains, this paper focuses on a related aspect specific to the precarious data link between blockchain and IoT for improving data provenance and integrity. The investigation draws on our industry-based experience leading a two-year AUD 1.5 million project that involved the integration of IoT and Blockchain to track and protect the authenticity of Australian beef in the rapidly growing Chinese market. The economic significance of Australia's beef export industry is illustrated by the fact that pre-coronavirus, Australia exported up to 80% of the total production, generating export value of AUD 10.8 billion in 2019 [7]. Yet, demand from markets like China placed increasing pressure on Australia's supply capacity. This opens the door to food fraud, a USD 40 billion-a-year problem globally, which is risking Australia's brand reputation and

* Corresponding author.
E-mail addresses: w2.powell@qut.edu.au (W. Powell), m.foth@qut.edu.au (M. Foth), shoufeng.cao@qut.edu.au (S. Cao), valeri.natanelov@qut.edu.au (V. Natanelov).

https://doi.org/10.1016/j.jii.2021.100261
Received 3 March 2020; Received in revised form 30 May 2021; Accepted 29 July 2021
Available online 3 August 2021

value in China [8]. This problem illustrates the significance of our project and guides our research exploring the potential of IoTs and DLT to rebuild Australia's beef supply chains to China. Our research indicates that food traceability and supply chain integrity can be improved by combining good science with decentralised cryptographic data platforms based on mechanisms that go towards the creation of common knowledge.

The contribution of this paper is threefold. We initially discuss how IoT and Blockchain address the issues of data provenance and integrity and illustrates the incompetent way of integrating IoT and blockchain. Second, we developed a design-led framework that was used to guide the development of our food supply chain project as a specific integration of IoT and blockchain to a particular food supply chain context. Third, built on our industry-based learnings and experience in the beef supply chain, we illustrate how the introduction of 'common knowledge' can fundamentally change oracle identity and data validity practices rather than seeking for absolute truth, and crypto economics.

This paper is structured as follows. We first review prior work relevant to investigating the issue of 'garbage in garbage out' using IoT and blockchain in supply chains. We then describe the approach we take to build our argument, which is theoretical in nature. Next, we report our observations and learnings from the Beefledger project that is a novel blockchain-based beef supply chain project combining IoT and blockchain [73]. Built on the theoretically derived insights and practical explorations, we propose solutions for data oracle identity and data quality issues that occur when deploying IoT in the food industry before the conclusion of the paper.

2. Prior Work

> *On two occasions I have been asked, "Pray, Mr. Babbage, if you put into the machine wrong figures, will the right answers come out?" I am not able rightly to apprehend the kind of confusion of ideas that could provoke such a question.*
>
> — Charles Babbage, Passages from the Life of a Philosopher [9]

In computer science and data science, the saying 'garbage in, garbage out' (GIGO) has been coined usually to illustrate errors in human decision-making due to faulty, incomplete, or imprecise data. In this article, we specifically look at the risk of faulty, incomplete, or imprecise data originating from non-human input, that is, IoT devices being fed into blockchain systems. In this section we briefly review recent studies relevant to these two main themes of this article: IoT and blockchain, both in the context of agriculture and cross-border food supply chains.

2.1. Internet of things

IoT is a cornerstone in the emerging Industry 4.0 landscape thanks to its capability to enable autonomous data collection and sharing with minimal human intervention [10,11]. However, multiple survey studies into IoT [12-16] indicate that while the IoT technology promises great opportunities for promoting industrial automation and intelligence across various domains, including cities and homes, environment monitoring, health, energy, and business, it inherently comes with a multitude of challenges due to their architectural styles and computational complexities. Data provenance and integrity in the IoT-run environment is one of the most concerning challenges surrounding IoT [17-19]. The IoT devices produce data originates from dynamic real world and volatile environments and facilitate the communication with the physical world via the machine-to-human and/or machine-to-machine manner, which indicates the issue of data provenance and integrity pertaining to data generation, data quality, and data interoperability [6]. The dynamics and heterogeneity of data from IoT sensors present multi-variable complexity [20]. The use of multiple IoT devices to track and measure different variables further exacerbates the complexity due to the variation of sensors and different data formats in use. Accordingly, data quality can suffer from missing readings, sensor accuracy and inconsistency, and ambiguity from large volumes of data [6]. These factors make it challenging to ensure data provenance and integrity.

IoT devices have seen increasing applications in various stages of the food supply chain for real-time monitoring (e.g. of temperature and location) [5,21-23]. However, the mobility of supply chain assets and the continuously changing industrial environment, complemented by device faults, impersonation attacks or malicious data manipulation [17, 19], make it difficult to assure data provenance and integrity in the supply chain context. The issue of data provenance and integrity is more challenging in international food supply chains because their complex and fragmented structure makes it more difficult to identify and track products and processes from farm to fork [24]. Further, a multiple supply chain environment can result in the problems of data ambiguity in machine-to-human interactions that cascades to the human data consumer that requires the data to meet certain criteria such as accuracy, timeliness, completeness and reliability to name a few [25,26]. Whereas in machine-to-machine interactions machines as consumers (in) require semantics to process the IoT data independently [27]. The balance between machine-to human and machine-to-machine interactions can lead to interoperability issues of IoT data. Considering that IoT data is often – if not always – used as a combination of data from multiple sources, and given that this process relies on cooperation of mobile and distributed things, it often results in data incompleteness that can further compromise data integrity. The value of IoT in food supply chains has attracted several explorations in the literature [21-23]; however, the issue of data provenance and integrity in IoT-enabled food supply chains mostly remains unexplored. In response, this paper will conduct an exploratory research into this issue.

2.2. Blockchain and IoT integration

Since the invention of blockchain as a distributed ledger technology that can enable a time-stamped series of trackable and immutable data records in a decentralized network, a range of applications in many areas such as finance [28], design [29], and agriculture [30]. The decentralised, verifiable, and immutable characteristics of blockchain have seen it increasing adoption for improving supply chain traceability and product provenance [31-38]. Although Blockchain offers supply chain transparency and ensure the immutability of data recorded on the distributed ledger, there raises the concern about the integrity of the data relevant to supply chain events in machine-to-human interactions as it does not have the capability to ascertain the authenticity of data uploaded by supply chain actors [5]. The integration of IoTs and blockchain is proposed as a solution to ensure data provenance and integrity [5,17,19]. The use of IoT devices waive on-site or remote human intervention for data collection and transfer [23]. When the data stored on the blockchain system come from the IoT devices, rather than the input from humans, the risk of malicious data manipulation can be significantly minimised and accordingly the authenticity and trust of the data on the blockchain system can be improved. Some researchers argue the IoT system can also benefit from the integration with blockchain which has the capability to ensure information safe and secure through cryptography [39,40]. In this regard, the integration of blockchain technology and IoT is seen as an appropriate solution to address the data relevant issues of trust, security, privacy and integrity in the IOT enabled environment [41-43]. Although it seems that blockchain and IoT are a perfect pair in the digital world as they complement the limitations of the other, there are several challenges [44-46]. As previously noted [47, 48], applying blockchain in IoT applications entails various issues inherent to blockchain technology, such as computation, storage, communication latency, and energy incompatibility.

3. Approach

One of the first industry deployments of IoT and Blockchain was in the global diamond trade [49-51]. The application of IoT and DLT in diamond supply chains is different to food supply chains. The latter are usually characterised by high volume, low margin, diverse products and production processes (e.g. beef turns into steak, sausages, mince, etc.) and shorter lifespans viz. perishable or continually consumed [52,53]. While there are some emerging approaches involving novel IoT devices and forensic or analytical science such as Raman spectroscopy to analyse meat quality [54], identifying epigenetic markers as a proxy for a unique ID ('nature's own blockchain') [55,56], and consumable food additives either as labels or as invisible taste-neutral traceable ingredients [57, 58], the tight coupling between bits and atoms is far more difficult to achieve, cost-prohibitive, and arguably – as we outline below – not the only way to innovate food supply chains for integrity.

This paper reports our reflections on empirical observations and learnings from our ongoing beef supply chain project with BeefLedger (beefledger.io), which is an integrated provenance, blockchain security and payments platform. BeefLedger is a general purpose technology platform project, utilising blockchain technologies, that seeks to harness a diverse range of product provenance information as a basis of improved payments and confidence amongst supply chain participants in the beef supply chain [73].

Through the BeefLedger project, we developed a platform by which consumers can validate the credentials of the product they are purchasing, and drive efficiencies in the supply chain by reducing information asymmetries between transacting parties. Different from existing work by [2,5], BeefLedger combines the blockchain's attribute of being a robust validator of historic states (as a record of past events) and the power of crypto-economics to drive incentivised systems shaping behavioural optimisation in beef supply chains.

We begin by presenting the design architecture for integrating IoT and Blockchain for supply chain event tracking and beef provenance assurance (Fig. 1), which has guided the design and deployment of IoT and Blockchain DLT in beef supply chain for the sake of data integrity, provenance trust and better social, ecological and economic outcomes in a broad range of industry and societal context. While the argument presented in this paper is grounded in learnings from empirical observations and research surrounding the BeefLedger project, our contribution is better characterised as one of theoretical reflections.

4. BeefLedger project-based observations and learnings

Ours are possibly provocative claims, particularly when much discourse on IoT and blockchain in food supply chains revolves around ideas of re-instituting trust, and delivering transparency and truth. On these points we demur. Our learnings indicate that IoT and blockchain's potential lies in the more feasible possibilities of improving food supply chain outcomes without the need to presuppose trust or truth.

4.1. IoT and Blockchain in food supply chains

Our project learnings of the integration of IoT and blockchain are generalisable to the context of food supply chains. Let's begin by restating some fundamentals about blockchains and their properties:

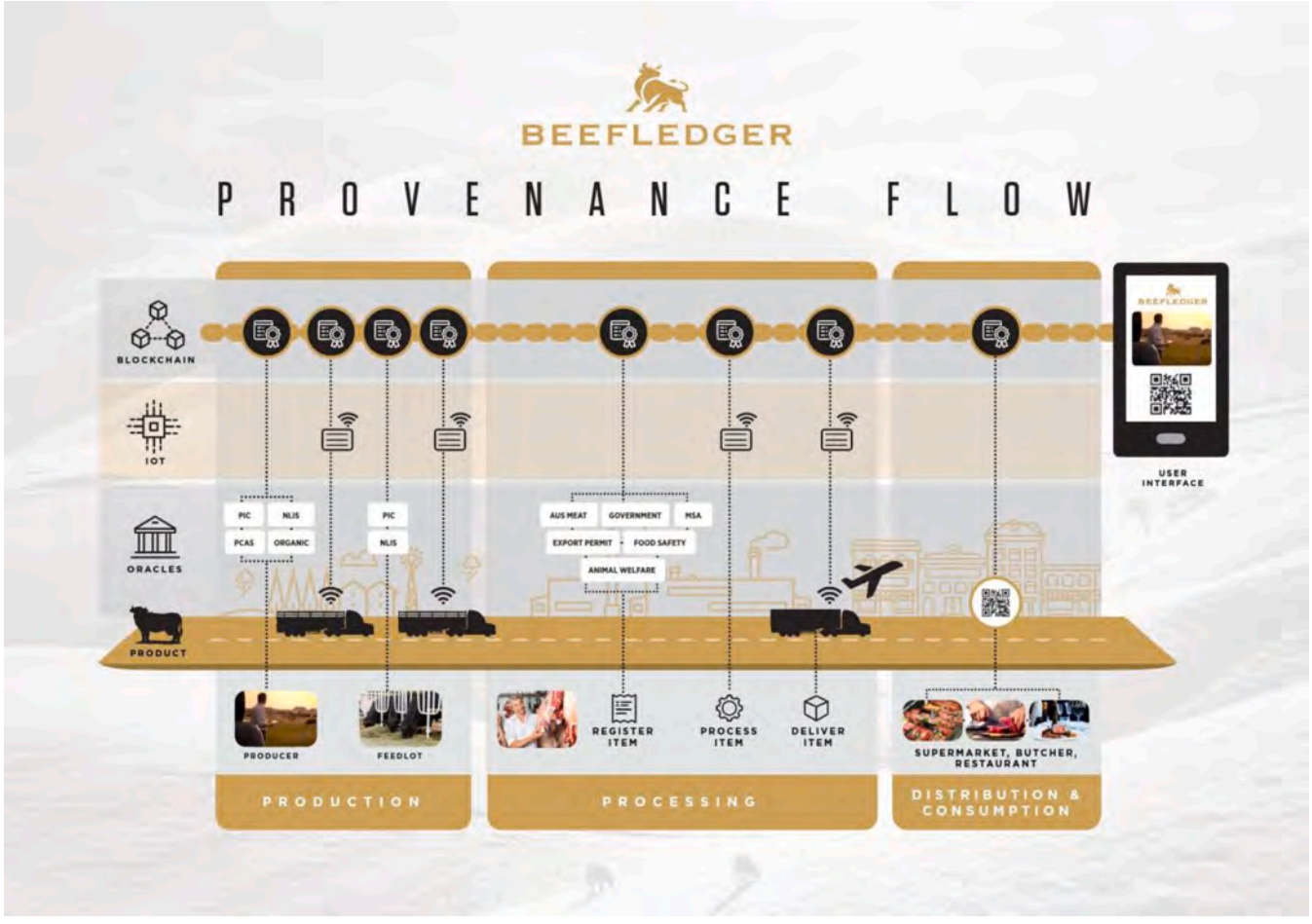

Fig. 1. BeefLedger's Blockchain and IoT-enabled beef supply chain architecture. Source: authors.

i Blockchains are good at ensuring that the application data state is valid, that is, the state was matched with the virtue of a process that followed explicit rules.
ii The process itself is transparent to the participating network of actors, so they can see what the rules are and how states transitioned from one to another.
iii The states as recorded are irreversible and immutable.
iv The data is censorship and fraud resistant, meaning altering or blocking data cannot be done singularly and capriciously. These properties are achieved by a consensus mechanism that enables the secure updating of a state in accordance with specific state change rules, where the right to perform the state update is distributed amongst a set of network agents.

It is for these reasons that many have been drawn to the possibilities of IoT and Blockchain systems to deliver an immutable record of events in food supply chains. Here, claims around traceability are postulated as a core attribute of blockchains. Indeed, a data structure based on Merkle Trees and block hashes enables the 'tracing' of any state via its link to previous states and so on. This is a data traceability truism. It is useful for a host of reasons, predominantly enabling a proof of data state validity, and therefore a valuable attribute. In this sense, this is the 'rear view mirror' property of blockchains: They are a lag indicator, a record of the past, just like all other ledgers that came before it.

Despite the merits of these attributes, they do not obviate the issues of data capture and the validity itself of the data submitter(s). This goes in the first instance to the garbage in, garbage out problem, and secondly to issues about the relationship between the digital and the physical world. These two points sit at the heart of most critical reactions to claims about food product traceability using blockchain, because – so the criticism goes – tracing data does not prove that the thing itself has any of the attributes claimed by the data, and that data on a blockchain may simply be immutable garbage.

4.2. Transactional dependability in conditions of zero trust

The mainstream literature posits that the deployment of blockchain technologies in supply chain ecosystems enhances trust between supply chain partners. Our learning is that it is about increasing transactional dependability in conditions of zero trust at best, and distrust or mistrust at worst, rather than the instituting trust in the first instance. Transactional dependability refers to the presence of information asymmetry amongst participants as the basis of actor decision-making and conduct and the likelihood of actor behaviours and behavioural outcomes to meet required conditions. Should trust emerge at all via these dynamics and interactions, it is a by-product as an ephemeral condition produced through human interactions [29,59]. This is in contrast to non-trust relationships, such as between unfamiliar humans and between humans and non-humans (machines). Not unrelated is the idea that trustworthiness is a result of safety and dependability [60]. Market design, therefore, must be about safety and dependability for participants, and trustworthiness is a residual consequence. Sabel [61] introduces the idea of "learning by monitoring" to explain successful collaboration, and signifies that trust is the consequence of learning embodied in ongoing monitoring.

Supply chains in complex financialised economies largely do not presuppose trust to function. A key feature of successful economies is that they involve the ability for strangers to engage in commerce [62]. Thus, transactions – the flow of goods and services on the one hand, and the flow of funds on the other – typically involve strangers and institutional agents. Functional supply chains require transactional dependability in conditions of zero trust. A zero trust environment is characterised by the presence of fundamental uncertainty as opposed to simply the presence of calculable risk [63].

4.3. Transparency is not a precondition of trust and data integrity

The integration of IoT and Blockchain in food supply chains can bring greater transparency to supply chain processes. However, transparency may not contribute to higher levels of trust due to the 'GIGO' issue that is still unsolved in the Blockchain and IoT enabled beef supply chain. The higher level of transparency may even lead to lower levels of trust if data integrity is not assured. With this understanding, supply chain transparency is not a sufficient precondition of trust and data integrity, but is an indisputable precondition for accountability processes. Much discussion [e.g., 64] claims that there is a significant social cost to establishing trust for supply chain transactions, via mechanisms and institutions such as 'the rule of law,' and various associated arbitration and court systems, etc. Rather than the costs of establishing trust, these are better understood as the costs of dealing with the consequential uncertainty of outcomes of non-trust and the costs exacted upon particular parties due to counterparty non-performance or change of circumstances. The existence of legally enforceable contracts, governing supply chain transactions, which include punishments in the event of non-performance, is symptomatic of a zero trust environment [65]. If parties trusted each other, there would be no reason for such contracts. Blockchains in supply chains will not hasten the demise of legally enforceable contracts.

Transparency is a necessary condition for data dependability in conditions of zero trust. It is however not a condition of the existence of trust. When there is trust between two actors, transparency is not needed. In other words, when one's word is as good as one's bond, there is no requirement for transparency beyond the promise. Transparency is demanded, because there is no trust. For one party to "just say so" is not enough for the other to accept the claim or the promise. Where there is, at best, zero trust, actors demand a level of transparency that is not necessary where there is trust. Blockchains are dependable in conditions of zero trust amongst a network of strangers for the very reason that each stranger is both watching everyone else and is also being watched by everyone. (Again, if trust emerges then that is a by-product.) This is the *panopticon* effect of blockchain consensus algorithms [66,67].

5. Data integrity solutions and discussion

We proposed three responses to addressing problems of data integrity: the identity of the data oracle (Section 5.1); the validity of the information based on notions of common knowledge (5.2), and; data integrity assurance mechanisms (Section 5.3).

5.1. Oracle identity for data integrity

Oracles – a source and communicator of data about things or situations – can be devices, actively or passively collecting data about certain things or conditions and/or some form of exogenous authority, e.g., a food certification, or by an act of law, e.g. food safety inspection. This data is foundational as a record of the past; and is also necessary to drive state changes via self-executing smart contracts. If the data source is exogenous to the blockchain itself, risks of false identities (imposters) and bad raw data exist. The relationship between the physical world and the digital ledger is what is at issue here. Because of this, some blockchain critics argue that blockchains cannot deliver 'true provenance,' because that can only be delivered via forensic or analytical science. The problem is actually the epistemological claim itself, and neither the hype nor the critic can resolve the reductive conundrum.

A food-laboratory-as-oracle cannot be taken as given. In the first instance, we have an identity issue. Fortunately, cryptographic tools can tackle this quite effectively. The second issue is that the knowledge that the lab produces in fact comes in the form of an artifact, which emerges through a set of procedures utilising a range of equipment, operated by certain lab personnel. The artifact is the lab report. All of these techniques, implements and agents are situated in specific socio-economic

contexts, which can impinge on their conduct [68]. How is it that we accept that the lab technician undertaking the procedure is capable? In what ways can we be confident that the right procedure was followed? Do we know that the equipment was in good condition and was appropriately calibrated? When was it last tested? What economic pressure is there impacting the work of the lab?

We actually do not need to solve this set of problems for blockchain-validated data to be meaningful in food supply chain authentication and state change processes, which support the core purposes of supply chains and can address sub-optimal outcomes occasioned by capricious action. A range of approaches can be mobilised to deal with risks associated with identities and data validity. From a blockchain point of view alone, We do not treat Blockchain in isolation from other approaches and adopt a pragmatic complementary approach, likening different interventions as threads that can assist in securing confidence in the food supply chain. Our project looks to things such as decentralised validation protocols for networks of devices (for instance), decentralised protocols for identity validation, multi-sig data proposal and game theory-inspired voting mechanisms on data proposals, and the introduction of cryptographic tools like Zero Knowledge Proofs to validate data oracles without compromising their status (and, therefore, opening them up to imposter attack risks).

Within an IoT and blockchain-enabled supply chain environment, Blockchains can be used to prove when Oracle X sent a message and can also prove that Oracle X did not send a message. On this basis, blockchain can prove that some set of messages is the entire set of messages that some set of participants sent. In other words, blockchain, combined with cryptography, can increase the extent to which users can have confidence that they are not being cheated. And if they are being cheated, they are not being cheated in isolation. This is because messages sent by Oracle X must assume the status of common knowledge. If we can be satisfied that a message (data) was made and sent by an oracle, and complied with the rules of the consensus algorithm, then the relevant socio-economic network – in our case, a network of food supply chain agents – can proceed with certain decisions and actions on the basis that the oracle and data are valid. In so doing, the message and its contents assume the status of common knowledge. Satisfaction that the identity of the oracle is valid is, in this environment, a question for the multitudes rather than something that can simply be asserted by way of fiat.

5.2. Common knowledge for data validity

Informational dependability is not about the absolute truth or the view from nowhere in any epistemological sense [69]. Rather, it is about the establishment of a body of common knowledge upon which actors can go about their business wherein the downside risks of action taken on the basis of asymmetric information relations is mitigated. Common knowledge is not the same as absolute truth [70,71]. Epistemology deals with the relationship between two domains; the domain of knowledge on the one hand (sometimes described as the thought or language domain), and the domain of the thing-in-itself (the physical world). For example, we accept the procedures of genetic testing as a means by which a knowledge about biological objects can be generated; or that chemical trace analysis makes certain truth claims about provenance in a very specific sense. With this understanding, we dispel the myth that deploying blockchain is about delivering an absolute truth. This is an important point in our argument and system design, because this also deals with a range of associated conflations that have resulted in a misdiagnosis of IoT and blockchain's opportunities for better supply chain outcomes (the hype) and misplaced criticisms (the anti-hype).

Common knowledge is the basis upon which much coordination between supply chain actors takes place. If a body of knowledge is accepted by a consensus mechanism to be valid, it then forms the basis upon which those actors who participate in the consensus mechanism can go about making decisions and undertaking actions. Blockchains and their consensus mechanisms are the means by which messages created and delivered are either rejected or accepted into the 'cannon of common knowledge.' We do not presuppose that common knowledge has any epistemological properties at all. If we err, we err together, is the consolation in these circumstances. For example, if traditional approaches to institutional sources of truth confer an authority status on certain agents, we have a need to validate the identity of the agent in the first place. But that still leaves open the question of the knowledge artifact. Whereas the agent may make a claim that its artifact is valid, a decentralised approach to common knowledge production would turn this authority on its head: only the multitudes can determine the validity of the artifact insofar as the applicable set of agents rely upon a common knowledge for action and coordination. In this case, we need to understand that (a) the way in which common knowledge is accepted in a blockchain ecosystem makes no claims about truth or otherwise in an epistemological or positivist sense, and; (b) valid does not necessarily mean 'Truth.' On this basis, we only need valid common knowledge for food supply chain functionality.

5.3. Data integrity assurance mechanism

A data integrity assurance mechanism can be created with a data valorisation mechanism. Fig. 2 illustrates our data valorisation mechanisms *for the blockchain and IoT-enabled beef supply chain.* Aligning valid data states with value distribution protocols implies the creation of new markets that facilitate adaptive behaviours towards new desirable outcomes. We, therefore, introduce a powerful tool in food supply chains that is given rise to by IoT and Blockchain – namely, the possibility of creating coherent units of value via native cryptocurrencies, which could, perhaps, result in new behavioural 'markets' within food supply chain activities that reward valid data contributions and punish invalid (false) data contributions. The crypto economics dimension is forward looking, whereas for the most part, claims about the blockchain and what it can do for food supply chain veracity are focused on a blockchain's capacity to be a record of the past. What we can start to think through to design from a forward looking perspective, is how to maximise the probability that future desired states are realised and are relatively stable via the mobilisation of game theoretic ideas anchored in modes of behavioural incentivisation and dis-incentivisation [72].

Smart contracts (as persistent coded procedures stored and executed on a blockchain) are the state change tools to achieve these kinds of valorised links between actions and rewards. By aligning payments with realising desired future (data) states which are in themselves validated as common knowledge via blockchain protocols, one effectively has, prima facie, a mechanism by which behaviours can be shaped. Rather than presuppose the establishment of trust as a condition precedent of successful food supply chains, we posit behavioural dynamics that simply assume actors will prefer to avoid punishment or loss, and access rewards instead. We avoid the notion of 'maximisers' in any narrow sense. This is because we accept that actors in fact can and do frame rewards and punishments in complex, socially embedded ways, in which financial gain (loss) from a particular transaction is but one dimension – albeit in food supply chain calculus a crucial one. Data states have the validity and dependability of the blockchain consensus mechanism behind them. Furthermore, smart contracts are also executed on a blockchain so that the self-executing and self-enforcing properties are also quarantined from capricious alteration, censorship and malfeasance. Both of these properties are inherently capricious-proof. Another example could see the value of improved ecological outcomes in the production of food valorised and paid via explicit accounting, and the linking of consumer value and payment to activities (validated by data states) further up the chain. We could do similar things on the basis of data states about animal welfare as well as to reward actions that contribute to the provision of 'healthy' food versus 'unhealthy' food.

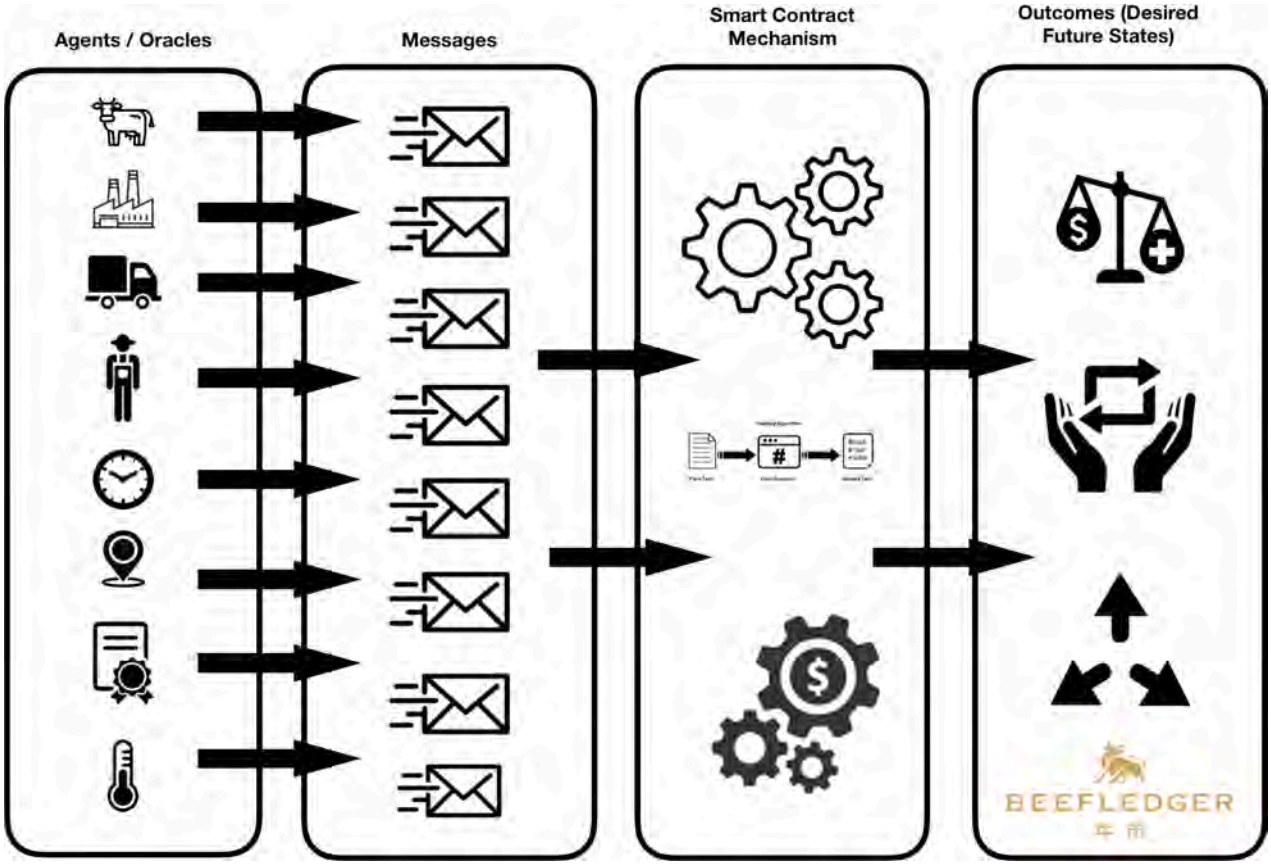

Fig. 2. Mechanism schematic of the blockchain and IoT-enabled beef supply chain. Source: authors.

6. Conclusions

If blockchains can be valuable records of the past, from our perspective, this is only the beginning of their potential. The capacity to formalise mechanisms for common knowledge formation amongst a group of agents opens up the possibility of not only historic validation but also the framing of desired future possibilities. Recalling that blockchains are good at ensuring data states are valid, we can now unshackle blockchains from being merely ledgers of the past and liberate their potential as specifiers of desired future states. Not only can desired future (data) states be specified, we can utilise blockchains to design mechanisms that link analogue behaviours in the wild to the realisation of desired futures wherein the extent of success can be confirmed by valid data states. We thus have the potential in the first instance to limit the possibility of capricious claims on performance; and secondly, we can design mechanisms by which behaviours that increase the probability of desired future states being realised can be encouraged.

In summary, the capacity of IoT and blockchain technology to support food supply chain improvements comes not so much from the technology's capacity to deliver a ledger of past events, though this is certainly useful especially in conditions where there are doubts about the product journey. Rather, it comes from the ability to deploy the technology in forward-looking ways to specify desired (future) data states and create incentive mechanisms by which actions required to meet those data states are economically justifiable. By removing or at the very least severely limiting the possibility of capricious action, the risks associated with incurring additional costs to pursue the required actions are also diminished. None of this presupposes truth or trust. Instead, the power of IoT and blockchains in food supply chains is premised on more mundane foundations: common knowledge and capricious-free dependability.

CRediT authorship contribution statement

Warwick Powell: Conceptualization, Writing – original draft. **Marcus Foth:** Writing – original draft, Writing – review & editing. **Shoufeng Cao:** Writing – review & editing. **Valéri Natanelov:** Writing – original draft.

Declaration of Competing Interest

Adjunct Professor Warwick Powell is a Director of BeefLedger Ltd.

Acknowledgements

This project was supported by funding from QUT, BeefLedger Ltd as well as the Food Agility CRC Ltd, funded under the Commonwealth Government CRC Program. The CRC Program supports industry-led collaborations between industry, researchers and the community.

References

[1] S. Mondal, K.P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, P. Chahal, Blockchain inspired RFID-based information architecture for food supply chain, IEEE Internet Things J. 6 (2019) 5803–5813, https://doi.org/10.1109/JIOT.2019.2907658.

[2] T.K. Dasaklis, F. Casino, C. Patsakis, Defining granularity levels for supply chain traceability based on IoT and blockchain, in: Proceedings of the International Conference on Omni-Layer Intelligent Systems, Association for Computing Machinery, New York, NY, USA, 2019, pp. 184–190, https://doi.org/10.1145/3312614.3312652.

[3] F. Tian, An agri-food supply chain traceability system for China based on RFID blockchain technology, in: 2016 13th International Conference on Service Systems and Service Management (ICSSSM), 2016, pp. 1–6, https://doi.org/10.1109/ICSSSM.2016.7538424.

[4] M. Kanellos, How big data and IoT initiatives render the "garbage in, garbage out" theory invalid, 2019. https://iottechnews.com/news/2019/oct/01/how-big-data-

and-iot-initiatives-render-garbage-garbage-out-theory-invalid/ (accessed April 2, 2021).
[5] S. Malik, V. Dedeoglu, S.S. Kanhere, R. Jurdak, TrustChain: trust management in blockchain and iot supported supply chains, in: 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 184–193, https://doi.org/10.1109/Blockchain.2019.00032.
[6] Y. Qin, Q.Z. Sheng, N.J.G. Falkner, S. Dustdar, H. Wang, A.V. Vasilakos, When things matter: a survey on data-centric internet of things, J. Netw. Comput. Appl. 64 (2016) 137–153, https://doi.org/10.1016/j.jnca.2015.12.016.
[7] MLA, Australia becomes the most valuable beef exporter, Meat Livestock Australia (2020). https://www.mla.com.au/prices-markets/market-news/australia-becomes-the-most-valuable-beef-exporter-in-2019/ (accessed July 2, 2020).
[8] PwC, Fighting $40bn food fraud to protect food supply, PricewaterhouseCoopers (2016). https://www.pwc.com.au/press-room/2016/food-fraud-jan16.html (accessed July 2, 2020).
[9] C. Babbage, Passages from the Life of a Philosopher, Longman, Green, Longman, Roberts, & Green, London, UK, 1864.
[10] C. Zhang, Y. Chen, A review of research relevant to the emerging industry trends: industry 4.0, IoT, blockchain, and business analytics, J. Ind. Intg. Mgmt. 05 (2020) 165–180, https://doi.org/10.1142/S2424862219500192.
[11] G. Aceto, V. Persico, A. Pescapé, Industry 4.0 and health: internet of things, big data, and cloud computing for healthcare 4.0, J. Ind. Inf. Integrat. 18 (2020) 100129, https://doi.org/10.1016/j.jii.2020.100129.
[12] C. Perera, A. Zaslavsky, P. Christen, D. Georgakopoulos, Context aware computing for the internet of things: a survey, IEEE Commun. Surv. Tutor. 16 (2014) 414–454, https://doi.org/10.1109/SURV.2013.042313.00197.
[13] A. Karkouch, H. Mousannif, H. Al Moatassime, T. Noel, Data quality in internet of things: a state-of-the-art survey, J. Netw. Comput. Appl. 73 (2016) 57–81, https://doi.org/10.1016/j.jnca.2016.08.002.
[14] J. An, X. Gui, W. Zhang, J. Jiang, J. Yang, Research on social relations cognitive model of mobile nodes in Internet of Things, J. Netw. Comput. Appl. 36 (2013) 799–810, https://doi.org/10.1016/j.jnca.2012.12.004.
[15] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Netw. 54 (2010) 2787–2805, https://doi.org/10.1016/j.comnet.2010.05.010.
[16] A. Whitmore, A. Agarwal, L.Da Xu, The Internet of Things—a survey of topics and trends, Inf. Syst. Front. 17 (2015) 261–274, https://doi.org/10.1007/s10796-014-9489-2.
[17] B. Liu, X.L. Yu, S. Chen, X. Xu, L. Zhu, Blockchain based data integrity service framework for IoT data, in: 2017 IEEE International Conference on Web Services (ICWS), 2017, pp. 468–475, https://doi.org/10.1109/ICWS.2017.54.
[18] G. Matsemela, S. Rimer, K. Ouahada, R. Ndjiongue, Z. Mngomezulu, Internet of things data integrity, in: 2017 IST-Africa Week Conference (IST-Africa), 2017, pp. 1–9, https://doi.org/10.23919/ISTAFRICA.2017.8102332.
[19] U. Javaid, M.N. Aman, B. Sikdar, BlockPro: blockchain based data provenance and integrity for secure IoT environments, in: Proceedings of the 1st Workshop on Blockchain-Enabled Networked Sensor Systems, Association for Computing Machinery, New York, NY, USA, 2018, pp. 13–18, https://doi.org/10.1145/3282278.3282281.
[20] A. Čolaković, M. Hadžialić, Internet of Things (IoT): a review of enabling technologies, challenges, and open research issues, Computer Networks 144 (2018) 17–39, https://doi.org/10.1016/j.comnet.2018.07.017.
[21] Y. Zhang, L. Zhao, C. Qian, Modeling of an IoT-enabled supply chain for perishable food with two-echelon supply hubs, Ind. Manag. Data Syst. 39 (2017) 88, https://doi.org/10.1108/IMDS-10-2016-0456.
[22] A. Pal, K. Kant, IoT-based sensing and communications infrastructure for the fresh food supply chain, Computer 51 (2018) 76–80, https://doi.org/10.1109/MC.2018.1451665.
[23] C.N. Verdouw, J. Wolfert, A.J.M. Beulens, A. Rialland, Virtualization of food supply chains with the internet of things, J. Food Eng. 176 (2016) 128–136, https://doi.org/10.1016/j.jfoodeng.2015.11.009.
[24] F. Casino, V. Kanakaris, T.K. Dasaklis, S. Moschuris, S. Stachtiaris, M. Pagoni, N. P. Rachaniotis, Blockchain-based food supply chain traceability: a case study in the dairy sector, Int. J. Prod. Res. (2020) 1–13, https://doi.org/10.1080/00207543.2020.1789238.
[25] Data quality dimensions, in: C. Batini, M. Scannapieca (Eds.), Data Quality: Concepts, Methodologies and Techniques, Springer, Berlin, Heidelberg, 2006, pp. 19–49, https://doi.org/10.1007/3-540-33173-5_2.
[26] A. Klein, W. Lehner, Representing data quality in sensor data streaming environments, J. Data Inf. Qual. 1 (10) (2009) 1–10, https://doi.org/10.1145/1577840.1577845, 28.
[27] A. Sheth, Internet of things to smart IoT through semantic, cognitive, and perceptual computing, IEEE Intell. Syst. 31 (2016) 108–112, https://doi.org/10.1109/MIS.2016.34.
[28] H. Hassani, X. Huang, E. Silva, Banking with blockchain-ed big data, J. Manag. Anal. 5 (2018) 256–275, https://doi.org/10.1080/23270012.2018.1528900.
[29] M. Foth, The promise of blockchain technology for interaction design, in: Proceedings of the 29th Australian Conference on Computer-Human Interaction, ACM, 2017, pp. 513–517, https://doi.org/10.1145/3152771.3156168.
[30] A. Kamilaris, A. Fonts, F.X. Prenafeta-Boldú, The rise of blockchain technology in agriculture and food supply chains, Trends Food Sci. Technol. 91 (2019) 640–652, https://doi.org/10.1016/j.tifs.2019.07.034.
[31] H.M. Kim, M. Laskowski, Toward an ontology-driven blockchain design for supply-chain provenance, Intell. Syst. Account. Finance Manag.. 25 (2018) 18–27. https://doi.org/10.1002/isaf.1424.
[32] K. Toyoda, P.T. Mathiopoulos, I. Sasase, T. Ohtsuki, A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain, IEEE Access 5 (2017) 17465–17477, https://doi.org/10.1109/ACCESS.2017.2720760.
[33] M.S. Ferdous, K. Biswas, M.J.M. Chowdhury, N. Chowdhury, V. Muthukkumarasamy, Integrated platforms for blockchain enablement. Advances in Computers, Elsevier, 2019.
[34] Feng Tian, An agri-food supply chain traceability system for China based on {RFID} amp; blockchain technology, in: 2016 13th International Conference on Service Systems and Service Management ({ICSSSM}), 2016, pp. 1–6.
[35] N. Hackius, M. Petersen, Blockchain in logistics and supply chain: trick or treat?, in: Hamburg International Conference of Logistics (HICL) 2017, epubli, 2017, pp. 3–18, https://doi.org/10.15480/882.1444.
[36] M.A. Amr, M.M. Eljazzar, S.S. Kassem, M. Ezzat, Merging Supply Chain and Blockchain Technologies, in: Proceedings of the 28th International Conference for the International Association of Management of Technology (IAMOT), National Institute of Industrial Engineering, Mumbai, India, 2019, pp. 224–228. ISBN 978-93-88237-54-3.
[37] K. Salah, N. Nizamuddin, R. Jayaraman, M. Omar, Blockchain-based soybean traceability in agricultural supply chain, IEEE Access 7 (2019), https://doi.org/10.1109/ACCESS.2019.2918000, 1–1.
[38] G. Zhao, S. Liu, C. Lopez, H. Lu, S. Elgueta, H. Chen, B.M. Boshkoska, Blockchain technology in agri-food value chain management: a synthesis of applications, challenges and future research directions, Comput. Ind. 109 (2019) 83–99, https://doi.org/10.1016/j.compind.2019.04.002.
[39] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: the blockchain model of cryptography and privacy-preserving smart contracts, in: 2016 IEEE Symposium on Security and Privacy (SP), 2016, https://doi.org/10.1109/sp.2016.55.
[40] M. Shen, X. Tang, L. Zhu, X. Du, M. Guizani, Privacy-Preserving Support Vector Machine Training Over Blockchain-Based Encrypted IoT data in smart cities, IEEE Internet Things J. 6 (2019) 7702–7712, https://doi.org/10.1109/JIOT.2019.2901840.
[41] B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, M. Peng, When internet of things meets blockchain: challenges in distributed consensus, IEEE Netw. 33 (2019) 133–139, https://doi.org/10.1109/MNET.2019.1900002.
[42] W. Viriyasitavat, T. Anuphaptrirong, D. Hoonsopon, When blockchain meets Internet of Things: characteristics, challenges, and business opportunities, J. Ind. Informat. Integrat 15 (2019) 21–28, https://doi.org/10.1016/j.jii.2019.05.002.
[43] D. Minoli, B. Occhiogrosso, Blockchain mechanisms for IoT security, Internet of Things 1-2 (2018) 1–13, https://doi.org/10.1016/j.iot.2018.05.002.
[44] Y. Lu, Blockchain: a survey on functions, applications and open issues, J. Ind. Intg. Mgmt. 03 (2018) 1850015, https://doi.org/10.1142/S242486221850015X.
[45] Y. Lu, Blockchain and the related issues: a review of current research topics, J. Manag. Anal. 5 (2018) 231–255, https://doi.org/10.1080/23270012.2018.1516523.
[46] Y. Lu, The blockchain: state-of-the-art and research challenges, Journal of Ind. Inf. Integrat. 15 (2019) 80–90, https://doi.org/10.1016/j.jii.2019.04.002.
[47] I. Makhdoom, M. Abolhasan, H. Abbas, W. Ni, Blockchain's adoption in IoT: the challenges, and a way forward, J. Netw. Comput. Appl. 125 (2019) 251–279.
[48] X. Wang, X. Zha, W. Ni, R.P. Liu, Y.J. Guo, X. Niu, K. Zheng, Survey on blockchain for Internet of Things, Comput. Commun. 136 (2019) 10–29, https://doi.org/10.1016/j.comcom.2019.01.006.
[49] N. Kshetri, Blockchain and the economics of customer satisfaction, IT Prof. 21 (2019) 93–97, https://doi.org/10.1109/MITP.2018.2881299.
[50] U.W. Chohan, Blockchain and the Extractive Industries: Cobalt Case Study, SSRN Elsevier, 2021, https://doi.org/10.2139/ssrn.3138271 https://doi.org/.
[51] S. Underwood, Blockchain beyond bitcoin, Commun. ACM. 59 (2016) 15–17, https://doi.org/10.1145/2994581.
[52] G. Farr-Wharton, J.H.-J. Choi, M. Foth, Food talks back: exploring the role of mobile applications in reducing domestic food wastage, in: Proceedings of the 26th Australian Computer-Human Interaction Conference on Designing Futures: The Future of Design, ACM, 2014, pp. 352–361, https://doi.org/10.1145/2686612.2686665.
[53] G. Farr-Wharton, M. Foth, J.H.-J. Choi, Identifying factors that promote consumer behaviours causing expired domestic food waste: factors promoting behaviours causing food waste, J. Consumer Behav. 13 (2014) 393–402, https://doi.org/10.1002/cb.1488.
[54] S.M. Fowler, H. Schmidt, R. van de Ven, D.L. Hopkins, Preliminary investigation of the use of Raman spectroscopy to predict meat and eating quality traits of beef loins, Meat Sci 138 (2018) 53–58, https://doi.org/10.1016/j.meatsci.2018.01.002.
[55] J. Van Doren, D. Grahek-Ogden, J. Richardson, F. Abbinante, C. Cascio, P. Devalier, N. Brun, I. Linkov, K. Marchal, B. Meek, C. Pagliari, I. Pasquetto, P. Pirolli, S. Sloman, L. Tossounidis, E. Waigmann, H. Schünemann, H. Verhagen, Managing evidence in food safety and nutrition, in: E.K.C.A.H.A. Devos Y (Ed.), Proceedings of the Third EFSA Scientific Conference: Science, Food and Society, 2019, https://doi.org/10.2903/j.efsa.2019.e170704.
[56] A. Schumacher, Chapter 23 - epigenetics of aging and longevity: challenges and future directions, in: A. Moskalev, A.M. Vaiserman (Eds.), Epigenetics of Aging and Longevity, Academic Press, Boston, 2018, pp. 499–509, https://doi.org/10.1016/B978-0-12-811060-7.00023-1.
[57] M. Puddu, D. Paunescu, W.J. Stark, R.N. Grass, Magnetically recoverable, thermostable, hydrophobic DNA/silica encapsulates and their application as invisible oil tags, ACS Nano 8 (2014) 2677–2685, https://doi.org/10.1021/nn4063853.
[58] M. Creydt, M. Fischer, Blockchain and more - algorithm driven food traceability, Food Control 105 (2019) 45–51, https://doi.org/10.1016/j.foodcont.2019.05.019.
[59] R.C. Solomon, Trusting, heidegger, coping, and cognitive science: essays in honor of Hubert L, Dreyfus 2 (2000) 229–244.

[60] A.E. Roth, Who Gets What—and Why: The New Economics of Matchmaking and Market Design, Houghton Mifflin Harcourt, 2015. http://assets1c.milkeninstitute.org/assets/Publication/MIReview/PDF/65-82-MR68.pdf.
[61] C.F. Sabel, Studied trust: building new forms of cooperation in a volatile economy, Hum. Relat. 46 (1993) 1133–1170, https://doi.org/10.1177/001872679304600907.
[62] P. Murphy, The stranger society: the case of economic and social development in the tropics, Budhi: A Journal of Ideas and Culture 19 (2016) 107–134. https://journals.ateneo.edu/ojs/index.php/budhi/article/view/BU2015.19204 (accessed November 29, 2019).
[63] J.M. Keynes, A Treatise on Probability. A Treatise on Probability, Courier Corporation, London, 2013.
[64] S. Davidson, M. Novak, J. Potts, The cost of trust: a pilot study, The JBBA 1 (2018) 1–7, https://doi.org/10.31585/jbba-1-2-(5)2018.
[65] O.E. Williamson, Calculativeness, trust, and economic organization, J. Law Econ. 36 (1993) 453–486, https://doi.org/10.1086/467284.
[66] J. Bentham, The Panopticon, Offenders or Citizens? Readings in Rehabilitation, Willan, London, 2012, pp. 13–15, https://doi.org/10.4324/9780203722855-8.
[67] M. Foth, T. Heikkinen, J. Ylipulli, A. Luusua, C. Satchell, T. Ojala, UbiOpticon: participatory sousveillance with urban screens and mobile phone cameras, in: Proceedings of The International Symposium on Pervasive Displays, ACM, 2014, p. 56, https://doi.org/10.1145/2611009.2611034.
[68] B. Latour, S. Woolgar, Laboratory Life: The Construction of Scientific Facts, Princeton University Press, Princeton, NJ, 2013. ISBN 9780691028323.
[69] M. Foth, N. Odendaal, G. Hearn. The view from everywhere: towards an epistemology for urbanites, Academic Conferences Limited, London, United Kingdom, 2007, pp. 127–133. https://eprints.qut.edu.au/9149/.
[70] R. Fagin, J.Y. Halpern, Y. Moses, M. Vardi, Reasoning About Knowledge, MIT Press, Cambridge, MA, 2004. ISBN 9780262562003, https://mitpress.mit.edu/books/reasoning-about-knowledge.
[71] J.-J.Ch. Meyer, W. van der Hoek, Epistemic Logic for AI and Computer Science, Cambridge University Press, Cambridge, UK, 2004. https://www.cambridge.org/9780521602808. ISBN 9780521602808.
[72] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, F. Wang, Blockchain-enabled smart contracts: architecture, applications, and future trends, IEEE Trans. Syst. Man Cybern. 49 (2019) 2266–2277, https://doi.org/10.1109/TSMC.2019.2895123.
[73] Cao Shoufeng, Powell Warwick, Foth Marcus, et al., Strengthening consumer trust in beef supply chain traceability with a blockchain-based human-machine reconcile mechanism, Computers and Electronics in Agriculture (180) (2021), 105886, https://doi.org/10.1016/j.compag.2020.105886.