THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-7-1-(2)2024

Improving the Trustworthiness of Traceability Data in Food Supply Chain Using Blockchain and Trust Model

Oratile Leteane, Yirsaw Ayalew
University of Botswana, Gaborone, Botswana

Correspondence: 200808199@ub.ac.bw
Received: 19 December 2023 **Accepted**: 15 January 2024 **Published**: 16 February 2024

Abstract

The food supply chain is characterised by its complexity and interconnectedness, involving various actors, from farmers to consumers. It emphasises the critical importance of maintaining product integrity, safety, and quality throughout the process to meet stringent regulatory standards and consumer expectations. However, food supply chain is plagued by challenges such as counterfeiting, quality issues, and safety concerns, prompting the adoption of product traceability as a remedy. Current traceability systems (e.g., systems based on centralised and EPCIS architectures) aim to capture traceability data from the initial link to the final link in the supply chain, allowing for tracing a product from the end consumer back to its origin. Nevertheless, trust issues persist in these systems, particularly concerning the integrity and reliability of traceability data. Blockchain has been proposed to address these trust issues by creating an immutable and transparent ledger distributed across all peers. Despite this innovation, different studies underscore the inadequacy of relying solely on blockchain to ensure the trustworthiness of traceability data. This paper addresses this gap by proposing an adaptable and extensible framework that combines blockchain with a multi-trust packages-based trust model. The framework seeks to strengthen trust relationships among supply chain actors by improving the accuracy of identifying specific areas within the supply chain where compromises in quality and safety have occurred.

Keywords: *Traceability, Trust Metrics, Trust Score, Trust Package, Trust Package Smart Contract, Metrics Developer, Trust Model, Blockchain, Data Trust*

JEL Classifications: *D82, D85*

1. Introduction

Several scandals and recalls resulting from quality and safety compromise, as well as product counterfeiting, have been reported from supply chains around the world [1–4]. Many lives have been lost due to quality and safety compromise problems. For example, regarding food supply chains, the World Health Organisation reported that an estimated 600 million people become sick because of consuming food products and 420,000 end up dying [5]. This has resulted in many consumers losing trust in supply chains. To address this issue, several studies have suggested end-to-end traceability [6–8]. End-to-end traceability can provide an audit trail in the movement of a product in the supply chain [9], which helps detect quality and safety issues at the early stages of the supply chain [10]. It also makes product recalls to be managed systematically [11] and shortens the time taken to trace and pinpoint exactly where the product might have been compromised [12]. In food and pharmaceutical supply chains, many governments have taken the initiative to make traceability a legal obligation to protect consumers [13, 14].

To support traceability processes in supply chains, automated traceability systems are being used. These traceability systems can store traceability data in centralised repositories [15] or in repositories using distributed ledger technologies such as blockchain [16–19]. Centralised traceability systems provide non-tamper-proof data repositories. However, repositories whose data can be tampered with have data trust problems, as nothing stops the parties from tampering with the data to favour their interests [10]. Therefore, traceability systems based on a centralised approach fail to protect traceability data from the possibility of tampering [20, 21]. Although blockchain can provide tamper-proof repository, Powell et al. [20] argue that there exists a Garbage in Garbage Out (GIGO) problem with the blockchain approach. This is because blockchain does not have the capability to correct faulty and malicious data from the source to the ledger. To address the GIGO problem, Malik et al. [22], Dedeoglu et al. [21], and Al-Rakhami and Al-Mashari [23] proposed approaches that

integrate blockchain and trust model, referred to in this study as blockchain + trust model approach. In this approach, the trust model's role is to establish trust in the ecosystem by computing the degree of trust (trust score) and associating the score with the network participants and data, while the blockchain provides tamper-proof repository. To develop trust models, trust metrics (TMs) are used. TMs are vital in determining whether a trust model accurately computes trust [24, 25].

In blockchain + trust model frameworks, a single set of TMs is used to quantify and compute trust scores. Using trust models that rely on a single TMs set to solve the trust problem is less effective because (1) as traceability data is generated by different data sources in different supply chain links, different sets of trust metrics are required to quantify trust values effectively; (2) whenever there are changes in the supply chain trust needs (e.g., new data produced in the supply chain), the framework's degree of accuracy in estimating trust score becomes low. This is because new trust requirements need different metrics to accurately compute trust. We agree with the views of other researchers that the problem can be solved by addressing the data trust problem [26, 8, 20, 21]. Therefore, our approach is to develop a framework that improves the end-to-end trustworthiness of traceability data by assessing the trustworthiness of traceability data and storing both data and associated trust values in a tamper-proof repository.

The remainder of this article is organised as follows: Section 2 discusses the existing traceability frameworks; Section 3 presents the proposed framework; Section 4 discusses the case study; Section 5 provides a description of how trust metrics are developed; Section 6 presents the evaluation procedure for the framework; Section 7 discusses the limitations of this research, and Section 8 summarises the main points of the research and future work.

2. Related work

The literature presents several frameworks that attempt to address the problem of data trust. The frameworks can be categorised into three based on their architectural designs [8]. These include centralised [15, 27], blockchain [28], and blockchain + trust model [21].

In a centralised architecture, data from the supply chain is sent to a centralised repository mainly hosted in wide area networks. Some systems use one central repository, while others have distributed repositories. Electronic Product Code Information Service (EPCIS) is an example of a distributed centralised repositories network. EPCIS network has an extra repository called Discovery Service, whose function is to route the data requests from traceability applications to the right EPCIS data servers and re-route the queried data back to the requesting traceability applications. Central repositories are managed by intermediaries in the supply chain [29, 15]. Whenever traceability is needed, the central data repository is queried by traceability systems to acquire the data used for tracing the product. Traceability in this approach is solely dependent on the central data repositories. In all traceability systems based on a centralised architecture, intermediaries can tamper with the data and, hence, do not adequately address data trust issues in the supply chain [21, 22, 26, 48].

In blockchain architecture, traceability data from the supply chain is evaluated for validity by a consensus mechanism and, if valid, then passed into an immutable ledger. However, one of the drawbacks with the current blockchain consensus mechanism is that it cannot verify data veracity [20, 21]. The merits of this approach lie in the following: (1) there is a high level of transparency as nodes can always see data from other peers, which many researchers claim it encourages nodes to be honest. It should be noted that transparency is observed at different levels depending on the type of blockchain. In public blockchains, the same ledger is visible to all members; therefore, transparency is guaranteed to all members of the blockchain, while in consortium and private blockchains, transparency is at the group members level (those with common ledger). For example, in the Hyperledger Fabric consortium blockchain, transparency is limited to those within the same cluster. In this study, transparency is discussed in the context of consortium blockchains featuring a shared ledger among members; (2) immutability of data once in the ledger.

Different researchers have proposed frameworks using this architecture. To control the distribution of counterfeit products in pharmaceutical supply chains, Kumar and Tripathi [31] developed a traceability system that uses blockchain technology and quick response (QR) code. In their traceability system, the encrypted QR code consists of the details of the medicine that a pharmaceutical company manufactures, and the information is stored in the immutable ledger. In agri-food supply chains, Lin et al. [32] integrated blockchain and Long-Range Radio (LoRa) IoT-based architecture and demonstrated that minimising manual data entry by humans improves trust in food supply chains. A similar approach was also proposed by Tan, Gligor, and Ngah [33], who developed a traceability system using blockchain technology for tracing and confirming the authenticity of halal products. Similarly, Walmart piloted a blockchain traceability system on mango and pork supply chains, showing that traceability can be reduced from seven days to 2.2 seconds [19]. The blockchain approach provides the advantages of transparency, immutable ledger, and consensus mechanism that filter invalid data from entering the ledger. Since there is a lack of a mechanism to check the trustworthiness of the data before entering the ledger, the current blockchain is not sufficient to guarantee the trustworthiness of traceability data [8, 21, 22, 49]. This has also been observed by Powell et al. [20], who highlighted the GIGO problem.

To address the drawbacks highlighted in the blockchain-based approaches, blockchain + trust model approach has been proposed. The trust model is introduced to establish trust in the blockchain network so that both network nodes

and data flowing into the network can be trusted to a certain degree. Trust and trustworthiness are two concepts used in the development of trust models. Trust is drawn from human life and, as Sagar et al. [24] highlighted, "It is a fundamental aspect of human life for building relationships with each other." Research in trust cuts across various disciplines, such as psychology [34, 35], sociology [36, 37], economics [38, 39], and computer science [40–46]. What is common in all the disciplines is that there is a trustor and trustee. The trustee makes a promise by sharing information, and the trustor accepts to rely on the information that the trustee will fulfil the promise. Computer science has multiple domains where the concept of trust is applied. These include software engineering [40], networking [41], data trust [42, 43], artificial intelligence [44], and web management [45, 46]. In these areas, trust is associated with the trustor and it is the behaviour displayed by the trustor based on the trustworthiness of the trustee. Thus, trustworthiness is a characteristic displayed by the trustee.

Our focus in this research is on addressing trust in traceability data for supply chains. Accordingly, trust models are built to mathematically quantify trustworthiness in a particular domain and context [47]. In the existing trust models, the quantified value is the measure of the trustworthiness of the trustee. It is mostly referred to as the trust score. Trust models typically normalise trust scores to fall between 0 and 1. 0 implies no trust at all, while 1 means full trust. Low trust values are those near 0, and high trust values are those near 1.

Few frameworks have been observed in the literature developed using this approach. These include Malik et al. [22], Al-Rakhami and Al-Mashari [23], Dedeoglu [21], and Rouhani and Deters [48]. Malik et al. [22] suggested trust metrics for generating trust scores that measure the level of quality and safety of the product. This means that a trust score close to 1 implies high quality and safety of the product. However, the framework does not adequately address the trust problem in traceability data. The IoT devices are vulnerable to data security compromise [60]. This is because: (1) the devices are heavily dependent on batteries for power supply, which makes them vulnerable to energy-depletion attacks [61]; (2) the devices have a limited amount of memory and processing power, incapable of running complex cryptographic security algorithms [62]. Since IoT devices are vulnerable to so many security attacks, there is no guarantee that the data from the devices used by the framework to calculate trust scores is not malicious.

Al-Rakhami and Al-Mashari [23] and Rouhani and Deters' [48] frameworks attempt to assess trust in the data using blockchain + trust model approach. The problem with the frameworks is the use of one set of trust metrics. A supply chain comprises a consortium that contributes to and records various traceability data for a product. The consortium uses diverse data sources and using one set of trust metrics by these frameworks is a bottleneck in accurately assessing the trustworthiness of traceability data. For example, if there is a supply chain link that uses GPS devices to send location data about a product and another supply chain link that uses temperature and humidity sensors to capture data about the environmental conditions of the perishable products storage, using a single set of trust metrics cannot accurately assess data from GPS devices and environmental condition sensory data. Thus, using one set of trust metrics is limited in computing accurate trust scores.

3. Adaptive and extensible framework

We propose the development of a framework which improves the trustworthiness of traceability data across all the links of a supply chain. The framework uses different packages of TMs to quantify trust into numerical values. Figure 1 shows the different components of the framework. These include trust model, ledgers, access management, metrics management module, application management module, supply chain and metrics developers.

The trust model comprises two smart contracts: metrics selection smart contract and trust computation smart contract. Overall, the trust model evaluates the data produced by data sources found in the supply chain links to check its validity in terms of trust. The trust model then computes trust scores and sends data and computed trust scores to the blockchain ledger. The trust model uses the metrics selection smart contract to select an appropriate trust package developed for trust assessment of the generated data. Trust packages refer to a set of TMs and the instructions on how they are used to establish trust. The metrics selection smart contract is triggered when an application sends data from the data generator to the blockchain. Trust computation smart contract uses the trust package to compute trust and send the data and trust score to the ledger. The data repositories consist of two main ledgers: the metrics ledger shaded green and the base ledger shaded grey. The base ledger stores traceability data and trust scores. This protects data and trust scores from tampering. Metrics ledger, on the other hand, stores different trust packages. TMs are protected in the ledger because of their criticality for accurately assessing trust scores. Metrics developers continuously assess the effectiveness of existing trust packages, and if some are seen to be less effective, then they develop new trust packages to replace them. Also, if new data generators generate data that none of the existing packages can assess for trust, then metrics developers develop trust packages to address those trust needs. This makes the framework to be more effective and relevant. The application module provides an interface between the blockchain ledger and end-user applications. Traceability systems used by end users will communicate load traceability data from the ledger by interacting with this module.

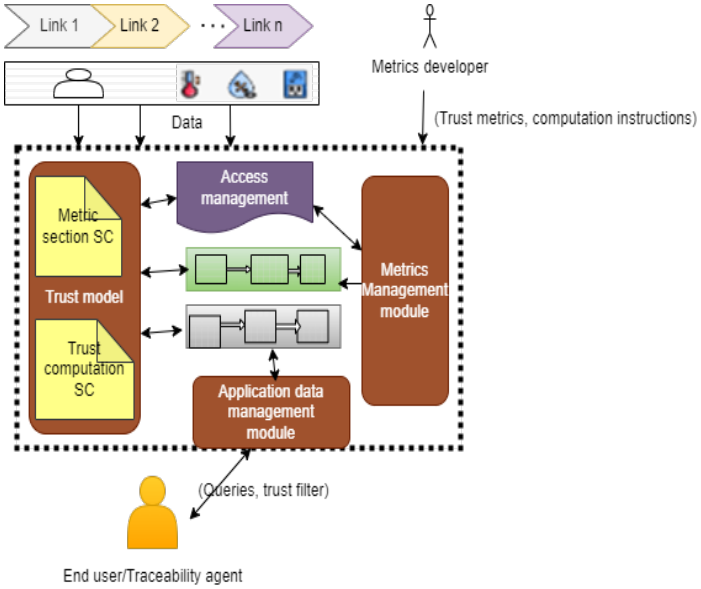

Figure 1. Framework for enhancing trust in supply chain links. Adapted from [25].

The supply chain is plugged into the framework, and data generators are available to generate data from traceability units and send it to the blockchain network. Data generators[1] may involve manual entry by a human being who observes the product, or it can be an autonomous set-up where various sensors transmit data to the network. Metrics developers are members of the consortium whose sole responsibility is to provide the framework with appropriate trust packages for efficient computation of trust scores. This helps the framework to be up to date in accurately computing trust scores.

4. Case study

Botswana beef supply chain is chosen as a case study. The two farming methods practised at the farm link are free range and ranched. About 90% of farmers practise free range [50]. In terms of quantity and quality, Botswana is the biggest supplier of beef to the European Union (EU) from the African region [51]. While the Botswana beef supply chain is one of the top exporters of high-grade cattle meat from the continent [52], an audit by Engelen et al. [50] highlighted issues related to data trust. Due to traceability data trust, the country was temporarily banned from exporting to the EU [50] and, in 2023, lost one of the lucrative markets in Norway [53].

Beef supply chain links have been identified from the Botswana Agri-food Value Chain Project [50] and attached to the framework as an off-chain pluggable component. Figure 2 shows the links extracted from the report. The Botswana beef supply chain currently uses a centralised traceability system called Botswana Animal Identification and Traceability System (BAITS) [54, 55].

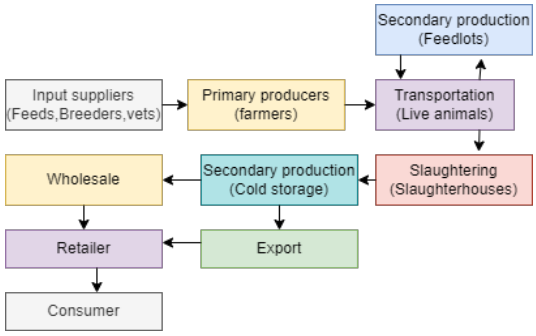

Figure 2. Product transformation links in Botswana beef supply chain.

5. Trust packages development

We used the guidelines provided by Leteane and Ayalew [25] to identify trust metrics and use them to develop trust packages for the Botswana beef supply chain. For demonstration purposes, trust packages for farm and cold room links are developed.

5.1 Trust at the farm link

Trust issues mainly emerge from free-range farming because it is difficult to monitor the location of the cattle. Botswana has different zones to identify areas affected by diseases such as foot and mouth disease (FMD). One of the major requirements of the EU market is that all meat products should be coming from disease-free zones. Assuring the markets that the cattle come from free-range farming has never passed through the FMD zones remains a big challenge. Collecting real-time data of cattle movement using IoT devices in this supply chain would be ideal. Nevertheless, the integrity and truthiness of the data from IoT devices could be compromised, resulting in data trust problems. Therefore, it is important to develop a trust package that the framework can use to enhance trust in the data coming from the cattle using IoT devices.

The location of cattle data is collected from a GPS device. The devices are attached to the cattle and continually send GPS coordinates to the blockchain network through the internet. In the above data source, where IoT devices generate the data, there is a correlation between data quality and trust. Therefore, data trust issues may arise from what Byabazaire, O'Hare and Delaney [56] identify as intrinsic data quality dimensions. The dimensions include problems associated with data quality and integrity, provenance, and abnormality. While we acknowledge that all the dimensions must be addressed for data trust to be enhanced, data trust is broader, and quality does not always mean trust. Since existing approaches can be used to enhance data quality, we focus on the metric that improves trust in the data. The following factors are identified to help extract the trust metrics: (1) device malfunction (hardware and software)

[1] In our case study, data generators are restricted to IoT sensory devices.

– we argue that a device with valid calibration is likely to generate correct data; (2) data tampering – IoT devices are known to have limited security features and are vulnerable to data attacks. For example, a node in the network can change its behaviour to become an adversary and try to inject malicious data into the ledger. This kind of attack can be addressed by both temporal and spatial sensory data correlation and by evaluating the trust score of the data item. In the free-range farming set-up where cattle can go astray and graze on their own, there are challenges with spatial data as there will be reliance on one sensor. Temporal correlation of time series data is likely to evaluate and provide high accuracy of trust in this scenario; (3) the battery problems (low battery or high power consumption) – devices with low battery are likely to generate faulty data, and devices with high power consumption are likely to be malicious [57]. This can be addressed by monitoring the battery level and usage. Thus, to compute the trust values of data from IoT devices, device calibration, battery level and consumption, and temporal correlation are used as TMs.

Device calibration: To quantify trust for device calibration trust metrics, a value of 1 is assigned if the device is calibrated; otherwise, a value of 0 is assigned, as shown in Equation (1).

$$T_v = \begin{cases} 0, & \text{if not calibrated or date expired} \\ 1, & \text{Calibrated} \end{cases} \quad (1)$$

Battery level and consumption: When the battery level goes below some threshold, the likelihood of the device producing correct data becomes low [57]. Also, malicious nodes are known to consume more energy than usual. Therefore, we chose energy level and consumption as one of the trust metrics of the data coming from IoT devices. We use two thresholds as follows: α = maximum energy consumption. Any node consuming energy above this threshold is considered malicious and produce untrustworthy data; ρ = minimum energy level. A device whose energy level is lower than ρ is considered to produce erroneous data that cannot be trusted. Like in [57], 5% is reasonable ρ. However, the appropriate threshold value can be chosen based on the application use case. The rate of consumption ΔE and energy level E_c are computed as:

$$E_c = E_{t+1} \quad (2)$$

$$\Delta E = E_t - E_{t+1} \quad (3)$$

Where $E_c < \rho \Rightarrow$ incorrect data produced and $\Delta E > \alpha \Rightarrow$ energy level trust value $T_e = 0$.

In Equation (4), we quantify the energy trust metrics using both E_c and ΔE to produce trust value as follows:

$$T_e = \begin{cases} 0, & if\ E_c < \rho\ or\ \Delta E > \alpha \\ 1, & Otherwise \end{cases} \quad (4)$$

Temporal correlation: Due to the movement of cattle, there is a gradual change in location data. As in [58], temporal features of the location data over time are used in changing the TMs to numerical values. The GPS sensor provides data as latitudes and longitudes. To use these latitudes and longitudes for estimating distance, we use Haversine's formula as in Equation (5). Let's denote the distance between two points (previous and current position) to be R_y. We use average deviation to compute distance deviation tolerance.

$$R_y = 2 \times R \times sin^{-1}\left(\sqrt{sin^2(\emptyset_2 - \emptyset_1) + cos(\emptyset_1) \times cos(\emptyset_2) \times sin^2(\Psi_2 - \Psi_1)}\right) \quad (5)$$

where R represents the earth's radius, $\emptyset_1$ and $\emptyset_2$ represent latitudes, Ψ1 and Ψ2 represent the longitudes.

To determine whether the data is trusted or not, we use the average deviation, like Zhang [59]. After calculating the distance covered, we determine the tolerance value range. The tolerance value range is used to determine the trust value. To determine the tolerance value, we look at the latest normal behaviour of the cattle movement. We consider five days of normal behaviour data and use it to define the tolerance value range. Five days is chosen to use just enough data to observe general distance coverage daily. We limit history data to five days since using large data covering more than five days can affect the efficiency of the framework by taking a long time to process data. On the other hand, using less data covering less than five days may not give the accurate behaviour of cattle movement. Let D represent the normal behaviour data for five consecutive days. The average of distances covered within a fixed defined time duration in D is R_0, and the degree of deviation of each distance is δ. If the degree of deviation $\delta_i > 0$, then an outlier exists that can be used to estimate the degree of trust in the incoming data.

$$R_0 = (R_1 + R_2 + R_3 + \ldots + R_n)/n \quad (6)$$

In Equation (6), there are n positions, and the nth position is represented by Rn. The deviation in the movement of cattle is calculated as follows:

$$\lambda_i = |R_y - R_0|\ i = 1,2,\ldots,n \quad (7)$$

In this formula, sample data is represented as R_y. The deviation in the expected distance of coverage is:

$$\delta_i = \lambda_i / R_0 \quad (8)$$

Next, we calculate the average sum of deviations from the previous samples. This gives us the approximate deviation of every sample. Thus, every deviation is expected to be close to the average degree of deviation. The average deviation and

average coverage distance are used to set the tolerance threshold. The tolerance value is calculated using Equations (9) and (10):

$$\Delta = \sum \frac{\delta_i}{n} \tag{9}$$

$$\eta = \Delta \times R_0 \tag{10}$$

We then check whether the incoming radius of coverage falls within the range of (R_0–η, R_0 + η). If the radius falls within the range, then the trust score Tc for the metrics is considered high and falls within the range $50 < ts < 100$. Otherwise, the trust score is low and falls in the $0 < Tc < 50$ range. Hence, we qualify the data set as trusted if the trust score is 0.5 or higher and not trusted if it is below 0.5. Tc is calculated as:

$$T_c = \begin{cases} 1 & if\ \lambda = 0 \\ 1 - \delta\ if\ \lambda > 0\ and\ R_0 - \eta \le \lambda \le R_0 + \eta \\ 0.5 \times \delta & Otherwise \end{cases} \tag{11}$$

The total trust score (Ts) represents the total trust score aggregated from all three TMs of the location. The choice of aggregation technique is determined by metrics developers based on the technique that gives better accuracy.

A weighted sum is chosen in this case for demonstration, as shown in Equation (12). Equation (5) gives the actual distance of coverage between two positions over a time window. The time window is defined at the time of sensor configuration.

$$T_s = w_1 T_v + w_2 T_e + w_3 T_c, w_1 + w_2 + w_3 = 1 \tag{12}$$

where w_1, w_2, and w_3 are weights of each TM. The weights are assigned based on the importance of the TM to the overall trust score.

5.2 Trust at the cold room links

IoT temperature and humidity sensors are used to collect and forward the data to the framework. Here, we are interested in ensuring that the data represents the actual condition of the environment where the product is stored. Unlike in location data, sensors are not mobile. However, the first two trust metrics from the previous section remain important as sensors depend on battery and correct calibration to provide trusted data. Thus, we use the battery management and calibration metrics again. According to Karthik and Ananthanarayana [57], a correlation exists between data from a sensor and data from neighbouring sensors. We consider the spatial correlation of the sensory data from all the sensors in the same room. It is suggested that multiple similar sensors be used in the same room to collect the same environmental condition data [43]. The expectation is that the data generated by the sensors must be almost the same. A correlation coefficient of data from all the sensors in the cluster observing the same phenomena is calculated and used to represent the trust score. Equation (15) is used to compute the trust score for spatial correlation of data. Let $\boldsymbol{Sen_i}$ be a sensor in a room with a set of $\boldsymbol{S}$ sensors measuring the same phenomena, in this case, temperature. Then, we calculate the mean as:

$$\mu = \frac{\sum_{i=1}^{n} sen_i}{n}, \forall sen_i \in \boldsymbol{s} \tag{13}$$

and the deviation of the sensory data as:

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(sen_i - \mu)^2} \tag{14}$$

The trust score is given by subtracting the correlation coefficient from the possible highest trust score:

$$T_{sp} = 1 - \left(\frac{\sigma}{\mu}\right) \tag{15}$$

Like in the previous package, a weighted sum is used to aggregate all trust scores from the metrics to compute the total trust score. Thus,

$$Total\_trust_{cold} = \alpha T_{corr} + \beta T_{sp} + \gamma T_{Batt}, \alpha + \beta + \gamma = 1 \tag{16}$$

ALGORITHM 1 BATTERY LEVEL

Input: $Battery_{level}$
Output: $Battery_{trustscore}$
$Battery_{thrsd} \leftarrow 0.05$
if $(Battery_{level} \le Battery_{thrsd})$ ***&*** $(consumption \le \theta)$ ***then***
  $TS_{bat} \leftarrow 1$
else
  if $(Battery_{level} \ge Battery_{thrsd})$ ***&*** $(consumption_{rate} \le \theta)$ || $(Battery_{level} \le Battery_{thrsd})$***&*** $(consumption_{rate} \le \theta)$ ***then***
    $TS_{bat} \leftarrow 0$
  else
    $TS_{bat} \leftarrow 1 - Battery_{level}$
  end if
end if
return TS_{bat}

5.3 Developing trust packages smart contracts

Each trust package is added to the framework as a special smart contract called trust package smart contract (TPSC). Four algorithms are provided below and used by the TPSC to quantify and compute trust from data coming from supply chain links.

The sensor collects environment data and proposes the transaction to the blockchain. Algorithm 1 is used by TPSC when data is sent from the supply chain to the framework. TPSC uses algorithm 1 to compute the trust score for battery-level trust metrics. The computation is based on Equations (2)–(4). Algorithm 2 computes trust score for the calibration trust metrics. TPSC uses the algorithm to get the trust score for the metrics and is used in computing the total trust score for the data. TPSC also uses algorithm 3 to compute trust score for temporal correlation metrics. The algorithm uses Equations (5)–(11) to compute the trust score. Then, TPSC uses Equation (12) to compute the trustworthiness of the location data. The sensor triggers the appropriate TPSC for computing the trust score for the data and passes the data together with the trust score to the ledger. Algorithms 1–3 use Equations (1)–(12) to compute the trust score.

ALGORITHM 2 CALIBRATION_DATA

Input: *Validation expiry date*
Output: *Total trust score for calibration (TS_cal)*

if *validation expiry date*≤ ***today then***
  $calibration_{valid} \leftarrow$ ***TRUE***
else
  $calibration_{valid} \leftarrow$ ***FALSE***
End if
If $calibration_{valid}$ = ***TRUE then***
  $TS\_cal \leftarrow 1$
else
  $TS\_cal \leftarrow 0$
End if
Return *TS_cal*

The trust package that computes the trust score of the data from the GPS data source in the farm link uses algorithms 1–3. The TPSC takes the quantified trust metrics values and uses weighted sum aggregation to compute the final trust score for the data. The trust score is then passed to the smart contract that writes the data and trust score to the blockchain ledger. Algorithm 4, on the other hand, is used by the TPSC to compute the trust score for the data coming from cold storage links. When the sensors send environmental condition data, it triggers the appropriate TPSC smart contract to execute. The TPSC then uses algorithm 4 and returns the trust score written with data to the blockchain ledger.

ALGORITHM 3 TEMPORAL CORRELATION TRUST SCORE

Input: *PosLat, PrevLat, PosLong, PrevLong, PrePos (latitudes and longitudes of previous and current positions)*
Output: *Total trust score based on data temporal correlation*

$R \leftarrow 6371$ *//Radius of the earth as a constant*
$Sleepdur \leftarrow 720$ *(maximum time in minutes of no movement)*
if *(PosLat = PrevLat) & (PosLong = PrevLong)* ***then***
  Total trust score $\leftarrow 0$
else
  $dlat \leftarrow |PosLat - PrevLat|$
  $dlon \leftarrow |PosLong - PrevLong|$
  $coverage_{Radius} \leftarrow sine(dlat/2)^2 + cosine(PrevLat) \times cosine(PosLat) \times sine(dlon/2)^2$
  $Actual_{distance} \leftarrow (2R \times sine^{-1}(\sqrt{coverage_{Radius}})$
  $Prev_{Averages} \leftarrow \frac{\sum_{i=1}^{5} ave\_d_i}{5}$
  $Deviation \leftarrow |Actualdistance - PrevAverages|$
  if *Deviation = 0* ***then***
    trust score $\leftarrow 1$
  else
    $deviation_{degree} \leftarrow \frac{Deviation}{Prev_{Averages}}$
    $Average_{deviations} \leftarrow \frac{\sum_{j=1}^{5} dailyDeviation_j}{5}$
    $tolC \leftarrow Average_{deviation} + Prev_{Averages}$ *//(maximum tolerance)*
    $tolF \leftarrow |Average_{deviation} - Prev_{Averages}|$ *//(minimum tolerance)*
    if $(deviation_{degree} \geq TolC)$ & $(deviation_{degree} \leq tolF)$ ***then***
      $Trust\_score = 1 - deviation_{degree}$
    else
      trust score $= 0.5 - deviation_{degree}$
    End if
  End if
End if
Return *trust_score*

5.4 Adding trust packages to the framework

After a trust package is developed, it must be accepted in the network by all affected supply chain actors for it to be used in the framework. The acceptance process is initiated by the metrics developer who wants the developed trust package to be used. If the package is accepted, then the metrics developer packages the accepted trust package as TPSC and adds it to the blockchain network.

ALGORITHM 4 TEMPERATURE DATA TRUST PACKAGE

Input: *Temperature and battery level data*
Output: *Total trust score for the cold room data*

$\mu \leftarrow \frac{\sum_{i=1}^{n} temp\_dataset_i}{tem\_dataset.size}$
$div \leftarrow \sqrt{\frac{1}{n}\sum_{i=1}^{n}(sen_i - \mu)^2}$
$corr_{coef} \leftarrow \frac{div}{\mu}$
$Trust_{spatial} \leftarrow 1 - corr_{coef}$
if $(Battery_{level} \geq Battery_{thrsd})$ & $(consumption\_rate \geq \theta)$ ***then***
  $TS_{bat} \leftarrow 1$
else
  if $(Battery_{level} \geq Battery_{thrsd})$ & $(consumption\_rate \leq \theta)$ || $(Battery_{level} \leq Battery_{thrsd})$ & $(consumption\_rate \leq \theta)$ ***then***
    $TSbat \leftarrow 0$
  else
    $TS_{bat} \leftarrow 1 - Battery_{level}$
  End if

13 **End if**
14 **if** $calibration_{valid}$ = **TRUE then**
15 $TS\_cal \leftarrow 1$
16 **else**
17 $TS\_cal \leftarrow 0$
18 **End if**
19 $Trust_{cold} \leftarrow \frac{Trust_{spatial}+TS_{bat}+TS\_cal}{3}$
20 **Return** $Trust_{cold}$

The cluster members accept the smart contract into the network. All the data from the supply chain is then proposed through the organisation's peer. The peer then selects and triggers the appropriate TPSC to compute the trust score. The metrics developers may now be given some incentives for successfully providing a useful trust package. However, the mechanism of providing incentives is outside the scope of this paper.

6. The development of the framework

We chose the Hyperledger Fabric blockchain platform. One key advantage is its modular architecture, allowing flexibility and customisation to meet diverse business requirements. Additionally, Hyperledger Fabric ensures enhanced privacy and permissioned access, making it well-suited for enterprise use, especially in industries where data confidentiality and fine-grained control over permissions are crucial. Its support for smart contracts and a pluggable consensus mechanism further contributes to its appeal for building the framework. As shown in Figure 3, data flows from the supply chain through the internet into the framework. Since the cattle being monitored are mobile, we recommend building a LoRaWAN

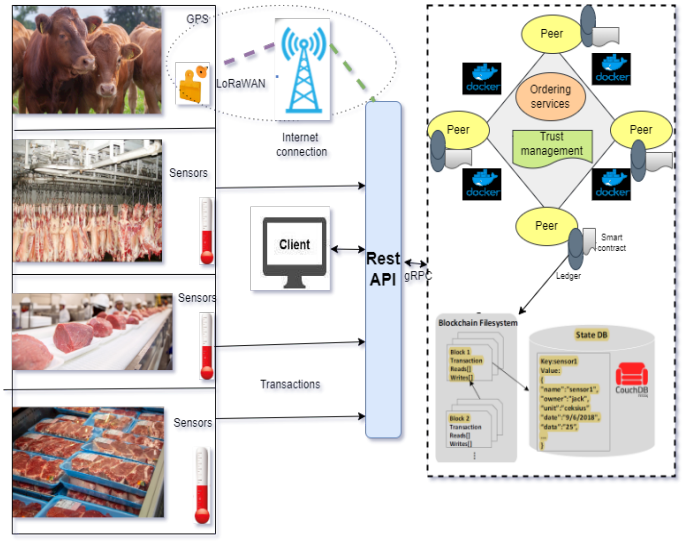

Figure 3. Implementation procedure.

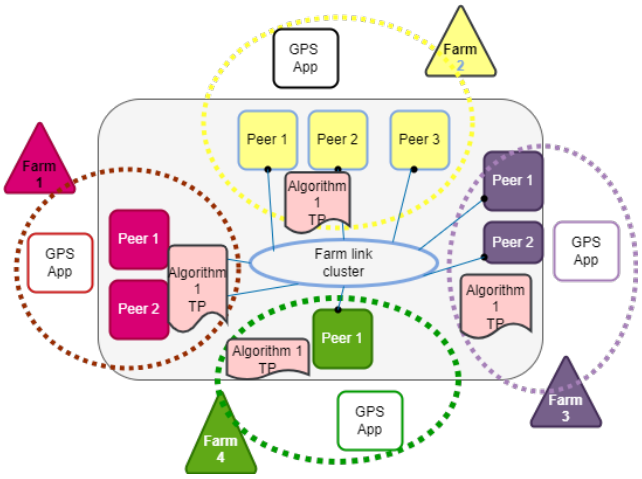

Figure 4. The farm link cluster.

network and attaching the LoRa end devices that sense and communicate GPS coordinates. In areas where there is no internet coverage, the gateway can communicate with the blockchain network through a GSM network. The LoRaWAN gateway will then redirect the data to the blockchain network, where the endorsement process will start. The fabric gateway will propose a transaction by sending the proposal to appropriate peers for endorsement signatures. The network set-up for the farm link cluster is shown in Figure 4. The procedure for adding location data to the ledger is as follows: the GPS data application proposes the transaction once the data is collected from the environment by connecting to the appropriate peers.

The phases starting with the endorsement to the commitment of the block to the ledger are followed. In this case, when data is proposed to be added to the ledger, the triggered trust package smart contract is the one that uses algorithms 1–3. All data from a GPS sensor in the farm link will trigger this smart contract. Organisations in the cold room link also form a cluster in the blockchain network. Similarly, applications from temperature and humidity sensors propose transactions by sharing the proposal with appropriate peers for endorsement, ordering service, and then committing peers. In this cluster, endorsing and committing peers compute trust score by engaging trust package smart contract that uses algorithm 4. It is important to note that trust package smart contracts used in this cluster are different from those used in the farm link cluster, hence our idea of the use of multi-trust package to improve trust in traceability data in the supply chain.

7. Limitations of the study

Most farmers rear their cattle in rural areas where there is no internet coverage, limited network infrastructures, and no power supply grid. This poses a challenge in collecting real-time data on the correct movement and positions of the animals using network devices. An option to address this

challenge is to build the infrastructure from scratch. Developing economies still face financial constraints to develop such infrastructure, hence low-power wireless area networks (LPWAN) are considered to be the most appropriate options. To address the challenge in our case study, we considered building LoRaWAN network with just a single gateway and 14 end devices to collect real-time data from the farm link. To tackle the power issue, solar panels will be utilised to supply power to the gateway.

To collect the data, LoRa end devices are attached to the cattle's neck. An adversary can potentially penalise the farmer by disconnecting the devices from the cattle and allowing them to enter the FMD zone. In this case, the data in our framework, which may be rated highly trusted, may not be true about the cattle. However, an approach proposed in [63] can be used to prevent the detaching of the LoRa end devices from live animal's neck. It can also be argued that an untrusted farmer may not attach the devices to the cattle but rather give them to herd boys or moving objects and still allow the cattle to graze in the FMD zones while our framework receives false data on the animal's location. The farmer can then attach the devices when it is time to take the cattle to the abattoir, where the data in our framework will perhaps suggest with a high degree of trust that the cattle has never grazed in the FMD zones. While this is a limitation in our case study, alternative devices such as rumen boluses with embedded RFID microchips can be used as end devices. The device is planted in the stomach of a cattle and starts sending signals to the gateway from the stomach [64]. The device is only removed when the cattle are slaughtered at the abattoir.
Another challenge in our framework is developing trust metrics to detect false data entered by a human being. A way around this is to limit human data entry using IoT devices. Thus, in the current implementation, our framework can evaluate trustworthiness of the data only from IoT devices. However, it should be noted that our framework has metrics developers whose sole responsibility in the network is to develop and provide trust packages. While trust packages that can detect the trustworthiness of data from manual entry seem to be far-fetched at the moment, we believe that with time, metrics developers may come up with such trust packages.

8. Conclusion

Current traceability frameworks do not adequately address issues of trustworthiness of the data. This makes it difficult to convince consumers that the traceability data represents the truth about the condition of the product they purchase for consumption. As a result, consumers lose trust in the quality and safety of products from supply chains. Our approach presented a framework that improves trust in traceability data by integrating blockchain with a trust model. We demonstrated how blockchain and trust model can be integrated in developing an adaptive and extensible framework. The use of blockchain ledger as a repository guarantees that no actor can tamper with the data to their favour at any time.

Our future work will focus on the evaluation of the framework and develop an incentive mechanism that can be used to reward metrics developers.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution
The two authors contributed equally to the manuscript.

Funding:
None declared.

Acknowledgement:
Not applicable.

References

[1] S. P. Gayialis, E. P. Kechagias, G. A. Papadopoulos, and D. Masouras, "A review and classification framework of traceability approaches for identifying product supply chain counterfeiting," *Sustainability*, vol. 14, no. 11, 6666, 2022.

[2] P. Danese, R. Mocellin, and P. Romano, "Designing blockchain systems to prevent counterfeiting in wine supply chains: A multiple-case study," *International Journal of Operations & Production Management*, vol. 41, no. 13, pp. 1–33, 2021.

[3] E. R. Blickem, J. W. Bell, D. M. Baumgartel, and J. Debeer, "Review and analysis of tuna recalls in the United States, 2002 through 2020," *Journal of Food Protection*, vol. 85, no. 1, pp. 60–72, 2022.

[4] W. Wu, A. Zhang, R. D. van Klinken, P. Schrobback, and J. M. Muller, "Consumer trust in food and the food system: A critical review," *Foods*, vol. 10, no. 10, 2021.

[5] The World Health Organisation, "Food safety," 2020. Available at https://www.who.int/news-room/fact-sheets/detail/food-safety.

[6] P. Jahanbin, The investigation of blockchain and IoT integration for designing trust-driver information systems in agricultural food supply chain. PhD thesis, The University of Canterbury, Christchurch, New Zealand, June 2022. Available at https://ir.canterbury.ac.nz/server/api/core/bitstreams/f4fa19ea-a083-4807-af9a-3bcf8123810c content.

[7] R. Cole, M. Stevenson, and J. Aitken, "Blockchain technology: Implications for operations and supply chain management," *Supply Chain Management: An International Journal*, vol. 24, no. 4, pp. 469–483, 2019.

[8] O. Leteane, Y. Ayalew, and T. Motshegwa, "A systematic review of traceability issues in beef supply chain

management," in *2021 IEEE International Conference on Big Data (Big Data)*, pp. 3426–3435, IEEE, 2021.

[9] G. Alfian, M. Syafrudin, N. L. Fitriyani, J. Rhee, M. R. Ma'arif, and I. Riadi, "Traceability system using IoT and forecasting model for food supply chain," *in 2020 International Conference on Decision Aid Sciences and Application (DASA)*, pp. 903–907, IEEE, 2020.

[10] 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)*, pp. 1–6, IEEE, 2016.

[11] T. K. Agrawal, V. Kumar, R. Pal, L. Wang, and Y. Chen, "Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry," *Computers Industrial Engineering*, vol. 154, p. 107130, 2021.

[12] L. C. H. Ghadafi, M. Razak, and M. Stevenson, "Supply chain traceability: A review of the benefits and its relationship with supply chain resilience," *Production Planning & Control*, vol. 34, no. 11, pp. 1114–1134, 2023.

[13] F. Fung, H.-S. Wang, and S. Menon, "Food safety in the 21st century," *Biomedical Journal*, vol. 41, no. 2, pp. 88–95, 2018.

[14] European Commission, "Regulation EC No 178/2002." https://eurlex.europa.eu/eli/reg/2002/178/oj, 2004.

[15] J. Feng, Z. Fu, Z. Wang, M. Xu, and X. Zhang, "Development and evaluation on a RFID-based traceability system for cattle/beef quality safety in China," *Food Control*, vol. 31, no. 2, pp. 314–325, 2013.

[16] R. Garrard and S. Fielke, "Blockchain for trustworthy provenances: A case study in the Australian aquaculture industry," *Technology in Society*, vol. 62, p. 101298, 2020.

[17] S. Cao, W. Powell, M. Foth, V. Natanelov, T. Miller, and U. Dulleck, "Strengthening consumer trust in beef supply chain traceability with a blockchain-based human-machine reconcile mechanism," *Computers and Electronics in Agriculture*, vol. 180, p. 105886, 2021.

[18] K. M. Botcha, V. V. Chakravarthy, and Anurag, "Enhancing traceability in pharmaceutical supply chain using internet of things (IoT) and blockchain," in *2019 IEEE International Conference on Intelligent Systems and Green Technology (ICISGT)*, pp. 45–453, 2019.

[19] R. Kamath, "Food traceability on blockchain: Walmart's pork and mango pilots with IBM," *The Journal of the British Blockchain Association*, vol. 1, no. 1, p. 3712, 2018.

[20] W. Powell, M. Foth, S. Cao, and V. Natanelov, "Garbage in garbage out: The precarious link between IoT and blockchain in food supply chains," *Journal of Industrial Information Integration*, p. 100261, 2021.

[21] V. Dedeoglu, R. Jurdak, G. D. Putra, A. Dorri, and S. S. Kanhere, "A trust architecture for blockchain in IoT," in *Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pp. 190–199, 2019.

[22] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Trustchain: Trust management in blockchain and IoT supported supply chains," in *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 184–193, IEEE, 2019.

[23] M. S. Al-Rakhami and M. Al-Mashari, "A blockchain-based trust model for the internet of things supply chain management," *Sensors*, vol. 21, no. 5, p. 1759, 2021.

[24] S. Sagar, A. Mahmood, Q. Z. Sheng, J. K. Pabani, and W. E. Zhang, "Understanding the trustworthiness management in the social internet of things: A survey," arXiv preprint arXiv:2202.03624, 2022.

[25] O. Leteane and Y. Ayalew, "An adaptive and extensible framework to enhance end to end trustworthiness of traceability data," in *2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA)*, pp. 1–8, IEEE, 2022.

[26] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain internet of things," in *2017 International Conference on Service Systems and Service Management*, pp. 1–6, IEEE, 2017.

[27] M. Thakur and E. Foras, "EPCIS based online temperature monitoring and traceability in a cold meat chain," *Computers and Electronics in Agriculture*, vol. 117, pp. 22–30, 2015.

[28] X. Yang, M. Li, H. Yu, M. Wang, D. Xu, and C. Sun, "A trusted blockchain-based traceability system for fruit and vegetable agricultural products," *IEEE Access*, vol. 9, pp. 36282–36293, 2021.

[29] A. Kassahun, R. J. M. Hartog, and B. Tekin-erdogan, "Realizing chain-wide transparency in meat supply chains based on global standards and a reference architecture," *Computers and Electronics in Agriculture*, vol. 123, pp. 275–291, 2016.

[30] G. Hartley, "The use of EPC RFID standards for livestock and meat traceability," New Zealand RFID Pathfinder Group, 2013.

[31] R. Kumar and R. Tripathi, "Traceability of counterfeit medicine supply chain through blockchain," in *2019 11th International Conference on Communication Systems Networks (COMSNETS)*, pp. 568–570, COMSNETS, 7–11 Jan. 2019.

[32] J. Lin, Z. Shen, A. Zhang, and Y. Chai, "Blockchain and IoT-based food traceability for smart agriculture,"

in *Proceedings of the 3rd International Conference on Crowd Science and Engineering*, pp. 1–6, 2018.

[33] A. Tan, D. Gligor, and A. Ngah, "Applying blockchain for halal food traceability," *International Journal of Logistics Research and Applications*, vol. 25, pp. 1–18, 2020.

[34] B. R. Schlenker, B. Helm, and J. T. Tedeschi, "The effects of personality and situational variables on behavioral trust," *Journal of Personality and Social Psychology*, vol. 25, no. 3, p. 419, 1973.

[35] S. M. Ghafari, "Towards time-aware context-aware deep trust prediction in online social networks," arXiv preprint arXiv:2003.09543, 2020.

[36] X. Zheng, Trust prediction in online social networks. PhD thesis, Macquarie University, Faculty of Science and Engineering, Department of, 2015.

[37] M. R. Welch, R. E. Rivera, B. P. Conway, J. Yonkoski, P. M. Lupton, and R. Giancola, "Determinants and consequences of social trust," *Sociological Inquiry*, vol. 75, no. 4, pp. 453–473, 2005.

[38] K. Jones and L. N. Leonard, "Trust in consumer- to-consumer electronic commerce," *Information & Management*, vol. 45, no. 2, pp. 88–95, 2008.

[39] R. E. Backhouse and S. G. Medema, "Retrospectives: On the definition of economics," *Journal of Economic Perspectives*, vol. 23, no. 1, pp. 221–233, 2009.

[40] M. T. Thielsch, S. M. Meeßen, and G. Hertel, "Trust and distrust in information systems at the workplace," *PeerJ*, vol. 6, p. e5483, 2018.

[41] K. N. Qureshi, G. Jeon, et al., "A trust evaluation model for secure data aggregation in smart grids infrastructures for smart cities," *Journal of Ambient Intelligence and Smart Environments*, vol. 13, no. 3, pp. 235–252, 2021.

[42] C. Dai, D. Lin, E. Bertino, and M. Kantarcioglu, "An approach to evaluate data trustworthiness based on data provenance," in *Secure Data Management: 5th VLDB Workshop, SDM 2008*, Auckland, New Zealand, August 24, 2008. Proceedings 5, pp. 82–98, Springer, 2008.

[43] H.-S. Lim, Y.-S. Moon, and E. Bertino, "Provenance-based trustworthiness assessment in sensor networks," in *Proceedings of the Seventh International Workshop on Data Management for Sensor Networks*, pp. 2–7.

[44] K. Siau and W. Wang, "Building trust in artificial intelligence, machine learning, and robotics," *Cutter Business Technology Journal*, vol. 31, no. 2, pp. 47–53, 2018.

[45] X. Yin, J. Han, and S. Y. Philip, "Truth discovery with multiple conflicting information providers on the web," *IEEE Transactions on Knowledge and Data Engineering*, vol. 20, no. 6, pp. 796–808, 2008.

[46] D. Gefen, I. Benbasat, and P. Pavlou, "A research agenda for trust in online environments," *Journal of Management Information Systems*, vol. 24, no. 4, pp. 275–286, 2008.

[47] S. P. Marsh, Formalizing trust as a computational concept. Thesis, 1994.

[48] S. Rouhani and R. Deters, "Data trust frame- work using blockchain technology and adaptive transaction validation," *IEEE Access*, vol. 9, pp. 90379–90391, 2021.

[49] W. Powell, M. Foth, S. Cao, and V. Natanelov, "Garbage in garbage out: The precarious link between IoT and blockchain in food supply chains," *Journal of Industrial Information Integration*, vol. 25, p. 100261, 2022.

[50] A. V. Engelen, P. Malope, J. Keyser, and D. Neven, "Botswana agrifood value chain project: Beef value chain study," Report, Food and Agriculture Organization of the United Nations and Ministry of Agriculture, Botswana, 2012.

[51] T. Prinsloo, Livestock traceability systems in Swaziland and Namibia: Towards an impact-for-sustainable-agriculture framework. Thesis, 2017.

[52] T. Seleka and P. Kebakile, "Export competitiveness of Botswana's beef industry," *The International Trade Journal*, vol. 31, pp. 76–101, 2017.

[53] K. Ontebetse, "Norway dumps BMC beef," Sunday Standard, 03 April 2023. Available at: https://www.sundaystandard.info/norway-dumps-bmc-beef/ (Accessed: June 24th, 2023).

[54] Botswana Government, "User application for Botswana animal identification and traceability system (BAITS)," https://www.gov.bw/animal-husbandry/user-application-botswana-animal-identification-and-traceability-system-baits, 2022.

[55] L. Modisa, "Botswana animal identification traceability system," 14 September 2022, 2013.

[56] J. Byabazaire, G. O'Hare, and D. Delaney, "Data quality and trust: Review of challenges and opportunities for data sharing in IoT," *Electronics*, vol. 9, no. 12, p. 2083, 2020.

[57] N. Karthik and V. Ananthanarayana, "Sensor data modeling for data trustworthiness," in *2017 IEEE Trustcom/BigDataSE/ICESS*, pp. 909–916, IEEE, 2017.

[58] G. C. Karmakar, R. Das, and J. Kamruzzaman, "IoT sensor numerical data trust model using temporal correlation," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2573–2581, 2020.

[59] Z. Zhang, "Computer simulation method for data trust analysis based on average deviation algorithm," *IEEE Access*, vol. 11, pp. 19602–19612, 2023.

[60] K. K. S. Gautam, R. Kumar, and D. N. Gupta, "Challenges, attacks, QoS, and other security issues for an IoT environment," in *AIP Conference Proceedings*, vol. 2555, AIP Publishing, 2022.

[61] A. Alsirhani, M. A. Khan, A. Alomari, S. Maryam, A. Younas, M. Iqbal, M. H. Siqqidi, and A. Ali, "Securing low-power blockchain-enabled IoT devices against energy depletion attack," *ACM Transactions on Internet Technology*, vol. 23, no. 3, pp. 1–17, 2023.

[62] S. K. Sharma and X. Wang, "Live data analytics with collaborative edge and cloud processing in wireless IoT networks," *IEEE Access*, vol. 5, pp. 4621–4635, 2017.

[63] P. K. Wamuyu, "A conceptual framework for implementing a WSN based cattle recovery system in case of cattle rustling in Kenya," *Technologies*, vol. 5, no. 3, p. 54, 2017.

[64] E. Hajnal, L. Kov´acs, and G. Vakulya, "Dairy cattle rumen bolus developments with special regard to the applicable artificial intelligence (AI) methods," *Sensors*, vol. 22, no. 18, p. 6812, 2022.