

Article

Blockchain-Enabled Provenance and Supply Chain Governance for Indigenous Foods and Botanicals: A Design Approach Study

Warwick Powell ^{1,2} , Yasmina Sultanbawa ³ , Madonna Thomson ⁴ , Dharini Sivakumar ³ ,
Mokaddes Ahmed Dipu ^{5,6,*} , Luke Williams ³ , Charles Turner-Morris ² , Gary Sigley ⁷ and Shan He ^{8,9}

- ¹ School of Design, Creative Industries Faculty, Queensland University of Technology, Brisbane, QLD 4000, Australia; wp@smartradenetworks.com
- ² Smart Trade Networks, Brisbane, QLD 4103, Australia; cm@smartradenetworks.com
- ³ Centre for Nutrition and Food Sciences, Queensland Alliance for Agriculture and Food Innovation, The University of Queensland, Brisbane, QLD 4072, Australia; y.sultanbawa@uq.edu.au (Y.S.); d.sivakumar@uq.edu.au (D.S.); luke.williams@uq.edu.au (L.W.)
- ⁴ Bushtukka and Botanicals Indigenous Enterprise Cooperative Limited, Brisbane, QLD 4068, Australia; madonna.thomson@jageradar.com
- ⁵ School of Agriculture and Food Sustainability, The University of Queensland, Brisbane, QLD 4072, Australia
- ⁶ Department of Agricultural Economics and Social Sciences, Faculty of Veterinary Medicine, Chattogram Veterinary and Animal Sciences University, Chattogram 4225, Bangladesh
- ⁷ Faculty of Geographical Sciences, Beijing Normal University, Beijing 100875, China; gary.sigley@bnu.edu.cn
- ⁸ School of Food and Pharmacy, Zhejiang Ocean University, Zhoushan 316022, China; shan.he@cdu.edu.au
- ⁹ Faculty of Science, Technology and Engineering, Charles Darwin University, Casuarina, NT 0810, Australia
- * Correspondence: s.dipu@uq.edu.au



Citation: Powell, W.; Sultanbawa, Y.; Thomson, M.; Sivakumar, D.; Dipu, M.A.; Williams, L.; Turner-Morris, C.; Sigley, G.; He, S. Blockchain-Enabled Provenance and Supply Chain Governance for Indigenous Foods and Botanicals: A Design Approach Study. *Sustainability* **2024**, *16*, 7084. <https://doi.org/10.3390/su16167084>

Academic Editor: Giada La Scalia

Received: 26 June 2024

Revised: 8 August 2024

Accepted: 14 August 2024

Published: 18 August 2024

Correction Statement: This article has been republished with a minor change. The change does not affect the scientific content of the article and further details are available within the backmatter of the website version of this article.

Abstract: Ensuring Indigenous producers realize and capture provenance value from the native foods and botanicals supply chain is a key part of achieving economic, community, and ecological sustainability for Indigenous communities. Utilizing blockchain technology to support validated provenance claims throughout supply chain processes is an important intervention toward achieving this objective. This paper presents the preliminary results of an ongoing project in which blockchain technology underpins a “whole of supply chain” approach to addressing issues of provenance value claims and how these are validated within a digitalized environment. The paper focuses on the overarching objectives of achieving provenance value-based growth, and sustainability within a collaborative governance framework that reflects Indigenous community practice. We discuss how technology design and application developments have been undertaken in the context of a cooperative governance model, with the long-term view of enabling ecosystem participants to share responsibility for system development, operations, and benefits. The paper presents a provenance claims approach anchored in a Resources, Events, and Agents (REA) framework. It showcases the first version of a digital application that was developed by engaging a user community. How the application may be applied to other sectors is also briefly explored.

Keywords: provenance; supply chains; blockchain; indigenous economic development; sustainability; REA supply chain schema; governance; traceability



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

There is a growing interest in food provenance among commercial buyers (viz. procurement managers and wholesalers), regulators, and consumers that is driven by various factors, including the prevention of fraudulent practices, the tracking of quality control to ensure food safety and nutritional value, and the need for transparency and traceability of the complete supply chain [1–4]. Food provenance refers to a specific source or origin of food, where and by whom it was grown, gathered, or raised, how it was produced, and its individual ingredients. It also encompasses claims about how the product is produced, stored, and transported and the marketing claims attached to it [4,5]. While provenance

is often conflated with place, it encompasses a much broader scope, including a spatial (origin), a social (production and distribution), and a cultural dimension (perceived qualities, reputation, and heritage) [3,6]. Provenance is involved with almost every aspect of the food's history; in fact, all food has a provenance [3].

For example, in Australia, the production of traditionally used native foods is gaining market traction due to their superior nutritional and functional attributes [7]. These native plant foods and ingredients often possess unique phytochemical and functional properties, resulting in them being labeled as "superfoods" [7,8]. The distinct composition that can be attributed to many of these underutilized foods not only provides beneficial nutritional aspects but also provides a distinctive chemical signature, which is instrumental in characterizing or defining their provenance that profoundly impacts the entire Indigenous food supply chain [7,8]. Changes in the biochemistry and chemistry of plant or food ingredients can cascade through the entire food supply chain, impacting a range of attributes, including flavor, texture, scent, functionality, bioactivity, nutritional value, shelf-life, and safety [7]. Therefore, detailed provenance information regarding these foods' nutritional, biochemical, chemical, and functional properties is invaluable for all value chain members, ensuring quality, consistency, and safety [7].

Additionally, as these traditionally used native foods and botanicals are based on deeply rooted traditional knowledge of native flora and local traditions, the traditional and cultural practices are also contributing to and defining the unique properties of these foods and, consequently, their provenance [7,9]. Indigenous communities employ specific cultivation techniques honed over thousands of generations, which enhance the nutritional value, flavor, and environmental sustainability of these food products [7]. These practices resonate with modern consumer values, emphasizing ethical production, environmental friendliness, and health and nutrition benefits. Hence, providing transparent and reliable provenance information about cultural and traditional practices reassures consumers that their purchases are part of a legitimate value chain, often rooted in sustainable and ethical practices. This provenance information can alleviate consumer concerns about safety, quality, authenticity, ethics, and sustainability by offering insight into the spatial, social, and cultural dimensions of food provenance [3,4].

The actual utility of provenance emerges when buyers and end-consumers are informed about it and can decide how much this provenance information aligns with their requirements or values [3,10]. For example, suppliers and end consumers may want to know if the quality and safety controls were maintained throughout the food supply chain, the trade was fair, growers were not exploited, workers' well-being was ensured, and environmental sustainability and local food sovereignty were not compromised [4,7]. Adding value can also be associated with the characteristics and attributes that are integral to the food's origin, production process, and cultural significance. These values may include information on grower communities' culture, heritage, history, traditional practices, food's health benefits, etc. Therefore, if such information is available for all the supply chain members and partners, it will help Indigenous producers capture maximum market potential facilitated through effective marketing [7]. As such, information about product and process attributes is central to the provenance value claims made about the products. Given the centrality of information in value claims, information system integrity becomes a focal point of risk and mitigation. This is a key issue underpinning this paper's research focus.

Within this provenance value context, the question of information often has a "taken-for-granted" character. That said, it is increasingly understood that provenance claims are open to a range of validity risks, such as error through omission, error through misrepresentation, and fraud. Failure to meet the social validity tests, what Baggini calls information "triage", renders information claims at best "value-less" and, at worst, "value depleting." As such, provenance information—if valid and credible—adds profound value to the product for consumers, enhancing their confidence in and connection to the foods they purchase [4]. Otherwise, erroneous, incomplete, or misleading information claims can adversely affect the market value of a food product or elements of the supply chain

from which it came. For instance, in the Australian native food and botanical supply chain context, valid information about whether the foods are ethically and sustainably sourced and grown by Indigenous communities who equitably share in the economic benefits is crucial. This information, coupled with food safety and nutritional values, can help buyers make informed purchasing decisions. This transparency and confidence in the validity of the information empowers buyers to have confidence in and endorse the ethical and sustainable practices employed in the native foods and botanicals supply chain, therefore fostering economic and ecological sustainability within Indigenous communities [11]. This expansion encompasses environmental and social welfare, characterized by community reverence for the environment, the grower community, production methods, social well-being, and the protection of Indigenous knowledge and cultural narratives [4]. A thorough comprehension and delineation of provenance can confer economic benefits to custodians and producers of Indigenous or native plant foods as these growing food sectors hold tremendous promise for crafting genuine, delectable, and distinctive foods and ingredients [7].

Although food provenance is significant for both food producers and buyers, establishing the provenance is crucial yet challenging. Validating traceability and credentialing systems is essential to provide clear, credible, and relevant knowledge and information about the history of Indigenous or native foods for all stakeholders and partners in the supply chain [7,12,13]. In this connection, Blockchain technology is a potentially powerful tool for traceability applications that can establish food provenance with credibility and reliability [14,15]. Enhanced credibility and reliability in product claims can also speed up the overall circulation processes, with economic benefits to supply chain participants [16,17].

This study aims to present a provenance claims approach anchored in a Resources, Events, and Agents (REA) framework and the first version of the blockchain-enabled live traceability project—called *ausTukka*—which bridges the technical aspects with social governance considerations, focused on how the technical design and functionalities have been undertaken to enable the implementation of off-chain governance protocols in an Indigenous-led cooperative setting in Australian native foods and botanicals supply chain. The insights produced from this research may facilitate a scalable solution for enhancing provenance value, which is also crucial for global markets focused on sustainability, ethical sourcing, and cultural preservation [18,19]. The successful implementation of the project could serve as a model for other sectors and regions, promoting fair trade practices, supporting Indigenous communities worldwide, and contributing to the United Nations' 2030 Agenda for Sustainable Development [20].

In this paper, followed by materials and methods, Section 1 reviews conceptual issues related to questions of data validation and what blockchains bring to the table. Section 2 reviews the project's design framework, particularly as far as the data schemas and approaches adopted to enable a WebApp to be scoped and developed. Section 3 describes the WebApp (proof of concept—POC V0.1) through a detailed descriptive examination of the App, as well as preliminary user feedback. Section 4 draws together some of the learnings to date, from which future directions are outlined from both a research and App development perspective before concluding the paper.

2. Materials and Methods

From an information system point of view, blockchain technologies, in general terms, provide a number of important functional properties:

- They are a distributed or decentralized ledger with a secure network of information that is relatively immutable [2,5,12,15]. What information is stored on this distributed ledger (i.e., "on-chain") and what information is stored elsewhere (i.e., "off-chain") is an operational decision. Off-chain data can be "linked" to a blockchain by way of a state update "hash", which is, in effect, an immutable digital receipt for a given body of data. Changes to those data would cause a new "hash" to be generated when an

update is made. This mechanism enables proof of data discrepancies between two bodies of data uploaded at various times.

- Data state updates take place via protocols that enforce a set of rules that supply chain actors understand, for which—if they are also involved in the operations of the blockchain network—they are responsible. These rules are known as “consensus protocols”, which denote (a) a method by which a particular node in the network of computers is selected to perform the state update for a specific block and (b) a method by which the network of computers is aligned with the same transactions database [21,22]. There are many potential consensus protocols.
- Blockchains enable applications (input-output functions or smart contracts) deployed on the blockchain to operate consistently for all users, all the time, whereby the applications are not exposed to risks of capricious alterations [23]. This provides confidence to supply chain participants that the system performs consistently and reliably. Changes to applications, such as the deployment of a new smart contract, require that the consensus protocol in question is satisfied. As such, parties to the blockchain are notified of any proposed update and can play a role in enabling the update. The update is traceable.
- The transactions ledger can be queried, enabling the implementation of audits [24]. This goes to all transactions committed to the blockchain, whether it is a data state update or a new smart contract deployment. Auditability contributes to system behavior shaping, as data state updates are signed by unique public-private keys, which cannot be duplicated. The extent to which the ledger and any off-chain data are accessible and can be queried is an operational decision impacted by factors such as legislative provisions. Transparency, in general terms, is seen as an essential system virtue that can assist buyers in developing trust in those who procure, process, and supply food, therefore ensuring the integrity of Indigenous food provenance [5,25].

The interactions between an information ecosystem and a real supply chain are a complex mediation process between actors, information ecosystem properties, and governance parameters (protocols and other “rules”). In this regard, technological tools can have different implications depending on how they are designed to suit particular non-technological ecosystems and requirements. For example, the blockchain framework is governed by a consortium of key supply chain entities that may include the government, regulatory bodies, or other stakeholders [25,26]. This holistic approach benefits the supply chain actors, consumers, and auditors by tracing individual key ingredients, ensuring detailed provenance and traceability of the final product. Blockchain access control is strictly limited to the consortium, preventing any single entity from having absolute control over the blockchain [25,26]. It requires a governance framework that balances autonomy with governmental oversight, using blockchain-based traceability systems to monitor trade activities [25].

In this project, a joint undertaking involves university-based researchers, an Indigenous enterprises network organized via Bushtukka and Botanicals Indigenous Enterprise Cooperative (BBIEC), and experienced supply chain technology solutions partners. By working with a cooperative as the principal community/enterprise organizational form, the project aims to explore ways distributed-ledger technologies can be aligned with membership-based real-world organizational forms. In doing so, we draw on the concept of a supply chain “on the blockchain” as an information association [16], in which cooperative members also fulfill roles within an information ecosystem and seek to explore ways in which membership-based governance can be executed using distributed-ledger-enabled tools. In some respects, this approach enables us to revisit and reflect on a recent trend in blockchain-enabled governance models that revolve around a Distributed Autonomous Organization (DAO) concept.

The research utilizes the “design approach” to analyze the living design and its implementation. This approach employs iterative development, continuous feedback, and adaptation to ensure the design remains responsive to real-world conditions and

stakeholder needs [27]. The focus on living design facilitates the creation of a robust and adaptable system that can effectively address emerging challenges and opportunities within the supply chain. We followed three crucial interconnected cycles proposed by [27] to facilitate practical testing and refinement, ensuring the final implementation is practical, functional, and sustainable.

Relevance Cycle: This cycle ensures that the research is grounded in real-world problems and opportunities. It involves gathering requirements from the application domain and testing the research artifacts in practical settings. This cycle helps ensure that the design is relevant and applicable to real-world scenarios.

Rigor Cycle: This cycle focuses on grounding the research in established theories and methodologies. It draws from the existing knowledge base and contributes new knowledge. This cycle ensures that the research is scientifically sound and builds on prior work.

Design Cycle: This central cycle involves the iterative process of building and evaluating design artifacts. It supports a tighter loop of research activities, allowing for continuous refinement and improvement of the design. This cycle is essential for the practical construction and assessment of the application.

Integration of these three cycles helps us provide a comprehensive approach to studying and developing applications. It ensures that the design is both practically relevant and scientifically rigorous, making it highly effective for creating living designs that evolve and adapt over time.

In this study, our initial hypothesis is that blockchain-based traceability tools, such as our developed web application, will assist Indigenous producers in improving the provenance value of their products. While the project is in its initial stages, and we have yet to obtain user and market feedback to evaluate its effectiveness, we believe the tool will enable Indigenous producers to differentiate their product values and secure better prices. However, it remains uncertain whether this tool will enable producers to capture a larger share of the overall value within the supply chain.

3. Results and Discussion

3.1. Issues of Data Validation and Blockchains

Data validity refers to the operating protocols of an entire information ecosystem and how these protocols satisfy the requirements of social and economic actors. Valid does not ipso facto equate with Truth, with a capital T, but notions of social truths are essential to understanding validity within specific contexts. Social truths can be understood as a set of explicit and non-explicit processes and “rules” applied in specific contexts for an information claim to be valid by the social actors involved. What is valid in one context may not be valid in another. One of the most common social truth types is what Baggini [28] has called “authority truth”. Authority truth is a valid information claim that is premised on the idea that the claim is made by an actor that is considered to have the status and capability to make such claims and that in making such claims, the appropriate or applicable method has been adopted to substantiate or enable such claims to be made. For claims of authority truth to be validated, social actors process such claims by way of a triage process, which involves attending to four questions:

- (1) Is the claimant suitably qualified? The claimant could be a non-human actor, such as a sensor device.
- (2) Is the claim being made about a body of knowledge that people can know something about?
- (3) Is the proposed information part of the claim about such a body of knowledge?
- (4) Is the method by which the claim is made relevant or applicable by which people can know something about the subject matter?

Throughout a supply chain process, there are many events and activities about which various actors are making information claims. For example, claims will be made about harvesting a particular fruit: what is harvested, when, and by whom? How is it harvested? How much is harvested? Answers to these questions are something about which a body of knowledge can be created (triage question 3). So, the issue is who is making the claim,

whether they are qualified to make it (1 and 2), and whether the method that backs up the claim is right (4).

A suitably designed information system must first and foremost address the question of the processes and protocols that govern the collection of data and the validation of data itself. Once collected and validated, data are sent as a message to be stored in an information system. Therefore, a suitably designed information system must address questions of the security of the sending mechanisms (can the information be intercepted and altered “mid-journey”, for example?) and the adequacy of the storage methodology. Is data to be stored in a single location? Is it to be stored in multiple locations? Who is responsible for the storage of the data? If it is stored in multiple locations, how can users be certain that data from one location is the same as data stored at all the other locations? Once stored, how secure is the data? Stored data are then available for consumption or use in other data-producing processes. Who can access what data under what conditions? Who determines these protocols, and how are they executed?

Blockchain information systems open up numerous ways of addressing the issues raised when the overall data ecology is broken down into parts. At root, blockchain systems provide a distributed ledger that directly addresses the question of data storage; data are stored on a network of devices, and the consistency of the data across a network of devices is maintained by way of some form of consensus protocol. However, the other issues are less straightforward and need to be addressed, so to speak, on their merits, i.e., consideration needs to be given to the applicable operating environment—the use case—for which the data ecology is being designed and built.

3.2. Design Framework and Approach

The ausTukka project has worked on a blockchain-enabled data ecology that provides specific responses to the overarching challenges of information system design in the context of native food and botanical supply chains, in which a cooperative is the analog-cum-legal governance framework. The design responses to the specific issues within a data ecology have considered the questions across the core functions of such a data ecology and how these questions could be addressed at each key activity node within a supply chain.

The specific approaches adopted in the project are summarized in Table 1. The table shows four key supply chain activity nodes (producer, transporter, processor, and distributor) and five data ecology functions (collection, validation, storage, access, and dissemination).

The data collection framework for the supply chain as a whole has been developed in line with the broad framework of an REA (Resources, Events, and Agents) data schema. In this schema, all supply chains are a series of events linked to each other. Each event involves actions undertaken by agents concerning a resource or set of resources. Resources are material and immaterial inputs required for the event to take place. There are many kinds of events in supply chains, from production to assembly and disassembly, consumption, relocation (picking up and dropping off), transfer of rights, exchange, etc. Agents can be individuals, organizations, or non-human actors. Non-human actors include machines, such as data collection and transmission devices (e.g., sensors, GPS trackers, etc.). For the supply in question, a modified or truncated REA schema was adopted to aid in designing the data collection protocols.

The App provides for three main event types: (i) produce (when a new resource is registered to the database); (ii) consignment (pickup and drop-off); (iii) resources update—enabling additional events to be added to an existing resource. A resources update is a highly generic event type, which could, in the POC, function as a proxy for all sorts of events such as processing (a generic event type to include value-added manufacturing, packaging, etc.), storage, etc. A standardized data collection form was developed in the WebApp for each event type. Data are attributed to the forms, and file uploads can be added to the consignment. The assembled data are then signed and pushed as a data state update. The signing is executed through the public-private key, which links the public key information (the wallet’s public address) with the update.

Table 1. Specific approaches adopted in the project.

| Function/ Nodes | Producer | Transporter (Consignment) | Update |
|--------------------|--|--|--|
| Collection | Data are collected by way of a Web App. The WebApp runs on a standard server array (e.g., AWS). | Data are collected by way of a Web App. The WebApp runs on a standard server array (e.g., AWS). | Data are collected by way of a Web App. The WebApp runs on a standard server array (e.g., AWS). |
| | Users create accounts, which enables the creation of a personal Web3 wallet—that is, a public-private key—which is used to sign data messages (updates). | Users create accounts, which enables the creation of a personal Web3 wallet—that is, a public-private key—which is used to sign data messages (updates). | Users create accounts, which enables the creation of a personal Web3 wallet—that is, a public-private key—which is used to sign data messages (updates). |
| | A standardized supply chain data schema (Resources, Events, Agents—REA) is the basis of the data structure (discussed below). | A standardized supply chain data schema (Resources, Events, Agents—REA) is the basis of the data structure (discussed below). | A standardized supply chain data schema (Resources, Events, Agents—REA) is the basis of the data structure (discussed below). |
| Validation | For this phase of development and trial, authorized signers validate data. | | |
| | Authorized access to the blockchain is governed by an “authority token” issued by the ecosystem administrator and data update credits (digital tokens). | | |
| Storage | Data are stored on-chain. The blockchain network is a Proof of Authority (POA) protocol EVM-compatible system. | | |
| Access | Anyone can access the Blockchain Explorer. Transaction numbers enable querying the explorer to validate signers and time stamping. | | |
| Dissemination | Data updates can be notified to a specified array of recipients via email. | | |

Data updates are made through the WebApp as well. Data updates are valid only when the “right” agents sign them. Data are validated in two ways: First, the signer’s signature must have access to the App. This is governed via off-chain governance mechanisms in terms of access permissions and the provision of non-transferable authority tokens to the specified wallet address. Without approval to access the App and a valid authority token, the data state update would be invalid and fail. Second, once pushed, the blockchain consensus mechanism incorporates the state update within the next available block when a sealer node accepts the state update, seals a block, and then propagates the update and transaction details to all nodes.

It is to be noted that validity does not imply truthfulness. This is an important distinction. Validity is simply compliance with a set of protocols. The design architecture of the validity mechanism enables a socially acceptable governance protocol to be applied through a confirmed identity and provision of authority to access the App. In this architecture, it is possible to subsequently assign specific user types with a range of information state update-related rights so that only certain user types can sign certain updates. This feature is part of a more detailed and ongoing consideration of how the technology can be integrated into non-technical governance protocols as determined within (a) a cooperative governance model and (b) a community-cultural authority environment.

At this stage of project development, data validity is designed to enable an ecosystem administrator to fulfill the function of authorizing App access. The ecosystem administrator is currently the App development team; however, the design intent is to enable the cooperative to fulfill this function once the App leaves the development sandbox environment. Authorized users create their own accounts, and access to the blockchain is enabled through a Web3 wallet. A Web3 Wallet is an essential management tool that allows the user to govern access to particular blockchain networks and control the execution of transactions (by “signing” the transaction with their public-private key). The Web3 wallet is compatible with the WebApp is MetaMask, a “universal” wallet that anyone can download and install at no cost.

The design intent is to enable the governance of permissions at each supply chain activity node for a specific array of signatories to submit and sign data updates. For example, claims about cultural provenance are valid if made by a certain range of signers and not others, including people with the accepted cultural status and knowledge to substantiate the claim. The App also has an identity verification process built in to enable this design intent, but it has yet to be activated. Questions of identity verification are part of the ongoing field research and testing process, so while the function is available, how it is to be activated remains an open question.

A single signer is required to push data state updates. A multiple-signatory smart contract (multisig) has been developed that enables the requirement of multiple signatories for an update to be pushed [16,26]. The multisig has not yet been embedded into the overall workflow of the App, as further field research and user community feedback will be needed to determine the context of the application and the operating parameters.

When a data state update is pushed to the database, the data are stored on the blockchain. The blockchain that is used for this project is the Smart Trade Networks (STN) blockchain. The STN blockchain is an Ethereum Virtual Machine (EVM) compatible blockchain operating a Proof of Authority consensus protocol. The blockchain is a private blockchain with three node layers. These are:

- Authority Node—the Node from which subordinated functional authorities are assigned.
- Sealer Nodes—these are nodes that have the authority to publish new blocks and, therefore, publish data state updates
- Archive Nodes are nodes that maintain a copy of the database but do not have the authority to publish data state updates.

The blockchain protocol design enables the management of the locations of nodes and the identity of the organizations or individuals that operate the nodes. This design enables the blockchain network to address operating requirements related to the location of nodes (e.g., data sovereignty requirement, which mandates the location of data storage infrastructure) and the identities of those operating the nodes. Unlike public permissionless blockchain networks (e.g., Bitcoin and Ethereum), the POA network design enables the identity of node operators to be known. The network protocol supports future network “forking” so that a specific node location and identity configuration can be established for a specific user community. In the context of the ausTukka project, one possible outcome is that a dedicated fork would be created so that the cooperative could assume overarching authority for the operations of sealer and archive nodes (including enabling members to fulfill those roles).

In terms of data storage, there are two types of data: on-chain and off-chain. For now, we can note that on-chain data storage means that the relevant state update data are immutable and stored across a network of computer nodes (archive nodes), the synchrony among which is maintained through the consensus mechanism. The nodes can be any device running an appropriate version of Ubuntu OS (an open-source operating system) with an Ethereum Virtual Machine deployed. Archive nodes can be located inside commercial data centers or operated on desktop computers and devices like Raspberry Pi (4). These data are also viewable when the blockchain is queried. In this environment, confidentiality and privacy issues are critical design (and legal) considerations. The design approach has

opted for a relatively data-lite approach to on-chain data at this stage, with little detailed transactional data—such as data concerning product properties—being stored immutably on-chain. This can be amended in future renditions, subject to user feedback. In this context, the blockchain is principally utilized as a generator of timestamped unique hashes for each data state update.

On-chain data also has one other aspect—when a final certified product is created, a unique non-fungible token is also created on-chain. This is a unique digital certificate or artifact of provenance that can be traced through the associated antecedent data state update transactions. At this stage, the principal function of this non-fungible token is to enable auditability of data state update provenance so that signers can be identified and confirmed, and temporality and temporal sequencing can be proven. Future applications of the non-fungible token could include but are not limited to the digitalization of transactions whereby the non-fungible token product is the counterpart of a digitalized transaction. The non-fungible token could also be embedded in property relations as a digital proof of ownership, as the token cannot be replicated.

Off-chain data are registered and “tagged” with a hash returned from the blockchain when the update is pushed. In practical terms, this means that should data be modified in the off-chain environment, it would be pushed as a data state update, therefore generating a new unique hash turn (and timestamp). This mechanism enables data changes to be identified and audited and proofs of temporal sequencing to be made if necessary.

Data access is available through links to transactions and event updates from within the App. All data in the present POC implementation is stored directly on-chain.

3.3. The App as Implemented in This Current Phase

The WebApp is accessible from a desktop. It has not yet been calibrated for a mobile environment. Internet access is needed to utilize the App. This section provides a detailed review of the App through commentary associated with screenshots of the App. Appendix A provides a detailed and comprehensive App Flow and Interaction Diagram.

The first interface that a user will experience is a login/new account creation panel (Figure 1). It can be seen that a user needs to log in using a MetaMask wallet.

Once logged in, the user will be presented with the following view, showing who the current product “manufacturers” are within the App (Figure 2). A manufacturer is an agent within the REA data schema. The concept of “manufacturer” is generic; it can be applied to both producers of raw materials, e.g., farmers, harvesters, etc., or value-added factories. (A future version of the App will likely introduce a more granular nomenclature concerning role descriptions.) As a first-time user, the user would see no manufacturers, but they become visible as they are registered into the system.

New manufacturers of products can be registered with the App and the blockchain. This is completed via functions accessed from the dropdown tab in the top left-hand corner of the App (Figure 3).

A new manufacturer can be added by completing the form and the function (Figure 4).

Similarly, a new product can be added by completing the add product form (Figure 5). As can be seen, the details are deliberately generic at this stage. This is part of the design methodology approach adopted for this project, which sees iterative processes of App refinement through rounds of user engagement.

Once a product has been added to the system, the user can begin registering actual resources within the product category (Figure 6). The example shown is for a product known as Kakadu Plum. It is important to note that creating a new product is not the registration of specific resources. Creating a product is a categorization activity in which real-world events and resources are registered.

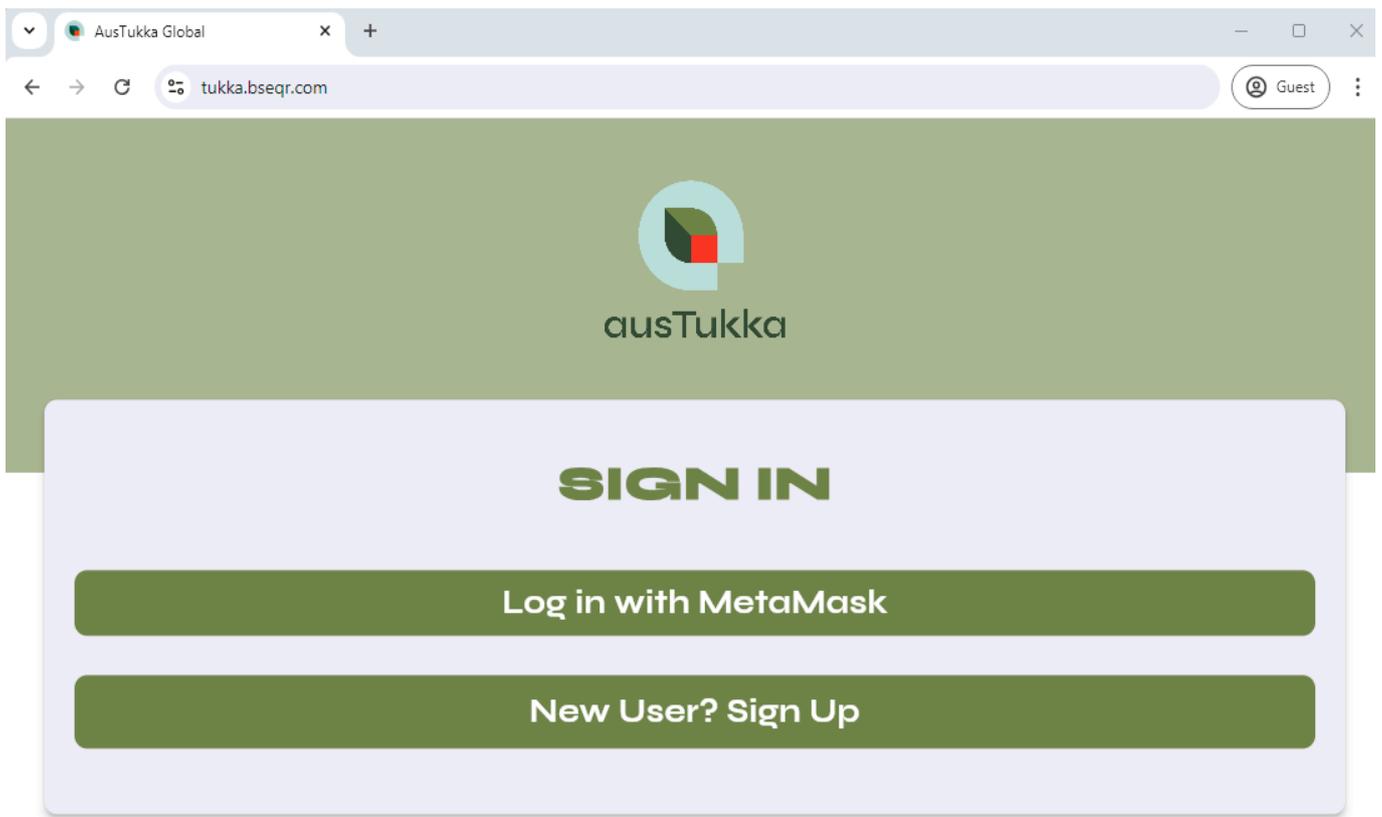


Figure 1. First interface.



Figure 2. Current manufacturer interface.

Adding resources requires the user to complete a detailed form (Figure 7). The user completing the form will need to sign the form. There are two steps to registering a new resource:

- (1) A user completes the add resources form and hits the *issue button*. They fulfill the role of *new resources submitter*. This then enables the user to request approval from another party (Figure 8). The request is emailed with a link to a pending new resource requesting approval.

- (2) The approving party receives the email, follows the link, and reviews the new resource details. Should the approving party be satisfied with the details, they can approve the new resource. The approving party simultaneously performs two functions: *evaluate* and *approve*.



Figure 3. Dropdown tab under current manufacturer.

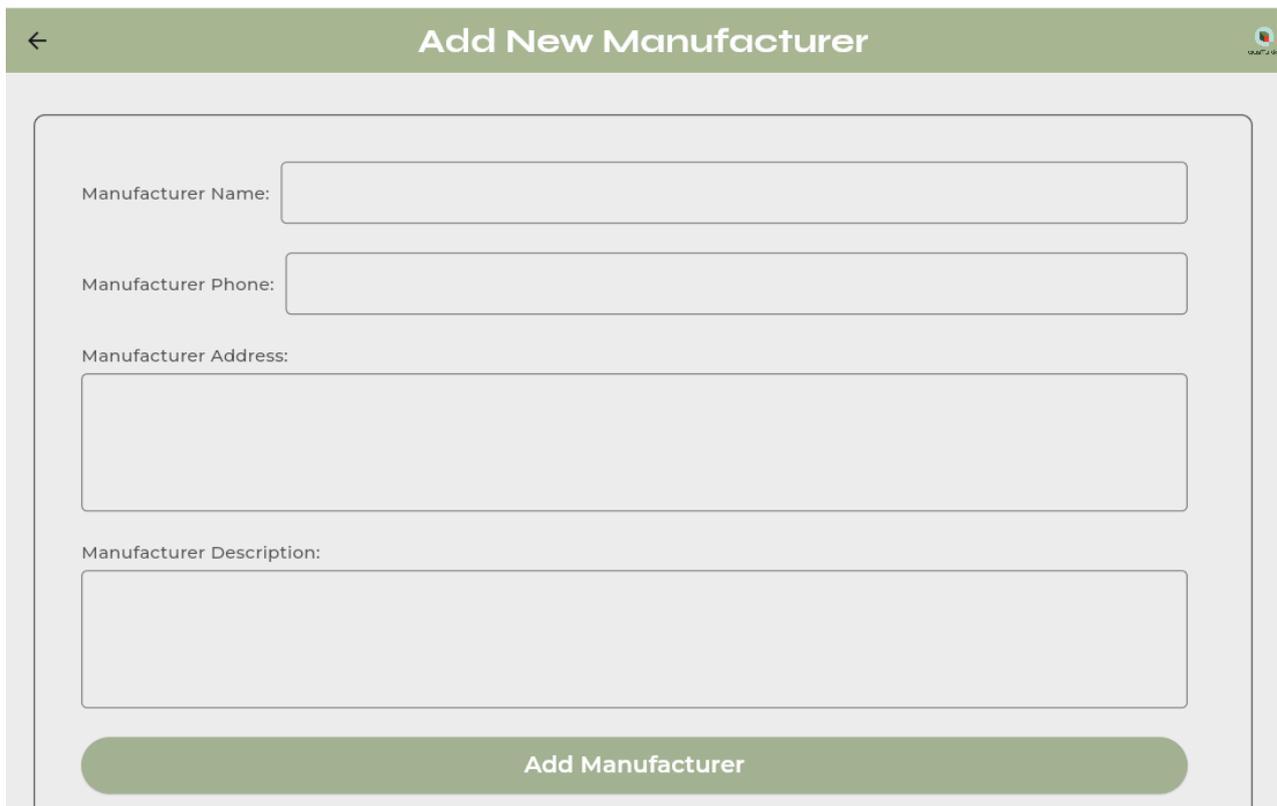


Figure 4. Adding new manufacturer.



Figure 5. Adding new product.

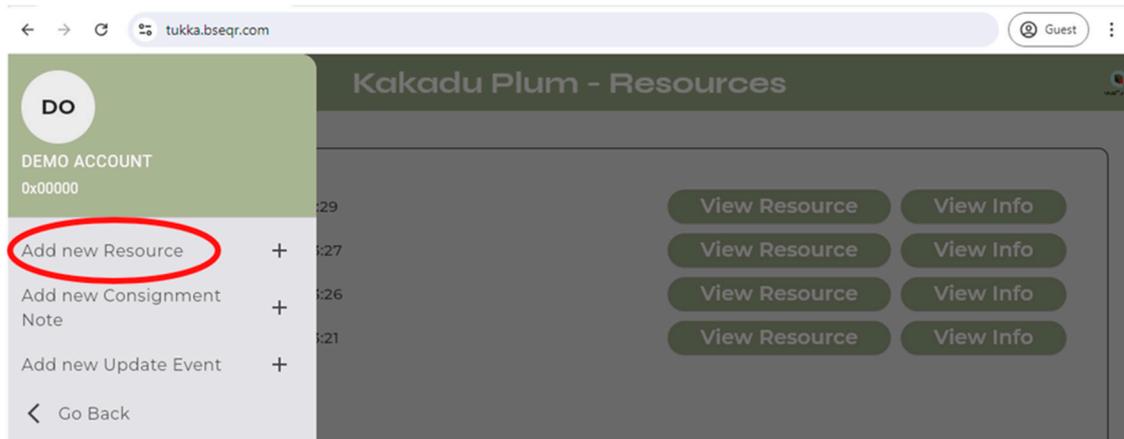


Figure 6. Adding new resources.

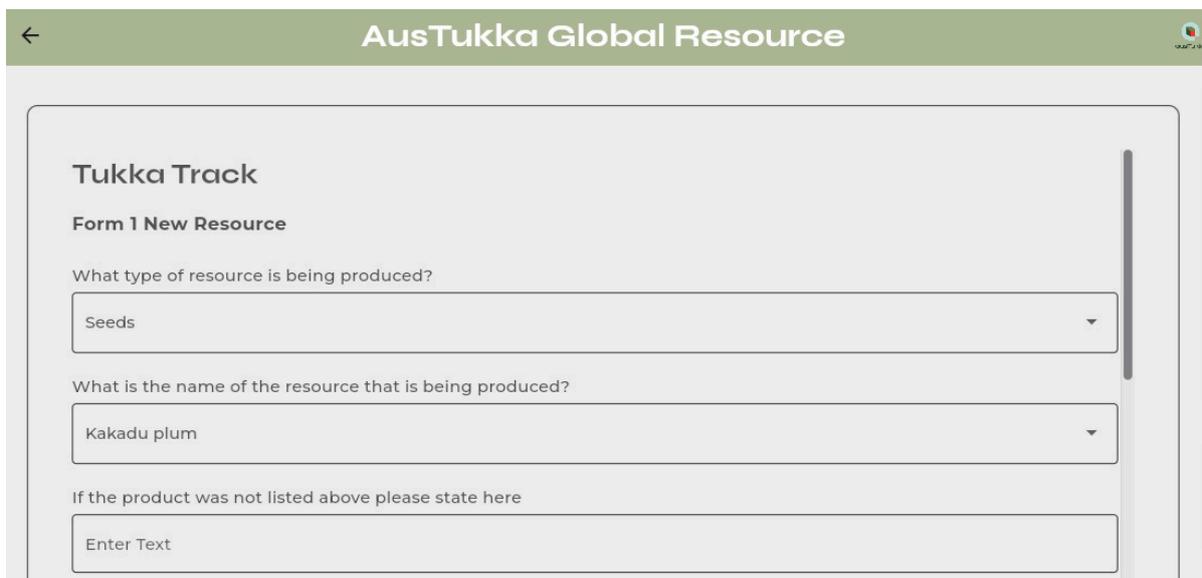
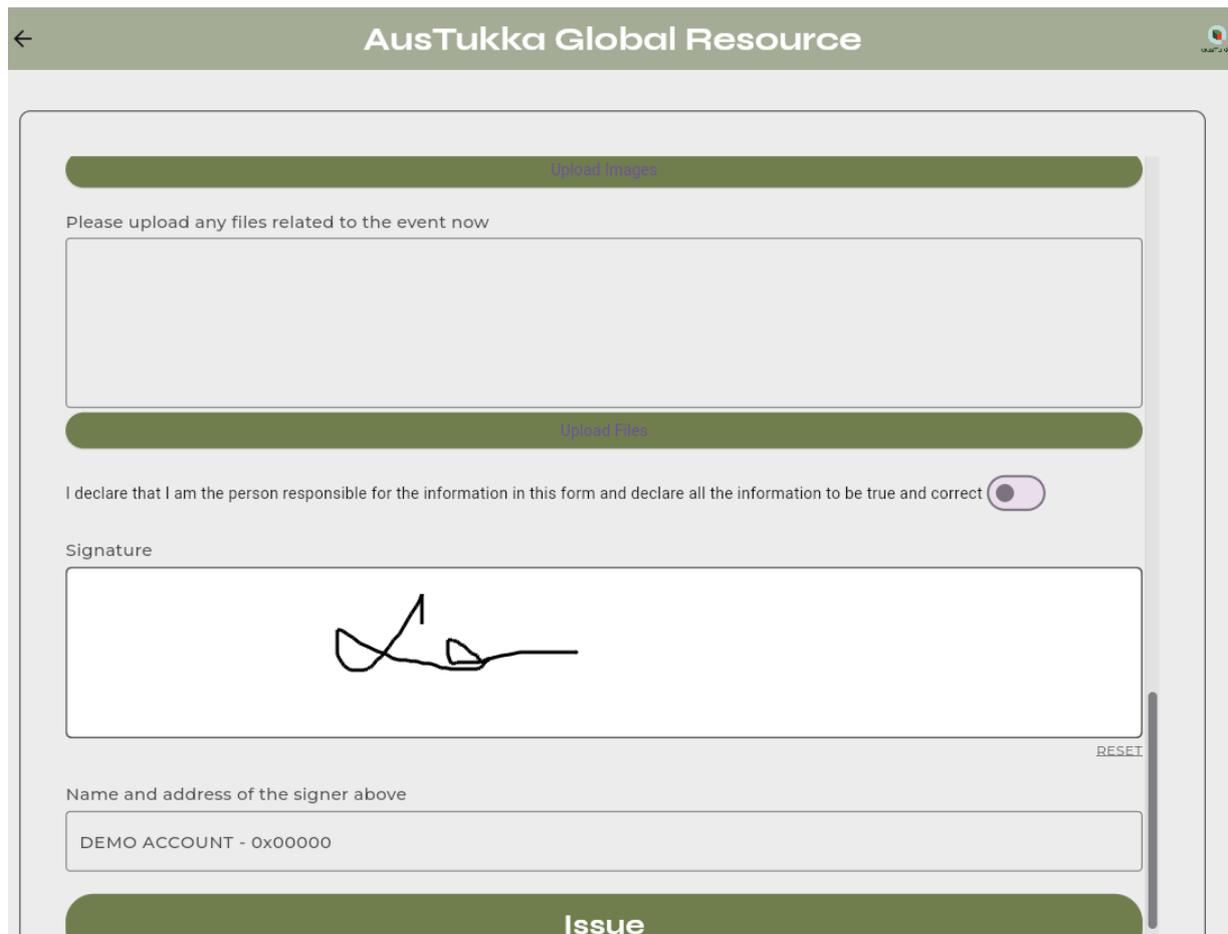


Figure 7. Resource form.



The screenshot displays the 'AusTukka Global Resource' app interface. At the top, there is a green header with a back arrow on the left and the app name 'AusTukka Global Resource' in the center. Below the header, there is a section titled 'Upload Images' with a green bar and a text prompt: 'Please upload any files related to the event now'. This is followed by a large empty rectangular box. Below that is another green bar titled 'Upload Files'. Underneath is a declaration statement: 'I declare that I am the person responsible for the information in this form and declare all the information to be true and correct' with a toggle switch that is currently turned off. The next section is labeled 'Signature' and contains a large white box with a black handwritten signature. To the right of this box is a 'RESET' link. Below the signature box is a text input field labeled 'Name and address of the signer above' containing the text 'DEMO ACCOUNT - 0x00000'. At the bottom of the form is a green bar with the word 'Issue' in white text.

Figure 8. Resource ready for request approval.

At this stage in version 1, there are no permissions structures in terms of which App users can fulfill either of these roles, and they can perform all available functions. After receiving the user feedback, the permission structure of the ausTukka app (POC Version 0.1) will be expanded to improve security and governance. This system will consider both security requirements and culturally driven authorities, ensuring that different users, such as elders and traditional owners, have appropriate levels of access and control. This will necessitate the development of a culturally aligned authorization governance framework, enhancing the app's functionality while respecting and integrating Indigenous cultural hierarchies and protocols. By incorporating these elements, we aim to ensure the app is secure, culturally sensitive, and effectively governed.

When the new resource registration process is completed, the user is returned to the resources view page (Figure 9). From there, users can view the data details. The issuance of a resource registration is a data state update on the blockchain. The resource, as described through the form, is now a unique digital transaction tracked on the blockchain. This unique digital transaction is identified with a unique transaction hash and block number details, together with a timestamp and the public key of the signing App user. These four elements form an integrated data integrity anchor, being tracked on a distributed ledger. Unless the majority of sealer nodes agree to alter the record, the registered resources and the associated data are immutable for all practical intents and purposes.

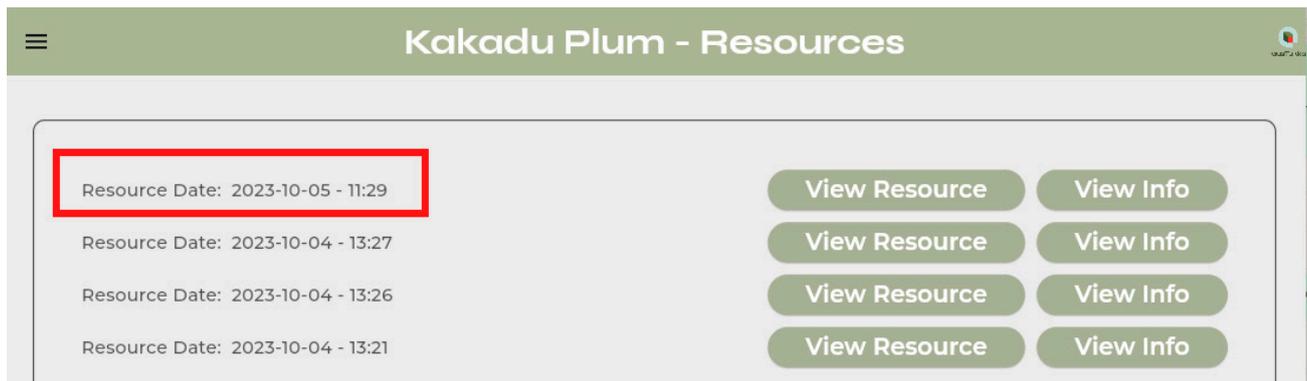


Figure 9. Resources view page.

At this stage, resource details can be viewed. However, note that the resource update has not yet been “approved” (Figure 10).



Figure 10. Not approved resource.

Approval is pending, and a request to an Approver is sent via email. This is completed by navigating to the Request Approval tab (Figure 11) in the navigation bar (left-hand side of the App).

From there, a selection is made of which resource approval is sought. The user then completes the approver’s email address details and submits via Request Approval (Figure 12).

An email is automatically generated by the App and sent to the identified recipient. The recipient is invited to follow the link to review the requested resource’s details (Figure 13).



Figure 11. Navigation to request approval page.



Figure 12. Request approval page.

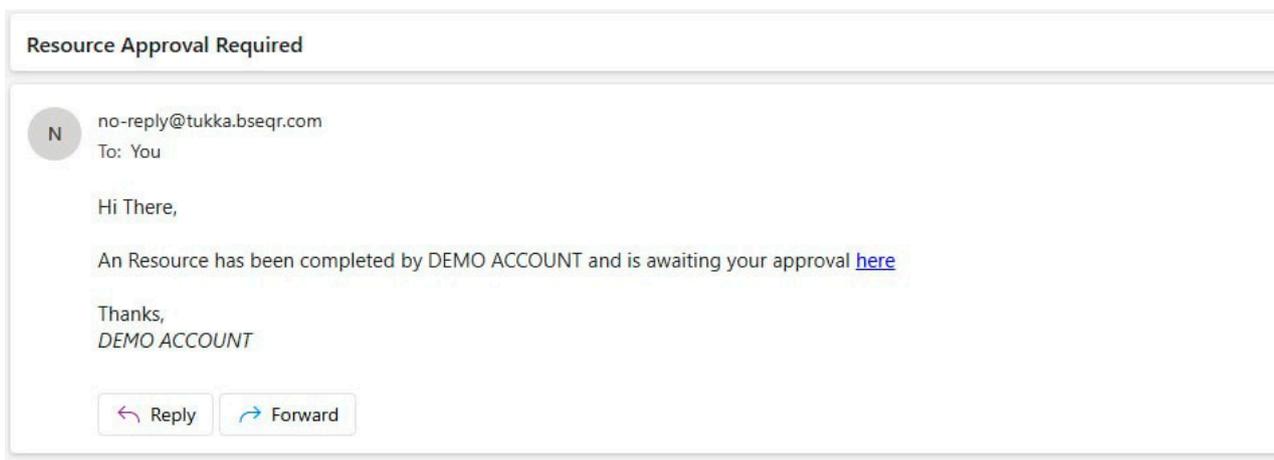


Figure 13. System-generated email for request approval.

Following the link, the approver will then have a view of pending requests. They are then able to view the resource and related information. If they are satisfied with the request, they proceed by clicking Get Certificate (Figure 14).

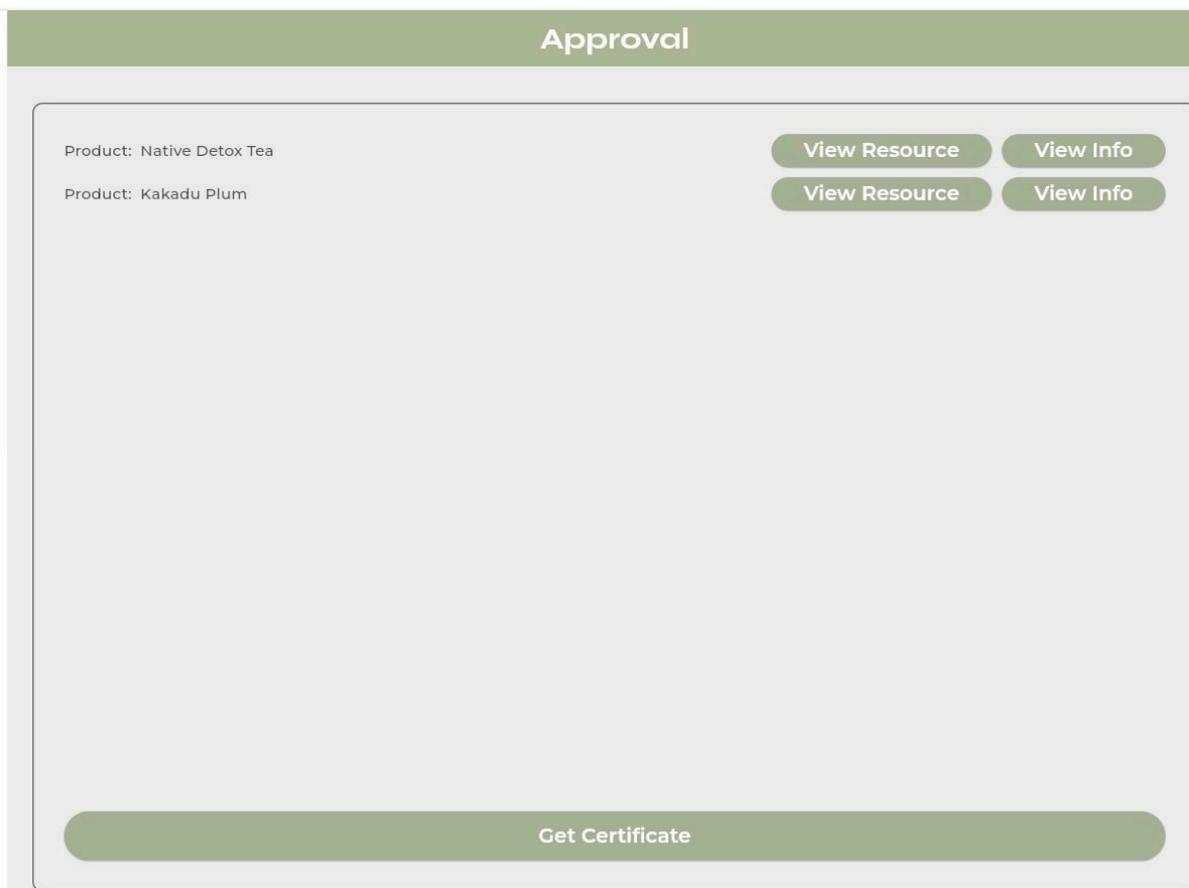


Figure 14. Get the certificate page.

An Approve and Generate Certificate screen is then presented. A certificate for the resource in question can then be generated (Figure 15).



Figure 15. Certificate generation.

Approval of a resource registration is also a data state update on the blockchain. In the present version of the App, a PDF certificate is also generated at this stage (Figure 16). The resource, as described through the form, is now a unique digital transaction tracked on the blockchain and the data are also presented in the PDF certificate. This unique digital transaction is identified with a unique transaction hash and block number details, together with a timestamp and the public key of the signing App user. These four elements form an integrated data integrity anchor, being tracked on a distributed ledger. Unless most of the nodes agree to alter the record, the registered resources and the associated data are immutable for all practical intents and purposes. The PDF certificate has a QR Code that

can be scanned. The QR Code takes the viewer to the STNScan blockchain explorer, where details of the state update transaction can be viewed.

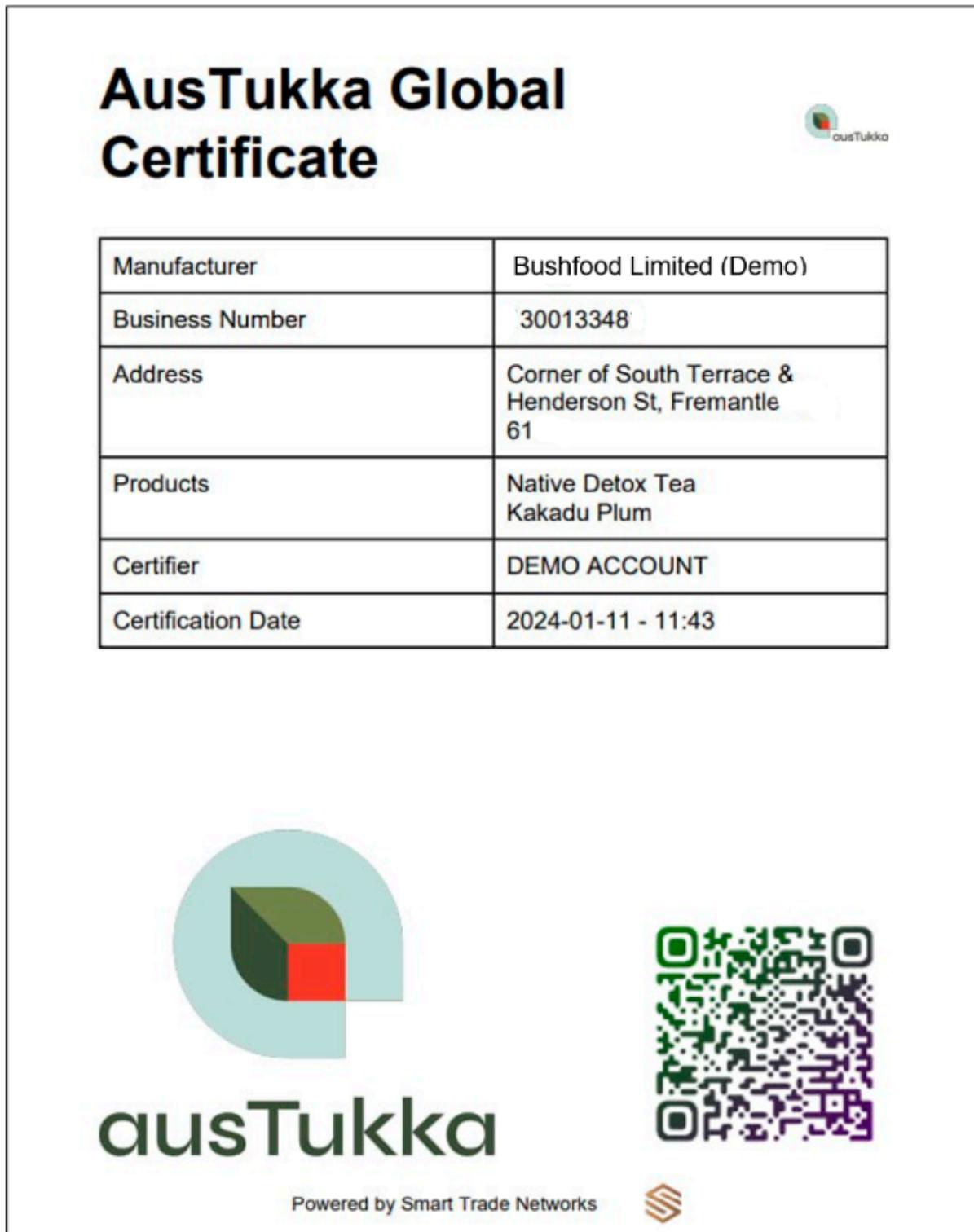


Figure 16. PDF certificate sample.

The PDF can be downloaded for sharing.

Having described the functional interfaces of the POC App, we can summarize its key features as follows:

- (1) User accounts can be created and are governed by public-private key security architecture. A Web3 wallet is used to manage keys and tokens. There are two tokens:
 - (a) The administrator issues an authority token to the account. The authority token is a unique (non-fungible) digital token. The token is non-transferable. It can be time-limited, with parameters set by the administrator. An authority token is necessary to access data state update functions. This feature has been designed to align with the cooperative's governance requirements, which may, in the future, wish to govern and manage the App user community.
 - (b) Transaction credits. Transaction credits are fungible tokens, enabling users to "pay" for data state updates. The EVM requires transaction fees to be "paid". This feature will support the cost-recovery requirements of the App in the future, as users will need to have a supply of transaction credits to utilize the App.
- (2) A standardized workflow and data schema have been designed for the App. These features are:
 - (a) The ability to add new agents (in this case, manufacturers).
 - (b) A data schema hierarchy is one in which there are product categories, and for each product category, there are specific resource data fields. App users can add products to the App and then add resources under the products category.
 - (c) New resources can be registered via a two-step process of submission and approval. Upon approval, a certificate can be generated as a PDF with links to the blockchain for audit and validation purposes.
 - (d) New updates can also be created for each existing resource. These updates are undertaken through the same workflow: new information > submit and request approval > review and approve.

As can be seen, the focus has been to address the core functionality requirements enabling the registration and certification of products and specific resources. Such specific resources could be different product forms, e.g., seeds, seedlings, harvested crops, etc. The data update workflows also provide the mechanisms by which authorized signatories can be specified, enabling a prescribed range of users to approve certain kinds of updates. This has been conceptualized and designed from a generic or abstract technical point of view so that a core set of patterns can be deployed to support specific real-world requirements. These real-world requirements and issues for the subsequent phases of the App development project are the subject of the concluding section.

3.4. Future Directions and Possible Applications to Other Contexts

The POC development process has been part of a design-led approach to technology applications development, which seeks to iterate improvements and refinements based on user community engagement and feedback. To gather user feedback for the ausTukka app, we will engage three user groups: Indigenous user groups (growers, processors, traders), researchers, and technical users. Participants will be guided through a structured process, starting with registration on the app as manufacturers, followed by registering two products within the system. They will then add all three event types to each product, ensuring comprehensive interaction with the app's features. After this, participants will complete a feedback form via email, addressing questions about the app's functionality, essential features, and additional desirable features. Additionally, we will collect feedback through personal interviews. The gathered feedback and insights will be instrumental in enhancing user engagement, app usability, and overall functionality, ensuring the app meets the needs and expectations of its diverse user base.

This approach is more aligned with what software developers would describe as an "agile" approach, as opposed to a "waterfall" methodology [29]. An agile approach is underpinned by a belief that user-driven iterations through real application testing enable responsive technology development. An agile approach is more practical in an

environment where there are many so-called “unknown unknowns”. A detailed plan-driven approach with few iterations and long development test cycles is implemented where the operating environment is more mature and well-understood. The project team has received preliminary user feedback, though further rounds of user testing are being undertaken. The initial feedback has identified the need to address the following issues:

- (1) Account identity verifications. From a verification point of view, a KYC process has been developed to enable a user’s identity verification documents to be matched against approved databases. Such documents include driver’s licenses, for example. However, while technically feasible, the question of identity is a complex and challenging one in the context of remote Indigenous communities.
- (2) Account user authority status. In addition to questions of identity narrowly defined, issues of user status from a supply chain authority point of view require further consideration. Given our understanding of “authority truth”, the project team will need to further consider the kinds of authorities needed for the approval of different information claims. A key element of this goes to cultural knowledge authority, how that is conferred on specific user accounts, and how such authorities are governed. Here, technical tools must align with cultural practices and the cooperative structure requirements of this “information association” inspired project concept. Other forms of authority will also need to be considered, particularly when claims are being made about:
 - (a) Locations (should the App activate GPS tracking, and how should locational confidentiality be preserved?);
 - (b) The compliance of the products in question in relation to programs such as organic certifications;
 - (c) The nutrition or other scientifically validated properties of products (should a whitelist of approved laboratories or scientists be created? And how should this process be governed into the future?)
 - (d) The conditions of the products and the role of IOT devices and sensors in capturing and providing relevant data. Such data could include storage temperatures, humidity, duration of storage, etc., all of which could impact product quality;
- (3) Notifications. At present, data state updates are visible within the App. Still, there is a need to consider how data state updates are notified to relevant stakeholders and who those stakeholders are. Information asymmetry and asynchrony are two of the most significant transaction cost factors in supply chains [30]. As such, a notifications management process requires further research to address questions like—Who needs to be notified? Who is responsible for ensuring they are notified? How are they to be notified?
- (4) Consignments management. The App so far enables the registration of specific resources. The practical challenge is enabling these digital resources to be activated as part of transaction consignments. In doing so, issues to be addressed include:
 - (a) Who has the authority to create consignments into which specific digital assets (as representations of real-world resources) can be placed?
 - (b) How is the consignment management function aligned with both commercial transaction requirements and workflows (e.g., logistic management and trade documentation, such as bills of lading, insurance certificates, and other required declarations) and finance flows?
 - (c) Can consignments be created and made available in digitized market formats, enabling buyers and sellers to interact with each other?

These issues, mundane in appearance, also raise important questions about how provenance value drives transformations in supply chain structures and value distribution. Provenance value differentials, demonstrated by a range of relevant and available data, could lead to a more granular differentiation of products to which different market values

could be ascribed. What is the role of provenance value standards (or lack thereof) in enabling such markets to be created? How can such standards drive the data schemas that ultimately “sit behind” data state updates for supply chain events? Nutritional properties demonstrated via validated scientific analysis could be a significant driver of value differential and other provenance information associated with cultural knowledge, location, and times of harvest and production. In an era in which foods are increasingly commoditized, critical points of difference validated through blockchain-enabled data governance protocols may open up opportunities for new value or new channels for premium quality native food and botanical products.

The digitalization of products can also impact the business models that predominate in supply chains. Can the disintermediation of supply chains enable a more direct relationship between producers and buyers and create a cost-effective, risk-mitigated relationship? Can virtual scale economies be achieved through digitized aggregation without necessarily requiring any change in the ownership structure of the supply chain enterprises? That is, rather than seeking scale economies (including reducing information asymmetry and asynchrony via consolidated ownership), how can blockchain-enabled technological innovations support the same performance outcomes while leaving a distributed network of micro, small, and medium-sized enterprises in place?

The approach adopted here can be applied in many other contexts. One particular context worth considering is that of tea provenance, specifically teas in China that are produced using sustainable practices developed over millennia by local peoples with a strong cultural attachment to the place. In Yunnan province in southwest China, local peoples of various ethnic heritage—including Bulang, Dai, Hani, and Lahu peoples—have been cultivating the large leaf variety of tea—*Camelia sinensis assamica*—using a system of agroforestry for thousands of years. Unlike typical tea plantations that are monoculture and grown as hedges in terraced formations, this tea is grown arboreally as trees in a biodiverse forest canopy (hence “agroforest”). The trees are long-lived, and ages between 200 and 400 years are common. The tea cultivation process is a well-integrated part of local cultures, and the trees are revered in animistic-style rituals. One region—Jingmaishan—was recently inscribed as UNESCO [31] World Heritage in the cultural landscape category. The puer (pu-erh) tea produced is highly sought after in markets across East and Southeast Asia, and there is growing interest among tea connoisseurs worldwide. The highest quality puer teas can fetch prices above USD 10,000/kg.

The therapeutic benefits of tea drinking have also been well demonstrated [32]. Puer tea cultivators and merchants make health claims about their products based on certain teas’ chemical and microorganism properties—especially of the aged variety—that cannot be readily verified. Tea buyers are also keen to confirm that the tea has been sustainably cultivated, yet soaring prices encourage over-harvesting, which harms tea tree health. The potential effects of climate change on how tea cultivation is managed to develop resilience and preserve ancient tea trees is also a growing area of buyer concern [33,34].

The brief overview shows many parallels with the issues confronting Indigenous foods described in this article. Yet given such factors as demand, prices, health benefits, sustainability, and so on, it is not surprising that the puer tea market is also flooded with fake products. Given that China is rapidly applying blockchain technology in food and health systems [35], the tea market is an ideal environment for further application of the authentication system proposed here. Interestingly, therefore, many of the questions are not technological issues, strictly speaking.

4. Conclusions

Our work on the ausTukka project has shown how important it is to recognize that technologies are tools that become meaningful when embedded into and mediated through real-world (analog) processes and practices. The efficacy of technological innovation is amplified when there is a sensibility to the contexts in which they are situated and deployed. While the application of technological tools addresses and enhances supply chain performance by validating provenance value claims, it also raises critical issues within supply chain actors' relationships and the design and operations of the associated information ecosystem. Data validity and the systems that enable credible validity claims can no longer be treated as a foreign or exogenous component of real-world product supply chains. Rather, information ecosystems need to be designed to be endogenous to the institutions and practices of supply chains, recognized as an inimical component of supply chain value and function. Analog provenance and data provenance systems are inseparable, symbiotic twins.

Author Contributions: Conceptualization, W.P. and G.S.; methodology, W.P.; software, C.T.-M.; validation, Y.S., M.T. and D.S.; formal analysis, W.P.; resources, W.P. and C.T.-M.; writing—original draft preparation, W.P.; writing—review and editing, M.A.D., L.W., S.H., Y.S., M.T. and G.S; project administration, M.A.D.; funding acquisition, Y.S., D.S. and W.P. All authors have read and agreed to the published version of the manuscript.

Funding: National Agriculture Traceability Grants Program, Sustainability Reporting Uplift Grant Round, Department of Agriculture, Fisheries and Forestry (ID# 4-IMHSNRC).

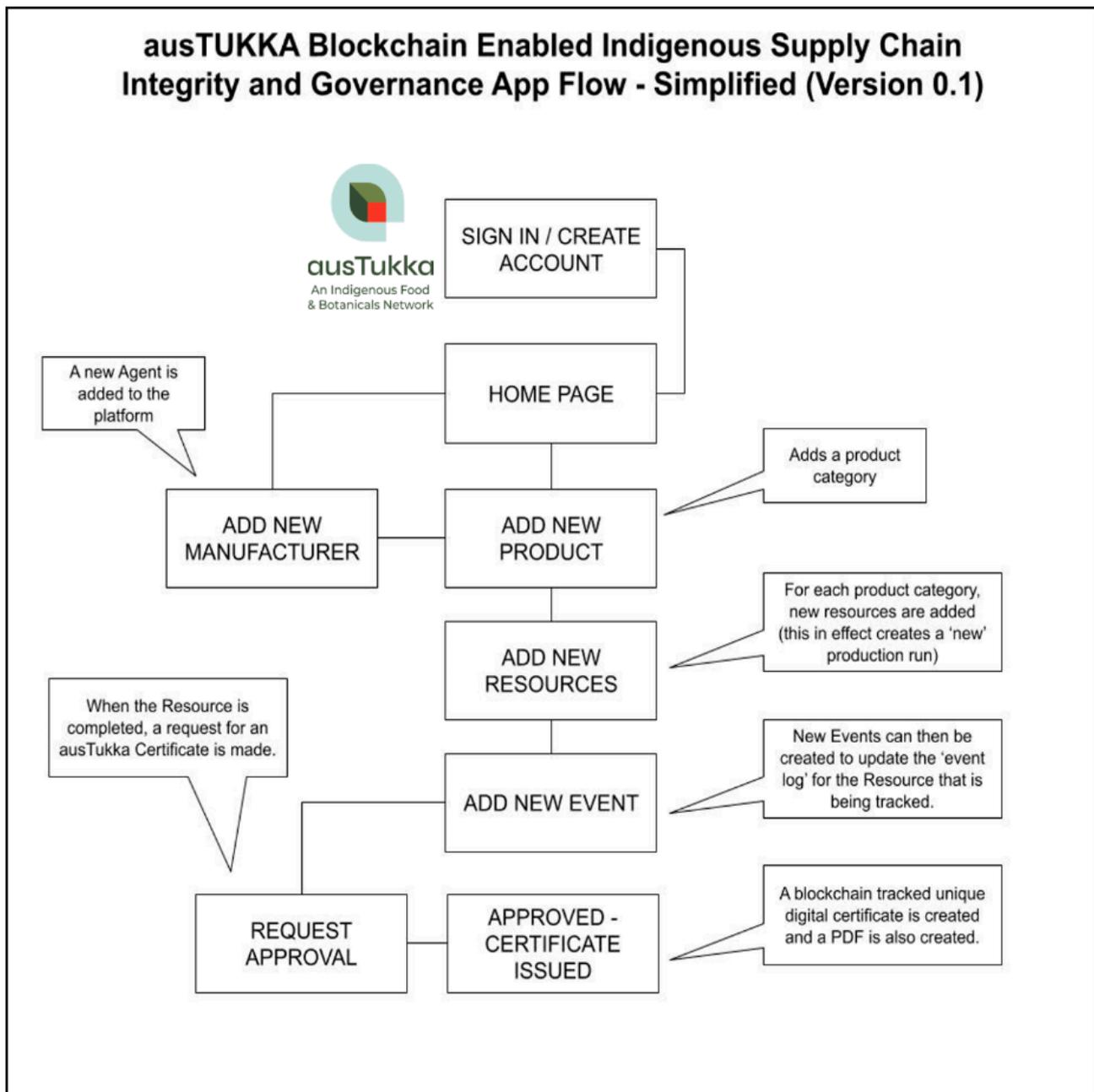
Institutional Review Board Statement: Human research ethics approved by University of Queensland Human Research Ethics Committee A (ID# 2019/HE002607).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

Conflicts of Interest: Author Warwick Powell and Charles Turner-Morris was employed by the company Smart Trade Network, and Author Madonna Thomson was employed by the company Bushtukka and Botanicals Indigenous Enterprise Cooperative Limited. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Appendix A. App Flow and Interaction Diagram



References

1. Cebeci, U.; Arat, E. Establishing Agri and Food Supply Chain Provenance Based on Blockchain: Literature Review. *Eur. J. Sci. Technol.* **2022**, *37*, 59–64. [[CrossRef](#)]
2. Menon, S.; Jain, K. Blockchain Technology for Transparency in Agri-Food Supply Chain: Use Cases, Limitations, and Future Directions. *IEEE Trans. Eng. Manag.* **2024**, *71*, 106–120. [[CrossRef](#)]
3. Reid, J.; Rout, M. Getting to know your food: The insights of indigenous thinking in food provenance. *Agric. Hum. Values* **2016**, *33*, 427–438. [[CrossRef](#)]
4. Sharma, C.; Torrico, D.D.; Carpenter, L.; Harrison, R. Indigenous Meanings of Provenance in the Context of Alternative Food Movements and Supply-Chain Traceability: A Review. *Soc. Sci.* **2021**, *10*, 255. [[CrossRef](#)]
5. Wallace, C.A.; Manning, L. Food provenance: Assuring product integrity and identity. *CABI Rev.* **2020**. [[CrossRef](#)]
6. Morgan, K.; Marsden, T.; Murdoch, J. *Worlds of Food: Place, Power, and Provenance in the Food Chain*; Oxford University Press: New York City, NY, USA, 2006.

7. Smyth, H.; Sultanbawa, Y.; Cozzolino, D. Provenance and Uniqueness in the Emerging Botanical and Natural Food Industries—Definition, Issues and Tools. *Food Anal. Methods* **2021**, *14*, 2511–2523. [[CrossRef](#)]
8. Gorman, J.; Pearson, D.; Wurm, P. Old Ways, New Ways—Scaling Up from Customary Use of Plant Products to Commercial Harvest Taking a Multifunctional, Landscape Approach. *Land* **2020**, *9*, 20. [[CrossRef](#)]
9. Goldsmith, P.; Bender, K. Ten conversations about identity preservation. *J. Chain Netw. Sci.* **2004**, *4*, 111–123. [[CrossRef](#)]
10. Jackson, P. *Food Words: Essays in Culinary Culture*; A&C Black: London, UK, 2013.
11. Vazquez Melendez, E.I.; Bergey, P.; Smith, B. Blockchain technology for supply chain provenance: Increasing supply chain efficiency and consumer trust. *Supply Chain Manag. Int. J.* **2024**, *ahead-of-print*. [[CrossRef](#)]
12. Kumar, N.; Upreti, K.; Mohan, D. Blockchain Adoption for Provenance and Traceability in the Retail Food Supply Chain: A Consumer Perspective. *Int. J. E-Bus. Res.* **2022**, *18*, 17. [[CrossRef](#)]
13. Shahid, A.; Sarfraz, U.; Malik, M.W.; Iftikhar, M.S.; Jamal, A.; Javaid, N. *Blockchain-Based Reputation System in Agri-Food Supply Chain*; Springer International Publishing: New York City, NY, USA, 2020; pp. 12–21.
14. Chandan, A.; John, M.; Potdar, V. Achieving UN SDGs in Food Supply Chain Using Blockchain Technology. *Sustainability* **2023**, *15*, 2109. [[CrossRef](#)]
15. Sharma, M.G. Supply chain, geographical indicator and blockchain: Provenance model for commodity. *Int. J. Product. Perform. Manag.* **2023**, *72*, 92–108. [[CrossRef](#)]
16. Cao, S.; Foth, M.; Powell, W.; Miller, T.; Li, M. A blockchain-based multisignature approach for supply chain governance: A use case from the Australian beef industry. *Blockchain Res. Appl.* **2022**, *3*, 100091. [[CrossRef](#)]
17. Ellahi, R.M.; Wood, L.C.; Bekhit, A.E.A. Blockchain-Based Frameworks for Food Traceability: A Systematic Review. *Foods* **2023**, *12*, 28. [[CrossRef](#)] [[PubMed](#)]
18. Gassler, B.; von Meyer-Höfer, M.; Spiller, A. Exploring Consumers’ Expectations of Sustainability in Mature and Emerging Markets. *J. Glob. Mark.* **2016**, *29*, 71–84. [[CrossRef](#)]
19. Mol, A.P.J.; Oosterveer, P. Certification of Markets, Markets of Certificates: Tracing Sustainability in Global Agro-Food Value Chains. *Sustainability* **2015**, *7*, 12258–12278. [[CrossRef](#)]
20. United Nations. *Transforming Our World: The 2030 Agenda for Sustainable Development*; United Nations: New York City, NY, USA, 2015.
21. Lashkari, B.; Musilek, P. A comprehensive review of blockchain consensus mechanisms. *IEEE Access* **2021**, *9*, 43620–43652. [[CrossRef](#)]
22. MacCarthy, B.L.; Das, S.; Ahmed, W.A.H. Smell the Perfume: Can Blockchain Guarantee the Provenance of Key Product Ingredients in the Fragrance Industry? *Sustainability* **2024**, *16*, 6217. [[CrossRef](#)]
23. Jellason, N.P.; Ambituuni, A.; Adu, D.A.; Jellason, J.A.; Qureshi, M.I.; Olarinde, A.; Manning, L. The potential for blockchain to improve small-scale agri-food business’ supply chain resilience: A systematic review. *Br. Food J.* **2024**, *126*, 2061–2083. [[CrossRef](#)]
24. Subashini, B.; Hemavathi, D. Scalable Blockchain Technology for Tracking the Provenance of the Agri-Food. *Comput. Mater. Contin.* **2023**, *75*, 3339–3358. [[CrossRef](#)]
25. Malik, S.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R.; Paik, H.-Y. Traceable, trustworthy and privacy preserving agri-food supply chains. In Proceedings of the 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Virtual, 13–15 December 2021.
26. Malik, S.; Kanhere, S.S.; Jurdak, R. ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains. In Proceedings of the 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 1–3 November 2018.
27. Hevner, A.R. A three cycle view of design science research. *Scand. J. Inf. Syst.* **2007**, *19*, 4.
28. Baggini, J. *A Short History of Truth: Consolations for a Post-Truth World*; Quercus: Gay, GA, USA, 2017.
29. Molina Ríos, J.; Pedreira-Souto, N. Approach of Agile Methodologies in the Development of Web-Based Software. *Information* **2019**, *10*, 314. [[CrossRef](#)]
30. Wang, Z.; Zheng, Z.; Jiang, W.; Tang, S. Blockchain-Enabled Data Sharing in Supply Chains: Model, Operationalization, and Tutorial. *Prod. Oper. Manag.* **2021**, *30*, 1965–1985. [[CrossRef](#)]
31. UNESCO. *Cultural Landscape of Old Tea Forests of the Jingmai Mountain in Pu’er*; World Heritage Convention: Paris, France, 2023.
32. Banerjee, B.; Chaudhuri, T. *Therapeutic Effects of Tea*; Science Publishers: Hauppauge, NY, USA, 2005.
33. Ahmed, S.; Stepp, J.R.; Orians, C.; Griffin, T.; Matyas, C.; Robbat, A.; Cash, S.; Xue, D.; Long, C.; Unachukwu, U.; et al. Effects of Extreme Climate Events on Tea (*Camellia sinensis*) Functional Quality Validate Indigenous Farmer Knowledge and Sensory Preferences in Tropical China. *PLoS ONE* **2014**, *9*, e109126. [[CrossRef](#)] [[PubMed](#)]
34. Biggs, E.M.; Gupta, N.; Saikia, S.D.; Duncan, J.M. The tea landscape of Assam: Multi-stakeholder insights into sustainable livelihoods under a changing climate. *Environ. Sci. Policy* **2018**, *82*, 9–18. [[CrossRef](#)]
35. Hong, W.; Mao, J.; Wu, L.; Pu, X. Public cognition of the application of blockchain in food safety management—Data from China’s Zhihu platform. *J. Clean. Prod.* **2021**, *303*, 127044. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.