Blockchain-Enabled Fish Provenance and Quality Tracking System

Xu Wang, Guangsheng Yu, Ren Ping Liu, Jian Zhang, Qiang Wu, Steven Su, Ying He, Zongjian Zhang, Litao Yu, Taoping Liu, Wentian Zhang, Peter Loneragan, Eryk Dutkiewicz, Erik Poole, and Nick Paton

***Abstract*—Accurate assessment of fish quality is difficult in practice due to the lack of trusted fish provenance and quality tracking information. Working with Sydney Fish Market (SFM), we develop a Blockchain-enabled Fish provenance And Quality Tracking (BeFAQT) system. A multi-layer Blockchain architecture based on Attribute-Based Encryption (ABE) is proposed to tackle the privacy issue caused by applying Blockchain to secure supply chain data and achieve trusted and confidential data sharing among parties in fish supply chains. An Internet of Things (IoT) chain saves encrypted fish provenance and quality tracking data, and an ABE chain is specifically designed for the access control to the data in the IoT chain. Latest IoT and Artificial Intelligence (AI) technologies, including NarrowBand-IoT, image processing, and bio-sensing, are developed for fish origin proof, supply chain tracking, and objective fish quality assessment. As proven by field trials with SFM and a local fish supply chain, the BeFAQT is able to provide trusted and comprehensive fish provenance and quality tracking information in real-time.**

***Index Terms*—Blockchain, access control, IoT, image processing, electronic nose, fish supply chain.**

I. Introduction

Seafood is one of the most valuable food-based primary industry. However, the fishing industry has not been well regulated. Over 30% of the world's global fish stocks are overfished [1]. Meanwhile, seafood quality is hard to be assessed in practice because the critical origin proof and temperature records are not entirely visible to consumers. In 2018, the Food Agility Cooperative Research Centre organised two workshops attended by representatives from fish markets, research teams, fishermen's co-operatives, government departments, and Non-Governmental Organisations (NGOs). The workshops identified a number of problems, including the lack of fish origin and quality information, within fish supply chains as important constraints to innovation and growth for the seafood industry. Automated fish quality tracking and trusted full chain traceability will provide regulatory bodies, buyers and consumers confidence in the provenance of seafood.

X. Wang, G. Yu, R. P. Liu, J. Zhang, Q. Wu, S. Su, Y. He, Z. Zhang, L. Yu, T. Liu, W. Zhang, P. Loneragan, and E. Dutkiewicz are with University of Technology Sydney, Australia, e-mail: {Xu.Wang-1, Guangsheng.Yu, RenPing.Liu, Jian.Zhang, Qiang.Wu, Steven.Su, Ying.He, Zongjian.Zhang, Litao.Yu}@uts.edu.au, Taoping.Liu@student.uts.edu.au, {Wentian.Zhang, Peter.Loneragan, Eryk.Dutkiewicz}@uts.edu.au.

E. Poole and N. Paton are with Sydney Fish Market, Australia, e-mail: {erikp, nickp}@sydneyfishmarket.com.au.

Blockchain [2], a distributed and immutable ledger technology, has the potential to make fish supply chains more transparent and traceable, allowing consumers to refuse mislabelled produce, and therefore promote sustainable livelihoods and ensure food security [3]. A variety of NGOs work with stakeholders to reform fisheries management globally, focusing on sustainable practices that conserve ecosystems. Several recent projects, such as World Wide Fund for Nature [4] and Provenance [5], have integrated Blockchain technologies in their systems. These platforms only contain static seafood pictures and information. They do not provide real-time provenance and traceability information, and there is limited quality information associated with the products.

Privacy is a major concern when applying Blockchain to secure supply chain data because Blockchain transactions can be accessed by all nodes in a distributed manner. Some consortium Blockchains, e.g., Hyperledger Fabric [6], encrypt transactions with session keys and manage session keys for access control. However, the required number of session keys linearly grows with the number of users. The key management and access control policies can be complicated in large-scale supply chain applications with many participants. Attribute-Based Encryption (ABE) is a promising technology to simplify the complicated key management and achieve fine-grained access control, which allows ciphertext to be decrypted when the attributes of a user match the requested attributes [7]. Most existing ABE-Blockchain schemes [8]–[10] rely on a centralised Trusted Authority (TA) that can be a bottleneck or a weak point.

Accurate assessment of fish quality is difficult in practice due to the lack of provenance and quality tracking information. The latest Internet of Things (IoT) and Artificial Intelligence (AI) technologies have the potential to achieve real-time and objective quality tracking. Recent embedded devices and sensor technologies can provide diverse views with unprecedented details in spatial, temporal, temperature, odour and other environmental domains [11]. NarrowBand-IoT (NB-IoT) is a recent cellular-based Low Power Wide Area Network (LPWAN) technology that connects low-power IoT devices using existing cellular networks. The NB-IoT technology is gradually being supported by network operators yet has rarely been adopted in supply chain applications. Fish quality can be objectively assessed using AI and image processing technologies. Early statistical image processing models have demonstrated that the images of fish eyes, gills and skin tissue can reveal fish freshness [12], [13]. The rapidly developing AI technologies, such as Convolutional Neural Network (CNN),

have shown their effectiveness on challenging computer vision tasks but have not been specifically developed for fish quality assessment tasks.

We develop a Blockchain-enabled Fish provenance And Quality Tracking (BeFAQT)[1] system by integrating Blockchain, ABE, IoT and AI technologies. The BeFAQT system provides trusted fish origin, real-time supply chain condition tracking, and automated quality assessment. Working with our industry partner, Sydney Fish Market (SFM), BeFAQT is being integrated into seafood supply chains for trusted provenance and automated quality tracking. With BeFAQT, consumers are able to verify trusted provenance, quality, and sustainable fishing information for their purchasing decisions. Fishers can receive fish quality feedback to encourage the best fishing practice. SFM and industry regulatory bodies are able to store, manage, share, and audit the captured data in the Blockchain-enabled trusted system. As a winner of 2020 New South Wales (NSW) iAwards [2], the BeFAQT system has shown the potential to evolve the seafood industry for enhanced consumer confidence, efficient supply chain and sustainable fishing practices.

The key contributions of this paper are as follows.

1) We propose a multi-layer Blockchain system for trusted and confidential data sharing, where an IoT chain ensures data integrity and an ABE chain provides fine-grained access control to the IoT chain with decentralised trusted authorities.
2) We develop the latest IoT and AI technologies, including mobile App, NB-IoT device, electronic nose and image processing, for fish origin proof, real-time quality tracking and objective quality assessment.
3) We design and implement a Blockchain-enabled fish provenance and quality tracking system. The system has been integrated with the SFM trading platform by providing Blockchain-certified fish provenance and quality tracking records.
4) Comprehensive trials have been carried out with SFM and a local fish supply chain to demonstrate the system feasibility and benefits. Trial data are annotated by SFM experts to train AI models.

The rest of the paper is organised as follows. Section II gives the industrial background, followed by related works in Section III. The proposed BeFAQT system and the multi-layer Blockchain are presented in Sections IV and V, respectively. In Section VI, the system development and trial results are presented, followed by conclusions in Section VII.

II. Preliminary

A. The Supply Chain of SFM

SFM is a major component of the seafood industry in NSW, Australia. It controls over $150M worth of seafood sales annually. The local fish supply chain starts from fishing near coasts. After fishing, the fishers pack the harvested fish into boxes, which are rented from SFM, at local Co-Ops. Meanwhile, the fishers print paper labels, containing fishing date, fish species, sizes and others, and attach the paper labels to the boxes. The boxes of fish are temporally chilled and stored in cool rooms and then transported to the SFM by local Co-Ops. When the fish arrive at SFM, SFM staffs and buyers can read the fishing information from the paper labels and manually assess fish quality. The fish are then sold in SFM, mainly in the form of the Dutch auction. After the auction, the buyers distribute the fish at SFM, fish shops and restaurants. Key steps in the supply chain, e.g., fishing and transportation, are manually recorded in paper logbooks for regulation and quality tracking.

B. Fish Quality Measurement

Chilled fish is a highly perishable product. The deterioration process immediately starts after harvest and can be at different rates according to fish species and storage temperature. SFM adopts the quality index (QI) to guide the measurement of changes in chilled seafood from the point of harvest through transport, auction and distribution [14]. Starting from zero, the QI linearly grows with the period of storage in ice at 0 °C (known as icedays). The growth varies among different fish species. High temperature can accelerate fish deterioration and also the growth of QI. In the case without trusted temperature records, the QI can be evaluated by manually checking fish appearance, texture and odour. The measurement is designed to be the accumulation of demerit points where each demerit point usually ranges from zero to three. A sufficient number of parameters, e.g., fish eyes, gills, mucus, abdomen and cut surfaces, have been chosen by SFM to cover important indicator attributes.

C. Demands and System Goals

Participants in the supply chain have various demands. Fishers want feedback from SFM, buyers and consumers to build an incentive for good fishing practice and high-quality seafood. Co-Ops and SFM want to reduce potential loss in the supply chain and improve efficiency. SFM, accounting firms and government departments want trusted supply chain data for effective audit and regulation. Buyers and consumers want easy access to trusted provenance and quality tracking information and the reduction of expensive, subjective and inaccurate manual quality measurement. Thus, the BeFAQT system is designed to achieve the following goals.

1) Real-time Fish Quality Tracking: We design the BeFAQT system to track the fish temperature and location from catch to sale. SFM and Co-Ops will be able to estimate fish quality and reduce accidental loss in real-time comparing with the conventional paper logbook.

2) Objective and Reliable Fish Quality Measurement: We design the BeFAQT system to measure fish quality from multiple data sources in an objective and reliable way. SFM, buyers and consumers will be able to save time on the fish quality measurement and reduce the expensive labour cost.

[1]https://www.befaqt.com/

[2]https://aiia.com.au/iawards/about/2020-winners-and-merit-recipients/2020-nsw-winners-and-merit-recipients

3) Trusted Platform: We design the BeFAQT system to provide trusted provenance proof and quality tracking data to all participants. Fishers can differentiate their fish from others and have the incentive to improve fish quality. Co-Ops and SFM can simplify the trading process and improve supply chain efficiency. Buyers and consumers can get trusted quality information and build confidence in the seafood.

4) Fine-Grained Access Control: We design the BeFAQT system to preserve the privacy of all participants and enable confidential data sharing. The fish tracking data will be produced, processed and consumed as designed. The access control is to be managed by decentralised parties.

III. Related Work

Beyond cryptocurrency, Blockchain has been developed for supply chains to improve transparency, reliability and security [3], [11], [15]–[18]. FishNet is a demo project showing the concept of combining Sawtooth Blockchain and IoT for the provenance of fish from catch to plate [3]. In the project design, authorised IoT servers can update the states or transfer ownership of fish assets on behalf of IoT sensors. Although demonstrated with sample data, the design of FishNet has not been implemented in real supply chains. The Sawtooth Blockchain has also been employed for the steel quality tracking in [11], where a Proof-of-Competition (PoC) consensus mechanism is adopted as the Blockchain consensus protocol. Industrial IoTs collect raw quality data, such as location and shipment info, at distribution points and then feed the quality data to the Blockchain. A similar Blockchain-IoT supply chain solution has been commercialised by IBM Food Trust which provides transparent digital food supply chain service based on the Hyperledger Fabric [16]. Proved by trials on pork and mango supply chains, the Food Trust platform enhances the supply chain traceability by collecting supply chain data, such as pack date and shipment identifiers, in real-time.

Data confidentiality is a significant challenge when applying the Blockchain technology to supply chains. Consortium Blockchains can apply access control policies to protect data confidentiality, such as the private data scheme in Hyperledger Fabric [19]. In the scheme, the users who can access the private data are added into a permitted group, while the data consumers who do not have access to the private data can ask permitted users to verify data by comparing data hash values. This scheme would sacrifice data transparency and can hardly be adapted to applications with complicated access control policies. The public Blockchain technology assures data integrity and transparency but does not natively support access control on Blockchain data. It is possible to introduce access control to public Blockchains using the envelope encryption, where the data to be saved in public Blockchains are firstly encrypted with data encryption keys (DEKs) before uplodaing, and then the DEKs are encrypted with manageable keys [20]. The DEKs can be managed in an efficient and fine-grained way using the ABE encryption scheme [8]–[10]. However, most of ABE-Blockchain schemes, such as [9] and [10], rarely support attribute update in ABE due to the inherent immutability of Blockchain and thus can be inapplicable for dynamic IoT applications [10]. Our earlier work [8] develops the editable Blockchain technology using Chameleon Hash (CH) algorithms [21] to enable ABE attribute update. Nevertheless, the proposed scheme relies on a centralised TA to control main phases in ABE, which can be a performance bottleneck and a weak point.

IoT technology has been widely adopted for objective quality tracking in food supply chains, where early applications focus on location and temperature tracking [22]. One essential research is the low-power wireless communication technology which affects the battery life of IoT devices. A recent advanced LPWAN standard is NB-IoT which aims at low-cost devices, high coverage, long battery life and massive capacity and is being gradually commercialised worldwide [23]. New features of IoT devices, such as olfaction in electronic nose, are invented to monitor the environment and improve food safety [24], [25]. The active gas sensor is the core of electronic nose, which can detect the odour and generate electrical signals from chemical vapours [26], [27]. Powered by AI technology, the odour and vision data can be analysed for semantic and objective fish quality measurement. For example, the image processing technology has been extended for fish species recognition and freshness identification [12]. The principal technologies are fine-grained object recognition and image processing on the image features of important fish parts [13], [28].

To the best of our knowledge, most of the Blockchain and IoT research focuses on some specific tasks and has not been extensively developed and integrated for the temperature-sensitive fresh fish supply chain. It is necessary to propose a comprehensive end-to-end solution to address the demands in the supply chain as analysed in Section II and solve concrete issues in implementation.

IV. BeFAQT System Design

A. System Overview

The developed BeFAQT system adopts Blockchain as a trust centre, integrates the latest IoT tracking, image processing and electronic nose (E-nose) technologies, and provides user-friendly applications for various users, as shown in Fig. 1.

Each fish box is identified by a unique ID, denoted by the *fish ID*, which is stored in a Near Field Communication (NFC) tag on the box. The NFC tag enables the fish box to interact with other modules and participants' mobile phones. We design a Fisher App and NB-IoT devices for the fish origin proof and real-time quality tracking. We also introduce image processing and E-nose to assess the fish quality from vision and odour perspectives. An IoT chain runs as a trusted data platform ensuring the trustworthiness of fish provenance and quality tracking data. An ABE chain is specifically designed for the access control to the data in the IoT chain. Consumers can track and verify their purchased products in terms of provenance, trace, and quality indices. The BeFAQT system is also integrated into the SFM trading platform by providing Blockchain-certified provenance proof and quality tracking information through Application Programming Interfaces (APIs).

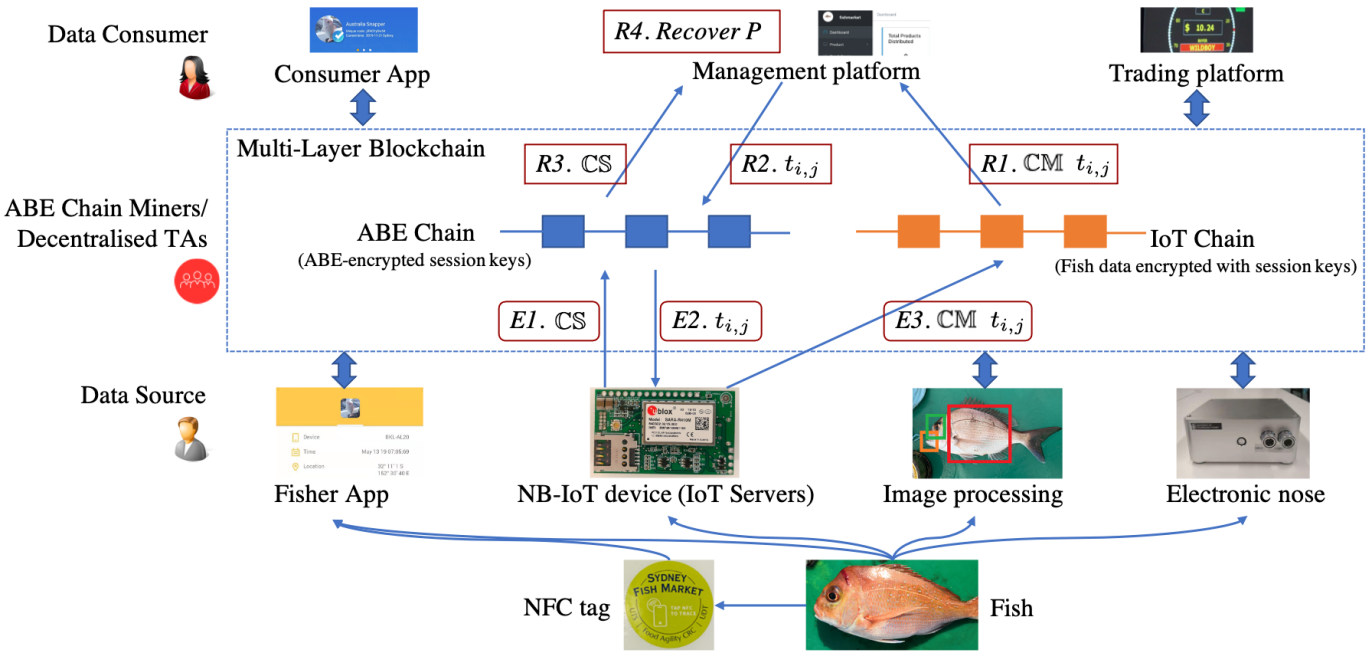


Fig. 1. The system overview of BeFAQT. Data sources, including Fisher App, NB-IoT devices, image processing, and electronic nose, provide objective and real-time fish data. An IoT chain stores encrypted fish data, while an ABE chain saves ABE-encrypted session keys for the access control to the IoT chain. The *encrypting and publishing message* protocol is illustrated with the IoT servers executing steps *E1*, *E2* and *E3*. The *retrieving and decrypting message* protocol is illustrated with the management platform executing steps *R1*, *R2*, *R3* and *R4*.

B. Fish Provenance Proof and Tracking

1) Fisher App for Provenance Proof: We design a Blockchain-based Fisher App to realise fish provenance proof. The Fisher App can be installed on fishers' mobile phones and enables the fishers to take Blockchain-certified photos of the catch, then the fish photos, together with time and location, are locked with certificates (i.e., their hash values) and uploaded to the Blockchain. We also engage with the NSW Department of Primary Industries (DPI) of to integrate our development with the DPI FishSmart App (an information App for fishers) [29].

2) IoT for Tracking: We design new NB-IoT devices to track the fish supply chain and monitor fish temperature and location. The IoT devices are small, water-resistant and with long battery life. They are mounted on the boxes from SFM, which are used by fishers to store and transport seafood across the state. Every IoT device is equipped with a Global Positioning System (GPS) sensor to track the box. It is also wired to an external temperature sensor which enables the IoT devices to sense the fish temperature rather than the onboard temperature. In terms of IoT communication, we choose the NB-IoT technology, due to its features of low-cost, low energy-consuming, and wide-coverage.

C. Fish Quality Measurement

1) Image Processing: Freshness identification, size measurement, and species recognition are three specific functions that are developed based on computer vision and deep learning technologies to provide objective and accurate quality measurement results. The species recognition and size measurement functions are performed on the fish that are just caught out of water, while the freshness identification is performed before the auction for buyers.

2) E-nose: We design an E-nose module to capture the odour information for the fish freshness identification at SFM before the auction. The E-nose equipment can interpret odour into electrical signals and extract the freshness information. The non-parametric kernel-based modelling [30], [31] is adopted to pre-process the E-nose data and extract the key features. On top of the feature extraction function, a Hidden Markov Model (HMM)-based model is developed to derive quality indices.

V. Multi-Layer Blockchain System with ABE-based Access Control

We propose a multi-layer Blockchain system, consisting of an IoT chain and an ABE chain, as shown in Fig. 1, which enables trusted and confidential data sharing utilising ABE in a decentralised manner. The ***IoT Chain*** can be an arbitrary Blockchain storing fish data encrypted with session keys, while the ***ABE Chain*** is a consortium Blockchain, managed by SFM and Co-Ops. The ABE chain stores ABE-encrypted session keys for access control. Users can get access to the encrypted session keys when their attributes match the set of rules associated with encrypted session keys. The transactions in the ABE chain are editable for the attribute update in ABE by applying the Chameleon Hash (CH) algorithm. Different from collision-free hash algorithms, an arbitrary hash collision can be efficiently constructed with a trapdoor in CH algorithms.

This design is an extension of our previous work [8], where a centralised Trusted Authority (TA) is replaced with a group

of ABE chain miners. By using new verification schemes, the distribution of updated ABE private keys and the version control of the keys can be conducted by the decentralised miners (TAs). In our design, a general Ciphertext-Policy-ABE (CP-ABE) [7] and a general CH [21] are specifically used. The details of these algorithms, such as ABE encryption/decryption and CH update [8], are beyond the scope of this paper and not presented. Tab. I summarises the notations used in the rest of the paper.

TABLE I: Notation Definition

Notation	Definition
DS	Data Source
DC	Data Consumer
P	Plaintext of fish data
$SK_{\mathbf{A},P}/PK_{\mathbf{A},P}$	Session encrypt/decrypt keys with access policy $\{\mathbf{A}\}$
$\mathbb{CM}$	Ciphertext of fish data
$\{\mathbf{A}\}$	Access policy that defines the access to session keys
$\mathbb{ABE}_{\mathbf{A}}$	ABE algorithm with access policy $\{\mathbf{A}\}$
$\alpha \vDash \mathbf{A}$	An attribute α satisfies an access policy $\{\mathbf{A}\}$
$ABE_{\alpha,PK}$	ABE public key for a member with attribute α
$ABE_{\alpha,SK}$	ABE private key for a member with attribute α
$\mathbb{CS}$	Ciphertext of a session decryption key
$t_{i,j}$	The j-th transaction in the i-th block of the ABE chain
$v_{i,j}$	The CH trapdoor for $t_{i,j}$
CH_{SK}/CH_{PK}	Private/Public key of the CH algorithm

A. System Roles

The system includes the following three roles:

- *Data Source (DS)*: The DS, e.g., the Fisher App and IoT servers, publishes tracking and quality data to the Blockchains in the form of transactions. Along with every piece of published data, an access policy set, defining the attributes to access the data, is also specified.
- *Data Consumer (DC)*: The DC, e.g., Consumer App and SFM trading platform, fetches data from the Blockchains. In the design, DC's attributes can be updated by the ABE chain miners as a part of the consensus. The attribute-related data, such as ABE-encrypted session keys, are updated simultaneously.
- *Miner*: The ABE chain Miners are managed by reliable participants in the fish supply chain, e.g., SFM and Co-Ops. Miners firstly mine transactions into the ABE chain like in general Blockchains. Two new responsibilities of the Miners are, 1) to be a multi-authority group of TAs in order to manage attributes for any entities on-chain by conducting the new privacy-preserving **ABE-Key-Verification-Scheme**; and 2) to track the updates of attributes and ABE-encrypted session keys by conducting the **Update-History-Verification-Scheme**.

Each participant in the fish supply chain is assigned with one or more attributes for the ABE scheme, which are stored in the ABE chain. It is worth noting that only Miners run consensus protocols to extend the ABE chain. The other roles only send transactions to the chains and read from the chains. Thus, the communication overhead can be suppressed.

B. The Multi-layer Blockchain System

In the multi-layer Blockchain system, the IoT chain provides the confidential and tamper-resistant data service. The data on the IoT chain are encrypted with session keys. The ABE chain manages the encrypted session keys to achieve access control to the data in the IoT chain.

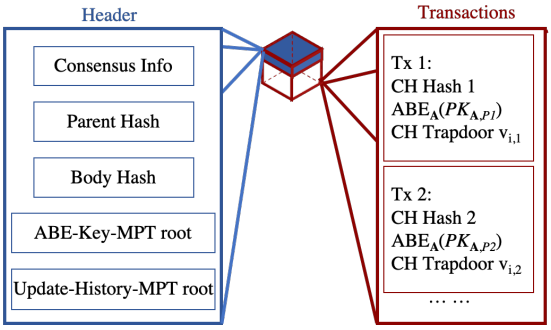


Fig. 2. The structure of the ABE chain block.

- *IoT Chain:* A DS collects the fish supply chain data, encrypts the data with a session key, and then publishes encrypted data to the IoT chain by embedding the encrypted data in transactions. The IoT chain can be any existing Blockchain or self-built Blockchain as long as the Blockchain can store arbitrary data.
- *ABE Chain:* An ABE chain manages the ciphertext of encrypted session keys, denoted by $\mathbb{CS}$, for access control. The ABE algorithm is employed here for encryption and decryption. The block structure of the ABE chain is given in Fig. 2. Different from immutable Blockchain, transactions in the ABE chain have editable data fields to allow attribute updates of ABE by employing the CH algorithm.
- *Inter-Chain Protocols:* The protocols are designed for data exchange among the IoT chain and the ABE chain. All roles, i.e., DS, DC and Miners, can act as clients on both IoT chain and ABE chain, running the Inter-Chain protocols.

The inter-chain protocols include the *encrypting and publishing message* protocol and the *retrieving and decrypting message* protocol; see Algos. 1 and 2 for details. Starting with an initialisation, in which the ABE key pairs w.r.t any attribute α ($ABE_{\alpha,SK}/ABE_{\alpha,PK}$) and CH key pairs ($CH_{SK}/CH_{PK}$) are securely generated and distributed, the inter-chain protocols are shown as follow.

Encrypting and publishing message P: A DS keeps session encryption/decryption keys $SK_{\mathbf{A},P}$ / $PK_{\mathbf{A},P}$ for a messages P. The DS encrypts $PK_{\mathbf{A},P}$ and obtains $\mathbb{CS}$ = $\mathbb{ABE}_{\mathbf{A}}(PK_{\mathbf{A},P})$, using its ABE public key, i.e., $ABE_{\alpha,PK}$. Here, $\{\mathbf{A}\}$ denotes an attribute policy, and α is an attribute satisfying $\{\mathbf{A}\}$, i.e., $\alpha \vDash \mathbf{A}$. This $\mathbb{CS}$ is saved in the transaction $t_{i,j}$ (the j-th transaction of the i-th block) of the ABE chain along with an editable chameleon hash by using the CH public key CH_{PK}. Then, a message P is encrypted into ciphertext, denoted by $\mathbb{CM}$, with $SK_{\mathbf{A},P}$ by the DS. The $\mathbb{CM}$ and the indices to $t_{i,j}$ are saved by the IoT chain.

Algorithm 1: The trusted and confidential data sharing

▷ **Define**

// This transmission is secured by any private and encrypted channels.
Receiver ⇐ Sender.***Send***(Message);

▷ **Initialisation**

// Miners of the ABE Chain, constituting the decentralised TA, generate the ABE key pair w.r.t attribute α and the global CH key pair with consensus.
1 $(ABE_{\alpha,SK}, ABE_{\alpha,PK})$, $(CH_{SK}, CH_{PK}) \leftarrow$ *Miner.**Initialise***();

// The ABE private key is secured by the ABE-Key-MPT.
2 $\text{Block}_{ABE,Pending} \leftarrow$ *Miner.**UpdateABE-MPT***$(Hash(ABE_{\alpha,SK}))$;

// Miners run the chain consensus protocol to append the block and update the ABE-Key-MPT.
3 *ABE Chain* ← ***Consensus***$(\text{Block}_{ABE,Pending})$;

// Miners broadcast the ABE public key and the public CH key to the public network.
4 *Public Network* ⇐ *Miner.**Send***$(ABE_{\alpha,PK}, CH_{PK})$;

// Miners multicast the ABE private key to the eligible nodes. The nodes verify the ABE private key using the MPT proof.
5 $Nodes_{\alpha}$ ⇐ *Miner.**Send***$(ABE_{\alpha,SK}$, MPT proof);
6 $Nodes_{\alpha}$.***Verify***$(ABE_{\alpha,SK}$, MPT proof);

▷ **DS Initialisation**

// A DS planning to publish a message P generates a session key pair with the access policy $\{\mathbf{A}\}$ that enables attribute α, i.e., $\alpha \vDash \mathbf{A}$.
7 $(SK_{\mathbf{A},P}, PK_{\mathbf{A},P}) \leftarrow DS.$***Initialise***();

▷ **Encrypting and Publishing**

8 $DS.$***EnAndPub***$(SK_{\mathbf{A},P}, PK_{\mathbf{A},P}, ABE_{\alpha,PK}, P)$;

▷ **Retrieving and Decrypting**

// A DC satisfying $\{\mathbf{A}\}$ retrieves $\mathbb{CM}$ and $t_{i,j}$ from a transaction in the *IoT chain*. After that, the DC retrieves $\mathbb{CS}$ by using $t_{i,j}$ and recovers $PK_{\mathbf{A},P}$ based on which the plaintext of message P can be obtained.
9 $P \leftarrow DC.$***ReAndDe***$(ABE_{\alpha,SK}, \mathbb{CM}, t_{i,j})$;

Algorithm 2: The *encrypting and publishing message* protocol ***EnAndPub()*** and the *retrieving and decrypting message* protocol ***ReAndDe()***

▷ ***EnAndPub()***
Input: $SK_{\mathbf{A},P}$, $PK_{\mathbf{A},P}$, $ABE_{\alpha,PK}$, P
Output: A new block appended to the *IoT chain* and the *ABE chain*, respectively

// The DS encrypts $PK_{\mathbf{A},P}$ with $ABE_{\alpha,PK}$ to get $\mathbb{CS}$.
1 $\mathbb{CS} \leftarrow ABE_{\alpha,PK}.$***Encrypt***$(PK_{\mathbf{A},P})$;

// The DS Chameleon-hashes the ciphertext with CH_{PK} and a trapdoor v prior to inserting it into a new pending block of the *ABE chain*.
2 $\text{Block}_{ABE,Pending} \leftarrow$ ***SendChameleonTx***$(\mathbb{CS}, CH_{PK}.$***CH_Hash***$(\mathbb{CS}, v))$;

// Append the block to the *ABE chain* by running the consensus protocol, obtain the transaction index $t_{i,j}$.
3 *ABE Chain*, $t_{i,j} \leftarrow$ ***Consensus***$(\text{Block}_{ABE,Pending})$;

// The DS encrypts P with $SK_{\mathbf{A},P}$ and sends a new transaction containing the ciphertext and $t_{i,j}$ to the *IoT chain*.
4 $\mathbb{CM} \leftarrow SK_{\mathbf{A},P}.$***Encrypt***$(P)$;
5 $\text{Block}_{IoT,Pending} \leftarrow$ ***SendNormalTx***$(\mathbb{CM}, t_{i,j})$;

// IoT chain miners append the block to the *IoT chain* by running the chain consensus protocol.
6 *IoT Chain* ← ***Consensus***$(\text{Block}_{IoT,Pending})$;

▷ ***ReAndDe()***
Input: $ABE_{\alpha,SK}$, $\mathbb{CM}$, $t_{i,j}$
Output: P

// The DC retrieves $\mathbb{CS}$ with $t_{i,j}$ in the *ABE chain*.
7 $\mathbb{CS} \leftarrow$ ***Find***$(t_{i,j})$;
8 $PK_{\mathbf{A},P} \leftarrow ABE_{\alpha,SK}.$***Decrypt***$(\mathbb{CS})$;
9 $P \leftarrow PK_{\mathbf{A},P}.$***Decrypt***$(\mathbb{CM})$;

Retrieving and decrypting message P: All the DC can retrieve $\mathbb{CS}$ from the ABE chain and $\mathbb{CM}$ from the IoT chain. However, only the DCs, whose attributes match the access policy, can decrypt them. The DC firstly identifies the transaction containing $\mathbb{CM}$ from the IoT chain and retrieves $\mathbb{CM}$ and as well as the indices to $t_{i,j}$. Next, the DC can retrieve transaction $t_{i,j}$, which contains $\mathbb{CS}$, from the ABE chain. Then, the DC can decrypt $\mathbb{CS}$ with its ABE secret key $ABE_{\alpha,SK}$ for the session decryption key $PK_{\mathbf{A},P}$. In this way, the DC with permitted attributes can decrypt $\mathbb{CM}$ with the session decryption key $PK_{\mathbf{A},P}$ and recover the message P.

C. Attribute Updates on the ABE Chain

Attribute updates is a challenging task in Blockchain with decentralised TAs. We present a solution to update attributes based on the CH algorithm in the previous work. In this section, we propose two new efficient verification schemes to improve the trustworthiness of ABE private keys and encrypted session keys while preserving the confidentiality of irrelevant keys, in the context of decentralised TAs; see Algo. 3 for details.

ABE-Key-Verification-Scheme: This scheme is used for DSs and DCs to ensure the validity of the ABE private keys distributed by the decentralised TAs.

A permitted DC/DS, which owns the attribute α satisfying $\{\mathbf{A}\}$, will be given an ABE secret key $ABE_{\alpha,SK}$ when it joins or updates. The $ABE_{\alpha,SK}$ is firstly generated by one of the Miners, e.g., the leader in the Byzantine Fault Tolerance (BFT)-based consensus protocol, employing the key generation algorithm in [8]. The hash value of the secret key $ABE_{\alpha,SK}$ is then locked in a Merkle Patricia Tree (MPT), namely ABE-Key-MPT as shown in Fig. 3, by all Miners via the ABE chain consensus process. In the MPT, each leaf keeps the hash value of an ABE secret key, i.e., $Hash(ABE_{\alpha,SK})$, while the root hash of the ABE-Key-MPT is immutably recorded in a header of the ABE chain.

The leaf gets updated where the corresponding leaf $Hash(ABE_{\alpha,SK})$ is replaced by a new $Hash(ABE'_{\alpha,SK})$, such as after user revocation. The $ABE_{\alpha,SK}$ is finally sent to the DS/DC along with an MPT proof message that includes

Algorithm 3: Attribute update

Input: An attribute α

▷ **Computation phase**

// The miner who is in charge computes the updating factor (UF) associated with the attribute α.

$(\text{UF}_{SK}, \text{UF}_{\mathbb{CS}}) \leftarrow$ *Miner.**ComputeUpdate***(α);

// The miner sends the update factor of $\mathbb{CS}$ to all the other miners.

Miner$_{other} \Leftarrow$ *Miner.**Send***$(\text{UF}_{\mathbb{CS}})$;

▷ **Updating phase**

// Miners retrieve $\mathbb{CS}$ with $t_{i,j}$ in the *ABE chain* and update it with the update factor of $\mathbb{CS}$.

$\mathbb{CS} \leftarrow$ *Miner.**Find***$(t_{i,j})$;

$\mathbb{CS}' \leftarrow$ *Miner.**UpdateCS***$(\mathbb{CS}, \text{UF}_{\mathbb{CS}})$;

// Miners overwrite the outdated $\mathbb{CS}$ with $\mathbb{CS}'$ in the $t_{i,j}$ transaction by using CH_{SK}.

*Miner.**Overwrite***$(\mathbb{CS}', t_{i,j}, CH_{SK})$;

▷ **Auditing phase**

// The updated ABE private key is secured by ABE-Key-MPT, and the updated $\mathbb{CS}$ is secured by the Update-History-MPT.

$\text{Block}_{ABE,Pending} \leftarrow$ *Miner.**UpdateABE-MPT***$(Hash(ABE'_{\alpha,SK}))$ **and** *Miner.**UpdateHistory-MPT***$(Hash(\mathbb{CS}', v))$;

// Miners append the block to the *ABE chain* by running the consensus protocol.

ABE Chain, $t_{i,j} \leftarrow$ ***Consensus***$(\text{Block}_{ABE,Pending})$;

▷ **Finalising phase**

// The miner sends the updating factor UF_{SK} and the MPT proof of $ABE'_{\alpha,SK}$ in ABE-Key-MPT to the non-revoked nodes.

$Nodes_{\alpha} \Leftarrow$ *Miner.**Send***$(\text{UF}_{SK}$, MPT proof$)$;

// Non-revoked nodes update their ABE private keys by using the updating factor UF_{SK}.

$ABE'_{\alpha,SK} \leftarrow$ $Node_{\alpha}$.***UpdateABE_SK***$(ABE_{\alpha,SK}, \text{UF}_{SK})$;

// **ABE-Key-Verification**: nodes verify new ABE private keys using MPT proof.

$Nodes_{\alpha}$.***Verify***$(ABE'_{\alpha,SK}$, MPT proof$)$;

// Non-revoked nodes can then decrypt $\mathbb{CS}'$ in $t_{i,j}$ by $ABE'_{\alpha,SK}$ to recover P.

$P \leftarrow Nodes_{\alpha}$.***ReAndDe***$(ABE'_{\alpha,SK}, \mathbb{CM}, t_{i,j})$;

// **Update-History-Verification**: nodes can also verify that $\mathbb{CS}'$ is the latest version using the MPT proof′ to the Update-History-MPT.

$\mathbb{CS}' \leftarrow$ ***Find***$(t_{i,j})$;

$Nodes_{\alpha}$.***Verify***$(\mathbb{CS}'$, MPT proof′$)$;

// New members of attribute α can also decrypt.

$Node_{new,\alpha} \Leftarrow$ *Miner.**Send***$(ABE'_{\alpha,SK})$;

$P \leftarrow Node_{new,\alpha}$.***ReAndDe***$(ABE'_{\alpha,SK}, \mathbb{CM}, t_{i,j})$;

the hash values adjacent to the path from $Hash(ABE_{\alpha,SK})$ to the root. The DS/DC also learns the latest block headers, including the immutable ABE-Key-MPT root from the ABE chain. Thus, the ABE secret key $ABE_{\alpha,SK}$ can be verified that it has been accepted by the ABE chain without revealing the confidential information of other keys via conducting the MPT proof.

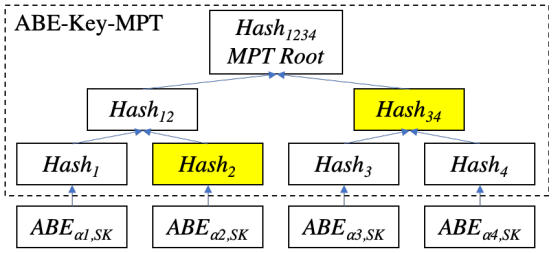


Fig. 3. Illustration of the ABE-Key-MPT, where the MPT proof of $ABE_{\alpha 1,SK}$ is highlighted.

Update-History-Verification-Scheme: This scheme is used to track updates of the encrypted session keys, due to the revocation in the ABE scheme, in the ABE chain.

The proposed scheme allows revocation in ABE where the session keys are re-encrypted with new ABE keys by Miners, and then updated to the corresponding transaction in the ABE chain. Every encrypted session key $\mathbb{CS}$ is embedded into a transaction in the ABE chain along with a CH trapdoor, i.e., $v_{i,j}$ in $t_{i,j}$, which allows the Miners, by using the CH private key CH_{SK}, to update encrypted session key and trapdoor simultaneously without changing the chameleon hash value of the transaction.

The update of the ABE secret keys $ABE'_{\alpha,SK}$ and the encrypted session keys $\mathbb{CS}'$ can be tracked by recording the update of the trapdoors. We trace $v_{i,j}$ with another MPT by the name of Update-History-MPT. Each leaf stores the hash value of the current version of $v_{i,j}$, i.e., $Hash(v_{i,j})$, while the root hash is saved in a header of the ABE chain. Thus, all updates are immutably recorded in the latest block of the ABE chain by storing the Update-History-MPT, and the abuse of attribute update can be eliminated. The revoked DSs/DCs cannot decrypt $\mathbb{CS}$ in the ABE chain for the session decryption key $PK_{\mathbf{A},P}$. The non-revoked and new DSs/DCs, whose attributes match $\{\mathbf{A}\}$, can access and verify $\mathbb{CS}$, and consequently recover P.

VI. Implementation and Analysis

Comprehensive trials were carried out with a snapper supply chain in NSW after the BeFAQT system had been developed. We first identified a snapper fisher in Forster, which is about 308 km to the north of SFM, as a test case. During fishing, fishers first sailed their boat to the fishing spots (about 10 km offshore and 40 m above reefs). At the spots, the fishers caught snappers with fishing rods and then chilled the snappers in an ice slurry box on the boat. After fishing and returning to the local Co-Op, the fishers measured the snappers individually, then packed the snappers in boxes and covered the snappers with ice. Some of the snappers were locally sold, while others were transported to SFM by the Co-Op and sold in SFM.

A. Multi-Layer Blockchain System

The multi-layer Blockchain system was developed based on the Ethereum open-source code [32]. We considered a semi-trusted fish consortium where both the ABE and IoT

chains were managed by four semi-trusted parties in the fish consortium, i.e., SFM and three Co-Ops. The four semi-trusted parties ran an optimised practical Byzantine Fault Tolerance (pBFT) [33] consensus protocol to achieve rapid block confirmation and high throughput of the chains. Specifically, in *pre-prepare* phase of the consensus protocol, the whole block was transmitted, while only the block index and the block hash value were transmitted in the rest *prepare* and *commit* phases to reduce the communication overhead.

TABLE II: Blockchain throughput under different payloads.

Case	$L = 1$	$L = 20$	$L = 30$	$L = 40$	$L = 50$
Throughput(tx/s)	1385	921	909	785	682

We tested the throughput of the implemented consensus protocol with four miners under different lengths of transaction payload. The block period was set to be five seconds so that transactions can be confirmed within five seconds for real-time tracking. The throughput under five cases, i.e., L = 1, 20, 30, 40 and 50, is given in Table II, where L is the transaction payload size measured in bytes. The consensus protocol can reach the throughput of thousands of transactions per second in lightweight tasks, e.g., $L \leq 30$, and process 685 transactions per second when the transaction payload is 50 characters. As a result, the multi-layer Blockchain system can handle up to 2.5 million (i.e., $685 \times 60 \times 60$) boxes of fish with a confirmation delay of five seconds in the case that a fish box generates a piece of tracking record every one hour.

We developed the cryptographic schemes, including CP-ABE and CH, using Charm[3]. The modules in BeFAQT, their roles and ABE attributes are given in Table. III.

TABLE III: System modules and their ABE attributes.

Modules	**Role**	**Attributes**
ABE Chain Miners	Miners	Manager, Miner
IoT servers	DS	SFM, IoT, Server
Image processing/E-nose	DS	SFM, IoT
Fisher App	DS	Fisher, Co-Op
API Servers	DC	SFM, Distributor, Buyer
Consumer App	DC	Buyer, Consumer

1) Security Analysis: The IoT chain and ABE chain collaborate to achieve the following properties.

System Availability: In regard to the ABE attribute update, the system can achieve the fault tolerance of the ABE chain. Benefited from the design of decentralised CAs, the key initialisation and update tasks can be transferred to the next CA if the current one is failed. In regard to read and write supply chain data, the system can achieve the fault tolerance of the IoT chain. Our implementation with four miners running the pBFT-based algorithm can tolerate one failed ABE chain Miner on the ABE attribute update. The implementation can tolerate four failed ABE chain Miners in terms of read/write supply chain data as long as the IoT chain is running.

Data integrity: The design of decentralised TAs ensures that all the DSs/DCs and the supply chain data are authorised by SFM and all Co-Ops. Once being published, the data cannot be tampered because of the tamper-resistance feature of the chains. The proposed two new verification schemes guarantee that DCs cannot be frauded with keys that have not been accepted by the ABE chain.

Fine-grained access control: The design of the ABE-encrypted session key can provide fine-grained access control on the public IoT chain. The encrypted supply chain messages in the IoT chain can only be decrypted by the DCs whose attributes match the access policies saved in the ABE chain.

Attribute update of ABE: In the multi-layer Blockchain system, the attributes can be updated due to the editability of the ABE chain. During the attribute update, all the related $\mathbb{CS}$ in the ABE chain are updated to stop revoked DCs from further access. Meanwhile, the related session keys remain fixed. Only the DCs whose attributes match the latest attribute policies can decrypt the session keys saved in the ABE chain and then decrypt the encrypted data saved in the IoT chain.

2) Deployment and Extension: The proposed multi-layer Blockchain system allows flexible and dynamic implementations. The ABE chain and the IoT chain are loosely coupled by the inter-chain protocols such that each of them can be independently customised. The chains can be customised according to specific requirements on security, performance, cost, etc. The consensus protocols of the chains can be replaced with alternatives [34] because new designs introduced in Section V can be embedded into consensus requests.

Choice of the IoT chain: The IoT chain in the multi-layer Blockchain system can be an arbitrary Blockchain or even general databases. The IoT chain can be a public Blockchain, e.g., the public Ethereum network, where the data transactions can barely be tampered [35]. The IoT chain can also be a Directed Acyclic Graph (DAG)-based Blockchain [36], consortium Blockchain or InterPlanetary File System [37] for high throughput and low storage cost.

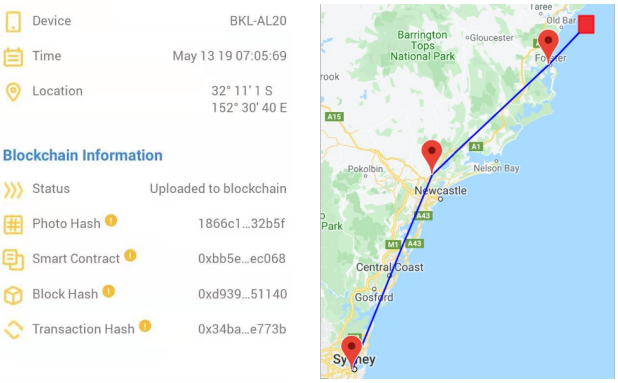
Multiple ABE chains and IoT chains: The system can have multiple ABE chains for independent sets of access policies. For example, two ABE chains are managed by two fish communities, and SFM is the DC of these two ABE chains. This implies that the two communities can manage their DSs/DCs separately. The system can also have multiple IoT chains for extensive data storage.

B. Fish Provenance and IoT Tracking

1) Fish Provenance: During fishing, fishers took fishing photos using the developed Fisher App and linked the photos with the fish by reading the NFC tags containing the *fish ID*. The hash values of the fishing photos, catch time, catch location, and other provenance data were securely stored in the IoT chain where the time and location were automatically identified by the Fisher App.

The Consumer App was developed to read the NFC tags and present the fish provenance and tracking information, as shown in Fig. 4. The Blockchain-certified catch date and area, and the certificates, such as the block hash and the transaction hash, were determined after the provenance data had been accepted by the IoT chain, as given on the bottom of Fig. 4(a).

[3]https://github.com/JHUISI/charm



(a) Provenance info. (b) Tracking map.

Fig. 4. The snapper provenance proof and tracking info.

According to the tracking map shown in Fig. 4(b), the scanned box of snappers was first caught to the northeast of the coast, then collected in the local city, and finally delivered to SFM with one-stop.

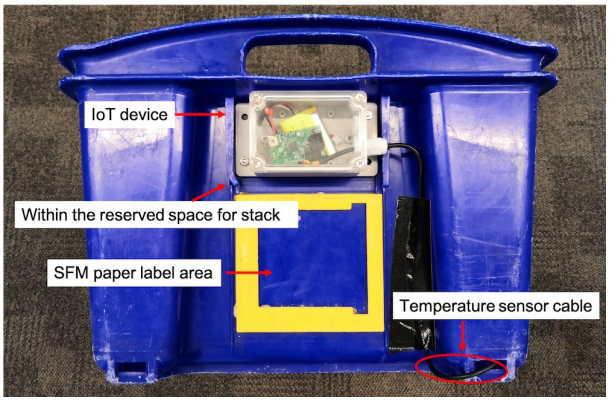
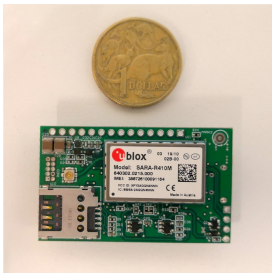
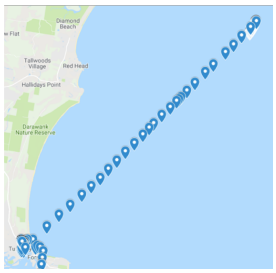


Fig. 5. A fish box with an NB-IoT device.

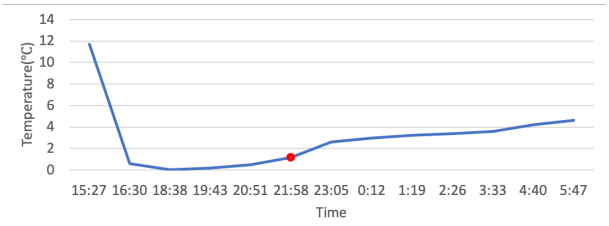
2) IoT-based Tracking: The PCB board of the developed NB-IoT embedded device (50mm*30mm), as shown in Fig. 6(a), was designed to equip with an NB-IoT module (SARA-R410M-02B, UBLOX) and integrate environmental sensors (BME680, BOSCH) and a GPS sensor (EVA-8M, UBLOX) to provide real-time location and time measurements of the fish boxes. The IoT embedded device, together with the GPS sensor and a battery, were packed in a water-resistant (IP68) case, as shown in Fig. 5. The IoT device was mounted to the outside of the box within the reserved space and therefore did not block the boxes from stacking up. An external temperature sensor (DS18B20, Maxim Integrated) was assembled inside of the box and wired to the IoT device through the drain hole.

NB-IoT devices were attached to fish boxes to track fish location and temperature along the whole fish supply chain from fishing spots to SFM. NB-IoT devices were linked to the *fish IDs* of fish boxes, which were used to carry fish from offshore fishing spots to SFM, during installation. NB-IoT devices were configured to periodically wake up and get fish provenance and quality tracking data, including accurate locations from the GPS module and temperature from the





(a) An IoT device under a coin. (b) Offshore location tracking.



(c) Cool box temperature tracking results.

Fig. 6. IoT devices and tracking samples.

external temperature sensor. NB-IoT devices then transmitted the provenance and quality tracking data to IoT servers via the NB-IoT cellular network or cached the data in case of losing connection. The fish data were uploaded to the IoT chain by the IoT servers running the *encrypting and publishing message* protocol (i.e., ***EnAndPub*** in Algo. 2) and later read by authorised DCs. Fig. 6(b) shows GPS coordinates of an offshore fishing trip, which are used as the provenance proof of the caught snappers caught during the fishing trip. The coordinates are from an NB-IoT device subscribing to the Telstra[4] NB-IoT service. The farthest location is 12 km offshore, indicating that the Telstra NB-IoT network covers offshore fishing spots. The temperature tracking results of the box of snappers are shown in Fig. 6(c). The NB-IoT device can precisely capture the fish temperature, without the impact of board temperature, from being caught at 16:30 to auction at 5:47 the next day. The red dot is a piece of temperature record cached by the buffering scheme. We can see from the figure that the box of snappers are well chilled such that the fish quality is preserved.

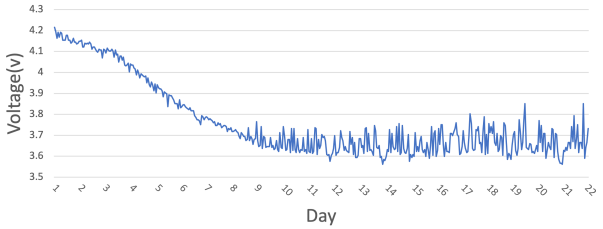


Fig. 7. Power consumption of the NB-IoT device.

We also tested the battery life of the developed NB-IoT devices. An NB-IoT device was powered with a 604560 LiPo battery (3.7 V and 2200 mAh) and tested at room temperature.

[4]The largest wireless carrier in Australia.

The NB-IoT device was configured to wake up after one hour of sleep. During the active period, the NB-IoT device searched for GPS signals from cold-start with a three-minute timeout, read metadata (i.e., location coordinators, temperature and battery voltage), searched for NB-IoT network services with a one-minute timeout and transmitted data to an IoT server using the User Datagram Protocol (UDP). The electricity was mainly consumed by the GPS sensor and the radio module. According to the specification [38], the power consumption of the GPS sensor is 16mA on the continuous mode. The power consumption of the NB-IoT module is 8 μA on the power save mode, 2 mA on the active idle mode, and up to 140 mA on the LTE Cat NB1 connected mode [39]. The battery voltage was used to evaluate the battery. As shown in Fig. 7, the NB-IoT device had sent 457 pieces of records through 21 days before the battery ran out. The sleeping time can be tuned according to the requirements on the battery life and sampling rate. For example, the sleeping time can be configured to be 20 minutes for temperature-sensitive seafood, under which the battery life would be one week and can support end-to-end tracking.

It is possible to implement a simplified *encrypting and publishing message* protocol on NB-IoT devices if the end-to-end data trustworthiness is preferred to the battery life. To this end, the key registration, i.e., Steps 1 – 3 in Algo. 2, can be done by IoT managers, while NB-IoT devices only need to interact with the IoT chain, i.e., Steps 4 and 5 in Algo. 2. The NB-IoT devices do not need to run heavy Blockchain consensus protocols nor store chain data. Before tracking, an NB-IoT device can be configured with a session encryption key $SK_{\mathbf{A},P}$ (used to encrypt tracking data), the transaction index $t_{i,j}$ (used to locate $\mathbb{CS}$) and a private key (used to sign transactions). For every piece of tracking record, the NB-IoT device needs to encrypt the tracking record with $SK_{\mathbf{A},P}$ and sign the transaction containing the encrypted record. These cryptographic operations are too heavy for our current NB-IoT devices but can be carried out with extra cryptographic chips [40]. It is worth noting that transaction control fields, e.g., Blockchain addresses and signatures, increase the transmission overhead of the IoT devices and thus raise the power consumption of the transmission.

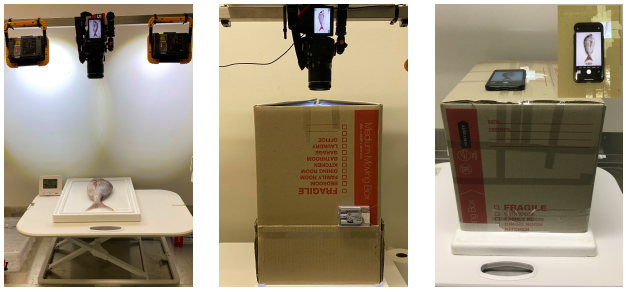
C. Fish Quality Measurement

A joint lab was set up at SFM for the image processing and E-nose modules, as shown in Fig. 8. In the lab, a comprehensive benchmark dataset was built up with rich quality annotations, provided by SFM Quality Assurance (QA) experts, for training and testing the models.

1) Image Processing: The realised workbenches are shown in Fig. 9 and can simulate different lighting conditions. The lighting box in Figs. 9(b) and 9(c) can achieve perfect lighting condition and compatible with different cameras.

In the fish size measurement, two types of rulers were designed: a) a chessboard with known size on the bottom of the fish box; b) a rectangle mark on the box bottom. The fish size measurement model consists of ruler detection and fish detection. The ruler detection algorithm detects the rulers and measures their lengths in image pixels for the pixel-length ratio. Then, the fish detection algorithm detects the fish and its pixel length through four components, i.e., image perspective correction, coarse fish detection, fine-grained fish segmentation, and fish principal orientation detection. Finally, the fish length can be calculated. In the trial, an image benchmark with 700 images was collected on 34 snappers with sizes ranging from 29.7 cm to 38 cm. The two cases achieved mean absolute errors 0.5 cm and 0.97 cm, respectively.

Fig. 8. Workbench for image processing and E-nose.



(a) Open lighting. (b) Lighting box. (c) Mobile camera.

Fig. 9. Image capturing workbenches.

In the fish freshness identification, the algorithm analysed five key appearance features, i.e., skin colour, skin spots, skin scale, eye form and eye pupils. The algorithm first divided the fish image into the eye part and the skin part. Then, the freshness regression algorithm, which is based on EfficientNet [41], measured the fish freshness. A high-quality and large-scale image dataset was created to train the algorithm, which consists of 9K images and 2K videos of 41 snappers using open lighting. SFM QA experts also annotated the freshness of fish at three levels: 0, 1 and 2 (score 0 means the freshest, whereas 2 means the least fresh but still eatable). To fine-tune the algorithm for mobile camera, a small dataset of 20 fish was collected, as shown in Fig. 9(c). We conducted 30 rounds of cross-validation testing on the dataset to evaluate the model accuracy. In every round, images of a randomly chosen majority fish were used for training, while data from the remaining fish were used for testing. F1 scores were calculated for three freshness levels to evaluate the model's performance on different freshness levels. The final accuracy results were obtained by averaging these 30 test results, as given in Table IV. The overall freshness identification accuracy is 86.1% for the open lighting and 93.6% for the lighting box. The stable lighting condition provided by the lighting box can greatly improve the model accuracy for all freshness levels.

TABLE IV: Freshness identification accuracy.

	Freshness 0	Freshness 1	Freshness 2	Overall
Open lighting	0.874	0.795	0.909	0.861
Lighting box	0.956	0.918	0.925	0.936

2) E-nose: We developed the E-nose module and deployed it in the joint lab. The laptop ran the quality measurement model, as shown in Fig. 8. The E-nose module was tested on snappers for twelve days, and the snappers were stored in the cool room from 0 °C to 4 °C after they had been caught. Every single day, the snappers were tested on the E-nose module five times, where every single test took eight minutes, allowing the E-nose devices to capture enough odour molecules. The snappers were also manually assessed by the QA experts for the reference purpose. The numerical quality indices were compared by calculating the log-likelihood. The experiment results are shown by a box plot in Fig. 10, where the y-axis gives the log-likelihood calculated with the forward-backward algorithm, and the x-axis gives the icedays. We paid particular attention to the period from the fourth day to the eighth day when the fish were hard to be assessed. The quality indices from E-nose match the manual results which are provided by QA experts and under the boxes in the figure. In the case that snappers are freshest, i.e., score zero, the quality indices from E-nose are consistent and close to the manual indices, especially in the first four days.

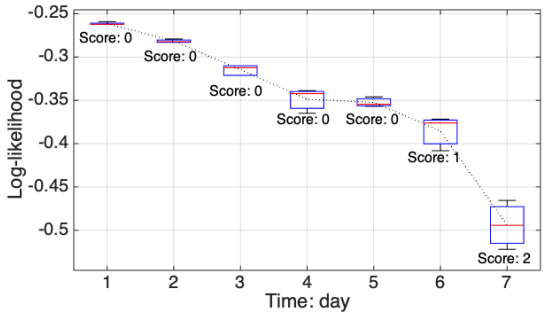


Fig. 10. The likelihood of the E-nose quality model [42].

VII. Conclusion

In this paper, we presented the BeFAQT system, where IoT, AI, image processing and E-nose technologies were employed for real-time tracking of fish origin proof and quality information. A multi-layer Blockchain system was developed to ensure the trustworthiness of the provenance and tracking data, where the ABE chain provided access control to the data stored in the IoT chain based on the ABE scheme. Verified by the trial on a local snapper supply chain, the BeFAQT system was proved to be able to connect fishers and Co-Ops with SFM and consumers to provide trusted fish tracking and quality information in real-time.

Acknowledgment

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

References

[1] "The state of world fisheries and aquaculture 2018 - meeting the sustainable development goals," *Food and Agriculture Organization of the United Nations, Rome. Licence: CC BY-NC-SA 3.0 IGO*, 2018.

[2] B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, and M. Peng, "When internet of things meets blockchain: Challenges in distributed consensus," *IEEE Network*, vol. 33, no. 6, pp. 133–139, 2019.

[3] Sawtooth, "FishNet." [Online]. Available: https://demo.bitwise.io/fish/#!/

[4] WWF, "How blockchain & a smartphone can stamp out illegal fishing and slavery in the tuna industry." [Online]. Available: https://www.wwf.org.au/news/news/2018

[5] Provenance, "From shore to plate: Tracking tuna on the blockchain." [Online]. Available: https://www.provenance.org/tracking-tuna-on-the-blockchain

[6] E. Androulaki, A. Barger *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the 13th EuroSys Conference*. ACM, 2018, p. 30.

[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE Symposium on Security and Privacy (SP '07)*, May 2007, pp. 321–334.

[8] G. Yu, X. Zha, X. Wang, W. Ni *et al.*, "Enabling attribute revocation for fine-grained access control in blockchain-iot systems," *IEEE Transactions on Engineering Management*, pp. 1–18, 2020.

[9] Y. Rahulamathavan, R. C. . Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based iot ecosystem using attribute-based encryption," in *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2017, pp. 1–6.

[10] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38 437–38 450, 2018.

[11] Y. Cao *et al.*, "Efficient traceability systems of steel products using blockchain-based industrial internet of things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6004–6012, 2020.

[12] N. Sengar, V. Gupta, M. K. Dutta, and C. M. Travieso, "Image processing based method for identification of fish freshness using skin tissue," in *2018 4th International Conference on Computational Intelligence & Communication Technology (CICT)*. IEEE, 2018, pp. 1–4.

[13] R. Jarmin *et al.*, "A comparison on fish freshness determination method," in *2012 International Conference on System Engineering and Technology (ICSET)*. IEEE, 2012, pp. 1–6.

[14] S. P. Mark Boulter and A. Bremner, "Australian Quality Index Manual." [Online]. Available: https://www.sydneyfishmarket.com.au/Portals/0/adam/Content/20WFSQ8OH0O3R6xnl1GrEg/ButtonLink/Australian\%20QI\%20Manual.pdf

[15] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for internet of things," *Computer Communications*, vol. 136, pp. 10 – 29, 2019.

[16] 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.

[17] D. Tse, B. Zhang, Y. Yang, C. Cheng, and H. Mu, "Blockchain application in food supply information security," in *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, Dec 2017, pp. 1357–1361.

[18] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing secure lightweight blockchain-enabled rfid-based authentication protocol for supply chains in 5g mobile edge computing environment," *IEEE Trans. Ind. Informat.*, pp. 1–1, 2019.

[19] H. Fabric, "Private data." [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/private-data/private-data.html

[20] C. K. Adiputra, R. Hjort, and H. Sato, "A proposal of blockchain-based electronic voting system," in *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*. IEEE, 2018, pp. 22–27.

[21] G. Ateniese and B. de Medeiros, "On the key exposure problem in chameleon hashes," in *Security in Communication Networks*, C. Blundo and S. Cimato, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 165–179.

[22] N. Zhang and Y. Liu, "NB-IoT drives intelligent cold chain for best application," in *2019 IEEE 9th International Conf. Electronics Information and Emergency Communication (ICEIEC)*, July 2019, pp. 1–4.

[23] Telstra, "Telstra iot network coverage." [Online]. Available: https://www.telstra.com.au/business-enterprise/solutions/internet-of-things/iot-coverage
[24] A. D. Wilson and M. Baietto, "Applications and advances in electronic-nose technologies," *Sensors*, vol. 9, no. 7, pp. 5099–5148, Jun. 2009.
[25] M. Peris and L. Escuder-Gilabert, "A $21st$ century technique for food control: Electronic noses," *Analytica chimica acta*, vol. 638, no. 1, pp. 1–15, Apr. 2009.
[26] J. W. Gardner and P. N. Bartlett, *Electronic noses: principles and applications*. Oxford university press New York, 1999, vol. 233.
[27] T. C. Pearce, S. S. Schiffman *et al.*, *Handbook of machine olfaction: electronic nose technology*. John Wiley & Sons, 2006.
[28] S. Yang, L. Bo *et al.*, "Unsupervised template learning for fine-grained object recognition," in *Advances in Neural Information Processing Systems 25*. Curran Associates, Inc., 2012, pp. 3122–3130.
[29] N. DPI, "FishSmart." [Online]. Available: https://www.dpi.nsw.gov.au/fishing/recreational/resources/fishsmart-app
[30] W. Zhang, T. Liu *et al.*, "A novel data pre-processing method for odour detection and identification system," *Sensors and Actuators A: Physical*, vol. 287, pp. 113 – 120, 2019.
[31] T. Liu, W. Zhang *et al.*, "A novel multi-odour identification by electronic nose using non-parametric modelling-based feature extraction and time-series classification," *Sensors and Actuators B: Chemical*, vol. 298, p. 126690, 2019.
[32] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, 2014.
[33] M. Castro, B. Liskov *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, no. 1999, 1999, pp. 173–186.
[34] B. Cao, Z. Zhang, D. Feng, S. Zhang, L. Zhang, M. Peng, and Y. Li, "Performance analysis and comparison of pow, pos and dag based blockchains," *Digital Communications and Networks*, vol. 6, no. 4, pp. 480–485, 2020.
[35] X. Wang, P. Yu, G. Yu, X. Zha, W. Ni, R. P. Liu, and Y. J. Guo, "A high-performance hybrid blockchain system for traceable iot applications," in *Network and System Security*, J. K. Liu and X. Huang, Eds. Cham: Springer International Publishing, 2019, pp. 721–728.
[36] Y. Li, B. Cao, M. Peng, L. Zhang, L. Zhang, D. Feng, and J. Yu, "Direct acyclic graph-based ledger for internet of things: Performance and security analysis," *IEEE/ACM Transactions on Networking*, vol. 28, no. 4, pp. 1643–1656, 2020.
[37] Y. Chen, H. Li, K. Li, and J. Zhang, "An improved p2p file system scheme based on ipfs and blockchain," in *2017 IEEE International Conference on Big Data (Big Data)*, 2017, pp. 2652–2657.
[38] u blox, "EVA-8M SiP." [Online]. Available: https://www.u-blox.com/sites/default/files/EVA-8M_ProductSummary_\%28UBX-16007668\%29.pdf
[39] ——, "SARA-R4 (x2B) series." [Online]. Available: https://www.u-blox.com/sites/default/files/SARA-R4-x2B_ProductSummary_\%28UBX-16019228\%29.pdf
[40] S. S. Dhanda, B. Singh, and P. Jindal, "Lightweight cryptography: A solution to secure iot," *Wireless Personal Communications*, vol. 112, no. 3, pp. 1947–1980, 2020.
[41] M. Tan and Q. V. Le, "Efficientnet: Rethinking model scaling for convolutional neural networks," *ICML*, 2019.
[42] T. Liu, W. Zhang, M. Yuwono, M. Zhang, M. Ueland, S. L. Forbes, and S. W. Su, "A data-driven meat freshness monitoring and evaluation method using rapid centroid estimation and hidden markov models," *Sensors and Actuators B: Chemical*, vol. 311, p. 127868, 2020.