



BLOCKCHAIN: TRANSFORMING THE SEAFOOD SUPPLY CHAIN

Bubba Cook
Western and Central Pacific Tuna Programme Manager
WWF-New Zealand
acook@wwf.org.nz



EXECUTIVE SUMMARY

Seafood traceability is increasingly becoming a focal point to address the entry of illegally and unethically produced products into the supply chain. More and more, experts view full supply chain traceability and transparency as the only way to ensure against the continued entry of illegally or unethically produced seafood products into the seafood supply chain. Blockchain can be a significant part of the solution – providing the full transparency and traceability required to enable the market to reward responsible and ethical producers, and push those that are illegal and unethical out of the supply chain. By providing this transparency and traceability, it can enable the market to both reward producers who engage in best practices, and exclude illegal and unethical producers. This report describes a WWF-led pilot to prove blockchain supply chain traceability for use in seafood traceability, specifically for tuna caught in a Fijian longline fishery. The purpose of the report is to provide a description of the work undertaken, to offer lessons learned, and to provide a potential roadmap for others who wish to develop blockchain supply chain solutions.

TABLE OF CONTENTS

Introduction	5
<i>What's the problem that blockchain aims to solve?.....</i>	<i>5</i>
<i>Traceability</i>	<i>6</i>
What is Blockchain?	8
<i>Data Access</i>	<i>11</i>
<i>Public Blockchain</i>	<i>11</i>
<i>Consortium Blockchain</i>	<i>12</i>
<i>Private Blockchain.....</i>	<i>12</i>
<i>Asset Ownership Permissions.....</i>	<i>12</i>
<i>Blockchain for Supply Chains.....</i>	<i>12</i>
<i>Do You Need Blockchain?</i>	<i>13</i>
The WWF Pilot Project – Fiji Tuna Supply Chain Solution	14
<i>Viant.....</i>	<i>14</i>
<i>Modeler.....</i>	<i>15</i>
<i>Smart Builder</i>	<i>16</i>
<i>Tracker</i>	<i>16</i>
<i>Pilot Project Phase I: Proof of Concept.....</i>	<i>17</i>
<i>How It Works.....</i>	<i>17</i>
<i>Integrating with Existing Platforms.....</i>	<i>17</i>
<i>Supply Chain Mapping</i>	<i>18</i>
<i>Accounting for Every Fish.....</i>	<i>19</i>
<i>Landing and Processing</i>	<i>21</i>
<i>Distribution and Retail.....</i>	<i>22</i>
<i>Proving the Technology</i>	<i>23</i>
<i>Pilot Project Phase II: Expansion and Payments.....</i>	<i>23</i>
<i>Challenges.....</i>	<i>23</i>
<i>Reliance on paper-based processes.....</i>	<i>23</i>
<i>Availability of Local Suppliers and Technicians.....</i>	<i>24</i>
<i>Mapping the Supply Chain Past the Importer</i>	<i>24</i>
<i>Cooperation of Downstream Supply Chain Actors</i>	<i>24</i>
<i>Authenticity of Data.....</i>	<i>24</i>
Conclusion and Recommendations	28
Contacts.....	30
Glossary.....	30

List of Figures

FIGURE 1: WHAT IS BLOCKCHAIN?	9
FIGURE 2: BLOCKCHAIN BASIC DESCRIPTION	9
FIGURE 3: ETHEREUM SMART CONTRACTS ILLUSTRATION	10
FIGURE 4: ETHEREUM BLOCKCHAIN	11
FIGURE 5: DO YOU REALLY NEED BLOCKCHAIN?	13
FIGURE 6: VIANT CONCEPTUAL MODEL	15
FIGURE 7: INTEGRATION OF VIANT AND TRASEABLE PLATFORMS	18
FIGURE 8: VIANT TUNA PROCESS FLOW DIAGRAM	19
FIGURE 9: AUGMENTED REALITY FACILITATED BY BLOCKCHAIN AND NFC	22

List of Images

IMAGE 1: TAGGING A FISH	20
IMAGE 2: TAGGED TUNA ABOARD A FISHING VESSEL	20
IMAGE 3: TAGGED FISH ENTERING A PROCESSING FACILITY	21
IMAGE 4: SASHIMI AND QR CODE	22

List of Tables

TABLE 1: BASIC COSTS	27
----------------------	----



Blockchain: Transforming Seafood Supply Chain Traceability

Introduction

The purpose of this report is to share the knowledge and experience that WWF has gained working with Blockchain technology to improve the traceability of seafood.

This report has three parts. First, we explain what Blockchain is; second, we describe a pilot implementation of Blockchain for the Tuna longline fishery in Fiji which helps to show how Blockchain works, and the potential benefits, challenges and costs; and third, we make some key recommendations for those keen to start working with, and benefiting from, blockchain technology.

What's the problem that blockchain aims to solve?

Seafood is a truly global commodity. A fish caught in one part of the globe might change hands dozens of times and undergo multiple forms of processing and packaging before reaching its ultimate destination – or destinations – thousands of miles away. As a result, seafood supply chains are often opaque and complex. Information is maintained in silos by separate supply chain actors in such a way that it is virtually impossible to fully or effectively trace a seafood product from its origin to its ultimate fate. This obscured supply chain ecosystem allows some actors to access and exploit those supply chains without being subject to recognised legal and ethical standards.

Over the last five years, increasing international media coverage has highlighted evidence of human rights violations as well as other illegal and unethical practices in various fisheries across the globe. Analyses and associated media have highlighted Illegal,

Unreported, and Unregulated (IUU) activities, including overfishing, human rights abuses, and fraud in the global seafood industry.¹ The most recent assessments indicate that up to US\$23 billion of global fisheries value is lost to IUU.² In 2013, a study conducted by Oceana in the US found that up to 59 per cent of tuna samples were mislabelled.³ Most recently, a 2018 report from Greenpeace, “*Misery at Sea*”, highlighted some of the documented human rights abuses in fisheries.⁴ As a result, the global seafood industry faces unprecedented criticism and declining trust among consumers.

At the same time, companies practicing environmental and social responsibility are often not fully recognised for their efforts. People can often paint industry leaders with sustainable practices and fair labour standards with the same broad brush as the illegal and unethical producers. Additionally, in an effort to reduce brand and reputation risk, end markets are seeking mechanisms to ensure that they do not source from supply chains engaged in illegal or unethical practices. At its core, markets, and increasingly consumers, are simply seeking to purchase from supply chains that they can *trust*.

Fully transparent and traceable seafood supply chains, facilitated by the blockchain technology, could potentially solve the problem of IUU fishing in supply chains. Blockchain technology’s inherent transparency and traceability could effectively eliminate illegal or unethical seafood from the supply chain. It would achieve this unprecedented outcome by empowering seafood buyers and consumers to make well-informed commercial choices based on verifiable information. It would also provide an effective platform for regulatory authorities to identify and address potential risks.

Traceability

Seafood markets and the seafood industry have been seeking improved traceability for decades. While the term “traceability” can be somewhat ambiguous, it is essentially a system of records designed to track the flow of a product through the production process or supply chain.⁵ The seafood industry, regulatory authorities, and non-government organisations (NGOs) have developed and implemented several initiatives and systems designed to achieve product traceability. Those efforts have resulted in a variety of systems designed to achieve everything from supply chain efficiency to provenance and attribute verification.

¹ See e.g. Urbina, Ian. “The Outlaw Ocean.” The New York Times. July 25, 2015. *retrievable at* <https://www.nytimes.com/interactive/2015/07/24/world/the-outlaw-ocean.html>; McDowell, Robin, Margie Mason, and Martha Mendoza. “Slaves may have caught the fish you bought.” Associated Press. March 25, 2015. *retrievable at* <https://www.ap.org/explore/seafood-from-slaves/ap-investigation-slaves-may-have-caught-the-fish-you-bought.html>.

² Zabarenko, Deborah. “Fish piracy costs \$10 billion to \$23 billion a year.” Reuters. May 8, 2013. *retrievable at* <https://www.reuters.com/article/us-piracy-fish/fish-piracy-costs-10-billion-to-23-billion-a-year-report-idUSBRE94703R20130508>.

³ Mims, Christopher. “59% of the 'Tuna' Americans Eat Is Not Tuna.” The Atlantic. February 22, 2013. *retrievable at* <https://www.theatlantic.com/business/archive/2013/02/59-of-the-tuna-americans-eat-is-not-tuna/273410/>.

⁴ Greenpeace. “Misery at sea: human suffering in Taiwan’s distant water fishing fleets.” May 24, 2018. *retrievable at* <https://www.greenpeace.org/new-zealand/publication/misery-at-sea/>.

⁵ Future of Fish. “Traceability 101.” August 8, 2018. *retrievable at* <http://futureoffish.org/content/traceability-101>.

In an effort to clarify traceability roles and responsibilities, a recent joint industry and NGO initiative, the Global Dialogue on Seafood Traceability (GDST), recently embarked on an effort to develop standards and definitions around securing seafood supply chain traceability. This initiative includes some of the largest seafood firms on the planet. They collectively acknowledge that reliable data, that is secure and easily shared through interoperable traceability systems, is vital to the future of the seafood industry. The GDST also acknowledges that traceability systems can benefit the entire seafood ecosystem, from a production, marketing, and value chain management perspective. The benefits include:

- protection of public health;
- improved trade;
- strengthened sustainability practices;
- premium for sustainable produce;
- reduced recall scope;
- increased consumer trust;
- quality assurance and value-chain efficiencies;
- reduction of brand risk arising from association with unacceptable labour practices; and
- better regulatory compliance.

Anyone who has spent much time working in the fishing industry knows how reluctant, if not resistant this sector can be to change. However, it is past time for the seafood industry to embrace a digital revolution in supply chain management. With about 90 percent of fish stocks either fully fished or overfished,⁶ there is simply no room for an increase in volume to support further profitability within the system. For this reason, any economic gains must come from improvements in the overall *value* of the fisheries. While value increases can be secured through several means, it will inevitably require improvements in supply chain efficiencies that will only be secured through full traceability.

Efforts toward effective electronic supply chain traceability are not new. Several entities have developed electronic traceability systems designed to capture key data at various points in the supply chain that are designed to provide varying levels of traceability. These range from private companies such as [Trace Register](#)⁷, a seafood traceability firm based in Seattle, Washington, to the NGO Ecotrust's [ThisFish](#)⁸ initiative. Each of these systems offers full supply chain traceability. However, in each of these systems or services, they depend on a centralised system and implicit trust in the managing authority for the data and verification provided. This is where the recent innovation of blockchain would provide substantial improvement by offering not only secure traceability, but inherent trust. To explain how, we must first understand what Blockchain is.

⁶ Ramsden, Neil. "FAO: State of world fisheries declining." Undercurrent News. July 10, 2018. *retrievable at* <https://www.undercurrentnews.com/2018/07/10/fao-state-of-worlds-fisheries-is-declining/>.

⁷ See <https://www.traceregister.com/>

⁸ See <http://thisfish.info/>



Blockchain

What is Blockchain?

Blockchain is often referred to as the “next evolution of the internet” and the Economist justifiably referred to it as “the trust machine.” Essentially, Blockchain is simply an incorruptible, distributed digital ledger of transactions, which allows users to more effectively measure, record and transact value.

Blockchain can be described as a technology that increases trust and transparency in a system by storing all transactions in a decentralized manner. Everyone in the system can check those transactions and verify their accuracy. Additionally, cryptographic and game-theoretic mechanisms ensure data immutability and consistency. Because adding all the transactions one by one would take too much time, blockchain groups and verifies before being added to the blockchain.

What is a blockchain ?



Originally conceived as the underlying protocol of Bitcoin, blockchain technology has since evolved to support a number of applications with the introduction of “smart contracts” in Ethereum.

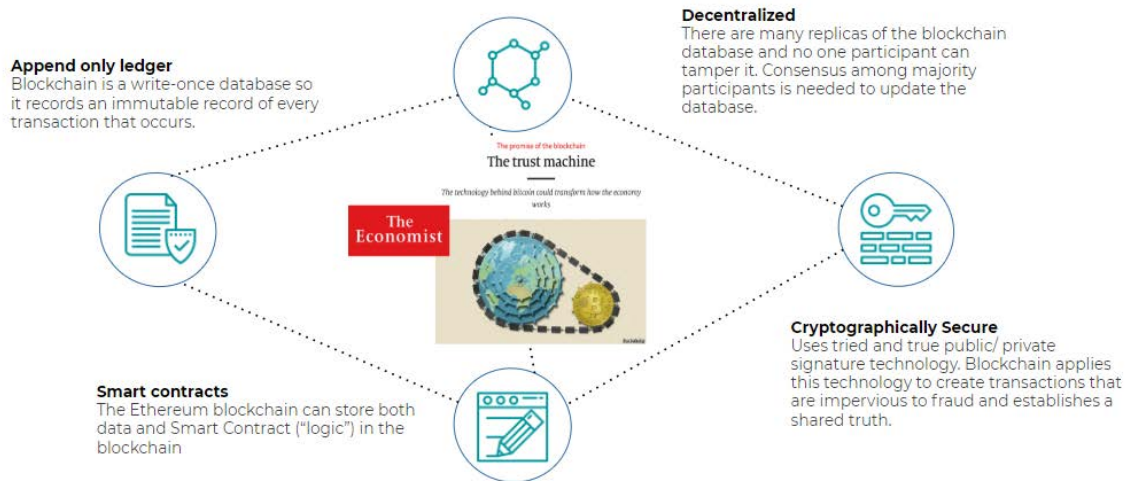


Figure 1: What is Blockchain?

A “transaction” can involve contracts, records, currency or almost any other information of value. Through a series of cryptographically secure algorithms, multiple blockchain nodes (individual computers connected to the internet) validate the transaction in a process known as “consensus protocol.” That transaction is combined in a block of data, which forms a chain of records maintained simultaneously across thousands of distributed nodes, hence forming a “blockchain”, that is permanent and unalterable.

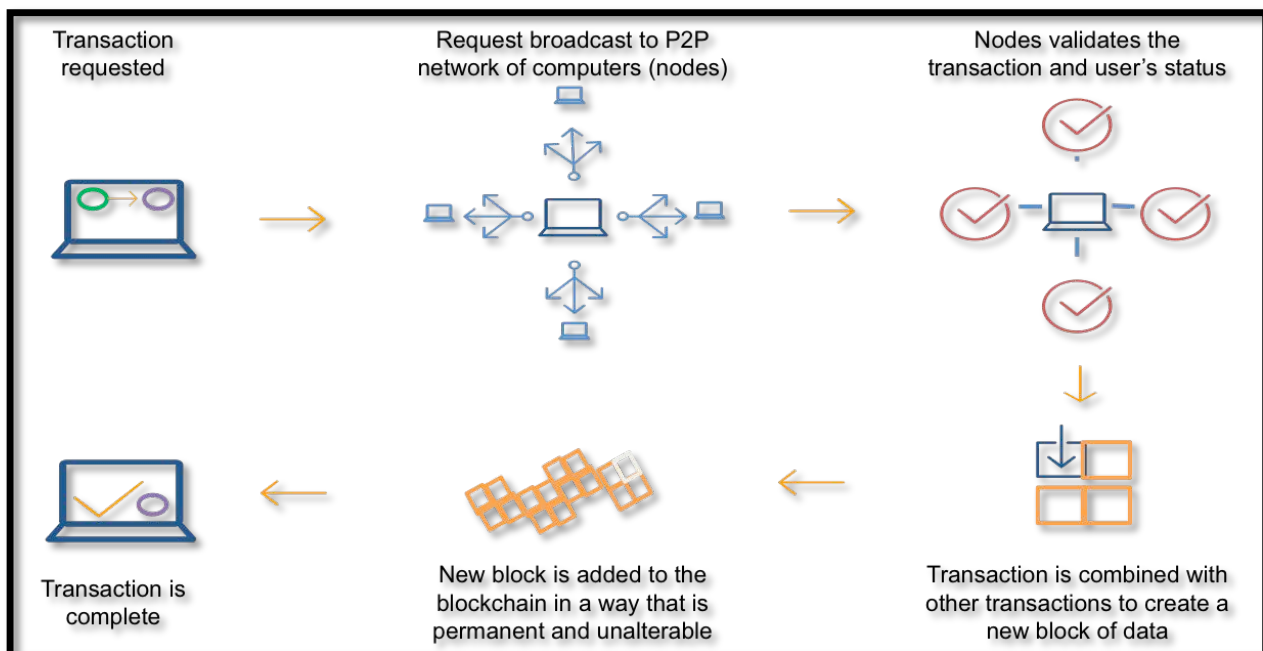


Figure 2: Blockchain Basic Description

Another way to think of blockchain is in relation to the popular online word processing app Google Docs. Before Google Docs (and similar online apps), if you wanted to collaborate on a piece of writing with someone online you had to create a document with a programme on your computer (such as Microsoft Word), send it to them, and then ask them to edit it. Then you had to wait until they made those changes, saved the document, and sent it back to you. Google Docs fixed that by making it possible for multiple people

to view and edit a document at the same time. However, most databases today still work like Microsoft Word: only one person can make changes at a time, locking everyone else out until they're done. Blockchain remedies that by instantly updating any changes to the database for everyone to see, with the added benefit of creating a permanent, append-only record of those changes.

Different blockchains exist such as Ethereum and Hyperledger, but Bitcoin was the first and provided the foundation for which Ethereum was built. At its simplest, Ethereum is an open software platform based on blockchain technology. The entire Ethereum network is a decentralized global collection of computers, or nodes, connected to one another through a shared set of rules known as consensus protocol. All the transactions that have happened and will ever happen in this network are automatically updated and recorded in an open and distributed ledger. Ethereum blockchain is not just a distributed ledger (e.g. record of all transactions), but is a Turing complete virtual machine, which means it theoretically can calculate anything assuming enough memory is available. This feature makes it possible for Ethereum to run smart contract scripts that are collectively attested to by thousands of computers around the globe.

A smart contract is comprised of both an agreement and its execution. Like any legal contract, it consists of the standard components of an *offer*, *acceptance* of that offer, and some form of exchange of consideration (some legal obligation that each party must take on) that must be bargained for between the parties. Smart contracts are a series of instructions, written in the programming language Solidity, which use boolean logic. Smart contracts allow programmers to create code that binds two parties to an agreement, without the need for an intermediary. The output of these agreements, and the code itself, cannot be altered on the blockchain; they are time-stamped, auditable, and immutable. All nodes (computers linked to the Blockchain network) know what other nodes should hold as truth at any given time. Together, they create a new type of security: *consensus*.

Blockchain 2.0 | Ethereum
A smart contract illustration

Conditions:

- If Alice's flight is delayed for more than 5 hours
- If Alice's flight is cancelled

Result:

- Alice will receive 1.5x insurance premium

```
if (alice.flight.delay > 5 or alice.flight == cancelled) =>
then {
  alice.refund = alice.premium * 1.5
  insurer.balance = insure.balance - alice.refund
  alice.balance = alice.balance + alice.refund
}
```

Figure 3: Ethereum Smart Contracts Illustration

As a result of this consensus mechanism, Ethereum presents additional opportunities with respect to transactions such as negotiating an economic agreement or a future transaction. The advantages presented by the immutable decentralized record provided by Ethereum will almost certainly prove useful in other contexts as well. Experts believe that as the Internet commoditized the cost for communication, Ethereum is commoditizing the costs of agreement and trust.⁹

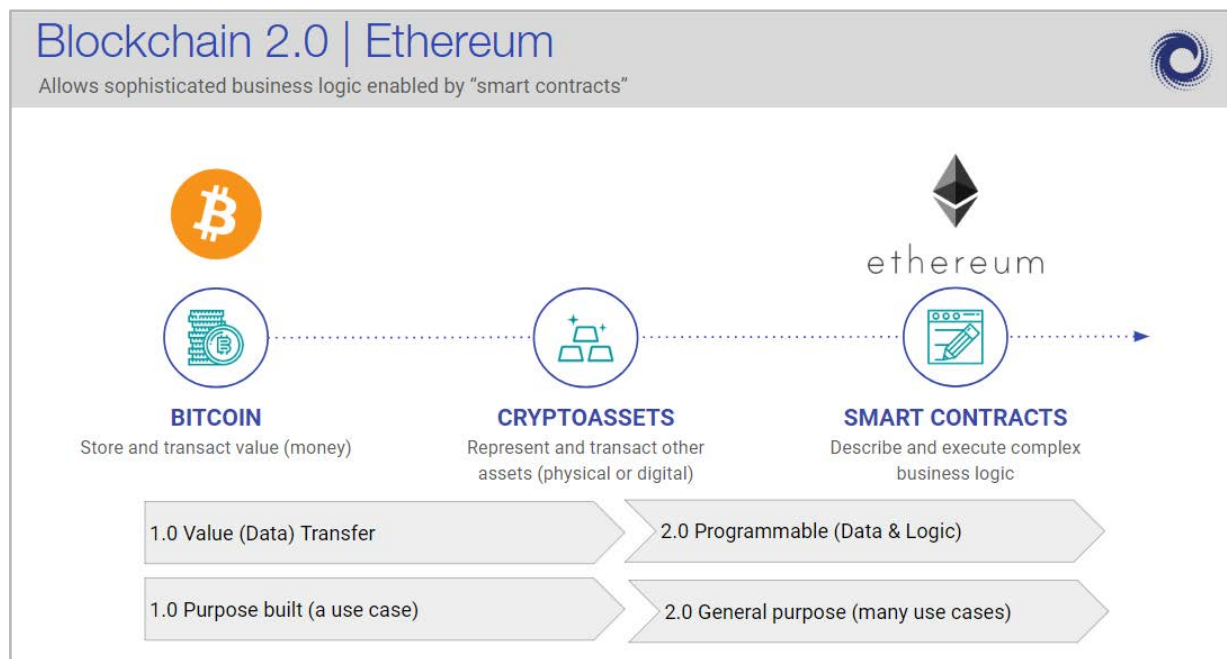


Figure 4: Ethereum Blockchain

Data Access

While complete transparency of transactions represents the gold standard for conducting supply chain transactions, there is often certain information that participants desire to keep private or otherwise concealed.

One way to control who can see data on the blockchain involves permissioning based on the type of blockchain that is used which are typically bucketed into either public or private blockchains. Another way to control who can access data on a blockchain is through asset ownership permissions. This section summarises each.

Public Blockchain

A public blockchain has no access restrictions, allowing anyone with an internet connection to participate in or validate transactions as part of the consensus protocol by, for example, reading and writing to an append only database.

⁹ Cretin, Andrew. "It's 2018 — Blockchain is on its way to Become the New Internet." Medium. January 4, 2018. retrievable at <https://medium.com/@andrewcretin/its-2018-blockchain-is-on-it-s-way-to-become-the-new-internet-7055ed6851ec>.

Consortium Blockchain

A “consortium” or “federated” blockchain is a quasi-private blockchain that is permissioned so that a number of companies might each operate a node on the network and share in its administration and governance. The administrators of a consortium blockchain may restrict users’ participation rights.

Private Blockchain

A private blockchain is permissioned such that a participant cannot join unless invited by the network administrators, thereby restricting participant and validator access. In form and function, it is very similar to a centralised database.

Asset Ownership Permissions

There is another way to address access to information that is not as blunt a tool as establishing a consortium or private blockchain. Instead, you can set permissions at the asset ownership level as we did in the pilot study described in this report.

To address data access concerns during trials of the tuna project, Viant implemented a discrete asset ownership system where each asset could be assigned to an entity and that entity could turn on or turn off certain input fields depending on the stage of the process and who will be viewing the record. So, from the application end of the user interface, both Viant and TraSeable developed access restrictions based on assigned roles or users.

Under this scenario, the data would remain visible on a public blockchain or to all parties in a consortium, but it would be hashed and somewhat meaningless to anyone reviewing it without knowing who the users involved in the transaction are and what the data specifically pertains to.

Blockchain for Supply Chains


Blockchain experts recently identified supply chain traceability as a top use case for blockchain technology in part because it enables a single source of truth for traceability of any product from producer to consumer.¹⁰ Additionally, blockchain offers to reduce transaction costs and friction for supply chain actors through the use of smart contracts, allowing for instantaneous execution of payments and other transactional arrangements. Furthermore, blockchain potentially enables the removal of unethically or illegally sourced products by allowing improved targeted market leverage through informed purchasing. In short, it has the potential to rewrite the rules for the sustainable and ethical production and consumption of any commodity, including seafood products, on a global scale.

¹⁰ Vilner, Yoav. “5 Blockchain Product Use Cases To Follow This Year.” Forbes. June 27, 2018. retrievable at <https://www.forbes.com/sites/yoavvilner/2018/06/27/5-blockchain-product-use-cases-to-follow-this-year/#11fa9891b60b>.

Do You Need Blockchain?

Once you understand what blockchain is, the question becomes, “do you need it?” Viant created an easy assessment tool that can help you to realize if you really need blockchain or not.

If you answer ‘yes’ to the majority of the questions in Figure 5, you might consider exploring blockchain to unlock value within your business.



Do you really need blockchain?

1	2	3
Problem or Value identification	Stakeholder buy in	Technical considerations
<ol style="list-style-type: none">1. Is there a need to share information, credentials or value with others?2. Is trust a critical requirement to the process?3. Do you need to prove to others you are transacting/reporting accurately?4. Is there potential to monetize the data or digital asset in the value chain?5. Who owns the problem? Individual or industry wide challenge?	<ol style="list-style-type: none">1. Is there a network of stakeholders (i.e. more than 2?)2. Is there a dependency on others for information?3. Does more than one participant need to update the data?4. Is there scope to open up the ecosystem to ancillary parties in the future?5. Are you working with other industry players on any activities?	<ol style="list-style-type: none">1. Is there any ongoing need or future requirements for high data throughput?2. Do you rely or use public data sources to make decisions?3. Do you need to store a particularly rich/complex data structure?4. Do you need to digitise assets in your value chain?5. Do you need transaction privacy? Do you need anonymity?

Figure 5: Do you really need blockchain?



The WWF Pilot Project – Fiji Tuna Supply Chain Solution

Over the last year, World Wide Fund for Nature (WWF) engaged in a blockchain supply chain traceability project in the Fiji tuna fisheries. WWF partnered with [Viant](#)¹¹ – a [ConsenSys incubated company](#),¹² that built an asset and domain agnostic blockchain-based supply chain platform; [TraSeable Solutions](#),¹³ - a Fijian ICT provider specialising in blockchain; and [Sea Quest Fiji Ltd](#),¹⁴ - a progressive tuna longline fishing company operating out of Fiji. The goal of the project was to create a completely transparent and traceable supply chain, utilising innovative blockchain technology, for the fresh and frozen tuna supply chain.

Viant

[Ethereum](#)¹⁵ is one of the leading blockchain platforms. Essentially, Viant is a tool to make Ethereum more accessible and useful for supply chain asset tracking. Viant is a next-generation blockchain-based platform for modeling business processes, tracking assets, and building the transparent flexible supply chains of the future. Viant uses the Proof of Authority consensus mechanism, which is a type of algorithm by which a cryptocurrency blockchain network aims to achieve distributed consensus yet generally achieves greater performance and energy efficiency than

¹¹ See <https://viant.io/>.

¹² See <https://new.consensys.net/>.

¹³ See <https://traseable.com/>.

¹⁴ See <http://www.seaquestfiji.com/wp/>.

¹⁵ See <https://www.ethereum.org/>

original algorithms used in Bitcoin Proof of Work algorithms. The Ethereum platform leverages cryptographic security and smart contracts to provide organizations and users verifiable insights as assets are managed and propagated throughout their entire supply chain.

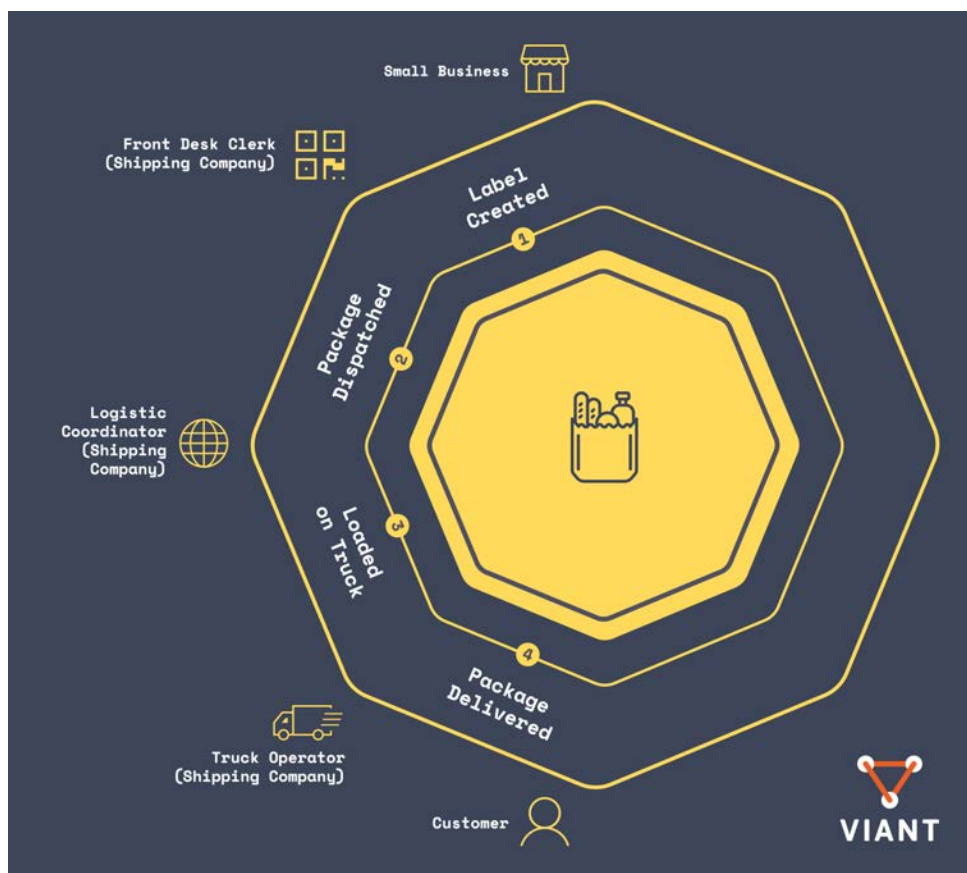


Figure 6: Viant Conceptual Model

Viant’s platform consists of three main core components: **Modeler**, **Smart Builder**, and **Tracker**.

Modeler

The Modeler allows a subject matter expert with no technical ability to log into the system, model a business process, define an asset and its attributes, and set permissions for each role and user in the network. This process can be shared, tested and edited ‘off-chain,’ meaning that it has not been deployed onto the blockchain. Once the process has been deployed and ‘turned on’ in the system, the business person or subject matter expert can define which assets to track, in our case, tuna. While defining the tuna asset you can assign various attributes that should be tracked throughout the process. In the tuna project, we chose to track: (1) weight; (2) unique RFID number; (3) species; (4) catch zone; (5) vessel; (6) crew details; and (7) catch details including several other attributes. Once the assets are defined and deployed onto the blockchain, the core foundation is set.

Smart Builder

The Smart Builder is responsible for auto-generating the smart contracts and the user interface of the end application. The smart building allows business users to build a supply chain application in minutes where it used to take us months.

With the click of one button, the previously modeled business process and asset are deployed on the blockchain. By removing the complexity of coding smart contracts and defining a user interface, this allows users to focus on their business rather than the technology.

The smart builder also holds the administrative functions such as tying roles, users, and permissions to the asset and process. A system administrator would be accountable for going into the smart builder and defining all of the roles that participate in this process. In the tuna scenario, roles include the Fisher, Regulator, Processor, Distributor/Retailer, and Consumer. Once roles are defined you can create users - specific individuals who would be provided a username and password to log in and participate in the process. Permissions are defined in this stage so that certain roles can perform actions while other actions are concealed.

Tracker

One may think of the Modeler and Smart Builder as the application creation tools and the Tracker as where the full production system comes together resulting in the end application. Once the application has been built using Viant – customers, manufacturers, and producers can log in to the application and create new assets, move assets along the defined workflow, and can search assets as they are being tracked along every node of the supply chain. This capability serves as a great way to loop in various stakeholders who want to see the provenance and journey of each asset.

Viant also has a Public View functionality as a unique way to share the journey of every asset without having login credentials. A QR code, RFID, or any sensor device can be assigned to an asset and, at any given time, an individual can scan the code with their smartphone and the entire journey of that asset will pop up on their phone - no application download or sign in needed. The public view demonstrates the journey step by step with exact timing of when the asset moved between actors, who did it, and a real-time map view of its journey.

Additionally, because it is expensive and typically not ideal to store large files on the blockchain, Viant uses InterPlanetary File System (IPFS) which is a distributed technology for storing files like documents and images. This augmenting technology is unique in that the files are stored on a decentralized database and only the hash of the files is stored on the underlying blockchain.

Lastly, Viant was built with an application programming interface (API) approach to allow a path for easy customization and integration. Realizing that Enterprise Resource Planning (ERP), the integrated management of core business processes mediated by existing software and technology, and existing systems are not going away overnight,

Viant's APIs intend to create a more seamless system integration process and allow for quicker movement from proof of concept to live production.

Pilot Project Phase I: Proof of Concept

To pilot blockchain technology in a seafood supply chain context, WWF joined an arrangement with Viant as one of the initial Beta customers for Viant, pioneering testing in collaboration with TraSeable Solutions and Sea Quest Fiji Ltd. An engaged process of intense coordination and collaboration among the team members across multiple time zones was made easier by the strong enthusiasm, shared interest, and understanding of the project's importance among each participant.

As with any innovation, we discovered various opportunities along the way to improve code and the user experience. The partnership required open dialogue and concrete processes to document any bugs or issues.

WWF invited Sea Quest to join the project because it offered a simplified use case for the application of the technology as a proof of concept. Sea Quest is a small company comprised of six vessels, delivering to a vertically integrated processing facility, which then delivers fresh and frozen tuna products to well-defined high value markets. Sea Quest also represents the best in class in terms of performance and ethical standards in fishing, as participants in multiple regional conservation initiatives in addition to being Marine Stewardship Council (MSC) certified. Sea Quest, for their part, recognised the potential of blockchain to facilitate better product control not only within their own operations, but also with respect to identification of end markets for their products in a way that could support better business decisions. With the added layer of trust that blockchain provides, a buyer could say with certainty that they are sourcing from the best possible fishing industry leader meeting the highest ethical and sustainability standards when purchasing from Sea Quest.

How It Works

TraSeable Solutions was engaged to provide on-the-ground technical input to integrate Viant with Sea Quest's existing processes. This was done through integrating Viant, via the APIs, with TraSeable's traceability platform, which provided the front-end for users. Project participants identified several advantages to this approach and expect that this will become the standard way to use Viant for complex supply chains where ERPs and/or digital traceability platforms already exist.

Integrating with Existing Platforms

One of the main reasons to consider integration with existing platforms involves the amount of data that needs to be digitally tracked with any product, such as tuna, as it moves through the supply chain. Working off the premise that blockchain is not a replacement for a centralised database system and should **only** capture Key Data Elements (KDEs) of a product, blockchain allows users to go beyond standard practice of simply storing KDEs to facilitate proving the provenance of the product and track changes

to its state. So, while there may be only about 100 KDEs for a tuna that you want to track through its supply chain, there are potentially thousands more data points about that tuna which is already being captured and is necessary for traceability purposes. Identifying which data elements need to be on-chain and which will be off-chain is an important exercise when mapping the supply chain.

The following graphic shows how the Viant and TraSeable platforms are integrated utilising APIs. TraSeable used RFID tags and sensors in the first few tests because the tools seemed like the logical technology to ease the data capture. With reusable RFID tags affixed to each piece of tuna, sensors are positioned on the fishing vessel and processing facility to capture the data automatically. Project participants faced numerous challenges trying to implement RFID technology and these are discussed later in this report.

The team also explored the possibility of the RFID sensors directly writing tag-related data to the blockchain via the Viant platform, but this was not possible with the existing equipment and associated limitations. Eventually, TraSeable evolved their solution to not rely on RFID.

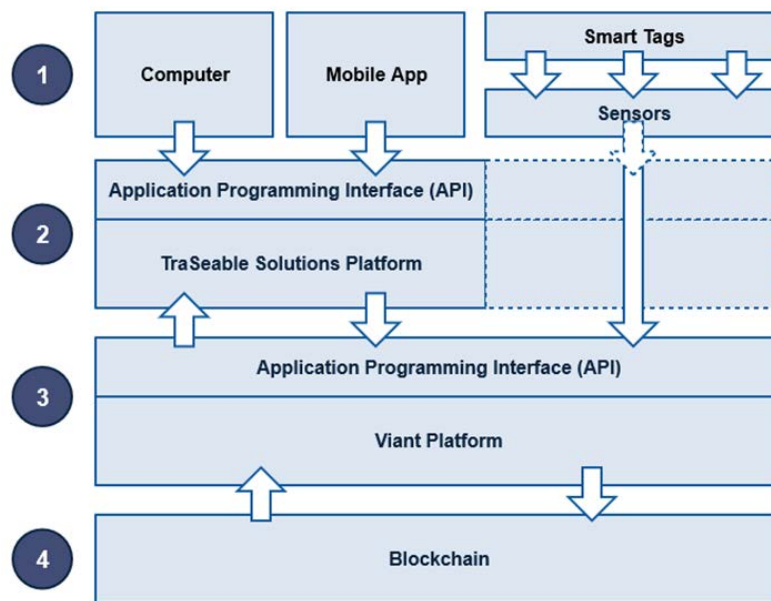


Figure 7: Integration of Viant and TraSeable platforms

Supply Chain Mapping

Supply chain mapping represents a key activity to ensure all the actors and processes are identified, as it has implications for how the traceability data is maintained through the supply chain. The “Bait to Plate” graphic in Figure 8 provides a good high-level visual summary of the main actors involved in the fresh export of tuna from Fiji to international markets. Many of the processes and actors in Fiji for Sea Quest’s fresh export operations were easily mapped, but the main challenge was that project participants could only trace fish as far as the international importers or distributors. Traditionally, Sea Quest only knew where their tuna went as far as the importer, and no further. Utilising blockchain

technology and a digital traceability platform will allow Sea Quest to trace their products further than previously available, even to the end buyer of the fish products, but this requires the participation of downstream actors to maintain and ensure the traceability of the products.

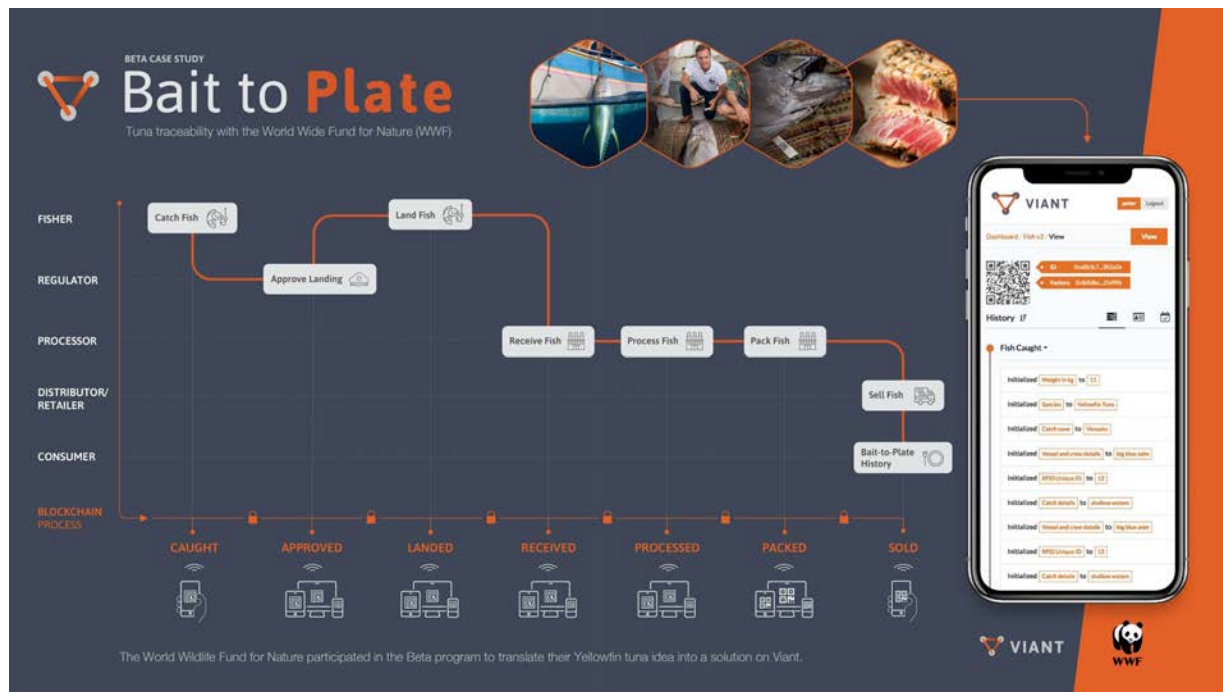


Figure 8: Viant Tuna Process Flow Diagram

Accounting for Every Fish

Very simply, under the current project a combination of RFID and QR codes are used to capture information throughout the supply chain. The nature of the longline fishery allows for each fish landed on a fishing vessel to be tracked by affixing a tag on the fish before it is placed into the hold. This tag follows the fish and registers automatically at various devices positioned on the vessel, at the dock, and in the processing facility. The image below shows this process of tagging being performed by a crew member. This is an additional step for the fishing vessel crew and is something that fishing companies must introduce into their workflow. In recognition of this additional task, Sea Quest is exploring ways to incentivise their crew to ensure accurate tagging and data capture of their catch.



Image 1: Tagging a Fish. © Ken Katafono

If there is Internet access onboard the vessel then the tagged fish data can be transmitted and recorded as digital assets on the blockchain. Fishing vessels that operate in the Fijian longline fishery do not have Internet access, but instead crew use their own mobile devices to access the Internet for personal use when in range of the local telecommunication company's reception on nearby islands. As fish are tagged, the TraSeable app records key data on a mobile device, which digitally signs that record and, once internet reception is available, the app automatically transmits recorded data to TraSeable's servers which then records the information on the blockchain.



Image 2: Tagged tuna aboard a fishing vessel. © Ken Katafono

Tagging individual fish with relatively cheap and reusable tags also provides additional, and sometimes unexpected, benefits for the fishing company. For instance, the technology provides a means to address issues of theft of catch onboard fishing vessels and provides much greater detail of the fishing activity that is useful for fishing companies to analyse their fishing effort.

Landing and Processing

At the end of the fishing trip and on return to port, each piece of tagged fish is verified at landing and is then transferred to a processing facility. Within the processing facility the tag stays with the fish through the entire process to ensure the continuity of the fish story.



Image 3: Tagged fish entering a processing facility. © Ken Katafano

The tag is typically removed at the point of packaging and is swapped with a unique QR code that goes with the fish or product to the market. Each QR code is specific to the original RFID tag identity, making real-time mass balance reconciliation possible.

TraSeable carried out a limited trial testing Near Field Communication (NFC) crypto tags adhered to packages of tuna loins. TraSeable identified that the tamper-proof NFC tags could be provisioned on the blockchain with a unique address similar to the RFID tags. Project partners generally believe that NFC tags, as a passive data capture technology, represent the future of traceability technology, not only because they provide a secure and durable tool for capturing information, but can also more effectively provide for technological advancements such as Augmented Reality (AR) experiences.



Figure 9: Augmented Reality Facilitated by Blockchain and NFC

Distribution and Retail

Once packaged, the products enter distribution channels to their destination markets. At this point users can engage either the TraSeable or Viant apps to track the fish downstream to the retail outlets and finally to the consumer. At each step of the way, the system, through different supply chain actors simply scanning the QR code on the packaging and entering some key pieces of information, maintains and builds the “story of the fish.” Actors can also view the history of the products they are handling. One such story is available here - <https://traseable.com/story/FJ00001/>



Image 4: Sashimi and QR Code. © Ken Katafano

Proving the Technology

Project participants have proven the technology in the domestic Fijian market, tracing a fish from its capture off the coast of Fiji all the way through a retail market in the Tamavua subdivision of Suva.

Recently, the Pacific tuna from this project was also featured as an example of blockchain based supply chain transparency and traceability for commodities in the Ethereum Summit in New York, thus proving the technology in a limited context into an export market. Participants at the event were able to sample the fish, scan the code, and connect with the story of the fish.

Pilot Project Phase II: Expansion and Payments

The current project partners are pursuing expansion into a more standardised delivery into an export market to further prove the viability of the technology. Existing project partners have entered an arrangement with new partners including a large regional bank, an additional seafood processor, a regional distributor, and a major retail outlet.

Phase II of the project will explore new ways to expand upon the existing project, including the incorporation of automatic payments into the tuna supply chain using smart contracts. As demonstrated by a [test blockchain delivery of tuna conducted by the Spanish banking giant BBVA in November 2017](#),¹⁶ automated payments and other legal instruments (customs documents, bills of lading, etc.) facilitate multiple benefits including a reduction in paperwork, payment processing time, and general reduction in risk premium. Viant seeks to work with existing and new members of the team to test various automatic payment mechanisms and ultimately support in driving the automatic payments into full production.

The team will also continue testing Near Field Communications (NFC) integration so that passive data collection – the collection of information without an explicit action by a supply chain actor - may be further developed and implemented for tracking and even marketing purposes.

Challenges

Reliance on paper-based processes

Much of the longline fishery in the Pacific remains heavily reliant on paper-based processes in both Government agencies, like Fiji's Ministry of Fisheries, and in fishing companies. For any kind of traceability to work well it requires as much digitisation of processes along the supply chain as possible in addition to some interoperability of information systems that are used across the Pacific. A first step to using blockchain

¹⁶ Espinosa, Luz Fernandes. "BBVA and Wave carry out the first blockchain-based international trade transaction between Europe and Latin America." BBVA. November 27, 2017. *retrievable at* <https://www.bbva.com/en/bbva-and-wave-carry-first-blockchain-based-international-trade-transaction-europe-and-latin-america/>.

technology would need to be the utilisation of a digital traceability platform that can capture the KDEs necessary for traceability.

Availability of Local Suppliers and Technicians

Implementing RFID technology proved challenging because no industry exists in Fiji to support the supply, implementation, and maintenance of the RFID equipment, including both the tags and sensors. TraSeable had to source equipment from Australia, which took more than four weeks to arrive causing delays. Since no local expertise was available to install the equipment, the team had to engage a local electronic communications company with limited experience using the technology to figure out how best to install and use the RFID equipment.

However, the experience of this trial suggested that the use of RFID, while preferable due to its ability to automate data collection through passive data capture, is not essential to implementing blockchain traceability. Traseable is currently experimenting with other technologies and methodologies that do not rely on RFID technology for data capture. A fully QR enabled data capture system could offer a similar level of data capture and security with appropriate standardised procedures that include independent verification and validation points.

Mapping the Supply Chain Past the Importer

Some fishing companies will not know what happens to their products past their international buyers. Thus, mapping what happens from the international importers and distributors onwards downstream becomes challenging. Vertically integrated companies that have control of their entire supply chain will be able to implement this technology more easily and effectively than others.

Cooperation of Downstream Supply Chain Actors

This is an important constraint on adopting blockchain traceability as all the supply chain actors must be incentivised to participate the process. Without agreement among all parties to maintain traceability or without appropriate incentives to effectively engage in the process it is difficult if not impossible to achieve “Bait to Plate” transparency.

Authenticity of Data

Any information system is only as good as the quality of its data. Like any other system, blockchain faces the same challenges with the well-known problem of “garbage in, garbage out.” It is extremely difficult if not impossible to verify the authenticity of data being recorded at each stage of the supply chain, but what blockchain offers is the ability to “see” what previous actors have recorded and so it is possible to identify where supply chain actors may have entered false data in the supply chain. Thus, the expectation is that

incorrect or fraudulent information will eventually be flagged, especially for repeat offenders, which will eventually be excluded from the supply chain.

One method of mitigation for incorrect or fraudulent data is the use of mass-balance reconciliation, which blockchain can facilitate in real-time or near real-time for certain products. For the sake of simplicity, we can use a theoretical tuna to explain how this works. For instance, consider a 20 kg tuna (dressed weight) is harvested and given a unique identifier. That fish will render a maximum of four loins at 5 kgs each when processed. Each loin is delivered to a distributor that registers the unique identifier on the blockchain before passing on the fish to a retailer, who then confirms receipt and processes the loin into ten 500g steaks for individual sale that each carry the same unique identifier entered into the blockchain. At no time should the total weight associated with the unique identifier for that tuna exceed 20 kilograms. If it does, it indicates that there has been an adulteration of the product or a substitution of another product. Because this is recorded in near real-time, the system can be periodically or automatically interrogated to identify or flag where errors or fraud might be occurring.

Other innovations such as product identifiers that include DNA information or biochemical and geochemical signatures could make it much more difficult to falsify product details or allow spot auditing of supply chains to verify and validate other controls. For example, the company [Oritain](https://oritain.com/)¹⁷ has successfully used a biochemical signature to track and audit shipments of high-quality Manuka honey from New Zealand through secondary processing in China. Although not currently available for tuna, DNA or biochemical techniques could provide an additional verification and validation tool in the near future.

While “garbage in, garbage out” remains a challenge, it is important to recognise that fraud and malfeasance, or even simple honest error, is infinitely more detectable under a blockchain scenario than any centralised database scenario. Moreover, the permanence of the blockchain allows instantaneous auditing of a historic record that could help identify patterns of ongoing fraud very quickly, allowing markets to avoid risk and affording regulatory authorities an opportunity to quickly identify and address those instances.

Transaction Time Limitations

Transaction times may also limit the feasibility of the technology, with public Ethereum currently allowing only 10 transactions per second and private permissioned versions of Ethereum allowing over 1,000. In comparison, the average credit card system can support around 50,000 transactions per second. However, these challenges are not insurmountable and solutions such as Viant’s use of an InterPlanetary File System (IPFS) for storing files like documents and images will help reduce the transaction time burden. As experienced with every other technology, it is expected that transactional limitations will evolve quickly, becoming more efficient, effective, and economical over time.

¹⁷ <https://oritain.com/>

Basic Costs

Because this technology is in its early stages of development and business models are currently evolving, a fully confirmed cost structure cannot be identified at this time. However, it is possible to estimate some basic costs that might be indicative of the implementation of comparable systems while providing insights to the future costs of implementation in more complex scenarios. The following spreadsheet represents the estimated indicative costs for the existing project.

Item	Frequency	Unit Cost	Qty	Total	Notes
					1. All costs in USD
<u>Hardware</u>					2. These costs are for 1 vessel
RFID tags	Per trip	\$1.00	800	\$800.00	3. RFID tags were reusable
RFID scanner - handheld	One off - replace 3 yrs	\$1,970.00	1	\$1,970.00	4. Approx 800 tags per trip for Sea Quest largest boat
RFID scanner - fixed mid-range	One off - replace 3 yrs	\$930.00	1	\$930.00	5. Sea Quest fishing trips run for about 3 weeks depending on catch
Tablet - vessel	One off - replace 3 yrs	\$380.00	1	\$380.00	
Tablet - landing & processing	One off - replace 3 yrs	\$380.00	3	\$1,140.00	
<i>Total - Hardware</i>				\$5,220.00	
<u>Software (per month)</u>					
Viant*	Per month	\$TBD	1	\$TBD	*Viant costs are variable and case specific.
TraSeable	Per month	\$1,000.00	1	\$1,000.00	
<i>Total - Software</i>				\$6,000.00	
<u>Resources (man-hours)</u>					
Training	One off	\$10.00	25	\$250.00	
Support	Per trip	\$10.00	5	\$50.00	
<i>Total - Resources</i>				\$300.00	
<u>Miscellaneous</u>					
Fish tag printing	Per trip	\$0.12	800	\$96.00	
Label printing - carton, loins	Per trip	\$0.40	800	\$320.00	
Mobile data (per tablet)	Per trip	\$7.50	4	\$30.00	
Internet bandwidth (per month)	Per month	\$25.00	1	\$25.00	
<i>Total - Miscellaneous</i>				\$471.00	
TOTAL**				\$11,991.00	**Total costs are meant to be indicative for this pilot and may not represent the true costs for future pilots or implementations.

Table 1: Basic Costs



Conclusion and Recommendations

The global seafood supply chain must address traceability in a genuine way if it hopes to address market concerns regarding illegal and unethically produced seafood products. Blockchain supply chain traceability holds immense promise to address those concerns. The transactional efficiencies made available to business participants alone should encourage participation. Additionally, the markets will continue to call for the level of transparency, traceability, and trust that realistically can only be afforded by blockchain.

While the promises of Blockchain are lofty, and there are challenges to work through, it is clear that Blockchain will inevitably change the face of supply chain traceability for commodities such as seafood. Like E-commerce, blockchain proposes to be another landmark transformative technology, and once we pass through the door, there will be no going back. Like with many technologies, those companies that lead the revolution will be the beneficiaries, while those slow to adopt Blockchain will find themselves either struggling to compete or out of business.

The following recommendations reflect the experience of the participants in this project. While they are not comprehensive, they are intended to capture the most important issues faced in the development and implementation of the project while providing

guidance to others how to go about executing their own blockchain supply chain implementation.

Recommendation 1: Supply chain mapping must occur as early as possible in the process.

Recommendation 2: Project partners should engage as many supply chain actors as possible as early as possible in the process to secure buy in and effective participation. Ideally, all actors along the supply chain must participate and agree to use blockchain.

Recommendation 3: Project partners should identify and promote incentives as early in the process as possible.

Recommendation 4: A waterline technical consultant that facilitates the design and implementation of data capture tools on the vessel and throughout the supply chain is critical.

Recommendation 5: A technical support network must be in place to support the applicable technology (e.g. RFID, QR, etc.). Suppliers and technicians should be available where the vessels and processors are located.

Recommendation 6: It is more feasible to implement a blockchain system with a traceability service provider who then provides the service to different actors along the supply chain when there are different companies involved. However, for substantially vertically integrated supply chains they could effectively subscribe to a blockchain supply chain product such as Viant directly and then integrate that system with their existing traceability system.

Recommendation 7: The information collected that goes onto the blockchain represents only a small subset of the data necessary for full traceability and other fisheries operations.

Recommendation 8: Ideally, data capture should be as automated as possible using passive data capture tools. Less human intervention allows for reduced error and less potential for fraud.

Recommendation 9: Asset ownership permissions can effectively address some concerns of data confidentiality.

Recommendation 10: Blockchain will not prevent the problem of “garbage in, garbage out,” where fraudulent or false data entered at one point carries through the entire system. However, companies can mitigate this problem by automating data capture and through additional verification and validation, which should be considered early in the development process.

Contacts

Bubba Cook
Western and Central Pacific Tuna Programme Manager, WWF- New Zealand
Email: acook@wwf.panda.org

Tyler Mulhilvill
Co-founder, Viant
Email: tyler.mulvihill@consensys.net

Ken Katafono
Founder and Managing Director, TraSeable Solutions Pte Ltd.
Email: founder@traseable.com

Brett "Blu" Haywood
CEO, Sea Quest Fiji Ltd.
Email: blu@sequestfiji.com

Glossary

This glossary is not fully comprehensive, but is meant to provide many of the standard terms and acronyms that might be encountered in the development of a blockchain supply chain system in addition to those encountered in this document.

A

AAL = "Account Abstract Layer" is a special point of contact or bridge between the Bitcoin Protocol and Ethereum Virtual Machine.

Address = In cryptocurrency terms, an address is a code used to send, receive or store cryptocurrency. These addresses consist of 26-35 characters, a combination of letters and numbers. The address can also refer to the public key, a pair of keys needed to sign their digital transactions.

Agreement ledger = An agreement ledger is distributed ledger used by two or more parties to negotiate and reach agreement.

Altcoin = "Alternative coin" ("altcoin" or "alt coin") is every other cryptocurrency than Bitcoin (BTC). Bitcoin is considered the main index for cryptocurrency market.

API = An "Application Programming Interface" is a set of subroutine definitions, protocols, and tools for building application software.

Attestation ledger = A distributed ledger providing a durable record of agreements, commitments or statements, providing evidence (attestation) that these agreements, commitments or statements were made.

B

BFT = "Byzantine Fault Tolerance" is the dependability of a fault-tolerant computer system, particularly distributed computing systems, where components may fail and there is imperfect information on whether a component is failed.

Bit = A unit used to designate a sub-unit of a bitcoin - 1,000,000 bits equals 1 bitcoin (BTC).

Bitcoin (uppercase) = Bitcoin with a capital “B” is typically associated with Bitcoin the protocol and payment network. Bitcoin is a well known cryptocurrency, based on the proof-of-work blockchain. Example: "I've studied a lot about Bitcoin."

bitcoin (lowercase) = Bitcoin with a lowercase “b” written as “bitcoin” is usually associated specifically with bitcoin as the currency. Bitcoin is the first decentralized, open source cryptocurrency that runs on a global peer to peer network, without the need for middlemen and a centralized issuer. Example: "Could you send me two bitcoins, please?"

Block = Blocks are packages of data that carry permanently recorded data on the blockchain network.

Blockchain = Originally block chain, is a continuously growing list of records, called blocks, which are linked and secured using cryptography.

Block explorer = An online tool to view all transactions, past and current, on the blockchain. They provide useful information such as network hash rate and transaction growth.

Block confirmation = Block confirmation is a successful act of hashing a transaction, including it in a block, and then adding that block to the blockchain.

Block height = Block height refers to the number of blocks connected together in the block chain. For example, Height 0, would be the very first block, which is also called the Genesis Block.

Block size = A block size is the number of transactions that a block can hold. Block sizes can have an impact on a network’s transaction timing and fees.

Block timestamp = Each block contains a timestamp in Unix. They help to make it more difficult for someone else to manipulate the blockchain.

BTC = A symbol for Bitcoin.

C

Central Ledger = A central ledger refers to a ledger maintained by a central agency.

Centralized = A system or organization that is controlled by one person or group.

Cipher = An algorithm used for the encryption and/or decryption of information. In common language, "cipher" is also used to refer to an encryption message, also known as "code".

Coin = The express purpose of a coin is to act like money: as a unit of account, store of value and medium of transfer. Coins tend to take the form of native blockchain tokens like Bitcoin (BTC), Litecoin (LTC), Monero (XMR), and so on. A crypto coin is just that: a coin, or means of payment, whilst a token has wider functionality.

Coinbase = One of the world’s most popular cryptocurrency web wallet.

Confirmation = The successful act of hashing a transaction and adding it to the blockchain.

Consensus = Consensus is achieved when all participants of the network agree on the validity of the transactions, ensuring that the ledgers are exact copies of each other.

Consensus algorithm = a process in computer science used to achieve agreement on a single data value among distributed processes or systems. Consensus algorithms are designed to achieve reliability in a network involving multiple unreliable nodes.

Consensus rule = Consensus rules are a set of rules that all nodes on a cryptocurrency network must enforce when the validity of a block and its transactions are concerned.

Consortium blockchain = A blockchain where the consensus process is controlled by a pre-selected set of nodes; for example, a consortium of 20 financial institutions.

CPU = A "Central Processing Unit" is the electronic circuitry within a computer that carries out the instructions of a computer program by performing the basic arithmetic, logical, control and input/output (I/O) operations specified by the instructions.

Cryptocurrency = Also known as tokens or coins, cryptocurrencies are representations of digital assets.

Cryptographic hash function = Cryptographic hashes produce a fixed-size and unique hash value from variable-size transaction input. The SHA-256 computational algorithm is an example of a cryptographic hash.

Cryptography = The study and practice of secret communication.

D

Dapp = A decentralized application ("Dapp" or "dApp") is an application that is open source, operates autonomously, has its data stored on a blockchain, incentivised in the form of cryptographic tokens and operates on a protocol that shows proof of value.

DBFT = "Delegated Byzantine Fault Tolerance" is a new type of algorithm used by NEO. Unlike the standard proof-of-work or proof-of-stake use in other networks, the dFBT allows the network to resolve issues without forcing a fork. It also makes it difficult for delegates to collude to harm the network.

Decentralized = A common term in cryptocurrency which means that the currency isn't issued or regulated by a centralized authority, such as a government or bank.

Decryption = A process of turning cipher-text back into plaintext.

Difficulty = Difficulty, in Proof-of-Work mining, is how hard it is to verify blocks in a blockchain network. In the Bitcoin network, the difficulty of mining adjusts verifying blocks every 2016 blocks. This is to keep bitcoin block verification time at ten minutes.

Digital asset = Anything that exists in a binary format and comes with the right to use. Data that do not possess that right are not considered assets. Digital assets include but are not exclusive to: digital documents, audible content, motion picture, and other relevant digital data that are currently in circulation or are, or will be stored on digital appliances.

Digital certificate = A public key certificate, also known as a digital certificate or identity certificate, is an electronic document used to prove the ownership of a public key.

Digital commodity = A scarce, electronically transferrable, intangible, with a market value.

Digital identity = An online or networked identity adopted or claimed in cyberspace by an individual, organization, or electronic device.

Digital signature = A mathematical scheme for presenting the authenticity of digital messages or documents.

Distributed = A computer system or organization that has entire copies of it being run and maintained simultaneously on multiple computers.

Distributed ledger = An agreement of shared, replicable and synchronized data, in this case spread across multiple networks, across many CPU's.

Distributed network = A type of network where processing power and data are spread over the nodes rather than having a centralized data centre.

DPOS = Delegated-Proof-of-Stake, the fastest, most efficient, most decentralized, and most flexible consensus model available.

E

EEA = The "Enterprise Ethereum Alliance" connects Fortune 500 enterprises, startups, academics, and technology vendors with Ethereum subject matter experts.

EIP = "Ethereum Improvement Proposal" is a standard to submit potential changes or improvements that will have a positive effect on the Ethereum protocol as a whole.

Encryption = A process of turning a clear-text message (plaintext) into a data stream (cipher-text), which looks like a meaningless and random sequence of bits.

Enterprise resource planning (ERP) = The integrated management of core business processes, often in real-time and mediated by software and technology.

ETC = A symbol for Ethereum Classic currency.

ETH = A symbol for Ether, token of the Ethereum blockchain.

Ethereum = A blockchain-based decentralized platform for apps that run smart contracts, and is aimed at solving issues associated with censorship, fraud and third party interference.

EVM = Ethereum provides a decentralized Turing-complete virtual machine, the "Ethereum Virtual Machine" (EVM), which can execute scripts using an international network of public nodes.

EVM code = A programming language in which accounts on the Ethereum blockchain can contain code. The EVM code associated with an account is executed every time a message is sent to that account, and has the ability to read/write storage and itself send messages.

F

FBA = "Federated Byzantine Agreement" is a model suitable for worldwide consensus. In FBA, each participant knows of others it considers important. It waits for the vast majority of those others to agree on any transaction before considering the transaction settled. In turn, those important participants do not agree to the transaction until the participants they consider important agree as well, and so on.

Fiat money / Fiat currency = A currency without intrinsic value established as money, often by government regulation (\$ USD, € EUR, £ GBP, ¥ JPY etc.).

Fork = Forks create an alternate version of the blockchain, leaving two blockchains to run simultaneously on different parts of the network.

Fungible = A positive quality where two or more of the same thing have identical value. That is to say, one of a group of things can be a substitute for another and it won't change the value.

G

Gas = A measurement roughly equivalent to computational steps.

Genesis Block = The very first block in a block chain.

Government = A group of people with the authority to govern a state or country.

GPU = A "Graphics Processing Unit" is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device.

H

Hash = The act of performing a hash function on the output data. This is used for confirming coin transactions.

Hash algorithm = A function that converts a data string of an arbitrary length to a fixed, shorter length.

Hashrate = Measurement of performance for the mining rig is expressed in hashes per second. Mh/S (mega hash per second) is the speed that a graphics processor, GPU, can hash per second.

I

ICO = "Initial Coin Offering", which takes a page from the usual IPOs investors know. Coins bought during ICOs are usually sold for a profit when the coin first hits exchanges. This is due to the initial hype which increases demand for the coin. On the supply side, ICOs create entry barriers as the buyer has to set up his private wallet to receive the coins from the ICO purchase.

IPFS = "InterPlanetary File System" is a hypermedia distribution protocol, addressed by content and identities. It is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files.

Irreversible = After confirmation, a transaction is unable to be reversed. By nobody. There is no safety net for that situation.

L

Ledger = An append-only record store, where records are immutable and may hold more general information than financial records.

M

Medium of exchange = An intermediary used in trade to avoid the inconveniences of a pure barter system. Fiat currencies are the generally accepted mediums of exchange. Their most important and essential function is to provide a measure of value.

Mempool = A technical term for a collection of unconfirmed transactions stored by a node until they either expire or get included in the main chain.

Miners = Servers/computers which are used to solve the cryptographic problems attached to blockchain transactions. Miners receive a reward in the form of cryptocurrency for providing transactions on the blockchain.

Mining = The process by which transactions are verified and added to a blockchain. This process of solving cryptographic problems using computing hardware also triggers the release of cryptocurrencies.

Mining algorithm = The algorithm used by a cryptocurrency to sign transactions, these vary across different cryptocurrencies. Bitcoin's mining algorithm is SHA256, whilst Litecoin and Dogecoin's are Scrypt.

Mining difficulty = Mining difficulty is simply a measure of how difficult it is to be the next person that gets to add a block to the blockchain, and receive the reward for doing so. A lower mining difficulty indicates that a cryptocurrency is easy to mine. Conversely, a higher mining difficulty suggest that a cryptocurrency is more difficult to mine.

Mining pool = A group of miners who have decided to combine their computing power for mining. This allows rewards to be distributed more consistently between participants in the pool.

Mining rig = A mining rig consists of dedicated computer systems that are specifically designed and setup to mine cryptocurrencies.

N

Near Field Communication (NFC) = a short-range wireless connectivity standard that uses magnetic field induction to enable communication between devices when they are touched together, or brought within a specified distance of each other. Passive NFC devices include tags, and other small transmitters, that can send information to other NFC devices without the need for a power source of their own.

Network = A group of two or more computers connected together with the purpose of sharing resources as well as information.

Node = A copy of the ledger operated by a participant of the blockchain network.

O

Open source = The practice of sharing the source code for a piece of computer software, allowing it to be distributed and altered by anyone.

Oracles = Oracles work as a bridge between the real world and the blockchain by providing data to the smart contracts.

Orphan = A block that has been abandoned and will not be built upon.

P

Passive Data Collection = Data collection in which information is gathered automatically, generally without any required action by a participant.

P2P / Peer to Peer = Peer to Peer (P2P) refers to the decentralized interactions between two parties or more in a highly-interconnected network. Participants of a P2P network deal directly with each other through a single mediation point.

PBFT = "Practical Byzantine Fault Tolerance" algorithm provides high-performance Byzantine state machine replication, processing thousands of requests per second with sub-millisecond increases in latency.

Permissioned blockchain = Permissioned blockchains provide highly-verifiable data sets because the consensus process creates a digital signature, which can be seen by all parties.

Permissioned ledger = A ledger where actors must have permission to access the ledger. Permissioned ledgers may have one or many owners. When a new record is added, the ledger's integrity is checked by a limited consensus process. This is carried out by trusted actors—government departments or banks, for example—which makes maintaining a shared record much simpler than the consensus process used by unpermissioned ledgers.

Permissionless = A positive quality, where anyone is permitted to join and participate in an activity. Permissionless is often used when describing blockchain technologies because anyone can download the digital record known as the blockchain and participate in recording and verifying information.

Public Key Infrastructure (PKI) = A set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

Proof-of-Authority (PoA) = A consensus mechanism in a private blockchain which essentially gives one client (or a specific number of clients) with one particular private key the right to make all of the blocks in the blockchain.

Proof-of-Importance (PoI) = A consensus mechanism that is different from other initiatives which use a fee-sharing model that does not take into consideration one's overall support of the network.

Proof-of-Stake (PoS) = A type of algorithm by which a cryptocurrency blockchain network aims to achieve distributed consensus.

Proof-of-Work (PoW) = An economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer.

Private key = A private key is a string of data that allows you to access the tokens (cryptocurrency) in a specific wallet. They act as passwords that are kept hidden from anyone but the owner of the address.

Private key cryptography = This key is encrypted so that it is confidential to only its owner.

Protocol = Protocols are sets of formal rules describing how to transmit or exchange data, especially across a network.

Public address = A public address is the cryptographic hash of a public key. They act as email addresses that can be published anywhere, unlike private keys.

Public key = In cryptography a public key is a cryptographic key that can be utilized by any party to encrypt a message. Another party can then receive the message and using a key that is only known to that individual or group, decode the message.

Q

QA = "Qualitative Analysis" is a research that uses subjective judgment based on nonquantifiable information, such as management expertise, industry cycles, and labor relations.

QR code = "Quick Response Code" is a digital representation of a Bitcoin public or private key that is easy to scan by digital cameras. QR codes are similar to barcodes found on physical products in that they are a machine-friendly way to embody a piece of data.

R

Recipient = A person (or object) who is capable of receiving something from someone, such as a cryptocurrency.

RFID = "Radio Frequency Identification" is a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object.

Ring signature = A type of digital signature that can be performed by any member of a group of users that each have keys.

Ripple = A payment network built on distributed ledgers that can be used to transfer any currency. The network consists of payment nodes and gateways operated by authorities. Payments are made using a series of IOUs, and the network is based on trust relationships. The banking industry is adapting this platform.

RNG = "Random Number Generation" is the generation of a sequence of numbers or symbols that cannot be reasonably predicted better than by a random chance, usually through a hardware random-number generator.

S

Satoshi Nakamoto = The name used by the unknown person or group of people who designed bitcoin and created its original reference implementation.

Scrypt = An alternative proof-of-work system to SHA-256, designed to be particularly friendly to CPU and GPU miners, while offering little advantage to ASIC miners.

Settlement system = A system that enables the contractual obligations of an agreement made between two parties to be fulfilled.

SHA-256 = A cryptographic algorithm used by cryptocurrencies such as Bitcoin. However, it uses a lot of computing power and processing time, forcing miners to form mining pools to capture gains.

Sidechain = These are theoretical, independent blockchains which are "two way pegged" to the Bitcoin blockchain. These can have their own unique features and can have bitcoins sent to and from them.

Signature = A mathematical operation that lets someone prove their sole ownership over their wallet, coin, data or on. An example is how a Bitcoin wallet may have a public address, but only a private key can verify with the whole network that a signature matches and a transaction is valid. These are only known to the owner and are basically mathematically impossible to uncover.

Smart contract = Smart contracts are contracts whose terms are recorded in a computer language instead of legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system.

Solidity = Solidity is Ethereum's programming language for developing smart contracts.

SPV = "Simple Payment Verification" allows a lightweight client to verify that a transaction is included in the Bitcoin blockchain, without downloading the entire blockchain.

Stealth address = A random, one-time address created for a transaction (utilized on the Monero blockchain).

Stratis = Stratis is a blockchain-based cryptocurrency created to help simplify the development, testing, and deployment of applications for enterprises in the finance sector that target to enjoy advantages of blockchain technology. It operates as a Blockchain-as-a-Service (BaaS) platform to help enterprises craft their own blockchains (side chains) with the features they need.

Stream cipher = Stream ciphers are a method of encrypting text ("cyphertext" or "ciphertext") in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time.

T

Testnet = A test blockchain used by developers to prevent expending assets on the main chain.

Token = Usually considered as a "coin", but a crypto coin is just that: a coin, or means of payment, whilst a token has wider functionality. Blockchain tokens do have value, but they cannot be considered money in quite the same way that a straightforward coin can. Tokens are generally hosted on another blockchain, like Ethereum or Waves: 2.0 protocols that allow users to create them using the core coin.

Tokenless ledger = Refers to a distributed ledger that doesn't require a native currency to operate.

TPS = "Transactions Per Second".

Transaction = Buying or selling of a cryptocurrency, which is broadcasted across the network and collected into blocks.

Transaction block = A collection of transactions on the Bitcoin network, gathered into a block that can then be hashed and added to the blockchain.

Trustless = A positive quality where you are not required to trust the person you're doing the transaction with. A trustless system or technology is so secure and smooth in handling your transactions, that both people in a transaction can safely hand over money and other valuables without the risk of being cheated.

Turing complete = Ability of a machine to perform calculations that any other programmable computer is capable of. An example of this is the Ethereum Virtual Machine (EVM).

Turing machine = A mathematical model of computation that defines an abstract machine, which manipulates symbols on a strip of tape according to a table of rules.

U

Unpermissioned ledger = Unpermissioned ledgers such as Bitcoin have no single owner—indeed, they cannot be owned. The purpose of an unpermissioned ledger is to allow anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies.

Utility = Utility simply means the usefulness of a cryptocurrency. The more useful a cryptocurrency is, the more likely it is to be noticed as valuable, and therefore, the more likely it is to be bought.

Utility token = A token that when purchased, gives the owner access to a specific protocol or network.

W

Wallet = A secure digital wallet that houses private keys. It usually contains a software client which allows access to view and create transactions on a specific blockchain that the wallet is designed for.

White paper = In cryptos is prepared by a party prior to launching a new currency. A White paper is authoritative reports that inform readers in short to understand complex issues, solve problem and make right decision.

Wire transfer = Electronically transferring money from one person to another. Commonly used to send and retrieve fiat currency from cryptocurrency exchanges.



Why we are here

To stop the degradation of the planet's natural environment and to build a future in which humans live in harmony with nature.

panda.org

© 1986 Panda symbol WWF – World Wide Fund for Nature (Formerly World Wildlife Fund)
® "WWF" is a WWF Registered Trademark. WWF, Avenue du Mont-Bland, 1196 Gland, Switzerland – Tel. +41 22 364 9111 Fax +41 22 364 0332. For contact details and further information, please visit our international website at www.panda.org