Sustainability Standards and Blockchains

Results of a pilot conducted as part of the project “The Blockchain Revolution: Application to Sustainably Certified Supply Chains” funded by the ISEAL Innovations Fund and led by the Roundtable on Sustainable Biomaterials (RSB) and Provenance.

March 2018

The ISEAL Innovations Fund is supported by the following partners:
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY AND RECOMMENDATIONS</td>
<td>2</td>
</tr>
<tr>
<td>CONTRIBUTORS</td>
<td>2</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>About the project</td>
<td>4</td>
</tr>
<tr>
<td>Defining the hypotheses</td>
<td>5</td>
</tr>
<tr>
<td>Selecting the pilot supply chain</td>
<td>5</td>
</tr>
<tr>
<td>Reducing audit inefficiency</td>
<td>6</td>
</tr>
<tr>
<td>Background</td>
<td>6</td>
</tr>
<tr>
<td>Suggestion</td>
<td>7</td>
</tr>
<tr>
<td>A single source of truth for chain of custody tracking</td>
<td>9</td>
</tr>
<tr>
<td>Background</td>
<td>9</td>
</tr>
<tr>
<td>Tier one: simple commitment by both actors</td>
<td>11</td>
</tr>
<tr>
<td>Tier two: zero knowledge proofs</td>
<td>11</td>
</tr>
<tr>
<td>Improving sustainability data reporting</td>
<td>12</td>
</tr>
<tr>
<td>Background</td>
<td>12</td>
</tr>
<tr>
<td>Suggestion</td>
<td>13</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>14</td>
</tr>
<tr>
<td>RECOMMENDATIONS FOR A FOLLOW-UP PROJECT</td>
<td>14</td>
</tr>
<tr>
<td>DEFINITIONS</td>
<td>15</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY AND RECOMMENDATIONS

This report documents ideas for how certifiers can leverage blockchain technology to reduce audit inefficiency, create a single source of truth for chain of custody (CoC) tracking and support sustainability data reporting. As a next step, RSB and Provenance recommend a follow-up project to investigate one of the hypotheses in detail. We suggest that this project involves a smaller group of certifiers who work with the same product and a commercial partner with a relevant supply chain.

CONTRIBUTORS

Provenance Team
Jessi Baker, CEO
Ian Kynnersley, CTO
Stephanie Lau, Business Analyst
Thibaut Schaeffer, Blockchain Engineer & System Designer

RSB Team
Arianna Baldo, Global Business Development Support
Rolf Hogan, Executive Director

With special thanks to UPM Biofuels
INTRODUCTION

When it comes to providing trust in supply chains, organisations are facing significant challenges: supply chains are becoming more complex, audits are increasingly costly, and the relevance of some standards organisations is being questioned by businesses launching their own schemes. Mike Coupe, CEO of Sainsbury’s, in describing a certification scheme, said it “might have been fit for purpose 25 years ago, but we’re in a new world with new technology”. Although technology is not the cure for everything, it is certainly part of the way forward for the certification industry.

Over the last 9 months, project partners Provenance and the Roundtable on Sustainable Biomaterials (RSB) have been working alongside the ISEAL Alliance to explore the opportunities that blockchain technology offers to sustainability certifications and partners, enabling ISEAL members to better understand this technology and capitalise on it.

About Project partners

The Roundtable on Sustainable Biomaterials (RSB) is a global, multi-stakeholder independent organisation that drives the development of a new world bioeconomy through sustainability solutions and collaborative partnerships. The RSB is directly engaged with sector pioneers who are seeking solutions for a new generation of products that are free of fossil fuels, and offers the world’s most trusted, peer-reviewed, global certification standard for sustainable biomaterials, biofuels and biomass production. The standard contributes to food security, rural development and restoration of ecosystems. Visit www.rsb.org for more information.

Provenance is a technology startup and social enterprise creating tools to bring a new digital dimension to products. Enabled by mobile, blockchain and open data, their software helps progressive companies gain a competitive edge with transparency and traceability. Provenance enables any physical thing to come with a digital passport - linking materials with proven claims, providing a platform for gathering and creating collaborative content and data related to supply chains, and tracking items through even the most complex chains of custody. Visit www.provenance.org for more information.

The ISEAL Alliance is a global membership association for credible sustainability standard systems, and provides tools, training, events, resources and a community to help shape an effective standards movement. ISEAL supports cooperation between our members and others to strengthen the effectiveness of that movement. Visit www.isealalliance.org for more information.
The project was funded by the ISEAL Alliance Innovations Fund which seeks to support the best innovations that help sustainability standards to deliver more value to different stakeholders and to be more effective at driving improvement over time and at scale.

**About the project**

“The Blockchain Revolution: Application to Sustainably Certified Supply Chains” is a 9-month pilot project aimed to demonstrate what opportunities blockchain technology can offer to sustainability standard systems and sustainably certified supply chains.

In its rationale, the project understands that blockchain is a disruptive technology with the potential to solve numerous challenges for sustainability certification and dramatically increase supply chain transparency and efficiencies. It however also acknowledges that blockchain is a new, complex technology that can be applied to numerous problems and that requires significant time, focus and investment to be fully developed and deployed at scale.

Within these limitations, the project set out to achieve its goal in three progressive phases:

<table>
<thead>
<tr>
<th>Phase</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>I - Learning and Scoping</td>
<td>Increase understanding of blockchain among ISEAL members by:</td>
</tr>
<tr>
<td></td>
<td>● Building a learning plan most appropriate for sustainability certifications</td>
</tr>
<tr>
<td></td>
<td>● Organise a learning workshop to increase blockchain understanding and to identify the problems / hypotheses to be tested in Phase II</td>
</tr>
<tr>
<td>II - Pilot</td>
<td>Test how blockchain can address the selected problems / hypotheses on a real, sustainably certified supply chain.</td>
</tr>
<tr>
<td>III - Sharing and Replication</td>
<td>Share the results with ISEAL members and the wider public, and discuss the potential to scale the project in the future.</td>
</tr>
</tbody>
</table>

If you’re not familiar with blockchain technology you can check out our [introduction](#) and [FAQ](#).
Defining the hypotheses

During a two-day workshop in September 2017, 15 ISEAL member organisations were introduced to blockchain technology and participated in supply chain mapping and group ideation on the role of blockchain in addressing existing challenges.

The outcome was a series of hypotheses statements to test where blockchain could be useful. These were grouped into five key areas: chain of custody, data collaboration, financial flows, trust in standards, and impact monitoring.

Upon further discussion with ISEAL members, it was decided that two areas in particular, chain of custody and data collaboration, would be examined in more detail.

Selecting the pilot supply chain

To research the hypotheses, the team chose to visit UPM Biofuels Bioverno supply chain. The supply chain was selected due to its applicability and practicality. The supply chain is relatively simple (one country) and holds multiple sustainability certifications. Moreover, UPM Biofuels were interested in the potential of blockchains.
In this section of the report we outline 3 opportunities for how blockchain could be applied to improve the efficiency and credibility of certifications. These 3 ideas for how to apply blockchain have been formed through interviews and surveys with certifiers and businesses, and a research trip, in which the Provenance team observed a dual RSB and ISCC audit at UPM Biofuels, an RSB-certified biofuel producer. Throughout the research we drew on key hypotheses devised during the September workshop. These related to standards organisations harnessing blockchains for verification of chain of custody, cryptographic data privacy and increased data collaboration.

1. Reducing audit inefficiency

Background
Today the number of certification schemes has grown to over 400¹. While there is differentiation among schemes, the sheer proliferation has created overlap among

¹ [http://www.iisd.org/ssi/about/#whyssi](http://www.iisd.org/ssi/about/#whyssi)
requirements. This overlap has led to the duplication of audit efforts as it is common for supply chain actors to participate in more than one certification scheme.

UPM Biofuels, for example, is certified through three distinct schemes: RSB, ISCC and the Finnish national scheme, with 80% overlap on the requirements of those schemes. They have opted to take part in three schemes to satisfy the requirements of different customers and prove industry best practice with regards to sustainability. However, each scheme is audited separately, and the claims auditors verify reside in siloed databases that do not talk to each other.

Standards organisations, auditors, and licensees, are aware that double auditing is inefficient and have started collaborating on audits to help save time and money. At UPM Biofuels, the ISCC and RSB audits were held together for the first time this year. RSB also offers joint audits or ‘top ups’ to businesses who are already certified by Bonsucro, FSC or SAN. Similarly Flocert - Fairtrade’s auditing body - provide joint audits for businesses wanting to be additionally UTZ or 4C certified. These examples of collaboration are indicative of the move to cut down on unnecessary audit efforts and also demonstrate a willingness among certifiers to collaborate.

Suggestion

As there are already examples of cooperation, audits present a good opportunity for blockchain technology to benefit the certification ecosystem. As an extension to current approaches, we believe it would be beneficial to use a public blockchain as the backbone of a collaborative database across certification bodies.

The concept of a microclaim - a granular, independent, digital, cryptographically secure, verified claim - stored on a blockchain is important for this approach. In the context of the UPM Biofuels audit, we identified audit points around management systems, material storage, permits and employee records as good candidates to become reusable microclaims.

1. Auditor A requests documents from the auditee about an audit point e.g “valid employee records”
2. Auditor A submits a microclaim to a public blockchain, for example:
   about: Farmer Bob
   subject: Employee records
   state: Valid
   signature: Auditor A
   supporting: Link to supporting documents

2 Interview with Maria Puustinen, UPM Biofuels
3 http://rsb.org/certification/about-certification/
4 https://www.flocert.net/solutions/standard-assurance/fairtrade-certification/
3. Auditor B wants to verify employee records
4. Auditee provides a link to the microclaim created by Auditor A for Auditor B to check. Actual employee records do not need to be provided again.

Sharing microclaims across a common database would reduce the time taken to audit a company, minimising overlap and providing auditors with more context when auditing a new business. Although general context was available for auditors visiting the UPM Biofuels supply chain for the first time, there is minimal time for them to review this information and examine specific points of interest. This meant that the auditors required a 30 minute to one hour session at each different location to familiarise themselves with the supply chain and specific areas of interest before beginning the audit. Reducing the amount of time taken to gain context on specific concerns would benefit auditors by providing them with time to investigate additional data more pertinent to sustainability.
2. A single source of truth for chain of custody tracking

Background
During sustainability certification audits, one of the auditor’s main tasks is to guarantee the consistency of data along the supply chain. Data about the flow of goods is usually stored on a database private to each node, meaning the same transaction exists in the supplier’s system as an outbound movement of goods and in the customer’s system as received goods.

From our research we have learnt how time-consuming it is for supply chain actors and auditors to track batches of material through supply chains and reconcile the inbound and outbound quantities of products throughout the CoC. Unlike many organisations, UPM Biofuels uses an internal CoC system, however even with a purpose built system it still took time to explain how the system works, collect data in the auditor’s desired format and provide evidence for each sample batch.
**Suggestion**
To overcome this challenge, blockchains could provide a single source of truth for the movement of goods across all actors in a supply chain. Essentially, if items moving through the chain could be tracked on one platform, businesses could easily prove claims to auditors and business partners.

However, when considering a single source of truth system, it’s important to understand the risks linked to commercial confidentiality. Just as these challenges are present in centralised solutions such as PalmTrace\(^5\) by RSPO and Nabisy\(^6\) by BLE, they need to be tackled in a decentralised setup. While centralised systems rely on trust in the central operator, blockchains use cryptography to hide sensitive data.

---

5 [https://rspo.org/palmtrace](https://rspo.org/palmtrace)
I. Tier one: simple commitment by both actors

Encrypted timestamping using digital signatures could be implemented to remove the need for records to be reconciled. This would enable the following scenario:

1. Supplier delivers x tonnes of sustainable material to manufacturer
2. Supplier creates a digital file specifying the type and quantity of the goods delivered, and signs it cryptographically
3. Manufacturer inspects the goods delivered and attached digital file, and signs the file cryptographically to acknowledge receipt of goods
4. A fingerprint of the signed document is published on a blockchain, giving it a timestamp and making it immutable
5. During the audit, the auditor can retrieve the proofs from the blockchain and compare them with records in both the customer’s and the supplier’s systems

This system would enable security advantages over the current system as actors cannot modify their claims after they’ve been entered into the system and digital signatures would guarantee the authenticity of the claims. However, limitations include a lack of flexibility, as the system would not support proving complex claims, such as the absence of double spending. To overcome this limitation we can look to zero knowledge proofs.

II. Tier two: zero knowledge proofs

With the example of the privacy-focused cryptocurrency Zcash\(^7\), blockchains are being upgraded with advanced privacy tools. In particular, zero knowledge proofs used by Zcash itself make it possible to hide transaction details while still enforcing certain rules, such as preventing double spending, or proving an aggregated statement without revealing individual values.

An example application is the evaluation of production yields, which can be highly confidential information. For a given industrial process which outputs certified products only if fed with certified material, an incentive to mix certified inputs with non-certified inputs exists, effectively “laundering” non-certified material. The way to detect such fraud is to compare the annual average yield of the process to standard values - a high yield constituting a red flag. Zero knowledge proofs could be used in this case to prove that the yield is below a given value without revealing processing volumes. In such a setup, actors transfer digital assets associated to the movement of physical goods, with all transaction details being encrypted. Based on those

---

7 https://z.cash/
transactions, a third party can verify that the yield was lower than a certain value, without the yield itself being revealed. A similar process can be used to prove that a batch originates from a certain area without revealing the exact supplier.

While we find this approach very exciting, it is important to recognise that the underlying cryptographic tools are still nascent. They are however very good candidates to underpin the next generation of privacy-preserving digital services.

3. Improving sustainability data reporting

Background
During audits, sustainability certifiers require companies to report on key metrics in order to prove compliance with standards. In the context of the European regulation on biofuels, greenhouse gas (GHG) emissions have to be measured along the supply chain and remain within given limits for the material to be certified. Calculations based on European Union (EU) regulation take into account many parameters covering

odology-v2.1.pdf
processing, storage, and transport. At UPM we observed how GHG emission calculations are calculated separately by each node in the chain. Calculating emissions in this way leads at best to time-consuming verification during audits, and in riskier supply chains this could result in mistakes or fraud.

Suggestion
Considering the GHG emissions example and taking advantage of an existing privacy-preserving chain of custody system as envisioned earlier in this report, GHG emissions could be calculated in real time, in an automated way. This would work in the following way:

- The sustainability standard uploads its framework for GHG emissions calculation as a smart contract running on a public blockchain
- The smart contract is connected to the chain of custody records from the different actors in a supply chain, taking the movement of goods as an input
- The sustainability standard can access the smart contract and update standard values if necessary
- The GHG emissions data is now easily shareable with customers and other actors in the supply chain
This solution could be applied to many other scenarios. For example, certifiers could develop similar smart contracts and require companies to input data on employee wages, waste, water quality, biodiversity and more. In future, this ecosystem could be further developed to incorporate other services such as supply chain finance or existing certifications.

CONCLUSION

Overall, we see that there is potential for blockchain technology to support sustainability standards and make audits more objective and efficient.

Throughout our research we have kept key hypotheses from the September workshop in mind. These related to how blockchain technology could enable certifiers to have verification of chain of custody, cryptographic data privacy and increased data collaboration. Although the scope of this project has not allowed us to draw firm conclusions, we have further defined our hypotheses and believe each of the three suggestions would provide interesting test cases for a follow-up pilot project to be developed in the future.

In addition, many of the introduced technologies are in their infancy - blockchains and zero knowledge proofs are still experimental, but have been under heavy development recently due to growing interest. However, there are still huge benefits that can be achieved today - simple steps such as connecting an existing certification to the blockchain, using digital signatures whenever possible or experimenting with public blockchain based timestamping are already possible.

RECOMMENDATIONS FOR A FOLLOW-UP PROJECT

As blockchain has the potential to address many different supply chain and traceability concerns, it will be challenging to develop a larger follow-up project that is as inclusive and all-encompassing as this one.

Therefore, our recommendations for a larger follow-up project include:

- Focus on a small number of hypotheses (one or two).
- Choose a select group of project partners with similar systems, capacity, supply chains and priority challenges; for example ISEAL members who work with the same products or product categories.
● Engage at least one corporate partner to provide match funding and access to supply chains and systems.
● Integrate the financing of resources needed to implement blockchain, such as hardware, software and HR, in the proposal and budget.
● Integrate a M&E framework to measure success.
● If the project focuses on auditing-related hypotheses, invite certification / auditing bodies to participate.
● Ensure expectations are managed: whilst having huge potential, blockchain is still a new technology that is currently being researched and tested across various applications and industries. It is not yet a proven and neatly packaged market solution. Follow-up projects should therefore keep the emphasis on research & development and work towards the achievement of a scalable blockchain solution for the given hypotheses.

**DEFINITIONS**

<table>
<thead>
<tr>
<th><strong>Blockchain</strong></th>
<th>Check out our <a href="#">introduction</a> and <a href="#">FAQ</a> to learn more.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cryptography</strong></td>
<td>Cryptography or cryptology is the practice and study of techniques for secure communication. It is also known as the art of writing or solving codes.</td>
</tr>
<tr>
<td><strong>Greenhouse gas (GHG)</strong></td>
<td>Any gases which are responsible for causing the greenhouse effect. The most well known greenhouse gas is carbon dioxide.</td>
</tr>
<tr>
<td><strong>International Sustainability and Carbon Certification (ISCC)</strong></td>
<td>A global standards organisation that contributes to the implementation of environmentally, socially and economically sustainable production and use of all kinds of biomass in global supply chains.</td>
</tr>
<tr>
<td><strong>Zero knowledge proofs</strong></td>
<td>Cryptographic tools enabling a prover to convince a verifier about a statement while keeping as much of the data private. For example, the prover could convince the verifier that they are older than 18 without revealing their actual age.</td>
</tr>
</tbody>
</table>