KLEROS

Fellowship

of Justice

LABOR CERTIFICATION ON THE BLOCKCHAIN

Elliot Talbert-Goldstein, PMP

FELLOWSHIP OF JUSTICE PROGRAM 2019

KLEROS

Fellowship of Justice Program

Labor Certification on the Blockchain

Elliot Talbert-Goldstein, PMP

October 15, 2019

Abstract

There are many risks in the steps along the supply chain that bring food from farm to table. For the consumer who buys the end product, for the companies that own the production processes, and for the workers who perform the labor required in fields and facilities. Certification and regulation frameworks that reduce risks for each party while increasing transparency make a major impact on food production and consumption by protecting consumers, workers, and companies. Those frameworks today can be drastically improved using blockchain technology and companies are looking for ways to implement distributed ledgers in order to create new value. The following case study analyzes a real-world example of designing a blockchain application that improves the confidentiality, integrity, and availability of data for the certification for food growers, processors, sellers, and, ultimately, consumers. The research is designed to inform key challenges and opportunities in using blockchain for regulation in the supply chain and regulatory frameworks more broadly.

Introduction

Blockchain technologies have the potential to help usher in the next stage of regulatory frameworks for the businesses of today and tomorrow. Researchers such as Gillian Hadfield and Primavera De Filippi have started to illustrate the "techno-legal tools and frameworks" that can help regulate modern businesses and industries. Hadfield introduces the concept of a competitive marketplace for regulatory bodies which are supervised by the government, instead of the government doing the heavy lifting of regulation (Hadfield, 2017). De Filippi, and her organization, COALA, have a working group investigating questions like "to what extent can blockchain technologies be deployed to achieve regulatory and policy goals?" (Coalition of Automated Legal Applications)

The use of blockchain in audits is also being investigated by professionals and academics. In 2017 a group of public and private organizations, including the US and Canadian certified/chartered public accountant (CPA) associations, released a report detailing blockchain's "potential to impact all recordkeeping processes, including the way transactions are initiated, processed, authorized, recorded and reported." Their final call to action "urge[s] CPAs, including CPA auditors, to continue to monitor developments in blockchain technology" (American Institute of CPAs, 2017). Other research from Rutgers Business School published in *The International Journal of Digital Accounting Research* includes a look at "operationalization and versatility of blockchain smart contracts" specifically as it applies to external auditors (Rozario & Vasarhelyi, 2018).

Why are each of these bodies focused on blockchain as a sea change across industries? According to the AICPA report, blockchain offers

- Near real-time settlement of transactions, which reduces risk of non-payment by one party
- A distributed ledger that contains a public history of transactions, which includes a secure record of proof that transactions have occurred
- Irreversibility, including a verifiable record of every single transaction
- Censorship resistance through economic rules that provide incentives for independent participants to continue validating information, making censorship expensive

In the food supply chain blockchain is emerging as a tool that can be used to improve food safety. Major companies including Unilever, Nestlé, and Walmart have partnered with IBM to integrate blockchain. Their goal is to use blockchain to "quickly trace outbreaks [of food-borne illnesses] back to specific sources. This could help increase consumer safety while limiting financial losses, as only the products directly impacted would need to be recalled" (CB Insights, 2017).

Issues and concerns like these have crucial implications for the future of business, law, and society. They may need to be answered sooner, rather than later, to meet the needs of industry today.

Decentralized Regulation

In order to effectively implement a decentralized system as a solution to such issues, there is still an abundance of work to be done. Development of such tools as part of the "regulatory marketplace," as Hadfield describes it, must overcome the practical limitations of blockchain technology. Problems such as network size, transaction costs, network speed, storage constraints, permissions, centralization, verifying physical data on-chain, and more.

One issue that would provide value to help understand whether technical and contractual means can solve these regulatory issues is the "oracle problem." The oracle problem, simply put, is validating that information from the real world is input correctly into a decentralized data storage system to prevent the risk of "garbage in, garbage out." In the worst case, a certified body could submit false information, meaning that while they are not meeting regulations, they are still certified. An oracle needs to be implemented to resolve this problem, and may be need to be specialized to meet unique, situational needs.

The goal of this case study is to answer questions like these through a practical example of a blockchain-based techno-legal regulatory tool. The final result includes initial plans for a tool to be used by third-party auditors, certification organizations, and regulatory bodies. The research investigated the development of a blockchain application to certify companies that provide a safe, stable, and dignified work environment to farmworkers, based on an existing set of standards. The subject organization, Equitable Food Initiative (EFI), operates a certification system that helps companies implement standards for labor protections on farms, as well as for pesticide management and food safety. Farmworkers suffer mistreatment at an incredibly high rate, ranging from wage theft to sexual harassment to modern day slavery. Consumers, companies, and farmworker advocates are looking for ways to reduce such abuses and improve labor relations in agriculture. A decentralized solution can help verify that standards are frictionless and visible to laborers, employers, consumers and others in the supply chain.

The final result and subject of the case study is a practical scope of work for a labor certification distributed application, or dapp. The scope, developed using project management best practices, will be used as a plan and requirements document for implementation. Additionally, it helps identify and resolve issues like the oracle problem as it pertains to standards and regulations. The analysis below explains the results of the scope, and gives key insight into how organizations might deploy blockchain technologies for regulating industries. The analysis also illustrates some of the key challenges and opportunities, provides a practical tool for implementation, and a resource for further research.

The Case

There are many risks in the steps along the supply chain that bring food from farms to consumers' tables. For the consumer who buys the end product, there is the risk of foodborne illness (Centers for Disease Control & Prevention, 2019), as well as concern regarding how the food was produced. For the companies that own the production processes there are risks of lost product, changing consumer interests, human resource issues, regulatory challenges, the cost of doing business and more. For the workers who perform the labor, risks include injuries and illness (Statistics), lost wages (MHP Salud), child labor (Association of Farmworker Opportunity Programs, 2007), workplace violence (MHP Salud), sexual violence (Kominers, 2015), and human trafficking and slavery (Human Trafficking Hotline, 2015).

There are a variety of regulatory and self-regulatory frameworks that help protect each actor, but for the worker the risk of harm is greatest. One way to protect workers is with the support of a certification system or scheme, and one such system is operated by the Equitable Food Initiative (EFI).

EFI originated as a multi-stakeholder initiative among workers and businesses in the fruit and vegetable sector of agriculture arising from concerns about abusive labor practices that harmed workers and hurt businesses that increasingly feel pressure from consumers about how food is produced. The EFI is governed by a Board of Directors that includes corporate buyers of produce (including supermarket chains and food service companies), growers (farm operators) of produce, farmworker advocates, consumer advocates and environmentalists. The EFI partners with growers and retailers to increase food chain transparency, improve food safety, and create healthier places to work through a certification (Equitable Food Initiative, 2019). Their process includes over 330 indicators that support social, food safety, and pest management standards and are the subject of independent audits by accredited auditors. Working with these companies, EFI's outcomes include skill and capacity development, integrated management systems, organizational culture shifts, multi-stakeholder approaches to systems change, and improved working conditions (BSD Consulting, 2017). A major innovation of the EFI is the establishment on each farm of a Leadership Team of managers and farmworkers that is trained to raise and address workplace issues through constructive means for the benefit of all.

EFI Certification Process

The first step in the certification process is Grower Mapping, where EFI learns about the grower's business and needs. The training and skill development process will be defined to complement your existing structures, systems and staff skills and knowledge.

1. Based on the information gathered in the Grower Mapping process, EFI facilitators custom design and lead a Leadership Team training.
2. Once in place, the Leadership Team works to ensure that the farming operation is in compliance with EFI Standards.
3. When they are ready, the Leadership Team calls for a third-party verification audit from a certifying body.
4. Upon receiving certification, the grower is licensed to use the EFI label on certified produce and charge participating retail buyers a premium that is returned to workers in the form of a bonus.

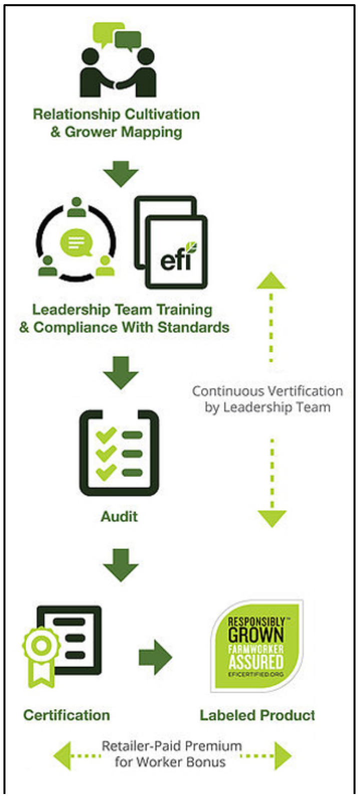
Relationship Cultivation & Grower Mapping
efi
Leadership Team Training & Compliance With Standards
Continuous Verification by Leadership Team
Audit
RESPONSIBLY GROWN FARMWORKER ASSURED
EFICERTIFIED.ORG
Certification
Labeled Product
Retailer-Paid Premium for Worker Bonus

Figure 1: EFI Certification Process

There are three categories of costs associated with the certification process: leadership team training, improvements to comply with EFI standards, and third-party audits (Equitable Food Initiative, 2019). There are two principal mechanisms for ensuring that growers are meeting the standards. One is a traditional audit. The grower is required to retain the services of an approved auditor who independently assess the farming operations of the grower. The audit process is part of what makes the certification "the most rigorous certification in the industry" according to EFI. The audit is a way of ensuring that a grower is meeting the standards set forth by EFI and tailored in the Grower Mapping process. The second mechanism for assuring compliance is the Leadership Team; workers and managers throughout the year, between audits, are expected to ensure compliance and the audits verify that the Leadership Team is operating as intended. The emerging technology native to blockchain offers new tools and techniques that can help improve the effectiveness and efficiency of ensuring that growers are meeting the demands of the standards.

Audit Process

Currently, the audit is a multi-step process that includes the grower, an auditor, and EFI and its stakeholders. Audits are initiated to provide the certification for a grower, and occur regularly to maintain the certification. The auditing company sends an auditor to the site of the grower's operations. The identity of the auditor is not known to the grower in advance. The auditor performs a number of functions including reviewing documentation, payment, conducting interviews with workers, managers, and leadership, inspecting facilities and observing operations. This evidence is captured and submitted to EFI for review. EFI reviews the reports internally including getting input from subject matter experts. If there are any nonconformities, the grower has 30 days to submit a corrective action plan. Once the corrective action plan allows the nonconformities to be closed, the certification is issued by the third-party auditor. The grower can then notify its customers, including corporations that purchase and sell food to consumers, that it is meeting the EFI standards, which provides the corporations with assurances they are seeking in their supply chains. The grower may also use the EFI label on their packaging to demonstrate their compliance with EFI's certification system. The EFI system includes a system by which a premium is paid by the corporation to the grower for the certified produce and most of the premium is then distributed to workers.

The current audit process is time consuming, costly, and has limited protection from malicious behavior by the grower. Despite significant safeguards in the audit and Leadership Team processes, a bad actor can defraud the process to become certified without meeting the standards or can violate the standards after becoming certified, at least until the next audit. In addition, growers report "audit fatigue" due to multiple certification systems and many in good faith request EFI and others for greater efficiency. Moreover, farmworkers take on additional responsibilities under the EFI and, despite very positive worker feedback, there are concerns that the workers' time and other costs are substantial but are not adequately compensated. As of June 30, 2019, EFI has certified 31 locations, which represents 29,080 workers. As the organization continues to scale, the inefficiencies and risks will only continue to grow.

At the same time the EFI is expanding to additional growers and corporations in the food sector, food industry leaders are investing in blockchain to support food safety (CB Insights, 2017). EFI has the opportunity to take advantage of emerging blockchain technology to improve their outcomes while meeting major interests where they are.

Research Questions

How can blockchain contribute to a safer, healthier, and more transparent food supply chain? How can decentralized applications provide a more safe, stable, and dignified work environment to farmworkers? What are the technical challenges associated with regulating companies? What broader obstacles must be overcome for applications like this to extend to other commercial and industrial sectors?

Research Foundations & Methodology

This project began as a proposal for the Decentralized Justice Fellowship sponsored by Kleros, a blockchain dispute resolution company. The Business Track of the fellowship is meant to focus on use cases of Kleros and business models in the field of decentralized justice. “Kleros is a decentralized application built on top of Ethereum that works as a decentralized third party to arbitrate disputes in every kind of contract, from very simple to highly complex ones” (Lesaege, Ast, & George, 2019). Research for the fellowship began on July 15th, 2019 and concluded October 15th, 2019. Kleros, which currently operates a number of dispute resolution mechanisms for a variety of use cases, aims to grow the application to meet the needs of multiple industries and has enlisted the support of its fellows from across the globe to discover new uses and drive product growth.

The research proposal, titled “Practical Challenges in Implementing Regulatory Methods and Technologies on the Blockchain,” was designed with Equitable Food Initiative in mind after a conversation with the Executive Director indicated that they were looking into blockchain technology to address the stated interests and meet the needs of various stakeholders and to improve the system’s outcomes.

The subject of the research is the definition and requirements for a proof of concept of a decentralized (blockchain) application that would meet the needs of EFI in regards to the case described above. In order to develop the final document, a scope of work, we relied on the Project Management Institute (PMI) Project Management Body of Knowledge, which outlines best practices in managing large projects. Based on this framework, we completed key aspects of the Initiating and Planning phases in order to create a document that could be used in a future software development project (Project Management Institute, 2019). Steps included collecting information; understanding the business case and benefits management; uncovering initial requirements, assumptions, risks, constraints, and existing agreements; assessing project feasibility; creating measurable objectives and success criteria; defining and prioritizing requirements; and creating the project scope statement. These steps, and others, were completed with EFI staff including the Executive Director, Director of Certification and Impact, and Senior Impact and Information Management Officer. The final documents were approved by these parties and their goal is to use them to create a future blockchain application.

By working closely with an entity that is interested in blockchain and envisions a real-world application for it, then creating a final result with practical use, this qualitative research can help answer the research questions defined above. The analysis is not based on hypothetical situations, but instead relies on the answers of subject matter experts in the field who ultimately need a working application in order to meet their organizational objectives and improve outcomes. The results avoid the traps associated with conjectural blockchain use cases, for example, seeing every problem as a nail and blockchain as the hammer. Practical obstacles like costs, adoption, understanding, and accessibility all arose in the creation of the scope of work, which gives excellent insight into the needs of the EFI, its diverse stakeholders and the regulatory community as they pursue these types of tools. Additionally, by using an industry framework provided by PMI, we can be sure that the resulting documentation is accurate, covers the actual requirements of EFI (the project sponsor in PMI parlance), and is therefore a reliable subject for analysis.

Any solution developed in support of EFI's objectives will need to offer options for redress if and when disagreements arise. A dispute resolution system that can be integrated into any smart contract implementation has near-ubiquitous uses. While most disputes that might arise in the course of the grower's operations can be handled with negotiation in the Leadership Team or audits, with the support of EFI's expert staff, a tool that can gain the trust of all parties to resolve disputes with the support of a neutral party and with little investment from either side is a great opportunity. This paper concludes that the Kleros dispute resolution protocol would be a valuable tool.

The final result, a scope of work and requirements definition for the "EFI Audit Document Capture Proof of Concept," Appendix A, was the product of a series of meetings and planning process. It is a narrow planning document that will ultimately be used in creating a suite of blockchain tools. By starting with a proof of concept, it will help determine the feasibility of future tools, and, once completed, provide additional insight to EFI in how to develop those tools most effectively.

The process, which included fundamental project management initiating and planning processes, began with open-ended discovery activities. These activities relied heavily on concepts like design thinking, such as those described by Margaret Hagan in her e-book, Law by Design (Hagan). It also included extensive stakeholder identification, in order to uncover potential requirements and obstacles that could arise throughout the project. The goal, defined early on, was to “create a Scope of Work (SOW) for a proof-of-concept (POC) of a blockchain-based certification platform based on EFI’s standards.”

Results & Analysis

Stakeholder Analysis

The first stage in planning a solution was determining stakeholders. This iterative process begins early on and is meant to be exhaustive in order to identify all potential requirements. Frequently, a project with many stakeholders runs into problems late in development because a key person or group was not included and their requirements have not been met. For this project, EFI identified a number of stakeholders throughout the supply chain, and taking their interests into account we identified multiple core requirements, without which, the project could not succeed. Later on, in future planning it will be crucial to get further input from those stakeholders to ensure that their more specific requirements are included.

Broadly, stakeholders fall into a number of categories. These include workers, managers, and leaders who work for the grower’s company. External to the grower are their customers including processing facilities, which can also be certified, and the customers, which are food retailers like grocery stores and restaurants. Among the customers are larger customers like national and international chains, and smaller customers, such as independent businesses. Growers also work with farm labor contractors and recruiters in order to hire workers. Outside the supply chain and connected to EFI are also the auditors, who work with the two auditing companies that have been selected for the certification. EFI also maintains a multi-stakeholder board which includes various subcommittees. Other external stakeholders include trade associations and government agencies, as well as individual consumers.

These stakeholders are engaged regularly by EFI and so we were able to generate eight requirements-as-known.

1. Allow certification bodies to perform audits that ensure auditees are adhering to applicable standards – for example, payroll documentation
2. Allow EFI & certification bodies to issue certification to companies that meet requirements
3. Reduce costs and time associated with certification process
4. Create immutable record of audit including evidence, documents, interviews, observations, processes, procedures, etc.
5. Help ensure that workers are getting paid quickly and accurately
6. Prepare for data interoperability and integration (DII) with other blockchain applications both internal and external

7. Maintain all records with security (permissions, privacy) as required by stakeholders
8. Meet accessibility needs of all users including ease-of-use, language, offline access, text/image/voice operability, and more

A longer register of stakeholders that includes their input, and analysis of their influence and interest, and more detailed requirements will be necessary at a later stage.

Initial Concepts

Towards the beginning of this process, the EFI team sought a perfect solution that would help their process by ensuring that all 330+ standards were being adhered to by growers. Identifying a value proposition for them short of that meant reviewing some of the key functionality that blockchain offered. By explaining in simple terms what the capabilities and limitations of blockchain included, we were able to proceed to develop more defined concepts that would still yield returns. This was a core learning that was valuable in planning blockchain implementation broadly. Limiting the scope of a potential project with non-technical staff requires digestible explanations of what can and cannot be done on decentralized systems, as well as what should and what might be suited to other technology like traditional databases.

The first product idea was a solution that could help give farmworkers an immediate return on their investment in the EFI in the form of a bonus paid from a premium paid on products sold. Part of the advantages of the certification for growers is that they negotiate a premium with their customers, which means more profit. However, a substantial portion of that premium must be paid to workers as a bonus. Calculating the amount of the premium on the grower's diverse products and the resulting worker bonus and verifying that it was paid appropriately to workers is incredibly challenging.

This concept had two major advantages and some potential obstacles. First, it took advantage of blockchain functionality by automating payments. This could mean a major improvement in outcomes for farmworker constituents. Second, it provided a verifiable record of transactions, meaning it could generate new efficiencies in the audit process. Ideally, auditors would not need to review nearly as much documentation to ensure that these payments were made appropriately. The first major disadvantage of this proposal is that this solution would have to layer on top of existing payroll systems. Today, no commonly used payroll software supports blockchain tools, so it was likely that a new integration would need to be developed, likely at great expense. Additionally, this could mean additional new training for payroll staff in order for them to use new software. Second, the value proposition for the grower did not seem immediately clear. The farmworkers might see the benefit, but it would likely be at great expense to the grower in terms of implementing new software and providing training to staff. In addition, growers will be concerned with confidentiality regarding their operations and their labor practices. Convincing them to get on board with this idea loomed as a key obstacle to any concept.

Another potential, and crucial, obstacle that arose was that this might require the involvement of farmworkers, not just leadership. While it seems that this solution might benefit the farmworker, there is still an issue of trust. They now need to trust that EFI is going to make good on this promise. If the project is not successful, EFI could fail to meet its objectives and ruin relationships. In short, the best intentions of EFI are not enough for workers to rely on.

Immediately, the challenges of getting buy-in from both of these stakeholders became obvious. The final application would need to provide business value to the grower and meet the needs of the farmworkers. It also could not require a substantial investment in time or resources from either party, and needed to mitigate the risk of impeding EFI's objectives should it not perform as expected. Although the corporations that sell the produce and the consumers who seek assurances about the supply chain might be willing to contribute toward such costs, it was far from clear that they would finance such expenses.

Fortunately, there was a key planning activity that was crucial, and without which, critical mistakes could have been made. This was the identification of stakeholders. Because this had been done early on as part of the project management best practices, we were able to review the requirements of all stakeholders and were alerted quickly to the fact that this concept may not be the right direction to go.

Another key development happened at this phase which led to a change in direction. While it seems unique to this project, it is inherent to any large project. Behind the scenes, EFI was working on changes to the way that premiums were calculated. This meant that continuing on with this concept might have proved fruitless. They immediately called for a hold on this idea and we moved forward with what ultimately became the final concept.

Document Capture POC

Focusing on the core concept that the final product would need to offer a crucial value proposition to any party that would need to participate, we circled back to one component that had arisen from the original concept: making the audit process more efficient. Immediately, it became clear that a blockchain application might be able to solve two problems, reducing the cost and resources associated with the audit process while increasing the integrity of the audit evidence.

The final proof of concept, EFI Audit Document Capture, defines an application that performs four key operations on audit documents: (1) upload, (2) explore, (3) compare, and (4) multi-source upload. The document upload capability uses a secure environment that minimizes the risk of file tampering and will support the confidentiality and integrity of documents that need to be audited. The document explore capability will support the availability of documents for audit purposes, without compromising confidentiality or integrity. The document compare and multi-source functionalities help the auditor determine whether a document has been tampered with. Ultimately, each of these tools helps improve information security for the auditors and growers by ensuring document confidentiality, integrity, and availability.

This concept stood up to the obstacles previously identified. It offered a value proposition to growers in that it saved time and money in the audit. While the auditor would have to learn a new application, the current platform for collecting evidence does not offer convenient user experience, so a new system could be built with their needs in mind. For the farmworkers, their processes are not impacted, and the end result for them is improved performance in EFI's existing system and potential expansion of the system to many more farmworkers.

It also met the needs of a new obstacle, physical documents. Much of the farming industry is still a paper-and-pencil system. In order for a blockchain application to work, particularly one that requires auditing of documents such as contracts, physical documents need to be supported. Another obstacle is the issue of confidentiality for the growers' operations. While the certification does require them to be transparent enough to prove that they are compliant, they are still entitled to maintain business secrets that are core to their operations. Forcing them to share private details of their operations could be a showstopper, and any new tools would have to be compatible with that need.

The final POC supported a number of use cases, (Appendix A) including legitimate and malicious document upload and audit for both digital and physical documents.

Core Technology Identified

During the planning phases for the audit document capture we identified six core decentralized technologies that could have an impact on the certification process (Appendix B). While not each of these ended up in the final result, they could have a place in a larger suite of tools built to meet the needs of EFI. The final scope was narrow enough that it was achievable, and these tools represent the broader ecosystem of blockchain technology that might drive improved outcomes going forward.

1. Oracles – smart contracts and auditors rely on real world data to operate. However, malicious parties can easily add incorrect data, so we use Oracles to improve integrity. The simplest way to reduce false data reporting is to have an oracle aggregate multiple data sources. Auditees can enter the same data from different sources, both internal and external, in order to prove to auditors that the data is correct. Eventually it may be possible to collect data from other parties, like workers and Leadership Teams, as well.

2. Internet of Things (IoT) & Smart Devices – Smart devices are used to capture data and measurements on-site and can relay that data directly to the blockchain. This automatic process helps ensure integrity and saves time. Smart devices can also be secured from tampering using Trusted Execution Environments.

3. Enclaves & Trusted Execution Environments (TEE) – Enclaves, also known as TEEs, can be used to ensure data is computed correctly and without tampering. This hardware-based technology can be trusted to operate correctly even if a device is compromised. Because data coming from this device can be trusted it makes a great tool for smart devices and performing calculations that are at risk for malicious behavior.

4. Zero-Knowledge Proofs & Calculations – Zero-Knowledge proofs allow one party to prove to another that data is accurate without actually revealing that data. This is useful for stakeholders, like growers, who want to prove that they have calculated something correctly, like wages, but don’t want to reveal private information in that calculation.

5. Immutable & Secure Storage – Immutable storage means that once information is uploaded, like a document, it cannot be changed or removed. This is useful to ensure that crucial pieces of information have not been tampered with. In addition to immutable storage, these same files can also be encrypted and stored securely so that only those with the right permissions can access them.

6. Dispute Resolution – Dispute resolution is not a new concept, but providing a platform that can integrate with the above technologies is. A dispute

resolution protocol that is based on blockchain technology can mean that if any of the rendition technologies fail, there is a mechanism for remedy.

The combination of these tools, while out of scope for the current project, could be put together to create a secure system for audits and certification.

Oracles and Real World Data

The current POC has limited support for oracles that can ensure real-world information can be trusted once it gets entered into a decentralized application. Thus, to scale, these applications may need to offer more functionality that helps auditors, EFI, and consumers ensure the rigor of the certification. Accepting documents from other sources such as from the workers, managers, leadership, and even whistleblowers, without adding workload could help improve the efficacy of the audit and protect the interests of all parties while reducing costs.

Some obstacles to generating data from other constituents include issues of accessibility for language and literacy, developing trust in the application, protecting the identity of whistleblowers, meeting technical requirements such as offline access and device specifications, and proving the integrity of submitted documents. However, if new tools can be created, either through hardware or software, there would be new efficiencies and improved outcomes.

Dispute Resolution

In many ways, this entire application can be seen as a conflict management tool, meant to balance the needs and requirements of multiple stakeholders in order to ensure that all parties meet their objectives. In practice, there will still be disputes that arise, around wages, results, actions, and other things that negatively impact one or more stakeholders. In order to address those conflicts, there must be a system in place to resolve disputes and create solutions that are beneficial for any party affected. While some of those processes can be interpersonal, such as negotiation, others may require additional attention, such as with the help of other staff or, for example, technology. Blockchain can help disputants by providing a platform to address a dispute that can be balanced, transparent, and private.

A blockchain tool could help workers report infractions anonymously, instead of worrying that their reports could result in retaliation. It would provide a simultaneously private and transparent method of reporting issues in the workplace.

Observers could see the dispute and its results, but the identity of the parties involved could be protected if necessary. Another example is mediation or arbitration, where a platform could be used to help disputing parties submit evidence and work with an independent third-party to come to a solution. This third-party could be compelled to be unbiased to ensure a fair result using a protocol like that provided by Kleros. These are just two examples of the ways that disputes could be resolved with the support of future versions of the application, and there are likely many other opportunities to provide mutually beneficial results.

Unanswered Questions

There is a lot that is not covered by the final plan. Some of this is by design, some is nature of the stage at which the process has been completed thus far. First is the final platform. What distributed environment will this dapp live on? This is a discussion that will be need to be made not only with the developers who implement the application, but also the broader stakeholders in the project. If the key need is interoperability with existing systems, the choice may be to work with Hyperledger, which so far seems to be the choice of the food supply chain industry. If the goal is open participation by the public, such as consumers, Ethereum may be the right choice. This is likely going to be one of the next decisions that need to be made before the project can progress and will require the input of technical experts and stakeholders.

Conclusion

Blockchain solutions that support regulatory frameworks can take advantage of the unique capabilities of distributed databases to permanently and irreversibly record transactions and make those records securely or publicly available, based on need. This technology can support a sea change in audits, certification, and regulation. Customizing a blockchain implementation to meet the needs of a specific industry, however, will be the critical challenge. And developing a tool that capitalizes on the nature of the technology without compromising the needs of stakeholders is also crucial. A sectoral approach will most likely be necessary, creating a patchwork of tools that companies can use in order to meet the needs specific to their work, and that can be evaluated, monitored, and approved by a body of subject matter experts in that field.

Equitable Food Initiative is actively seeking ways that they can improve their ability to certify companies and blockchain does appear to provide resources that can improve outcomes. In this project, we were able to formulate a series of blockchain-based tools to create a software suite that will be used to assure that companies are meeting the requirements of a certification. The certification process as it exists today is rife with technological, logistical, cost, and fundamental obstacles that make it hard to implement and maintain.

Although this research was limited to a specific type of certification in one industry, there are clear applications of this tool in other certification, regulatory, and audit processes that could be employed. There are six core functions outlined: oracles, internet-of-things devices, trusted execution environments, zero-knowledge proofs, immutable & secure storage, and dispute resolution. Together, this constellation of distributed application capabilities provide an excellent foundation for how audit and assurance technologies can take advantage of blockchain and distributed systems to improve outcomes. Finally, organizations or entities that are seeking to implement blockchain to meet their regulatory needs should be sure to employ project management best practices in order to realize a solution that meets their needs and the needs of their stakeholders.

Appendix A: EFI Audit Document Capture POC

Document Capture Application Scope

A decentralized application that provides the capacity for growers to upload documents and records that can be explored remotely by auditors in advance of an in-person, physical audit. The application should provide confidentiality for the content of the documents being entered, while demonstrating the integrity of those documents, and make them available to auditors.

Requirements

Document Upload

The document upload capability will support the confidentiality and integrity of documents that need to be audited. It should be based on a secure environment that minimizes the risk of file tampering.

1. User-friendly GUI that allows growers to upload a variety of file types and documents into decentralized storage
2. A secure environment that supports 2 types of file uploads
    a. Digital-only files
        i. Documents exported from software (such as CSV, Excel, and PDF) directly into a secure environment
        ii. A cryptographic hash of the file is created that can be used as a unique identifier
        iii. Documents will be flagged if they are modified before being uploaded or if multiple versions are submitted
    b. Scanned files
        i. Documents that are printed or pen/paper based (such as signed contracts) are scanned into a secure environment
        ii. A cryptographic hash of the file is created that can be used as a unique identifier (this will not be as useful for a scanned file)
        iii. Critical documents that are scanned and uploaded can be checked against the original, physical version in situ
3. The system should allow multiple files from multiple sources to be uploaded and associated with a single document or entity to improve integrity for critical documents (multi-source)
4. Logs of document creation and modification should be recorded in a decentralized database such as on a public or private blockchain

Document Explore

The document explore capability should support the availability of documents for audit purposes, without compromising confidentiality or integrity.

1. User-friendly GUI allows auditors to access documents and review them
2. Users should be able to examine
    a. Entered documents
    b. Upload logs
    c. Modification logs
    d. Metadata including how the document was created and what secure environment it was submitted from
3. Users should be able to make notes for later use
4. The system should also offer a compare function which allows auditors to upload a file themselves to compare it to a document previously uploaded by a grower
    a. For digital-only documents, this will allow auditors to perform the same export/upload process in situ to see if they get the same resulting unique ID. If any modifications have been made to the document, the content identifiers (created by a cryptographic hash) will be different
    b. For scanned files, auditors should request the originals to compare with the uploaded version for a visual inspection

System-wide requirements

1. All data, including documents and metadata, should use decentralized infrastructure that supports integration & interoperability with other decentralized systems such as Hyperledger Fabric and Ethereum Virtual Machine
2. Permissioned access for all users with username and password and various levels of read/write access
    a. Optional two-factor authentication
3. Logs of all user access
4. Ease of use for all users
    a. English and Spanish language
    b. Accessibility best practices
5. Support for future iterations and additional functionality including
    a. Data entry from other devices, such as IoT hardware
    b. Integration with other decentralized applications e.g. data sharing
    c. On-chain calculation and data processing such as zero-knowledge proofs
    d. Other secure environment implementations such as TEEs

Use Cases

Legitimate Document Upload

The user, which is a grower, is planning to upload documents ahead of an audit, 50 documents have been selected for the upload. Half of the documents can be exported in various formats from software and half are on paper and will need to be scanned.

The user starts by exporting the digital documents. The user logs into each software and locates the data that needs to be exported. The data is exported using the software's native functionality to a folder managed by the Document Capture application. In the case that data cannot be exported directly into the folder, the user will move the file into the Document Capture folder. The system will indicate whether the file has been opened or modified before going into the specified folder. The Document Capture application will allow the user to select what required document the files will be associated with. After the files have been uploaded, the user will receive receipts with the metadata associated with each file, including its unique ID and will be able to login to the Explorer tool to see the files uploaded.

Next, the user scans physical documents. Each document is scanned and sent to the Document Capture folder. The system will flag any file that did not go directly into the folder after being scanned. The user will be able to select which document the files will be associated with including if multiple files should be associated with a particular required document. The user will receive receipts for each document uploaded and the metadata associated with each, including the unique ID. Additionally, the user can login to the Explorer to see the uploaded files.

Audit of Legitimate Document Uploads

The user, an auditor, will login to the Document Explorer and can see an overview of all documents that have been uploaded. The user can begin reviewing those documents and make any necessary notes and record them as evidence for the audit. Documents that were not submitted properly including files that have been modified or uploaded from an unknown source will be seen as flagged for further review. The user can make note of specific files to be reviewed in situ.

Later, the auditor arrives physically on site. Any files on which he needs to perform additional checks can be handled in a variety of ways. At a minimum, the auditor can perform a visual inspection of the file, whether digital or physical. For digital files, to verify integrity, the auditor would be able to export the file in the same way that the grower exported it. That file could then be imported using the compare functionality. If the file has been tampered with, the compare tool would alert the auditor. For physical files, the auditor could compare what was uploaded versus the physical document. Additionally, the grower can submit multiple supporting documents that demonstrate compliance. If the documents have not been tampered with, or if any modifications are legitimate, this process will raise no issues.

Malicious Digital Document Upload

The grower has some information that, if shown to an auditor, could affect their certification status. So, they decide to alter it. There are a few options for how to change the information ahead of the audit. First, the grower could go into their system, change the information, export the data, and upload it. After uploading, they could go back into their system and change it back to the correct information. Alternatively, the grower could export the data, edit the exported file, and then submit it for upload. A third way would be to maintain a shadow system that only tracks incorrect, malicious data, designed to circumvent the audit and certification process.

In this case, the grower decides to tamper with the information using the first two methods on two different files. On the first file, a series of numerical values are changed in their software. The file is exported/created directly into the Document Capture folder, and the user changes their system back to the original values. However, this change does not coincide with a second file, so they must alter this one as well. However, this is a PDF and can only be edited on their computer. So, the file is exported from its native system, modified using a PDF editor, and then saved to the Document Capture folder. The files are uploaded and associated with their corresponding documents. The user receives a receipt of the files upload, including the unique ID, and all the data is in the system for the auditor to check.

Malicious Digital Document Audit

The auditor is examining documents in the system using the Explorer functionality. One document has been flagged because it was not entered directly into the

Capture folder before uploading. The auditor continues to review the additional documents, focusing on other files that might indicate whether this flag indicates tampering. While no additional files show evidence of tampering in the Explorer, the auditor has identified certain files to confirm when he arrives that the grower's location.

The auditor arrives on site and begins by reviewing the flagged PDF file. The auditor exports another version of the file from its original system. The auditor can't immediately see the differences, so he uploads the file to the comparison tool. The comparison indicates that the files are different. The auditor takes a closer look and finds the differences.

Now, the auditor will continue to review key files that will indicate whether the flagged file has been tampered with deliberately to change the outcome of the audit. While working with personnel from the grower's office, the auditor uploads files from the grower's computers using the comparison functionality. Various files are exported and uploaded, and they match. However, one document is uploaded and the resulting metadata does not match a document that was submitted in advance. The auditor visually inspects the recently exported file with the original upload. The newly exported file does not match the original upload. The auditor goes into the software where the file came from and does a final review, clearly showing that the most recent export is correct. The auditor has now identified two files which were clearly tampered with.

Malicious Physical Document Upload

A file with handwritten information exists that threatens the grower's certification. It must be scanned into the Capture system, but the grower decides to change the information before uploading. There are a few options. First, the file could be scanned outside of the Capture tool, then edited before uploading. Second, the document could be edited by hand. Third, a file could be completely falsified using physical means, then scanned and uploaded.

In this case, the grower decides to tamper with the files using the first two methods on two different files. The first file was a printed document that was signed in-person, but the information on the file needs to be changed. So the grower scans the file to their computer and edits the document using a PDF editor. The file is then printed and scanned into the Capture folder. The second document is missing a signature, so the grower forges it. The document is scanned directly into the Capture folder. The files are uploaded and associated with their corresponding documents. The user receives a receipt of the files upload, including the unique ID, and all the data is in the system for the auditor to check.

Malicious Physical Document Audit

The auditor is examining documents in the system using the Explorer functionality. One document has been flagged because it was not scanned directly into the upload folder. The auditor continues to review the documents but sees no other potential tampered documents.

On site the auditor examines the flagged document. The file looks like it has been printed and edited before being scanned. During the rest of the process, he finds no other evidence of tampering, all uploaded documents are compared and the results match. However, during worker interviews, some evidence does not align. The auditor reviews signed contracts and presents them to workers. One contract has been signed but it contradicts an interview.

The auditor has now identified two potential documents that have been tampered with.

Multi-Source Documents

One particular document has been the cause of concern between a grower and an auditor in the past. The grower wants to demonstrate as easily as possible to the auditor that they are not tampering with the evidence. So, they upload six files, both digital and scanned, connected with a single document to be submitted as evidence. Each file is submitted properly: digital files are exported directly to the secure environment, and scanned files are scanned directly into the secure environment.

When the auditor is reviewing the documents in advance, she already knows that this particular document might raise some concerns. Now that there are 6 files supporting the evidence, she can review them and confirm their validity. When she arrives on location, she only validates one of the documents, saving both parties time.

References

American Institute of CPAs. (2017). *Blockchain technology and its potential impact on the audit and assurance profession.*

Antonopoulos, A. M., & Wood, D. (2018). *Mastering Ethereum: Building Smart Contracts and DAPPS.* Sebastopol, CA: O'Reilly.

Association of Farmworker Opportunity Programs. (2007). *Children in the fields.*

BSD Consulting. (2017). Driving Change Across Agricultural Systems. Retrieved from https://equitablefood.org/wp-content/uploads/bsd-consulting-2017.pdf

CB Insights. (2017, December 13). How Blockchain Could Transform Food Safety. Retrieved October 6, 2019, from https://www.cbinsights.com/research/blockchain-grocery-supply-chain/

Centers for Disease Control & Prevention. (2019, September 11). Highlights from the 2017 Surveillance Report. Retrieved September 29,, 2019, from https://www.cdc.gov/fdoss/annual-reports/2017-report-highlights.html

Coalition of Automated Legal Applications. (n.d.). Retrieved from https://coala.global/working-groups/

Equitable Food Initiative. (2019, September 29). *Equitable Food Initiative*. Retrieved from https://equitablefood.org/

Hadfield, G. K. (2017). *Superregulation: competitive approved private regulators.*

Hagan, M. (n.d.). Law by Design. Retrieved October 5, 2019, from http://www.lawbydesign.co

Human Trafficking Hotline. (2015, September). *Labor Trafficking Story | Agriculture*. Retrieved from https://humantraffickinghotline.org/resources/labor-trafficking-story-agriculture-sergio

Kleros. (2019). *DISPUTE REVOLUTION: The Kleros Handbook of Decentralized Justice.*

Kominers, S. (2015). Working in Fear: Sexual Violence Against Women Farmworkers. Retrieved from http://www.oxfamamerica.org/static/media/files/Sexual_violence_against_women_farmworkers_full_doc.pdf

Lesaege, C., Ast, F., & George, W. (2019, September). Kleros Short Paper v1.0.7. Retrieved October 6, 2019, from https://kleros.io/whitepaper.pdf

MHP Salud. (n.d.). *Farmworkers In the United States*. Retrieved from https://mhpsalud.org/who-we-serve/farmworkers-in-the-united-states/

Project Management Institute. (2019). A guide to the project management body of knowledge (PMBOK guide). (6th). Newton Square, PA.

Rozario, A. M., & Vasarhelyi, M. A. (2018). Auditing with smart contracts. *The International Journal of Digital Accounting Research* , 1-27.

Sheppard, S. M. (Ed.). (2011). *Bouvier Law Dictionary.* New York: Wolters Kluwer.

Statistics, B. o. (n.d.). *Occupational Handbook: Agricultural Workers* . Retrieved from https://www.bls.gov/ooh/farming-fishing-and-forestry/agricultural-workers.htm#tab-3

Stewart, W. H. (2016). *Alabama Politics in the Twenty-First Century.* Tuscaloosa, AL: The University of Alabama Press.