MINESPIDER

Protocol for Supply Chain Due Diligence

v.0.33a

Nathan Williams

Abstract

The following white paper outlines the Minespider blockchain protocol for supply chain integrity for raw materials. Responsible sourcing has become a top priority issue for the raw materials industry, with special focus on conflict free minerals, child labor, and proper environmental stewardship. Proper supply chain due diligence is essential but brings into opposition a number of conflicting interests:

- Upstream due diligence costs are borne by upstream suppliers instead of the downstream users who benefit from the data
- The costs of responsible sourcing act as a negative incentive for small scale producers to participate
- Competing companies often wish to use their own system to avoid having their supply chain data visible to competitors, resulting in multiple competing systems that are not interoperable,
- Companies acting as independent trusted third parties for audit purposes gain a large amount of control over the industry if they gain access to large amounts of supply chain data

To address these issues we propose an open, interoperable blockchain protocol. Data collected will be stored as encrypted self-sovereign data packets, under complete control of the data owner. The protocol itself will be largely data agnostic, allowing companies freedom to use any service provider they choose for certification and access to the protocol, however the data collected by the Minespider DApp will be structured according to guidelines developed by the Responsible Minerals Initiative.

Core principles

- The protocol for responsible blockchain sourcing must be open source, interoperable and decentralized
- Supply chain data must be self-sovereign. Neither Minespider nor other actors on the platform should be able to access supply chain data they do not own
- The protocol should incentivize all responsible supply chain actors to adopt it as a standard
- Small companies should be able to use the protocol as easily as large ones

Throughout this white paper we will focus on conflict mineral due diligence, as this is a topic of primary concern and a critical beachhead market for the transformation of the raw materials industry. Our aim remains, however, to construct a protocol and platform that is malleable to all forms of responsible sourcing for fungible commodities.

Introduction

There is increasing focus on the need to perform supply chain due diligence for the raw materials in our consumer products. When metals that we use in our manufacturing processes are mixed with metals from conflict zones, we can end up inadvertently funding armed conflict, slavery and child labor. Gold, tin, tantalum,

tungsten, and more recently cobalt have been identified as problematic minerals that are critical to the global supply chain but have contributed to funding the Congolese civil war which has killed over 5.4 million people as of 2008 when the statistics were compiled.

The OECD has written due diligence guidelines for responsible sourcing, and the US and the EU have both passed conflict minerals legislation, however there have been two unintended consequences from these actions:

1. Responsible companies have attempted to stop sourcing from conflict areas, leaving the non-responsible actors active, compounding the problem.
2. The cost of gathering due diligence data has fallen on the miners in poorer regions. This creates a negative incentive for sourcing legally, as these miners receive the world market price for their minerals, while having to incur increased costs.

Some industry players have experimented with blockchain due diligence schemes already in order to track their supply chain. These first pilots are promising but have highlighted some challenges:

1. Raw materials are fungible and cannot be easily identified uniquely.
2. Individual downstream companies do not want their competitors to see their supply chain data.
3. Many of these systems only take into account the needs of Large Scale Miners (LSMs) whereas the Artisanal and Small-scale Miners (ASMs) are where the abuses happen.
4. Most systems focus on one metal instead of offering a cross-commodity solution

Our proposed solution is a single, open, blockchain-based system that meets the following criteria:

1. **Data self-sovereignty:** A company will own and see their own supply chain data but not anybody else's. Only the data owner has access to their data
2. **Decentralized:** No one for-profit entity will garner fees from the system, or be able to see the supply chain data. Data will be submitted to the system via a DApp, and any entity can build their own specialized DApp. Moreover, no one party will have sole authority to authorize which DApps are recognized as responsible, but rather governance for DApp recognition will be overseen by a decentralized body of stakeholders.
3. **Mass-balance:** The system needs to account for unique tagged-container systems as well as mass-balance in order to ensure the system is able to be scaled.

This whitepaper details how the system will function, it's technical specifications, limitations, and our implementation plan.

The challenge of conflict minerals

Background

The United States was the first country to implement conflict minerals regulation; section 1502 of the Dodd-Frank act, requires companies to perform due diligence on four metals in their supply chain, gold, tin, tantalum, and tungsten. The mining proceeds of these materials, particularly tin, are known to be financing

armed conflict and in particular are known for fueling the decades-long civil war in the Democratic Republic of Congo (DRC).

There have been two unintended consequences of section 1502 of Dodd-Frank:

1. Collecting due diligence data is expensive and the cost burden falls on the mineral producers, resulting in a disincentive for responsible participation when they could sell illegally for more money.
2. The regulation specifically targeting DRC has made some companies who want to source responsibly withdraw from the region altogether in order to not contribute to the problem. This leaves more of the market to be controlled by companies who do not prioritize responsibility, making the problem worse.

Any traceability solution for responsible minerals must be designed in such a way as to avoid these unintended consequences if it is to be effective in the long term.

In 2017, the European Union signed into law their own conflict minerals legislation with the aims of avoiding these unintended consequences further deepening the market for minerals traceability. This legislation will have wide reaching effects and will come into force January 1 2021 giving companies time to find and adopt solutions.

Industry attempts to address the problem

It is a common misconception to think that conflict minerals legislation is burdensome regulation imposed on enterprise by government regulators, in many cases companies themselves have pushed for a regulatory framework because non-compliance risks not only legal consequences but dangers to a company's brand if human rights abuses or other improper production practices are present in their upstream supply chain. According to The Wall Street Journal, the cost of conflict mineral due diligence in 2014 alone reached 736 million dollars. Companies have tried a number of schemes with varying levels of success, but the issue remains a problem industry-wide.

Supply chain mapping

Many of the largest downstream companies tried to identify problem smelters which could serve as entry points for conflict-sourced minerals into the world market. A number of software solutions, questionnaires, and service providers performing on-site inspections were used in an attempt to determine which smelters were the providers in a company's supply chain. They discovered that if a downstream company was large enough, every smelter fed into their supply chain.

Tagged traceability

Raw materials present a particular challenge for traceability because they can undergo transformation at multiple processing points along the supply chain. One solution that has seen large scale adoption in at-risk areas is tagged tracking schemes. These schemes involve placing material in a weighed, sealed container, recording the data about the point of origin, and tracking the container to the point of first processing. These schemes are generally limited to tracking in the first phase of the supply chain because during processing many batches end up mixed together.

Early blockchain pilots

A few companies have started experimenting with blockchain solutions as a way of increasing transparency in the supply chain while decreasing costs. Due to the sensitive nature of supply chain data, most of these pilots have been developed on private permissioned blockchains. These pilots have generally been run by a single end user and have used simplified supply chains and tagged containers, making use of blockchain immutability to verify shipments beyond points of transformation.

Proposed Minespider Protocol

The earlier industry attempts to address the problem of conflict minerals have laid the groundwork for the proposed Minespider protocol. The Minespider protocol integrates the existing upstream due diligence solutions with an open protocol to transmit this data downstream beyond points of transformation to reach the companies who then benefit from a secure raw material supply chain. The Minespider Protocol will be composed of encrypted certification data packets stored in a decentralized database that are purchased using the Minespider ERC20 cryptocurrency called SILQ. These data packets are produced, encrypted, and sold via a DApp. Every purchase of an encrypted data packet will be associated with an amount of material shipped that will be registered in the Ethereum blockchain.

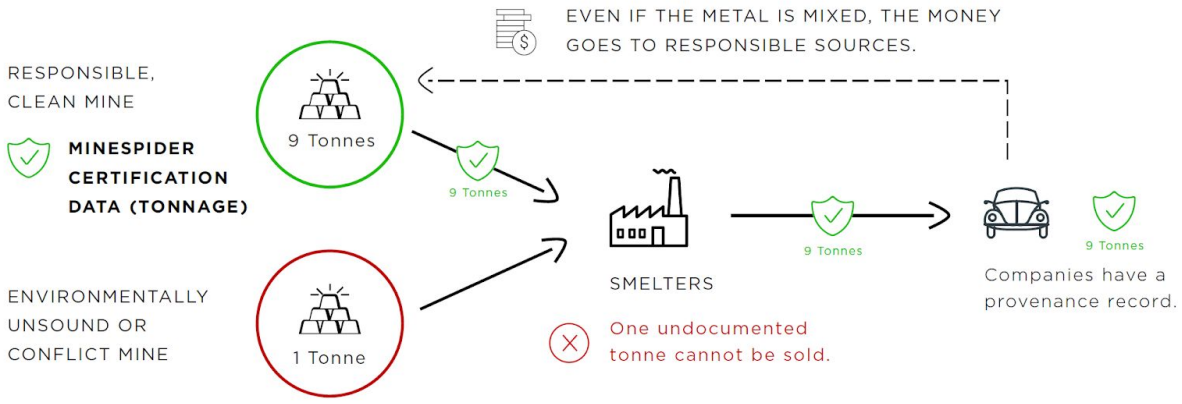
Protocol Features

Mass Balance

One key issue with the scalability and applicability on an industry-wide scale is the fungible nature of raw materials. For any protocol to be useful to the industry, it will need to be functional even when adopted by only a portion of industry players, and account for the possibility of registered shipments being mixed with shipments that are not part of the system. The Minespider protocol incorporates a mass-balance approach to address this need.

Mass-balance traceability operates similarly to green energy tracking on the electrical grid. The primary focus is not on mixing, but on the amount of material produced at a certified source. By tying the certification data to an amount of material, and ensuring that the data is sold with an equivalent volume of material each time, then

the money paid for that material is always traceable back to the certified source, even if the shipment itself is processed and mixed along the way.



As an illustrative example, imagine a scenario where a processor purchases 4 tons of material from a producer who is certified and participating in a blockchain traceability system, and 3 tons from a producer who is not part of this system. The processor would have 7 tons of material but only 4 tons of certification registered on the blockchain. The processor can only sell 4 tons of certified material to their next customer, as the remaining material would be undocumented. To increase the amount of blockchain certified material they can sell, they need to either purchase more from the participating producers, or encourage their other producers to become certified and participate in the blockchain traceability system. In this way anyone holding blockchain certification data can be sure that all the money paid for that amount of material is traceable to responsible sources.

Note: In line with RMI guidelines, Minespider will use the Calculated Metal Weight (CMW) as the mass balance limiter, not the raw tonnage. CMW is simply the tonnage of a shipment multiplied by grade, and should remain consistent through smelting and refining. As such it serves as a better traceability factor than tonnage alone.

Shipment Identifiers

The use of mass-balance does not mean that efforts should not be made to track the provenance of specific shipments. Minespider's data layer is data agnostic, retaining the ability to track microtags, isotopic identifiers, and shipment numbers. This helps ensure participation is not limited by legacy systems, and adds layers of security to the provenance information.

Data Self-Sovereignty

There is an inherent conflict between data privacy and data transparency, and when dealing with supply chain due diligence, it appears at first glance to be a zero-sum game. Supply chain data can be very sensitive to a company, and companies that participate in a transparent supply chain system run the risk of having their

competitors or another third party gain access. Having a trusted third party manage the system is not good enough, as any company with an overview of the supply chain will gain disproportionate power over the industry..

For this reason, some companies have been experimenting with private or permissioned blockchains. Systems like this are an excellent proof of concept, but only work if supply chains are simple, and no upstream company supplies multiple downstream brands. As the number of brands using private blockchains increase, upstream suppliers may find themselves working with 20 or 30 different blockchain systems that all function differently, do not communicate with each other, and have different features and functions. This adds an enormous organizational cost to the upstream, and can result in error if the systems are neglected.

It is critical therefore that supply chain data remain self-sovereign, and not controlled or visible to any third party outside the data owner. This will remove the need for companies to create their own private blockchains, meaning that supply chains will not have to be redesigned for the protocol to work properly.

Decentralization

The Minespider protocol is designed to provide due diligence data and confidence of responsible sourcing for the entire raw materials industry. Therefore governance of the system cannot be centralized. Any one company determining who can or cannot join the system would wield a large amount of power over the industry, which would provide both a vector for corruption and an incentive for a competing protocol to form, defeating the purpose of such a system.

We propose a decentralized governance structure made up of a board of stakeholder representatives. This decentralized board would serve to evaluate responsible sourcing membership and provide input on development goals and directions.

Data Quality and Rating

Customers purchasing due diligence data packets will need a way of determining the quality of data and an appropriate price before making a purchase. Entities such as the Responsible Minerals Initiative (http://www.responsiblemineralsinitiative.org) and BetterChain.org have been working to develop guidelines and frameworks for data collection in various mining contexts that Minespider will incorporate. These standards of data collection will serve to structure data and ensure that all the components necessary to ensure to end users that the minerals have their due diligence and were extracted in a responsible way. The protocol itself will not be bound to the data framework. Rather the users themselves will be able to determine which data framework is most suitable for their industry and transmit this data using the Minespider protocol.

Operational design

Constraints

Minespider is an open platform project that has been designed around three key constraints outlined above:

- **Mass-Balance:** Certification on all raw materials should be restricted by amount of material responsibly produced in order to manage the fungibility of the commodities.
- **Self-sovereign data:** All supply chain, certification, and supporting data should be visible only to the owners of the data. This data should be visible only to the owners of the data and not to third parties or other users of the system
- **Decentralized:** Supply chain participants wishing to incorporate proprietary data and additional user features should be able to construct their own DApp to do so, while still integrating with the other participants in the system

Components

Minespider is made up of the following components:

- **Minespider DApp:** The interface between the smart contract and the real-world tracking. The DApp will allow certifiers to register certified mines in the system, mines to submit due diligence data and mineral supply chain participants to explore their data stored in the blockchain with the Minespider Protocol. Companies can use the Minespider DApp or build their own.

- **Minespider Smart Contract:** This will be built on the Ethereum blockchain. The smart contract can interface with any proprietary DApp that fulfils the requirements, making the system decentralized. The smart contract will have functions to:
    - **Register mines.** Mines are registered with a unique account, a certifying DApp, the mineral they are producing, and the production amount.
    - **Register DApps.** This will be controlled by a consortium of stakeholders so we know which DApps are trusted by the industry.
    - **Register and integrate third party certification agencies:**
    - **Transaction function** which will handle the actual passing of data up the supply chain.
    - **Function controlling transaction price**. Using an oracle the price paid in the DApp are translated into fiat currency for easy reference.
    - **Function tracking allowable sales.** Ensuring no participant sells more certified minerals than they have produced or purchased.

This clear separation of functions means that Minespider operates in a truly decentralized way. No one entity has access to supply chain data, no one entity can control who builds a DApp that accesses the system, and companies requiring specific functions, integrations, or data formats can easily build their own DApps that incorporate these features and mesh with the rest of the system.

Data Handling Process

The DApp data handling is designed to ensure:

1. When a participant purchases certified material the they receive access to its supply chain history.
2. Participants can see upstream information in the supply chain but not downstream after they sell the information.
3. Participants cannot see any data from other participants unless they are upstream from them in the supply chain.
4. Non participants do not have access to any supply chain history directly. This includes Minespider.

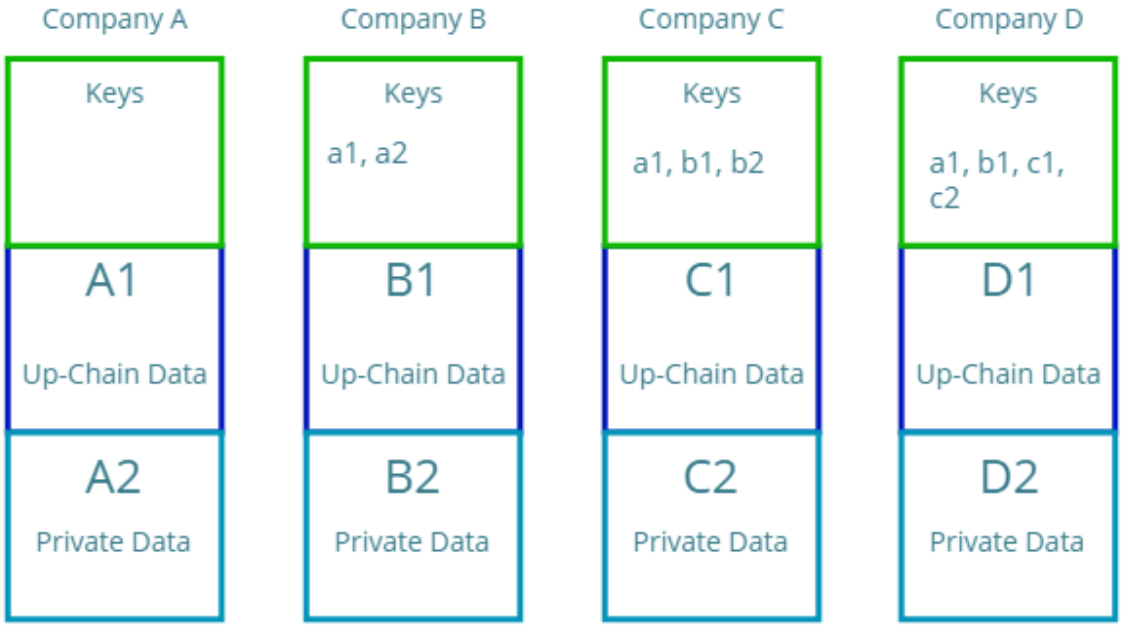
To accomplish this, Minespider will employ will create a "russian doll" data structure where keys to access supply chain history are passed as a nested, encoded data packet. To accomplish this we propose data be stored in 3 segments.

Key Packet contains keys for the segments of the doll to which the company has access.
Segment 1 contains data which should be visible to every member of the supply chain.
Segment 2 contains data which should be stored but visible only to the current and successive member of the supply chain. A company will create one of these for each sale.

Companies selling a data packet follow the following procedure in the Minespider DApp:

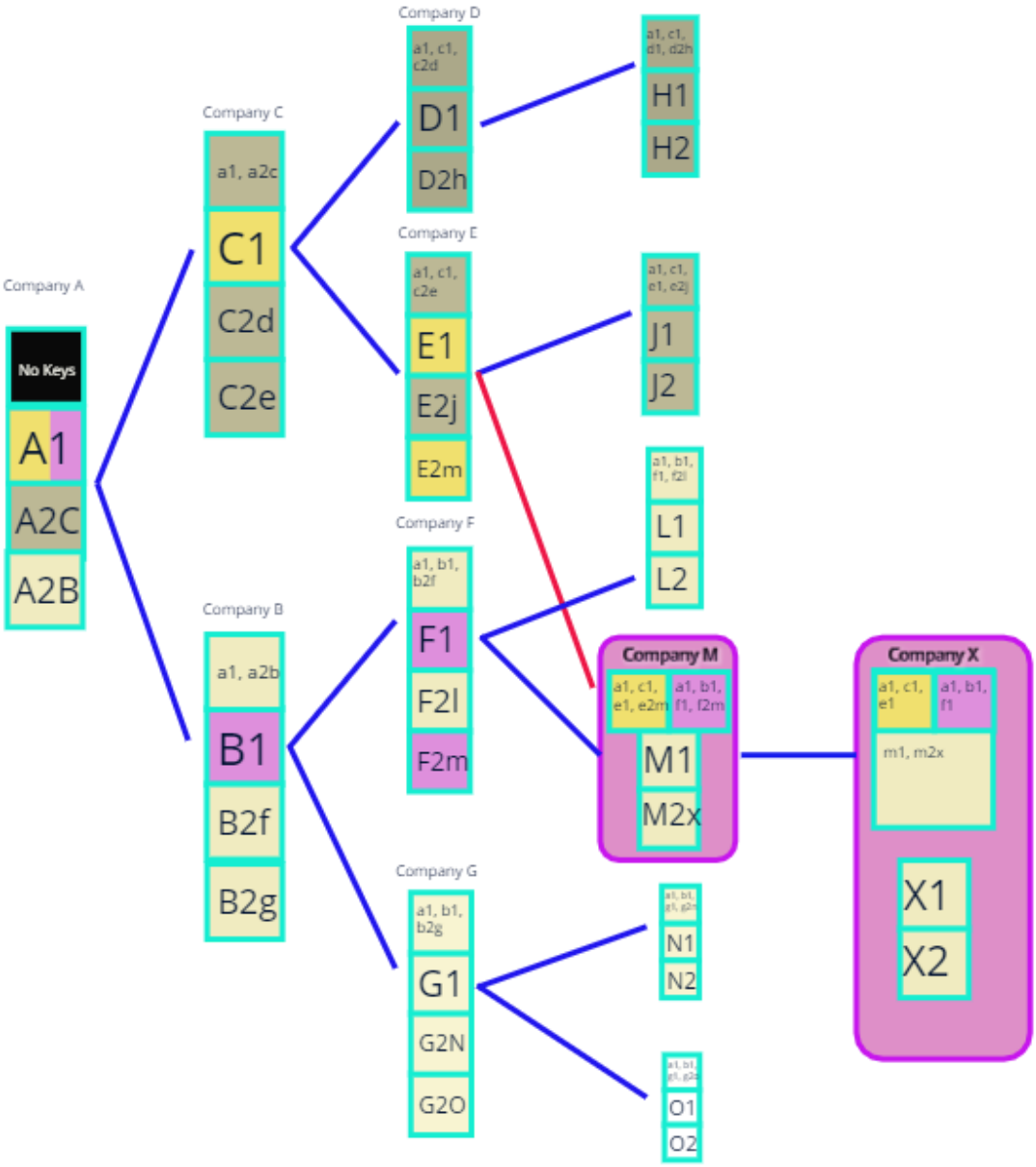
1. Symmetrically encrypt their own **Segment 1** data creating key **K1. Segment 1** data is due diligence data that is visible up the supply chain
2. For each customer **N**, create and encrypt **Segment 2N** data generating key **K2n**.
3. Post encrypted **Segment 1** and **Segment 2N** in decentralized data store.
4. Decrypt **Old Key Packets** received from other suppliers using private key.
5. Remove the keys to **Segment 2** from all **Old Key Packets** received from other suppliers
6. Add these **Old Key Packets** (with segment 2 keys removed) to a **New Key Packet**, along with **K1** and **K2n**
7. Encrypt the **New Key Packet** with the public key of the customer. (asymmetric encryption)
8. Post **New Key Packet** to decentralized data store
9. Broadcast addresses to the blockchain

The figure below details the structure of the "doll" in a straight supply chain with 4 companies.



1. **Company A** is a material producer. **Company A** collects up-chain-visible and private due diligence data and encrypt these symmetrically in a public and private data segment stored in a decentralized data store, **A1** and **A2**, generating keys **a1** and **a2**.
2. **Company A** encrypts keys **a1** and **a2** asymmetrically with the public key of Company B and posts in the decentralized data store.
3. **Company B** decrypts its keys, **a1** and **a2** and accesses **A1** and **A2**.
4. **Company B** collects and encrypts up-chain visible and private due diligence data, **B1** and **B2**, generating keys **b1** and **b2**.
5. **Company B** encrypts keys **a1**, **b1** and **b2** asymmetrically using the public key of company C and posts in the decentralized data store
6. **Company C** now decrypts its keys, **a1**, **b1**, and **b2** and accesses **A1**, **B1**, and **B2**
7. **Company C** collects and encrypts up-chain visible and private due diligence data, **C1** and **C2**, generating keys **c1** and **c2.**
8. **Company C** encrypts keys **a1**, **b1**, **c1**, and **c2** asymmetrically using the public key of company D and posts in the decentralized data store.
9. **Company D** can now decrypt its keys, **a1**, **b1**, **c1**, and **c2** and access **A1**, **B1**, **C1**, and **C2**

Data structure with branching and overlapping suppliers



When we look at the effect of a branched overlapping supply chain we can see the model in action.

Company M has purchased two Key Packets, one from **Company E** and one from **Company F.**

- The Key Packet from **Company E** grants access to **E1, E2m, C1,** and **A1** shown in yellow
- The Key Packet from **Company F** grants access to **F1, F2m, B1,** and **A1** shown in pink.

Company M then strips the Segment 2 keys from the Key Packets, adds its own and encrypts them with the public key of **Company X.** This creates a nested data packet, allowing **Company X** to demonstrate unbroken chains back to **Company A**.

It is important to note:

- All supply chain data is posted to the decentralized data store only once. This prevents exponential growth of the data storage needs.
- Segment 2 data needs to be separately encrypted for every transaction, as this will likely include a contract, bill of sale, or other private information meant only for the immediate customer which may change from transaction to transaction.
- The metadata from the nested nature of the data packet allows a company to determine the structure of their supply chain. Without this metadata, they would have access to the due diligence data of all of the companies in their supply chain but not know who sold to whom.

Underlying Technology

Minespider's MVP is built on the Ethereum blockchain.

Ethereum is currently the dominant player in smart-contract enabled blockchain platforms, and with the flexibility of ERC20 tokens and the robustness of a tested public blockchain, it will provide the best option for the development of an MVP. Nevertheless, the success of the protocol should not be tied to the success of the underlying blockchain, and as such the Minespider protocol is designed to be blockchain agnostic. This allows flexibility for the protocol to be transferred should a more suitable underlying blockchain be identified.

Data Storage

Our Proof of Concept is being built on IPFS for testing purposes however for the MVP we are experimenting with alternatives given the following criteria

- Data needs to be guaranteed to be permanently available and accessible
- Storage should be paid up front or free to avoid data loss
- Storage should be distributed and decentralized
- Storage should be able to handle the exponential growth of data storage needs

We have started working with Arweave.org as the most likely candidate for a long term solution. Arweave incentivizes distributed data storage on-chain with block rewards. This overcomes the issue of monthly fees or low data availability.

Governance

In order to incentivize the secure transmission of supply chain due diligence data, it is very important that there be **one standard** that the global raw material market feels comfortable using. If one centralized entity imposes a traceability system on the entire supply chain, there is a risk of other entities creating a competing standard, which threatens the stability of the entire system. Therefore we plan that after initial development and testing, that the protocol be separated from the DApp and governed in a decentralized manner.

Governance of the Minespider protocol will be overseen by a Decentralized Governance Group (DGG). This group will decide on issues of governance for the Minespider protocol including further development goals, allocation of decentralized resources, maintaining a list of trusted DApps, and deciding on membership admittance.

Starting the group

To launch this group, a set of trusted industry players will stake an amount of Minespider SILQ tokens to maintain their membership. By staking Minespider tokens, member have a vested interest in the governance being performed properly. Staking these tokens gives the members voting rights in allowing new trusted members and in accepting a new DApp in the system.

New members

Prospective members may join the decentralized governance group by staking an equivalent amount of Minespider SILQ tokens and then taking a vote from a randomly selected subset of the existing governance team.

If the vote is in favour of the prospective member joining, they are registered as a trusted members of the oversight group, and every member who voted against them loses their stake which is then transferred to the Minespider smart contract..

If the vote is against the prospective member joining, the prospective member loses the SILQ they had staked which is transferred to the Minespider smart contract.

These staking measures incentivize discussion between members of the oversight group and collective action, while discouraging malicious entities from spamming the oversight group with requests to join.

Membership Renewal

Membership renewal is an essential component to governance to ensure that malicious actors do not take on trusted roles in trusted entities. At regular intervals chosen by the oversight group, every member will need to renew their membership. The process for renewing membership will be the same as for admitting prospective members. Membership will be renewed on a staggered basis to avoid all votes happening on the same day, and collusion between members who are up for renewal simultaneously.

Financing

The Decentralized Governance Group may have funding requirements in order to operate. This could be for auditing certifiers and producers, for liaising with government, representing the DGG at events, further development of the protocol, promoting the protocol, or starting funding initiatives to onboard small producers, etc. These funds can be raised through fees, either for DAPP / producer registration, or transactional fees. It is critical, however, that these fees are charged at the DApp level and not on the protocol itself. Charging the fees on protocol would create an incentive for competing groups to form a separate competing protocol, potentially centralizing power in the DGG, weakening the case for an industry standard.

Potential attacks and recourse

During the ideation process a number of potential attack vectors have been identified that could compromise the Minespider protocol if not addressed. The core team will continue to update security as additional threats are identified.

Minerals laundering scenario:
It is possible that a certified mine launders minerals by purchasing them from a mine that is not part of the system, passing them off as having originated at the certified mine.

Possible ways to address this problem:

a. To participate in Minespider, a producer will need a "speed limit" based on audited production numbers. The speed limit is set by a certifier registered in the system and is tracked on the blockchain. This limits the amount they produce per month.
b. Data packets from mines who go over their limit are flagged to be audited to see if their capacity has increased or if they are purchasing from another mine.
c. If they are purchasing their minerals from another mine, we visit this mine to attempt to incorporate it into the system.

Corporate spying scenario
A malicious actor could get access to a competitor's supply chain data by purchasing certified mineral from them. Collecting supply chain data could provide an opening to individuals acting maliciously to share this data.

Possible ways to address this problem:

a. A multi-signature wallet so that data packets cannot be transferred by one actor
b. Registration of authorized users so that the remains a record of who signed off on any data sale
c. Including only non-sensitive information in the data packet. This solution is always possible because the decision of what information is to be included is handled on the DApp, not in the smart contract, however care must be taken to ensure traceability remains.

Unsecure DApp Scenario
Data packet encryption is done on the DApp in order to maintain confidentiality. If a third party DApps is created to interact with the Minespider protocol, it could be insecure. A malicious actor could create a DApp that appears to operate normally for example, but sends a copy of a data packet to a third party, compromising data privacy.

Possible ways to address this problem:

a. Maintaining a list of trusted DApps, curated by the decentralized governing body.
b. Educating companies who use Minespider DApps about how to maintain data security

Key Loss Scenario

Private Keys can be lost due to employee turnover, hardware failure, or other reasons. This is an ongoing issue with all blockchain projects: the tradeoff between self-sovereignty and accessibility.

a. A Multisig wallet can provide some protection in this scenario.
b. Companies may wish to trust a third party with their keys, possibly an oversight body. This would be at the company's discretion and should not be built into the system.

Misrepresenting the amount of mineral produced scenario

At the mine level, if the person registering the mine in the system assigns a larger mineral limit than the production capacity of the mine, there is potential for fraud. The mine could then sell the excess capacity by purchasing minerals from non-registered mines.

a. The data being immutable means it is auditable. Larger scale fraud would be able to be detected in the long run because data on how much material was shipped would not stand up if the auditors were rotated.
b. Most certification schemes require weight and purity to be measured. This issue will be caught by cross-referencing of due diligence data, and only really becomes an issue if the certification body requires very little documentation.
c. Ultimately this is an issue of which certifiers are trusted. It is an issue that should be addressed by the industry, and not built in to a blockchain platform directly.

Misrepresenting the amount of mineral transferred scenario

Up the supply chain, it is possible for 2 adjacent supply chain actors to collude to register a larger transfer of material in the blockchain than was actually transferred. For example 10 tons of certification may be transferred between parties even though only 1 ton of material is actually shipped. A seller may do this if they only have a few buyers who are participants in the due diligence scheme and wish to offload excess responsible capacity for profit. Buyers may wish to do this if they want to appear to have more responsible stock than they actually purchased.

a. This is a bigger issue in the early days before the system is widely adopted. Once a critical mass of participants are in the system, the incentive for a seller to collude with a buyer is reduced, though still present if one buyer is willing to pay a premium.
b. As above, this can be identified with corroborating documentation. Moreover, as the system expands, a colluding seller will end up with increasing amounts of undocumented mineral in store

Minespider DApp

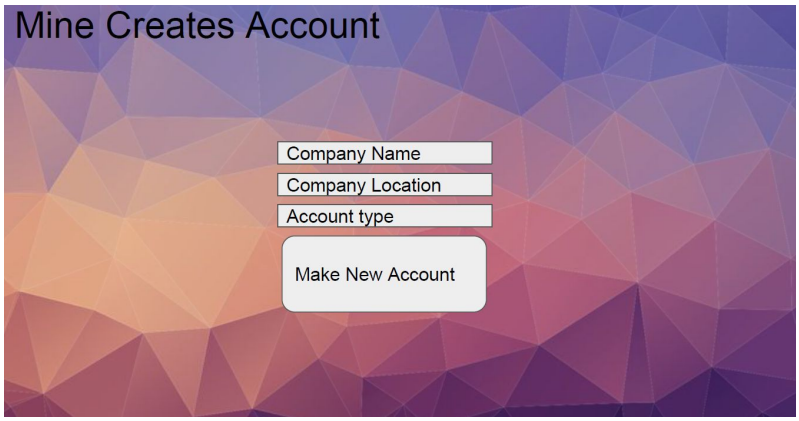
For early pilots Minespider will produce a Decentralized Application (DApp) that will use the Minespider protocol and interface with the Minespider smart contract. This DApp will be open source and serve as a basis for other service providers to develop systems and companies that use the Minespider protocol.

Functions

Register new user account

There will be 3 types of users handled by the Minespider DApp:

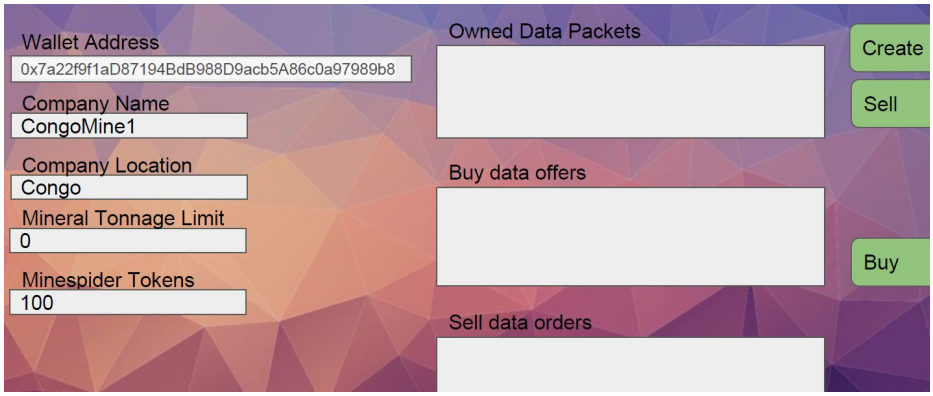
- **Certifiers.** These accounts are for third party service providers who have the authority to register new mines in the system.
- **Normal Account.** These accounts are able to purchase data packets, add data to an existing data packet, and sell data packets.
- **Producer Account (Mine).** These accounts have the functions of a Normal Account, but with the ability to generate a new data packet. Producer accounts are created as Normal Accounts and then registered by a Certifier account to be able to produce data packets.



Account registration screen

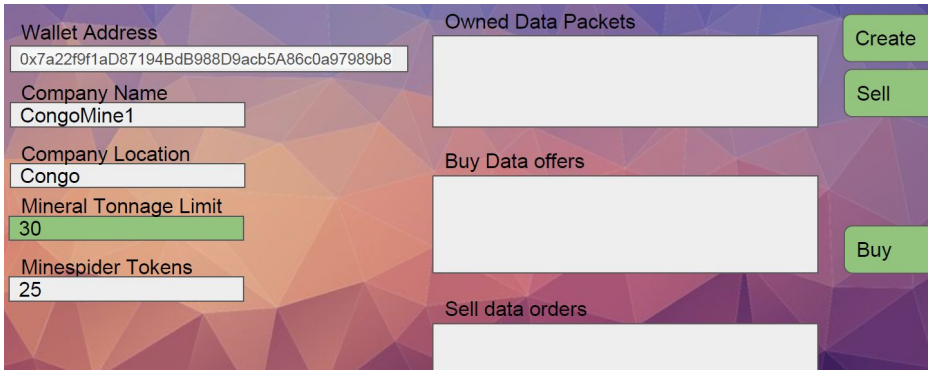
Register producer account

Certifier accounts have the ability to register a Normal account as a Producer account. A certifier enters the wallet address of the mine to be registered along with the production tonnage limit for the mine and the cost of certification. The account and tonnage limit is broadcast to the blockchain.



The account of a mineral producer starts as a normal account with no tonnage limit

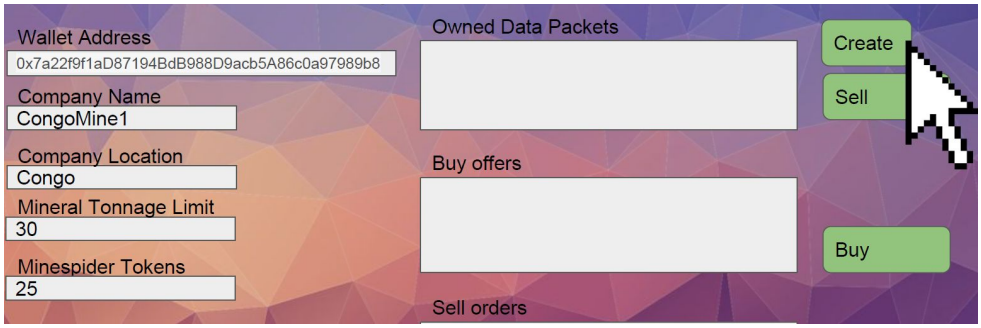
A certifier registers the producer's information in the blockchain



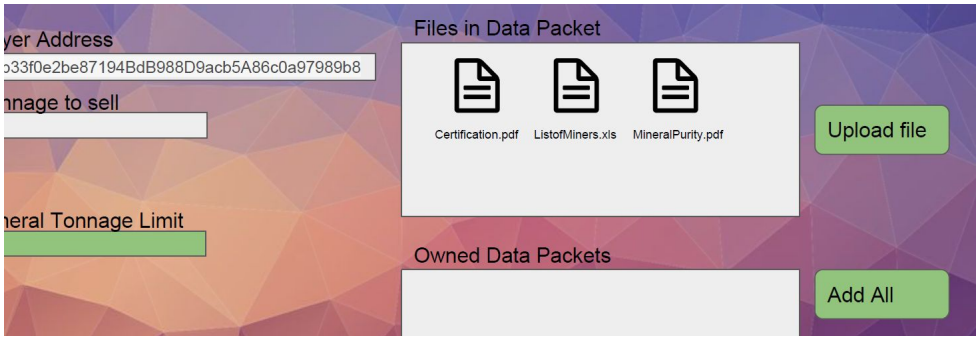
The producer then has a tonnage limit and can create a data packet

Create Data Packet

Data packets contain files with due diligence information chosen by the company creating or adding to a packet. The data packets are collections of files encrypted with the public keys of the buyers. There are no in-app restrictions on files that can be added to the data packet.



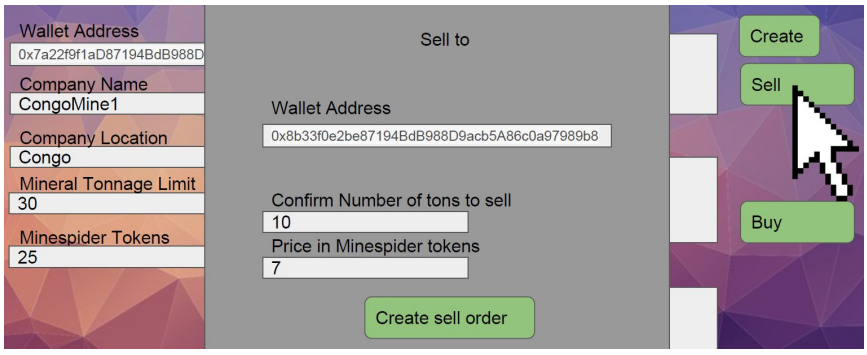
A producer account with a tonnage limit is able to create a new packet



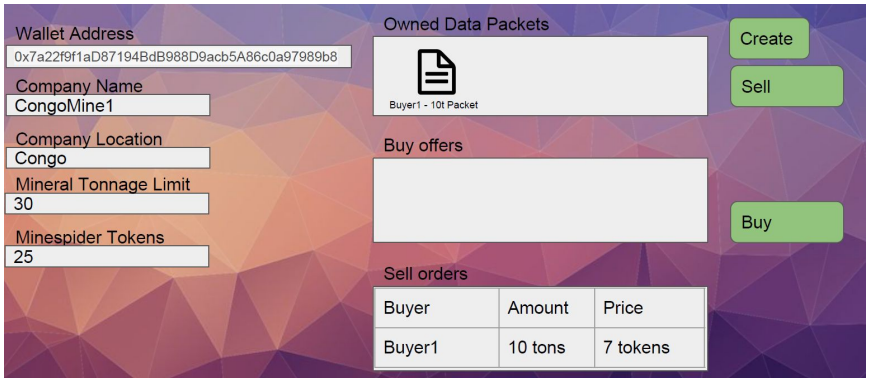
Any files can be added to a packet. If the account already owns a data packet, they can add to it.

Sell Data Packet

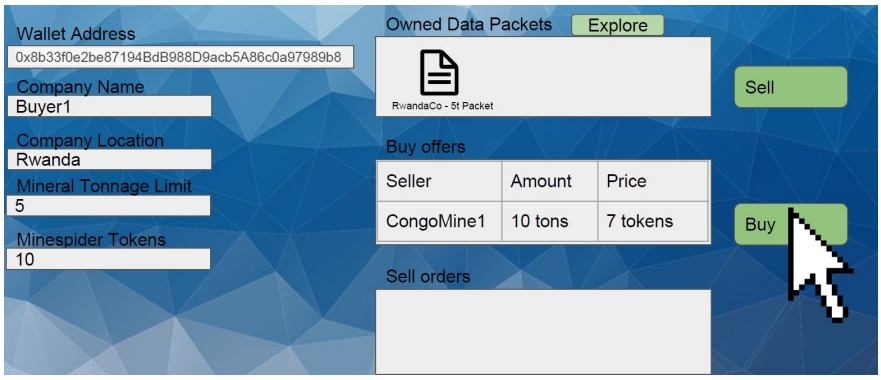
Any company holding a data packet and having a remaining tonnage limit can sell a data packet to a customer. This process encrypts the data packet with the public key of the buyer, posts the encrypted packet on a decentralized database, and broadcasts the tonnage of the sale on the blockchain.



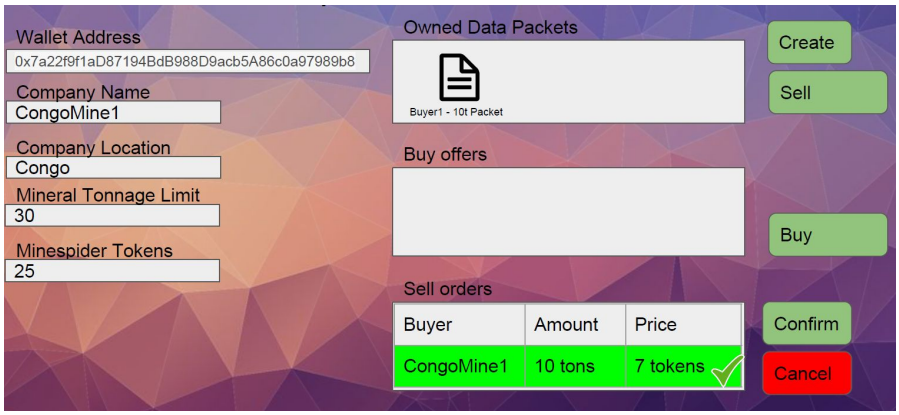
Mine selects a data packet to sell, sets a price and enters the wallet address of the buyer



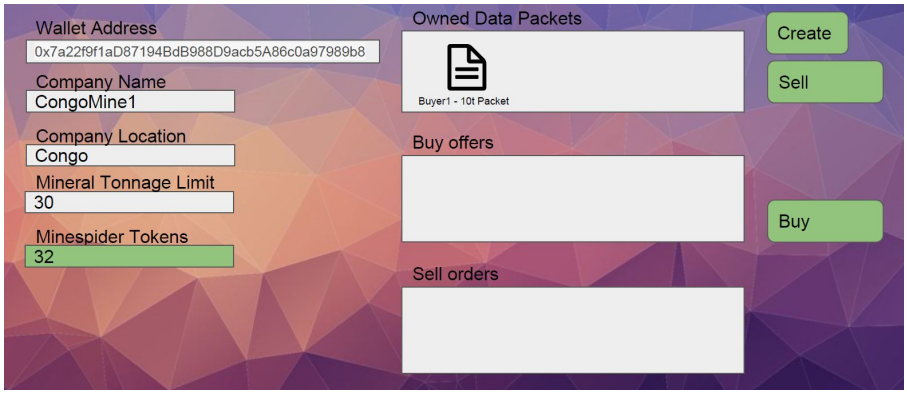
The sell order is created and awaits buyer confirmation



The buyer sees the offer and is able to accept it



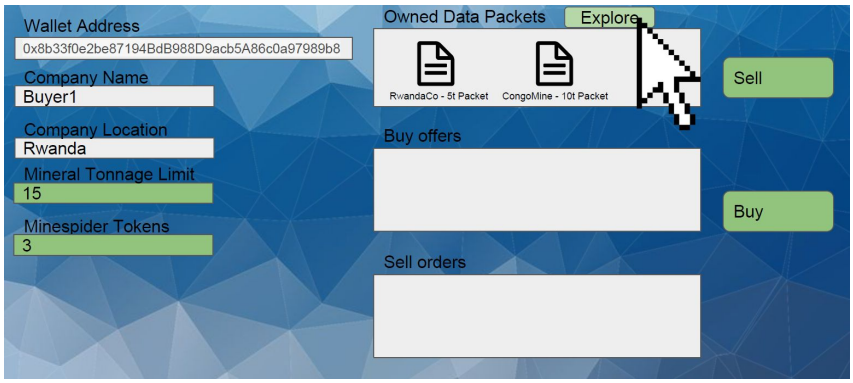
The seller sees the accepted offer and confirms the transaction



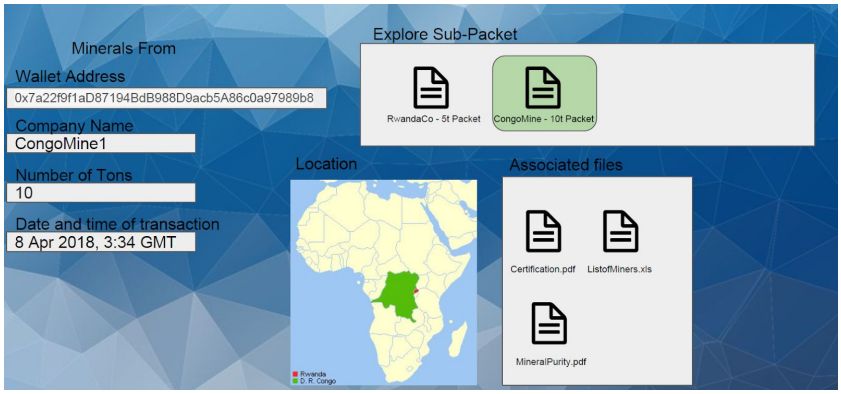
With the transaction complete, the seller's token balance is updated

Explore Data Packet

Owners of data packets can open and explore them to see their due diligence data on raw material shipments.



User chooses to explore their owned data packets



User selects a data packet and sees the contained files and the regions of origin.

Certification data collection

A blockchain system for creating digital assets from due diligence data and transferring them up the supply chain is only as useful as the source data entered into the system. Evaluating the quality of due diligence data is a delicate process. Having no evaluation scheme leaves the system open to useless data being sold as useful, and having a rigorous evaluation scheme could result in the concentration of power in a cartel that keeps out competition.

Minespider's position is that an open system is best, and that the issues of data quality assurance can be dealt with by incorporating the possibility of independent data quality audits and evaluation. Multi-stakeholder groups can then create standards for appropriate data and events to be captured by the protocol and use existing certifications and document costs to assign value to the data assets.

The Minespider DApp will be incorporating data guidelines set by the Responsible Minerals Initiative (RMI).

ASM Inclusion and Onboarding

In the mining industry, Artisanal and Small-scale Mines (ASMs) are often found in rural areas of poorer regions, and are a primary target for conflict groups looking to collect illegal taxes, launder money, or impose forced labour. Finding a solution to incentivize ASM inclusion in the world market remains a priority for responsible industry, NGOs, and state actors. Small-scale producers have reduced access to technology and education and so a portion of the tokens will be allocated for onboarding and incentive programs:

- ASMs will receive subsidized SILQ holding accounts for joining the system. Subsidies will be based on a sliding scale so that joining the system will have zero cost for the poorest producers.
- The Minespider DAPP will be extensively field tested amongst ASMs to ensure that it is data-light, will be translated into local languages, and will work offline for remote locations.
- Some of the SILQ tokens will be allocated to forming partnerships with NGOs and providers of needed services in at risk regions including mining capacity building, microfinance, microsavings, health, and education services, in order to provide a comprehensive outreach and onboarding program.
- The effectiveness the platform and associated services on the improvement of the lives of ASMs and ASM communities will be rigorously evaluated to improve the platform and ensure that it meets the relevant development goals.

Minespider Token

Minespider's due diligence ecosystem is facilitated by the Minespider SILQ utility token. These tokens enable the transfer of value and incentives from downstream beneficiaries of due diligence data to data providers and certifiers in the upstream, without the need of a centralized, trusted third party. Tokens are required to participate in the system as they enable traceability and activation of the smart contract.

SILQ Tokenes from the wider community, all without depending on a centralized entity.

Token Utility

Certification on the Minespider Protocol
Mineral producers obtain certification by staking SILQ when they have been certified by a certification partner approved by the DGG. This allows producers to create new certification data packets and sell the access to them to their customers.

When a producer is certified by a third party certifier using a DApp for the Minespider protocol, the certifier attests that the producer is responsible, their monthly production volume, and their location. Certification is not permanent - it has an expiry date. The mine will pay a number of SILQ tokens per unit of production determined by the Decentralized Governance Group for that raw material, and be registered for that production amount in the blockchain.

By staking these tokens a responsible producer has the right to create data packets equal to the production amount registered in the blockchain. If the producer leaves the system, for example, if the mine's production has been exhausted, they are able to get back the SILQ they staked.

Staked Protocol Access
Companies in the mineral supply chain who are not producers need to stake tokens to access the Minespider protocol. While the stake is active, companies are able to purchase data packets, add their own data to a supply chain, and sell data packets onward. If a company withdraws their stake or it is revoked by the DGG their status will remain in the blockchain but they will be unable to make further transactions until their stake is restored.

Staking to enable protocol access provides a negative incentive for supply chain actors from selling wallets directly to customers to bypass a supply chain step and provides a record of registration the DGG can use for enforcement.

Viewer Accounts

Individual consumers need to know that their products were sourced responsibly, however it is important that individuals do not have direct read access to supply chain data so that company privacy is protected.

To solve this, individuals can stake tokens to formally request responsibility data on one of their products. The company can then authorize or deny this request. Staking tokens helps prevent DDoS attacks, and attempts at data scraping.

Authentic Medium of Settlement

SILQ will act as a medium of settlement allowing certifiers, DApp creators, data providers, and data purchasers to transact atomically through the Minespider protocol. Both read/reporting functionality and write/transfer functionality constitute a decentralized cost in the system that are compensated with SILQ. In addition, the token provides an incentive for members to perform operations supporting the network such as data storage and processing.

Minespider's protocol will rest on top of an underlying blockchain and distributed database which require small crypto token fees to perform the necessary operations. These will be charged transactionally using the SILQ token.

Protocol Governance

In order to maintain oversight of the Minespider protocol and which DApps and suppliers are trusted on it, entities can apply to be part of a Decentralized Governance Group by staking SILQ. The onboarding process for individuals or entities to join the Decentralized Governance Group is outlined above.

Community Engagement to Responsible Sourcing

At its core, responsible sourcing is driven by the demand from the wider community for responsible products. Individuals want responsible jewelry, electronics, automobiles, and more. The SILQ token provides a mechanism for individuals to engage with their favourite brands on the topic of responsible sourcing. Individuals can pledge SILQ toward their favourite brands that they would like to source responsibly. When the brand joins Minespider, the SILQ pledged is used to help the players in that brand's supply chain implement responsible tracking mechanisms so they can participate. This is especially effective when smaller mining companies are found in the supply chain that might need assistance to participate.

Pledging SILQ also facilitates communication of the community's commitment to responsible sourcing directly to the brand as well as their willingness to share the burden of implementation. The more tokens an individual pledges, the greater their individual voice and impact.