MINESPIDER

# Protocol for Due Diligence in the Raw Material Supply Chain

v.0.36

Nathan Williams

# Table of Contents

# 1. Abstract

The following whitepaper 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 packet "certificates", 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

**Due Diligence Focus**

Throughout this whitepaper 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.

# 2. The Challenge of Conflict Minerals

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:** Data is stored in a decentralized manner. Data is submitted to the system via a DApp. Governance of the system is controlled through token staking.
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.

## 2.1 Legal 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.

## 2.2 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.

### 2.2.1 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.

### 2.2.2 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.

### 2.2.3 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.

# 3. Minespider Infrastructure

Minespider is a raw material supply chain infrastructure that consists of a number of components which operate in concert to make the entire system work:

- The Minespider Protocol
- The Minespider Smart Contract
- The Minespider DApp
- The Minespider Certification
- The SILQ Utility Token

These components are distinct yet interoperable and work together to create a traceability system for the entire supply chain.

**Underlying Technology**

The Minespider Infrastructure 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 a “minimum viable product” (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.

## 3.1 Minespider Protocol

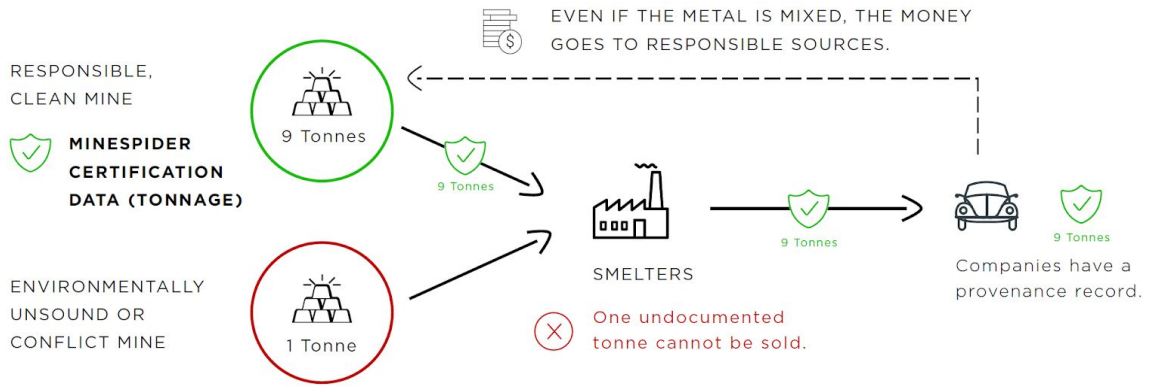
The Minespider Protocol integrates the existing upstream due diligence solutions with an open protocol to transmit this data downstream beyond points of transformation to reach the companies who then benefit from a secure raw material supply chain. The Minespider Protocol will be composed of encrypted certificates stored in a decentralized database that are purchased using the Minespider ERC20 cryptocurrency called SILQ. These certificates are produced, encrypted, and sold via a DApp. Every purchase of an encrypted certificate will be associated with an amount of material shipped that will be registered in the Ethereum blockchain.

The protocol is designed with the following features in mind:

**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**

In order to reduce the need for centralized governing bodies in the system Minespider incorporates a utility token staking system and incentive model. This provides the base mechanism to decentralize the governance of the system after the early phases when the protocol is ready to scale.

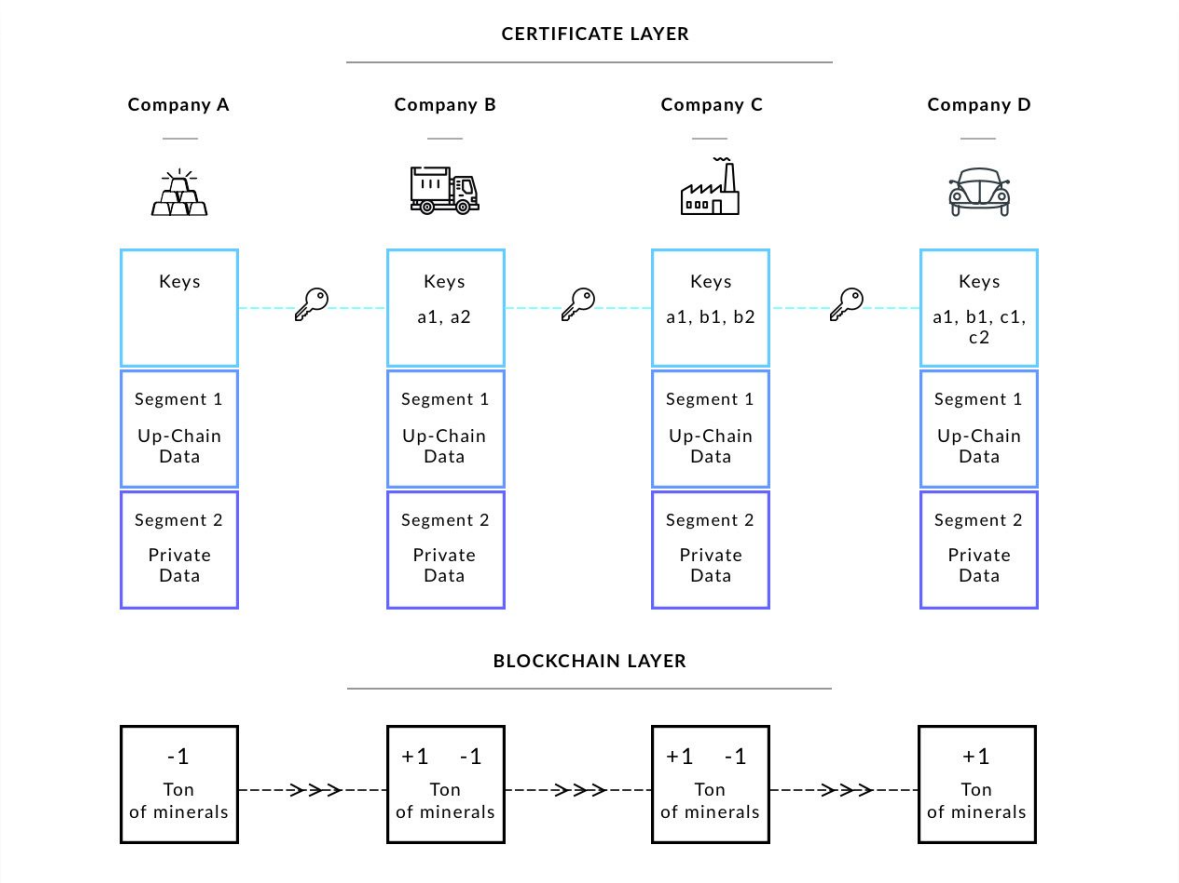
**Data Quality**

Customers purchasing Minespider Certificates will need assurance that the data the certificate represents is sufficient to demonstrate responsible sourcing. Entities such as the Responsible Minerals Initiative (http://www.responsiblemineralsinitiative.org) have been working to develop guidelines and frameworks for data collection in various mining contexts that Minespider will consider to incorporate. These standards of data collection can serve to structure data and allow purchasers to demonstrate the origin and responsible production of their product.

**Protocol Operational Design**

The Minespider Protocol was designed by minespider GmbH. The Minespider Protocol is built on the Ethereum blockchain and consists of two elements ("layers"): A "certificate" layer and a blockchain layer which are linked. The blockchain layer records the amount of metal produced by responsible sources and who owns it. The certificate layer stores specific data, e.g. scans of certificates of origin, authorizations, production limits, transfers of possession, tonnage limits, and other relevant data. We look to the Responsible Minerals Initiative official Blockchain Guidelines for structuring the information stored.

Within the scope of the MVP of the Minespider Infrastructure, the certificate layer is built on the IPFS Protocol. IPFS stands for the InterPlanetary File System: a peer-to-peer method for storing and sharing hypermedia in a distributed data system. Although, as the Minespider Protocol and Infrastructure scales, other decentralized data storages/providers may be evaluated.




### 3.1.1 Data Handling Process

The Minespider Protocol has at its core a method of securely storing and transmitting raw material provenance data, designed according to the following principles: :

1. When a participant purchases certified material 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 data stored on the blockchain without having the respective key. This includes Minespider GmbH.

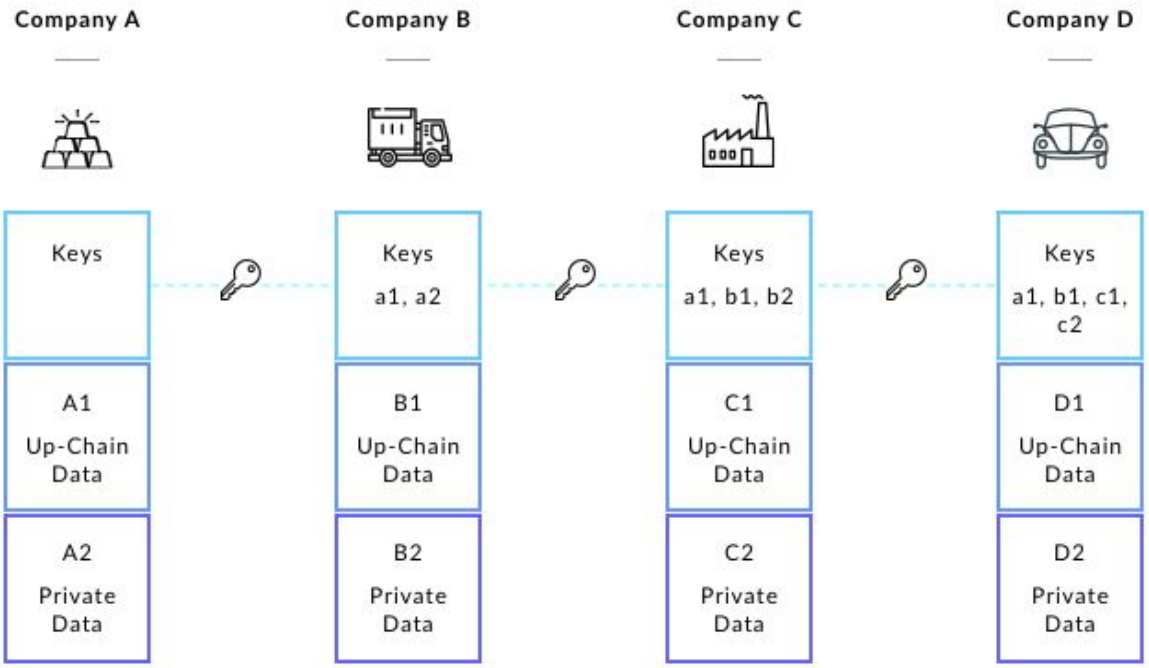
To accomplish this, the Minespider Protocol will employ a "russian doll" data structure where keys to access supply chain history stored in the certificate are passed as a nested, encoded data packet. To accomplish this we propose data be stored in 3 segments.

**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 certificate follow the following procedure in the Minespider DApp:

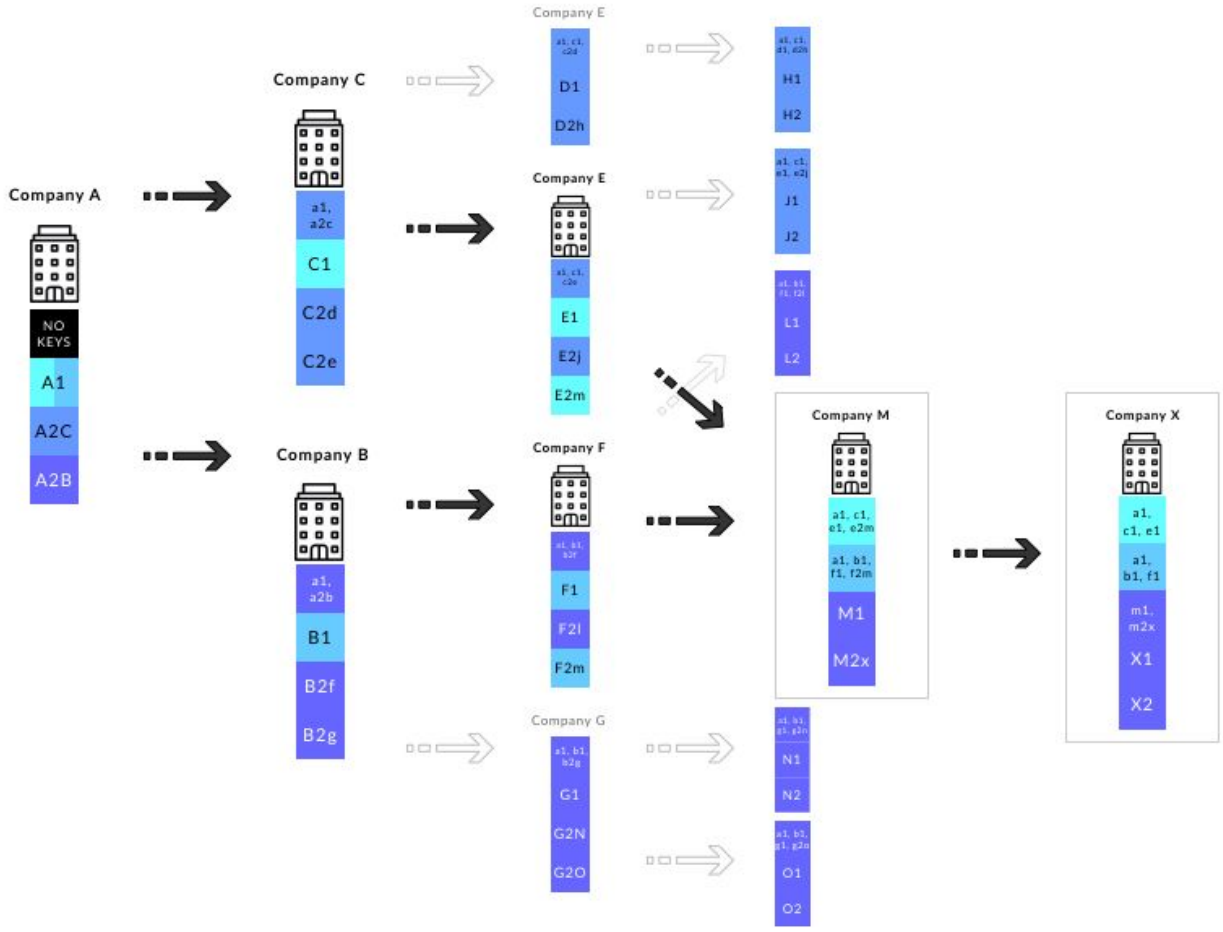
1. Symmetrically encrypt their own **Segment 1** data creating key **K1. Segment 1** data is due diligence data that is visible up the supply chain
2. For each customer **N**, create and encrypt **Segment 2N** data generating key **K2n**.
3. Post encrypted **Segment 1** and **Segment 2N** in a decentralized data store ( the **Certificate Layer**).
4. Decrypt **Old Key Packets** received from other suppliers on the **Certificate Layer** 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 the **Certificate Layer**
9. Broadcast addresses to the **Blockchain Layer**

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 (the **Certificate Layer**) , **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 **Certificate Layer**.
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 **Certificate Layer.**
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 **Certificate Layer.**
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 **Certificate Layer** 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 demonstrate an unbroken chain of custody throughout their supply chain.

**Note on Data Storage**

As mentioned above, our MVP is built on IPFS and its peer-to-peer method for storing and sharing hypermedia in a distributed data system. Although, as the Minespider Protocol and Infrastructure scales, other decentralized data storages/providers may be evaluated according the following criteria:

- Data needs to be permanently available and accessible
- Storage should be distributed and decentralized
- Storage should be able to handle the scaling of data storage needs

## 3.2 Minespider Smart Contract

The Minespider Smart Contract is built on the Ethereum blockchain. The smart contract interfaces with the Minespider DApp as well as potentially any other proprietary DApp that fulfils the requirements of the Minespider Protocol and Smart Contract, making the system decentralized. The Minespider Smart Contract will have functions to:

- **Register mines.** Mines are to be registered with a unique account, a certifying registered Certifier, the mineral they are producing, and the production amount.
- **Register DApps.** DApps wishing to interact with the Minespider Protocol must first stake SILQ and then be approved to be registered. This mechanism allows for version control of DApps, for specialized functionalities, and for potential competition on the DApp level, to disincentivize fracturing of the mineral traceability market. For the MVP the registration of third party DApps is controlled by Minespider GmbH. In future this may be controlled by a consortium of stakeholders who defines which DApps are trusted by the industry.
- **Register and integrate third party certifiers.** These can be state inspectors, third party consultants, or agencies.
- **Register supply chain participant.**
- **Function managing production and transacting of Minespider Certificates.** Ensuring no participant sells more certified minerals than they have produced or purchased.

It is important to note that certain security functions such as certificate access will be handled not on the smart contract, but on the Minespider DApp. This means that from a security point of view, any DApp working with the protocol needs to undergo code review.

## 3.3 Minespider DApp

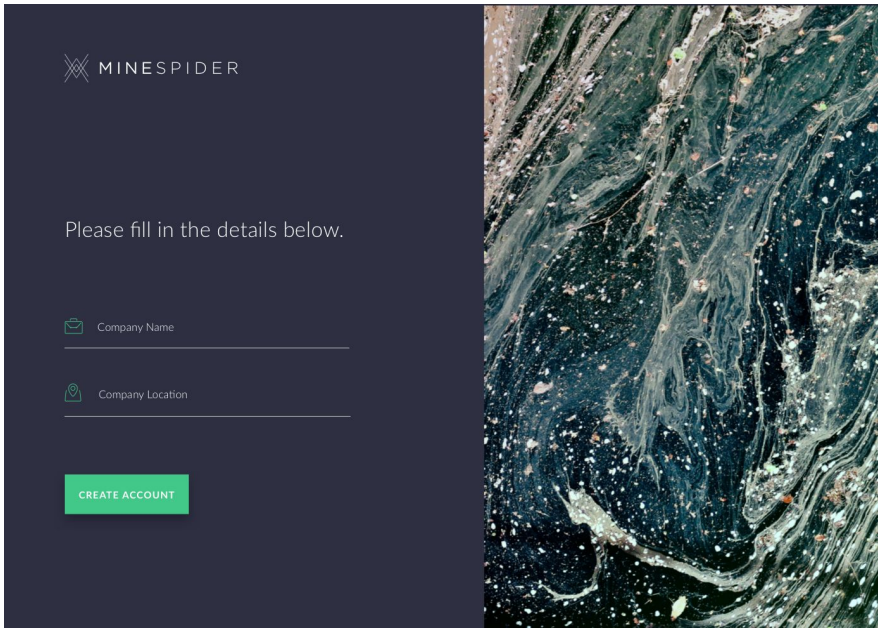
For early pilots Minespider will produce a Decentralized Application (DApp) that will use the Minespider Protocol and interface with the Minespider smart contract. This DApp will be open source and serve as a basis for other service providers to develop systems and companies that use the Minespider Protocol. The DApp requires sufficient amounts of SILQ in order to interact with the Minespider Protocol and the Minespider Smart Contract.

Please note that the "screenshots" as shown in the following are meant to be for the purpose of illustration only. Whereas the frontend appearance and the data to be filed or shown by the DApp may be different and/or change in the MVP or in the course of any further developments

**Register new user account**

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

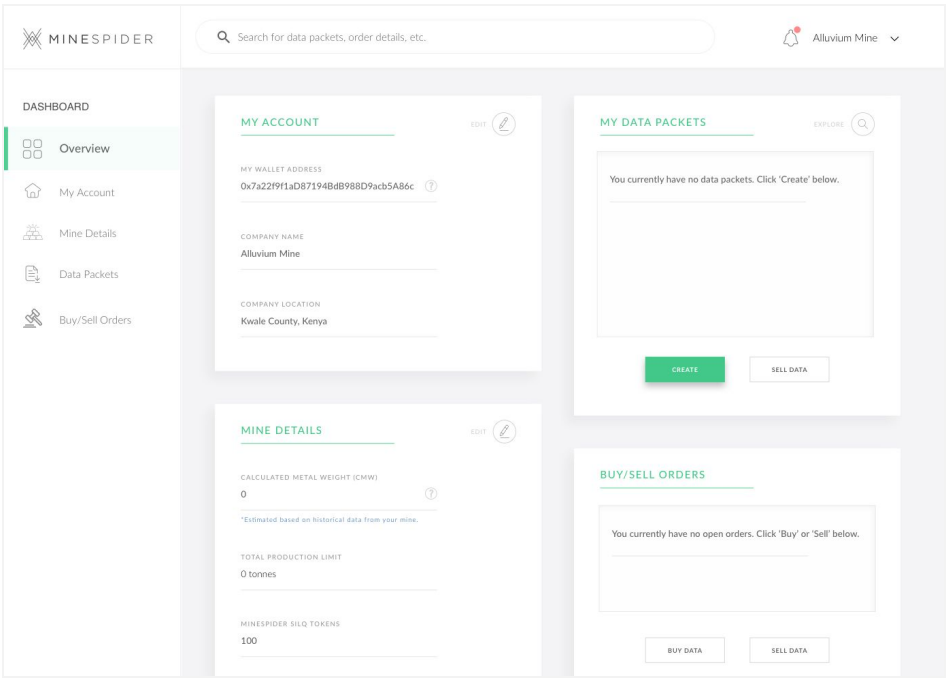
- **Certifiers.** These accounts are for third party service providers who have the authority to register new mines in the system.
- **Normal Account.** These accounts are able to purchase certificates, add data to an existing certificates, and sell certificates.
- **Producer Account (Mine).** These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



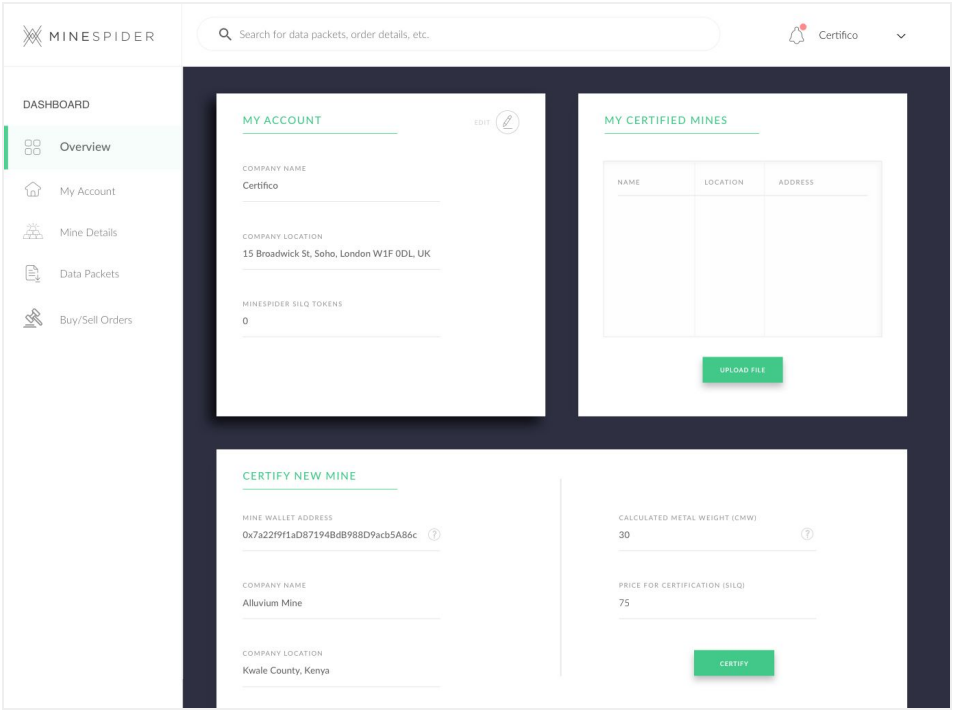

Account registration screen

**Register producer account**

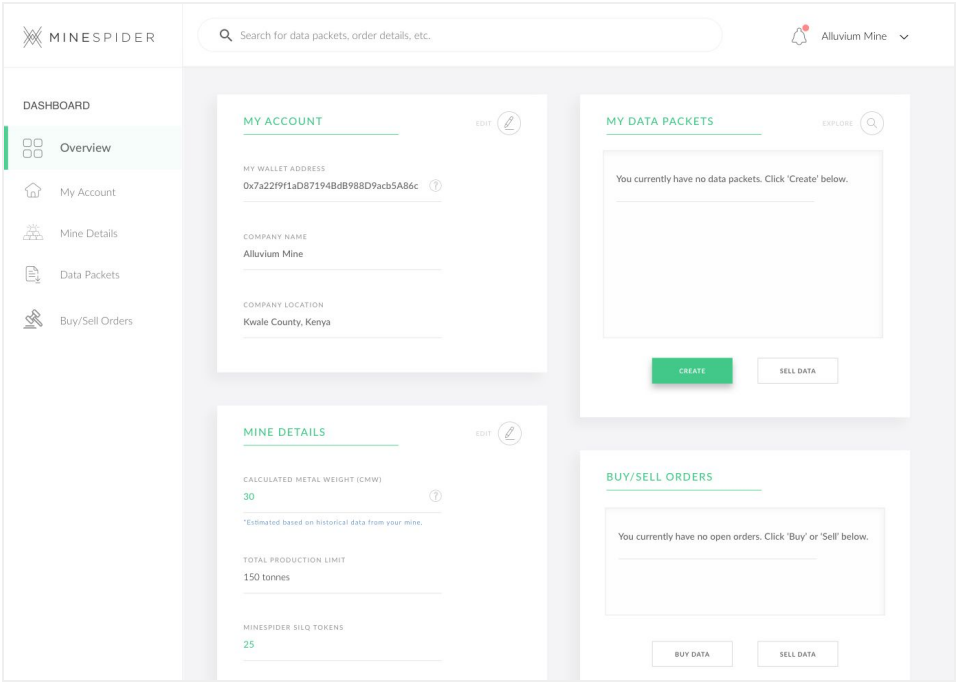
Certifier accounts have the ability to register a Normal account as a Producer account. A certifier enters the wallet address of the mine to be registered along with the production tonnage limit for the mine and the cost of certification. The account and tonnage limit is broadcast to the blockchain.




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



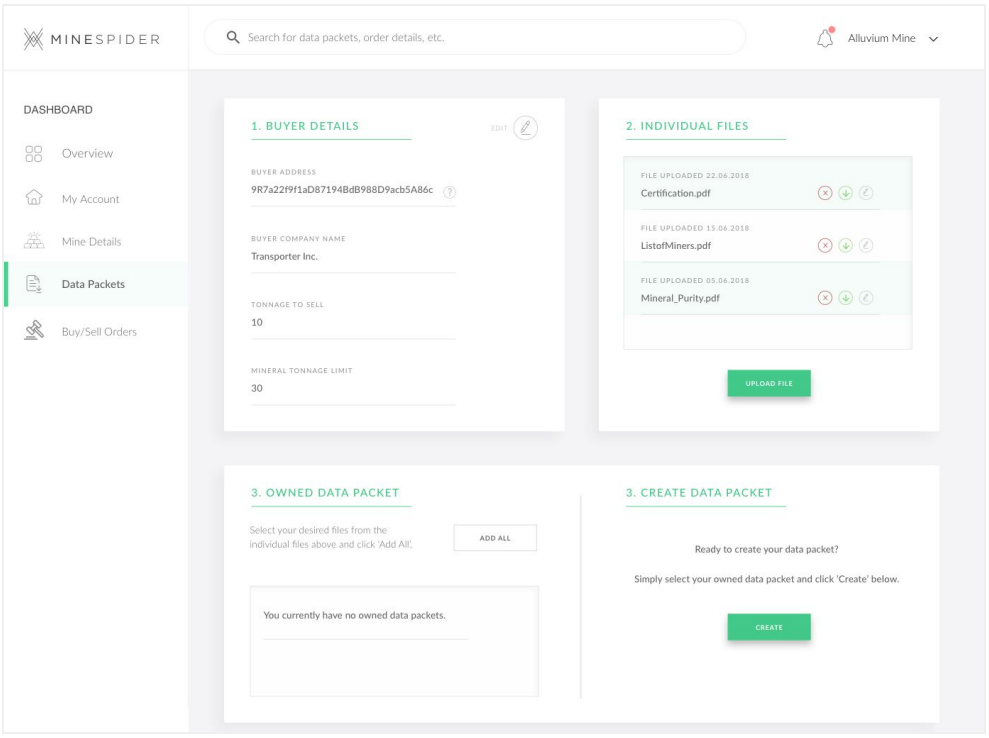

**A certifier registers the producer's information in the blockchain**



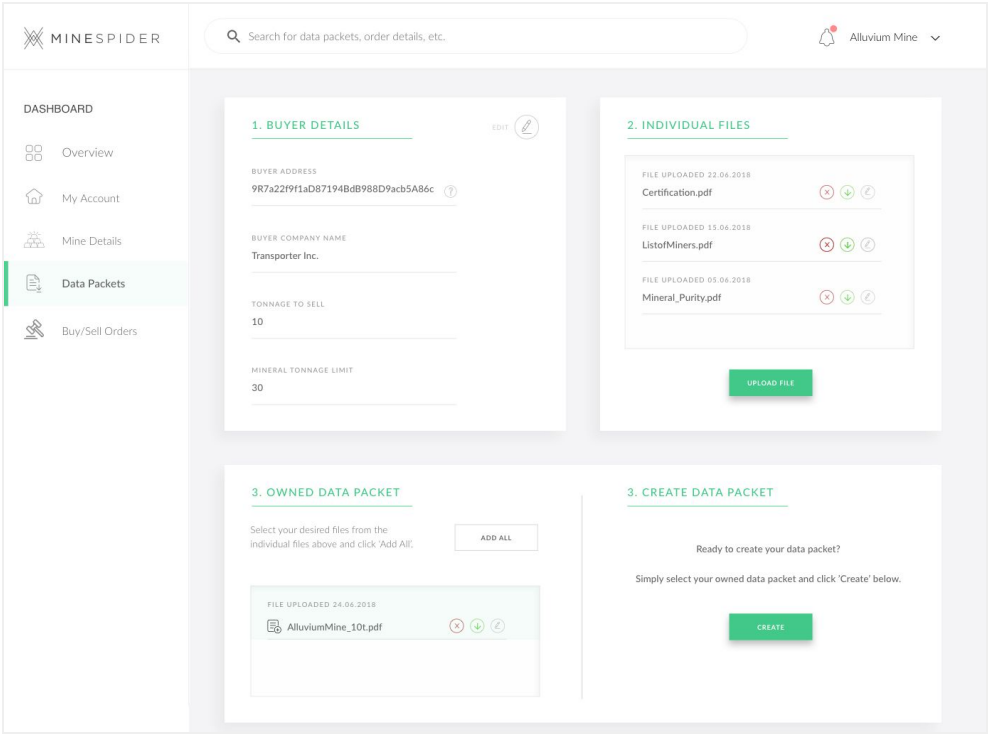

**The producer then has a tonnage limit and can create a certificate**

**Create Certificate**

Certificates contain files with due diligence information chosen by the company. The certificates 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 certificate.



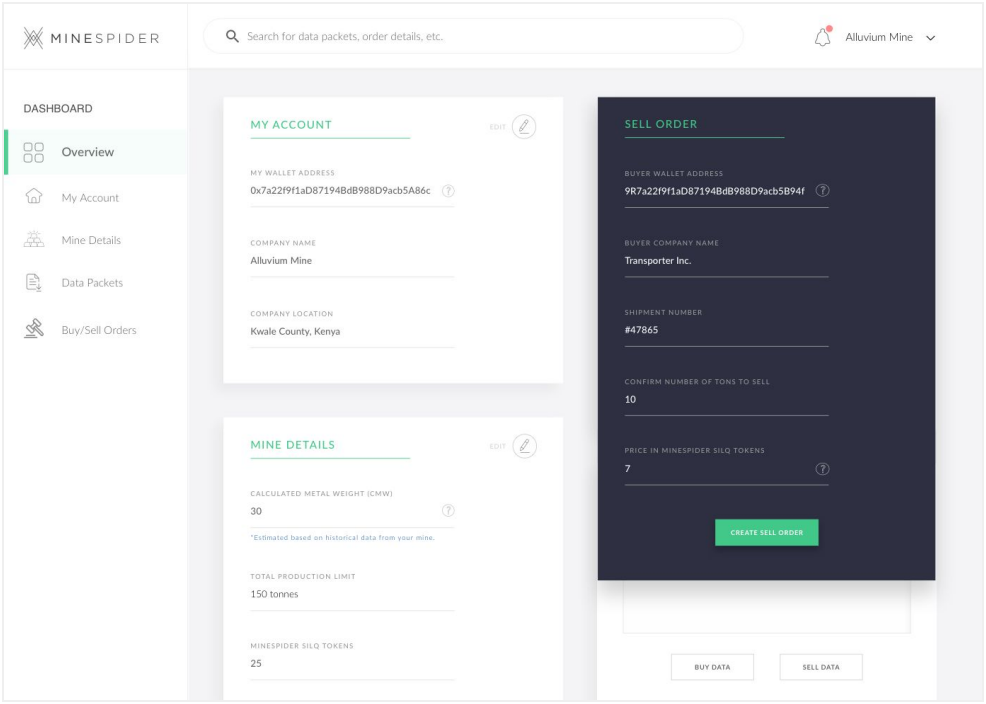

**A producer account with a tonnage limit is able to create a new packet**



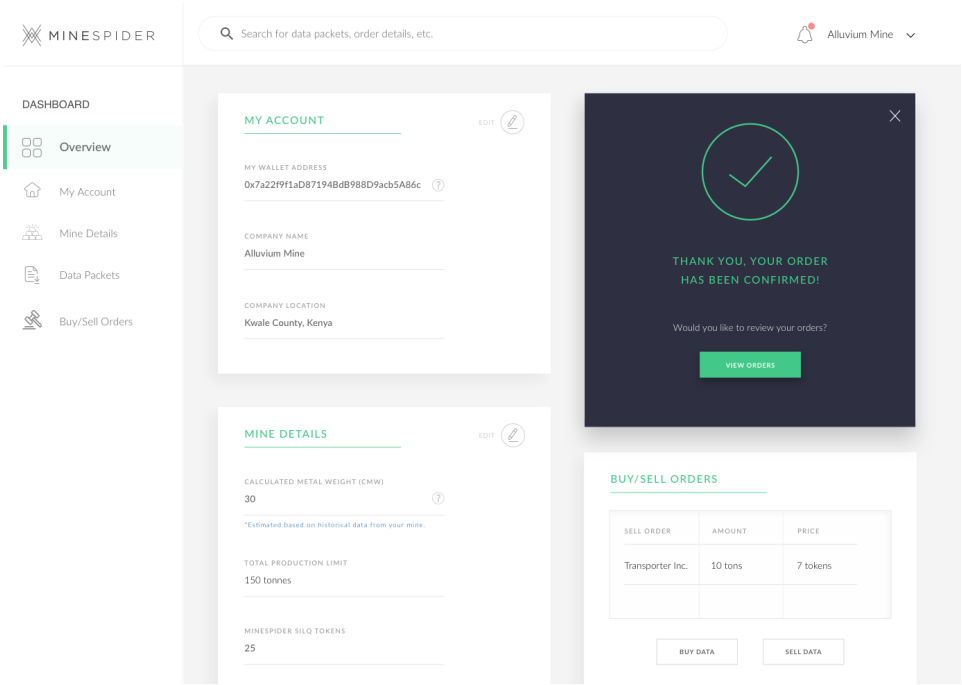

**Any files can be added to a packet. If the account already owns a data packet, they can add to it.**

## Sell Certificate

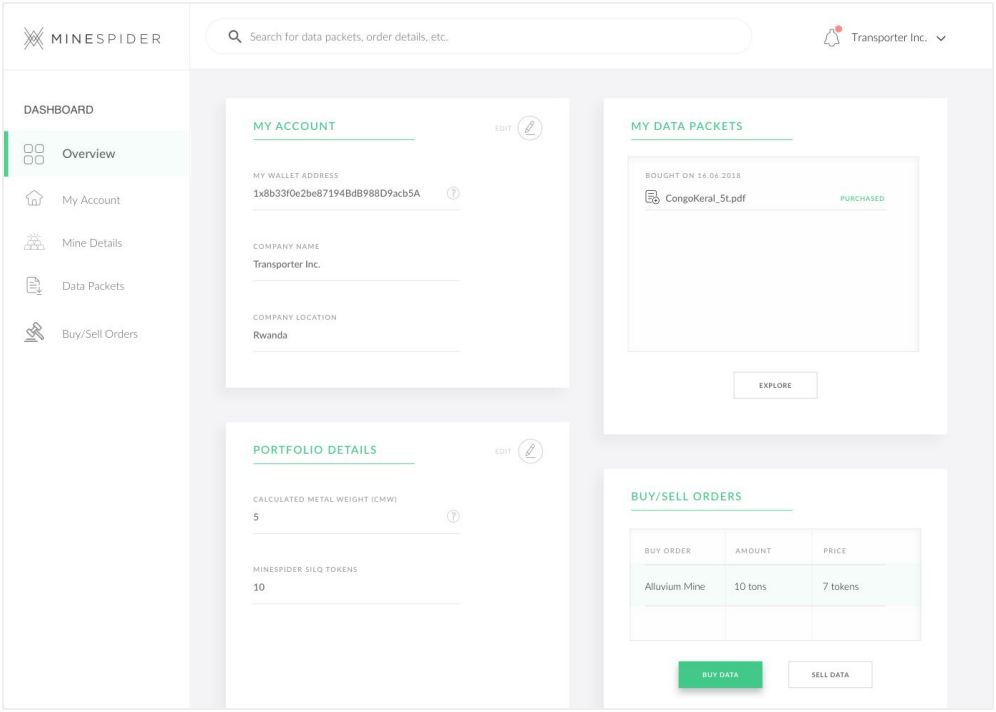
Any company holding a certificate and having a remaining tonnage limit can sell a certificate to a customer. This process encrypts the certificate with the public key of the buyer, posts the encrypted packet on a decentralized database, and broadcasts the tonnage of the sale on the blockchain.



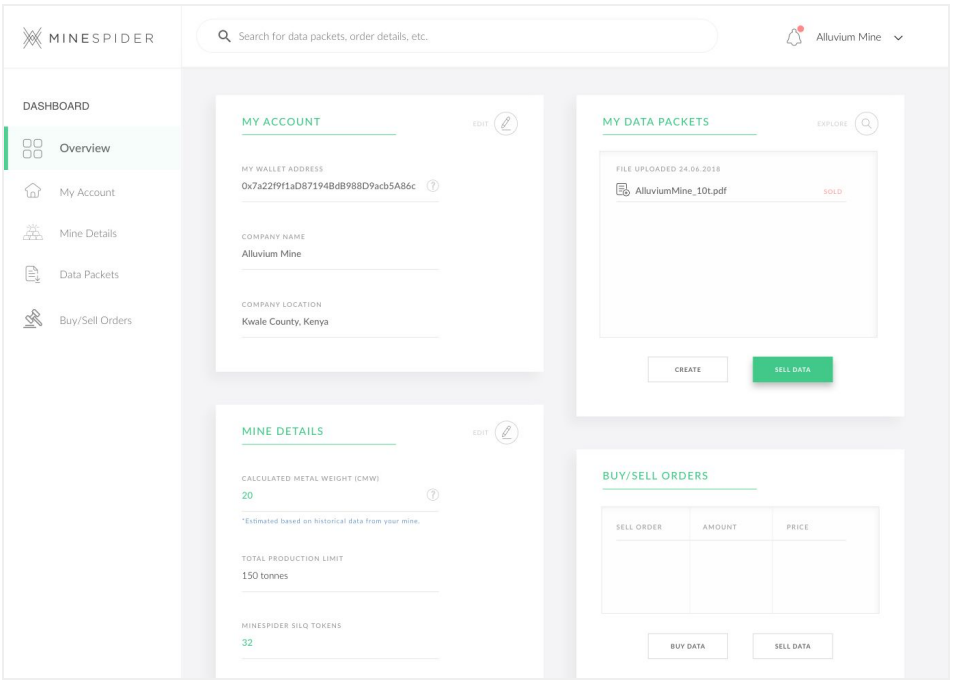

**Mine selects a certificate to sell, sets a price and enters the wallet address of the buyer**



**The sell order is created and awaits buyer confirmation**



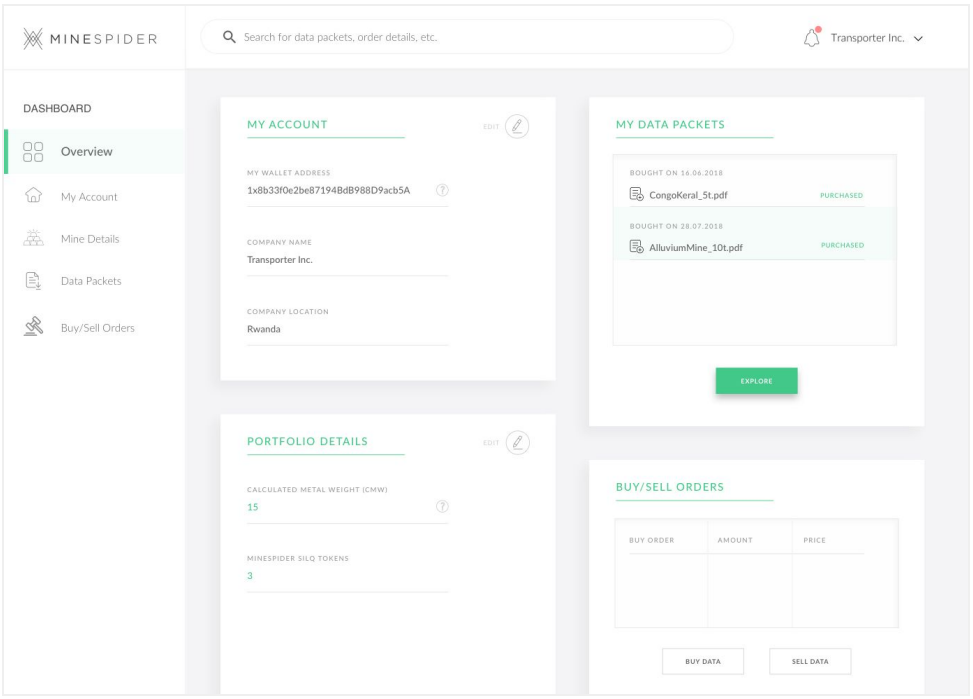

**The buyer sees the offer and is able to accept it**



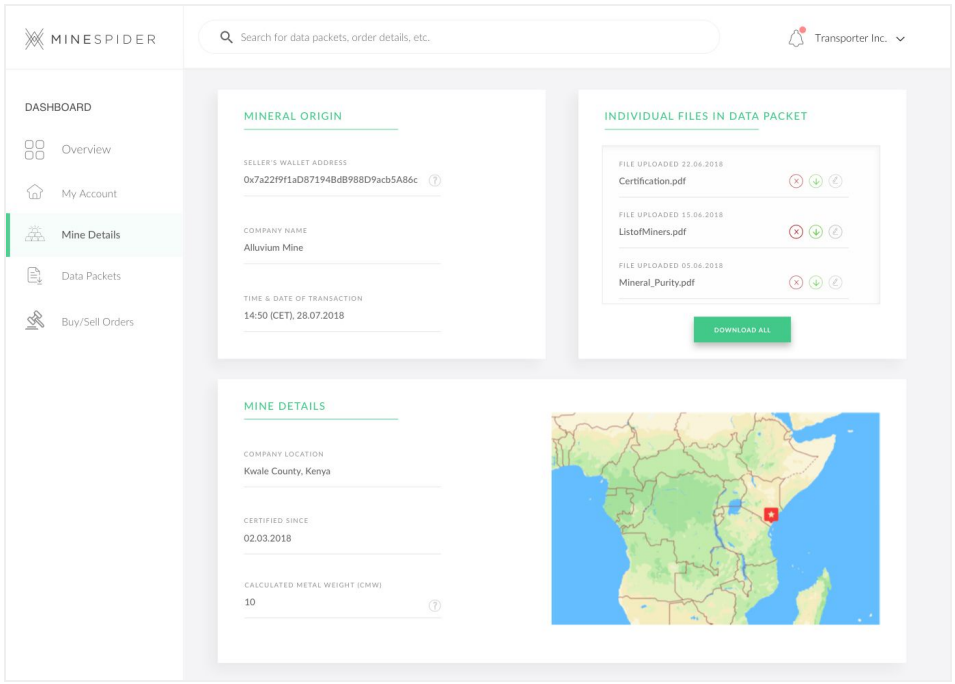

**With the transaction complete, the seller's token balance is updated**

### Explore Certificate

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




**User chooses to explore their owned certificates**




**User selects a certificate and sees the contained files and the regions of origin.**

## 3.4 Minespider Certificate

Minespider Certificate are not tokens.

Minespider Certificates are an immutable record of origin for an amount of minerals produced at a source that has been certified by a registered Minespider Certifier. They are digitally-linked records that document the ownership and link the provenance of mineral data. A Minespider Certificate consists of two components, one on each layer of the protocol (as described in 3.2):

1. Keys to access the linked data packets from the supply chain history of the metal, on the certificate layer (as described in 3.1.2)
2. An amount of mineral allowed to be sold, stored on the blockchain layer.

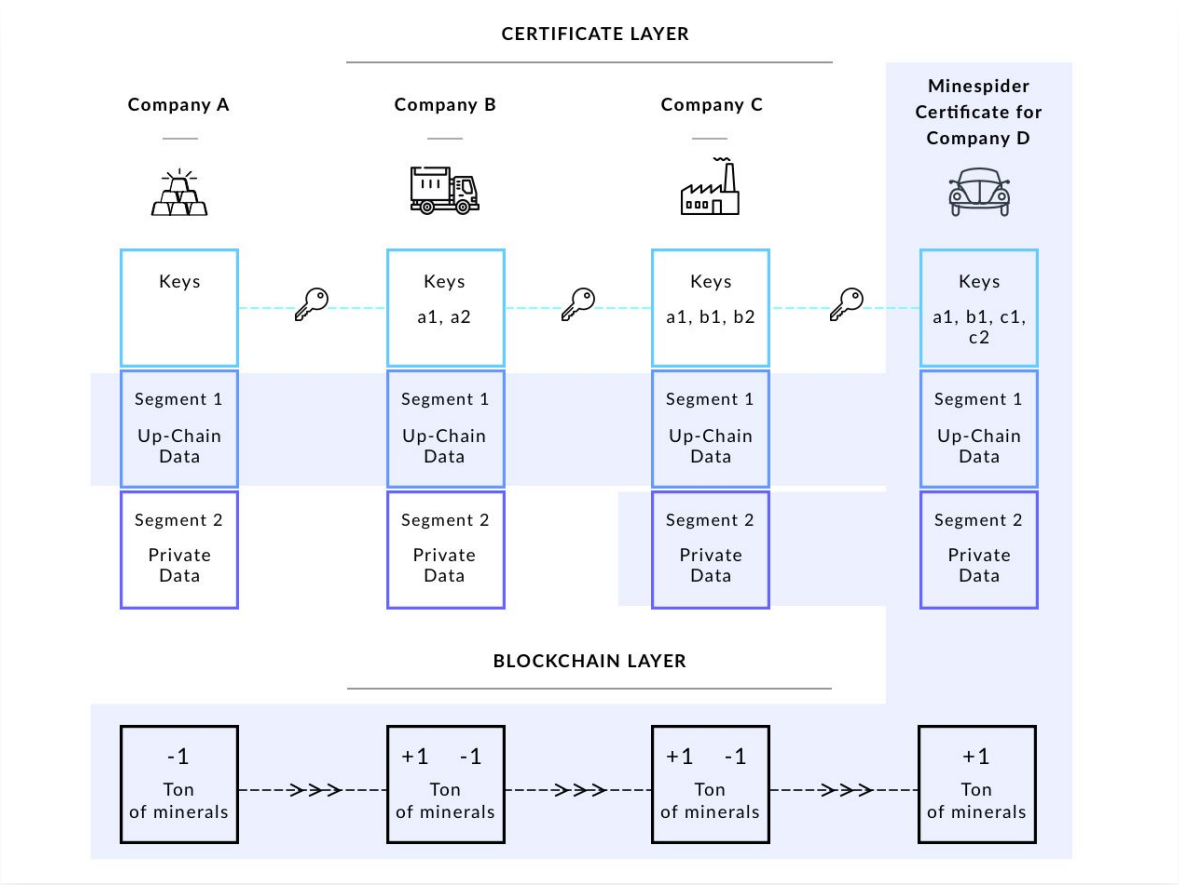
Purchasing a certificate to one ton of material means receiving:

1. An allowance on the blockchain layer to sell one ton of the material
2. The key to segment 2 of the entity the minerals were purchased from (private data)
3. The keys to segment 1 of the entity the minerals were purchased from and every entity who came before them in the supply chain also. (up-chain visible data)

Selling a certificate for one ton of material means:

1. On the blockchain layer, reducing the allowable mineral sale allowance by one ton.
2. On the certificate layer, creating a data packet with up-chain visible (segment 1) and private (segment 2) data.
3. Encrypting all the segment 1 keys held for the mineral and the new segment 2 key with the public key of the buyer and posting it in the certificate layer.

Note that selling a certificate does not mean losing access to the provenance for the mineral. Once a supply chain participant purchases a certificate they remain able to access the history of that certificate. In addition, when a supply chain participant sells a certificate, the supply chain data they provide will remain, providing a provenance link for downstream users of the mineral.




### 3.4.1 Certification Data Collection

The quality of the data in the Minespider Infrastructure is very important. Evaluating the quality of due diligence data is a delicate process. Having no evaluation scheme may leave the system open to useless data being sold as useful, yet having a too-rigorous evaluation scheme could hinder adoption, as different companies, state actors, and metals may have different requirements.

Minespider's position is that an open system is best, and that the issues of data quality assurance may 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 Responsible Minerals Initiative (RMI) is developing official blockchain guidelines for data and events to be collected and Minespider is considering these as a guideline for data collected by the system.

## 3.5 SILQ Token

The Minespider Infrastructure and ecosystem is facilitated by the Minespider SILQ utility and payment token ("SILQ"). The SILQ is issued by Minespider GmbH. It is an Ethereum based and ERC20 compatible token (Ethereum Blockchain based standard), that serves to incentivize and utilize an active participation in the Minespider Infrastructure.

The SILQ token enables at minimum the following functionalities at the time when the SILQ is first emitted:

### 3.5.1 Using the Minespider DApp

SILQ provides the means for using the Minespider DApp within the Minespider Infrastructure. This includes

- Option to register as a Mineral Producer or Certifier of mines on the Minespider infrastructure by staking SILQ.
- Option to register as a mineral producer to receive a certificate production limit on the Minespider Infrastructure by paying a certifier and staking SILQ.
- Option to register as another supply chain participant (smelter, refiner, transporter, manufacturer etc) by staking SILQ.
- Option to create Minespider Certificates for mineral shipments as a registered Mineral Producer, up to a maximum of the registered production amount.
- Option to sell owned Minespider Certificates or purchase Minespider Certificates from a certificate owner.
- Option to register a mineral transformation on a Minespider Certificate as a registered smelter or refiner.
- Option to add relevant due diligence, provenance, audit, or other relevant data to an owned Minespider Certificate.
- Option to create or process relevant data sets for owned Minespider Certificates on the Minespider Infrastructure by staking SILQ.

### 3.5.2 Payment Function

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 SILQtoken provides an incentive for members to perform operations supporting the Minespider Infrastructure such as data storage and processing. SILQ can in particular be used as a means of payment to obtain/sell Minespider Certificates.

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

### 3.5.3 Incentive Function

Moreover, SILQ can be a means to incentivize supply chain actorss from the minerals industry, manufacturers of products and end-customers to use the Minespider Infrastructure, to prepare, use or circulate Minespider Certificates.

### 3.5.4 Governance Function

SILQ can also be used as a stake to register a DApp for use on the Minespider Protocol. DApps wishing to interact with the Minespider Protocol must first stake SILQ and then be approved by Minespider GmbH (or, in future, by a trusted entity or stakeholder group). In addition to allowing for version control of the Minespider DApp, this protects supply chain participants from data vulnerabilities. DApps are distributed in nature and certain data security functions occur at the DApp level. Requiring apps to stake tokens and undergo code review for being officially registered helps protect this sensitive data from malicious actors.

# 4. 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 the Minespider team is committed to working toward ASM inclusion and incentivization as the infrastructure is rolled out. Some of the initiatives we are considering include:

- ASMs may receive subsidized SILQ holding accounts for joining the system. Subsidies should be based on a sliding scale so that the poorest producers do not bear a disproportionate cost burden for joining the system.
- Developing a specialized DApp for ASMs with a focus on usability by the artisanal demographic.
- Working on integration with official state buying systems for artisanally mined minerals.
- 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 Minespider Infrastructure and associated services on the improvement of the lives of ASMs and ASM communities may need to be evaluated to improve the platform and ensure that it meets the relevant development goals.

# 5. Potential attacks and recourse

During the ideation process a number of potential attack vectors have been identified that could compromise the Minespider Infrastructure if not addressed.

Please note that the following scenarios are not exhaustive. This list is by far not a complete list of all actual or potential risks. Also the mentioned "possible ways to address" the risks are meant to be understood as assumptions that may not have been tested or verified. For more information, you may contact us. For a full risk assessment do not rely on the Minespider team nor the following scenarios alone, but contact an independent external professional for risk assessment and guidance.

## 5.1 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 create Minespider Certificates, a mineral producer given a "speed limit" based on their estimated production. The speed limit is set by a certifier registered on the protocol and is tracked on the blockchain. This limits the amount of certificate they produce. The certifier's attestation to the production limits of the mine add a layer of trust.
b. The risk of mineral laundering is higher in some geographies than others. By working with NGOs or other entities it may be possible to identify which mineral sources are of a higher risk than others.
c. In the future, analytical software may be developed by Minespider or third parties to assess and evaluate certificates and their provenance data.

## 5.2 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 certificates 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 segment 1 of the certificate.

## 5.3 Unsecure DApp Scenario

Certificate 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. Requiring new DApps to stake SILQ and then undergo code review before allowing them to use the protocol.
b. Educating companies who use Minespider DApps about how to maintain data security

## 5.4 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 independent entity offering custodial services  This would be at the company's discretion and should not be built into the system.

## 5.5 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 can mean it is auditable.  Larger scale fraud may 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. Traditional anti-corruption measures, such as 4-eyes principles as well can be used in conjunction with Minespider Certifications to prevent this scenario.
c. Ultimately this is an issue of which certifiers are trusted. Requiring certifiers to stake SILQ in the system to maintain their status gives a mechanism for the policing of certifiers by the industry.

## 5.6 Misrepresenting the amount of mineral transferred scenario

It is possible for two adjacent supply chain actors to collude to register a larger transfer of material in the blockchain than was actually transferred.  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. The potential for this scenario may be addressed by requiring shipment numbers for most supply chain actors. This could limit the opportunities for misrepresentation to refineries and smelters where mass balance needs to be employed.

# 6. Next Steps

The Minespider Protocol is a work in progress and the project as a whole is under development. If you are interested in supporting the project, investing, or being part of a pilot project, please reach out to our team.

hello@minespider.com