Why Blockchain?

This document is intended to summarise the principal benefits of using blockchain technology as a backbone to Veratrak's software, primarily as an irrefutable audit trail.

What is blockchain:

First, some keyword definitions:

- **Blockchain** (a.k.a. *Distributed Ledger Technology*) is a ledger which is distributed across different regions or environments.
- **A ledger** is a time ordered list of transactions.
- **A transaction** is a tamper-proof, uneditable digital record distributed across the entire network of computer systems on the blockchain.
- **Smart contract:** transaction data can be a list of instructions, or a piece of code. This is called a Smart Contract.

In a way, most blockchains are similar in the way they store data to a NoSQL database. Traditionally a ledger or database would be owned and managed by a single entity, which means that trust has to be instilled in the administrator and the way they validate information passed through their system.

However, with blockchain, this responsibility is decentralised and trust is made explicit by being able to verify the code used to store data and to run one's own instance for an equal stake in contribution to the global ledger state.

How is the blockchain controlled:

Networks like Bitcoin's are what's known as public, 'permissionless' blockchains. For applications like currency, this makes sense because anyone can participate in the network and typically may "mine" currency by providing validation to the network, which means there must be a way for a user to create a "node" for validating transactions on the blockchain.

This public network structure results in significant additional performance and security considerations.

Networks like Veratrak's are what's known as private, 'permissioned' blockchains. For enterprise applications, these kinds of blockchains make by far the most sense. There is no reason for the public to be able to host validators for the network, since the information is intended to be used for internal and chosen third party reasons (like an audit).

This means that the architecture of a private network–while still decentralised–can be much more tailored for the performance of the network and security is more easily achieved.

Why is blockchain needed:

Blockchain technology has several properties that make supply chains a powerful application context. In essence, to decide whether a blockchain application might supersede a typical application for a given purpose or industry, it's important to note what blockchain is especially useful for.

In particular, for systems where there are multiple parties involved who do not necessarily share implicit trust, blockchain provides the necessary validation capabilities to effectively alleviate this concern–this can increase visibility and trust for key partners and the organisation itself.

When it is integrated within the pharma supply chain, it offers many benefits such as traceability and high operational efficiency of supply chain management via secure monitoring, auditing and mapping.

With our solution, the source code (of our smart contracts) which store transactions on the blockchain can be cryptographically verified by desired parties. This means that there is zero ambiguity of what software is running on the system in order to validate information being passed to the network.

This is different from a distributed database because the validation of information stored on the blockchain occurs in a decentralised manner rather than a centralised one. This means that trust does not have to be implied, rather it can be proven and shared across multiple parties.

Benefits of applying blockchain to a supply chain audit trail:

- **Immutable** - the ledger cannot be tampered with because its current state is the sum of all previous states–everything is continuously validated, per transaction and beyond–this means things cannot be edited after the fact (without submitting a new transaction), and any retroactive tampering (though extremely unlikely) would be evident.

There are some "traditional" software solutions/databases which adopt similar concepts, but they do not benefit from the smart contract system Fabric supports.

- **Secure** - Hyperledger Fabric is an open-source blockchain project built for enterprise by some of the most established & innovative technology companies in the world. Its well-considered architecture builds upon best practice software development concepts & solid cryptography, as well as an efficient blockchain implementation.

- **Verifiable** - Chaincode (a.k.a. a smart contract) is core to how Fabric operates, and means we can have a repository of code that can be inspected and validated by whomever necessary. Further to this, it can subsequently be cryptographically verified as the exact source code the chaincode instances running on a given blockchain are using. Chaincode runs across multiple peers and must reach "consensus" before a record is stored on-chain.

In future, our "External Peer" support will arrive which will allow our customers to run their own distributed peer which become partially responsible for the validation of transactions.

- **Unique** - our novel solution for industry-wide analytics is that partner blockchains can share (verifiably non-sensitive) information with our "parent" blockchain (codenamed "The Oracle") which in turn processes the event and uses its knowledge to disseminate relevant information to the intended partner chains–all supported by additional chaincode to the core contract.

In turn, partner chains will process these events and generate relevant insights or opportunities within our dashboard. The intention is this will allow for unprecedented collaboration between Veratrak partners in future.

- **Private** - the way we store information on-chain means that the data stored there has utility, but only when accompanied with the requisite associated information, stored ephemerally by Veratrak and after successful export owned solely by your organisation. On its own the data stored in our default records is not useful nor is any private information contained within them.