SynComm Hardware Oracle (SHO)

Introduction:

WHAT ARE ORACLES?

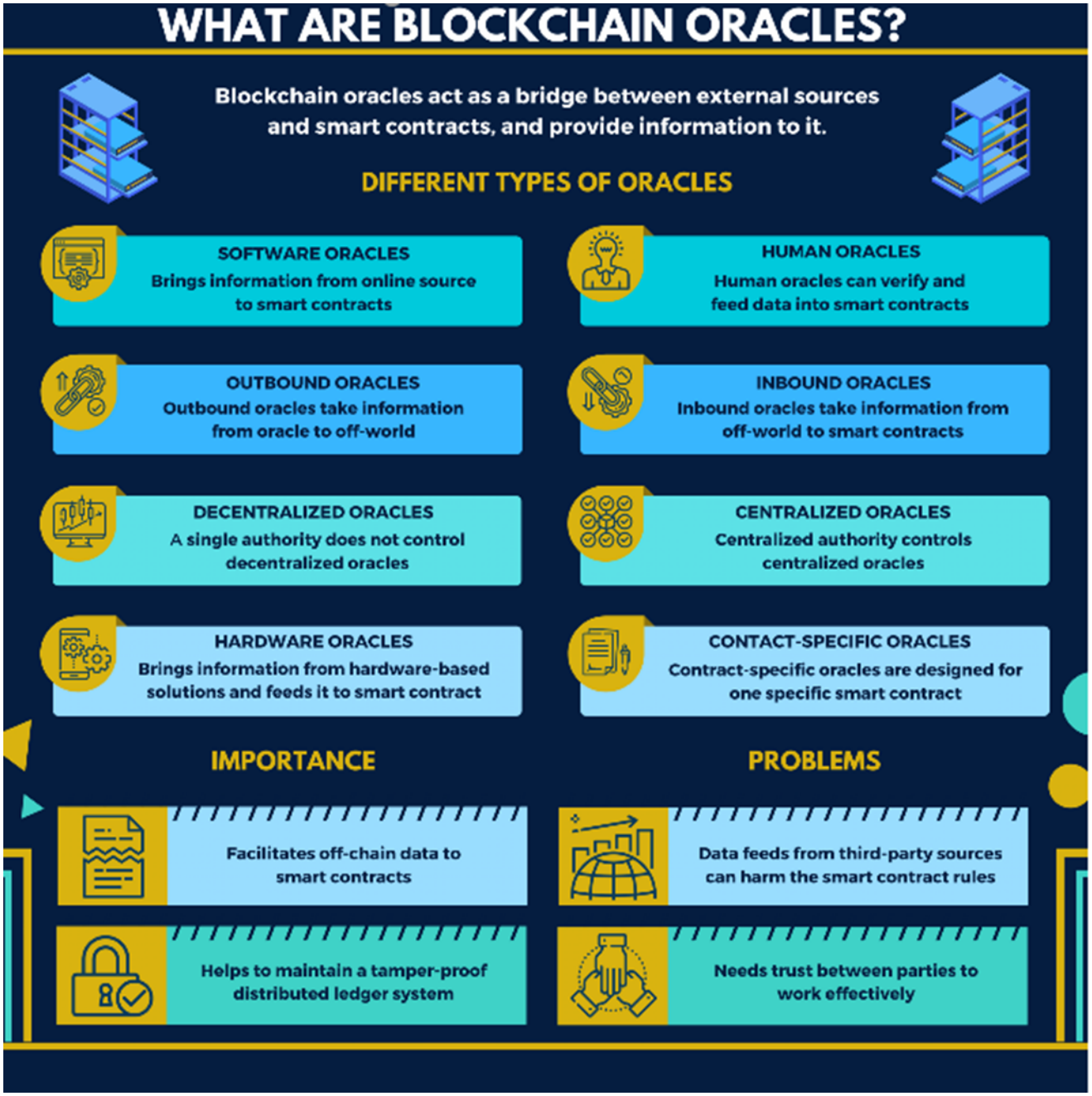
Oracles are middleware which allow blockchains to communicate with external data sources, then deliver this data to a contract safely. Oracles allow market data, iot data, shipping data, and real-world event data to be delivered without manipulation or corruption. They bring end-to-end reliability to smart contracts. If a smart contract can be manipulated or easily broken by tweaking inputs or outputs of data, it destroys the entire system's integrity. Oracles bring system reliability, allowing smart contracts to become a superior way to do digital agreements.

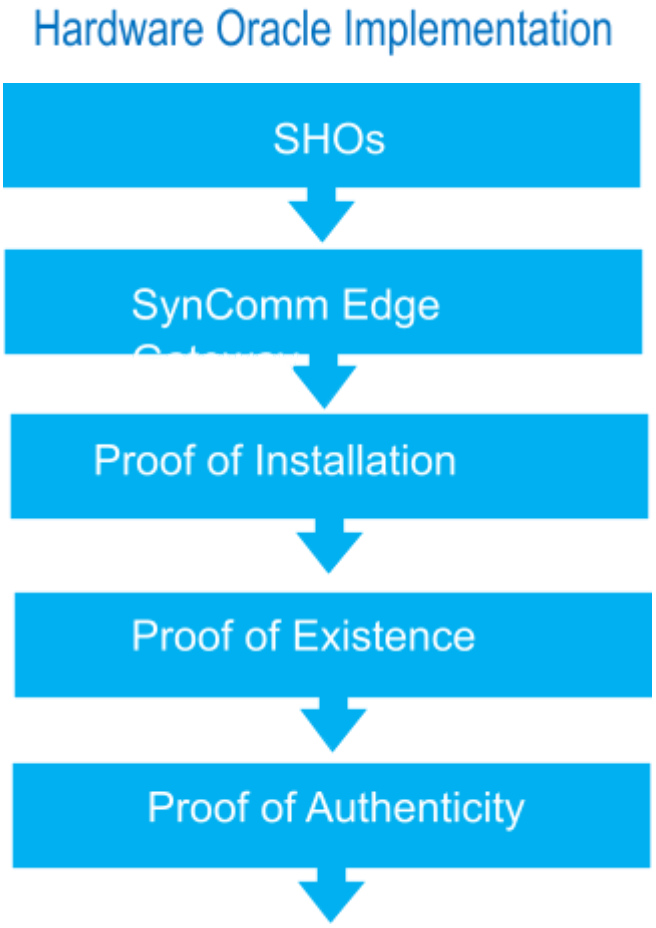
SynComm hardware oracles are light clients on the SynComm network and are trustless data feeds to SynComm smart contracts using cryptographically signatures to sign all data an asset produces, proving its source.
HO's have been developed to communication linkages between the real-world economy and the blockchain ecosystem, SynComm has developed a series of proprietary hardware oracles with limitless functionality through the use of IOT sensors, off chain data feeds and encrypted communication channels using data generated from dataloggers. This type of information is crucial for applications such as registering event occurrences, which in turn are used to execute conditions contained within smart contracts. The hardware Oracle (datalogger) provide a pathway for decentralized applications to connect with physical businesses, in a supply chain environment it can track goods arriving at a warehouse and execute a smart contract based on this event.
This ongoing cryptographic verification is recorded on a public blockchain, providing a trustless verification of provenance for all output of the system, including production data.
The SynComm oracle ecosystem seeks to form a decentralized network of industry and application agnostic telemetry sensors at the edge, using light nodes and staking wallets to deter any manipulation of off chain data sources. Built on the Binance Smart Chain and using certified and witnessed metering data at key nodal branches, the hardware oracles will provide for trustless onboarding real world data and market conditions as inputs into smart contracts.

SynComm Oracle provides a way to get outside data from any web API or IOT device data steam onto the blockchain.

To use it, you'll use SynComm Oracle smart contracts to send a query to SynComm with your API call. Once they get a result from the API, they call a function named

__call back in your smart contract and pass it the result as an input.
“oracles”—which are basically contracts which pump data into the blockchain for use by other smart contracts.





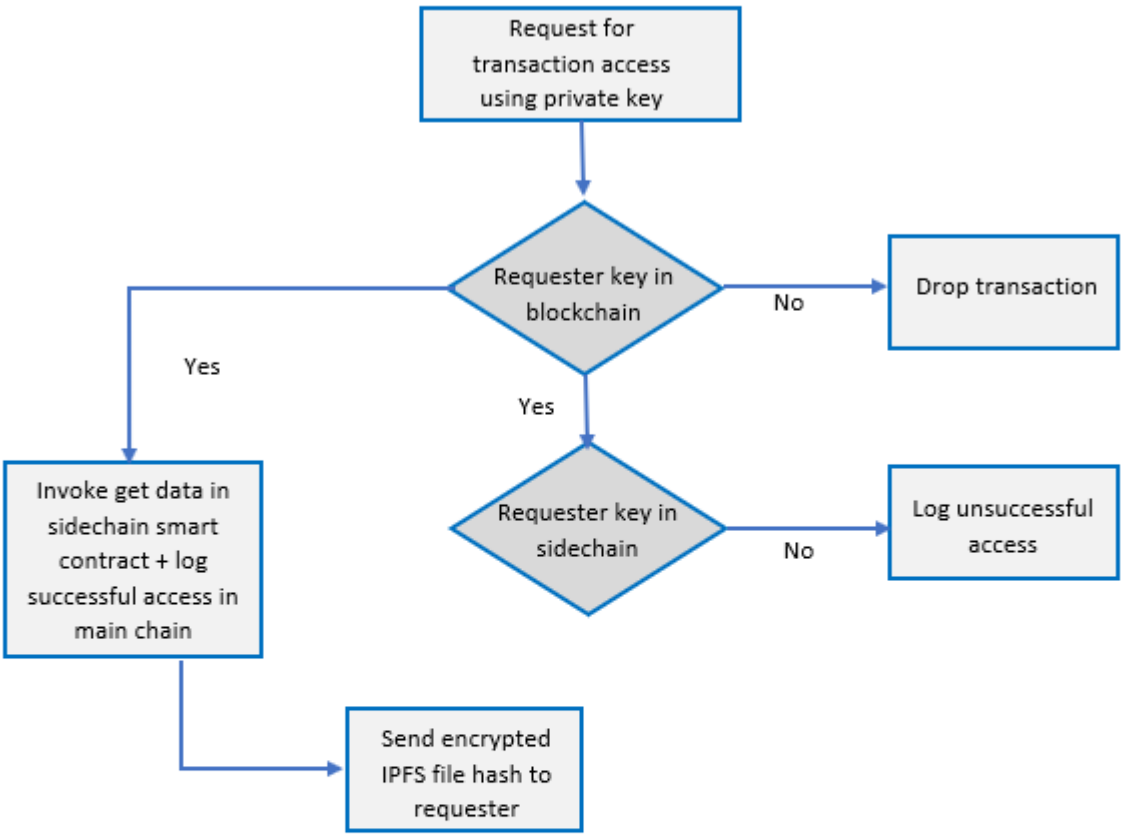
SHO's

SHO' provide the basic building blocks for the SynComm oracle ecosystem, its design ensures a distributed trustless supply of data through a robust, cryptographically verifiable data stream from the generating asset through the entire chain of supply, through to the end user. SHO's are designed to be installed on virtually any asset in any environment both mobile and fixed applications, using grid, intermittent or battery power supply. SHO's are designed to be integrated into any asset either at the time of manufacture or later through pairing via a proof of installation. The private key for the SHO is provisioned at the factory. The public key is then signed by the SynComm Certificate Authority. The SHO combined with Distributed Ledger Technology provide assets and smart contracts with tamper resistant, high-quality data that can be traced and traded on with confidence.
The SHO contains a unique key hardwired into the module, which cryptographically signs all data an asset produces, proving its source.

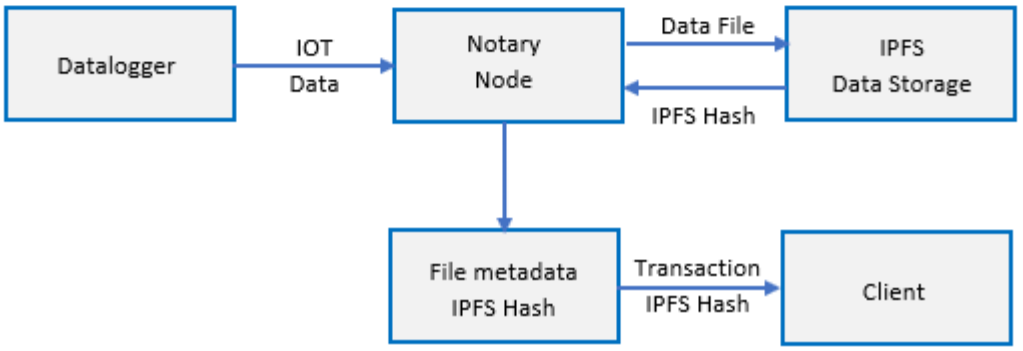
Provenance is guaranteed through a combination of the Proof of Installation and Proof of Existence events. These events together provide an initial and ongoing

cryptographic proof that guarantees the existence of a physical asset and tie it to a particular source.

ACCESS CONTROL STRATEGY (ACS)



DISTRIBUTED DATA STORAGE SYSTEM (DDSS)

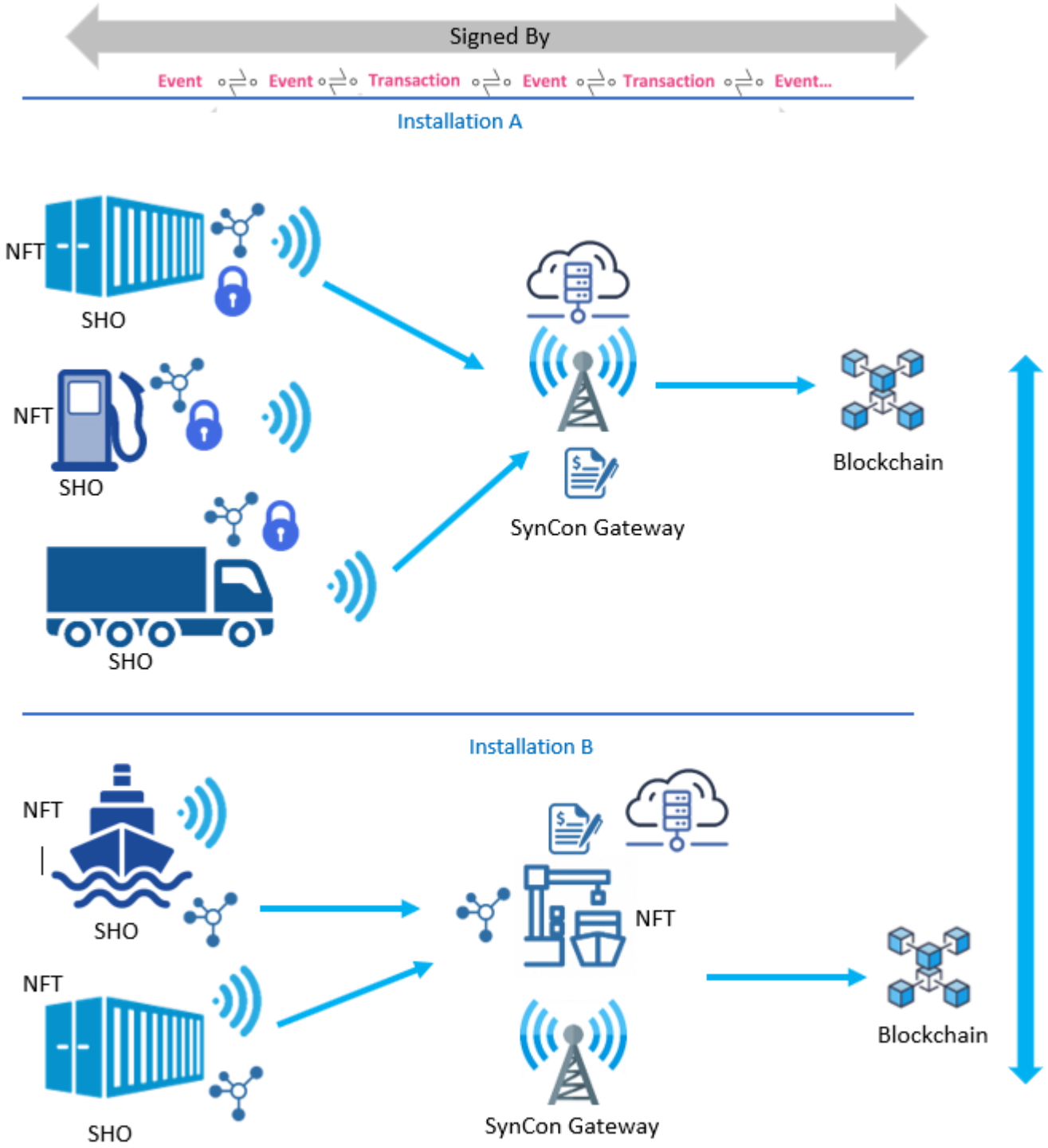


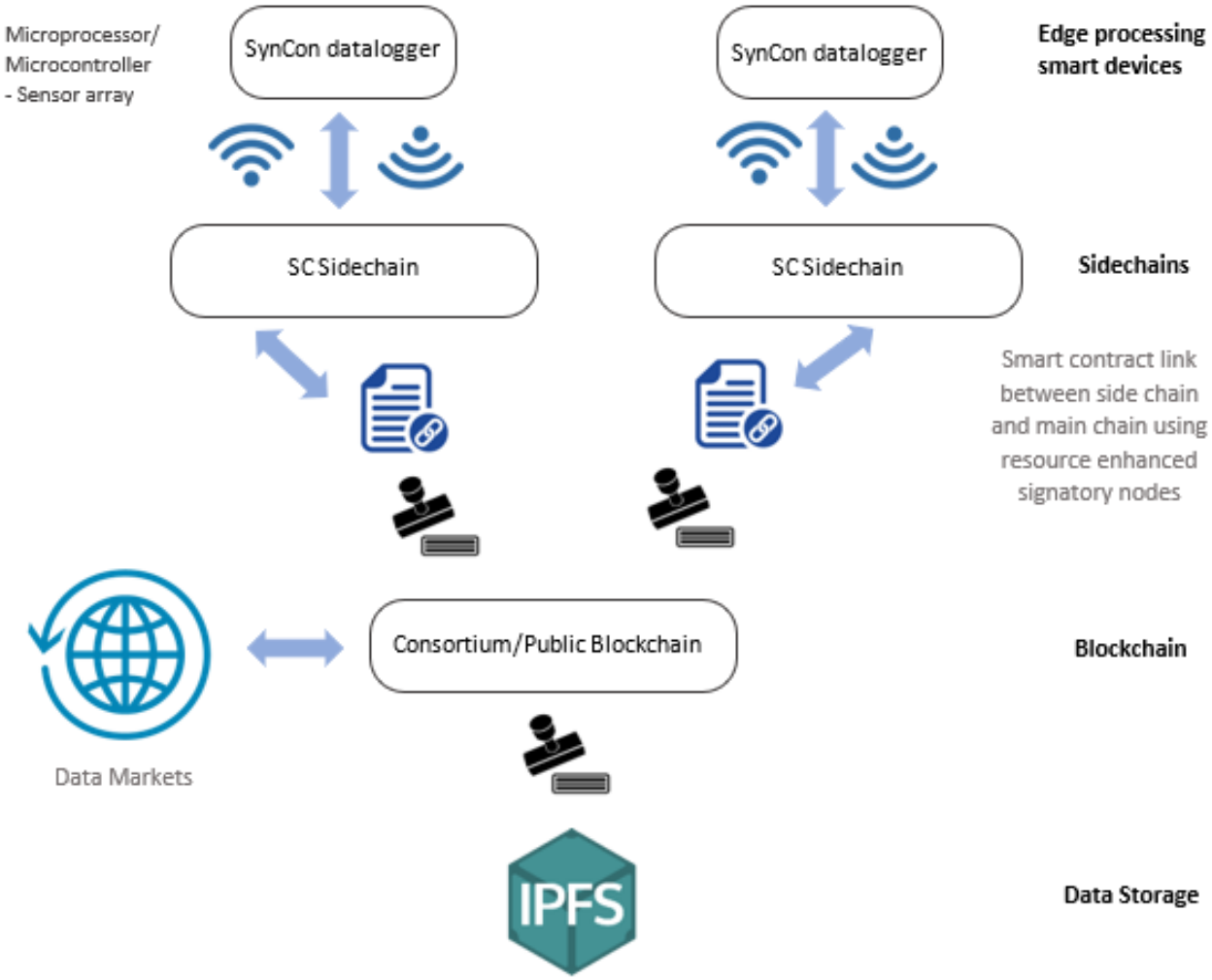
SynComm Edge Gateway

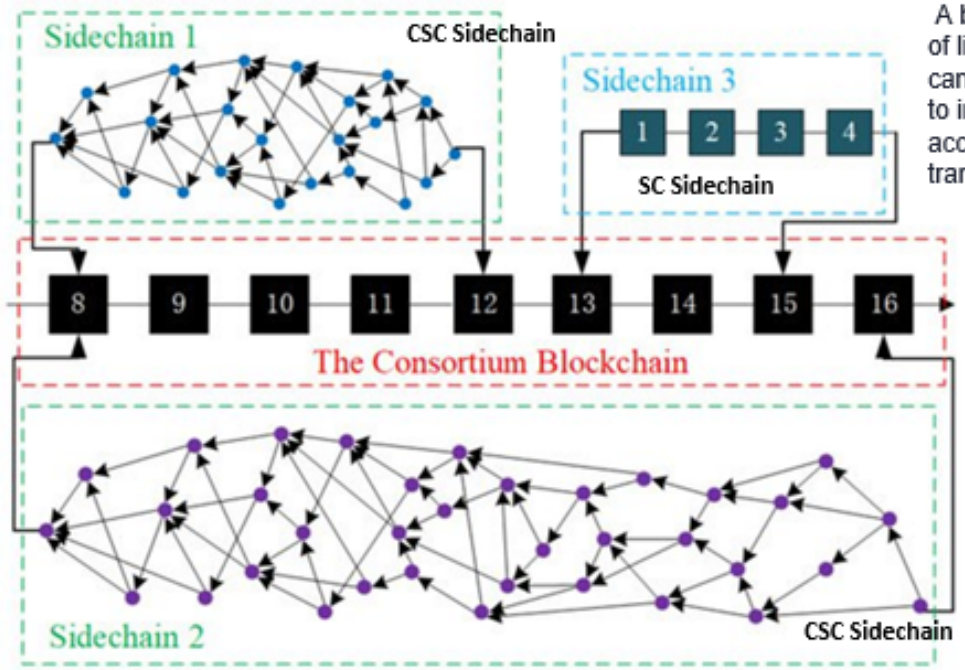
In each installation there may be several different assets and multiple SHO's vehicles, shipping containers, generators, etc., these assets SHO's are in fact lightweight nodes on the SynComm blockchain.

The SynComm edge nodes which are full nodes and support the network by accepting blocks and transactions from other full nodes, validating those blocks and transactions, and then relaying them to other full nodes. They are trustless, they will reject any block or transaction that violates consensus rules, even if every other node on the network thinks that it is valid. Full nodes can also act as an edge gateway for lightweight nodes (also known as lightweight clients). Lightweight nodes verify transactions using a method called simplified payment verification (SPV). SPV allows a node to verify if a transaction has been included in a block, without having to download the entire blockchain. With SPV, full nodes serve lightweight nodes by allowing them to connect and transmit their transactions to the network and will notify them when a transaction affects them. A lightweight node need only download the headers of all blocks on the blockchain, which means that download and storage requirements are significantly less intensive than that of a full node.

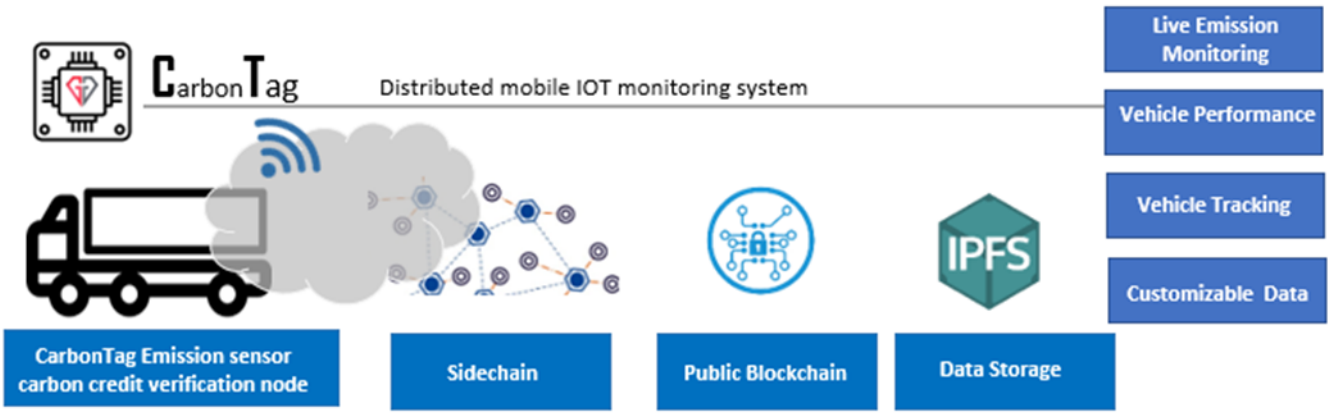
The SynComm Edge Gateway nodes coordinates the behaviour of each of the lightweight clients. SHO's are lightweight clients with low-power and low-cost devices with minimal computing power. The SynComm Edge Gateway provides the nodal intelligence and computing power to aggregate signed telemetry sensor proofs, facts about the current deployment, and production of the infrastructure. The SynComm Edge Gateway acts as a secure collection point and aggregator for various supply chain, distribution, storage, and consumption components. It absorbs signatures from the SHOs and provides witness to the broader SynComm blockchain and is the point from which decisions are made and automatically executed from lines of code embedded into smart contracts that drive the greater ecosystem. SynComm Edge Gateways aggregate mesh network telemetry and coordinate via backhaul for public-facing proofs.


Signed By
Event
Event
Transaction
Event
Transaction
Event...
Installation A
NFT
SHO
NFT
SHO
SHO
SynCon Gateway
Blockchain
Installation B
NFT
SHO
NFT
SHO
NFT
SynCon Gateway
Blockchain





A blockchain consortium of like-minded companies can leverage information to improve workflows, accountability, and transparency.



Proof of Installation

To be able to provide public confidence and to guarantee the authenticity in the data generated by the hardware oracles a Proof of Installation (PoI) needs to be undertaken.

The Proof of Installation is a cryptographic “handshake” that binds an asset’s serial number and device manufacturing metadata to a derive a hardware based cryptographic “seed” that instantiates the device’s profile, to be then recorded on a blockchain.
Trust (via key management) is established at the very beginning of the asset’s life cycle, preventing fraud and market manipulation that may undermine investor’s confidence in trustless assets.

The asset will also undertake a digital identity process where it will be converted into a Non-Fungible Token (NFT) which assigns the assets features and identity as well as ownership details on the blockchain. The NFT can then be used to generate liquidity pools, traded to raise capital along the lines of traditional financing where the asset for the security for centralized debt financing.
The PoI can be used for any assets, supply chain actions, component of a project, and be aggregated to a single, cryptographically secure authenticity rating. This increases the difficulty for bad actors to fake or manipulate a single aspect of a project, supply chain, or financing and insurance funding and claims.

Proof of Existence

The next level in the SynComm ecosystem is centred around the continued validity of data from the SHO after the PoI has been completed and involves another process referred to as the Proof of Existence (PoE). The Proof of Existence utilises the unique identifiers of a device in combination with the digital output flow off its

SHO to continually prove the functioning of an asset. For example an off chain in-bound oracle linked to the Department of Transport can confirm the registration of a vehicle (its existence) the NFT database can confirm the ownership of the vehicle and the vehicles SHO through its Proof of Installation and connection with the vehicles CanBus link will provide the unique identifiers which will confirm the location and trip logs of the vehicle, weight loads along the pickup and drop off locations its emissions, fuel consumption, driver behaviour, incidents and accidents, any modifications to or performance changes in the vehicles engine outside the unique identifiers margin of error will trigger an audit and/or penalty against the SHO's staked wallet. Each asset through its SHO has a unique identifier, this identifier is unique to each SHO and the digital signature of each identifier will be recorded during the PoI process.

The unique identifiers in the SHO microcontrollers already ensure a that they have a hardcoded unique 128-bit unique ID that can be read using IAP functions, and this can be further enhanced and managed by shell-scripts to hard-core an additional Unique ID during the PoI on each firmware built along with its asset NFT identifiers.

Then there's coding the ID in non-volatile memory. This will be input via an in-circuit programming device, with the ability to write to non-volatile memory (for example IAP flash-writing functions, or built-in EEPROM).

These unique identifiers prevent bad actors attempting to fraudulently provision infrastructure would first have to compromise the security of the individual SHO and simulate their unique characteristics simultaneously with every other SHO on the SynComm gateway – a process that becomes increasingly difficult to try orchestrating with scale as more assets are deployed.

Upon registering an asset and deploying it in the form of a NFT on a decentralized Asset Registry (IPFS), asset owners will be able to create, finance/refinance and distribute their assets as digital assets in the form of a NFT Asset Token. Asset owners may choose to issue ERC20/EIP20/ ERC721 tokens to represent fractionalised ownership of solar assets.

This would allow asset owners and SYC token holders to participate in additional secondary markets for asset trading, financing and data services or analytics resale, all secured by the Proof of Installation event and the SynComm Hardware Oracle (SHO).