Using Blockchain: A Practical Example

Whitepaper | Authored by Quisitive Consultant, Chris Rogers

THE BIRTH OF BLOCKCHAIN

10 years has passed since the birth of blockchain. In that time, many crypto-currencies have been created and the technology has been investigated and discussed to death in academic and technological circles, yet most businesses have not added it to their IT toolbox. Some attribute this to the fact that there hasn't been a "killer app" for block chain to use. Others simply believe that blockchain is a meaningless technology that serves no real purpose aside from currency speculation and masking transactions. But, the simplest reason for the lack of large scale adoptation of blockchain in the business world might be that practical examples of how blockchain can be used to address real business challenges are few and far between.

BLOCKHAIN TO IMPROVE REGULATORY COMPLIANCE

This article will attempt to illustrate one practical approach for utilizing a private blockchain. Rather than focusing on financial transactions or tracking products, this case will examine how blockchain can be used to provide improved regulatory compliance, minimize losses due to equipment failure, and ensure vendor compliance with SLAs.

The subject of this case study is a fictional company called MQI. MQI is a small oil and gas firm that was formed as the result of divestiture of equipment and staff from a larger energy company. MQI inherited three fields across the globe with a total of 20 active pumps, a few kilometers of pipeline, and 3 active drilling sites. Whereas the larger company had the resources and staff to stay on top of each of these sites—keeping the equipment operational and safe—MQI has found itself in over its head and has had many malfunctions and leaks since the creation of the company. This has led to increased regulatory oversight, fines, and a loss of revenue.

The primary challenges facing MQI are:

- National, Regional, and local regulations regarding reporting and enforcement of environmental and safety matters vary between the three different fields. MQI needs to be able to supply the raw data to one or more providers who can craft the correct reports for each area.
- Equipment breakdowns, leaks, and sabotage have been plaguing MQI and driving up costs through product losses, fines, and additional regulatory compliance. MQI needs to ensure that maintenance on their equipment is being performed on a regular basis and can be verified at any time by a third-party auditor.
- Much of the equipment is very remote, far outside of the coverage of cell phone towers. To check on the status of the equipment, MQI has been relying on contractors to perform scheduled visits and report back. Emergency notifications are handled through expensive radio links that are subject to environmental disruptions. MQI needs to improve its monitoring capabilities and response times. MQI would also like to receive near real time updates of the status of the equipment and be able to dispatch technicians on demand, so that minor problems can be resolved before they become major issues.
- MQI does not hire the engineers and technicians directly. Instead, they subcontract out maintenance and repair work to local contractors. Every year, MQI reviews the performance of these contractors and renews or cancels their contracts based on these results. MQI needs to be able to correlate the performance of the field equipment with the contractors that were assigned to maintain or repair that equipment.

BLOCKCHAIN IMPLEMENTATION TO MINIMIZE LOSS

After a review of their options, MQI elects to implement a system backed by a private consortium blockchain. The members of the consortium will be some of MQIs vendors, a third-party auditing firm, and MQI itself. MQI will utilize Microsoft Azure to host the blockchain along with the other servers and functions that will be needed to communicate with the blockchain and with external providers.

The biggest hurdle MQI is facing with the population of the blockchain is acquiring information about the status of the equipment in the field. Most of the equipment is far too remote to send information to internet based servers via cell towers. For this challenge, MQI has decided to turn to the Iridium satellite constellation.

The Iridium constellation gives MQI the ability to send messages from their equipment to the constellation and then, by way of ground stations, to a host on their Microsoft Azure instance. The high availability and low latency (40–50 ms) provided by having a constellation of satellites in low earth orbit (multiple satellites moving across the sky in a predictable orbit) vs a singular satellite in a geo-synchronous Orbit (fixed place in the sky) gives MQI the ability to send emergency alerts in near real time as well providing regularly scheduled system updates.

At each well site and at strategic locations along their pipelines, MQI will install a small computer (known as an edge computer) along with a robust battery system and a solar charging station. Smart sensors at each site will provide data to the computer, which will maintain a local view of the status of the various equipment being monitored. In addition, the edge computer will analyze the smart sensor data for any critical values.

In the case of a critical value, an alert will be composed and sent via modem to the Iridium constellation immediately. Otherwise, the monitoring software will compose a delta report showing changes to its view of the equipment since the last report was sent and will send that delta report in one-hour increments. This delta report will reduce data costs while ensuring that the blockchain always contains a reasonably accurate representation of the equipment. Once a day, and at the end of a maintenance session, a full report of the current state of the equipment will be sent to validate that the blockchain and the edge server are in sync.

When the edge server sends a message to the constellation, it is routed to the nearest base station which then sends it to a predetermined IP address. MQI has chosen to utilize Microsoft Azure's Service Bus to listen for incoming messages from the Iridium base stations. Once a message is received from the base station, it will be processed and routed to the blockchain and any other internal monitoring services that have subscribed to that message type.

Iridium does not perform any message management, thus in order ensure that the messages are received in the correct sequence, MQI has chosen to mark each message with a precursor tag indicating the order in which the messages should be processed. If a precursor message has not yet arrived, a possibility if there are service outages or delays in the delivery of a message, the messages are queued until they can be processed in the correct order.

SMART CONTRACTS TO ENSURE VENDOR COMPLIANCE

When a message is processed, the updated data is fed to a smart contract on the consortium blockchain. This smart contract will update values related to the equipment being monitored. External systems that are monitoring the equipment status, such as a systems dashboard at MQI headquarters, will realize these changes as soon as the blocks are mined and take the appropriate actions.

One external system that MQI has also chosen to implement is an automatic dispatch system to improve response times for equipment failure and environmental emergencies. When a message arrives indicating sensor readings that are out of family or if a station has failed to report in for two intervals, a monitor service which is polling the blockchain, will locate the assigned contractor for the equipment and will initiate the appropriate dispatching process for that contractor. It will then update the blockchain to indicate that the dispatch occurred, why it occurred, and what the expected SLA is for that dispatch.

Mechanite, one of MQI's vendors and a partner on the private consortium blockchain, has elected to host their own dispatcher service that integrates directly into their internal dispatching software. The principal dispatch service hosted by MQI will continue to behave as normal for the devices assigned to Mechanite, thus ensuring that SLA expectations, etc. are recorded correctly; however, Mechanite will be able to add additional information regarding when they sent their technician and which technician was assigned.

All technicians that will be servicing MQI's equipment, regardless of which contractor they work for, will be required to check in and out of the facility by swiping their assigned smart badge at the edge computer. The edge computers at each location will have a touch enabled display that will provide the technician with a dashboard illustrating the status of the equipment being monitored. This same display will also allow technicians to summarize their visit without the need for specialized equipment. Once a technician has checked out of a facility, a maintenance report and a current systems status report will be transmitted via Iridium.

Mechanite, has chosen to utilize their own specialized mobile devices for their technicians. Technicians will use the mobile devices to capture bar codes of the equipment they are servicing as well as log if parts are being replaced and other maintenance notes. At the end of their visit, Mechanite technicians will use near field communication from their mobile device to send a report to the edge computer that matches the MQI specification. The complete Mechanite report, including any images and video, will be uploaded automatically when the technician reaches an area with cellular or wi-fi service.

The MQI maintenance report will track the check in and check out times for the technician. It will also note what equipment was removed, added, or otherwise affected. Once the report has been processed by the blockchain, a service will evaluate the before and after metrics of the equipment as well as the response time of the technician and provide a score for the visit as well as updating the overall score of the contractor. If a score has fallen below acceptable values, alerts will notify management from both MQI and the contractor as well as the third-party auditing firm.

Stewartson & Partners, LLC (S&P) is an auditing firm that is also a member of the private consortium. Their responsibility is to ensure that MQI is meeting regulatory compliance needs and that they are achieving stated company objectives regarding costs, reliability, and safety in the field. In addition to receiving the alerts mentioned above, S&P has established their own polling system to track changes in the status of the equipment as well as monitoring response times, report submissions, etc.

While S&P is a consortium member, they are operating as independent observers. Thus, apart from mining nodes, they do not have any rights to write data to the blockchain. Instead, when a problem occurs at a field location, their polling software recognizes and tracks the status of that incident. Once the incident has been resolved, the necessary reports are automatically generated and sent to the correct regulatory bodies. On a periodic basis, regular maintenance reports are also generated and delivered to interested parties.

However, one of the municipalities that MQI must report to is unwilling to receive reports from S&P and insists on having access to the raw data. MQI has chosen not to give that municipality membership to the consortium—they do not have the computer power for nor interest in mining blocks—but has instead given it read privileges to the blockchain. The municipality will be responsible for polling the blockchain and generating their own reports as needed.

A SINGLE SOURCE OF TRUTH

This case study has been crafted as an example of how a blockchain can be used to provide a source of truth that can be trusted across multiple independent organizations. A case can be made that everything the blockchain is doing could be also done utilizing a central SQL database with clustering or even by using Microsoft's distributed CosmosDB. In fact, as with many technology challenges, there is often more than one way to accomplish a task. Picking the correct solution is a matter of deciding which is most appropriate for the business problem.

MQI chose to use a private consortium blockchain as a way of satisfying critics that were dubious about its reputation as a responsible company. With any sort of centralized database system under the control of MQI, there exists, at least in theory, a potential that MQI could modify the data to their favor. Even using a third party to host and run the database, there is a risk of agenda-driven manipulation of the data. Blockchain offers protection against this sort of data manipulation.
It is possible to forcibly alter a blockchain. In fact, the fewer nodes that are involved in the blockchain, the easier it is to alter it. However, such manipulation will result in a fork of the blockchain. It will be obvious that the manipulation happened, when it happened, and who changed it. In the case of MQI, this forward only immutability provides a valuable level of trust with their partners, regulators, and investors.

In addition to the trustworthiness provided by the blockchain, the distributed nature of it allows for security and loss protection. Each node on the blockchain—consortium members can have many nodes distributed around the world (or even above it)—has a complete copy of the blockchain. So if a node is lost due to a partner being removed or hardware failure, the rest of the nodes can still operate without worry of data loss. Conversely, if a new partner is added, the nodes they add to the consortium will each receive a copy of the blockchain and then begin mining blocks.

There is also a level of flexibility inherit in using blockchain technologies. As shown at the end of the case study, access can be given to organizations that are not consortium members for read only operations. New consortium members can also be added or removed as needed and they can host as many or as few nodes as they like. This allows for the organization that the blockchain services to grow or shrink in an organic fashion without the need for extensive planning on the part of any single member.

BLOCKCHAIN IS NOT A PANACEA

Blockchain is not a panacea. There are many circumstances where traditional database or even blob storage technologies are a better choice. However, when dealing with trust matters or business challenges that are distributed over multiple geographic, political, or organizational areas, blockchain can serve as a solid foundation for maintaining a reliable source of truth.

When blockchain is combined with other technologies, such as IoT and satellite communications, seemingly insurmountable business challenges can readily be solved. As more and more businesses discover how blockchain can help them reach their goals, their innovation will serve as inspiration for others and blockchain will become a foundational part of the IT landscape.

CLICK HERE TO LEARN MORE ABOUT QUISITIVE'S APPROACH TO BLOCKCHAIN SOLUTION DEVELOPMENT.