Blockchain Case Studies

Case Study 1 – Retail

Industry Retail

Highlight Establishing unconditional transparency in the food supply chain using blockchain hyperledger fabric

Overview

Company ABC Retail is an American Multinational Retail Corporation established in the 1960s. ABC Retail operates a chain of hypermarkets, discount department stores and grocery stores, globally. It has wholly owned operations in Argentina, Chile, Canada, and South Africa.

In terms of revenue, ABC Retail is the world's largest company, with more than US$ 500 billion. It has more than 2 million employees across the globe. ABC Retail was the largest U.S. grocery retailer in 2019, and 65 percent of BC Retail's US$ 500 billion sales came from US operations.

Problem Statement

The company under study has access to fresh produce all year round and buys exotic food from worldwide markets; it is known to have more variety than any other food retail chain in the world. Their food is generally harmless to eat; nevertheless, they still occasionally have had cases where their consumers fell sick. Recently, there were at least 18 reported outbreaks of foodborne illnesses in the USA, including the E. coli found in romaine lettuce.

With consumers in recent times having access to agricultural produce across the world despite seasons, locations or the environment, they have expectations of trust on these products available to them. The retail chain has four significant challenges in assuring consumer expectations.

The first one is about food fraud, where there are a lot of possibilities of substituting, tampering, and faking the products, either at the production level or during the transit.

The other issue is about illegal production, where statistics show that 10% to 22% of the agricultural products are not reported or not regulated.

The major challenge faced is about foodborne illness, where it was proved in 2018 that 1 in 6 people fall sick from contaminated food or beverages per annum.

In such cases, the costs of food recall are very high, as much as $10 Million for ABC Retail, in addition to the loss in goodwill, loss of consumer confidence, and legal implication.

All the above challenges have resulted in high costs of the food chain in the following areas:

- Visibility into the status of goods as they move through the supply chain
- The cost of human health and life
- The cost of recalling contaminated food.

When there is an adverse event of a foodborne disease outbreak, it takes a long time, often in the order of days, to find the source of the disease. This is because the contamination could have occurred during the production, transit, or distribution channels. If there is better traceability possible, the companies can act fast, try to solve the issue and protect the farmers by removing the produce from the affected farms.

This, in retrospect, led to their interest in enhancing transparency and traceability throughout the food system. The company has tried many methods and approaches to solving this problem over the years, but none of them gave them the results they were looking for.

Approach

In 2016, ABC Retail established the Food Safety Collaboration Center in China, to develop its food provenance pilots using blockchain with a plan to invest about $25 million over the next five years to research global food safety.

The company looked into several blockchain technologies and eventually decided to use hyperledger fabric because it met most of their demands for blockchain technology. Hyperledger is an enterprise-grade blockchain technology. Hyperledger is also a permissioned blockchain. The team also found it essential to use an open-source-based blockchain so that it is vendor-neutral. The technology ecosystem has to be open since ABC Retail worked with many suppliers, distributors, direct competitors, and geographical collaborations.

ABC Retail decided to run two pilots concurrently to test the blockchain solution for traceability and transparency of the supply chain from end to end. Two use cases were tested – the traceability of mangoes, which are sold in the US stores of the company and the traceability of pork sold in their stores in China.

Life of ABC Retail mango typically consists of the following duration milestones:

- It takes 5 to 8 years for a mango tree to grow and bear fruits
- Usually, mangoes are produced by small farmers in Central or South America
- Once the mangoes are harvested, they are sent to a packing house for washing, drying, and packaging.

- The mango cartons are shipped to the US by air, sea or land (custom border)
- Then these mangoes are washed, peeled, sliced and put into convenient containers in a facility centre and then later shipped to ABC Retail Distribution centres to get refrigerated
- They are subsequently transported to one of the company's 11,200 stores, refrigerated and shelved.

In the course of an adverse event, it took ABC Retail an average of 6.75 days to track these mangoes within which time the damages would have already happened. However, after implementing the Blockchain solution, the 6.75 days tracking time of mangoes was reduced to 2.2 seconds. This created greater transparency across ABC Retail's food supply chain in 2017.

Solution

ABC Retail combined AI, IoT, and blockchain to improve the quality of the food supply chain from end to end. The Application logic of the system was hosted in the smart contract called "Chaincode" in the hyperledger. To put this system to test, the company created a food traceability system based on hyperledger fabric. The company roped in another technology partner, IBM Food Trust, and ran two proof-of-concept projects to test the system. The blockchain system built using hyperledger was designed to accurately record batch number, farm origin data, expiration dates, storage temperatures, and shipping details. ABC Retail used AI to predict and analyze the various patterns and trends of the retail policies that impact the supply chain. They also studied road traffic prediction and used the analysis to expedite the delivery. When the food products passed through the supply chain, sensors, and RFID tags supported by IoT technology were used to write the real-time data into the blockchain. These data helped ABC Retail to implement hazard management systems and critical control points for supporting the Food Safety Modernization Act and Inspection Service.

Every node in the blockchain network owns its data and will have control of those who can access the data elements based on the permission granted to share the pertinent records. The bolt-on adapters of the blockchain interfaced with the existing data stores like SAP Master Data of ABC Retail to make use of the business details like inventory, sale orders, and vendor master data. An API connector was built for the blockchain network administrators to manage the other complex environments and automatic web uploads of legacy data. The user was able to interact with the blockchain network either through the desktop or mobile interfaces or use the certifications module for uploading the regulation and inspection documents for supply partners. This solution also provided business-critical digital certificates needed for provenance verifications to ensure authenticity. The end-to-end traceability helped in fast product recall with real-time location and status of the food product or produce. To authorize users, predefined roles were created, such as given below:

- Account Owner
- Account Administrator

- Certifications Manager
- Food Safety Team Manager
- Onboarding Team Member.

Results

Thus, ABC Retail can now trace the origin of over 25 products from 5 different suppliers with the support of a system powered by hyperledger fabric. The company plans to span out the system to more products and categories, moving ahead in the future. It has recently announced that it will require all of its fresh leafy greens suppliers (like suppliers of salad and spinach) to trace their products using the system.

Now, ABC Retail will have the advantage to regain customer confidence because of the following:

- Food safety
- Food freshness
- Waste reduction
- Confidence and sustainability
- Traceability.

They collaborated with their technology partner to set up a blockchain, involving prominent players in the food industry, like Nestle and Unilever. ABC Retail is planning to extend this system in collaboration with Food Trust to more food products.

Case Study 2 – Banking and Financial Services

Industry Banking and Financial Services – Core Banking

Highlight Increasing transaction volume and network resilience while maintaining confidentiality requirements for real-time gross settlement among different banks of a central banking consortium

Overview

Banking institutions, central banks, and financial markets in the domestic and international space are going through a disruptive phase with the emergence of niche technologies and modern infrastructures. While some of the countries are still nascent in their strategy and planning to keep up with these advancements, the South African financial services industry has taken active steps to learn, grow and adapt to these opportunities. Having understood the broader implications and long-term benefits of automation, they were able to derive a contextual view of the finance sector in South Africa. South African Reserve Bank (SARB) required an innovative approach to enhance the resilience of interbank payment systems while ensuring the reduction of the overall cost of these systems.

The National Payment System Department (NPSD) executed the vision of the SARB by ensuring the overall effectiveness and integrity of the payment system.

The key aims of a properly functioning payments system are to:

- improve the stability of the financial system
- reduce the cost of the banking transaction
- encourage optimum use of financial resources
- enhance financial market liquidity
- facilitate the conduct of monetary policy.

Problem Statement

To understand the problem statement, it is essential to know how bank payments and settlements happen in South Africa.

As per the National Payment System Act 78 of 1998 in South Africa, settlement can be carried out using cash or through bank entries in the book of the SARB. For this to happen, the participants of the settlement system should have an account at the SARB through which interbank settlement takes place. This occurs on a pre-funded basis through the South African Real-time Gross Settlement System called SAMOS or South African Multiple Option System. The aim of this system is to reduce the risk of settlement failure by a participant in the payment system. Only if the issuing bank has sufficient funds, the transfer is carried out in the SAMOS. This reduces the risk of exposure for the participating banks as well as SARB. The funds transferred are final and irreversible.

With each bank in the country operating at different levels of maturity and business goals with their customers and vendors, inter-bank transactions are involved. They need to be highly secured for the customers to have a high degree of trust in them. Despite the design of the SAMOS system being aligned to SARB policy requirements, the system gradually became customized, slowly making the reconciliation payments inefficient. Also, the entire burden of suspicious transactions rested with the participating banks although it was not their fault.

Solution

Project Khokha is a project driven by the SARB, in collaboration with the consortium of South African settlement banks as well as participating technical and support partners. The prime goal of the Khokha was to build a proof of concept (PoC). With the modalities of the process being as vital as the outcome, it provided an opportunity to expand the distributed ledger technology (DLT) skills base in the South African banking industry. It also presented an opportunity to explore the approach of collaborative innovation, which could be a critical success factor for future developments. A distributed ledger was created between participating banks to have a payment system so that the participating banks can pledge, redeem, and track their balances and transactions of the tokenized rand. As part of Project Khokha, specific vital measurements such as scalability, privacy, security, and flexibility of the DLT were also assessed to know whether the DLT can be extended for other functions too. The RTGS system was built using tokens supported by funds held in the Central Bank. The tests were conducted for the performance of each node when

each participant bank executed its code with different deployment models from separate locations.

To mobilize the project fast, Quorum technology was selected since many of the participating banks used Quorum, and the implementation partner had the necessary skills in Quorum.

Quorum is an enterprise version of Ethereum (developed by JPMorgan and EthLab) and works on an open-source platform that enables collaboration between entities. Quorum uses the Go Ethereum code. The main distinctions of Quorum are in-network and peer permissions management framework, enhanced transaction, contract privacy, and voting-based consensus mechanism.

Project Khokha followed an agile approach. The design and development of the RTGS DLT platform were executed through four iterations.

In Iteration 1, two banks (restricted to SARB) were enabled to transfer tokens and minting functions were designed, developed, and tested.

In Iteration 2, the payment approvals were made by SARB, with all participating banks being able to view the transactions in the whole network.

Iteration 3 involved shielding the amounts of transactions and balances using Pedersen commitments (these are commitment schemes that deal with "how the counterparty engages with value" – the surrendered value remains private and can be discovered only later when the employee finds the required parameter of the commitment process); access was given to SARB for opening the commitment, enabling it to verify and approve the payment.

Iteration 4 used range proofs and Pederson commitments to enhance the flexibility of the system. SARB nodes continue to have complete visibility of the Pederson commitments, and therefore, of the transactions. However, it does not have the need to verify them since the other nodes would have already performed this role. Quorum solution utilizes Whisper for private messaging, Pedersen commitments, and range proofs.

Results

With the blockchain implementation, the central bank consortium was able to surpass the transaction performance target of 70,000 transactions in much less than two hours. They were able to achieve 95% of block propagation time is less than 1 second and 99% propagation in less than 2 seconds. This proved that acceptable performance and service level is achievable, despite the geographical distribution of the banks' hardware. The system was able to achieve privacy and information security while meeting the required transaction volumes.

The final results were positive, indicating that the Quorum platform can deliver the performance required, matching, and even exceeding the current performance criteria.

This was the first time that the banking consensus mechanism, legal commitments, and a set of legal proofs for confidentiality were used in tandem in an integrated enterprise. Together, all these essential elements delivered a combination of scalability, resilience, privacy, and settlement finality.

Case Study 3 - Healthcare

Industry Healthcare

Highlight Electronic health records and medical research data digitization

Overview

The first information technology-related changes in medical science were the digitization of medical files, now known as electronic health records (EHRs). The data contained in the EHR, other data sources, technology, and healthcare have the potential to transform medical practice by improving its overall performance. EHRs have produced a large volume of data.

Currently, for instance, most EHRs collect quantitative, qualitative, and transactional data, all of which could be collated, analyzed, and presented using sophisticated procedures and techniques.

Problem Statement

Electronic Healthcare Records (EHRs) were initially planned to manage distinct and straightforward medical records. As per their design, EHRs cannot maintain multi-institutional medical records of patients for their lifetime. Based on the various phases of the lives of patients who may have moved from one provider to another, the medical records will be scattered and not integrated. Some of the past data may be lost, since access to old data is controlled by the healthcare service provider who owns the medical history, rather than the patients. As per the HIPAA privacy rule, providers can take up to 60 days maximum to update or delete any record as per the patient's request.

In most cases, this 60-day maximum rule is also not complied with. Hence, beyond this time delay, maintaining the records with history becomes very challenging. Added to this is the complexity of the medical data being handled by different providers whom the patient may have approached during his or her lifetime. So we need a cohesive medical health record management solution that helps patients, providers, hospitals, and physicians/doctors to access the medical records in a hassle-free manner to prevent any adverse health-related events in a patient's life.

Solution

MedRec is a Blockchain product built for handling patient medical history. Since the permission management feature is enabled in blockchain, MedRec can allow patient-validated data exchange between medical jurisdictions and the record management system so that the physicians/doctors can have the needed access to these records. Now in this blockchain product, various stakeholders like physicians, patients and providers are thoroughly informed on the updated medical history and claims payment. They are also empowered to update, validate or delete the records based on their roles and responsibilities. Hence, the blockchain ledger has the convenience of auditable history

with accurate traceability for root-cause analysis, if needed by the physicians, insurance regulators, or patients.

One of the key features built in this blockchain product is the robust fail-over model that depends on the many stakeholder entities, thereby preventing a single point of failure. Also, medical records are safe and secure from any cyber-attacks since the data is stored separately in provider and patient databases; authorization data is stored in each node of the network. With this, the raw medical data and log of the global authorization are distributed; this blockchain product is not a target to any content attack or data leak.

MedRec solution provides exhaustive patient agency across provider and treatment sites so that the citizens are empowered to make the right decisions of healthcare. This blockchain solution allows the patients to have a long-term confidential log of their medical information, current and historical, thereby enabling the patients to have predictive and preventive medicinal treatments. MedRec can also receive data from hardware devices such as Fitbit. Apple Watch, etc. to update the patient's daily health data.

Patients can create a holistic medical record and allow essential stakeholders to view or edit, receive a second opinion from physicians, and share it with guardians, family members, hospitals, or caretakers. MedRec also has modules of Predictive Analytics using which patients and physicians can learn from the family medical history and conditions, past medical care, the pattern of results, etc. so that this can be used for further treatments. An accurate Learning Health system can be created by deploying open APIs, machine learning, and AI on top of the data layers in MedRec. The modularity design also allows additional layers of functionality like disease surveillance, epidemiological monitoring, alerts to physicians if the patients consistently abuse prescription access such as in drug abuse, personal health dashboards, etc.

Another salient feature of MedRec is Community Model, which primarily helps medical research with evidence-based data collected from the medical records system residing on the blockchain. This insight from the model can facilitate research into comparative clinical effectiveness and enable a better understanding of treatment outcomes among similar medical issues. Medical research costs can be substantially reduced with a blockchain system like MedRec, where the records can be accumulated, organized, and expert insights received based on the reports that are available for analysis. Such medical research is otherwise very expensive due to the recruitment process cost and the lack of proper access to medical records.

EHRs are not directly stored on the Ethereum Blockchain but in a set of smart contracts that are used to locate the records. Based on the various agreements of patients, providers, and other users, MedRec has three types of contracts, namely, Registrar Contract, Patient–Provider Relationship Contract, and Summary Contract. These are briefly explained below:

Registrar Contract

The registrar contract ensures that participant IDs (providers, patients, and insurers) are mapped to their Ethereum address identity, which is treated as the public key. The rules and

regulations are coded into the contract, so only authorized institutions can add data into the network. Hence, if there is new patient information to be added to the blockchain, the patient has to concede such information addition. Each ID is stored in a blockchain address referenced by the summary contract.

Patient–Provider Relationship Contract

This contract gives the relationship contract linking the two nodes in the system so that one node stores the data and manages the medical records for the other node. This kind of relationship exists typically between patient and provider but can be extended to different entities like insurers, physicians, etc. who have to access the records.

Summary Contract

Summary contract is like an indexed table of contents where each participant can locate the overall summary of their relationship with the other participants. This gives the list of references so that current and older engagements with other nodes can be referenced in the Patient–Provider contracts. This also provides a relationship "status" when the connection is established. The full control of the link, such as append, delete, and accept actions, is with the patient only. Thus summary contract gives a single point of dedicated location pointing to fragmented records of the patient while establishing the current and previous relationships.

The MedRec smart contract structure embodies as a single model of a "Healthcare Directory and Resource Location," secured with public-key cryptography and enabled with fundamental properties of provenance and data integrity. This blockchain directory model allows adding new participants and changing organizational relationships through additions to the smart contracts.

Whenever a patient wants to have access to a specific medical record, MedRec sends a request to the provider's database gatekeeper, part of the off-chain infrastructure of MedRec. The database gatekeeper executes the access interface call to the requester patient node's local database, based on the permissions stored on the blockchain. A server listening call is run to query requests, cryptographically signed by the issuer from clients on the network. The cryptographic signature is tallied to confirm identities. If it is a valid address, the question is run on the node's database, and the medical records are returned to the client; in this case, to the patient.

MedRec also gives the complete audit log information for the HealthIT ecosystem so that safety and security standards are taken care of.

Results

MedRec product strives to enable Precision Medicine and a holistic understanding of patient medical status without creating a centralized repository of data. Centrally stored data is challenged by the threat of cyber-attacks and data leaks. MedRec works on open APIs. Hence, it can be integrated into other applications of the Healthcare IT stack.

Case Study 4 – Energy and Utilities

Industry Energy and utilities

Highlight Renewable energy trading

Overview

In the current energy ecosystem, community and locally sourced energy projects and microgrids are becoming increasingly popular. Energy projects which are locally owned deliver benefits that are environmentally relevant for the communities involved.

In microgrids, distributed generators, storage devices, uncontrollable and controllable loads form an interconnected system that can operate in synchronization with the primary grid or in complete autonomy, if working in island-mode. Microgrids act as a central system which has clear electrical boundaries for the primary grid. Streamlining the control of supply and demand outside the physical and electrical boundaries can be done with a new concept of the virtual microgrid. Usage of microgrids helps in promoting localized energy production and utilization, which leads to a reduction in transmission and distribution losses.

Problem Statement

With energy systems becoming more complex, multi-agent, and decentralized, a higher degree of management control is needed with many stakeholders in the ecosystem. Advanced communication protocols, data exchanges within the global power network and operation of the central management need to be much smarter. Different models and techniques are required to facilitate these latest trends in the energy sector.

Solution

The solution developed is a blockchain-based, decentralized energy trading platform that will operate on a distributed P2P blockchain network, which allows users to sell and buy electricity harnessed from solar panels automatically. This is how it works: If a village has extra power that was captured during the day and is stored on a lithium-ion battery, it could automatically sell a specific predetermined portion to another village on the network. Without relying on big centralized power plants, microgrids will supply a small area with electricity consolidated from distributed sources such as diesel generators, solar power generators with battery storage, crowd-funded low-power source, etc. These localized microgrids will operate either separately or attached to the national grid so that small businesses, hospitals and other organizations can keep working without a break, in case large grids break down.

Brooklyn Microgrid is a blockchain-based P2P energy trading platform run by TransActive Grid, a partnership between LO3 Energy, Consensys, Siemens, and Centrica.

The microgrid is situated in the Gowanus and Park Slope communities in Brooklyn, New York, and a three-month trial run of P2P energy trading between community members has been done using this blockchain platform. With this platform, now the prosumers can sell their surplus energy produced to other community members who are in need of energy. This is enabled on the Ethereum-based smart contracts implemented by a company called Tendermint. The first energy transaction was recorded in the first trial, where five prosumers and five neighbouring consumers were piloted. Specially designed smart meters measure the surplus energy and convert them into equivalent energy tokens, which are traded in the marketplace. Each token denotes solar panels that produce a specific unit of energy. These tokens can be transferred from the smart meter wallet of prosumer to end-consumers using blockchain technology. Whenever the consumer uses this unit of energy in his house, these tokens are deleted by the consumer's smart metering device and marked as being purchased by the consumer.

The users of Microgrid can specify their price preferences for selling or buying the electricity by interacting with the blockchain platform. Based on the pricing preferences entered in the system, the platform is designed to display real-time energy prices. The blockchain ledger will have a record of the transacting stakeholders, contract terms, pricing, energy traded and consumed, which are measured by the smart metering devices.

Additionally, all payments are automatically executed by the smart contracts. As defined by the access and authorization, each member of the community will have access to all previous transactions in the ledger and will be able to validate/verify the transactions themselves. Several houses and small businesses have signed up for the next phase of implementation, which has the goal of fully automated transactions. All of these transactions will be done in native ICO token.

In the Energy sector, business is looking for new paradigms like demand response, mechanisms for auctioning energy, and automatically scheduled power consumption based on predefined agreements between stakeholders. This is possible only if the underlying framework allows synchronous flow of information. Smart contracts built on top of the blockchain will provide these functionalities a robust, transparent, secure, and reliable transactional system.

Results

The Brooklyn Microgrid project has become the model for exploring innovative business models for new projects to promote better consumer participation in communities. With the help of localized energy trading, better potential for energy cost savings is possible.

With this implementation, now all the participants will be able to have partial ownership of the grid infrastructures represented by tokens in the system. Since the prosumers use a decentralized network instead of a third party, the cost is also substantially reduced. Because of the lower price, now small-scale companies will be able to participate; thus the end-users would be allowed to choose the best option of electrical power trading.