Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 164 (2019) 143–148

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies

Application of Blockchain to Supply Chain: Flexible Blockchain Technology

Natsuki Kawaguchi*

Chuo University, 742-1 Higashinakano Hachioji-shi, Tokyo 192-0393, Japan

Abstract

It has been ten years since Satoshi Nakamoto created bitcoin and introduced the concept of a blockchain. The original goal was to propose a solution to the double-spending problem using a peer-to-peer network. Now, Blockchain proves to have the capacity to deliver a new kind of trust to a wide range of services. Applications are being explored in healthcare (patient records), government (land registries) and electronics (Internet of Things). The supply chain is one of the fields that Blockchain is expected to be applied. The paper aims to combine blockchain with distributed storage and propose blockchain for the supply chain. Blockchain is not fit to record a lot of information. It requires both on-chain storage of the core ledger data and off-chain storage of data required by smart contracts for verification and documentation. The Inter Planetary File System (IPFS) is a concrete solution. IPFS is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files. Participants can address large amounts of data with IPFS and place the immutable, permanent IPFS links into a blockchain transaction. This timestamps and secures their content, without having to put the data itself on the chain. By combining blockchain with distributed storage, the supply chain system is fit to the industry of the next generation. The characteristics of Industry 4.0 meets the blockchain-based system and the model can aid these changes.

Keywords: Blockchain; Distributed ledger technology; Smart contract; Supply chain;

* Corresponding author.
E-mail address: natsuki.kawaguchi889@gmail.com

10.1016/j.procs.2019.12.166

1. Introduction

The concept of distributed computing has been around since 1990. In 2009, Satoshi Nakamoto created bitcoin and introduced the concept of Blockchain [1]. The original goal was to propose a solution to the double-spending problem using a peer-to-peer network [2]. It has been about ten years since then and cryptocurrency has developed. Now, Blockchain proves to have the capacity to deliver a new kind of trust to a wide range of services [3]. Applications are being explored in healthcare (patient records), government (land registries) and electronics (Internet of Things). The supply chain is one of the fields that Blockchain is expected to be applied. Estimated 90% of the world trade is carried out by the international shipping industry every year [1]. But the logistics behind global trade is highly complex as it involves many parties with conflicting interests and priorities as well as the use of different systems to track shipments. According to one estimate from the World Economic Forum, reducing supply chain barriers to trade could increase GDP by nearly 5% and global trade by 15%. Blockchain technology can help reduce many of the frictions in global trade logistics including procurement, transportation management, track and trace, customs collaboration, and trade finance. In this paper, I combine blockchain with distributed storage and propose a blockchain model for the supply chain.

2. Related work

2.1. Blockchain

Blockchain can be defined as a database that can record transactions between parties in a secure and permanent way [1][3]. Each block contains three elements, a hash, timestamped batches of recent valid transactions, and the hash of the previous block. A hash function is a function that converts the data it is given into an irregular value of fixed length [4]. The timestamp proves that the data must have existed at the time [2]. The previous block hash links the blocks together and prevents any block from being altered or a block being inserted between two existing blocks. In this way, each subsequent block strengthens the verification of the previous block and hence the entire blockchain. The method renders the blockchain tamper-evident, lending to the key attribute of immutability. A smart contract is a component of a blockchain-based system that can automatically enforce stakeholder-agreed rules and process steps [1]. There are two key features, data transparency, and security [1]. Blockchain technology ensures that stored records are accurate, tamper-evident, and from a verifiable source. Instead of multiple parties maintaining copies of their own dataset, every stakeholder receives controlled access to a shared dataset creating a single source of truth. This gives confidence to everyone working with this data that they are using the most recent, accurate, and reliable dataset. Secondly, Traditional ledgers typically provide an overall layer of security which once breached allows access to all stored data. In a blockchain-based system, the security mechanisms make sure that individual transactions and messages are cryptographically signed. This ensures essential security and effective risk management to tackle today's high risks of hacking, data manipulation, and data compromise.

2.2. Supply chain

A supply chain is often described as a system of organizations, people, activities, information, and resources involved in moving a good or service from the initial supplier to the final customer [6]. Supply Chain Management (SCM) is the planning and management of all activities involved in sourcing and procurement, conversion, and all logistics management activities to meet the customer's need. It also includes coordination and collaboration with channel partners, including suppliers, intermediaries, third-party service providers, and customers. There are these key concepts;

- Client demand: Clients in different field missions request goods and services.
- Monitoring, tracking, and reporting: Tracking is enabled for any requisition or shipment to monitor progress
- Planning: Field support teams develop optimized plans for sourcing, logistics, storage, transport and distribution.
- Sourcing: Field support teams evaluate and secure the best suppliers.

- Inbound logistics: Field support teams organize transport from supplier to a first distribution hub.
- Storage and transport: Goods are stored or prepared for transport according to an optimized schedule.
- Outbound logistics: Goods and services are distributed to clients.
- Delivery and receipt: Clients receive the right goods, with the right quality at the right time.

2.3. IBM Food Trust

IBM Food Trust uses the blockchain solution to build transparency of supply chain from the farmer, processor, retailer, to the consumer. The solution provides participants with a permission-based, shared view of food ecosystem information [7]. It allows convenient data publishing and controlled sharing of information. IBM Food Trust users can quickly locate items from the supply chain in real-time by searching food product identifiers using the product name and filtering on dates. Any IBM Food Trust participants can use a Smart Contract in a Private Channel between two or more specific network members. Data in that channel is unencrypted. By using this technology, decision making is automated.

IBM Food Trust has an integrated set of modules.

・Trace module

Trace module provides the provenance of a product through immediate access to end-to-end data. This module also shows real-time location and status, so allows expedited product recalls.

・Fresh Insights module

Fresh Insights module connects disparate product data to draw insights and gain visibility into inventory across the supply chain. Then, it shows time since production and to expiration.

It becomes easier to calculate an at-risk inventory. So, suppliers can identify inefficiencies, improve freshness, and reduce product losses.

・Certifications module

Certifications module digitizes business-critical certificates and inspection documents. It can optimize efficiency for information management, certify provenance, and ensure authenticity.

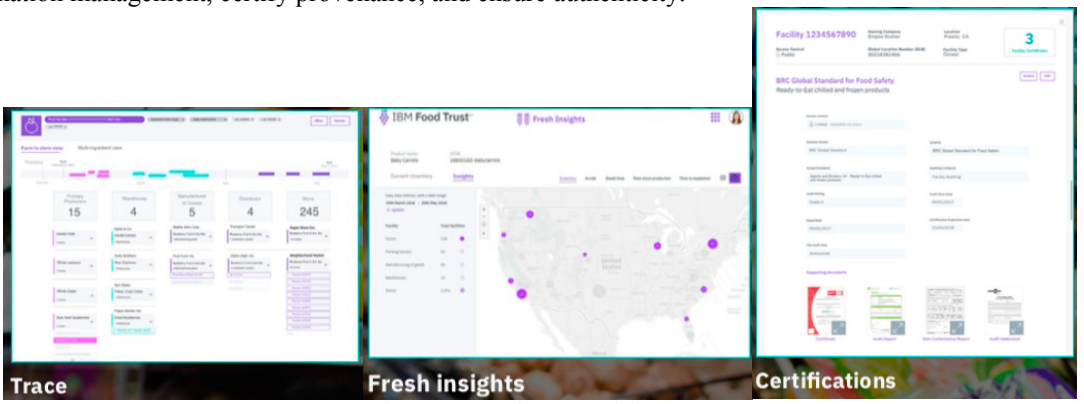

Fig. 1. IBM Food Trust Module Demo.

IBM Food Trust combines supply chain with blockchain core functions successfully. IBM explains the advantage of the Food Trust system is "All data is stored on blockchain ledgers, protected with the highest level of commercially-available, tamper-resistant encryption."

But, blockchain records who owns what and who transacts what. In other words, it is not fit to record a lot of information. If the supply chain becomes more complex, there will be mass data and blockchain should be used with any other storage. So, I combine blockchain with distributed storage and use this technology more appropriately.

3. Methodology

I propose Blockchain for supply chain. Fig. 2. is the whole picture of it. In this system, I define the low layer, high layer, lower blockchain and higher blockchain as such.

- Low Layer: trades between traders at the stage of production and processing.
- High Layer: trades between traders at the stage of sales and consumption.
- Lower Blockchain: records of transactions on the low layer.
- Higher Blockchain: records of transactions on the high layer.

(In case of a large-scale system, we can create a middle layer and a middle Blockchain.)

Low Layer is a public community. On this layer, participants look for potential business partners. The important thing on this layer is to find good partners from a wide variety of options. So, the community must be open. On the other hand, High Layer is a private community. On this layer, retailers and customers conclude a contract. The important thing on this layer is to deliver products to customers accurately. There is personal information such as name and address. So, the community must be close.

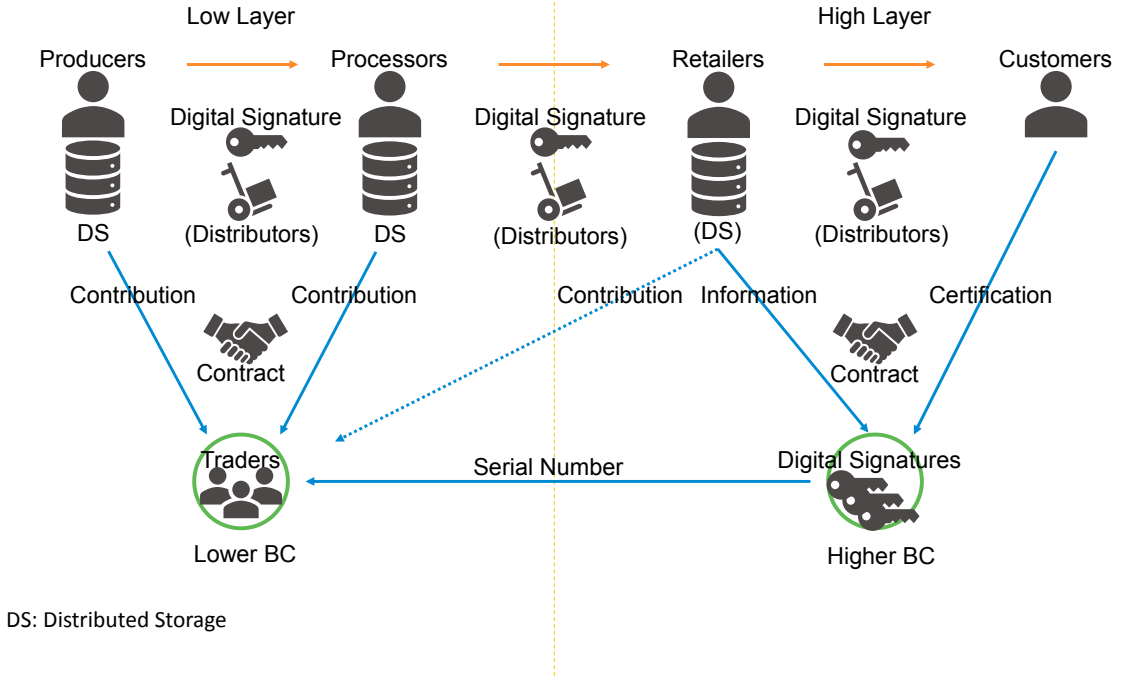

Fig. 2. Blockchain application model for supply chain.

In the production stage, a serial number is assigned to the raw material. In each stage, participants verify the digital signature of the previous stage and create a new one. Also, they record information on each stage in distributed storage. Lower Blockchain and Higher Blockchain is automatically generated at the formation of contracts. Goods are tracked by the parcel code, QR code, serial number and so on if it is necessary. Customers can search for goods by the serial number on Lower Blockchain and Higher Blockchain.

The key features of the system are as shown below.

- Comprehensive records of ordering, receiving, cash flow, logistics, and information flow: In this system, every transaction is recorded. In general, companies do not know enough about the products that they buy and sell to navigate the many complex challenges facing today's global supply chains. This system can solve the issue.
- Client demand: Clients can make to order on Lower Blockchain network. When an order is placed, traders will react to it. Good projects will gather many traders. On the contrary, bad projects will be at a standstill.

This feature is important for the industry of the next generation. INDUSTRIE 4.0 is set to revolutionize manufacturing and production [8]. I 4.0 represents a paradigm shift from "centralized" to "decentralized" smart manufacturing and production. "Smart production" is an ICT technology-driven approach that utilizes Internet-connected machinery to manage the production process. The goal of SM is to identify opportunities for automating operations and use data analytics to improve manufacturing performance. Table 1 shows the Comparison between characteristics of Industry 3.0 and Industry 4.0 in manufacturing [9]. The characteristics of I 4.0 meets the blockchain-based system and the model can aid these changes.

Table. 1. Comparison between characteristics of Industry 3.0 and Industry 4.0 in manufacturing

Characteristic	Industry 3.0	Industry 4.0
Processes	Automation	Autonomous decision making
Industry defining technology	Industrial robots	Collaborative robots
Production planning	Demand forecasting	On-Demand manufacturing
Alignment	Interconnection of production processes	Interconnection of the whole value chain
Variation	Delimited variation	Individually unique products
Goal	Efficiency	Flexibility
Base for revenue model	Selling products	Servitisation

- Distributed storage: Blockchain is not fit to record a lot of information. It requires both on-chain storage of the core ledger data and off-chain storage of data required by smart contracts for verification and documentation [10]. The Inter Planetary File System (IPFS) is a concrete solution. IPFS is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files [11]. Each file is given a cryptographic hash. Each network node stores only content and some indexing information that helps figure out where data is stored. When looking up files, participants search the network to find nodes storing the content behind a unique hash. IPFS and the Blockchain are a good match. Participants can address large amounts of data with IPFS and place the immutable, permanent IPFS links into a blockchain transaction. This timestamps and secures their content, without having to put the data itself on the chain.
- Digital signatures: As long as there are not three digital signatures, a Higher Block is not generated. The system builds transparency of supply chain from the producers, processors, retailers, to the consumer. That can be regarded as a kind of smart contract. Digital signature infrastructures have two distinct goals [12]; Firstly, Digitally signed messages assure the recipient that the message truly came from the claimed sender. They enforce nonrepudiation (that is, they preclude the sender from later claiming that the message is a forgery). Secondly, Digitally signed messages assure the recipient that the message was not altered while in transit between the sender and recipient. This protects against both malicious modification (a third party altering the meaning of the message) and unintentional modification (because of faults in the communications process, such as electrical interference). Digital signature algorithms rely on a combination of the two major concepts, public key cryptography and hashing functions .
- Blockchain interconnection: Serial number enables the interconnection of Lower Blockchain and Higher Blockchain.

In addition, Digital signature has an expiration data. So, data cannot be stored for a long time. By using distributed storage, the system can treat long storage data.

4. Conclusion

In this paper, I combine blockchain with distributed storage and propose a blockchain model for the supply chain. Blockchain is not fit to record a lot of information. It requires both on-chain storage of the core ledger data and off-chain storage of data required by smart contracts for verification and documentation. The Inter Planetary File System

(IPFS) is a concrete solution. By combining blockchain with distributed storage, the supply chain system is fit to the industry of the next generation. Industry 4.0 represents a paradigm shift from "centralized" to "decentralized" smart manufacturing and production. It is an ICT technology-driven approach that utilizes Internet-connected machinery to manage the production process. The characteristics of Industry 4.0 meets the blockchain-based system and the model can aid these changes. But, there is still room for improvement. This system is only a concept. The real supply chain is more complex. To put this model into practice, it should be more concrete and realistic.

Vannevar Bush published an essay, "As We May Think" in the Atlantic. In this essay, he introduced the concept of the memex as follows. A memex is a device in which individual stores all his books, records, and communications, and which is mechanized so that it may be consulted with exceeding speed and flexibility. It is an enlarged intimate supplement to his memory [13]. His essay influenced generations of computer scientists. Douglas Engelbart is one of them. He coined the term Collective IQ as a measure of how well people can work together on important challenges – how quickly and intelligently they can anticipate or respond to a situation, leveraging their collective perception, memory, insight, vision, planning, reasoning, foresight, and experience into applicable knowledge. He devoted his life to boosting mankind's capability for coping with complex, urgent problems [14]. And, when Berners-Lee created the web, it was a decentralized platform. Anyone could publish a website and link to any other site. But as the web has grown from an obscure research-sharing tool for the scientific community into a global medium for commerce, communication, journalism, and entertainment, the power dynamics have shifted. Today, huge companies like Amazon, Facebook, Google, and Netflix dominate the web. These corporate giants enjoy an enormous amount of control not only over what people see and do online but over users' private data [15].

Blockchain technology can be an opportunity to get back to the original goal and re-decentralize the Internet. I expect destructive technology with great potential.

References

[1] DHL Customer Solutions & Innovation. (2018) “Blockchain in logistics.” DHL Customer Solutions & Innovation.
[2] Nakamoto S. (2009) “Bitcoin: A peer-to-peer electronic cash system.” Bitcoin.org.
[3] Government Office for Science. (2016) “Distributed ledger technology: beyond block chain.” Government Office for Science.
[4] Ishii M. (2017) “Algorithms: Explained and illustrated” Tokyo, Shoeisha.
[5] IBM. (2018) “Blockchain for Dummies, 2nd IBM limited edition.” John Wiley & Sons, Inc.
[6] United Nations. (2015) “Supply chain management.” United Nations.
[7] IBM (2019) “About IBM Food Trust.” IBM
[8] Germany Trade & Invest [online]. Available: https://www.gtai.de/GTAI/Navigation/EN/Invest/Industries/Industrie-4-0/Industrie-4-0/industrie-4-0-what-is-it.html
[9] I.A.R. Torn, T.H.J Vaneker (2019) “Mass Personalization with Industry 4.0 by SMEs: a concept for collaborative networks” *Procedia Manufacturing* **28** :135-141
[10] IBM (2018) “Why new off-chain storage is required for blockchains” IBM
[11] Benet J. “IPFS -Content Addressed, Versioned, P2P File System” IPFS.
[12] (ISC)2. (2015) “CISSP official study guide seventh edition.” Indiana, John Wiley & Sons, Inc.
[13] Bush. (1945) “As we may think” Boston, The Atlantic.
[14] Doug Engelbart Institute. [online]. Available: http://www.dougengelbart.org/
[15] Finley K. (2017) “Tim Berners-Lee, inventor of the web, plots a radical overhaul of his creation” [online]. Available https://www.wired.com/2017/04/tim-berners-lee-inventor-web-plots-radical-overhaul-creation/
[16] Kawaguchi N. (2018) “Blockchain for Supply Chain: Flexible and Secure Blockchain” *Journal of Transformation of human behavior under the influence of The Infosocionomics Society* **4**: 33-41
[17] Kawaguchi N. (2019) “Study of Blockchain Application Model for Supply Chain” *Journal of The Infodocionomics Society* **13(2)** :99-109
[18] Okajima Y. (2019) “Blockchain: New security achieved by mutual distrust” Tokyo, Kodansha.
[19] Tapscott D. (2016) “Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world.” New York, An imprint of Penguin Random House L.L.C.