Blockchain Architectural Proposal for Radical Transparency of IoT Records in Supply Chains

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Robert Atticus Owens
Spring, 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Briana Morrison, Department of Computer Science
Rosanne Vrugtman, Department of Computer Science

Blockchain Architectural Proposal for Radical Transparency of IoT Records in Supply Chains

CS4991 Capstone Report, 2023

Robert Owens
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
rao7utn@virginia.edu

ABSTRACT

This proposed blockchain architecture will increase supply chain efficiency and transparency. The architecture is designed to generate a global commerce trust-building technological institution. It will solve information transparency issues for 3 major stakeholders: consumers, businesses, and regulators. The blockchain stores Internet of Things (IoT) sensor data thereby tracking the condition of products throughout a supply chain. The architecture is designed to accommodate three key features: access control list (ACL) permissions which read and write to blocks, removal of stale blocks from the blockchain to limit storage size, and feedback from downstream supply chain partners to upstream firms on the blockchain. The high-level architecture can be re-iterated and adapted to specific industries.

1. INTRODUCTION

According to Law (2017), blockchain-enabled supply chains will increase agility and strengthen relationships among partners by enabling transparency, traceability, and efficiency. And according to Park (2021), blockchain-enabled supply chains promote environmental, social, and economic sustainability. To illustrate the scale and potential for improvement in this domain consider that "Each year, 1.6 billion tons of food worth about $1.2 trillion are lost or go to waste—one-third of the total amount of food produced globally" Esben, et. al. (2022).

Blockchain is a publicly viewable digital ledger that allows for a distributed computer network to keep an immutable record of accounts. Each computer called a node, coordinates with other nodes to append new records via rules defined by open-source code that anyone can read, run or revise. Blockchain applications can support *smart contracts* which are programs that can contribute new data to the ledger. IoT devices are low-power computer devices such as digital sensors.

2. RELATED WORK

This proposal integrates design patterns from different blockchain applications that solve specific problems which are also applicable to a food supply chain blockchain. The first technical problem is *auditable privacy*. Different types of records on the blockchain should only be viewable by specific stakeholders. The second problem is limiting the quantity of data stored on the blockchain by allowing certain records to *archive* after a period of time. The third problem is ensuring the *accuracy* of IoT data on the blockchain. This final problem is not based on other researchers' work.

2.1 Auditable Privacy

Daraghmi (2019) designed a blockchain system, MedChain, for storing medical records with permission management between

patients, care providers, and insurance company stakeholder groups. This proposal is valuable because it also includes three stakeholder groups and includes extensive security considerations because of the sensitivity of medical information. MedChain solves the auditable privacy problem via an Access Control Contract, which records which computers are allowed to view (decrypt) and which records (blocks) on the blockchain.

2.2 Archiving Stale Data

Pyoung (2020) designed a blockchain called LiTiChain, which unlike most other blockchains allows records (blocks) to expire. This ensures that computers do not store the data on every past transaction. For example, Bitcoin blockchain is 389 GB and the Ethereum blockchain is 658 GB. IoT records are different to payment records in that the new records are not dependent on the old. LiTiChain solves the data problem by using a graph data structure that tracks blocks that have expired via timestamps. The stale data blocks are removed from the blockchain during programmatic maintenance. Additionally, LiTiChain was designed for edge computing and IoT devices running blockchain so the design falls perfectly within the scope of this proposal.

2.3 Consensus Algorithm & Data Accuracy

Proof of Authority (PoA) is when one computer in the network can both propose and accept the same block to the blockchain. PoA creates a moral hazard problem because firms can misrepresent when products are out of compliance.

3. PROPOSED DESIGN

The first section outlines how data is structured within blocks. Subsequent sections offer solutions from the related work sections.

3.0 Blocks

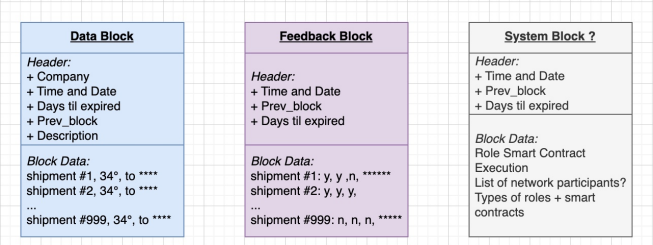

Figure 1: Description of Blocks

Most blocks in this solution will consist of aggregated IoT sensor statistics that are associated with specific products or batches of products, e.g. shipping containers of fruit. These blocks are "Data Blocks", and their purpose is to promote transparency. They will have information about the shipping company, date, time, location, destination, etc. Second, "Feedback Blocks", a collection of individual review records about the direct upstream partner's services, can be written by recipient regulators and stakeholders. Last, "System Blocks" are data created by the blockchain system to manage its internal state.

3.1 Auditable Privacy

The blockchain is designed to accommodate the following broad groups of stakeholders. First, businesses that are involved in supply chains, second regulators and governments who enforce customs etc., and finally the general public. The blockchain will be a public and permissioned blockchain. This means that while the blocks that compose the blockchain are publicly available, they can only be created and validated by specific permission users. Additionally, while the default is public data, some data can be made private using encryption. These permissions will be enforced by digital certificates using symmetric cryptography like SHA-3. In this scheme, the public key is associated with a stakeholder identity, and the corresponding private key is used to validate a user's identity when they are performing any specific action on the blockchain. Each certificate, or identity, is associated with a specific role. Basically, roles can be divided into two groups:

businesses and regulators. However, it would be natural to break businesses into sub-roles such as producers, vendors, transportation, distribution, and retailers. Each role will be governed by a *role smart contract*. Smart contracts are extremely flexible and can be refined for each industry's needs. Smart contracts will use authorization logic to ensure that specific actions (transactions) are permissible. Some examples of possible restrictions include: regulators cannot produce IoT record blocks and businesses cannot provide feedback on their own blocks. Businesses can only provide feedback for their own shipments.

When a new business or regulator would like to join as a permissioned user on the blockchain, they can appeal to the certificate authority (CA), for a smart contract. The CA conducts a review of the identity's authenticity, issues a certificate and finally informs the distributed networks' other computing nodes. This scheme ensures that information can only be viewed by authorized users. The privacy restrictions prevent other businesses from learning about individual orders. Additionally, restrictions can prevent private information from being disclosed in the feedback blocks, for example, a textual description of things that were wrong with a shipment could be made private, viewable only by the receiving company and the supplier. *Role smart contracts* can write blocks in specific ways to ensure the correct privacy levels. The role of smart contracts will ensure a user has permission to read a specific record before releasing it. Other records can be accessible to general users by writing the block in plain text.

3.2 Archiving Stale Data

Timestamps in block headers will be used to archive stale data. The timestamps will indicate when the blocks expire and remove them from the system during scheduled network purges. Distributed network nodes will coordinate block removal ensuring the resultant blockchain is identical on all nodes.

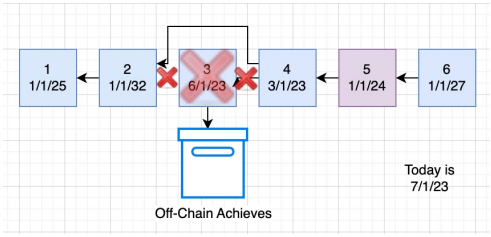

Figure 2: Removing blocks from blockchain

The blocks removed from the blockchain could be archived in each node so that they are available for future system analysis. This process ensures that only a limited amount of data is stored and synchronized between nodes, keeping a manageable data block size. Data cleanup is necessary for blockchain efficiency.

3.3 Consensus Algorithm & Data Accuracy

It is impossible for validators to definitively know that a block has inaccurate IoT data. The feedback records encourage honest behavior because disreputable stakeholders will tarnish their reputations publicly.

Proof of Authority (PoA) is the appropriate consensus algorithm to ensure that the producers of records truthfully attest to their data. Nodes will only check to ensure a block is properly formatted and then append that new block to the blockchain. When a shipment is received, the receiving stakeholder can provide a feedback record that rates the condition of the product, using binary metrics like damaged, spoiled, temperature compliant, sealed, etc. as well as an option to add text. The metrics on this feedback block will be publicly observable allowing firms to scrutinize and choose between shipping companies with more complete information.

3.4 Overview of the Whole Proposal

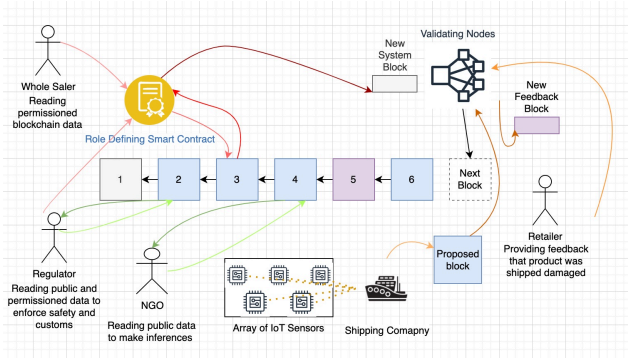

Figure 3: System Diagram

Figure 3 shows an overview of the entire proposed system. Light to darker colors indicates the temporal ordering of events. The green arrows are for reading public, unencrypted records. The red is for reading encrypted records. The orange is for producing new blocks.

Access to public records (green) is simple, just download the block and the information is written in plain unencrypted text. Permissioned data (red) is read in 3 situations. First, a user requests some information on a specific block to read and is authenticated by the smart contract that manages stakeholder roles. Second, the smart contract reads the data, unencrypts it, then re-encrypts it using the user's public key from the authenticating certificate. This new encrypted data is added to the mempool and to the next system block which the original user can decrypt and read. Note by this mechanism the smart contract manages the initial encryption of data when it is produced and only the smart contract decrypts it for permissioned stakeholders. Creating a new data case (orange) occurs in different ways for different blocks. Whenever the mempool has enough records to produce a system or feedback block the validating nodes add that block to the blockchain. Businesses like shipping companies will aggregate IoT sensor metrics into a block and propose it to the blockchain network.

3.5 Design Limitations

There are a number of limitations to this proposal. The first and most important is that smart contracts are not designed to support payment. Blockchain needs to better facilitate payments between parties when the conditions specified in the smart contract code (based on legal contract agreements) are met. This proposal does not enable this feature because currently there are no reasonable mediums of exchange suitable for international trade. Crypto-currencies are volatile and stable coins frequently "de-peg".

Additionally, there is limited incentive to be a validator or to join this system. Unlike cryptocurrencies which have monetary value, information is the only commodity in this system. However, the incentive to join this blockchain would be increased overall efficiency for all participants. Alternatively, governments and regulators could require this system to resolve transparency concerns.
Finally, businesses in supply chains would have to adapt to new technology. Initially, there would be a steep learning curve.

4. ANTICIPATED RESULTS

This system will increase transparency to the benefit of each stakeholder. For consumers, this will increase confidence that products conform to their ethics. Regulators can ensure safety through increased oversight provided by IoT measurements. Finally, businesses can build trust between partners without disclosing private information and can also increase trust with regulators and consumers through transparency.

5. CONCLUSION

This paper offers a blockchain system that would radically increase transparency in supply chains. This proposal is a unique combination of different blockchain ideas and significantly deviates from status quo blockchain supply chain designs. It takes a more grounded yet feasible approach. The intent is for future designers and researchers to

take this high-level proposal and implement the design details required to make this proposal a reality.

6. FUTURE WORK

Researchers should take this work and critique and revise it, then create a working demo. Ideally, this proposal will be implemented in various supply chains. Each supply chain will have its own unique considerations and adaptations within this proposed framework.

REFERENCES

E. -Y. Daraghmi, Y. -A. Daraghmi and S. -M. Yuan, "MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management," in IEEE Access, vol. 7, pp. 164595-164613, 2019, doi: 10.1109/ACCESS.2019.2952942.

Esben Hegnsholt, Shalini Unnikrishnan, Matias Pollmann-Larsen, Bjorg Askelsdottir, and Marine Gerard. 2022. Tackling the 1.6-billion-ton food loss and waste crisis. (August 2022). Retrieved February 26, 2023 from https://www.bcg.com/publications/2018/tackling-1.6-billion-ton-food-loss-and-waste-crisis

Law, A. (n.d.). Smart Contracts and their Application in Supply Chain Management. *Supply Chain Management*, 89.

Park, A., & Li, H. (2021). The Effect of Blockchain Technology on Supply Chain Sustainability Performances. *Sustainability*, *13*(4), 1726. https://doi.org/10.3390/su13041726

C. K. Pyoung and S. J. Baek, "Blockchain of Finite-Lifetime Blocks With Applications to Edge-Based IoT," in IEEE Internet of Things Journal, vol. 7, no. 3, pp. 2102-2116, March 2020, doi: 10.1109/JIOT.2019.2959599.