2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) | 978-1-6654-3924-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/BRAINS52497.2021.9569817

Multi-Layer Aggregate Verification for IoT Blockchain

1st Jingze Wu
Department of Computer Science
National Taiwan University
r08922153@csie.ntu.edu.tw

2nd Ming-Fong Sie
Department of Computer Science
National Taiwan University
d07922015@csie.ntu.edu.tw

2nd Seth Austin Harding
Department of Computer Science
National Taiwan University
b06902101@csie.ntu.edu.tw

3rd Chien-Lung Lin
Department of Computer Science
National Taiwan University
d08922023@ntu.edu.tw

4th San-Tai Wang
Department of Computer Science
National Taiwan University
p09922006@csie.ntu.edu.tw

5th Shih-wei Liao
Department of Computer Science
National Taiwan University
liao@csie.ntu.edu.tw

***Abstract*—We design a Multi-Layer Aggregate Verification (MLAV) solution to improve supply chain management with IoT Blockchain devices. We apply MLAV to IoT Blockchain applications in Agriculture 4.0 to demonstrate the feasibility of our solutions and models. In the current Agriculture 4.0 structure, large companies have successfully applied blockchain solutions and ecosystems for tracking and tracing agricultural produce, achieving transparency, traceability, and digitalization. However, these existing blockchain solutions are not comprehensive. First, the upstream nodes they serve are all large-scale production suppliers, and smallholders are not taken into consideration. In order to solve this problem, we use a multi-layer architecture that serves three purposes: facilitating smallholders in joining the agricultural blockchain as equal-opportunity nodes, uploading of production activity data, and reducing costs (ex. Ethereum gas fee). Second, the majority of IoT blockchains adopt an ID-based signature scheme in IoT devices, which frequently has lower efficiency. In applying aggregate verification, we may effectively increase ID-based verification efficiency while processing large clusters of data transferred by IoT devices. Finally, we design a blockchain management framework using smart contracts to facilitate the financing of upstream producers.**

***Index Terms*—IoT, Blockchain, ID-based Signature, Aggregate Verification, Agriculture 4.0, Supply Chain Management**

I. Introduction

IoT is what drives Agriculture 4.0 [1]; it is estimated that the widespread adoption of IoT devices may increase agricultural productivity by 70% by 2050 [2]. The blockchain allows for both tamper-proofing and transparency of data, which is highly beneficial to Agriculture 4.0. However, ID-based signatures with IoT devices have higher time complexity which results in lower throughput. In this paper, we use a multi-layer architecture that facilitates smallholders in joining the agricultural blockchain, using aggregate verification to solve the efficiency bottleneck of ID-based signature verification. We design a framework for distributed supply chain management with smart contracts to allow for the smallholder to gain access to loans.

II. Related Work

Distributed ledger technology facilitates the flow of information between nodes and resolves inefficiencies relating to information asymmetry [3] like the peer-to-peer hypermedia protocol IPFS [4]. Our platform uses the Ethereum blockchain structured around a decentralized virtual machine that processes smart contracts [5].

A. IoT Blockchain in Agriculture 4.0

IoT-blockchain-enabled transactions possess the following advantages [6] in Agriculture 4.0: first, new levels of product traceability, authenticity, and legality may be achieved; second, a real-time food tracking system built on blockchain enables all supply chain members to access all information; third, blockchain reduces verification and transaction costs by eliminating intermediaries; fourth, blockchain eliminates the need for centralized databases which may be prone to data loss or have data that is difficult to retrieve; fifth, blockchain provides fast, real-time payments that increase cash flow and working capital while reducing transaction costs and risks [7].

B. Aggregate Verification

Aggregate verification may allow for devices to evolve to new software threats, fix bugs, and upgrade functionality by releasing periodic firmware updates [8]. In addition, a new aggregate verification application has been proposed in [9] in which a system may need to verify a smaller number of signatures with high efficiency and minimized confirmation time. For systems with a large quantity of nodes frequently generating new data, aggregate verification may be implemented to efficiently verify many signatures simultaneously in one action [9]. We adopt an aggregate verification method that may be used even in cases of high traffic in the network.

III. Benefits of Multi-Layer Blockchain

We describe the advantages of using our multi-layer blockchain on both system level and framework level.

978-1-6654-3924-4/21/$31.00 ©2021 IEEE

A. *Multi-Layer Blockchain System*

Facilitating small upstream entities in joining the blockchain system, we define a three-layer blockchain shown in Fig. 1. As Quorum is a permissioned blockchain and lacks information transparency, data is uploaded to Ethereum for public access [10]. Layer 3: the IoT devices of large manufacturers and smallholders' Android app stores data in a MySQL database during the data collection stage; Layer 2: smallholder nodes directly hash data and upload it to the chain, and aggregator nodes' smart contracts perform aggregate ID-based signature verification from IoT devices and then upload the transactions through Web3.js API; Layer 1: to reduce Ethereum gas fee, the Ethereum smart contract batch converts the layer 2 data to Merkle tree format and then uploads its Merkle root.

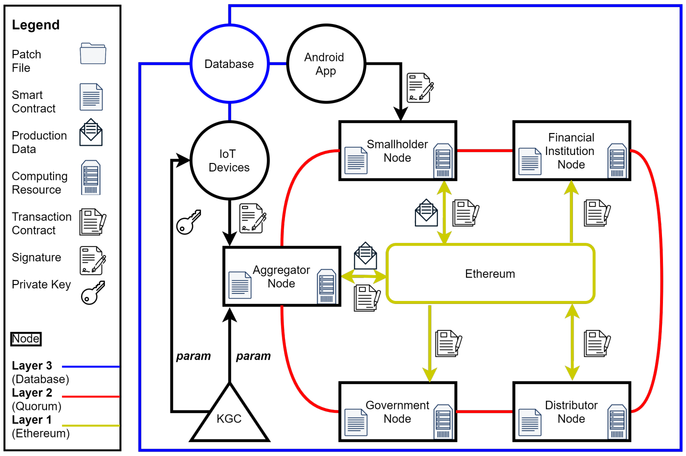

Fig. 1. Multi-layer Platform: Blockchain View

B. *Supply Chain Framework Based On Smart Contracts*

MLAV uses smart contracts to define the different rules, responsibilities, and relations of three types of nodes: Upstream Producer, Financial Institution, and Distribution Channel. Small upstream entities may upload and access their own production activity records, contracts, and transaction records to the blockchain while also solving supply chain finance.

IV. Experimental Results

We evaluate the performance of ID-based aggregate verification and other cases presented by [11]. Cases 1-5 consist of two types of operations. Our computational cost performance comparison and overhead are shown in Fig. 2. In our scheme, there are five components that are passed into the smart contract for updating the data.

V. Conclusion

We propose MLAV for IoT Blockchain and demonstrate its high efficiency in signature verification for Agriculture 4.0. By using ID-based signature verification for IoT devices, we reduce network traffic from IoT devices on the blockchain network significantly and transfer computing overhead to aggregator nodes. We design a highly efficient and effective supply chain management framework for agriculture 4.0. Smallholders may join the blockchain network without complex infrastructure; financial institutions may access this network and gain access to transparent data. This framework reduces the workload of all participants and accelerates the financial processes of the agriculture industry.

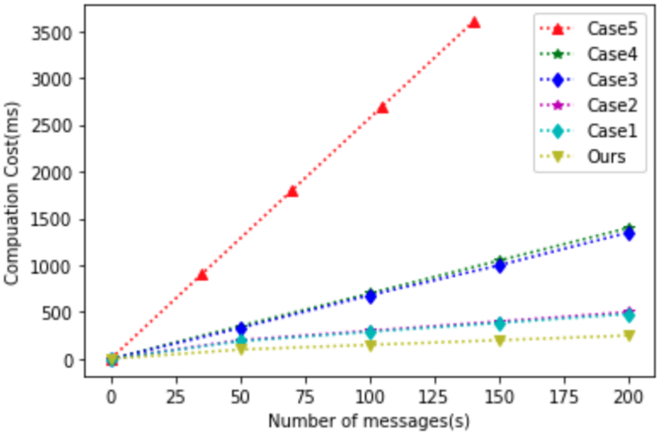

Fig. 2. Computation Cost

Acknowledgement

Ming-Fong Sie and Seth Austin Harding contributed equally to this paper.

References

[1] P. Gralla, "Precision agriculture yields higher profits, lower risks," *Hewlett Packard Enterprise*, 2018.

[2] W. Sarni, J. Mariani, and J. Kaji, "From dirt to data, the second green revolution and the internet of things," *Deloitte Review*, no. 18, 2016.

[3] A. Ellebrecht and N. Schouten, "Shared ledgers." [Online]. Available: https://www.compact.nl/articles/shared-ledgers/

[4] J. Benet, "Ipfs-content addressed, versioned, p2p file system," *arXiv preprint arXiv:1407.3561*, 2014.

[5] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[6] Y. Wang, J. H. Han, and P. Beynon-Davies, "Understanding blockchain technology for future supply chains: a systematic literature review and research agenda," *Supply Chain Management: An International Journal*, 2019.

[7] M. Tripoli and J. Schmidhuber, "Emerging opportunities for the application of blockchain in the agri-food industry," *FAO and ICTSD: Rome and Geneva. Licence: CC BY-NC-SA*, vol. 3, 2018.

[8] J.-W. Hu, L.-Y. Yeh, S.-W. Liao, and C.-S. Yang, "Autonomous and malware-proof blockchain-based firmware update platform with efficient batch verification for internet of things devices," *Computers & Security*, vol. 86, pp. 238–252, 2019.

[9] K. Hakuta, Y. Katoh, H. Sato, and T. Takagi, "Batch verification suitable for efficiently verifying a limited number of signatures," in *International Conference on Information Security and Cryptology*. Springer, 2012, pp. 425–440.

[10] H. Flatt, S. Schriegel, J. Jasperneite, H. Trsek, and H. Adamczyk, "Analysis of the cyber-security of industry 4.0 technologies based on rami 4.0 and identification of requirements," in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2016, pp. 1–4.

[11] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an internet of things environment," *The Journal of Supercomputing*, vol. 73, no. 3, pp. 1152–1167, 2017.