EasyChair Preprint

№ 596

The Blockchain Application in Supply Chain Management: Opportunities, Challenges and Outlook

Mark H. Meng and Yaou Qian

October 29, 2018

The Blockchain Application in Supply Chain Management: Opportunities, Challenges and Outlook

Mark H. Meng
Institute for Infocomm Research
Agency for Science, Technology and Research
Singapore
menghs@i2r.a-star.edu.sg

Yaou Qian
Monash Business School
Monash University
Caufield, VIC, Australia
yqia70@student.monash.edu

***Abstract*—Blockchain is a game changer in nowadays information technology and financial industry. Since Nakamoto invented the concept of blockchain together with its first application called "Bitcoin", the topic of blockchain has been inundated with the booming of cryptocurrencies. People expect this novel distributed ledger technology to bring a revolution to the entire industry and thereby grab the opportunity to expand and strengthen their business. The supply chain is treated as a typical use case to adopt blockchain and relevant technologies in many previous studies. In this paper, we conduct an interdisciplinary study on business supply chain management and the latest distributed ledger technology. In accordance with our discussion and experiments, we list three major benefits that the adoption of blockchain is able to bring to contemporary supply chain management. Meanwhile, we also identify a few of challenges that the nowadays blockchain application could not effectively excel, and the potential mitigation to those challenges as well.**

***Index Terms*—blockchain, business intelligence, distributed ledger, logistics, supply chain management**

I. Introduction

Blockchain is firstly invented by Satoshi Nakamoto in 2008 as a cryptocurrency called "*Bitcoin*" [1]. It is proposed as a public ledger in a peer-to-peer (P2P) distributed network. Despite an idea to replace the existing fiat currency, blockchain is known as a great innovation to record and store data on a distributed ledger with an effective protection mechanism. The blockchain technology provides a novel approach to building trust in a trustless environment and thereby guarantees data integrity, availability, traceability and security in data management [2].

Since the debut of *Bitcoin*, blockchain technology has experienced several rounds of evolution in the past decade. At the beginning, most of the blockchain applications are developed as cryptocurrencies. The first milestone in blockchain evolution is the introduction of *Ethereum* in 2014, where the concept of distributed contract has been firstly applied into blockchain [3]. From then on, the blockchain is no longer limited to recording financial transactions but a platform to execute arbitrary code on distributed applications [4]. However, the cryptocurrency is still a compulsory component in *Ethereum* to maintain the trust and consensus among the distributed network. In December of 2015, the Linux Foundation announced the creation of the *Hyperledger* project, which marks another significant evolution of blockchain technology. The *Hyperledger* is advertised as an umbrella project of open source blockchain and related tools. It supports multiple execution platforms and offers developers a wide range of API choices in different programming languages [5]. In *Hyperledger* projects, the cryptocurrency ceases to be a native and mandatory component and instead the concept of "smart contract" becomes the core feature of blockchain projects. The blockchain is placed into a context of pervasive computing, and those distributed applications in blockchain system are enabled to interact with the physical world through ubiquitous IoT devices [6]. Nowadays, a blockchain application could be analyzed from 4 perspectives – (1) a distributed ledger, (2) the cryptography behind, (3) the choice of consensus protocol and (4) the smart contracts [7].

In blockchain, all the data is inserted into and maintained by a public distributed ledger in form of transactions [8]. The ledger consists of a series of blocks in irrevocable order and open to access by any participants within the network. The transaction is the smallest unit to record data in the blockchain system. Every a fixed number of transactions will be enclosed into a block.

Consensus is another key component of a blockchain system to ensure the distributed network is able to eventually reach an agreement although there are some malfunctioning parties. The consensus protocol is an algorithm essentially designed to solve the *Byzantine General Problem* in a distributed collaboration and it is critical to maintain the fairness and liveness of a blockchain system [9]. The best known consensus protocols includes *proof-of-work*, *proof-of-stake*, *practical byzantine fault tolerance* (PBFT), etc [7], [10].

Cryptography is used in blockchain to guarantee the data integrity and security. Each transaction or block contains a unique digital signature, which allows an arbitrary user to easily verify its authenticity [8]. Moreover, the integrity of a block and all enclosed transactions is protected by a *Merkle*

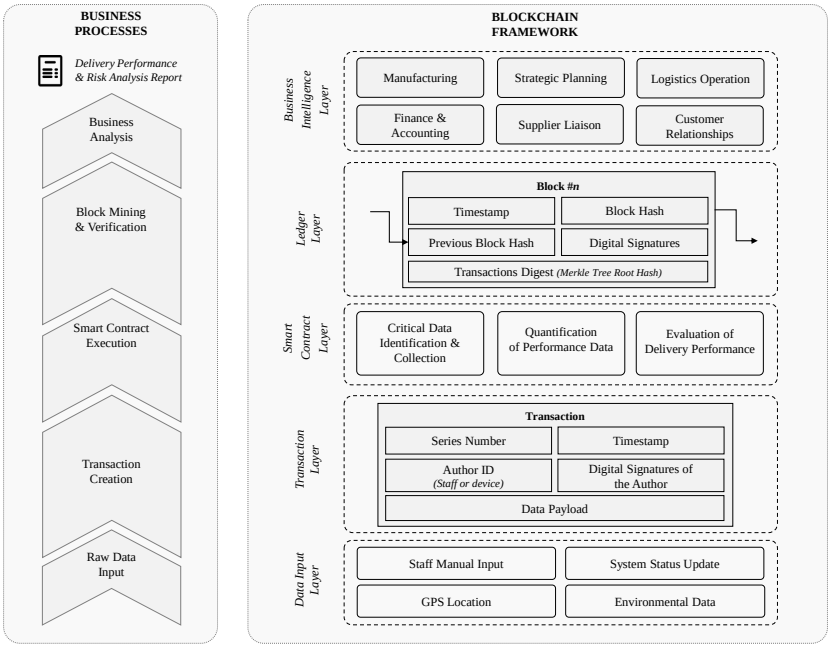

Fig. 1: The Layered Architecture of *DelivChain* and Corresponding Business Processes in Supply Chain Management

tree root hash. Any alteration in that data will result in a completely different hash value. As each block contains the hash value of its previous block, any modification made on the data within it will destroy all the subsequent blocks on the same ledger. For those reasons, it makes an attacker impossible to forge or tamper the data stored in the ledger [7].

Lastly, smart contract could be understood as an event-driven program to be executed at the moment a transaction is taking place. A smart contract exists as a reusable compiled source code stored in the blockchain system which could be automatically triggered to perform one or multiple contractual clauses at some specific circumstances. A smart contract could be simple as digital signature validation or financial balance checking. However, the complexity of smart contract grows rapidly along with the evolution of blockchain from a cryptocurrency to an integrated solution system in nowadays industry and business.

II. Blockchain Framework

In supply chain management (SCM), the most commonly used metric for delivery performance is so called "*OTIF*" (On-Time In-Full). The *OTIF* is a percentage value calculated from the division of the number of deliveries on-time in-full over the total number of planned deliveries. It transforms delivery performance from a qualitative description to a quantitative value and thereby facilitates the SCM in evaluation of the overall business performance [11]. The classic *OTIF* model has a limitation that it only enables business organizations to passively evaluate its delivery performance at post-delivery stage. Moreover, the lack of transparency and trust in traditional SCM makes business organizations difficult to obtain the data from other parties in a timely manner, and consequently influences the feasibility of real-time delivery performance evaluation. Under such circumstance, we proposed a blockchain framework for SCM called "*DelivChain*", and we explained the assessment model for real-time delivery performance evaluation in the previous literature [12].

DelivChain is designed as a consortium chain that only allows access and contribution from permissioned users, which makes it different with popular open access blockchain platforms like *Bitcoin* and *Ethereum*. A *DelivChain* instance is initialized for a specific contract that involves a group of organizations spanning over different stages in a supply chain. The staff and all data input devices belonging to the participating organizations are considered as users of *DelivChain* so that each of them is assigned to an account to access and contribute to the ledger. Prior to joining in the network, each user needs to generate a public and private key pair by following a commonly agreed encryption algorithm, share its public key across the network and meanwhile ensure the private key would not be known by any others. The network is usually led and regulated by the final manufacturing party that integrates all materials and semi-finished products into the final product for the customer delivery.

The functionality of *DelivChain* is implemented to capture all the data related to the latest status or progress throughout the supply chain and finally transform those raw data into analytics reports and profitable business intelligence. We show the layered architecture of *DelivChain* framework and corresponding business processes in Fig. 1. In that figure, we illustrate how a blockchain system defines the data model, collects the raw data, records into the immutable ledger and finally assists in achieving business intelligence by executing one or more well-designed smart contracts.

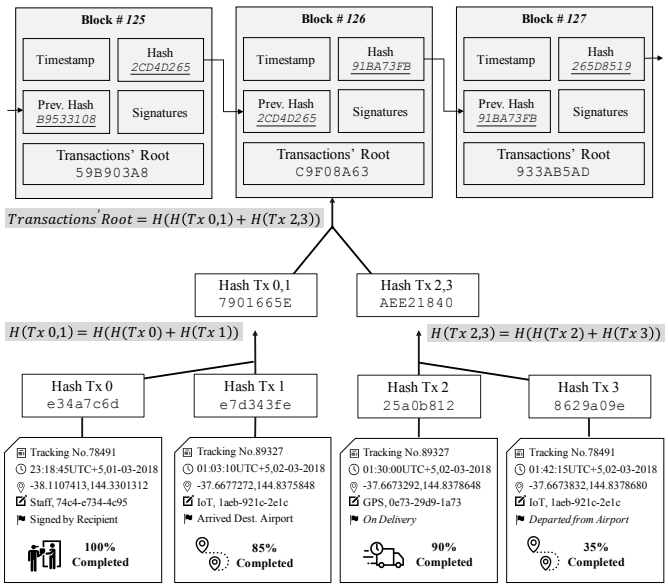

Fig. 2: Merkle Tree Hash Root Algorithm of Transactions in a Block

The data input layer of *DelivChain* defines the source of raw input data that can be used in subsequent layers. The raw data comes from both production and delivery happening in the supply chain. It could be recorded manually by staff, or automatically by the system. All the raw data captured are later formatted into a data structure called "transaction" in the next layer. A transaction is usually created immediately after a raw input data entity has been obtained, and then broadcast to the network for verification. A *DelivChain* transaction instance contains one raw input data entity and other relevant details includes the ID of input staff or device, the tracking number, a timestamp and an optional note-to-user. All the transactions which have passed the verification are distributed in the network and sorted in chronological order by their timestamps.

Smart contract is the core functionality of *DelivChain* to bring benefits to stakeholders of the supply chain. In *DelivChain*, a smart contract is performed right after the submission of a new transaction. The smart contract completes all role-based logical operations to select useful raw data from the ledger and then transfer those real-time raw data to a series of values which are properly formatted for business analytics.

In ledger layer, all the recently created transactions are placed in a distributed pool across the network and wait for the next block miner to package all of them into a new block and append into the ledger. As in Fig. 2, those transactions associated with one block are not saved as text but a hash digest generated by calculating the root of a Merkle Tree. *DelivChain* is designed as a consortium blockchain where a certain level of trust exists among the participants. For that reason, it adopts Practical Byzantine Fault Tolerant algorithm as the consensus protocol. The miner of next block could be elected from the active participants at the moment of new block being appended to the ledger. Moreover, there could also be an administrative account randomly determines and appoints the miner of the next block. In this way, a block, including all the transactions associated with it, becomes permanently immutable after being appended into the distributed ledger.

The business intelligence layer at the top denotes the application deployed upon our *DelivChain* system to perform business analytical tasks. It could be done purely automatically by using a business analytics software, or mixture of systematic analytics and manual analysis. The goal of this layer is to transform real-time quantitative values that reflect the estimated delivery performance to a periodical qualitative report written in business readable language and expression.

III. Opportunities for SCM

In this section, we discuss the potential benefits that *DelivChain* can bring to the real business operation in SCM.

A. Data Security

First of all, as a blockchain framework, our *DelivChain* platform enables all registered users to access and contribute to the distributed ledger. Owe to a group of ingenious cryptographic algorithms adopted in the blockchain technology, any data is impossible to be tampered or deleted once it has been appended to the ledger. Moreover, the distributed feature of the ledger of blockchain makes malicious user impossible to completely erase a part of the ledger over the entire network. By making advantage of Practical Byzantine Fault Tolerant consensus, the distributed ledger could always maintain the order of the network and eventually reach an agreement as long as there are not more than one third users are anomalous simultaneously. Compared with other traditional data storage solution, blockchain offers greater integrity, accountability, accessibility and non-repudiation to its users.

B. Trust and Transparency

In use case of the industrial supply chain, our *DelivChain* can serve as a trusted medium in a trustless environment that filled with omnipresent business competition. All participants in a supply chain can trust *DelivChain* platform even they do not trust each other. In addition, the *DelivChain* ensures transparency within a supply chain since all users have to append the data under promise into the ledger on time and without any reservation. Both trust and transparency are crucial in building a healthy and sustainable business environment – our *DelivChain* could give a helping hand to it.

C. Business Intelligence

Data is the key component to enable a business organization to conduct strategic analysis. Performing analytics and analysis based on historical data could help an organization in making not only accurate but also long-term decisions and thereby achieve profitable business intelligence. Nowadays, blockchain technology is the catalyst of the pursuit of business intelligence due to a series of advantages such as low cost, perfect security and high level automation. Blockchain moves a step further to provide a business organization with real-time large-scale

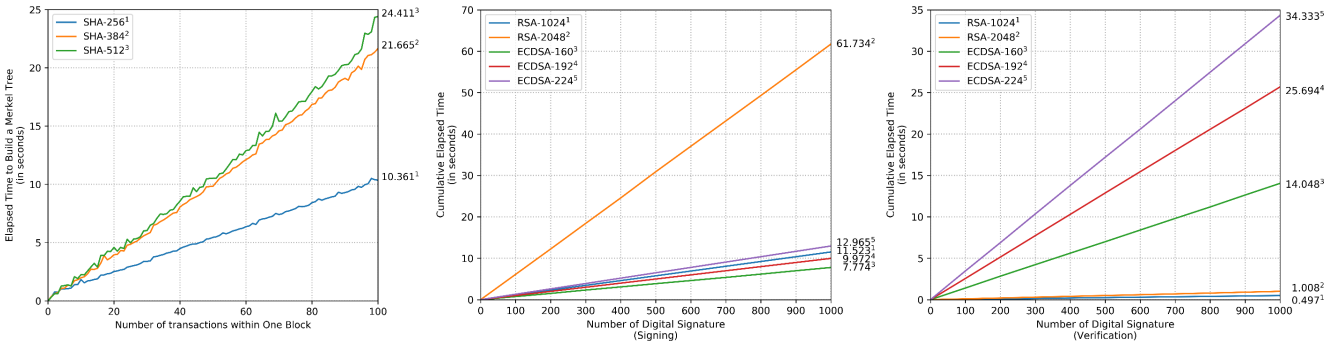

Fig. 3: Benchmarking of 3 Most Common Cryptographic Operation in DELIVCHAIN System on Mainstream IoT Devices (Raspberry Pi Model 2B) with Single Thread Execution

data. An ideal smart contract can filter out all irrelevant data from the ledger and perform quantitative analytics for users. By taking the capability of both suppliers and delivers into consideration, our proposed estimated-OTIF model in *DelivChain* could provide more comprehensive result compared with the traditional static evaluation. It will be extremely helpful when there is a severe, unpredicted and unexpected impending hazard in the supply chain.

IV. Challenges and Future Directions

Despite a series of opportunities that the adoption of blockchain technology brings to the industry, the shortcomings of blockchain are still notable for discussion. In this section, we discuss the challenges that the industry is currently facing to whilst the integration of blockchain into the existing SCM system. We summarize 3 challenges that are urgently waiting for a solution to facilitate large scale adoption of blockchain into industry, and moreover we also discuss the potential mitigation as the direction of future advance.

A. Performance

The successful digital transformation in SCM owes to the development of Internet of things (IoT) technologies [13]. The omnipresent IoT devices and sensors, which is considered as the key to achieve the blockchain integration, could collect various kinds of data and upload to the network in a controllable way [14]. Compared with traditional programmable machines, the latest IoT technology provides industry users a lightweight solution in deployment with a lower cost and less energy consumption. However, the comparable low performance is one of the biggest challenges in the blockchain integration. In order to discuss the performance of IoT device in blockchain system, we conducted an experiment to benchmark the 3 most common cryptographic operations, which are Merkle root hash calculation, digital signature signing and digital signature verification, on a typical IoT device model *Raspberry Pi*. As we show in Fig. 3, our experiment unveils that the digital signature signing and verification are the greatest limitation in the performance aspect in blockchain applications. Moreover, the Merkle tree hash calculation could also slow down the overall processing if a large number of transactions are set in per block. One possible mitigation could be selection of cryptography to optimize the IoT features in blockchain use case. For example, the IoT formed blockchain system is encouraged to adopt Elliptic curve cryptography algorithm (ECC) to replace the traditional RSA algorithm as it has smaller key in size and saves much computational resources in signature signing [15].

B. Scalability

Once a blockchain system has been deployed, the total number of transactions will tremendously grow. Due to the immutable feature of the distributed ledger, each participant in the network has to keep an independent copy of the ledger to verify transactions and mine new blocks, which will inevitably result in data redundancy and database overloading. There are some researchers working hard to address the scalability concern in blockchain application. The concept of *Bitcoin-NG* is an innovative approach which redesigns the classic ledger organization of blockchain and decouples the traditional ledger into two parts: the microblock to store transaction information, and the key block for leader election [16].

C. Privacy

Participants in a blockchain system are identified by their key pairs. Other users could not directly recognize the actual identity by reading the ledger in a distributed network. However, anonymity doesn't imply untraceability. The classic blockchain could not perfectly preserve users' privacy because there is still a possibility to unveil the identity by observing one or more fixed transaction patterns from the ledger [17]. Global supply chain is filled with business competition so the privacy issue is more significant and urgent. Any confidential data of a business organization obtained by its rivals could possibly lead to loss in core competitiveness. Some cryptocurrency variances such as *Zerocoin* choose to pursue an absolute anonymous solution as the response to people's concern. They use zero-knowledge proof to validate if a transactions is derived from

other verified transactions rather than if it is signed by a specific user [18]. Another approach is to identify the author of the transaction by affiliation instead of by a single user. By making use of group signature or ring signature techniques, the participants in a supply chain could group themselves by geographic distribution or by specific contract, thereby maximize the obfuscation effect in anti-tracing protection [19].

V. Outlook

During past a few years, there are a number of blockchain models and applications have been discussed within academia around the world. Meanwhile, the blockchain technology also receives bullish statements by a wide range of industries.

Blockchain is born to be a great solution to record and manage data that changes correspondingly in different phases. In the era of ubiquitous computing, blockchain technology could tremendously strengthen other existing applications of industrial IoT (IIoT), such as the process tracking in next-generation of manufacturing [20], food traceability management for the smart agriculture [21] and building trusted communication among different fields and channels [22]. In addition to the commercial application, blockchain technology could also benefit the collaboration between individuals and public agencies. Some illuminating topics have been recently published, for example the adoption of blockchain in intelligent transportation system [23] and police forensics [24].

To sum up, the blockchain technology brings a lot of opportunities in the industry. The challenges of blockchain applications are believed to be eventually addressed and solved by the endless development of new technology. In the future, the blockchain, or perhaps its derivatives, shall be pervasively involved into our daily lives and protect users' data against loss, leakage and tampering.

VI. Conclusion

In this paper, we conducted an interdisciplinary study on the application of blockchain and relevant technologies in nowadays supply chain management. We provide a comprehensive effort to construct a layered blockchain framework with concrete technical details based on previous literature. In order to simulate the actual operation and benchmark the performance of computing units across the supply chain, we make use of IoT hardware to carry out a series of experiments. Furthermore, we summarize the potential opportunities and benefits of *DelivChain* could bring to nowadays industrial supply chain from different perspectives, and we discuss the most significant challenges that the industry faces to during the adoption of blockchain technology into their existing systems. In the end, we propose a number of directions for future advance as the mitigation and we illustrate our outlook on potential industrial applications of blockchain technology.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] N. Levenson, "Trust In A Trustless System? How Ontology Could Bring Big Business To Blockchain," 2018, (Accessed 19-Sep-2018). [Online]. Available: https://hackernoon.com/trust-in-a-trustless-system-how-ontology-could-bring-big-business-to-blockchain-fd73260ffee9

[3] V. Buterin, "Ethereum: Now Going Public," 2014, (Accessed 1-April-2018). [Online]. Available: https://blog.ethereum.org/2014/01/23/ethereum-now-going-public/

[4] K. Zhang and H. Jacobsen, "Towards dependable, scalable, and pervasive distributed ledgers with blockchains," in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, July 2018, pp. 1337–1346.

[5] Hyperledger, "Hyperledger Fabric 1.0 is Released!" 2017, (Accessed 1-April-2018). [Online]. Available: https://www.hyperledger.org/blog/2017/07/11/hyperledger-fabric-1-0-is-released

[6] M. Swan, *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[7] D. T. T. Anh, M. Zhang, B. C. Ooi, and G. Chen, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, 2018.

[8] S. Apte and N. Petrovsky, "Will blockchain technology revolutionize excipient supply chain management?" *Journal of Excipients and Food Chemicals*, vol. 7, no. 3, 2016.

[9] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982.

[10] A. Castor, "A (Short) Guide to Blockchain Consensus Protocols," 2017, (Accessed 19-Sep-2018). [Online]. Available: https://www.coindesk.com/short-guide-blockchain-consensus-protocols/

[11] M. Christopher, *Logistics & supply chain management*, 4th ed. Pearson UK, 2011.

[12] M. H. Meng and Y. Qian, "A blockchain aided metric for predictive delivery performance in supply chain management," in *2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, 2018.

[13] K. Patel and M. McCarthy, "Digital transformation," *The Essentials of e-Business Leadership. New York*, 2000.

[14] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," in *proceedings of the 50th Hawaii international conference on system sciences*, 2017.

[15] E. F. Jesus, V. R. Chicarino, C. V. de Albuquerque, and A. A. d. A. Rocha, "A survey of how to use blockchain to secure internet of things and the stalker attack," *Security and Communication Networks*, vol. 2018, 2018.

[16] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol." in *NSDI*, 2016, pp. 45–59.

[17] J. Clifford, "Privacy on the blockchain," 2017, (Accessed 1-Sep-2018). [Online]. Available: https://hackernoon.com/privacy-on-the-blockchain-7549b50160ec

[18] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *Security and Privacy (SP), 2013 IEEE Symposium on*. IEEE, 2013, pp. 397–411.

[19] S.-F. Sun, M. H. Au, J. K. Liu, and T. H. Yuen, "Ringct 2.0: a compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero," in *European Symposium on Research in Computer Security*. Springer, 2017, pp. 456–474.

[20] S. Trouton, M. Vitale, and J. Killmeyer, "3D opportunity for blockchain: Additive manufacturing links the digital thread," 2016, (Accessed 1-Sep-2018). [Online]. Available: https://www2.deloitte.com/insights/us/en/focus/3d-opportunity/3d-printing-blockchain-in-manufacturing.html

[21] J. Lin, Z. Shen, A. Zhang, and Y. Chai, "Blockchain and iot based food traceability for smart agriculture," in *Proceedings of the 3rd International Conference on Crowd Science and Engineering*. ACM, 2018, p. 3.

[22] J. Lin, Z. Shen, and C. Miao, "Using blockchain technology to build trust in sharing lorawan iot," in *Proceedings of the 2nd International Conference on Crowd Science and Engineering*. ACM, 2017, pp. 38–43.

[23] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, 2017.

[24] D. P. Le, H. Meng, L. Su, S. L. Yeo, and V. L. L. Thing, "Biff: A blockchain-based iot forensics framework with identity privacy," *Region 10 Conference, TENCON 2018 IEEE*, 2018.