International Journal of Computer (IJC)

ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Distributed Ledger Technology: Applications and its Convergence in Industrial Revolution 4.0

Khiam Ping Chih[a]*, Sokchoo Ng[b]

[a,b]*Faculty of Science, Technology, Engineering and Mathematics, International University of Malaya-Wales, Kuala Lumpur, Malaysia*

[a]*Email: khiamping@yahoo.com*

[b]*Email: ashleyng@iumw.edu.my*

Abstract

Distributed ledger technology (DLT) has garnered a tremendous amount of attention in recent years due to the popularity of blockchain-related cryptocurrencies. However, layperson will have difficulty cutting through the hype and being objective enough to evaluate the benefits and shortcomings of this technology. This study attempts to provide answer to the following questions: 1) what is DLT, and the difference of its two popular specializations: blockchain and directed acyclic graph (DAG)? 2) how far have the society achieved through DLT applications in the field of healthcare, identity management as well as copyright and intellectual property? 3) how does the general public view the convergence of DLT applications in Industrial Revolution 4.0? Through rightly education and understanding of DLT, the society will value the technology better of its application in different sectors.

Keywords: Distributed ledger technology; blockchain; directed acyclic graph; industry revolution 4.0.

1. Introduction

Distributed ledger technology (DLT) has gained tremendous amount of attention in recent years due to the popularity of blockchain-related cryptocurrencies [1]. The number of startups and tech-related companies worldwide that seek to provide DLT-based products and solutions have risen in quantities and sizes. Scores of consultation report and whitepaper have been commissioned and published by various governmental bodies to solicit public feedbacks on the adoption and usability of DLT in their respective countries [2].

----

* Corresponding author.

The academia, on the other hand, advanced this technology through various research and teaching activities [3,4]. As the result of its establishment, a technical committee on blockchain and distributed ledger technology, known as ISO/ TC 307 has been formed in 2016 under the International Organization for Standardization (ISO), gearing towards a common standard in this technology. The overwhelming momentum and popularity gained by DLT in such a short span of time has given an impression to the layperson in the society that something revolutionary is coming the way. There is a mixed form of reaction, however, towards DLT. On one hand, the early price boom of cryptocurrency such as Bitcoin have got the exponents of this technology hype up [5]. Many theoretical solutions that applies DLT for existing problems followed through, and compounded with wide media coverage provide an impression that DLT could be applied in most, if not all, application domains to enhance online transaction security and trustworthiness. The detractors, on the other hand, remain noncommittal and skeptical about its adoption and potential capabilities. From their view point, it could be just another technological-hype that eventually will die off. Eventually, the layperson will have difficulty cutting through the hype and being objective enough to evaluate the benefits and shortcomings of this technology. A proper understanding of DLT is crucial so that public able to justify feasibility of the technology in their respective domain applications and able to anticipate the inherent risks and impact of its application. In the early stage of DLT, the technology is always associated with finance and digital currency domains. This study seeks to review on the current application of this technology that it could bring about over and above the financial context. This study attempts to provide answer to the following questions:

1. What is DLT, and the difference of its two popular specializations: blockchain and directed acyclic graph (DAG)?
2. How far have the society achieved through DLT applications in the field of healthcare, identity management as well as copyright and intellectual property?
3. How does the general public view the convergence of DLT applications in Industrial Revolution 4.0?

The remaining of this article is according to the following structure: Section 2 provides an overview on DLT, and its two popular specializations: blockchain and DAG. This section provides good-enough information for layperson to understand and differentiate DLT, blockchain and DAG, in general. In section 3, we explore the current applications of DLT which span beyond the finance and digital currency domains. Section 4 provides the future directions for DLT application in view of the Industrial Revolution 4.0 (IR 4.0). Section 5 provides a concluding remark on this study.

2. DLT Overview

General public are confused between DLT and blockchain due to the lack of standard definition for both. Quite often the terms are used interchangeably and often they are being treated as synonym. Schueffel [6] is of the opinion that blockchain technology should be treated as a specialization under DLT together with other forms of specialization such as Tangle and Hashgraph. The important distinction between these specializations rest on the architecture and the way consensus protocol is reached within the respective networks. In the discussion paper published by the UK Financial Conduct Authority, DLT is described as "a set of technological solutions that enables a single, sequenced standardized and cryptographically-secured record of activity to be safely distributed to, and acted upon by, a network of varied participants" [7]. Technically, DLT works through a combination of technologies such as cryptography, peer-to-peer (P2P) networks and decentralized database systems. Therefore, DLT should not be viewed as a whole unique technology. Instead, it is just the way DLT is being pooled and applied into a new scenario. The structural composition of DLT will very much determine the practicability of its application. As such, there is a need to understand its underlying structure so that the public community is able to gauge the potential DLT use cases in a meaningful way.

2.1. Blockchain

Blockchain has enjoyed much publicity and attention due the first appearance of Bitcoin in 2008 [5]. Bitcoin is essentially a digital currency that is being proposed to solve the double-spending problem [8]. Blockchain has characteristics which are very much similar to that of a DLT in the way of anonymous, auditable, decentralize, fault-tolerant and persistent [9]. The anonymity character of blockchain allows user to interact with the network by using a public key hash address which does not reveal the true identity of the user. Since every recorded transactions is timestamp and transparent, users can audit the record and back-trace the past transactions stored in the blockchain network. A decentralized system in blockchain is formed through a large number of nodes across the network. It allows for a P2P transaction to be carried out without the need of control and approval from a central authority. Once a transaction is verified by a particular node via certain protocols, it will be broadcasted to all the connecting nodes in the network. The fault-tolerant feature of blockchain allows for continuous operation of the network even in the event that some of its nodes are malfunction. This is unlike a centralized system where any malfunction at its core will cause the entire network to cripple. Finally, the persistency feature of blockchain will forbid any users to amend or delete any transactions which have been added into the blockchain network. The transactions cannot be modified once verified by the nodes and as a result any fabrication is deemed to be difficult. In the literature by [10], the researcher categorized various blockchain applications into three major categories, namely Blockchain 1.0, 2.0 and 3.0. Blockchain 1.0 is about cryptocurrency that is being deployed for applications related to digital payment systems and money remittance. Blockchain 2.0 looks further than decentralization of currency and payment systems. It has propagated into the idea of a shared database that enables access from the public [11]. Reference [10] categorized various smart contract applications that involved in transfer of assets of any kind beyond currency under this category. Blockchain 2.0 is essentially the decentralization of the markets. Lastly, the Blockchain 3.0 gathered all blockchain applications that is beyond crypto currency and finance related domain such as intellectual property management systems, record repositories and digital arts.

2.2. Working Structure of Blockchain

Blockchain architecture consists of a growing list of sequential 'block' maintained by peers whereby all transactions recorded in the blocks are secured cryptographically, and thus immutable [12]. Figure 1 provides an illustration of a basic blockchain where the genesis block is the starting block in the chain and every other blocks are being backward-linked via hash values. Each block has two separate parts, namely the block header and the block body. The block header includes information like the block version, the preceding block header hash, a merkle tree root hash, a timestamp for the transaction, nBits (also known as target hash), and the nonce.

The block version refers to a set of validation rules that must be comply with. Since blockchain is formed through a sequence of validated transactions, each block will carried the preceding block header hash (a 256-bit hash value) with exception to the genesis block. The merkle tree root hash, on the other hand, indicates the hash value for all transactions in the block. Each block header consists of a timestamp for the transaction and the target threshold for each valid block hash is represented by nBits. While the nonce is added in an encrypted block, when rehashed, it meets the difficulty level constraints set by the target. The maximum amount of transactions allowed in a block is determined by the size of individual transaction and the block size as well. Meanwhile, the block body consists of a collection of transactions and each of it will have an input transaction IDs and an output that specify the transacted amount and the destination address. An input transaction IDs refers to the unspent transaction outputs (UTXO), i.e. the balance owned by sender before a transaction. A digital signature based on asymmetric cryptography algorithms that ensures the nonrepudiation and uphold the integrity of the transaction is used to secure it [13].

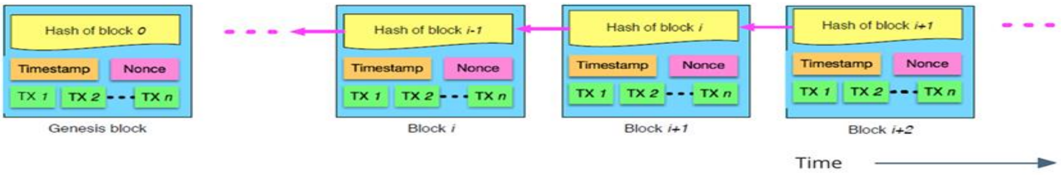

Figure 1: Generic Blockchain Structure

2.3. Directed Acyclic Graph (DAG)

Catching up with the popularity of blockchain, DAG is an alternative under the umbrella of DLT. Tangle and Hashgraph are two examples of DAG. Fundamentally, they are different from blockchain in terms of architecture and consensus-reaching mechanism. For Tangle and Hashgraph, they do not have “blocks” and “chains” that formed the continuous ledger like in blockchain. They are not required to have a majority of nodes in the network to always be sync about the all transactions contained in the network. Instead, it is based on the concept of acyclicity, where no assumptions to be made about when a particular information reaches an individual participant in the network [6]. A DAG network can be viewed as a “tree”, where a single transaction is linked to multiple differing transactions.

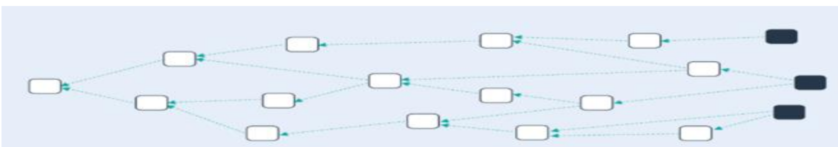

Figure 2: A DAG network of transactions

Figure 2 shows a DAG network of transactions. In terms of consensus protocols, unlike blockchain which requires some validation rules to be complied before a particular transaction is deemed successful, DAG only requires the user who initiates a transaction to provide validation for other transactions. It removes the need for “miners” in a blockchain network and fees associated with the transactions validation. This enables DAG network to scale efficiently and could well handle large volume of transactions. The larger is the volume of transactions, the faster it will be for each transaction to be validated.

3. DLT Applications

Blockchain 3.0 is all about the application of DLT beyond the realm of finance. In this section, we will look at some of the DLT applications in the field of healthcare, identity management as well as copyright and intellectual property.

3.1. Healthcare

Plenty of research have been conducted into use cases of blockchain in healthcare. A distributed record-keeping using blockchain is deemed to be cheaper, reliable and faster to access [14]. Ivan [15] works on patient-managed healthcare record using blockchain. Patients will own and control access to their healthcare record and data that basically remove the need to acquire physical copies of it when they are transferred to another healthcare service provider. Similarly, in [16], the authors proposed an App called Healthcare Data Gateway (HGD) that is based on blockchain architecture that allows patient to own, control and share their own data effortlessly and securely without violating privacy. Blockchain is being used as a medium to store a secure copy of patient's own medical record for the purpose of exchanging and validating among stakeholders. Reference [12] summarizes the detail implementation of blockchain in the healthcare ecosystem. Apart from medical data management, blockchain is also applicable to enhance the insurance claiming process by providing real-time claim processing that effectively remove the need for intermediaries [17]. An auditable trail of the claim process and the data provenance can be established. It will reduce the chances of fraud and provide an easier way for verifiable claim qualification.

3.2. Identity Management

Reference [18] proposed a novel framework for human identification management that integrates biometric identification and DLT. The framework works to embed accurately personal information into a blockchain-based system that allows construction of digital IDs which will be stored in a mobile device. On the other hand, Lee [19] introduced a novel blockchain ID as a service (BIDaaS) for digital identity management. BIDaaS is essentially a private blockchain in which the entire network is controlled by the provider or a consortium of members. The benefit to the user is that no unnecessary accounts creation for services that the user may only use for a short period of time. It allows user a choice not to provide his personal information to various service providers.

3.3. Copyright and Intellectual Property

Blockchain can introduce long-awaited transparency in matters of copyright and intellectual property ownership. It provides for a substantial risk aversion of online digital privacy through the control over digital ownership. Reference [20] argued for the use of blockchain to facilitate the application of creative common rights (also known as open source) licenses with revenue streams that will be enforced using blockchain smart contract.

4. Convergence of DLT in Industrial Revolution 4.0

The IR 4.0 was conceptualized in the middle of 2010 through a strategic initiative by the German government with the aim of transforming industrial manufacturing through digitalization and other mean of new technologies [21]. The model for IR 4.0 is not based upon a sole technology or disruptive theory. The concept of IR 4.0 predicts interconnectivity, either horizontally or vertically, among all technologies present in the industrial environment. Looking into the future of DLT applications, specifically the convergence of Blockchain technology on Industry 4.0, it contributes to the operational process of IR 4.0, incorporating the provenance of goods, raw materials, financial transactions between industries, consumers and stakeholders as well as legislative compliance. The immutable feature of blockchain could be a potential application to provide reliable provenance of every single operation registry. Besides that, the transparency feature of blockchain to evaluate the goods and data provenance in an industrial scenario, granting the traceability of not only logistics, but also fostering the acknowledgement of the compliance with the standards. Furthermore, DLT can be linked to the concept of Economy of Things, which is the amalgamation of Internet of Things (IoT) and other technologies. The utilization of IoT devices on top of blockchain architecture will have enough autonomy to establish contracts with peers, and can automatically clear the payment upon the accomplishment of a certain task or services. Lastly, DLT contemplates the improvement of the whole supply chain given these benefits when the blockchain is integrated in the IR 4.0 environment.

5. Conclusion

Distributed ledger technology is a newly coined word for existing technologies and being applied into new scenarios that most of the time is used interchangeably with blockchain due to lack of standard definition. Two specializations of DLT, namely blockchain and DAG, differs in their own way in terms of structure and application of consensus protocols to validate a particular transaction. Many attempts to apply DLT or blockchain for existing problems revolved around digital currency and in financial context. This study achieve its aim to review on how DLT has been applied to practical use cases beyond the financial context. What is known at this very moment is that DLT have yet to reach the required disruptive level in the society in terms of adoption and implementation. It is interesting to note about how far can the integration between DLT and IR 4.0 happens in the future.

References

[1]. El Ioini, Nabil, and Claus Pahl. "A Review of Distributed Ledger Technologies.", in Proc. OTM 2018 Conferences Confederated International Conferences: CoopIS, C&TC, and ODBASE 2018, vol. 11230, LNCS, Springer, 2018, pp. 277–88.

[2]. S. Ølnes, J. Ubacht and M. Janssen. "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing." Government Information Quarterly, vol. 34, issue. 3, pp. 355 – 364, 2017.

[3]. J. Moubarak, M. Chamoun and E. Filiol. "On distributed ledgers security and illegal uses." Future Generation Computer Systems, vol. 113, pp. 183 – 195, 2020.

[4]. A. Shahaab, B. Lidgey, C. Hewage and I. Khan. "Applicability and appropriateness of distributed ledgers consensus protocols in public and private sectors: a systematic review." IEEE Access, vol. 7, pp. 43622-43636, 2019.

[5]. N. Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008.

[6]. P. Schueffel. "Alternative distributed ledger technologies blockchain vs. Tangle vs. Hashgraph - a high-level overview and comparison." SSRN Electronic Journal, 10.2139/ssrn.3144241, 2017.

[7]. UK Financial Conduct Authority. "Discussion Paper on distributed ledger technology." https://www.fca.org.uk/publication/discussion/dp17-03.pdf, 2018.

[8]. G. O. Karame, E. Androulaki and S. Capkun, S. "Double-spending fast payments in bitcoin." in Proceedings of the 2012 ACM conference on Computer and Communications Security, United States, 2012, pp. 906 – 917.

[9]. Z. Zheng, S. Xie, H. N. Dai and H. Wang. "Blockchain Challenges and opportunities: A survey." International Journal of Web and Grid Services, vol. 14, no. 10, pp. 352-375, 2016.

[10]. M. Swan, Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015.

[11]. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang. "An overview of blockchain technology: architecture, consensus, and future trends." in Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, 2017, pp. 557-564.

[12]. E. Mirdah, Sokchoo Ng and Khiam Ping Chih. "Review on Blockchain Technology for Healthcare Records." Internatioanl Journal of Computer, vol. 33, no. 1, pp. 39 – 45, 2019.

[13]. K. Christidis, and M. Devetsikiotis. "Blockchains and smart contracts for the internet of things." IEEE Access, vol.4, pp. 2292-2303, 2016.

[14]. M. Alharby and A. V. Moorsel. "Blockchain based smart contracts: A systematic mapping study." Computer Science & Information Technology (CS & IT), 2017, pp. 125-140.

[15]. D. Ivan. "Moving toward a blockchain-based method for the secure storage of patient records." in Proceedings of the Use of Blockchain for Healthcare and Research Workshop, United States, 2016.

[16]. X. Yue, H. Wang, D. Jin, M. Li and W. Jiang. "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control." Journal of Medical Systems, vol. 40, no. 10, pp. 218, 2016.

[17]. K. Culver. "Blockchain technologies: A whitepaper discussing how the claims process can be improved." in Proceedings of the Use of Blockchain for Healthcare and Research Workshop, United States, 2016.

[18]. Z. Gao, L. Xu, G. Turner, B. Patel, N. Diallo, L. Chen and W. Shi. "Blockchain-based identity management with mobile device." in Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Germany, 2018, pp. 66 – 70.

[19]. J. Lee. "BIDaaS: Blockchain based ID as a service." IEEE Access, vol. 6, pp. 2274-2278, 2018.

[20]. A. Savelyev. "Copyright in the blockchain era: Promises and challenges." Computer Law & Security Review, vol. 34, no. 3, pp. 550-561, 2018.

[21]. A. Rojko. "Industry 4.0 concept: background and overview." International Journal of Interactive Mobile Technologies, vol. 11, no. 5, pp. 77-90, 2017.