Blockchain and IoT-based architecture design for intellectual property protection

Jun Lin
Alibaba-NTU Joint Research Institute, Nanyang Technological University, Singapore and Joint SDU-NTU Centre for Artificial Intelligence Research (C-FAIR), Shandong University, Jinan, China

Wen Long
Intellectual Property Publishing House Co., Ltd, Beijing, China

Anting Zhang
Department of Automation, National Engineering Laboratory for E-Commerce Technologies, Tsinghua University, Beijing, China, and

Yueting Chai
Tsinghua University, Beijing, China

Abstract

Purpose – The blockchain technology provides a way to record transactions that is designed to be highly secure, transparent, trustable, traceable, auditable and tamper-proof. And, the internet of things (IoT) technology provides the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction, which is able to link computing devices and digitized machines, things, objects, animals and people that are provided with digital unique identifiers (UIDs). This paper aims to explore the combined application of blockchain and IoT-based technologies, especially on the intellectual property protection area.

Design/methodology/approach – In this paper, the authors propose a high-level architecture design of blockchain and IoT-based intellectual property protection system, which can help to process three types of intellectual property: (1) patents, copyrights, trademarks etc.; (2) industrial design, trade dress, craft works, trade secrets etc.; and (3) plant variety rights, geographical indications, etc.

Findings – Using blockchain peer-to-peer network and IoT devices, the proposed method can help people to establish a trusted, self-organized, open and ecological intellectual property protection system.

Originality/value – To the best of the authors' knowledge, this is the first work that applied blockchain and IoT technologies on traditional intellectual property protection and trade ecosystem.

Keywords Internet of things (IoT), Blockchain, Intellectual property protection

Paper type Research paper

1. Introduction

Intellectual property (IP) is a category of property that includes the intangible creation of human individuals or crowd intellect, such as intangible knowledge, ideas or crafts. In general, forms of IP protection, which were recognized by most of global countries, include patents, copyrights, industrial design rights, trademarks, plant variety rights, trade dress, geographical indications and, in some jurisdictions, trade secrets. In today's digital and globalized economic era, the intangible nature of IP brings difficulties of protection compared to traditional assets such as money, land and goods, which makes IP protection more challenging.

Firstly, the digitization of knowledge or creativity makes the reproduction and plagiarism of the works easier, and the difficulty and cost of discriminating the originality of the works are greatly increased. Secondly, this is an era of big data and data explosion. The protection of IP needs the ability to analyze and verify the authenticity of massive samples. Finally, globalization and the digitization of works have led to faster and faster infringement and dissemination, and there is a strong timeliness requirement for the determination of the rights and infringement of IP rights in original works.

Traditional IP protection requires a high degree of professionalism and usually requires practitioners with professional background and familiarity with relevant laws and regulations. Limited by the problems of cost and institutional settings, there are large gaps in IP practitioners and serious shortage of manpower. This requires the use of the power of technology to protect the creative enthusiasm of innovators. Unfortunately, existing IP protection technologies are not sufficient to track, discover, authorize and prohibit the abuse of IP, especially for digital products, which are easily copied and disseminated through the network, as well as counterfeiting and tampering of non-digital works also happen from time to time. For example, in the case of Beijing Palace Museum and Prince Gong's Mansion, they often launch some crowdfunding projects with the theme of art production, but often in the early days of crowdfunding, their ideas are stolen and counterfeited, and even went on sale in advance, leading to the loss of creativity or the failure of the project.

Regarding the issue above, in China, the Intellectual Property Publishing House has explored a new model of IP protection – "Maker-IP". Maker-IP is an original certification protection platform designed and developed by the Intellectual Property Publishing House and supervised and approved by China National Intellectual Property Administration. By collaborating with the Judicial Identification Center and the Beijing Digital Certification Center, the platform provides defensive public services; provides authoritative, objective and convenient evidence preservation services for intellectual creators; and provides knowledge management services for enterprises and research teams. The "Maker IP" platform can record screens, capture screens, upload, deposit and authenticate documents in real time across different operating systems. The scope of certification includes dozens of categories and fields, including art creation, industrial design, academic documents and business documents. The preservation safety of documents reaches a level of three. The main certification objects currently offered by the platform include the following.

1.1 Technological achievements certification

It means defensive disclosure of patented technology. Defensive disclosure refers to the disclosure of an invention/creation to prevent others from applying for a patent. Its advantage is that it can ensure that no one can obtain the exclusive right of the invention or technology, and meanwhile, it also gives everyone the freedom to use, transform and update the invented technology. When conducting defensive disclosure, the more traditional way is to publish it in widely recognized technical magazines or publications that are likely to be

reviewed by patent examiners for future patent applications. In the internet era, there are new channels for disclosure access. The Maker-IP platform uses trusted timestamp technology to realize the solidification of data disclosure time, ensuring its legitimacy and non-tampering. The module can help users achieve the goal of defensive public access in a real-time, convenient and economical manner.

1.2 Copyright certification
It means that through the Maker-IP platform, the creation process and results of works can be completely saved in real time, and the preserved data can be stamped with timestamps while being uploaded to ensure the legality and non-tamperability of the data. In case of infringement, relevant data of the preserved works can be easily extracted from the platform and used as effective evidence for submitting for judicial rights protection. The works can be kept confidential or publicized freely according to users' needs.

1.3 Trademark and trade name certification
It refers to the fact that the trademark and trade name to be applied for registration can be uploaded to the platform through the Maker-IP platform, and the platform can be used to certify them, confirm the time when the owner uses the unregistered trademark and trade name and solidify and preserve the fact that the owner uses the trademark before the trademark is approved for registration. In case of infringement, relevant data of the preserved trademarks and trade names can be easily extracted from the platform and used as effective evidence for submitting for judicial rights protection. Trademarks and trade name certification materials can be kept confidential or publicized freely according to users' needs.

1.4 Origin certification
It refers to uploading a series of images or other types of data related to the origin of a commodity through the Maker-IP platform. The platform authenticates the data and provides a data preservation certificate to indicate that the commodity originates from a specific location. In case of infringement or challenging, the preserved information on origin can be easily extracted from the platform and used as effective evidence for submitting for judicial rights protection. Relevant information of origin can be kept confidential or publicized freely according to users' needs.

1.5 Traditional knowledge certification
It means that the applicant voluntarily applies for the certification of the rights holder of traditional knowledge and folk literature and art works through the Maker-IP platform. After the platform certification, the traditional knowledge owned by the applicant can be qualified to be included in the traditional knowledge gene pool, so as to ensure the realization and transformation of its relevant rights and obtain the necessary personal rights and property rights such as benefit sharing. Information related to traditional knowledge certification can be kept confidential or publicized freely according to users' needs.

However, as a tradeable property, IP not only requires functions such as original certification, electronic deposit and verification, but also transactions, which requires that it should be able to trace and verify the whole process of all transactions. The credibility, legitimacy and privacy of all parties in all transactions also need to be verified and protected. Furthermore, for some IP works, which require verification and certification for raw material sources and the processes of design and production, such as traditional craft

works designed and manufactured by national intangible cultural heritage inheritors based on traditional techniques and work process. We also need to use some technologies to ensure that it is authentic when they are designed, manufactured and produced. According to our previous research works (Lin *et al.*, 2017), the combination of blockchain and IoT technology can be very helpful to these requirements. The blockchain technology provides a system-level trusted mechanism to the business scenario that each party involved in transactions cannot be trusted by others. This mechanism can ensure that transactions are not denied, tampered and forged. The IoT technology can replace manual operations during the process of inspection or verification by using automated devices as much as possible, reducing artificial unintentional or intentional tampered or false inspection data, to accurately identify originals and cottage goods.

The rest of this paper will first review the state of art on the blockchain and IoT-related research and application for IP protection, and then propose our framework design for using the blockchain and IoT technologies to enhance the protection of IP. At the end, we will discuss the feasibility and application prospects of the framework.

2. Related work
There are many research papers that discussed the blockchain applications in IP-related areas and the combination application of blockchain and IoT technologies. This section will review those papers, as well as two comprehensive survey papers on blockchain applications.

2.1 Blockchain applications in intellectual property-related areas
In 2017, Wei-Tek Tsai *et al.* proposed a blockchain-based model and framework for microfilms' IP protection in China, especially for microfilms' scripts and names. Both names and scripts can be used to distinguish one from other microfilms, and they can be stored in blockchains and databases. In their model, for protecting microfilms' scripts (such as story synopsis, outline, scene-by-scene description, etc.), a lightweight binary watermark is used (Wei-Tek Tsai *et al.*, 2017).

In 2017, Savelyev and Alexander Ivanovitch discussed various legal-related aspects of applying blockchain technologies in the copyright sphere. Specifically, they reviewed the existing challenges for distribution of copyrighted works in the digital environment, possible solutions with using the blockchain technology, and associated issues need to be addressed in this regard. They thought that when using blockchain technology, much work needs to be done on the legal side: special provisions aimed at facilitating user's trust in blockchain records and their good faith usage of copyrighted works based on them need to be introduced and transactions with cryptocurrencies have to be legalized as well as the status of smart contracts and their legal consequences. Finally, the economics of blockchain copyright management systems need to be carefully considered to ensure that they will have necessary network effects (Savelyev and Ivanovitch, 2017).

In 2017 and 2018, Martin Holland *et al.* discussed the use of blockchain technology and digital rights management as a key technology for the successful transition to additive manufacturing methods and a key for its commercial implementation and the prevention of IP theft for three-dimensional (3D) print supply chain. They proposed the project of secure additive manufacturing platform (SAMPL), which develops secure chains of trust for additive manufacturing procedures. The entire process is seen – from development of digital 3D printing data via the exchange with a service provider of 3D printers trusted by specific secure elements up to labeling of printed components by means of adio-frequency identification chips. In addition to the available encoding mechanisms, a digital license

management based on blockchain technology was integrated into the data exchange solution OpenDXM GlobalX of PROSTEP AG (Martin Holland *et al.*, 2017, 2018).

Through a systematic literature review on blockchain-based applications that across multiple domains.Fran Casino *et al.* stated that blockchain integrity verification applications store information and transactions related to the creation and lifetime of products or services. The possible applications include provenance, counterfeit and IP management. An integrity verification subset of blockchain applications are those oriented to IP protection (Fran Casino *et al.*, 2019). As stated in Swan's book (M. Swan, 2015), the term digital art refers to IP very generally, not just online artworks. So, blockchain technologies can be considered to cover all such scenarios. They also stated that the accountability, automation and safety that blockchain offers for handling public records could eventually obstruct corruption and make government services such as IP service more efficient.

In 2018, Gonenc Gurkaynak *et al.* proposed blockchain-based solutions to foster the operation of IP offices, reinforce customs procedures in detecting counterfeit products and enhance the efficiency of IP rights management by the right holders. They also gave some suggestions to pave the way for the advancement of blockchain technology and to increase the number of people that this technology affects, as well as its successful integration into the various services and registration/transaction channels in IP management (Gonenc Gurkaynak *et al.*, 2018).

Alexander Schönhals *et al.* proposed a blockchain-based approach that makes it possible to protect developed ideas and early concepts for product design and development. To guarantee both proof-of-existence and proof-of-origin, a unique hash is generated from each digital artifact stored and embedded into the bitcoin blockchain by the OriginStamp decentralized trusted timestamping service. Once this unique fingerprint is embedded in a transaction in the underlying blockchain network, it can be proven where particular contributions originated because of the characteristics of the blockchain architecture (Alexander Schönhals *et al.*, 2018).

In 2018, Martin Zeilinger explored the use of blockchain technologies in attempts to create proprietary digital art markets. They thought that the combination of blockchain-based protocols with established ambitions of IP policy yields hybrid conceptual-computational financial technologies (such as self-enforcing smart contracts attached to digital artifacts) that are unlikely to empower artists but which serve to financialize digital creative practices as a whole, curtailing the critical potential of the digital as an inherently dynamic and potentially uncommodifiable mode of production and artistic expression (Martin Zeilinger, 2018).

2.2 Blockchain and internet of things combined applications

In 2016, Steve Huckle *et al.* explored how the Internet of Things and blockchain technology can benefit shared economy applications. They discussed how to combine the internet of things and blockchains to create secure shared economy distributed applications and presented some examples of such distributed applications in the context of an internet of things architecture using blockchain technology, such as Airbnb and Uber, which are well-known shared economy applications. The focus of their research is understanding how blockchain can be exploited to create decentralized, shared economy applications that allow people to monetize, securely, their things to create more wealth (Steve Huckle *et al.*, 2016).

In 2017, Lin *et al.* proposed a blockchain built-in solution for LoRaWAN network servers to build an open, trusted, decentralized and tamper-proof system, which provides the indisputable mechanism to verify that the data of a transaction has existed at a specific time in the network. They think it is the first work that integrates blockchain technology and

LoRaWAN IoT technology and uses advantages of both blockchain and IoT technologies (Lin *et al.*, 2017).

To apply the combined technology to the food safety issues, Lin *et al.* proposed a trusted, self-organized, open and ecological food traceability system based on blockchain and internet of things (IoT) technologies in 2018, which involves all parties of a smart agriculture ecosystem, even if they may not trust each other. They use IoT devices to replace manual recording and verification as many as possible, which can reduce the human intervention to the system effectively. By combining the blockchain and IoT technologies, they can provide a trusted food traceability system that can track and monitor the whole lifespan of food production, including the processes of food raw material cultivation/breeding, processing, transporting, warehousing, selling, etc. (Lin *et al.*, 2018).

In 2018, Ana Reyna *et al.* focused on the relationship between blockchain and IoT. They investigated challenges in blockchain IoT applications and surveyed the most relevant work to analyze how blockchain could potentially improve the IoT (Ana Reyna *et al.*, 2018).

In 2019, Merlinda Andoni *et al.* focused on blockchain and IoT solutions for the energy industry and informed the state of the art by thoroughly reviewing the literature and current business cases. After reviewing 140 blockchain research projects and startups, they constructed a map of the potential and relevance of blockchains for energy applications and provided a systematic review of blockchain activities and initiatives in the energy sector (Merlinda Andoni *et al.*, 2019).

2.3 Comprehensive survey on blockchain applications
In 2018, Archana Joshi *et al.* tried to conduct a comprehensive survey on the blockchain technology by discussing its structure to different consensus algorithms as well as the challenges and opportunities from the prospective of security and privacy of data in blockchains. They thought that the spectrum of blockchain applications range from financial, healthcare, automobile, risk management, IoT to public and more social services (Archana Joshi *et al.*, 2018).

In 2018, Phan The Duy *et al.* conducted a comprehensive survey on the blockchain technology adoption by studying blockchain's influences, opportunities and challenges when using it in the real-world scenarios. They thought that in the "Industry 4.0" era, blockchain technology has been an unmissable trend for both academy and industry recently, which has become famous as the innovative technology that underlies cryptocurrencies such as Bitcoin and Ethereum systems. It also has been spreading with multiple industries exploring their capabilities and new blockchain use cases springing up on a daily basis. Its emergence has brought a great deal of impact on how the information will be stored and processed securely (Phan The Duy *et al.*, 2018).

3. Proposed method
In this section, we present our research approach and the architecture design in our system.

3.1 Blockchain and internet of things-enhanced intellectual property protection system
The above research works show that the combination of IoT and blockchain technologies can be applied to IP protection, but most of them are *ad hoc* solutions for one function or some specific aspects. Based on the Maker-IP platform and our

previous trusted trade blockchain network cloud platform (TTBNCP) (Lin *et al.*, 2017, 2018), we propose a general blockchain and IoT-based IP vprotection system, as shown in Figure 1.

Based on the Maker-IP platform, our system can process three types of IP, including:

(1) patents, copyrights, trademarks etc., which need the inventor to submit some official documentaries to the Maker-IP system, then the hashed transaction data will be sent to our blockchain regional node or full node. The regional node only runs partial functionaries of full node for specific type of transaction data or business;

(2) industrial design, trade dress, craft works, trade secrets, etc., which normally need a notary to record the working process of designers or workers using videos or photos. Those data also need submit to the Maker-IP system and then send the hashed value to some blockchain nodes. To avoid manual intervention as much as possible, some IoT devices with edge computing function will be deployed to record some working data during the process, for example, the raw material inspection data;

(3) Plant variety rights, geographical indications etc., which normally need some IoT devices to send location or IoT data to Maker-IP system as evidence. Then, our system will collect those evidences to build a chain of evidence in the blockchain database. For Types 2 and 3 IP productions, sometimes, they need to be transported during the trading process; IoT devices that have been deployed in the logistics system can collect the location and transportation environment data, then the hashed transaction data will be sent to blockchain node server via IoT gateway. As for the trade customer and online trading platform, all related transaction behavior data will be sent to a blockchain node to add into the chain. Finally, sometimes, a court or judicial appraisal agency
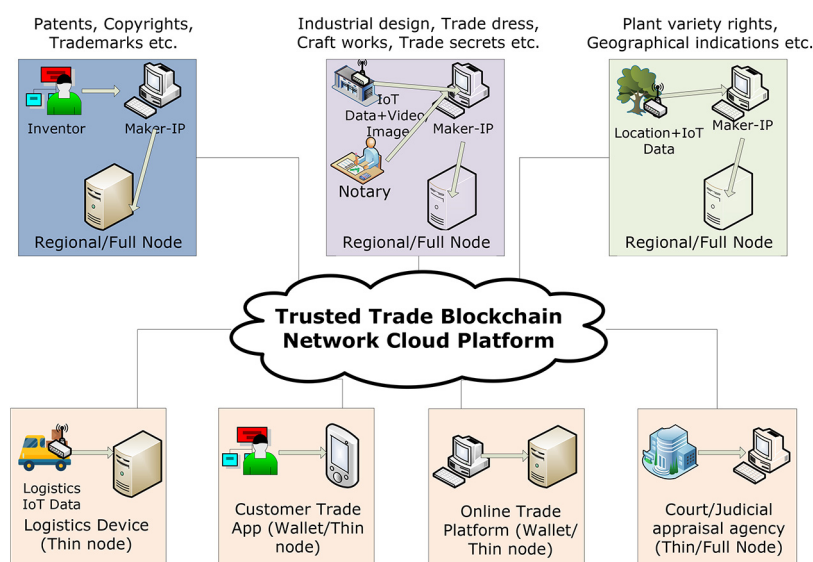

Figure 1.
Blockchain and IoT-based IP protection system

can require a chain of evidence from any of full node or the specific related regional node of the blockchain network. The core of the whole architecture is our virtual TTBNCP.

3.2 Blockchain system architecture
The virtual TTBNCP consists of all nodes in the blockchain system, as shown in Figure 2, which is a peer-to-peer system. All Full-Node servers are equipped with full functionalities of blockchain, such as symmetric encryption and decryption, consensus algorithm, Merkle trees building, distributed ledger, etc.; other node, liking wallet, just includes functionalities such as simplified payment verification, storing transaction related data, etc.

3.3 Data processing flow and structure
Figure 3 shows the transaction data process flow in our blockchain system. After hashing and digital signing, all transaction data will be sent to the blockchain network via the IoT gateway with edge computing function; further, they will be verified, added into transaction pool and stored into the blockchain.

IP trading customers can use their computers or mobile app to retrieve all related transaction data and verify them. For example, one buys a craft from online trade market, and then he/she can use the app to retrieve the authors, producing process, raw material, logistics data, etc. All that information can be verified by the blockchain system without human intervention. Figure 4 shows a typical sample of the blockchain data structure.

Our design follows existing popular and standard blockchain head data structure. In the list of transactions, each transaction includes sender's unique identity address, sender's public key, hash value of original craft data, process data or trade data, uniform resource locator of original data, sender's digital signature, sent timestamp, receiver's unique identity address, received timestamp, etc.
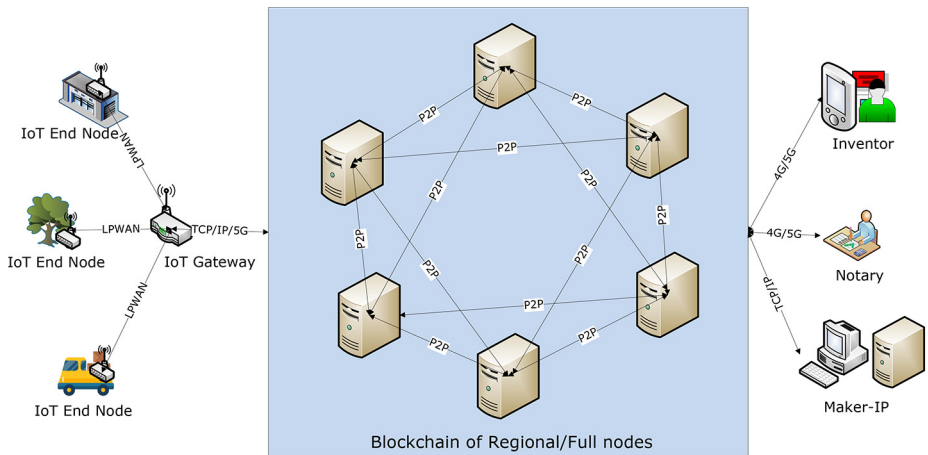

Figure 2.
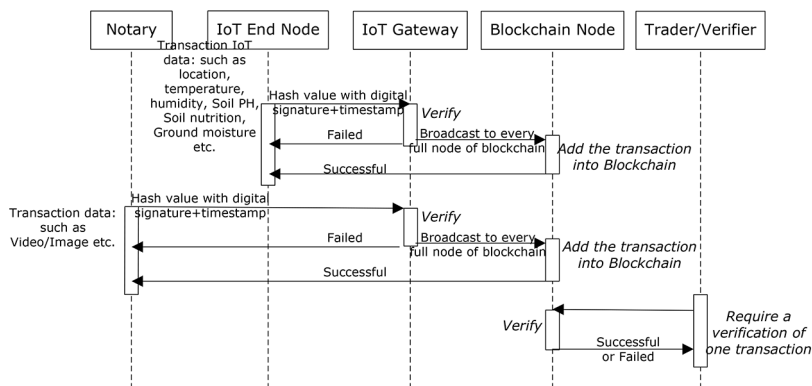Blockchain system architecture

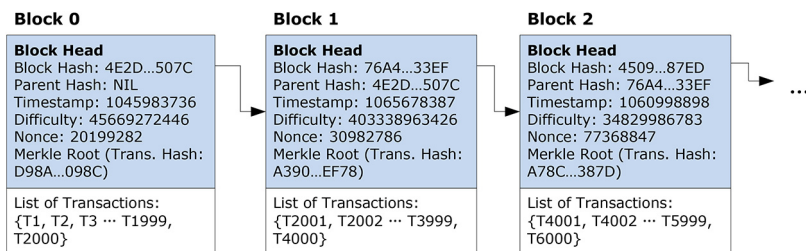Figure 3.
Transaction data
process flow

Figure 4.
Blockchain data
sample

4. Conclusion

Blockchain and IoT technologies can help us to build a trusted, self-organized, open and ecological IP protection system, which can involve all different parties in the IP protection and trade procedures, and even they may not trust each other.

During the design of our proposed architecture, the main challenges we are facing include:

- How to build the links between things in the physical world and data in the digital world? Our application of IoT technology is just a very preliminary trial to solve this problem, with more practical data coming into the system, more efficient method will be explored.

- How to find a low-cost and fast consensus mechanism in distributed network environment? We will try to explore this mechanism for a private chain or small alliance chain in future research.

- How to apply smart contract technology on the trade of IP products? Further, we will explore this direction in our research work.

To the best of our knowledge, this is the first work that applying blockchain and IoT technologies on traditional IP protection and trade ecosystem. Our proposed method uses IoT technology and blockchain ledger instead of manual recording and verification, which can reduce human intervention as more as possible.

References

Andoni, M., V., Robu, David Flynn, S., Abram, D., Geach, D., Jenkins, P., McCallum, A. and Peacock, (2019), "Blockchain technology in the energy sector: a systematic review of challenges and opportunities", *Renewable and Sustainable Energy Reviews*, Vol. 100, pp. 143-174, doi: 10.1016/j. rser.2018.10.014.

Casino, F., Dasaklis, T.K. and Patsakis, C. (2019), "A systematic literature review of blockchain-based applications: Current status, classification and open issues", *Telematics and Informatics*, Vol. 36, pp. 55-81, doi: 10.1016/j.tele.2018.11.006, ISSN 0736-5853.

Duy, P.T., Hien, D.T.T., Hien, D.H. and Pham, V.H. (2018), "A survey on opportunities and challenges of blockchain technology adoption for revolutionary innovation", *Proceedings of the Ninth International Symposium on Information and Communication Technology (SoICT 2018). ACM, New York, NY*, pp. 200-207, doi: 10.1145/3287921.3287978.

Gurkaynak, G., Yılmaz, İ., Yeşilaltay, B. and Bengi, B. (2018), "Intellectual property law and practice in the blockchain realm", *Computer Law and Security Review*, Vol. 34 No. 4, pp. 847-862, doi: 10.1016/j.clsr.2018.05.027.

Holland, M., Nigischer, C. and Stjepandić, J. (2017), "Copyright protection in additive manufacturing with blockchain approach", *Transdisciplinary Engineering: A Paradigm Shift*, Vol 5, IOS Press, pp. 914-921, 10.3233/978-1-61499-779-5-914.

Holland, M., Stjepandić, J., (2018), and C. and Nigischer, "Intellectual property protection of 3D print supply chain with blockchain technology", *Proceedings of 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), IEEE, Stuttgart*, 10.1109/ice.2018.8436315.

Huckle, S., Bhattacharya, R., White, M. and Beloff, N. (2016), "Internet of things, blockchain and shared economy applications", *Procedia Computer Science*, Vol. 98, pp. 461-466, doi: 10.1016/j.procs.2016.09.074.

Joshi, A., Han, M. and Wang, Y. (2018), "A survey on security and privacy issues of blockchain technology", *Mathematical Foundations of Computing*, Vol. 1 No. 2, pp. 121-147, doi: 10.3934/mfc.2018007.

Lin, J., Shen, Z., (2017), and C. and Miao, "Using blockchain technology to build trust in sharing LoRaWAN IoT", *Proceeding of the 2nd International Conference on Crowd Science and Engineering (ICCSE'17), ACM, New York, NY*, pp. 38-43, doi: 10.1145/3126973.3126980.

Lin, J., Shen, Z., Miao, C. and Liu, S. (2017), "Using blockchain to build trusted lorawan sharing server. 2017", *International Journal of Crowd Science*, Vol. 1 No. 3, pp. 270-280, doi: 10.1108/IJCS-08-2017-0010.

Lin, J., Shen, Z., Zhang, A., (2018), and Y. and Chai, "Blockchain and IoT based food traceability for smart agriculture", *Proceedings of the 3rd International Conference on Crowd Science and Engineering (ICCSE'18). ACM, New York, NY*, Article 3, pp. 1-6, doi: 10.1145/3265689.3265692.

Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M. (2018), "On blockchain and its integration with IoT. Challenges and opportunities", *Future Generation Computer Systems*, Vol. 88, pp. 173-190, doi: 10.1016/j.future.2018.05.046.

Savelyev, A. and Ivanovitch, (2017), "Copyright in the blockchain era: promises and challenges (November 21, 2017)", Higher School of Economics Research Paper. No. WP BRP 77/LAW/2017, available at SSRN: https://ssrn.com/abstract=3075246, doi: 10.2139/ssrn.3075246.

Schönhals, A., Hepp, T., (2018), and B. and Gipp, "Design thinking using the blockchain: enable traceability of intellectual property in problem-solving processes for open innovation", *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock'18). ACM, New York, NY*, pp. 105-110, doi: 10.1145/3211933.3211952

Swan, M. (2015), *Blockchain Blueprint for a New Economy*, O'Reilly Media.

Tsai, W.-T., Feng, L., Zhang, H., You, Y., Wang, L., and Y. and Zhong, (2017), "Intellectual-property
blockchain-based protection model for microfilms", *Proceedings of 2017 IEEE Symposium on
Service-Oriented System Engineering (SOSE)*, IEEE, San Francisco, CA, April 6-9, doi: 10.1109/
SOSE.2017.35.

Zeilinger, M. (2018), "Digital art as `monetised graphics': enforcing intellectual property on the
blockchain", *Philosophy and Technology*, Vol. 31 No. 1, pp. 15-41, doi: 10.1007/s13347-016-0243-1.

Corresponding author
Jun Lin can be contacted at: junlin@ntu.edu.sg

293