IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 26, 2021, accepted March 13, 2021, date of publication March 17, 2021, date of current version March 26, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3066573

Developmental Trajectories in Blockchain Technology Using Patent-Based Knowledge Network Analysis

SOHEE KIM[1], SEJUN YOON[1], NAGARAJAN RAGHAVAN[2], (Member, IEEE), NGUYEN-TRUONG LE[3], AND HYUNSEOK PARK[1]

[1]Department of Information Systems, Hanyang University, Seoul 04763, South Korea
[2]Engineering Product Development Pillar, Singapore University of Technology and Design, Singapore 487372
[3]Fraunhofer Institute for Industrial Engineering (IAO), 70569 Stuttgart, Germany

Corresponding author: Hyunseok Park (hp@hanyang.ac.kr)

This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (No. 2019S1A5A8036427).

ABSTRACT The blockchain is a technology with high growth potential that increases social benefits by streamlining procedures, reducing costs, and innovating the way we work. Considering the growth potential of blockchain technologies, countries around the world are attempting to graft into various fields such as finance, logistics, and healthcare, and actively promoting technology development. Tracing and analyzing the developmental trajectories of blockchain technology can give great insight for R&D direction and strategies. We developed an improved knowledge persistence-based main path approach to identify technological trajectories of the blockchain technology. In addition, future technological directions for each sub-technology under blockchain technology were identified by the knowledge unconventionality metric. The results show that the blockchain technology can be divided into five sub-technologies, and each sub-technology has evolved with high technological interactions among other sub-technologies. Based on the last knowledge streams of the main paths, this paper suggests potential future directions for each sub-technology in the blockchain technology.

INDEX TERMS Blockchain, hashchain, distributed ledger, technological trends, knowledge persistence, patent citation network, knowledge unconventionality, main path analysis.

I. INTRODUCTION

The blockchain is a technology with high growth potential that increases social benefits by streamlining procedures, reducing costs, and innovating the way we work. Considering the growth potential of these blockchain technologies, countries around the world are attempting to graft into various fields such as finance, logistics, and healthcare, and actively promoting technology development. The blockchain ensures the contract without trusted third party of the middle. It is mainly used for authentication of cryptocurrency transactions such as Bitcoin and Ethereum. The blockchain has also been widely used in the fields of finance, medical treatment, contents, public service, logistics/distribution, energy, etc. Since the blockchain technology is one of the most significant technologies for future digital economies, analyzing R&D trends of blockchain can help researchers and R&D planners better understand the evolving characteristics of blockchain and it will give insight for development of R&D direction and strategies. The aim of this paper is to quantitatively analyze trace developmental trajectories of blockchain technology using reliable data. We used a patent database and analyzed a patent citation network. Patents are one of the most reliable sources for technological knowledge [1]–[3] and have been widely used for identification of recent trends of high technologies discovery of new technology opportunity and development of technology roadmaps and plans [4]–[20]. Since patent citations represent knowledge flows or inheritance between the cited patent and the citing patent, a patent citation network was constructed to visualize all knowledge flows within the blockchain technology. To identify main knowledge streams in the patent citation

The associate editor coordinating the review of this manuscript and approving it for publication was Justin Zhang.

network, this paper employed knowledge persistence (KP) based main path analysis, suggested by Park and Magee [5]. Even though KP-based main paths resolved the limitations of a conventional search path-based main path analysis, such as single path problem and omission of key patents, it still needs to be improved for future-oriented analysis. The KP-based main path approach basically connects patents having high knowledge persistence. However, knowledge persistence values of all patents on the last layer are zero, and so the last knowledge flows are usually diverged to a number of patents in the main paths. This characteristic makes it difficult to find future technological directions. In particular, IT related technologies usually have more patent citations than other technological domains and so knowledge flow divergence issue can be critical drawback for this research. To overcome the limitation, this paper developed an improved KP-based main path analysis by adopting the radicalness metric to identify potential directions of the blockchain technology. The major contribution of this paper is to significantly reduce the network complexity in the last layer of the KP-based main paths. To this end, we developed the knowledge unconventionality (KU) metric to weight the last knowledge flows. From the main path analysis, we found that the blockchain technology can be divided into five sub-technologies, such as Cryptography, Hardware blockchain, Decentralized applications, Exchanges, and Digital transaction, and each of sub-technologies has high interrelations to other sub-technologies. Based on the last knowledge streams of the main paths, this paper suggests potential future directions for each sub-technology in the blockchain technology. The rest of this paper is structured as follows. The section 2 reviews backgrounds for this research. The section 3 describes the method, the section 4 presents the trends of blockchain technology, and finally discussion and conclusion are drawn in the section 5.

II. BACKGROUND

A. BLOCKCHAIN TECHNOLOGY

1) CONCEPT OF BLOCKCHAIN

Blockchain refers to a technology that enables network participants to jointly verify transaction information, create and record and store blocks based on a hash, to ensure integrity and reliability without an authorized third party, thereby enabling distributed ledger [21], [22]. Distributed ledger technology refers to processes and related technologies that enable network nodes to safely propose, verify, and record state changes using a decentralized consensus mechanism for distributed and synchronized ledgers. The blockchain is a hash-based block processing, and distributed ledger technology has a broader meaning of using a consensus mechanism, but international standardization organizations use a mixture of blockchain and distributed ledger technology [23]. Therefore, in this paper, the name blockchain is used in a comprehensive sense including makeup ledger technology. Blockchain refers to a technology that creates blocks containing information at regular intervals and then connects them to previous blocks like a chain. A block is a unit that stores transaction information, and each block records the hash value of the previous block and is connected in sequence, so it is impossible to forgery or alter the past block. Starting from the first block, consensus blocks that have been verified as correct by multiple participants are sequentially added. When a block is created, it is transmitted to all participants and stored in a distributed manner, so all participants in the blockchain share transaction records.

2) TREND OF BLOCKCHAIN

Recently, as interest in cryptocurrencies such as Bitcoin has increased, it has been shown that the patent application related to blockchain, which is the technological base, is also explosively increasing worldwide [22]. The basic concept of blockchain is a free technology that is open source and has no patent. Therefore, patent applications are mainly made around peripheral technologies such as security, operation, and utilization. In particular, as the scope of use of blockchain from cryptocurrency to logistics, medical care, and public services gradually expands, patent applications are also expected to increase mainly in the field of use. Most of the blockchain patent applications are led by companies, and the US is actively applying for patents by financial companies such as banks. The various application fields of blockchain technology are described in Table 1 [24], [25].

3) TYPES OF BLOCKCHAIN

Blockchain is an important tool that enables important decentralized applications without centralized trust and is divided into public blockchain, private blockchain, and hybrid blockchain according to the nature of network participants and the role of the subject [26]–[28]. A public blockchain is such kind of blockchain where anyone from anywhere can join the network and reserves equal rights to view, download and add nodes for everyone. And so, you can join the blockchain network anytime and you will have complete and equal authority just like others. It is a 'Public' network in a true sense. Public blockchain have been used to enable many different cryptocurrencies. Existing public blockchain and smart contracts deployed on them may disclose sensitive information. Although there is some ongoing work that leverage advanced cryptography to address some of these sensitive information leakage issues, they require significant changes to existing and popular blockchain such as Ethereum and are usually computationally expensive. Private blockchain is developed and maintained by a private organization who has the authority over the mining process and consensus algorithm. The private organization decides who can join the network and have the access download the nodes. Private blockchain have been proposed to allow more efficient and privacy-preserving data sharing among pre-approved group of nodes/participants. Although private blockchain address some of the privacy challenges by allowing sensitive data to be only seen by the select group of

TABLE 1. Field of blockchain technology.

Field	Content
Finance	Stock trading, insurance contract, loss insurance claims, payment, deposits and loans, asset management, Credit rating, Investor recruitment, Cloud funding, etc.
Healthcare	Medical record management, personal medical information management, genome information sharing, etc.
Entertainment	Music database without intermediate distribution process, Track and prove artist ownership, Smart content creation and license transaction, Digital sound distribution, photo copyright management, etc.
Online voting	Prevent fraudulent voting, Voting verification solution, etc.
Military	Military secret transmission and reception, Gun Tracking, Legal evidence management, etc.
Public Service	Security and tracking management of government records, Electronic certificate distribution, postal service, land register management, Wills and Legacy, Donation tracking, etc.
Logistics/Distribution	Personal clearance, Shipping logistics, Delivery system, international trade system, supply chain management, etc.
Manufacturing	Product history management, facility efficiency improvement, consumer marketing strategy, etc.
Education	Student register security, Student register sharing, Open infrastructure related to academic proof, etc.
Social/Culture	Art industry, sport entertainment, car lease, car sharing, real estate transaction, gift certificates and gift cards, Reward exchange between brands, etc.
Energy	Direct energy trading without the power market, Power transactions between neighbors, charging electric vehicles, etc.

TABLE 2. Characteristics of blockchain type.

Element	Public	Private	Hybrid
Management Entity	All trading participants (decentralized)	Central agency	Participants in the consortium
Governance	Very difficult to change the rules once set.	Easily change the law according to the decision of the central agency.	The rules can be changed relatively easily according to the consortium of the consortium participants.
Transaction Speed	Network expansion is difficult and transaction speed is slow.	Network expansion is easy and transaction speed is fast.	Network expansion is easy and transaction speed is fast.
Data access	Anyone can access	Only authorized users can access.	Only authorized users can access.
Discrimination	Anonymity	Identifiable	Identifiable
Proof of Transaction	The proof of transaction is determined according to the verification algorithm, and it is not known in advance who the proof of the transaction is.	Transaction verification by a central agency.	The proof of transaction is in a known state through authentication, and transaction verification and block generation are performed according to pre-agreed rules.

participants, they do not allow public accountability of transactions since transactions are approved by known set of users and cannot be accessed publicly. Hybrid blockchain is defined as the blockchain that attempts to use the best part of both private and public blockchain solutions. The hybrid blockchain is distinguishable from the fact that they are not open to everyone, but still offers blockchain features such as integrity, transparency, and security. As usual, Hybrid blockchain is entirely customizable. The members of the hybrid blockchain can decide who can take participation in the blockchain or which transactions are made public. This brings the best of both worlds and ensures that a company can work with their stakeholders in the best possible way. The characteristics of blockchain type are described in Table 2.

4) BLOCKCHAIN RELATED TECHNOLOGY

Blockchain technologies include cryptographic mechanism, transaction verification, usage controlling, data integrity, peer-to-peer (P2P) computing, cloud computing, and so on [21]. First, cryptographic mechanism is a technique associated with the process of converting ordinary plain text into unintelligible text and vice-versa. Blockchain uses cryptography to protect the user identities in a network, to ensure secured transactions, and to protect all sorts of valuable information. Different blockchains use different cryptography algorithms. The modes of operation of block ciphers are configuration methods that allow those ciphers to work with large data streams, without the risk of compromising the provided security. These modifications are called the block cipher modes of operations, e.g. cipher block chaining (CBC), electronic codebook (ECB) or Galois/counter mode (GCM). Second, transaction verification is a technique for authorization. A transaction is a new record of exchange of some value or data between two public addresses of the blockchain. Transactions can happen in new node and take time to get verified when a new block is created containing that transactions. Validated transactions are stored into a block and are dealt with a lock (hash). This block becomes part of the blockchain when other computers in the network validate if the lock on the block is correct. This transaction is now part of the blockchain and cannot be altered in any way. Activating many cards, including financial cards, such as credit cards and other payment cards, may be used as a tool to verify transactions, but those are susceptible to attack and vulnerable to hacking or other unauthorized access. Accordingly, there exist needs to provide users with an appropriate solution that overcomes these deficiencies to provide verification for contactless cards. Third, usage controlling technique is a simple but powerful idea enables various policy specifications and thus extends the expressiveness of access control systems immensely. Usage control must not be limited to granting access to right only once; instead, it should constantly keep track of the usage of objects and decide continuously whether to allow a subject access to objects or not. If a subject exceeds the allowed quota or if another constraint is violated during the use of an object, the subject's right should be revoked. It also allows for the specification of constraints, such as allowed usage time per session and the revocation of usage after a specified limit. Usage controlling is techniques for restricting cryptographic keys to pre-authorized uses, different access levels, validity of crypto-period, different key- or password length, or different strong and weak cryptographic algorithms. The problem in the prior art of public key crypto systems is in the distribution of public keys from a sender to one or more receivers. Therefore, the improved methods for distributing public keys in public key cryptosystems have been developed. Fourth, data integrity is a technique of the maintenance/assurance of the accuracy and consistency of data over its entire lifecycle, and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data. Blockchain just might be the solution to improve data integrity to the highest standards. By design, blockchains are inherently resistant to the modification of data. Blockchain ledgers are immutable meaning that if data addition or transaction has been made, it cannot be edited or deleted. Data integrity is used to describe the degree to which a data unit received by a receiver, can be relied upon as being identical to a data unit sent by the sender, to whom the received data unit is attributed. In electronic data handling systems, such as computers and other data storage and communication systems, it is often necessary to prevent disclosure of sensitive data to unauthorized persons and to determine whether such data has been tampered with or not. So it is required to have a fast, simple and economical system for protecting data in an electronic data handling system and for authenticating. Fifth, peer-to-peer (P2P) computing is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes. Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts. Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model in which the consumption and supply of resources is divided. Secure communication is a technique based on the P2P network architecture and inherits the decentralized characteristics. A peer-to-peer (P2P) network consists of a group of devices that collectively store and share files. Each participant acts as an individual peer. Today, P2P networks are at the core of most cryptocurrencies, making up a great portion of the blockchain industry. With the increased utilization of distributed data processing systems to share and communicate sensitive and confidential information, the computing and relating industries are paying significantly increased attention to improving and refining known techniques for securing data which is communicated over insecure communication channels such as telephone lines and electromagnetic-based communication systems. The term cloud theoretically signifies abstraction of technology, resources and locations that are used in building an integrated computing infrastructure. All cloud computing models rely heavily on sharing of resources to achieve coherence and economies of scale similar to a utility over a network. Sixth, cloud computing provides services with a user's data, software and computation on over multiple networks. End users access cloud based applications through a web browser or a light weight desktop or mobile application while the rest of the application software and data are stored on servers at remote locations. Cloud computing provides a same or better service and performance with cloud software programs as if all the cloud software programs were actually installed locally on end-user devices.

5) BLOCKCHAIN STANDARDIZATION

Blockchain technology is being evaluated as a driving force to change the financial and ICT paradigm, and is diversifying applications in digital cryptocurrency, smart contracts, distribution, digital content copyright, and health care. The technology classification for global distributed ledger service is classified as the core infrastructure technology of blockchain, platform and interlocking technology that provides services using it, application technology that implements services on various platforms, and security and management technology that manages and controls the blockchain system. The contents of international standardization activities related to blockchain technology are shown in Appendix A.

B. KNOWLEDGE PERSISTENCE-BASED MAIN PATH ANALYSIS

Main path analysis was developed to identify and visualize the major knowledge streams in a technology domain by reducing network complexity [5], [17] and so many innovation studies adopted this tool to trace developmental trajectories. To construct knowledge flows occurred within a specific technological domain, patent data has been widely utilized. Since patent citation can denote knowledge flow from the citing patent to the cited patent, patent citation network can be used as a global knowledge network. Most previous studies using main path analysis are based on a search path, e.g. SPLC (search path link count), SPNP (search path node pair), and NPPC (node pair projection count), suggested by Hummon and Doreian [29]. The basic logic behind these indices is that a link (and node) included in many search paths in a citation network plays a critical role in the knowledge diffusion, so a sequence of high-weighted links (or nodes) constructs a main path [17]. The major limitations of search-path based main path analysis are as follows. First, most of them identify only one single main path. However, it is generally difficult to be accepted single path for technological trajectories. Second, they cannot show combinatorial relationships between sub-fields in technological domain. Third, traversal counts based search path from the starting nodes has high possibility to omit important

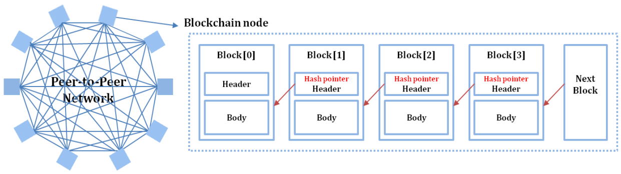


FIGURE 1. **Blockchain Network.**

patents and knowledge flows [5]. Recent research in complex networks has greatly improved the understanding in structure and complexity of knowledge network and introduced KP-based main path analysis [5], [13], [14]. KP is a metric to measure how much knowledge in a patent is inherited to the recent developments in a knowledge network [30], [31] and so KP can quantify patent's technological value from the global citation perspective. The KP-based main path analysis overcomes the previous limitations by identifying the dominant knowledge flows first and then linking them based on the backward/forward search. This approach can generate multiple main paths and dramatically reduce network complexity without missing any dominantly important patents. Park and Magee [5] empirically showed that KP-based main path approach can generate 10 times smaller but include about 20% more of critical knowledge flows than a search path-based approach. However, KP-based main paths sometimes generate many diffused knowledge flows in the last layer and it can make difficult to analyze and forecast the further development in the given technological domain. Therefore, this paper resolves this problem by adopting new metric to minimize the diffusion in the last layer.

III. METHOD

A. CONSTRUCTION OF CITATION-BASED KNOWLEDGE NETWORK

The knowledge network of a technological domain is generated based on patent citations with the basic assumption being that a patent citation represents a knowledge flow from cited patent to citing patent. Even though technologies are not dependent on a specific technological domain and can be used or applied to many other domains, this paper only considers knowledge flows within the technological domain, i.e. citations occurred within the technological domain, because most knowledge is inherited within the technological domain. The cited-citing patent pairs can be extracted from backward citation information.

B. IDENTIFICATION OF KNOWLEDGE PERSISTENCE-BASED MAIN PATHS

The underlying concept for knowledge persistence is that patent citation indicates knowledge inheritance from the citing patent to the cited patent and the proportion of each knowledge inheritance, i.e. weight for each knowledge flow, is different. By measuring the proportion of each knowledge inheritance, how much knowledge of a patent is persistent or impact on the recent technological developments.

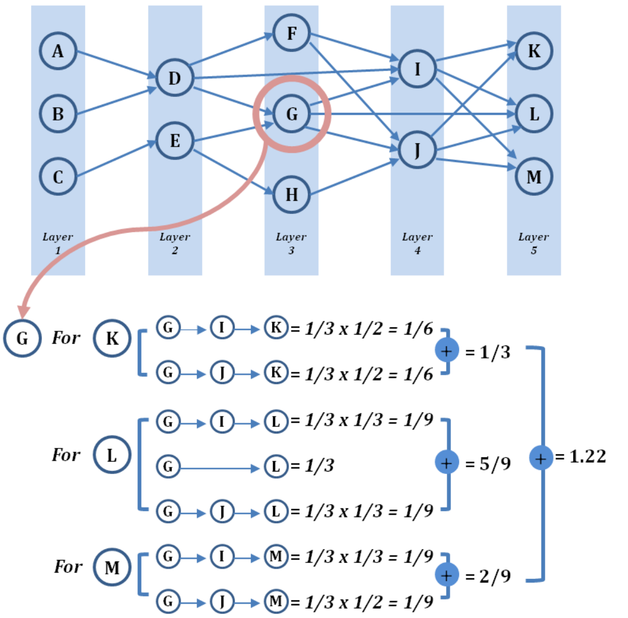

A
B
C
D
E
F
G
H
I
J
K
L
M
Layer 1
Layer 2
Layer 3
Layer 4
Layer 5
G For K
G → I → K = 1/3 x 1/2 = 1/6
G → J → K = 1/3 x 1/2 = 1/6
+ = 1/3
For L
G → I → L = 1/3 x 1/3 = 1/9
G → L = 1/3
G → J → L = 1/3 x 1/3 = 1/9
+ = 5/9
+ = 1.22
For M
G → I → M = 1/3 x 1/3 = 1/9
G → J → M = 1/3 x 1/2 = 1/9
+ = 2/9

FIGURE 2. **Knowledge persistence calculation. Note: Layer denotes the topological structure of knowledge flows in a technological domain; The number of layers in the technological domain can be calculated based on the longest sequence of citation flow from endpoints to startpoints. Once the longest knowledge flow is identified, each patent can be assigned to one of the layers. The inheritance proportion is 1/n, and n is the number of backward citations of the patent in the next layer.**

KP-based main path analysis first identifies the dominantly significant patents, i.e. high KP patents, by calculating KP of each patent in a knowledge network. The procedure for KP calculation is as follows. First, all *endpoint* patents, which do not have forward citations, and *startpoint* patents, which do not have backward citations, are identified. Second, the longest citation link between *startpoint* and *endpoint* patents is identified. This flow is recognized as the number of layers of the technological domain. Third, all patents are rearranged by layer. Fourth, KP, how much knowledge is inherited by endpoint patents in the layer-based citation network, is calculated. The inheritance proportion is 1/the number of backward citations of the patent in the next layer. Figure 2 illustrates how knowledge persistence is calculated with an example, and the formulation for KP is as follows [5]:

$$KP_A = \sum_{i=1}^{n} \sum_{j=1}^{m_i} \prod_{k=1}^{l_j - 1} \frac{1}{BWDC_{it}(P_{ijk})},$$

where P_A means the patent A, P_{ijk} is the k-th patent on the j-th backward path from P_i to P_A; $BWDC_{it}(P_{ijk})$ is the number of backward citations of P_{ijk} without considering backward citations by patents included in between the first layer and layer t-1, when P_A belongs to layer t; l_j is the number of patents on the j-th backward path from P_i to P_A; m_i is all possible backward paths from P_i to P_A; i is the number of patents in the last layer, which are indirectly connected to P_A.

The dominantly significant patents are determined by normalizing KP values from the global perspective (global persistence: GP) or local perspective (layer persistence: LP); the global persistence (GP) is calculated by dividing by the maximum KP in the given technological domain; the layer persistence (LP) is calculated by dividing by the maximum KP in the layer. As KP is one of citation-based metrics has a time-effect [8], GP generally cannot identify relatively recent patents as significant ones and so LP is essential metric to solve the time effect problem. Based on the Park and Magee [5], this paper determines high persistence patents (HPPs) whose GP $\geq$ 0.3 or LP $\geq$ 0.8 as dominantly significant patents. Then, the backward and forward searching from the identified high KP patents identifies main paths. Since the mechanism of the backward and forward searching is to select patents having the highest value of global persistence among the directly linked patents on the citation network, main paths from *starting* patents to *endpoint* patents can be identified [13].

C. FORECASTING FUTURE DIRECTIONS ON MAIN PATHS

The algorithm for KP-based main path analysis sometimes generates many knowledge flows in the last layer. This is because all nodes in the last layer are not cited by later inventions and so have no KP value. Since each of the nodes in the last layer can be potential direction for major knowledge streams, knowledge divergence toward the last layer should be minimized to focus on specific knowledge flows as future directions. To this end, this paper developed the metric based on the knowledge recombination theory [32]–[34]. Innovative inventions have high possibility to become the next knowledge streams, and innovative knowledge is usually created by atypical knowledge combinations. Therefore, the knowledge unconventionality can be high if the patent classifications of backward citation patents are different from the classifications of the focal patent. Specifically, the knowledge unconventionality (KU) metric is defined as follows:

$$KU_p = \sum_{j}^{n_p} \mathrm{DC}_j / n_p ; CPC_{p_j} \neq CPC_p,$$

where DC_j denotes the number of different classifications in patent j cited by patent p, specifically, DC_j is counted when 4-digit CPC (Cooperative Patent Classification) codes CPC_{p_j} of patent j is not allocated to patent p, and n_p is the number of patents cited by patent p on the main paths. Based on the KU value of patent in the last layer, patents having the highest KU value are remained. Figure 3 shows the network complexity of the main paths for blockchain technology before and after adopting KU metric.

IV. TRENDS OF BLOCKCHAIN TECHNOLOGY

A. DATA

We used patent database service Patsnap (www.patsnap.com) to retrieve patent data corresponding to our query. The search query for Blockchain technology and the summary of the collected data is described in Table 3.

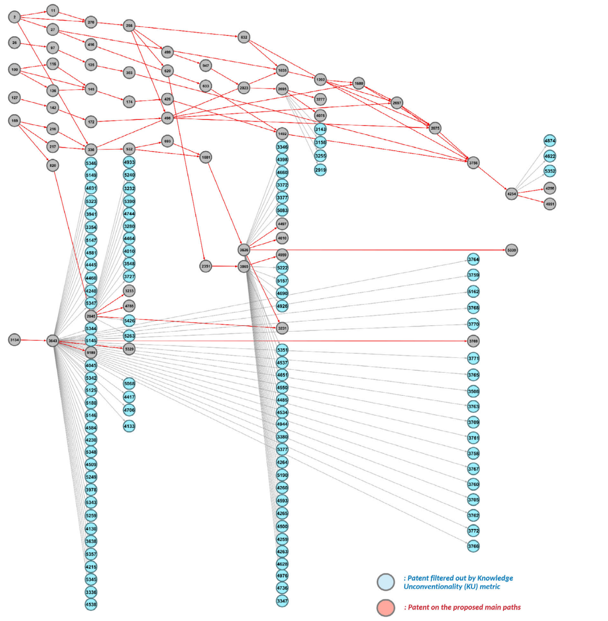

: Patent filtered out by Knowledge Unconventionality (KU) metric
: Patent on the proposed main paths

FIGURE 3. Network complexity reduction of main paths for blockchain technology by knowledge unconventionality (KU) metric.

TABLE 3. Data overview.

Data range	1 January 1976 ~ 17 June 2020
Search query	blockchain* or block-chain* or "block chain" or hashchain* or hash-chain* or "hash chain" or "distributed ledger" or distributed-ledger*
# of patents	5,437

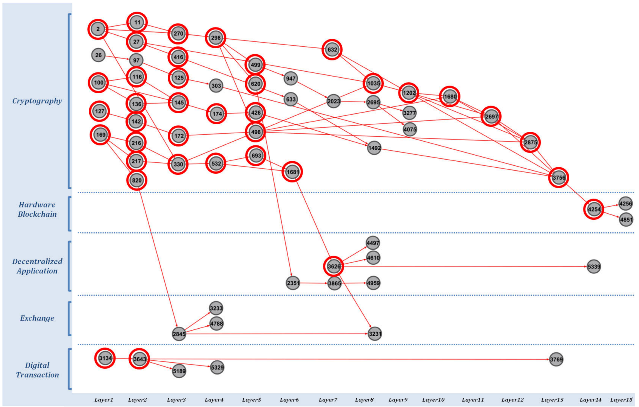


FIGURE 4. Main path network for Blockchain determined by GBFP. Note: # of nodes and links are 63 and 78; # of high persistence patents are 38; HPPs are highlighted with red circles.

B. RESULTS

The main paths of blockchain technology by the proposed method is shown in Figure 4 drawn by Gephi (www.gephi.org). We used Event graph layout plug-in to arrange patents in the layer order and each node is assigned to one of the layers. Cutoff values for HPP are $GP \geq 0.3$

or $LP \geq 0.8$. There are 63 patents on the identified main paths and 38 out of them are HPPs (see Appendix B). Blockchain-related technologies include authentication, forgery, encryption, access, agreement, and synchronization, cryptocurrency, transaction verification, and etc. By qualitatively analyzing patent documents on the main path network, we found five sub-technologies under blockchain technology, such as Cryptography, Hardware blockchain, Decentralized application, Exchange, Digital transaction, and the patents on the main paths were classified into each sub-technology. Figure 4 shows the developmental trajectories of blockchain technology. In the blockchain technology, most HPPs belong to the cryptography sub-technology and they affect to other sub-technologies. Main knowledge streams are mainly led by large companies, and future developments of blockchain technology will be focused on the hardware blockchains based on cryptography technologies.

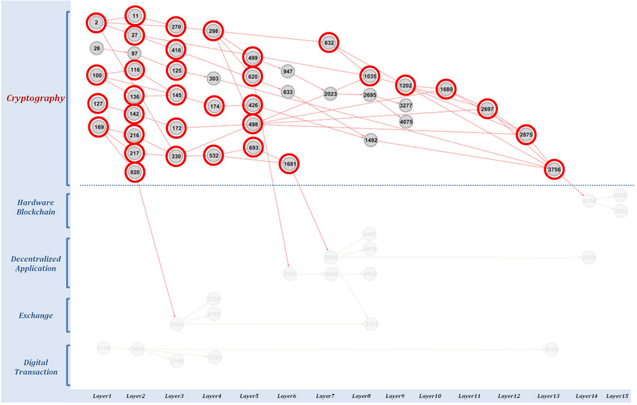


FIGURE 5. Main path network for Cryptography sub-technology. Note: HPP represents a red circle.

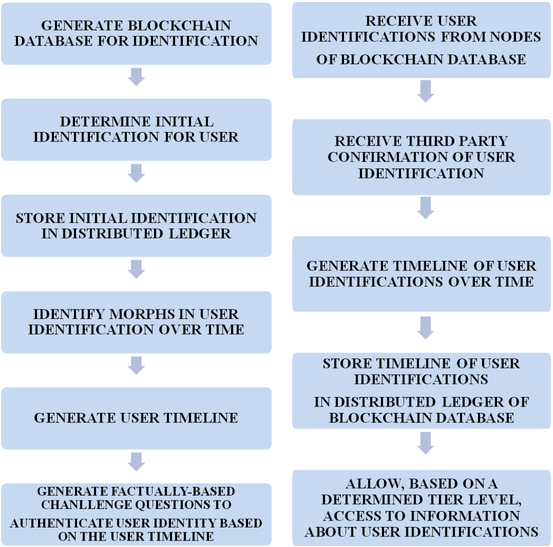

GENERATE BLOCKCHAIN DATABASE FOR IDENTIFICATION
DETERMINE INITIAL IDENTIFICATION FOR USER
STORE INITIAL IDENTIFICATION IN DISTRIBUTED LEDGER
IDENTIFY MORPHS IN USER IDENTIFICATION OVER TIME
GENERATE USER TIMELINE
GENERATE FACTUALLY-BASED CHANLLENGE QUESTIONS TO AUTHENTICATE USER IDENTITY BASED ON THE USER TIMELINE
RECEIVE USER IDENTIFICATIONS FROM NODES OF BLOCKCHAIN DATABASE
RECEIVE THIRD PARTY CONFIRMATION OF USER IDENTIFICATION
GENERATE TIMELINE OF USER IDENTIFICATIONS OVER TIME
STORE TIMELINE OF USER IDENTIFICATIONS IN DISTRIBUTED LEDGER OF BLOCKCHAIN DATABASE
ALLOW, BASED ON A DETERMINED TIER LEVEL, ACCESS TO INFORMATION ABOUT USER IDENTIFICATIONS

FIGURE 6. Blockchain user identification. Note: (Left) Flow (Right) Map.

Figure 5 shows the sub-network for Cryptography. Cryptography is a technique associated with the process of converting ordinary plain text into unintelligible text and vice-versa. Blockchain uses cryptography to protect identities of the users of a network, to ensure secure transactions, and to protect all sorts of valuable information. Cryptography sub-technology related patents have been applied for most of the layers from layers 1 to 13, and it has been found that large companies such as IBM and Microsoft have licenses. The node 2, 11, 97, 100, 116, 136, 145, 172, 174, 216, 217, 270, 330, 693, 1492, and 1681 are all filed by IBM, and most are related to cryptography. The node 2 (US4074066) is about a system for the secure transmission of multi-block data messages from a sending station to a receiving station. The node 100 (US4850017) is about a system for secure generation and transmission of cryptographic keys from a generating station to one or more using stations where the use of the cryptographic key at each using station is controlled via a control value established by the generating station. The node 116 (US4941176) prevents unauthorized disclosure or modification of cryptographic keys and provides a method for validating that key management functions requested for a cryptographic key by the programs authorized by the originator of the key. The node 136 (US4918728) is about cryptographic applications in data processing and complex combinations of data manipulation functions are possible using the control vectors, in accordance with this method. The node 174 (US5142578) is about cryptographic systems and methods for use in data processing systems to enhance security. The node 330 (US5673319) is about computer-implemented methods to encrypt plaintext into ciphertext. The node 1492 (US7428306) is an encryption apparatus and method for providing an encrypted file system. The node 1681 (US8107620) is a method for cryptographically transforming an input message into an output message while assuring message integrity. This invention provides encryption schemes and apparatus, which are more efficient than the existing single pass authenticated encryption schemes, while providing the same level of security. The initial vectors, which are an essential part of these schemes, are chosen in an incremental and safe fashion. This also leads to an incremental method for generating the pair-wise differentially uniform sequences or XOR-universal sequences which are another essential part of such schemes. The incrementality of the generation of these sequences extends to even across different plain-text messages being encrypted, leading to substantial savings in time to encrypt. A further step of encryption is shown to be redundant and leads to savings over earlier schemes. The node 426 (US6249866) and 532 (US6226742) are all filed by Microsoft Corporation, and most are core technologies related to protection against unauthorized use of memory or access to memory by using cryptography. The node 426 (US6249866) is an encrypting file system and method for computer systems. The node 532 (US6226742) provides fast and extremely secure encryption and decryption, but also assures integrity of a ciphertext message. The node 820 (US7716484) filed by RSA Security is a method for accessing encrypted data by a client. The method includes receiving from the client by server client information derived from a first secret wherein the client information is derived such that the server cannot feasibly determine the first secret. The method also includes providing to the client by the server intermediate data, which is derived responsive to the received client information, a server secret, and possibly other information. The intermediate data is derived such that the client cannot feasibly determine the server secret. The method also includes authenticating the client by a device that stores encrypted secrets and is configured not to provide the encrypted secrets without authentication. After the authentication step, the method also includes providing the encrypted secrets to the client. The encrypted secrets are capable of being decrypted using a third secret that is derived from the intermediate data. The node 498 (US6307936), 499 (US6704871) and 620 (US6704871) are all filed by SafeNet, and most are core technologies related to protecting specific internal or peripheral components leads to protecting of the entire computer to assure secure computing or processing of information in cryptographic circuits. The node 498 (US6307936) is a method of creating and manipulating encryption keys without risking the security of the key. The node 499 (US6704871) is about a digital signal processor with embedded encryption security features. The node 620 (US6708273) is a method for implementing IPSEC (Internet Protocol Security Standard) transforms within an integrated circuit. The integrated circuit includes a callable library of cryptographic commands and encryption algorithms. An encryption processor is included to perform key and data encryption, as well as a high-performance hash processor and a public key accelerator. IPSEC is a generally used security standard that provides security when communicating through the Internet. This standard requires DES to encrypt Internet Protocol data packets, SHA-1 for authentication, and a public key algorithm for handshaking. The node 3756 (US9825931) is filed by Bank of America and is a system to track and verify the user's changing identity through a blockchain database. This is a system for generating and using a blockchain distributed network for tracking and validating a user identification morphing over time. The blockchain database comprises a distributed ledger that is updated with real-time identification information including an initial identification of the user. Figure 6 shows the process flow and map illustrating a blockchain user identification timeline generation process. Entities and individuals alike utilize their identification for daily operations. Identities of entities and individuals tend to morph overtime, with name changes, signature changes, and maturation. As such, identifications may need to be updated for entities and individuals to be authorized for daily operations.

Figure 7 shows the sub-network for Hardware blockchain. With the rapid development of electronic and communication technologies, a new complex network transaction chain has emerged. The hardware implementation of the underlying processing for the transaction chain is improved, improving security, stability and speed of implementation. Therefore, it is expected that the Hardware blockchain will lead the spread of the big data market by reinforcing fast speed and data security, so that it is suitable for the era of the industrial revolution where large amounts of data collection and operation are important. The node 4254 (US9998286), 4256 (US9998286) and 4851 (US10298405) are all filed by Accenture Global Solutions Limited, and most are core technologies related to cryptographic mechanisms or cryptographic arrangements for secret or secure communication including means for verifying the identify or authority of a user of the system or for message authentication. The node 4254 (US9998286) is a system for providing hardware acceleration for blockchain-based record entry. This node referred to the knowledge of the node 3756 (US9825931). As shown in Figure 8, this node embeds a BMC (Blockchain Management Circuitry). The BMC access a consensus operating procedure. The BMC may apply the consensus operating procedure to the record entry to gain append permissions for a blockchain. After completing the consensus operating procedure, the BMC append a block generated based on the record entry to the blockchain. Accordingly, the system ensures that blocks added to the blockchain were generated in compliance with the consensus operating procedure.

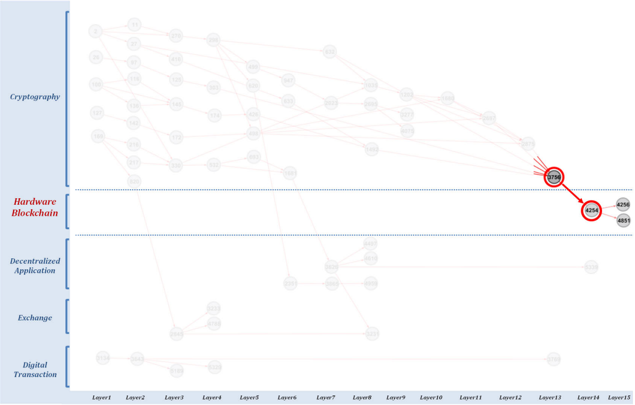


FIGURE 7. Main path network for Hardware blockchain sub-technology. Note: HPP represents a red circle.

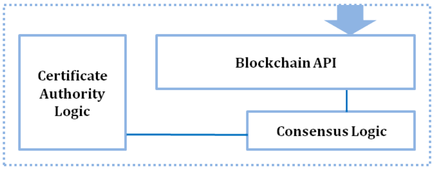


FIGURE 8. BMC (Blockchain Management Circuitry).

Figure 9 shows the sub-network Decentralized applications. Blockchain is not a technology that completely replaces the existing legacy system but is a technology that can be applied to areas that require cost reduction and improved transaction reliability. Therefore, in this sub-technology, it is speculated that blockchain technology is highly likely to be fused with cryptography technologies that will lead the

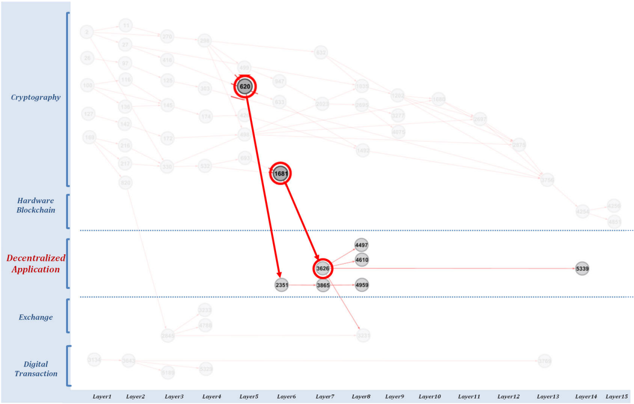


FIGURE 9. Main path network for Decentralized application sub-technology. Note: HPP represents a red circle.

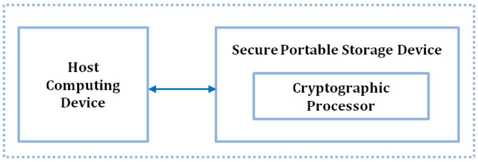
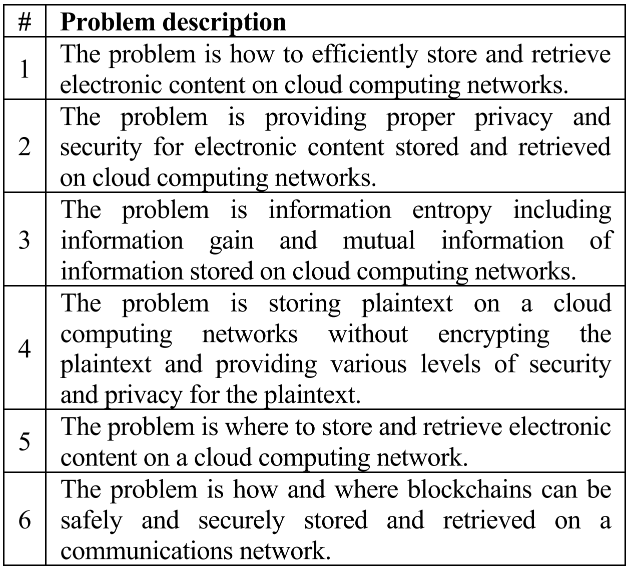


FIGURE 10. A block diagram of a HCD and SPED.

industrial revolution such as Artificial Intelligence and IoT in the future. The node 2351 (US9049010) is about a portable encryption device with logon access controlled by an encryption key, with an on board cryptographic processor for reconstituting the encryption key from a plurality of secrets generated by a secret sharing algorithm. This node referred to the knowledge of the node 620 (US6708273). As shown in the Figure 10, this node embeds a DSP that acts as a cryptographic processor in a SPSD (Secure Portable Storage Device). Cryptographic operations are implemented on data for secure storage and transport by means of a system comprised of one or more than SPED (Secure Portable Encryption Device) capable of such cryptographic operations, and optionally storing and communicating such secure data to host or peripheral devices, one or more than HCD (Host Computing Device), and means for securely protecting access to that data. Figure 10 shows a block diagram of HCD and SPED. The node 3626 (US9569771) is filed by Stephen Lesavich and is a method for storage and retrieval of blockchains blocks using Galois Fields. This node referred to the knowledge of the node 1681 (US8107620), which is a method of cryptographically converting an input message into an output message while ensuring message integrity. One or more blocks for a blockchain are securely stored and retrieved with a modified Galois Fields on a cloud or peer-to-peer (P2P) communications network. The modified Galois Field provides at least additional layers for security and privacy for blockchains. The blocks and blockchains are securely stored and retrieved for cryptocurrency transactions including, but not limited to, BITCOIN transactions and other cryptocurrency transactions. In accordance with this method, some of the problems associated with electronic content storage and retrieval on cloud computing networks are overcome. Table 4 shows the problems associated with electronic content storage and retrieval on cloud computing network. The node 3865 (US9992022) is about a digital identity management and permission controls within the distributed network nodes. The node 4497 (US10493996) is a method for impaired driving detection, monitoring and accident prevention with driving habits. The node 4610 (US10673618) is natively integrating blockchain charging for network services in telecommunication networks. The node 4959 (US10489278) is an entitlement framework with proof of entitlement consensus. The node 5339 (US10628454) relate to the field of data storage using blockchain and more specifically, to relational blockchain database.

Figure 11 shows sub- network for Exchange technology. This sub-technology was filed over layers 3-8, and it

TABLE 4. The problems associated with electronic content storage and retrieval.



#	Problem description
1	The problem is how to efficiently store and retrieve electronic content on cloud computing networks.
2	The problem is providing proper privacy and security for electronic content stored and retrieved on cloud computing networks.
3	The problem is information entropy including information gain and mutual information of information stored on cloud computing networks.
4	The problem is storing plaintext on a cloud computing networks without encrypting the plaintext and providing various levels of security and privacy for the plaintext.
5	The problem is where to store and retrieve electronic content on a cloud computing network.
6	The problem is how and where blockchains can be safely and securely stored and retrieved on a communications network.

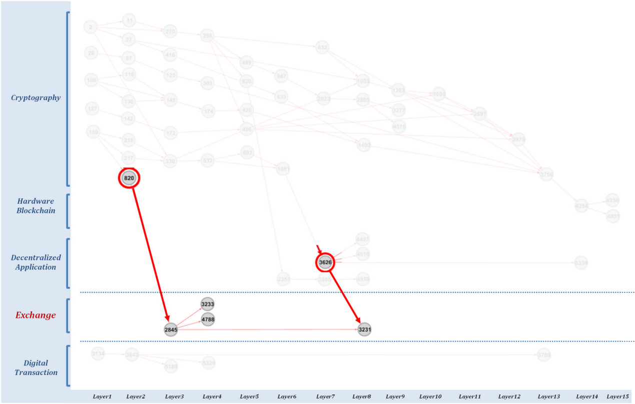


FIGURE 11. Main path network for Exchange sub-technology. Note: HPP represents a red circle.

appears to be affected by the cryptography and decentralized application sub-technologies. The exchange sub-technology includes the transaction management such as cryptocurrency transaction efficiency, verification, security, exchange operation, user authentication, mining management, mining compensation, remittance, electronic wallet, and currency exchange. The node 2845 (US9892460) is a method for providing an exchange traded product holding digital math-based assets are disclosed. A digital math-based asset is a kind of digital asset based upon a computer generated mathematical and cryptographic protocol that may, among other things, be exchanged for value and/or be used to buy and sell goods or pay for services. This node referred to the knowledge of the node 820 (US7716484), which is a method for how to access encrypted secret data. Shares based on digital math-based assets may be created using one or more computers by determining share price information based upon quantities of digital math-based assets held by a trust, electronically receiving a request from an authorized participant user device to purchase a quantity of shares, electronically transmitting a quantity of digital math-based assets to one or more destination digital asset accounts for receipt of digital math-based assets from the authorized participant based on the determined share price information and the requested quantity of shares, and electronically issuing shares to the authorized participant. The node 3231 (US10229396) is a method for transacting bitcoin. Bitcoin transacting requires the use of a public key and a private key. The private key is used to sign an authorization and the public key is used to verify the signature. Some users may require control over their private keys in order to ensure to such users that Bitcoin transacting will not take place without their express authorization. This node referred to the knowledge of the node 3626 (US9569771), which is blockchains are securely stored and retrieved for cryptocurrency transactions. Bitcoin can be sent to an email address. No miner's fee is paid by a host computer system. Hot wallet functionality is provided that transfers values of some Bitcoin addresses to a vault for purposes of security. A private key of a Bitcoin address of the vault is split and distributed to keep the vault secure. Instant exchange allows for merchants and customers to lock in a local currency price. A vault has multiple email addresses to authorize a transfer of Bitcoin out of the vault. User can opt to have private keys stored in locations that are under their control. A tip button rewards content creator for their efforts. A Bitcoin exchange allows for users to set prices that they are willing to sell or buy Bitcoin and execute such trades.

Figure 12 shows sub-network Digital transaction. Digital transaction sub-technology relates to a network architecture or network communication protocol for network security to provide confidential data exchange between entities communicating over a data packet network in which data content is protected. In order to make various transactions, many transactions occur. It is necessary to store and manage the data of all transactions distributed and stored by each manager, and the problem of handling and managing such large amounts of data must be solved. In other words, digital transaction sub-technology is expected to develop in the direction of solving the problem of processing large amounts of data in the future. The node 3134 (US9298806) is filed by Coinlab and this is about a method for analyzing transactions in a distributed ledger. Blockchain technology uses the blockchain, otherwise known as a distributed ledger, to create a publicly verifiable record of digital transactions. Digital transactions may include cryptocurrency transactions such as Bitcoin, Litecoin, Namecoin, Ethereum, and/or other similar digital transactions. The node 3643 (US9635000) is filed by Sead Muftic and describes an IDMS (IDentity Management System) based on the concept of peer-to-peer protocols and the public identities ledger. The system manages digital identities, which are digital objects that contain attributes used for the identification of persons and other entities in an IT system and for making identity claims. The node 5189 (US10592710) is a method for the cryptographic authentication of contactless cards and provides a method for contactless card verification include a contactless card including a substrate, a processor, and a memory. The node 5329 (US10535062) utilized a contactless card to securely share personal data stored in a blockchain and the verification service may verify the signature based on a public key. The node 3769 (US10496989) is an enable contactless access to a transaction terminal using a process data network.

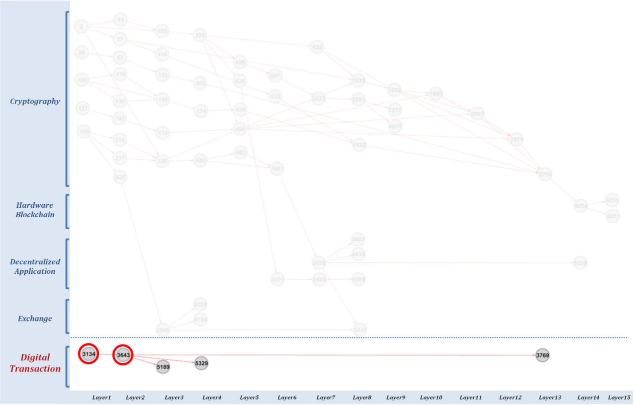


FIGURE 12. Main path network for Digital transaction sub-technology. Note: HPP represents a red circle.

V. CONCLUSION

This paper developed an improved KP-based main path analysis to identify technological trajectories. Specifically, we designed the knowledge unconventionality (KU) metric to reduce network complexity in the last layer and so to find future developmental directions in a specific technological domain. This paper conducted an empirical analysis using blockchain technology. The empirical result overall shows that there are five sub-technologies under the blockchain domain, and each sub-technology has evolved with high technological interactions among other sub-technologies.

TABLE 5. Standardization of blockchain technologies.

TABLE 5. *(Continued.)* Standardization of blockchain technologies.

Committees			Title
ISO/TC 307 Blockchain and distributed ledger technologies	JWG 4		Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Blockchain and distributed ledger technologies and IT Security techniques
	SG 7		Interoperability of blockchain and distributed ledger technology systems
	WG 1		Foundations
	WG 2		Security, privacy and identity
	WG 3		Smart contracts and their applications
	WG 5		Governance
	WG 6		Use cases
ISO/TC 46/SC 11 Archives/records management	JWG 1		Joint ISO/TC 46/SC 11 - ISO/TC 307 WG: Blockchain
	WG 1		Metadata
	WG 8		Management systems for records
	WG 16		Systems design for records
	WG 17		Records in the cloud
	WG 18		ISO 13008:2012 Revision
	WG 19		Risk assessment for records processes and systems
ITU-T SG17 Telecommunication/ICT Security, Cyberspace security, Application security, Identity management and authentication	WP1/17	Q2/17	Security architecture and framework
		Q3/17	Telecommunication information security management systems
		Q6/17	Security aspects of telecommunication services, networks and Internet of Things
		Q13/17	Security aspects for Intelligent Transport System
	WP2/17	Q4/17	Cybersecurity
		Q5/17	Countering spam by technical means
		Q14/17	Security aspects for Distributed Ledger Technologies
	WP3/17	Q7/17	Secure application services
		Q8/17	Cloud computing and Big data infrastructure security
		Q12/17	Formal languages for telecommunication software and testing
	WP4/17	Q9/17	Telebiometrics
		Q10/17	Identity management architecture and mechanisms
		Q11/17	Generic technologies (Directory, public key infrastructure (PKI), privilege management infrastructure (PMI), Abstract Syntax Notation One (ASN.1), object identifiers (OIDs)) to support secure applications
ITU-T SG16 Multimedia content delivery, Multimedia e-services, Media coding and immersive environments	WP1/16	Q11/16	Multimedia systems, terminals, gateways and data conferencing
		Q12/16	Visual surveillance systems and services
		Q13/16	Multimedia application platforms and end systems for IPTV
		Q14/16	Digital signage systems and services
		Q21/16	Multimedia framework, applications and services
	WP2/16	Q22/16	Distributed ledger technologies and e-services
		Q23/16	Digital culture-related systems and services
		Q24/16	Human factors related issues for improvement of the quality of life through international telecommunications
		Q26/16	Accessibility to multimedia systems and services
		Q27/16	Vehicle gateway platform for telecommunication/ITS services and applications
		Q28/16	Multimedia framework for e-health applications
	WP3/16	Q5/16	Artificial intelligence-enabled multimedia applications
		Q6/16	Visual coding
		Q7/16	Speech/audio coding, voiceband modems, facsimile terminals and network-based signal processing
		Q8/16	Immersive live experience systems and services
ITU-T SG13 Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures	WP1/13	Q6/13	Quality of service (QoS) aspects including IMT-2020 networks
		Q20/13	IMT-2020: Network requirements and functional architecture
		Q21/13	Network softwarization including software-defined networking, network slicing and orchestration
		Q22/13	Upcoming network technologies for IMT-2020 and Future Networks
		Q23/13	Fixed-Mobile Convergence including IMT-2020
	WP2/13	Q7/13	Big data driven networking (bDDN) and Deep packet inspection (DPI)
		Q17/13	Requirements, ecosystem, and general capabilities for cloud computing and big data
		Q18/13	Functional architecture for cloud computing and big data
		Q19/13	End-to-end cloud computing management, cloud security and big data governance
	WP3/13	Q1/13	Innovative services scenarios, deployment models and migration issues based on Future Networks
		Q2/13	Next-generation network (NGN) evolution with innovative technologies including software-defined networking (SDN) and network function virtualization (NFV)
		Q5/13	Applying networks of future and innovation in developing countries
		Q16/13	Knowledge-centric trustworthy networking and services
ITU-T SG20 Internet of things (IoT) and smart cities and communities (SC&C)	WP1/20	Q1/20	End to end connectivity, networks, interoperability, infrastructures and Big Data aspects related to IoT and SC&C
		Q2/20	Requirements, capabilities, and use cases across verticals
		Q3/20	Architectures, management, protocols and Quality of Service
		Q4/20	e/Smart services, applications and supporting platforms
	WP2/20	Q5/20	Research and emerging technologies, terminology and definitions
		Q6/20	Security, privacy, trust and identification for IoT and SC&C
		Q7/20	Evaluation and assessment of Smart Sustainable Cities and Communities
ITU-T Focus Groups	FG-DLT		Focus Group on Application of Distributed Ledger Technology Distributed ledger technology (DLT) refers the processes and related technologies that enable nodes in a network to securely propose, validate and record state changes (or updates) to a synchronized ledger that is distributed across the network's nodes. · to identify and analyse DLT-based applications and services · to draw up best practices and guidance which support the implementation of those applications and services on a global scale · to propose a way forward for related standardization work in ITU-T Study Groups

TABLE 5. ***(Continued.)*** **Standardization of blockchain technologies.**

	FG-DFC	The ITU-T Focus Group on Digital Currency including Digital Fiat Currency (FG DFC) was established in May 2017. The main objectives of the Focus Group were: · Study the economic benefit and impact of introducing DFC over mobile money; · Investigate the ecosystem of digital fiat currency implementation for financial inclusion · Map the functional network reference architecture and process components required to implement digital fiat currency and integration with existing payment systems for interoperability · Identify use cases, requirements and applications of digital fiat currency · Develop better understanding of the security, regulatory implications, consumer protection, fraud prevention and counterfeiting issues of DFS and how can digital fiat currency can address these concerns · Identify critical sovereign security, transparency and verifiability of DFC technology and provide guidelines towards the escrow of critical software and hardware components to ensure trust and verifiability · Identify new areas for standardization in ITU-T study groups
	FG-DPM	The Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities was established by ITU-T Study Group 20 at its meeting in Dubai, 13-23 March 2017. FG structure · WG1 - Use Cases, Requirements and Applications/Services · WG2 - DPM Framework, Architectures and Core Components · WG3 - Data sharing, Interoperability and Blockchain · WG4 - Security, Privacy and Trust including Governance · WG5 - Data Economy, commercialization, and monetization · Ad-hoc team - Global picture of DPM capabilities

https://www.iso.org, http://www.itu.int

Based on the characteristics of blockchain patents and developmental trajectories shown on main paths, we suggest further R&D directions as follows. First, further R&D direction for cryptography will more focus on the capability in fast big data processing. In addition, the main paths show that main knowledge stream of cryptography is converged with the hardware blockchain technology and therefore the cryptography will be the significant basic technology for the hardware blockchain. Second, hardware blockchain technology will lead the spread of big data market by reinforcing fast speed and data security. Since data collection and operation is the critical role in the era of data, the importance and demand of hardware blockchain is getting more increased. Third, the future technologies related to the decentralized

TABLE 6. **List of patents in knowledge persistence-based main path network for blockchain technology.**

Patent	Label	Layer	Year	Knowledge Persistence	GP	LP
US 4074066	2	1	1976	58.3697	0.72194	1
US 4229818	11	2	1978	49.6205	0.61372	0.97335
US 4317957	26	1	1980	14.0354	0.17359	0.24046
US 4319079	27	2	1980	44.5378	0.55086	0.87365
US 4747050	97	2	1987	15.2565	0.1887	0.29927
US 4850017	100	1	1987	49.177	0.60824	0.84251
US 4868877	127	1	1988	31.6736	0.39175	0.54264
US 4933969	125	3	1988	27.3476	0.33824	0.43815
US 4941176	116	2	1988	35.5687	0.43993	0.69771
US 4918728	136	2	1989	48.7968	0.60354	0.95719
US 5005200	142	2	1989	50.9791	0.63053	1
US 5073934	145	3	1990	62.4159	0.77198	1
US 5142578	174	4	1991	57.8962	0.71608	0.71608
US 5200999	172	3	1991	25.9897	0.32145	0.4164
US 5241599	169	1	1991	51.824	0.64098	0.88786
US 5491749	217	2	1993	25.6677	0.31747	0.50349
US 5491750	216	2	1993	33.2359	0.41107	0.65195
US 5432848	270	3	1994	59.6183	0.73738	0.95518
US 5631960	298	4	1995	80.8516	1	1
US 5671283	303	4	1995	19.9829	0.24715	0.24715
US 5673319	330	3	1995	57.492	0.71108	0.92111
US 6061449	416	3	1997	28.7464	0.35555	0.46056
US 6249866	426	5	1997	24.2685	0.30016	0.73388
US 6226742	532	4	1998	47.6356	0.58917	0.58917
US 6307936	498	5	1998	25.252	0.31233	0.76362
US 6704871	499	5	1998	24.4547	0.30246	0.73951
US 6708273	620	5	1999	28.9833	0.35848	0.87645
US 7093126	693	5	2000	33.0688	0.40901	1
US 7184549	632	7	2000	25.3407	0.31342	0.85901
US 7203842	633	6	2000	3.5549	0.043969	0.12051
US 7716484	820	2	2001	38.5833	0.47721	0.75685
US 7028191	947	6	2002	16.0333	0.19831	0.5435
US 7321910	1035	8	2003	23.2667	0.28777	1
US 7885405	1202	9	2004	35	0.43289	1
US 7428306	1492	8	2006	16.95	0.20964	0.72851
US 8107620	1681	6	2007	29.5	0.36487	1
US 8379841	1680	10	2007	31.5	0.3896	1
US 8386800	2023	7	2010	15	0.18553	0.50847
US 9049010	2351	6	2012	12	0.14842	0.40678
US 8707052	2695	8	2013	6	0.07421	0.25788
US 8737606	2697	11	2013	30	0.37105	1
US 8983063	2875	12	2014	29	0.35868	1
US 9892460	2845	3	2014	13.8333	0.1711	0.22163
US 10229396	3231	8	2015	0	0	0

TABLE 6. ***(Continued.)*** **List of patents in knowledge persistence-based main path network for blockchain technology.**

US 10614430	3233	4	2015	0	0	0
US 9298806	3134	1	2015	38.477	0.4759	0.65919
US 10262141	3277	9	2016	0	0	0
US 10496989	3769	13	2016	0	0	0
US 9569771	3626	7	2016	29.5	0.36487	1
US 9635000	3643	2	2016	25.4362	0.33138	0.53531
US 9825931	3756	13	2016	6	0.07421	1
US 10291413	4256	15	2017	0	0	0
US 9940463	4075	9	2017	0	0	0
US 9992022	3865	7	2017	6	0.07421	0.20339
US 9998286	4254	14	2017	5	0.061842	1
US 10298405	4851	15	2018	0	0	0
US 10489278	4959	8	2018	0	0	0
US 10493996	4497	8	2018	0	0	0
US 10644879	4788	4	2018	0	0	0
US 10673618	4610	8	2018	0	0	0
US 10535062	5329	4	2019	0	0	0
US 10592710	5189	3	2019	0	0	0
US 10628454	5339	14	2019	0	0	0

applications will be developed closely with encryption technologies which are essential part for artificial intelligence and IoT. Blockchain technologies will not completely replace the existing legacy system, so it will be applied to areas that require cost reduction and transaction reliability improvement. Fourth, the exchange related technologies will focus on solving the problems in cryptocurrency transactions. The cryptocurrency field has made technological progress as a new means of online transaction, and it seems that it is currently in the stabilization stage. Fifth, the further directions of the digital transaction technologies will focus on the big data processing. The number of online transactions is dramatically increasing over time and so it is necessary to store and manage the data of all transactions distributed and stored by each manager. Therefore, the data processing and managing during online transactions are solved on priority. Even though this paper objectively provides the developmental trajectories and further directions of Blockchain technology, some methodological issues should be improved. First, this paper adopted the basic hypothesis that patent citations denote knowledge flows from citing to cited patents and the proportion of the inherited knowledge is calculated based on the size of referred knowledge sources. This hypothesis basically works for a large volume of data, but the real knowledge flows might not be reflected if the size of technological domain is very small. To solve this issue, each patent citation should have different weight and textual and classification similarity-based measurements can be the solutions. Second, the proposed method requires the qualitative analysis of each node on the main paths. It is basically inevitable step, but the qualitative analysis can be more effective and efficient if keywords of each node can be extracted. Therefore, our further work will develop a keyword extraction approach which can separately extract the domain-generic keywords and patent-specific keywords for better representation of inventive knowledge in a patent. Finally, this paper qualitatively decomposed sub-technologies under the blockchain technology. However, since the reproducibility of the method is an important characteristic for quantitative methods, this step should be replaced by an automatic decomposition method.

APPENDIX

See Table 5 and Table 6.

REFERENCES

[1] H. Park, J. J. Ree, and K. Kim, "Identification of promising patents for technology transfers using TRIZ evolution trends," *Expert Syst. Appl.*, vol. 40, no. 2, pp. 736–743, Feb. 2013.

[2] H. Ernst, "Patent information for strategic technology management," *World Pat. Inf.*, vol. 25, no. 3, pp. 233–242, Sep. 2003.

[3] C. Mun, S. Yoon, N. Raghavan, D. Hwang, S. Basnet, and H. Park, "Function score-based technological trend analysis," *Technovation*, vol. 101, Mar. 2021, Art. no. 102199.

[4] S. Choi and H. Park, "Investigation of strategic changes using patent co-inventor network analysis: The case of samsung electronics," *Sustainability*, vol. 8, no. 12, p. 1315, Dec. 2016.

[5] H. Park and C. L. Magee, "Tracing technological development trajectories: A genetic knowledge persistence-based main path approach," *PLoS ONE*, vol. 12, no. 1, Jan. 2017, Art. no. e0170895.

[6] C. Mun, Y. Kim, D. Yoo, S. Yoon, H. Hyun, N. Raghavan, and H. Park, "Discovering business diversification opportunities using patent information and open innovation cases," *Technol. Forecasting Social Change*, vol. 139, pp. 144–154, Feb. 2019.

[7] C. Mun, S. Yoon, Y. Kim, N. Raghavan, and H. Park, "Quantitative identification of technological paradigm changes using knowledge persistence," *PLoS ONE*, vol. 14, no. 8, Aug. 2019, Art. no. e0220819.

[8] H. Park and C. L. Magee, "Quantitative identification of technological discontinuities," *IEEE Access*, vol. 7, pp. 8135–8150, 2019.

[9] C. V. Trappey, H.-Y. Wu, F. Taghaboni-Dutta, and A. J. C. Trappey, "Using patent data for technology forecasting: China RFID patent analysis," *Adv. Eng. Informat.*, vol. 25, no. 1, pp. 53–64, Jan. 2011.

[10] L. Y. Y. Lu and J. S. Liu, "A novel approach to identify the major research themes and development trajectory: The case of patenting research," *Technol. Forecasting Social Change*, vol. 103, pp. 71–82, Feb. 2016.

[11] Y. Kajikawa, J. Yoshikawa, Y. Takeda, and K. Matsushima, "Tracking emerging technologies in energy research: Toward a roadmap for sustainable energy," *Technol. Forecasting Social Change*, vol. 75, no. 6, pp. 771–782, Jul. 2008.

[12] T. U. Daim, G. Rueda, H. Martin, and P. Gerdsri, "Forecasting emerging technologies: Use of bibliometrics and patent analysis," *Technol. Forecasting Social Change*, vol. 73, no. 8, pp. 981–1012, Oct. 2006.

[13] S. Yoon, C. Mun, N. Raghavan, D. Hwang, S. Kim, and H. Park, "Hierarchical main path analysis to identify decompositional multi-knowledge trajectories," *J. Knowl. Manage.*, vol. 25, no. 2, pp. 454–476, Jun. 2020.

[14] D. You and H. Park, "Developmental trajectories in electrical steel technology using patent information," *Sustainability*, vol. 10, no. 8, p. 2728, Aug. 2018.

[15] S. Kwon, A. Porter, and J. Youtie, "Navigating the innovation trajectories of technology by combining specialization score analyses for publications and patents: Graphene and nano-enabled drug delivery," *Scientometrics*, vol. 106, no. 3, pp. 1057–1071, Mar. 2016.

[16] S. Lee, B. Yoon, and Y. Park, "An approach to discovering new technology opportunities: Keyword-based patent map approach," *Technovation*, vol. 29, nos. 6–7, pp. 481–497, Jun. 2009.

[17] B. Verspagen, "Mapping technological trajectories as patent citation networks: A study on the history of fuel cell research," *Adv. Complex Syst.*, vol. 10, no. 1, pp. 93–115, Mar. 2007.

[18] D. Zhu and A. L. Porter, "Automated extraction and visualization of information for technological intelligence and forecasting," *Technol. Forecasting Social Change*, vol. 69, no. 5, pp. 495–506, Jun. 2002.

[19] Y.-H. Tseng, C.-J. Lin, and Y.-I. Lin, "Text mining techniques for patent analysis," *Inf. Process. Manage.*, vol. 43, no. 5, pp. 1216–1247, Sep. 2007.

[20] A. L. Porter, S. W. Cunningham, J. Banks, A. T. Roper, T. W. Mason, and F. A. Rossini, *Forecasting and Management of Technology*. Hoboken, NJ, USA: Wiley, 2011.

[21] R. Lai and D. L. K. Chuen, "Blockchain-from public to private," in *Handbook of Blockchain, Digital Finance, and Inclusion*, vol. 2. Amsterdam, The Netherlands: Elsevier, 2018, pp. 145–177.

[22] S. Underwood, *Blockchain Beyond Bitcoin*. New York, NY, USA: Communications of the ACM, 2016.

[23] W. Viriyasitavat, L. Da Xu, Z. Bi, and A. Sapsomboon, "New blockchain-based architecture for service interoperations in Internet of Things," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 4, pp. 739–748, Aug. 2019.

[24] R. M. A. Latif *et al.*, "A remix IDE: Smart contract-based framework for the healthcare sector by using blockchain technology," *Multimed Tools Appl.*, 2020, doi: 10.1007/s11042-020-10087-1.

[25] A. P. Singh, N. R. Pradhan, A. K. K. Luhach, S. Agnihotri, N. Jhanjhi, S. Verma, Kavita, U. Ghosh, and D. Roy, "A novel patient-centric architectural framework for blockchain-enabled healthcare applications," *IEEE Trans. Ind. Informat.*, early access, Nov. 16, 2020, doi: 10.1109/TII.2020.3037889.

[26] J. Chen, "Flowchain: A distributed ledger designed for peer-to-peer IoT networks and real-time data transactions," in *Proc. 2nd Int. Workshop Linked Data Distrib. Ledgers (LDDL)*, 2017, pp. 1–11.

[27] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[28] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, Mar. 2017.

[29] N. P. Hummon and P. Dereian, "Connectivity in a citation network: The development of DNA theory," *Social Netw.*, vol. 11, no. 1, pp. 39–63, Mar. 1989.

[30] A. Martinelli and Ö. Nomaler, "Measuring knowledge persistence: A genetic approach to patent citation networks," *J. Evol. Econ.*, vol. 24, no. 3, pp. 623–652, Jul. 2014.

[31] I. von Wartburg, T. Teichert, and K. Rost, "Inventive progress measured by multi-stage patent citation analysis," *Res. Policy*, vol. 34, no. 10, pp. 1591–1607, Dec. 2005.

[32] M. L. Weitzman, "Recombinant growth," *Quart. J. Econ.*, vol. 113, no. 2, pp. 331–360, 1998.

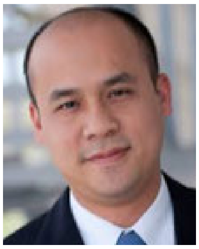
[33] M. A. Schilling and E. Green, "Recombinant search and breakthrough idea generation: An analysis of high impact papers in the social sciences," *Res. Policy*, vol. 40, no. 10, pp. 1321–1331, Dec. 2011.

[34] L. Fleming, "Recombinant uncertainty in technological search," *Manage. Sci.*, vol. 47, no. 1, pp. 117–132, Jan. 2001.

SOHEE KIM is currently pursuing the Ph.D. degree with the Department of Information Systems, College of Engineering, Hanyang University, Seoul, South Korea. Her research interests include patent management, knowledge networks, and data mining.

SEJUN YOON is currently pursuing the Ph.D. degree with the Department of Information Systems, College of Engineering, Hanyang University, Seoul, South Korea. His research interests include technology management, patent mining, technological trajectory, and machine learning.

NAGARAJAN RAGHAVAN (Member, IEEE) received the Ph.D. degree in microelectronics from the Division of Microelectronics, Nanyang Technological University (NTU), Singapore, in 2012. He is currently an Assistant Professor with the Engineering Product Development (EPD) Pillar, Singapore University of Technology and Design (SUTD). Prior to this, he was a Postdoctoral Fellow with the Massachusetts Institute of Technology (MIT), Boston, and IMEC, Belgium, in joint association with Katholieke Universiteit Leuven (KUL). His work focuses on reliability assessment, maintenance modeling, characterization and lifetime prediction of nanoelectronic devices as well as material design for reliability, uncertainty quantification and prognostics, and health management of electromechanical/industrial systems.



NGUYEN-TRUONG LE received the Ph.D. degree in technology management from the University of Stuttgart, Germany. He is currently a Senior Researcher with the Fraunhofer Institute for Industrial Engineering IAO. In the Open Photonics Laboratory, companies professionals and students practice the method "Make2Learn and Innovate" to explore emergent technologies, like AI, 5G, and photonics. His research interests include biologization of technology, patent information analysis, and open innovation.

HYUNSEOK PARK received the Ph.D. degree in technology and innovation management from the Pohang University of Science and Technology (POSTECH), Pohang, in 2014. In 2014, he worked with the Fraunhofer Institute of Industrial Engineering (IAO), as a Visiting Researcher. From 2014 to 2016, he was a Postdoctoral Associate with the Institute for Data, Systems and Society (IDSS), Massachusetts Institute of Technology (MIT). He is currently an Assistant Professor with the Department of Information Systems, College of Engineering, Hanyang University, Seoul, South Korea, and the Director of the Future Intelligence Laboratory. His work focuses on patent analytics, functional analysis, design science, technology intelligence, technology and innovation management, and applications of machine learning to multi-dimensional industrial problems.