A Critical Review of Blockchain and Its Current Applications

Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, Kyung-Hyune Rhee*
Department of IT Convergence and Applications Engineering
Pukyong National University, Busan, South Korea
Email: {bayuat, drbruno}@pukyong.ac.kr; {pyhoya, khrhee}@pknu.ac.kr
*corresponding author

***Abstract*—Blockchain technology has been known as a digital currency platform since the emergence of Bitcoin, the first and the largest of the cryptocurrencies. Hitherto, it is used for the decentralization of markets more generally, not exclusively for the decentralization of money and payments. The decentralized transaction ledger of blockchain could be employed to register, confirm, and send all kinds of contracts to other parties in the network. In this paper, we thoroughly review state-of-the-art blockchain-related applications emerged in the literature. A number of published works were carefully included based on their contributions to the blockchain's body of knowledge. Several remarks are explored and discussed in the last section of the paper.**

***Index Terms*—Blockchain; cryptocurrency; review; applications**

I. Introduction

A software system can be characterized into two main architectural approaches, i.e. centralized and distributed [1]. In centralized software system, the nodes are located around and connected with one central node of coordination. Distributed system, on the contrary, have several connected nodes without any central node of control. Fig. 1 illustrates the contrast of these two architectures. There are several benefits of a distributed system, i.e. having more computing power by combining the computing power of all connected nodes, an increased reliability due to the fact that it does not have a single of failure, and so forth. However, several drawbacks of a distributed system include communication overhead and security issues which is related to misuse network access by untrustworthy nodes.

Meanwhile, blockchain can be seen as a part of the implementation layer of a distributed software system. The data integrity in distributed systems can be achieved and maintained using blockchain [2]. Furthermore, blockchain could be also considered as a purely peer-to-peer system which is made up of the individual nodes in a network. Dishonest and malicious peers become the crucial integrity threat in peer-to-peer systems. The individual nodes try to exploit the system for their own purposes since unknown peers with unknown reliability and trustworthiness may exist [3]. Thus, these critical problems are needed to be solved by blockchain.

Along with blockchain, Bitcoin was originally invented by Nakamoto [4] as the first and most prevalent cryptocurrency. It enables *trustless* and reliable transaction where a centralized management is not required though the users do not trust each other or there are unreliable users in the network. Since then, blockchain has drawn a lot of attention to the decentralized transaction ledger functionality which could be used to register, confirm, and send the payment or contracts. Furthermore, blockchain technology has been applied beyond financial transactions, to any kind of transaction and applications, i.e. healthcare, utilities, real estate, and the government sector [5]. These are found to be feasible as the blockchain structure develop for Bitcoin is portable and extensible.

Originally, the main area for blockchain is connecting cryptocurrencies with conventional banking and financial institutions. Blockchain technology offers a novel banking ecosystem thus enabling financial institutions to conduct their financial transactions directly between themselves without any central authorities or intermediaries. Every transaction must be authenticated through the agreement of more than half of those participating in the network [6]. This means that no participants would be able to modify any data within the blockchain without the approval of other participants.

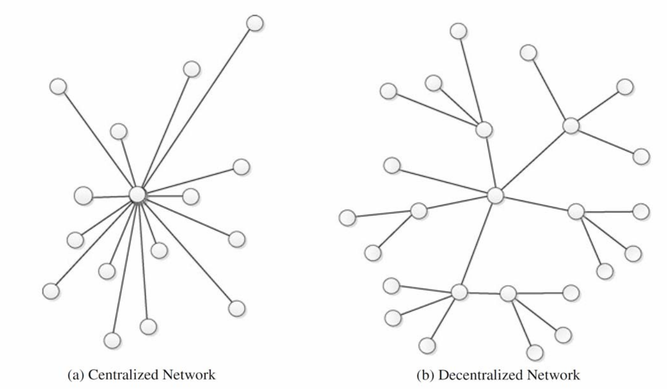
The objective of this paper is to provide and explore insight into blockchain technology and its current practical applications. The paper thoroughly classifies the published works found in the literature, i.e. academic journals, conferences, technical reports, and so on. Regarding the review studies about blockchain technology, several works have been conducted such as in [7], [8], [9], and [10]. However, most studies have not considered a comprehensive discussion about blockchain-related applications.

The rest of the paper is structured as follows. Section II presents an overview of blockchain technology, whilst Section III describes in detail about the practical facets of blockchain. Several remarks and an in-depth discussion are given in Section IV, and finally some concluding remarks are drawn in Section V.

II. Fundamentals of Blockchain Technology

Blockchain is a type of distributed ledger (data structure) which contains information about transactions or events. It is replicated and shared among the participants in the network [4]. The size of chain unceasingly increases since blocks are

978-1-4799-7675-1/17/$31.00 ©2017 IEEE



(a) Centralized Network

(b) Decentralized Network

Fig. 1. Centralized and distributed network architecture, adapted from [1]

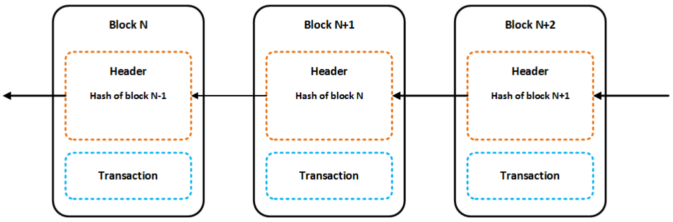


Fig. 2. A chain of blocks - *blockchain* in the Bitcoin, adapted from [4]

added and chained to the previous block using a hash function (see Figure 2 for further illustration of the Bitcoin's blockchain as an example). A cryptographic hash function is used to produce a hash. For instance, Bitcoin uses SHA-256, whilst Litecoin [11] and Primecoin [12] use Scrypt and Cunningham chain, respectively. In addition, it enables us to simply verify the input mapping to a given hash value. It would not be feasible for two different inputs having the same hash [13].

The ledger in the blockchain is validated and preserved by a network node (user) in pursuance of *consensus* mechanism (a collection of rules that allow users to reach a mutual agreement [14]) thereby a central authority or intermediary is not required. Each node keeps a complete replica of the entire ledger. As the first aim of blockchain is to solve the problems exist in Bitcoin cryptocurrency, Section III discusses in detail the practical implementation of the blockchain for financial transaction.

III. Blockchain Applications

In this section, the implementation of blockchain technology in different areas are thoroughly discussed. Furthermore, such applications have been categorized into several groups, i.e. financial services, healthcare, business and industry, and other novel applications.

A. Financial Service

Blockchain has been widely applied for financial transaction which is so-called cryptocurrency. Nowadays, cryptocurrencies have appeared as prominent software systems. Recalling the above-mentioned of Fig. 2, the first block or *genesis block* (is not appeared in the figure) contains the first transaction. The hash of the first block is forwarded to the *miner*, who employs it and generates a hash for the second block. In similar fashion, the third block creates a hash that comprises of the first two blocks, and etc. All blocks in the blockchain can be traced back to the genesis block [7] [15].

TABLE I
The Current Existing Cryptocurrency Systems

Cryptocurreny	Year	Hash Function	Mining Method
Bitcoin [4]	2008	SHA-256	Find all possible nonce values by computing proof of work and other users agree and verify the proof.
Litecoin [11]	2011	Scrypt	Similar to Bitcoin (proof of work)
Peercoin [17]	2012	SHA-256d	proof of work and proof of stake
Primecoin [12]	2013	Cunningham chain	proof of work
Ripple [18]	2014	EC digital signature	consensus system
Ethereum [19]	2014	Ethash	proof of work
Permacoin [20]	2014	Floating digital signature	proof of retreivability
Blackcoin [21]	2014	Scrypt	proof of stake
Auroracoin [22]	2014	Scrypt	proof of work
Darkcoin [23]	2014	X11	proof of work
Namecoin [24]	2015	SHA-256d	proof of work

Cryptocurrency has its own currency (coin). Mining is the process of introducing a new block into blockchain. Each node uses blockchain to verify whether the coin is legitimate or if it has not spent already. Before the transaction records are appended into blockchain, a greater number of participants reach an agreement. Mining process is a resource-intensive task, thus makes it tough for an attacker to validate an invalid transaction. Each mined-block is verified to see if it has whether a valid proof of work [12] or a proof of stake [16].

The followings are the prevalent steps in cryptocurrency: (i) a generated address (public key) is available for a user who has a wallet, (ii) a private key is assigned to the wallet. It is used to sign transaction and proving ownership, (iii) the payer sends coin to the payee using given address and sign it using payer's private key, and finally (iv) the transaction is validated via mining process. Eleven cryptocurrency sytems are included in our study, i.e. Bitcoin [4], Litecoin [11], Peercoin [17], Primecoin [12], Ripple [18], Ethereum [19], Permacoin [20], Blackcoin [21], Auroracoin [22], Darkcoin [23], and Namecoin [24]. Table I summarizes the afore-mentioned cryptocurrency systems which is presented in chronological order of occurrence.

B. Healthcare

Blockchain has a tremendous potential in addressing the interoperability issues exist in the current healtcare systems [25]. It can be used as a standard which allows the stakeholders, i.e. healthcare entities, medical researcher, etc to share electronic health record (EHR) in a secure manner [26]. Sharing of EHR enables us to improve the quality of medical care [27] and enhance the recommendation for doctors [28], for instance.

However, managing healthcare data, i.e. acquiring, storing, and analyzing is not a simple task, particularly in case of privacy issues. Healthcare data should not be revealed to other parties which it might be vulnerable to be used fraudulently by malicious users or attackers.

In order to get the better of those issues, a healthcare data gateway (HDG) based on the blockchain storage platform is proposed by [29]. It is a smartphone application which can be used to manage and control the data sharing easily. The proposed system enables users to process the patient data without exposing patient privacy. Furthermore, a private blockchain cloud is used to stored the data thus ensuring the medical data can not be altered by anybody, including physicians and patients.

The work [30] emphasizes on the designing of a new system to prioritize patient agency, called MedRec. It is a distributed ledger protocol that uses public key cryptography to create blockchain. The blockchain replicas are distributed on each node in the network. Similar to prior work, blockchain technology is used as a access control in order to automate and track certain tasks, i.e. append a new record, change in viewership rights, etc. Furthermore, smart contracts on an Ethereum blockchain [19] is utilized to create intelligent representation of EHR that are stored in each individual node.

Subsequently, the application of pervasive social network (PSN) based healthcare using blockchain is proposed by [31]. PSN allows us to share medical data acquired by medical sensors. PSN-based healthcare system comprises two main security protocols, i.e. an authentication protocol between medical sensors and mobile devices in wireless body area network (WBAN) and an EHR data sharing using blockchain in PSN area. Each node in the PSN is responsible for generating and broadcasting of medical data transactions, i.e. node address and medical sensors. The miners, on the other hand, are responsible for transaction verification and new block creation.

Lastly, a blockchain-based access control mechanism is proposed by [32]. Access control includes identification, authentication, and authorization process. It ascertains a condition of being accountable where user access can be traced for what particular action in a system. The proposed system permits users to access EHR from a shared data pools using blockchain after verifying their identity and cryptographic keys. To achieve user's authentication, an identity based authentication is adopted. In addition, an efficient lightweight block format is proposed to enhance the current implementation of blockchain. Table II compares the related study of blockchain technology for healthcare application.

TABLE II
THE CURRENT EXISTING BLOCKCHAIN FOR HEALTHCARE

Study	Year	Hash Function	Mining Method
HDG [29]	2016	NA	NA
MedRec [30]	2016	Ethash	proof of work
PSN [31]	2016	NA	NA
BBDS [32]	2017	SHA-256	proof of work

C. Business and Industry

The emergence of Internet of Things (IoT) has brought many advantages such as delivering an inter-connection between objects and humans. This motivates authors in [33] [34] to propose an e-business architecture which is particularly developed for IoT environment. For this purpose, distributed autonomous corporation (DAC) is adopted as an entity that gives transaction services in the absence of human intervention. The core of the proposed system is a transaction mode in which peer to peer transaction is performed autonomously, whilst Bitcoin and IoTcoin are adopted as the currency and exchange certificate, respectively.

The authors [35] consider the importance of food safety and quality when proposing a agri-food supply chain traceability system using RFID and blockchain technology. Blockchain is adopted for ensuring the shared and published information is reliable and valid. Furthermore, a term 'smart manufacturing' in the era of Industry 4.0 is also extensively discussed in [36] [37]. Industry 4.0 denotes the flexibility of products and services to be shared over the Internet or other networks, i.e. blockchain. With regard to the supply chain management, Industry 4.0 is expected to attain the circumstance of decentralization and self-regulation.

To date, an extension of cloud computing which is so-called fog computing or edge computing, has been attracted authors to develop a fair payment system based on Bitcoin [38]. Fog computing can be regarded as a large-scale, ubiquitous, and decentralized system which processes any computing tasks. The proposed system is established to improve the traditional e-cash system which needs a trusted authority, i.e. bank to generate payment token. By employing the Bitcoin-based payment, the fog users (outsourcers) can directly make a transaction to the fog nodes (workers) without involving third party. The authors argue that the proposed system can assure a payment for any completed tasks performed by honest workers regardless of the outsourcers is malicious or not.

D. Other Implementations

In this section, the current implementation of blockchain in many areas such as right management system, reputation system, digital content distribution system, WiFi authentication and IoT security are discussed.

The two papers [39] [40] present and discuss a new concept of decentralized right management system by using blockchain technology (BRIGHT). It is entirely different with the traditional approach in which a central third-party is commonly taken into account. The proposed system is expected to have a strong mechanism against attack and it enables us to lower user's service fees. In addition, a reputation system is great potential to measure the trust valuation of us in the community. It is measured based on our previous transactions and interactions in such network, i.e. e-commerce website [41]. By involving blockchain in the reputation system, it can solve the major issues exist in the current reputation system, i.e. freeloaders.

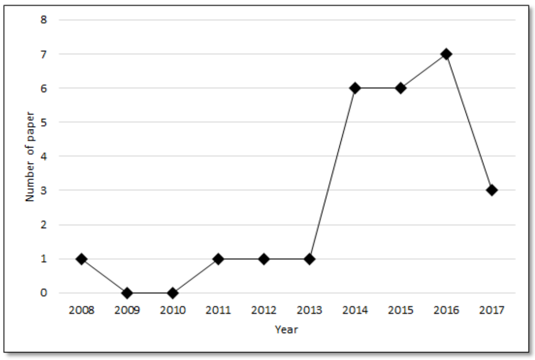


Fig. 3. Paper distribution by year

A new authentication protocol for WiFi is proposed by [42]. This is based on Bitcoin 2.0 which is an alternative cash system derived from Bitcoin. At first, users have to install an application called Auth-Wallet then the tokens called Auth-Coins are issued. Users and access points exchange the tokens for authentication. At last, the implementation of blockchain for smart home security is described in [43]. In order to provide secure access control to the IoT devices, a private and local blockchain is utilized. In addition to allowing a lightweight security mechanism for smart home devices, the blockchain also generates an immutable time-ordered of transactions. Also, smart home miner is considered to be a device that centrally processes transactions in the smart home.

IV. Some Remarks

Twenty six research papers which are related with blockchain applications were thoroughly discussed. The papers were carefully chosen from the online database, i.e. Google Scholar in terms of their practical implementation. The literature were searched using a keyword 'blockchain' which yielded about 9,840 results, and finally 26 papers were considered for classification. Fig. 3 depicts distribution of papers by year of publication. It is obvious that the number of blockchain technology-related papers have increased significantly since it firstly appeared in 2008. It is also worth mentioned that blockchain has fascinated researchers as this technological innovation brings the possibility of cooperatively produce and maintain transactions (distributed ledger) in the network.

There are tremendous advantages of blockchain such as speed, robustness, openness, and so forth. Before the transaction is appended into blockchain, all participants in the network have to reach an agreement. However, blockchain is not an universal cure for all problems and there are several issues that have been identified such as financial transaction for criminal activities, legal aspects, and other economic risks. Blockchain become one of the promising technology in the future if well exploited.

V. Conclusion

The state-of-the-art research papers which are related with blockchain technology have been reviewed and discussed. A number of papers were comprehensively chosen from the online database then they were classified into several different areas. This paper offers an understanding of the current blockchain research and its real-world implementations.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (2017-0-00156, The Development of a Secure Framework and Evaluation Method for Blockchain)

References

[1] A. S. Tanenbaum and M. Van Steen, *Distributed systems: principles and paradigms*. Prentice-Hall, 2007.

[2] D. Drescher, "Blockchain basics," Springer, Tech. Rep.

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

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *URL: http://www.bitcoin.org/bitcoin.pdf*, 2008.

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

[6] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, pp. 6–10, 2016.

[7] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, "A brief survey of cryptocurrency systems," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2016, pp. 745–752.

[8] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2015.

[9] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?a systematic review," *PloS one*, vol. 11, no. 10, p. e0163477, 2016.

[10] S. Seebacher and R. Schüritz, "Blockchain technology as an enabler of service systems: A structured literature review," in *International Conference on Exploring Services Science*. Springer, 2017, pp. 12–23.

[11] C. Lee, "Litecoin," 2011.

[12] S. King, "Primecoin: Cryptocurrency with prime number proof-of-work," *July 7th*, 2013.

[13] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 1996.

[14] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. J. Kishigami, "Blockchain contract: A complete consensus using blockchain," in *Consumer Electronics (GCCE), 2015 IEEE 4th Global Conference on*. IEEE, 2015, pp. 577–578.

[15] S. Ahamad, M. Nair, and B. Varghese, "A survey on crypto currencies," in *4th International Conference on Advances in Computer Science, AETACS*. Citeseer, 2013, pp. 42–48.

[16] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published paper, August*, vol. 19, 2012.

[17] ——, "Peercoin–secure & sustainable cryptocoin," *Aug-2012 [Online]. Available: https://peercoin. net/whitepaper*.

[18] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," *Ripple Labs Inc White Paper*, vol. 5, 2014.

[19] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, 2014.

[20] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, "Permacoin: Repurposing bitcoin work for data preservation," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2014, pp. 475–490.

[21] P. Vasin, "Blackcoins proof-of-stake protocol v2," 2014.

[22] D. Cawrey, "Auroracoin airdrop: Will iceland embrace a national digital currency," *CoinDesk, March*, vol. 24, 2014.

[23] E. Duffield and K. Hagan, "Darkcoin: Peertopeer cryptocurrency with anonymous blockchain transactions and an improved proof of work system," *Mar-2014 [Online]. Available: https://www.dash.org/wpcontent/uploads/2014/09/DarkcoinWhitepaper.pdf*, 2014.

[24] H. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau, and A. Narayanan, "An empirical study of namecoin and lessons for decentralized namespace design," in *Workshop on the Economics of Information Security (WEIS)*. Citeseer, 2015.

[25] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on*. IEEE, 2016, pp. 1–3.

[26] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health IT and health care related research."

[27] B. A. Tama, "Learning to prevent inactive student of Indonesia open university." *Journal of Information Processing Systems*, vol. 11, no. 2, pp. 165–172, 2015.

[28] B. A. Tama and K.-H. Rhee, "Tree-based classifier ensembles for early detection method of diabetes: an exploratory study," *Artificial Intelligence Review*, 2017.

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

[30] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Open and Big Data (OBD), International Conference on*. IEEE, 2016, pp. 25–30.

[31] J. Zhang, N. Xue, and X. Huang, "A secure system for pervasive social network-based healthcare," *IEEE Access*, 2016.

[32] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.

[33] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," in *Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on*. IEEE, 2015, pp. 184–191.

[34] ——, "The IoT electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications*, pp. 1–12, 2016.

[35] F. Tian, "An agri-food supply chain traceability system for china based on RFID & blockchain technology," in *Service Systems and Service Management (ICSSSM), 2016 13th International Conference on*. IEEE, 2016, pp. 1–6.

[36] E. Hofmann and M. Rüsch, "Industry 4.0 and the current status as well as future prospects on logistics," *Computers in Industry*, vol. 89, pp. 23–34, 2017.

[37] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Applied Energy*, vol. 195, pp. 234–246, 2017.

[38] H. Huang, X. Chen, Q. Wu, X. Huang, and J. Shen, "Bitcoin-based fair payments for outsourcing computations of fog devices," *Future Generation Computer Systems*, 2016.

[39] S. Fujimura, H. Watanabe, A. Nakadaira, T. Yamada, A. Akutsu, and J. J. Kishigami, "BRIGHT: A concept for a decentralized rights management system based on blockchain," in *Consumer Electronics-Berlin (ICCE-Berlin), 2015 IEEE 5th International Conference on*. IEEE, 2015, pp. 345–346.

[40] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, and A. Akutsu, "The blockchain-based digital content distribution system," in *Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on*. IEEE, 2015, pp. 187–190.

[41] R. Dennis and G. Owen, "Rep on the block: A next generation reputation system based on the blockchain," in *Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for*. IEEE, 2015, pp. 131–138.

[42] T. Sanda and H. Inaba, "Proposal of new authentication method in Wi-Fi access using bitcoin 2.0," in *Consumer Electronics, 2016 IEEE 5th Global Conference on*. IEEE, 2016, pp. 1–5.

[43] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on*. IEEE, 2017, pp. 618–623.