EasyChair Preprint

№ 2472

Block chain Technology: Assessment from Application Perspectives

Shashank Saroop

January 27, 2020

Block chain Technology : Assessment from Application Perspectives

Shashank Saroop
Department of Computer Science
Banasthali Vidyapeeth, Rajasthan

Abstract— The termed block chain as being referred as the disruptive innovation in computing. The interest in block chain technology has been increasing since the idea was coined in 2008. Moreover it was observed that after 2008 the block chain technology has been separated from bitcoin to be injected to many other problems related especially to banking, healthcare and some other. In this paper I have done the assessment of various block chain technology related to the current application and discuss the major applications in brief by the help of previous papers.

Terms used: Block chain; Crypto currency; application

INTRODUCTION

A system software c a n be classified into two main approaches based on architectural i.e. centralized and distributed [1]. In centralized system software, 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 node.

Meanwhile, block chain can be seen as a part of the implementation layer of a distributed system software . The data integrity in distributed systems can be achieved and maintained using block chain [2]. Furthermore, block chain could be also considered as a purely peer-to-peer system which is made up of the individual nodes in a network.. The individual nodes try to exploit the system for their own purposes since unknown peers with unknown reliability

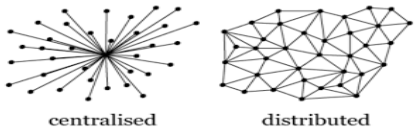


Figure 1: Centralized and Disturbed Network Architecture

and trustworthiness may exist [3]. Thus, these critical problems are needed to be solved by block chain. Along with block chain, Bitcoin was originally invented by Nakamoto [4] as the first and most prevalent crypto currency.

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, block chain 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, block chain 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 block chain structure develop for Bitcoin is portable and extensible

Originally, the main area for block chain is connecting cryptocurrencies with conventional banking and financial institutions. Block chain 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 block chain without the approval of other participants.

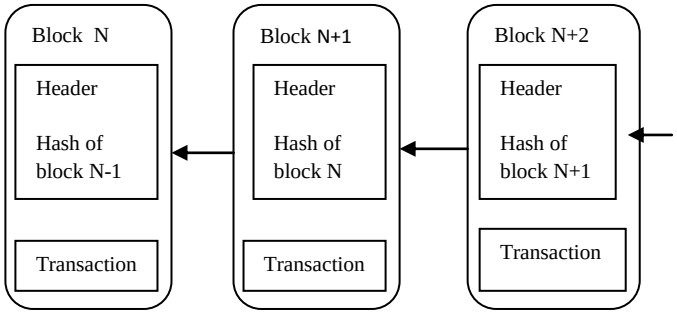
The objective of this paper is to explore the block chain technology and its current applications. The paper classifies the published works found in the literature. Several works in term of review about the block chain technology have been done in [7], [8], [9]. However most of the papers have not considered complete discussion about the block chain applications.

In this paper section-II introduce about the fundamental of block chain technology, Section III introduce about the block chain protocols, Section IV discuss about the implementation of block chain in major areas and finally some concluding remarks are drawn in Section V.

II.FUNDAMENTALS OF BLOCK CHAIN TECHNOLOGY

Block chain 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 added and chained to the previous block using a hash function. Figure 2. Shows the complete illustration of Bitcoin's block chain.

Figure 2. A chain of Blocks



A cryptographic hash function is used to produce a hash. For instance, Bitcoin uses SHA-256, whilst Lit coin [11] and Prime coin [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 block chain 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 block chain is to solve the problems exist in Bitcoin crypto currency, Section III discusses in detail the practical implementation of the block chain for financial transaction.

III. BLOCK CHAIN PROTOCOLS

Block chain eliminates the need for third party to conduct transactions on one's behalf. This implies that the consensus mechanism has to exist in the network itself. How a given block chain network implements its consensus mechanism, determines the strength of the network. A foolproof consensus mechanism, suitable for purpose (of the block chain in question) is essential to maintain sanity and coherence of data among the participating nodes of the network. The consensus mechanisms of block chain aim to eliminate mainly two known problems with digital currency - Remove the problem of double spend and Eliminate Byzantine Generals problem.

While much work has been done on block chain protocols, there are some key algorithms explained in brief here whose variations are being used and further developed to suit various applications of block chain. Cachin et al. have explained block chain consensus mechanism and various consensus algorithms in their research paper [9].

3.1 *Proof of Work*

PoW protocol requires all nodes on the network to solve cryptographic puzzles by brute force. For example, in case of Bitcoin block chain, the new transactions are tentatively committed and then based on the PoW output, a selected block created by the winning node is broadcast to all the nodes, at specific synchronization intervals. Once the block is transmitted using peer to peer communication to all other nodes, the same is included in the block chain and any tentative transactions are rolled back [10]. By rule of probability, the consensus is achieved as 51% of power rather than 51% of people count. Effectively the computing power used by all other nodes except the winning node, is wasted.

3.2 *Proof of Stake*

Proof of stake protocol of block verification does not rely on excessive computations. It has been implemented for Ethereum and certain altcoins. Instead of splitting blocks across proportionally to the relative hash rates of miners (i.e. their mining power), proof-of-stake protocols split stake blocks proportionally to the current wealth of miners. The idea behind Proof of Stake is that it may be more difficult for miners to acquire sufficiently large amount of digital currency than to acquire sufficiently powerful computing equipment. It is also an energy saving alternative [11].

A variation of POS is the Delegated Proof of Stake (DPOS) algorithm. Delegated proof of stake (DPOS) is similar to POS, as miners get their priority to generate the blocks according to their stake. The major difference between POS and DPOS is that POS is a direct democratic while DPOS is representative democratic. Stakeholders elect their delegates to generate and validate a block. With significantly fewer nodes to validate the block, the block could be confirmed quickly, making the transactions confirmed quickly. Meanwhile, the parameters of the network such as block size and block intervals could be tuned by the delegates. DPOS is implemented by Bit shares [11].

3.3 *Practical Byzantine Fault Tolerance*

An approach to deal with the Byzantine Generals problem is the Federated Byzantine Agreement (FBA). In this approach, it is assumed that the participants of the network know each other and can distinguish which ones are important and which ones are not. PBFT (Practical byzantine fault tolerance) is a replication algorithm whi utilizes this principle. Hyper ledger utilizes the PBFT as its consensus algorithm. There are designated validator (primary) nodes that are each associated with a group of nodes. The primary is responsible for multicasting requests to other replicas in its group. A service operation would be valid if it has received approvals from over 1/3 different replicas. Additionally, if a client does not receive the replies, it will send the request to all replicas instead of only sending it to the primary in case the primary is faulty. A primary is responsible for ordering the transaction and each replica commits the transaction in the same order. It has been seen that PBFT or its variations map well to the needs of various organizations like banks, supply chain or payroll systems.

IV. BLOCK CHAIN APPLICATIONS

In this section, the implementation of block chain technology in different areas is thoroughly discussed. Furthermore, various applications have been classified into several groups, i.e. financial services, healthcare, business and industry, and other novel applications.

Financial Service

Block chain has been widely applied for financial transaction which is so-called crypto currency. Nowadays, crypto currencies 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 block chain can be traced back to the genesis block [7] [15].

Crypto currency has its own currency (coin). Mining is the process of introducing a new block into block chain. Each node uses block chain to verify whether the coin is legitimate or if it has not spent already. Before the transaction records are appended into block chain, 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 crypto currency: (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 systems 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.

Healthcare

Block chain has a tremendous potential in addressing the interoperability issues exist in the current healthcare 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 block chain storage platform is proposed by [29]. It is a smart phone 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 block chain cloud is used to stored the data thus ensuring the medical data cann ot 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 block chain. The block chain replicas are distributed on each node in the network. Similar to prior work, block chain 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 block chain [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 block chain 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 block chain 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 block chain-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 block chain 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 block chain. Table II compares the related study of block chain technology for healthcare application.

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 block chain technology. Block chain 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. block chain. 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.

Voting

In the year 2014, a Danish political party was the first to use block chain technology for voting [39]. Online voting platforms such as 'Followmyvote' [40], which enable digitally secure block chain based voting have also been created.

Insurance

Cognizant Technology Solutions give an end-to-end view of how block chain can transform insurance in their perspectives [41]. Travel insurance, crop insurance, property and casualty insurance and most importantly health insurance are all set to change with the use of block chain technology. A multiparty shared network with insurers, hospitals, funeral homes, a department of health and the beneficiary forming the nodes of the block chain, can be created. This setup will provide the necessary disintermediation and speed required for the insurance and claim process to be streamlined and to eliminate frauds.

Smart Cities

A possible application of Block chain to smart cities is suggested by Sun et al. in [42]. Authors relate a smart city to a sharing economy where information and communication technologies are utilized to enhance opportunities of sharing of resources. Author proposes using a block chain based framework for sharing of resources across various services to ensure data immutability, accountability, proper asset utilization and to reduce transaction costs.

Comparative Analysis of Various Applications

In this Section I have done the assessment on the basis of parameters of block chain technology based applications and mainly focus on two important applications which having a vast area for the research perspectives i.e.-"**Healthcare Application**" AND " **Financial Application"**

Table I: Show the analysis of various approaches of healthcare applications

Study and Approach	Year of Introduced	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

Table II. Show the analysis of various approaches of financial application

Crypto currency	Year	Cryptographic Technique	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 Stack
Primecoin [12]	2013	Cunningham chain	Proof of Work
Ripple [18]	2014	EC digital signature	Consenus system
Ethereum [19]	2014	Ethash	Proof of Work
Permacoin [20]	2014	Floating digital signature	Proof of Retreivability
Blackcoin [21]	2014	Scrypt	Proof of Stack
Auroracoin [22]	2014	Scrypt	Proof of Work
Darkcoin [23]	2014	X11	Proof of Work
Namecoin [24]	2015	SHA-256d	Proof of Work

Remarks and Conclusion

Some Research Papers which are related with block chain applications were thoroughly discussed and this papers were chosen from goggle scholar in terms of practical aspects. However the overall literature was searched from the "Block chain". It is obviouous that the number of block chain technology-related papers has increased from year 2008. This paper shows the block chain research and its real-world implementation.

There are tremendous advantages of block chain such as speed, robustness, openness, and so forth. However, block chain 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. Block chain become one of the promising technology in the future if well exploited.

References

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

[2] D. Drescher, "Block chain 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, "Block chains 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, "Block chain 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 Sur-veys & 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 block chain technology?a systematic review," PloS one, vol. 11, no. 10, p. e0163477, 2016.

[10] S. Seebacher and R. Schuritz, "Block chain 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, "Block chain contract: A complete consensus using block chain," in Consumer Electronics (GCCE), 2015 IEEE 4th Global Conference on. IEEE, 2015, pp. 577–578.

[9] Cachin et al. 2017. Block chain, cryptography, and consensus , IBM Research, Jun 2017, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201703/Documents/Christian%20Cachin%20blockchain-itu.pdf

[10] Decker, Wattenhofer. 2013. Information Propagation in the Bitcoin Network, 2013 IEEE Thirteenth International Conference on Peer-to-Peer Computing (P2P). [Online] http://dx.doi.org/10.1109/P2P.2013.6688704

[11] BitFury group. 2015. Public versus Private Block chains Part 1: Permissioned Block chains, BitFury.com whitepapers [Online]: http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf

[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: Re-purposing 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 block chain 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 names-pace design," in Workshop on the Economics of Information Security (WEIS). Citeseer, 2015

[25] M. Mettler, "Block chain 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, "Block chain 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 block chain 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 block chain 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: Block chain-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 block chain 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 & block chain technology," in Service Systems and Service Management (ICSSSM), 2016 13th International Conference on. IEEE, 2016, pp. 1–6.

[36] E. Hofmann and M. Rusch, "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, "Block chain 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] Block chain Voting Used By Danish Political Party, 2014, https://www.cryptocoinsnews.com/block chain-voting-used-by-danish-political-party/

[40] Follow My Vote, Voting solutions to improve integrity of voting: https://followmyvote.com/contact/

[41] Cognizant Technology Solutions, 2017, https://www.cognizant.com/perspectives/how-block chain-can-transform-life-insurance-processes

[42] Sun et.al. 2016. Block chain-based sharing services What block chain technology can contribute to smart cities, Spring[Online].Available: http://dx.doi.org/10.1186/s40854-016-0040-y