View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Springer - Publisher Connector

Zhao et al. Financial Innovation (2016) 2:28
DOI 10.1186/s40854-016-0049-2

Financial Innovation

EDITORIAL Open Access

Overview of business innovations and research opportunities in blockchain and introduction to the special issue

J. Leon Zhao[1*], Shaokun Fan[2] and Jiaqi Yan[3]

* Correspondence:
jlzhao@cityu.edu.hk
[1]City University of Hong Kong, Hong Kong, China
Full list of author information is available at the end of the article

Abstract

Blockchain has become a new frontier of venture capitals that has attracted the attention of banks, governments, and other business corporations. The recent blockchain related attempts included legal blockchains by Fadada.com and Microsoft and pork tracking blockchains by Walmart and IBM. Blockchain is poised to become the most exciting invention after the Internet; while the latter connects the world to enable new business models based on online business processes, the former will help resolve the trust issue more efficiently via network computing. In this paper, we give an overview on blockchain research and development as well as introduce the papers in this special issue. We show that while blockchain has enabled Bitcoin, the most successful digital currency, its widespread adoption in finance and other business sectors will lead to many business innovations as well as many research opportunities.

Keywords: Bitcoin, Blockchain, Business innovation, Public ledger, Computational trust

Introduction

Since Blockchain was originally conceptualized by Satoshi Nakamoto in 2008 as a core component to support transactions of the digital currency – Bitcoin, blockchain has been known to be the public ledger for all transactions and resolved the double-spend problem by combining peer-to-peer technology with public-key cryptography. Literally, a blockchain is a chain of blocks of information that registers Bitcoin transactions; of course, there is a stringent set of rules that govern how to verify the validity of the block and make certain that the block will not be altered or disappear. The algorithms and the computational infrastructure of creating, inserting, and using the blocks are considered as the blockchain technology.

While Blockchain was born with Bitcoin, its applications have gone far beyond Bitcoin or digital currency. Many people believe that blockchain could revolutionize many fields, such as finance, accounting, management, and law leading to three generations of blockchains, namly, *Blockchain 1.0 for digital currency, Blockchain 2.0 for digital finance,* and *Blockchain 3.0 for digital society*. Interestingly, Blockchain 1.0 took a few years to mature starting from 2008, Blockchain 2.0 and 3.0 have emerged almost in parallel in an explosive manner around 2015. Nevertheless, while many experimental projects

Springer Open

© The Author(s). 2016 **Open Access** This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

have mushroomed, it will take some years for Blockchain 2.0 and 3.0 to take hold and create real economic impacts.

According to the search volumes of Bitcoin and blockchain in Fig. 1, Bitcoin had most of the search queries before the year of 2014. While blockchain was not very well recognized with the wave of Bitcoin, it is getting more and more attention from people in many industries recently.

While blockchain has been generating enormous impacts to many aspects of our life, research on blockchain technology is still sparse. We conducted a search of "blockchain" in the Web of Science search engine provided by Thomson Reuters and got only 15 published articles in total (As of 11-30-2016). The earliest publication was in 2015, which is just one year before this special issue. We also searched the SSRN database which may include mainly works that are research-in-progress. In total, we found 107 papers that are published in SSRN (As of 11-30-2016). Similar to the Web of Science data, most of these papers are published in the year of 2015 and 2016. The detailed numbers of papers published in both Web of Science and SSRN are shown in Table 1.

Blockchain research

The blockchain technology solves the double-spend problem with the help of public-key cryptography, whereby each user is assigned a private key and a public key is shared with all other users. The main idea of blockchain is a distributed database comprising records of transactions that are shared among participating parties. Each and every of these transactions is verified by the consensus of a majority of the participants in the system, making fraudulent transactions unable to pass collective verification. Once a record is created and accepted by the blockchain, it can never be altered. Existing research on blockchain has been mainly focused on system efficiency, security and innovative applications.

By design, efficiency is one of the most important concerns for blockchain. Blockchain requires a very strict verification process to create a new transaction record, which leads to a significant latency of confirmation time and waste of computing resources. Currently, it takes about 10 min for a transaction to be confirmed. In addition, thousands of nodes are running to compute and verify transactions. These issues limit the scope of blockchain applications to a large extent. For example, current blockchain techniques are generally not suitable for the Internet of Things (IoT) network, because IoT devices may have to work with low computational capability or very low power (Atzori 2016).

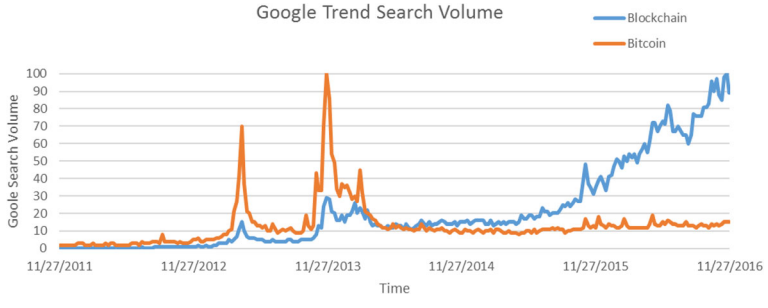

Fig. 1 Google Trends Search Volume (A value of 100 is the peak popularity, and a value of 50 means 50% of the peak search volume)

Table 1 Number of academic papers on blockchain

Year	WebOfScience	SSRN
Before 2014	0	0
2014	0	6
2015	4	22
2016	11	79

Some pioneer work has been done to improve the efficiency of blockchain. Zyskind et al. (2015) proposed a lightweight blockchain architecture to protect personal data. They improved the efficiency of blockchain by using off-chain data storage and heavy processing. Only references to data and lightweight processing tasks were handled in the blockchain. Paul et al. (2014) proposed a new scheme that could lead to an energy-efficient Bitcoin. The authors modified added some extra bytes to the present block header to utilize the timestamp more effectively.

Blockchain technology includes several preventive mechanisms (e.g., distributed consensus and cryptography) to reduce risks of cyber-attacks. According to Underwood (2016), immutability and other features to secure transaction are the top benefits considered by early adopters of blockchain in the finance sector. However, blockchain has been identified to be vulnerable to many types of attacks. The 51% attack is unique to blockchain and it happens when a single node controls more than half (51%) of processing power of the blockchain. The node can dominate all other nodes, manipulate the records in a the blockchain (Yli-Huumo et al. 2016). According to an analysis of the trend of security breaches in Bitcoin (Lim et al. 2014), the authors found that many security breaches had occurred, including DDoS attacks and private account hacking. Furthermore, privacy and confidentiality is still a problem with blockchain, because all the nodes of the blockchain have access to all the data (Atzori 2016).

The financial service sector, which must be innovate to cut transaction costs due to severe competitions in today's globalized economy, is leading the way with blockchain-related business innovations. Blockchain has been proposed as an innovative solution to areas such as clearing and settlement of financial assets, payment systems, smart contracts, operational risks in financial market, and so on (Kakavand et al. 2016; Peters and Panayi 2015).

One notable example of blockchain application in the financial market is chain.com, which is a startup backed by NASDAQ (Crosby et al. 2016). They aim to provide a platform for private equity exchange on top of BlockChain. In non-finance sectors, the applications of blockchain are getting more and more attention. In 2015, the Bitcoin Foundation started a new project that aims to develop a blockchain-based voting system, which "provides even greater transparency into the voting process, with every vote being recorded on the blockchain".

In supply chain management, blockchain technology provides a groundbreaking solution to product provenance (Kim and Laskowski 2016). A shared, consensus-based public ledger is used to track the origin and the processes in the supply chain. Other examples of blockchain applications are digital right ownership management, notary services, and so on (Crosby et al. 2016).

In summary, the blockchain technology is still at an early stage of development and further research is needed to enhance its efficiency and security. Researchers are confronted

with many opportunities as well as challenges to make blockchain successful in various business domains as illustrated by the seven papers in this special issue that explore the contemporary theories or state-of-the-art technologies of blockchain.

Blockchain, as an emerging technology, has been considered to be a new means to deal with the needs of people, technology, and organization. As shown in Fig. 2, blockchain research is expected to address the issues of trust, sharing, and privacy as part of human society. Trust has become a very important feature that blockchain can provide for a transaction. With new trust mechanisms arising from Blockchain, people may be able to share their properties without the concerns of losing privacy.

Underlying the blockchin technology, the organization of a business community can be decentralized, peer to peer, and coalition. The Bitcoin system has provided a practical example of a decentralized organization that there is not any central authority to control the issue and maintenance of the Bitcoin system. The relationships between nodes in the blockchain system is in the form of peer to peer. In addition, blockchains may unite, vote, and form coalitions.

The technological components underlying the blockchain system include trustless computing, smart contract, and network security. Trustless computing is the foundation to reach a consensus in a decentralized blockchain system. With the smart contract, an organization can be autonomous based on the autoexecution of codes as people do not need to worry about the trust issue. These features are built on network security, with which people can trust the system for business transactions.

To address the issues of blockchain adoption in a business environment, three levels of studies may be carried out by researchers, including conceptual, prescriptive, and descriptive levels (Iivari et al. 2010). Currently, business research in blockchain is found mainly in the conceptual level that conceptualize blockchain innovations in business and in the prescriptive level that outlines business applications of blockchain. Research in the descriptive level is lagging as it takes more efforts to uncover

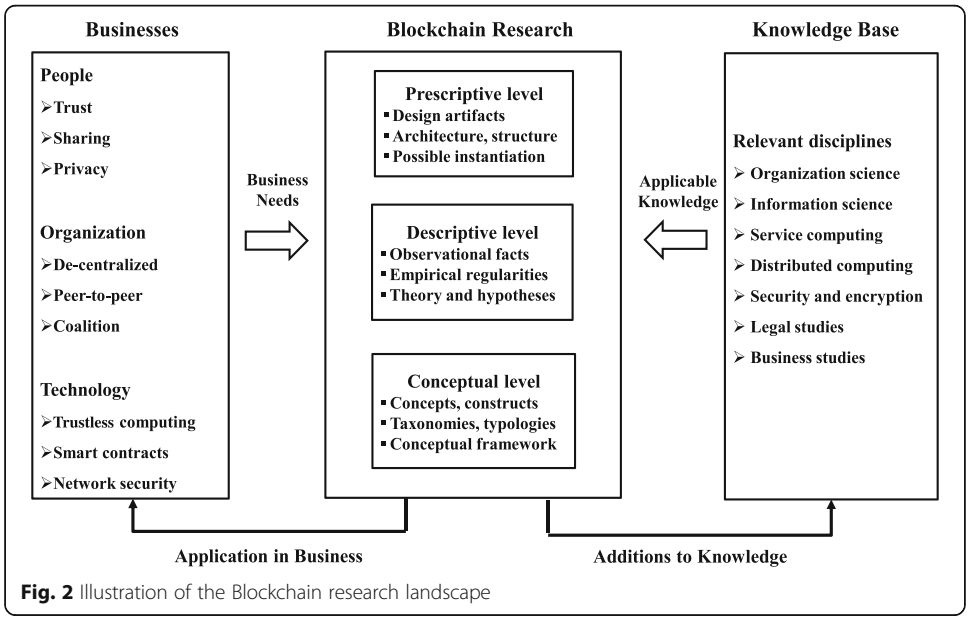

Fig. 2 Illustration of the Blockchain research landscape

new explanations and theories underlying blockchain phenomenon. For instance, there is a need to ascertain the economic and social validity of blockchain applications.

Blockchain research comes from various relevant disciplines. A partial list of such disciplines are shown in Fig. 2 to address scientific, business, and technological issues of blockchain applications. Initially, research in blockchain starts with technical and business issues, and more disciplines will be involved as the impacts of blockchain permeate deep into society and governments.

Articles included in the special issue

This special issue is the fifth issue of Financial Innovation (FIN), Volume 2, No. 3 (2016). It presents seven papers contributed by 14 authors and co-authors from three countries and areas: Australia, China and USA. The seven papers explore the contemporary theories or state-of-the-art technologies of blockchain for addressing challenges in today's global business environment with big data. Next, we introduce the seven articles of this special issue in no particular order.

1) As the technological capacity of the blockchain is being harnessed by companies to address real-world problems, it is important to understand the guidelines for adopting this revolutionary system. IT maturity model has long been applied to evaluate and guide software development processes. However, due to the unique social and technical features of blockchain, how to evaluate and guide blockchain development has been fully covered in previous literature. This is the issue addressed by Wang et al. (2016) in his paper, "A maturity model for blockchain adoption". Using a comparative analysis method, Wang et al. proposes a five-stage maturity model with four dimensions for blockchain system adoption. A progressive procedure is also proposed to guide the adoption of blockchain systems.
2) One of the most attractive features of blockchain is its security mechanism based on public ledger and distributed consensus. However, this does not mean that blockchain can resist any types of fraud and hacking. In her paper, "Are Blockchains Immune to All Malicious Attacks", Xu (2016) explores the types of fraud and malicious activities that can be prevented by blockchain technology and identifies attacks to which blockchain remains vulnerable. She also recommends appropriate defensive measures for fighting malicious activities that may compromise the security of blockchains.
3) While blockchain has captured attention of people from many industries such as property management, auditing, and copyright protection, finance has been the first and most important application area of the technology so far. In their paper, Zhu and Zhou (2016) propose to use Blockchain to address some critical issues in equity crowdfunding in China, which is an emerging field of Internet Finance. Based on their analysis, blockchain can help achieve efficient and low-cost equity registration, equity transaction and transfer, and shareholder voting in the crowdfunding industry, eliminating legal risks related to fund management. It can also help regulators supervise and understand the crowdfunding market.
4) Many people believe that blockchain will become the next generation technology that can revolutionize banking industry. It is still not clear that which specific areas of banking businesses can benefit the most from this disruptive technology. In the

paper titled "Blockchain Application and Outlook in the Banking Industry", Guo and Liang (2016) propose that payment clearing system and bank credit information systems can be the appropriate scenarios of blockchain application. The blockchain technology can be used to solve issues such as lack of mutual trust, high transaction cost, and fraud.

5) The development of smart cities benefits from innovative applications of new information and communication technologies. People are wondering what the blockchain technology can contribute to make a smart city. Sun et al. (2016) investigate this question from a sharing economy perspective. They explore a set of fundamental factors that make a city smart, and discusses what the emerging blockchain technology may contribute to these factors.
6) Blockchain was originally invented to support the operation of the digital currency (Bitcoin), which is still considered as the most successful application of blockchain so far. However, the well-known 51% attack is a major security concern of blockchain based system. In the paper titled "A New Proof-Of-Work Mechanism for Bitcoin", Shi (2016) proves that the computing power in Bitcoin system can be concentrated in a single node under the current proof-of-work design. He also proposes a new proof-of-work mechanism that encourages more nodes to participate in bitcoin mining and reduces the risk of 51% attack.
7) In the cyber world, people often make transactions with others that they have not met with. Reputation systems have been widely used in the cyberspace as an effective way to allow people to evaluate the trustworthiness of a potential seller. However, current reputation systems are vulnerable to fraud rating and the detection of fraudulent raters is difficult since they can behave strategically to camouflage themselves. This is the problem addressed in the paper "Fraud Detections for Online Businesses: A Perspective from Blockchain Technology", by Cai and Zhu (2016). They explore the potential strengths and limitations of blockchain based reputation systems under two attack goals: ballot-stuffing and bad-mouthing. They find that Blockchain systems are effective in preventing bad mouthing and whitewashing attack, but they are limited in detecting ballot-stuffing under Sybil attack, constant attacks and camouflage attack.

While these seven papers are quite interesting to read, they are by no means free from ambiguities, oversights, and even misconceptions. However, it is the nature of research, particularly in the exploratory stage, that researchers venture into unknown areas with their best of abilities. Regardless, this special issue offers readers interested in business research about blockchain a convenient place to get started. We hope that they will open the eyes of other researchers and help them to decide if they will join this great effort.

Concluding remarks

While many blockchain development projects are emerging, research in blockchain is in its infancy. This paper outlines research opportunities in exploring and validating blockchain applications in business that may involve many relevant disciplines. In particular, challenges remain to study blockchain related theoretical issues that will guide blockchain ventures towards dramatic societal impacts by trading manual control

with network computing, the corner stone of blockchain-based transactions. In addition, smart contracts embedded in business blockchains will revolutionize many industries that enable automatic business transactions that previously involve heavy human interventions. For instance, a combination of digital locks and smart contracts in blockchain-based transactions will enable renting hotel rooms without human intervention.

Nevertheless, many challenges remain in harnessing the power of blockchain to make the Internet more trustworthy. For instance, while the original value of blockchain is to decentralize organizations by running Bitcoin transactions with a bank, new blockchain applications are more likely applied in centralized or partially centralized organizations such as a national bank. It remains to be seen how a decentralized mechanism such as blockchain can be used to automate business operations in a centralized environment, which can be characterized as centralizing a decentralized mechanism.

In any event, if the prophecy of blockchain will become reality, i.e., the transformational power of blockchain to enable global trust among people parallels the transformational power of Internet to connection people globally. *The essence of blockchain lies in its ability to support trustworthy transactions via networked computation in place of human monitor and control.* It would be quite exciting for researchers to participate in realization of blockchain impacts, and inevitably, we will see more business research in blockchain in the next few years.

Author details
[1]City University of Hong Kong, Hong Kong, China. [2]Oregon State University, Corvallis, USA. [3]Nanjing University, Nanjing, China.

Received: 4 December 2016 Accepted: 4 December 2016
Published online: 15 December 2016

References

Atzori, Marcella, Blockchain-Based Architectures for the Internet of Things: A Survey (2016). Available at SSRN: https://ssrn.com/abstract=2846810
Cai Y, Zhu D (2016) Fraud Detections for Online Businesses: A Perspective from Blockchain Technology. Financial Innovation
Crosby MA, Pattanayak P, Verma S, Kalyanaraman V (2016) BlockChain Technology: Beyond Bitcoin. Applied Innovation, No. 2, pp. 6–10
Guo Y, Liang C (2016) Blockchain Application and Outlook in the Banking Industry[J]. Financial Innovation
Iivari J (2010) Twelve theses on design science research in information systems, in Design Research in Information Systems, Theory and Practice by Hevner, Alan, and Chatterjee, Samir, Springer, US, pp. 43–62
Kakavand, Hossein and Kost De Sevres, Nicolette (2016) The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies, Luther Systems. Available at SSRN: https://ssrn.com/abstract=2849251
Kim, Henry M. and Laskowski, Marek (2016) Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance. CoRRabs/1610.02922
Lim IK, Kim YH, Lee JG, Lee JP, Nam-Gung H, Lee JK. (2014) The Analysis and Countermeasures on Security Breach of Bitcoin. In International Conference on Computational Science and Its Applications. Springer International Publishing, pp. 720–732
Paul G, Sarkar P, Mukherjee S (2014) Towards a More Democratic Mining in Bitcoins. In: Prakash A, Shyamasundar R, editors. Information Systems Security. vol. 8880 of Lecture Notes in Computer Science. Springer International Publishing, Switzerland, pp. 185–203
Peters GW, Panayi E (2015) Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. Available at SSRN: https://ssrn.com/abstract=2692487
Shi N (2016) A New Proof-Of-Work Mechanism for Bitcoin[J]. Financial Innovation
Sun J, Yan J, Zhang K (2016) Blockchain-based Sharing Services: What Blockchain Technology Can Contribute to Smart Cities[J]. Financial Innovation
Underwood S (2016) Blockchain beyond bitcoin. Commun. ACM 59, 11 (October 2016), 15–17
Wang H, Chen K, Xu D (2016) A maturity model for blockchain adoption[J]. Financ Innov 2(1):12
Xu J (2016) Are Blockchains Immune to All Malicious Attacks? [J]. Financial Innovation
Yli-Huumo J, Ko D, Choi S, Park S, Smolander K (2016) Where Is Current Research on Blockchain Technology – A Systematic Review. PLoS ONE 11(10), pp.1–27
Zhu H, Zhou Z (2016) Analysis and Outlook of Applications of Blockchain Technology on Equity Crowdfunding in China[J]. Financial Innovation
Zyskind G, Nathan O, Pentland A (2015) Enigma: Decentralized Computation Platform with Guaranteed Privacy. arXiv preprint arXiv:1506.03471