Service Oriented Computing and Applications (2019) 13:279–285
https://doi.org/10.1007/s11761-019-00281-x

INTRODUCTION

Emerging blockchain-based applications and techniques

Yinsheng Li[1]

Published online: 22 November 2019

Abstract
The primary mission of the blockchain is to establish a creditworthy ecosystem among independent participants in a non-trustable distributed environment. A blockchain system is secure and autonomous based on its chained blocks, peer–peer nodes, consensus-based ledger mechanism, anonymous accounts, self-regulated data ownership, and programmable smart contracts. There are continuous arguments at which features from Bitcoin are fundamental for blockchains and what are changeable. Furthermore, a devoted credit system is required to make blockchain systems creditworthy although blockchains provide a creditworthy infrastructure for data-level storage and operations. The necessity, feasibility, efficiency, and expected benefits are crucial factors to evaluate a blockchain venture. Several popular and promising blockchain techniques are under-developed; among them are those for blockchain creditworthiness, performance, efficiency, security, privacy, supervision, and online-to-offline integration. A new prosperity of the blockchain is on its way since two symbolic projects, the Libra by Facebook and the DCEP by Central Bank of China, were announced.

Keywords Blockchain · Smart contracts · Ecosystem · Autonomous · Creditworthiness · DCEP · Libra

1 Introduction

The primary mission of blockchains is to establish a creditworthy ecosystem among independent participants in a non-trustable distributed environment. A blockchain system is secure and autonomous based on its chained blocks, peer–peer nodes, consensus-based ledger mechanism, anonymous accounts, self-regulated data ownership, and programmable smart contracts. Furthermore, the devoted credit mechanisms are required to make blockchain systems to be creditworthy although blockchains provide a creditworthy infrastructure for data-level storage and operations.

The first work on a cryptographically secured chain of blocks was published in 1991 by Stuart Haber and W. Scott Stornetta. The blockchain design was improved by a Hashcash-like method to timestamp blocks in a paper ‘Bitcoin: A Peer-to-Peer Electronic Cash System,’ under the name of Satoshi Nakamoto [1]. The blockchain was implemented as a public ledger in open-source Bitcoin software for all transactions on the cryptocurrency by Nakamoto [2]. It is the cryptocurrency Bitcoin that brings acceptance and prosperity of the blockchain-based technologies and applications, while it is the blockchain technologies that make Bitcoin a revolutionary financial model. The Bitcoin system does not need issuance authorities of the coins, which are generated on a blockchain consensus mechanism. Theoretically, Bitcoin can neither be shut down nor be investigated from outside of the system because of blockchain’s distributed ledger and anonymity mechanisms. As a result, Bitcoin and hundreds of derived cryptocurrencies have seen their successes since 2015. Thousands of ICO (Initial Coin Offering) programs were hastened around the industries and the world though most of them have been closed because of business infeasibility or official prohibitions.

Despite how Bitcoin booms or slumps, the blockchain technologies and application scenarios are continuously innovated and improved. Its ecological architecture, operation mechanisms and database models are getting well accepted, while the business features from Bitcoin are filtered out. Basically, a blockchain can be envisioned as a decentralized, distributed, and public digital ledger, which is proposed to record transactions across many peered nodes so that the records cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network [2]. The blockchain-based smart contracts

✉ Yinsheng Li
liys@fudan.edu.cn

[1] Software School, Fudan University, Shanghai 200433, People’s Republic of China

are proposed to be partially or fully executed or enforced without human interaction [3]. The blockchain and smart contracts enable the data and transactions to be recorded as they really are and not being altered nor tampered, which are competent in principle to build a secure data infrastructure and credible system. Therefore, it is on the basis of security and creditworthiness that all the potential blockchain-based applications are pursued and developed.

Another period of blockchain prosperity is on its way since the two symbolic projects, the Libra by Facebook and the DCEP by Central Bank of China, are going to be launched [4, 5]. Both projects are ambitious to provide anonymous digital wallets without bank accounts and make new electronic payment infrastructure across the world. The two grand ventures are destined to make tremendous impacts on transnational financial systems and international politics. Compared with the ownerless Bitcoin project, the two projects have been developed with tremendous resources and by most powerful groups either in America or China. Considering what the Bitcoin has made in the past few years, both the Libra and DCEP are becoming undoubtedly powerful catalysts for much more blockchain-based technologies and applications, which are changing the world.

2 Emerging blockchain-based applications

2.1 Best-fit application scenarios and models

The best-fit blockchain-based applications are elaborated to well exploring the reliability, immutability, and openness with blockchain technologies. There is not any superior participant in a blockchain system, in which transactions are recorded anonymously and cannot be altered or tampered. It is a prerequisite that the blockchain systems can address some pain spots with the subject scenarios, generally, through transforming a non-trustable environment to a creditworthy environment based on the blockchains.

As a distributed ledger, a blockchain system can be developed to be an ecosystem with blocks as its infrastructure, which is distributed not only at its architecture, but also at its data and operation rights. The ledger of the ecosystem is composed of a number of distributed peer nodes. The participants of the ecosystem are peer entities with equal privileges to each other. The data of the ecosystem records are private and self-regulated to decide which participants can receive and view.

There are tens of thousands of blockchain-based application systems have been developed for smart contracts, notarization, asset trading, bank clearance, ecommerce, social communication, Internet of Things, storage, data API, finance, to provide data-level, business-level, or service-level infrastructure. Many of them are shut down in a few years due to low necessity, feasibility or performance along with business operation issues. There are several basic concerns to be addressed when evaluating a blockchain venture, as shown by Fig. 1. Why is it necessary? How many benefits are expectable for the participants? What about its performance? Is it operable to start up? Furthermore, what are the innovations by introducing blockchains?

2.2 Blockchains for cryptocurrency and payment

It is the cryptocurrency Bitcoin that brings acceptance and prosperity of the blockchain-based technologies, as the blockchains provide secure, open, and decentralized transaction infrastructure for Bitcoin. Since then, thousands of Bitcoin-like or Bitcoin-derived projects have been launched. The numerous ICO (Initial Coin Offering) programs were prevailing for the time across the world. Most of the blockchain concepts are developed from the Bitcoin blockchain, and cryptocurrency and payment ventures are still emerging to be the most popular application areas, despite the fact that very few of them survive and Bitcoin is illegal in some countries.

Recently, two influential projects, the Libra by Facebook and the DCEP by Central Bank of China, are announced to be launched. The two projects are ambitious to provide anonymous digital wallets with no bank account, and make new electronic payment infrastructure across the world. The Libra is announced as a stable currency built on a secure and stable open-source blockchain, backed by a reserve of real assets, and governed by an independent association [4]. The DCEP currency is issued and endorsed officially by China Central Bank [5]. The two grand visions are destined to make tremendous impacts on transnational financial systems and international politics. Compared with the autonomous Bitcoin system, the two projects have been developed with tremendous resources and by most powerful groups either in America or China. Considering what the Bitcoin has made in the past few years, both the Libra and DCEP are becoming undoubtedly powerful catalysts for much more

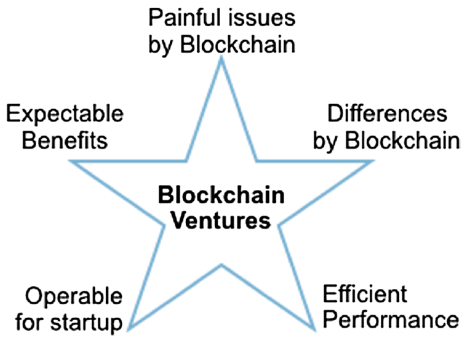

Fig. 1 Five concerns with a blockchain venture

blockchain-based technologies and applications, which are changing the world.

2.3 Blockchains for product tracing

The blockchain technology is best fit for reliable activity tracking. A blockchain-based application in the healthcare sector was proposed to reduce prescription drug fraud, integrate the medical information, and connect the dental industry. The blockchain is used to solve the problems that medical information is frequently held by individual providers or private data collectors without full patient access. The authors believe blockchains can make an effective and trustable tracking of transactional information at each step of a process in a transparent and immutable way [6].

Several commercial blockchain IoT solutions have been put into the market. For example, IBM Blockchain IoT is developed to make the transactions between things trustable. Within an IoT construct, blockchain can build a trusted and efficient business network based on shared ledger, reduce cost of creating, maintaining and enforcing contracts based on smart contract, produce a permanent or indelible record based on IoT device data, and accelerate transactions through IoT events to trigger smart contract execution directly [7]. Another example is RAIN RFID-IoT Tracking Services, which enable item-level tracking services both in-store and supply chain [8].

Furthermore, it is popular to use the blockchains to make anti-counterfeit solutions in that authenticity of products is verified by the blockchain network consisting of all market participants in electronic commerce (producers, merchants, and marketplaces) [9].

2.4 Blockchains for supply chains

The supply chain is one of the best-fit areas for blockchains as there are multiple entities in a supply chain and need a creditworthy mechanism to cooperate for a business. The blockchain ecosystem can be developed to provide secure, creditworthy, and complete information among the supply chain members to avoid cheating or commercial abusing. The creditworthy data are helpful for small and medium enterprises to get financial services, which is a painful issue with traditional industries. Also the author learns from some interviews and cooperative projects with industry partners that a number of blockchain projects have been underdeveloped in China to increase the efficiency of finance audit and solve the financial issues of the small enterprises. As illustrated by Fig. 2, the finance agency can lend money to the small suppliers and service providers due to creditworthy purchase orders. Several finance blockchain projects for supply chain can be found at information websites [10].

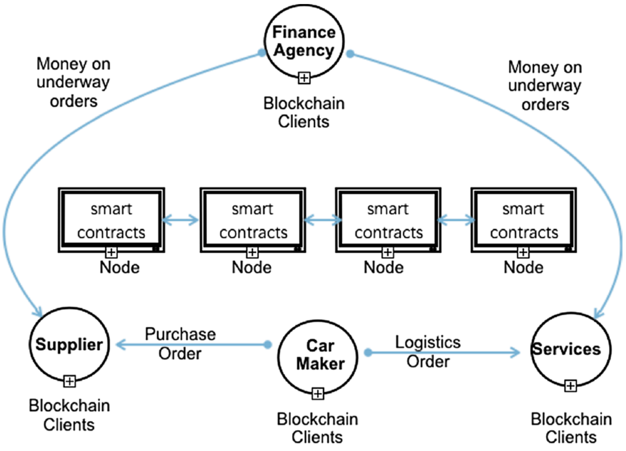

Fig. 2 A blockchain ecosystem for car supply chain

Further, with smart contracts, blockchains have the potential to make more secure and trustable trades or collaborative business among a supply chain. Smart contracts can be used to compose the entire transaction process and automatically executed in a cost-effective, transparent, and secure manner [11]. For example, a blockchain-based production credit mechanism (PCM) for manufacturing services is put forward to regulate the cross-enterprise collaborations among socialized manufacturing resources [12].

2.5 Blockchains for business applications

The blockchains are supposed to be applicable at many business areas though most of the ventures have failed as mentioned above. A feasible application scenario is the key for a feasible blockchain application. The scenario should be elaborated to explore the unique blockchain features, and follow invented business rules within the evolved instead of the conventional business environments. It is encouraging that numerous attempts and ventures are under development around the world.

On the blockchain-related information websites, you may find thousands of blockchain projects for tens of application areas [10]. Also, some blockchain attempts in can be found in the literature. For example, a scientific information blockchain system is proposed to lower the costs at scientific information access and make it open and universal. The intention is to make larger parts of the research cycle open to self-correction [13]. A global higher education credit blockchain platform is proposed to constitute a globally trusted, decentralized higher education credit, and grading system that can offer a globally unified viewpoint for students and higher education institutions, as well as for other potential stakeholders [14]. A digital identity blockchain ecosystem is developed to create secure and trusted digital identities to reduce identity theft and improve public safety, which allows citizens to carry out high-value and daily transactions online [15].

2.6 Blockchains for public services

The existing credit systems are not well recognized because of separate brokerage systems, non-pertinence, centralized and static evaluation models, and insufficient supporting information. The authors have been developing creditworthiness-related projects since 2009 and proposed an autonomous credit system to exploit potential feasibility and performance that the blockchain and smart contracts may make for online trading [16]. The autonomous blockchain system is envisioned as the next generation of credit system in that it is trading-oriented and to match all the trading-related participants. It is developed to be an integrated, traceable, dynamic, and personalized blockchain ecosystem. The goal is to make the participants and transactions credible besides credible data in a blockchain system. It, therefore, supports creditworthy business commitments, with life-cycle and multimedia tracing information while no dependency on any credit brokerages.

3 Advances at blockchain techniques

3.1 Underdeveloped blockchain techniques

The pioneer blockchain project, cryptocurrency Bitcoin, is surrounded by numerous skeptics as most of the deviated cryptocurrency projects have failed except those forked from Bitcoin. A large portion of blockchain applications have been aborted, and there is not yet any blockchain project found successful to its efficiency at other application scenario. However, blockchain-raised magic ideas are so attractive that people would never give up. Numerous researches have been conducted to improve or innovate its core techniques or discover feasible and efficient use scenarios around the world. In the following are a number of popular and promising blockchain techniques; among them are those for blockchain creditworthiness, performance, efficiency, security/privacy, supervision and online-to-offline integration. The underdeveloped techniques are objective to address the critical issues that block the acceptance and development of blockchain systems.

The blockchains are secure but not creditworthy. The devoted credit mechanisms are required to make blockchain systems to be creditworthy although blockchains provide a creditworthy infrastructure for data-level storage and operations. An autonomous credit system is proposed by the author [16]. It is trading-oriented to satisfy all the involved trading participants. A blockchain creditworthiness ecosystem is developed to implement the credit system as it provides an open, equal, and creditworthy infrastructure. And it is through a collection of smart contracts that all the blockchain operations are processed. A creditworthiness model is developed to implement the credit system to make it more integrated, traceable, dynamic, and personalized. Several pilot projects have been developed to test the feasibility and efficiency of the proposed autonomous credit system. Four creditworthiness clouds have been developed as public blockchain clients and creditworthiness query services.

Networking models of blockchain. Four types of blockchain networks have been identified, including public blockchains, private blockchains, consortium blockchains and hybrid blockchains. Public blockchains are difficult to be feasible, while private blockchains do not manifest their technical potentials. Most of the ongoing projects use consortium or hybrid blockchains, which take some centralized mechanisms and some decentralized mechanisms [17]. For example, Welink is a public blockchain network, which is composed of a public blockchain called 'Welink Chain,' open 'Welink AppChainss' and blockchain called 'Wel-Wallet' [18]. The mentioned Libra by Facebook and the DCEP by Central Bank of China can be classified to be hybrid, though the DCEP is declared to only take the blockchain core and some of its blockchain features. For now, what features from Bitcoin are fundamental for blockchains and what are optional or changeable is always a popular argument and not yet got concluded. For example, should a blockchain system be supervised or not? The Bitcoin, Libra, and DCEP have their different views, as shown in Fig. 3.

Many improvements in the blockchain techniques are needed, which are blockchain's online security, and the energy efficiency of proof-of-work public blockchains was found grossly inadequate [19]. New methods are required to develop audit plans that identify threats and risks [20]. The following are a number of basic techniques for critical blockchain issues: (1) distributed computing techniques with basic blockchain networks such as CAP theorem, FLP

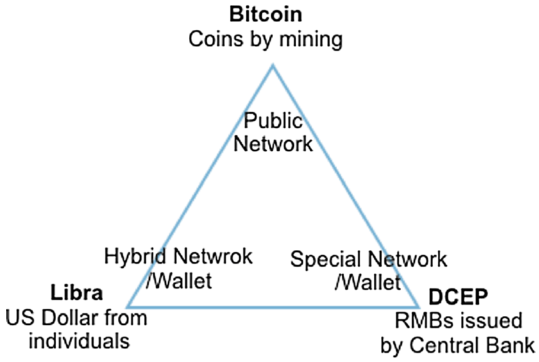

Fig. 3 Features of BitCoin/Libra/DCEP

impossibility theorem, ACID principle, and Paxos/Raft. (2) Specialized techniques for blockchain networks, such as consensus mechanism, Byzantine problems, and algorithms, secure multi-party computation. (3) Specialized techniques for blockchain data mechanisms such as decentralized storage, blockchain data structure, attribute-based encryption, zero-knowledge proof.

With boosting blockchain ventures, application-driven blockchain techniques have been developed to meet particular business features, and a variety of business-level techniques for blockchain-based applications have been delivered. The business-level techniques further boost and improve the fundamental blockchain techniques to make complete system solutions to the blockchain applications. In a joint project in which the authors have a part, it is for an autonomous creditworthy trading ecosystem that all layers of the blockchain techniques are research subjects and developed. To support efficient and complicate trading scenarios, the blockchain infrastructure is improved to explore interconnected blockchain networks with multi-layer and primary-secondary relationships, to define product-oriented block data structure, to replace the blockchain-layer proof-of-work with business-layer incentives, and to develop blockchain gateways and internetwork consensus mechanisms to connect multiple blockchain networks. For unmanned trading, smart contracts techniques for secure verification and interactive models are to be developed. Further special data processing techniques are developed to integrate data from outside and inside the blockchains, and address the data scarcity and insufficiency raised by self-regulated blockchain data.

3.2 Implementation techniques for blockchains

There are several critical issues to be addressed to implement a feasible and efficient blockchain application ecosystem. From the view of a software system, a typical blockchain ecosystem has four layers, including the blockchain, smart contracts, services, and user interfaces. The critical implementation issues for an ecosystem are to design network model, ecosystem architecture, participants and admission policies, nodes and polling mechanism, incentive mechanism, smart contracts, and clients. Furthermore, data collection and data processing algorithms are required to address the critical issues with blockchain applications.

The blockchain network model is a challenge for most of the current projects. The blockchain techniques are fast evolving, and no well-accepted technical specification has been released. Some projects following Bitcoin have not got acknowledged due to their in-efficiency and performance cost. Some only take blockchain as a distributed database infrastructure. More projects are designed with self-designed hybrid networks or variation network models.

A typical blockchain ecosystem is composed of a blockchain infrastructure, the participants' information systems with programming interfaces to the blockchain, and a collection of smart contracts for operation. Among them, the blockchain provides a decentralized and self-regulating data infrastructure in which all data and transactions are stored. The participants' information systems are developed to be blockchain clients, and are able to retrieve or upload business data on the blockchains.

Participants should be identified based on the blockchain network and their role. The number of nodes and evolvement policies are defined based on the polling mechanism and operation objectives. In the case of consortium blockchains, the admission policies and required information are designed based on the network model. A reasonable and efficient incentive mechanism should be developed to make the blockchain prevailing, and design an efficient consensus mechanism.

Smart contracts are well accepted as the greatest enabling technology for blockchains. With them a blockchain ecosystem becomes autonomous, open, consent, and credible. It is through a collection of smart contracts that the blockchains can operate without human intervention. The smart contracts are developed to deploy at the predefined blockchain nodes. They can be invoked by the callbacks either from the blockchain system, the other smart contracts, or the participants' information systems. Generally, both the blockchain operations and application-related rules can be programmed as smart contracts.

Blockchain clients for participants. There are three types of blockchain clients, which interact with the blockchain ecosystem through application programming interfaces. The first type of clients are developed in the participants' information systems; among them are both the management information systems and the embedded systems. The second type of clients are smart contracts or those provided by the blockchain operation system, such as the blockchain browsers. The third type of clients are public facilities by the blockchain, which provides a public user interface for both the participants and potential participants.

Data collection techniques are critical to support blockchain-based businesses. It is considered that the data are private and self-regulated by the participants in a blockchain, which raises several popular issues at collecting data; among them are data insufficiency, data scarcity, and data redundancy. It is necessary to develop well-defined compensation algorithms for missing data, attributes, and irrelevant or redundant data. At the same time, cross-checking and weighting algorithms should be developed to exploit the integrated participation information from inside and outside the blockchain, on blockchain and off blockchain, which could be developed as smart contracts to collect the integrated information. There are further some other concerns to be considered when processing the data. For example, it is required to address how to use the data from other blockchain ecosystems. After all, the ecosystem is developed to integrate inside and outside of the blockchain, and the requester may come from the other blockchain ecosystem.

3.3 Application development environments for blockchains

There are tens of general-purpose blockchain development environments released as open sources. The Bitcoin Blockchain is the first player from 2008, with the new concepts of Bitcoin, miner, proof-of-work, transaction, and permissionless [21]. The Ethereum Blockchain is derived from Bitcoin and prevails since its beginning, with which the concepts are Ether, Ethereumminer, proof of stake, account, permissionless [22]. Hyperledger Blockchain has been developed for business. The introduced concepts include Asset, chaincode (smart contracts), Practical Byzantine Fault Tolerance (PBFT), membership, and permissioned [23].

Hundreds of blockchain development environments have been developed for special applications or scenarios such as supply chain finance, financial clearance, business regulation and supervision. They have been improved with improved infrastructure, consensus mechanisms and design patterns to get higher performance and best-fit special scenarios on the general-purpose blockchain development environments. For instance, a permissioned blockchain, called Beihangchain, has been developed with its unique consensus algorithms, interfaces, and design. The blockchain used an account blockchain and a trading blockchain for a variety of applications including copyright protection and digital payment [24]. The Hyperchain is a self-contained and controllable blockchain platform that provides enterprise-level blockchain network solutions. It enables the enterprises to deploy, expand, and manage blockchain network based on existing cloud platforms, and provides real-time visual monitoring of its operation status [25].

4 Conclusions

The basic mission of blockchains is to establish a creditworthy ecosystem among independent participants in a non-trustable distributed environment. A blockchain system is secure and autonomous based on its chained blocks, peer–peer nodes, consensus-based ledger mechanism, anonymous accounts, self-regulated data ownership, and programmable smart contracts. Very few of the blockchain ventures are necessary, feasible, efficient and survive. Furthermore, the devoted credit mechanisms are required to make blockchain systems to be creditworthy although blockchains provide a creditworthy infrastructure for data-level storage and operations. Despite low successful cases, with its magic attraction, the blockchain technologies and application scenarios are continuously being innovated and improved. Another period of blockchain prosperity is on its way since the two symbolic projects, the Libra by Facebook and the DCEP by Central Bank of China, were announced to be launched. To embrace the booming blockchain time, this article provides some insights into blockchain applications and techniques. The advances and possible innovations and researches on blockchain applications and techniques are presented.

References

1. Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S (2016) Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press, Princeton. ISBN 978-0-691-17169-2
2. Blockchains: The great chain of being sure about things. The Economist. 31 October 2015
3. Franco P (2014) Understanding Bitcoin: cryptography, engineering and economics. Wiley, p. 9. ISBN 978-1-119-01916-9. Archived from the original on 14 February 2017
4. Libra White Paper. https://libra.org/en-US/white-paper/
5. CaiJing, RMB 3.0: The Operation Framework and Techniques of China Central Bank CryptoCurrency. http://www.chidaolian.com/article-31039-1
6. Engelhardt MA (2017) Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector. Technol Innov Manag Rev 7(10):22–34. https://doi.org/10.22215/timreview/1111
7. Trusting the transaction of things: IoT and blockchain intersect, IBM Watson IoT, June, 2016. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WWS12352USEN
8. What happened to the things? Steve Halliday, http://blogs.cisco.com/perspectives/what-happened-to-the-things
9. Nofer M, Gomber P, Hinz O, Schiereck D (2017) Blockchain. Bus Inf Syst Eng 59(3):183–187
10. BTC, blockchain projects. https://www.8btc.com/project?field=1
11. Fairfield J (2014) Smart contracts, Bitcoin bots, and consumer protection. Wash Lee L Rev Online 71:35–299
12. https://hyperledger-fabric.readthedocs.io/en/latest/
13. Van Rossum J (2017) Blockchain for research perspectives on a new paradigm for scholarly communication, [Digital Science Report], Digital Science. https://www.digital-science.com/resources/digital-research-reports/blockchain-for-research/
14. Turkanović M, Hölbl M, Košič K, Heričko M, Kamišalić A (2018) EduCTX: a blockchain-based higher education credit platform. IEEE Access 6:5112–5127
15. Wolfond G (2017) A blockchain ecosystem for digital identity: improving service delivery in Canada's public and private sectors. Technol Innov Manag Rev 7(10):35–40. https://doi.org/10.22215/timreview/1112
16. Li Y, Liang X, Zhu X, et al. A blockchain-based autonomous credit system. In: 2018 IEEE 15th international conference on e-business engineering (ICEBE). IEEE Computer Society, 2018, vol 1, pp 178–186
17. Distributed Ledger Technology (2018) Hybrid approach, front-to-back designing and changing trade processing infrastructure, By Martin Walker, First published: OCT 2018 ISBN 978-1-78272-389-9

18. Welink AppChain. http://www.weilianez.com/introduct
19. Illing S (2018) Why Bitcoin is bullshit, explained by an expert". Vox. Retrieved 17 July 2018
20. Kloch RC, Jr Simon J (2019) Little, Blockchain and Internal Audit Internal Audit Foundation, 2019 ISBN 978-1-63454-065-0
21. https://en.bitcoin.it/wiki/Block_chain
22. EthereumHomestead Documentation, http://www.ethdocs.org/en/latest/
23. Liu J, Jiang P, Leng J (2017) A framework of credit assurance mechanism for manufacturing services under social manufacturing context. In 13th IEEE conference on automation science and engineering (CASE), Xi'An, China, 20–23 Aug 2017
24. Tsai W-T, Yu L, Wang R, Liu N, Deng E-Y (2017) Blockchain application development techniques. J Softw 28:1474–1487. https://doi.org/10.13328/j.cnki.jos.005232
25. Hangzhou Qulian Technology Co., Ltd. Hyperchain Product Introduction. https://www.hyperchain.cn