Evolution of Blockchain-Based Digital Currencies: Postprint

Authors: Xie Kaibin

Date: 2018-07-09T00:00:00+00:00

Abstract

Blockchain is the mainstream technology and important prerequisite for digital currency research. As a decentralized distributed computing technology, blockchain possesses advantages such as collaborative maintenance, tamper resistance, and traceability that centralized technologies lack. Based on the fundamental principles of blockchain, key technologies in hash encryption, consensus mechanisms, and smart contracts are mainly analyzed; based on Bitcoin, the first application of blockchain, the development and evolution of digital currencies such as Ethereum, Dash, Cardano, and BitShares are analyzed. Based on the current research status of digital currency and the numerous challenges it faces, future research trends of blockchain in digital currency issuance and regulation, transaction tracking, and massive transaction data analysis are discussed.

Full Text

Preamble

Article URL: http://www.arocmag.com/article/02-2019-07-064.html
Journal: ChinaXiv Partner Journal *Computer Applications Research*
Title: Evolution of Digital Currency Based on Blockchain
Author: Xie Kaibin[1],[2]
Affiliations:
1. Northking Information Technology Co., Ltd., Beijing 100089, China
2. Key Laboratory of Intelligent Information Processing, Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China

Abstract: Blockchain represents the mainstream technology and critical foundation for digital currency research. As a decentralized distributed computing technology, blockchain offers advantages—including joint maintenance, tamper resistance, and traceability—that centralized systems cannot match. Grounded

in blockchain fundamentals, this paper analyzes key technologies in hash encryption, consensus mechanisms, and smart contracts. Building upon Bitcoin as blockchain' s first application, it examines the evolutionary trajectories of digital currencies such as Ethereum, Dash, Cardano, and BitShares. Based on the current state of digital currency research and its challenges, the paper outlines future research trends for blockchain in digital currency issuance and regulation, transaction tracking, and massive transaction data analysis.

Keywords: blockchain; decentralized; Bitcoin; digital currency; evolution
Classification: TP301
DOI: 10.3969/j.issn.1001-3695.2018.03.0258

0 Introduction

Since the 21st century, advances in ubiquitous computing, networking, and artificial intelligence have driven rapid development in the financial sector and broadened its application domains. However, financial transactions have traditionally relied on third-party institutions—such as banks, insurance companies, and exchanges—to serve as centralized trusted intermediaries. While this intermediary-based model performs adequately in most scenarios, it suffers from several fundamental problems: (a) opaque internal operations at centralized institutions create financial risks from potential insider manipulation; (b) the construction and maintenance costs of centralized institutions are substantial, requiring significant capital investment; and (c) centralized institutions are prime targets for cyberattacks, necessitating constant vigilance against potential security breaches.

To address these issues, a researcher under the pseudonym Satoshi Nakamoto innovatively proposed blockchain technology, which disrupts centralized architectures, and developed its first application: Bitcoin. The core concepts of blockchain and Bitcoin are articulated in the seminal paper "Bitcoin: a peer-to-peer electronic cash system" [1], which defines blockchain as follows: by performing hash operations on blocks containing transaction events, timestamps are added to blocks, and the hash values are broadcast to achieve consensus on transaction confirmation within the block. Different blocks are then linked chronologically based on their timestamp-corresponding hash values, forming an ever-growing transaction record chain [1].

As increasing numbers of researchers have joined blockchain studies, its core technologies—including hash encryption, consensus mechanisms, and smart contracts—have been thoroughly investigated. Hash encryption ensures the security of transactions within blocks and the validity of links between adjacent blocks [2, 3]. Consensus mechanisms primarily address how to incentivize distributed participants to join the blockchain ecosystem and enhance transaction reliability [4, 5]. Smart contract technology serves as a bridge between virtual and physical

spaces, enabling agreements reached in the physical world to be implemented through intelligent mechanisms in virtual space [6, 7].

1 Blockchain Fundamentals and Key Technologies

Blockchain, as a key technology for decentralized distributed systems, successfully enables trusted transactions between nodes without centralized endorsement. This achievement stems from its adoption of data structures suited for peer-to-peer transactions [8-10]. Moreover, hash encryption technology, consensus mechanisms, and smart contract technology have been critical to blockchain' s rapid development, advancing both theoretical research and practical applications of blockchain-based digital currencies.

1.1 Blockchain Fundamentals

The basic structure of a block in blockchain consists of four components: block delimiter, block size, block header, and block body. [Figure 1: see original paper] illustrates this fundamental structure. Block size determines the number of transactions that can be recorded in a block; the block header links to its adjacent blocks; and the block body records all transactions requiring verification.

The block header comprises six elements: block version number, parent block hash value, Merkle root value, timestamp, target value, and nonce. The block header links adjacent blocks through the parent block hash value. [Figure 2: see original paper] shows the block header structure.

The block body consists of two parts: the block' s transaction records and the details of each transaction record. [Figure 3: see original paper] depicts the transaction records.

1.2 Key Blockchain Technologies

As blockchain transitions from theoretical research to practical applications, three primary key technologies have emerged: hash encryption, consensus mechanisms, and smart contract technology. These are analyzed below.

1.2.1 Hash Encryption Technology Based on hash algorithms, hash encryption technology is a crucial security safeguard for blockchain systems. It possesses four characteristics that make it highly suitable for blockchain applications:

a) **Computational difficulty**: Reverse-engineering hashed information requires astronomical time scales, making decryption practically impossible.

b) **Simplicity of encryption/verification**: Given information and its hash algorithm, encryption can be performed rapidly. Similarly, given encrypted information, verifying whether it is the hash result of certain

data is straightforward.

c) **Information sensitivity**: Even minor alterations to the original information produce fundamentally different hash values.

d) **Collision resistance**: Different input information cannot produce identical hash values after algorithmic computation.

Additionally, Merkle hash trees [11, 12] enable verification of whether transaction data has been tampered with or deleted. A Merkle hash tree is a hash-based tree structure (typically binary, though multi-branch trees are possible) where leaf nodes are transaction data hash values and non-leaf nodes are hash values of their children' s concatenated hash blocks. The Merkle root can verify transaction data integrity and detect tampering with minimal data transmission and computational overhead—typically logarithmic in scale. [Figure 4: see original paper] illustrates the Merkle hash tree structure.

1.2.2 Consensus Mechanisms Consensus mechanisms address the challenge of establishing trust among distributed nodes in decentralized scenarios and are critical for ensuring blockchain systems operate continuously. Current consensus mechanisms primarily include Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT).

PoW operates on the principle that nodes with greater computational work receive higher rewards—approximately proportional to their effort [13]. This mechanism ensures blockchain security through substantial computational power but suffers from significant resource consumption and long transaction waiting times due to computational requirements. Bitcoin employs PoW, where all nodes solve complex yet easily verifiable mathematical puzzle, with only the most computationally powerful nodes able to solve them and earn Bitcoin rewards [14].

PoS uses "coin age" ownership to determine node eligibility for bookkeeping, aiming to reduce resource consumption while achieving consensus. The node with the greatest coin age creates new blocks and enjoys voting rights [15]. Compared to PoW, PoS significantly reduces consensus time and energy consumption but disadvantages nodes with fewer resources or coin age, making it nearly impossible for them to gain bookkeeping or voting rights [16]. Cardano employs PoS, and Ethereum plans to adopt this mechanism.

DPoS is a delegated proof-of-stake mechanism similar to corporate board voting, where each node elects delegates to perform bookkeeping and voting [17]. This approach reduces the number of participating nodes in bookkeeping and verification while allowing all nodes to participate in elections, effectively combining PoW and PoS advantages. BitShares currently uses this mechanism [18].

PBFT implements a Byzantine fault-tolerant distributed file system that ensures system liveness and safety with high fault tolerance [19]. The system remains secure and active as long as the number of failed nodes is less than

one-third of the total. Liveness means nodes receive responses after sending messages; safety means replicated copies maintain linear consistency. This mechanism is typically used in private chains.

Beyond these four primary mechanisms, China has proposed two additional consensus algorithms: Delegated Byzantine Fault Tolerance (dBFT) [20] and POOL verification pool algorithm [21]. dBFT improves upon PBFT by selecting bookkeepers based on node rights, with bookkeeping authority among bookkeepers achieved through Byzantine fault tolerance algorithms. The POOL verification pool algorithm is a fast consensus algorithm combining consistency algorithms like Pasox with data verification mechanisms.

1.2.3 Smart Contract Technology Smart contract technology was first proposed by interdisciplinary scholar Nick Szabo, who defined it as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises" [22]. In blockchain, smart contracts encapsulate various script codes that specify transaction execution methods and content. This makes blockchain a programmable currency system that is more flexible and efficient than traditional monetary transactions. Contracts can specify execution times, trigger rules, and other parameters. Digital currencies like Ethereum have implemented smart contract functionality.

Smart contract construction and execution on blockchain typically involves three aspects:
a) **Contract creation**: Designing script code according to participants' needs to implement contract terms.
b) **Contract storage**: The contract' s script code must be stored on the blockchain.
c) **Contract execution**: The contract's script code must execute automatically without human intervention.

2 Evolution of Blockchain-Based Digital Currencies

Since blockchain' s inception, thousands of blockchain-based digital currencies have emerged. All these currencies evolved from Bitcoin, blockchain' s first application, by improving upon Bitcoin's functional and performance limitations to meet diverse application scenario requirements.

2.1 Bitcoin' s Design and Limitations

Bitcoin is an encrypted digital currency built on P2P protocols and the Elliptic Curve Digital Signature Algorithm (ECDSA) [23]. "Miners" generate Bitcoin by mining—computing hash values that satisfy the difficulty coefficient in block headers. The initial reward per block was 50 Bitcoins, halving every four years to ensure a finite supply cap.

Despite its tremendous success as a cryptography-based digital currency, Bitcoin' s limitations have become apparent during its nine-year operation:

a) **Slow transaction speed**: With blocks generated approximately every ten minutes, a 1MB block size, and requiring confirmation across six consecutive blocks, Bitcoin transactions typically take hours—far below commercial requirements.

b) **Massive energy consumption**: Bitcoin generation uses PoW consensus, requiring extensive computations that consume enormous electrical energy.

c) **Limited application scope**: Bitcoin' s relatively single-function design makes developing other applications beyond trading with fiat or other digital currencies extremely difficult.

d) **Inadequate storage security**: Bitcoin exchanges and individual wallets have suffered numerous hacking attacks, causing Bitcoin theft, user panic, and hindering adoption.

e) **Regulatory gaps enabling money laundering**: Since private keys are known only to owners and identities remain anonymous, Bitcoin can easily be exploited for money laundering.

f) **Weakened decentralization**: As Bitcoin mining farms grow larger, major farms' computational power far exceeds that of smaller operations and individuals. Several large farms' combined hash rate has exceeded 50% of the total, forcing economically disadvantaged individuals and small groups out of mining and undermining Bitcoin' s decentralized vision.

2.2 Ethereum

Ethereum is a blockchain application development platform built upon Bitcoin. It supports diverse operating systems and development languages, offering multiple client implementations. Applications developed in languages like Python, C, and Java are compiled into Turing-complete script language (Ethereum Virtual Machine or EVM language) for execution [24].

Ethereum' s primary distinction from Bitcoin lies in its powerful smart contract programming environment. While Bitcoin' s functionality is limited to digital currency usage value—often termed Blockchain 1.0—Ethereum enables development of smart contract applications for complex commercial and non-commercial logic, vastly expanding digital currency applications and ushering in the Blockchain 2.0 era.

Compared to Bitcoin, Ethereum' s evolutionary improvements include:
a) **Diverse application development**: Smart contracts enable numerous ap-

plications on Ethereum, significantly expanding digital currency application domains.
b) **Faster transaction speeds**: Ethereum blocks are generated in seconds, much faster than Bitcoin.
c) **Enhanced decentralization**: Ethereum uses the SHA-3 hash algorithm, which prevents ASIC mining and makes super-mining machines difficult to develop, allowing more miners to participate and strengthening decentralization.

2.3 Cardano

Cardano is the first cryptocurrency in the industry to conduct academic research before implementation, with its properties and functions undergoing rigorous mathematical proof and peer review to ensure theoretical security and correctness.

Cardano employs the PoS consensus mechanism through a protocol called Ouroboros [25], which uses formal mathematical proofs to guarantee security. Cardano implements a layered architecture [26]:
a) **Settlement layer**: Cardano' s token circulates in this layer, forming the ecosystem' s foundation by recording transaction volumes and timestamps.
b) **Computation layer**: This layer provides smart contracts, message authentication, and communication functions, enabling developers to build diverse applications.

A major Cardano innovation is using formal methods to achieve controlled computation, balancing user privacy with regulatory requirements to reduce financial risks. Additionally, Cardano plans to adopt Recursive InterNetwork Architecture (RINA) [27] instead of TCP/IP, making node communication resemble inter-process interaction to accelerate information transfer.

Compared to Bitcoin, Cardano' s evolutionary features include:
a) **Improved transaction speed**: Functional layering and RINA architecture significantly enhance transaction speed.
b) **Reduced energy consumption**: The PoS consensus mechanism dramatically lowers energy usage.
c) **Regulatory feasibility**: Formal reasoning design incorporates financial regulation considerations.
d) **Diverse application development**: Smart contract functionality enriches application development possibilities.
e) **Enhanced storage security**: Formal implementation methods facilitate matching storage solutions.

2.4 Dash

Dash is a Bitcoin superset that inherits Bitcoin' s main characteristics, including mining-based generation, but with a faster block generation time of approximately 2.5 minutes per block, rewarding miners with 5 Dash per block.

Dash' s primary extension beyond Bitcoin is its masternode network [28]. Nodes possessing 1,000 Dash for qualification can serve as masternodes. This masternode network, built upon Bitcoin' s underlying blockchain, consists of dedicated servers with over 4,000 current masternodes.

Dash allocates mining rewards in a 45%/45%/10% split among miners, transaction-confirming masternodes, and the Dash community. The masternode network enables near-instant payments within seconds and significantly enhances transaction security through its credibility backing. The community provides a channel for addressing issues like block scaling and ecosystem development.

For mining, Dash uses the X11 algorithm, which performs 11 rounds of SHA-3 hashing with each round' s output serving as the next round' s input. This approach delays the development of specialized mining hardware, allowing more participants to mine using ordinary computers.

Compared to Bitcoin, Dash' s evolutionary features include:
a) **Commercial-grade transaction speed**: The masternode network meets most commercial requirements.
b) **High decentralization**: The X11 algorithm enables broader mining participation, and the community mechanism enhances decentralization.
c) **Community-based regulation**: The community mechanism provides some transaction oversight.

2.5 BitShares

BitShares is a comprehensive financial transaction service platform based on blockchain technology, aiming to build a decentralized free-market financial ecosystem. Individuals and institutions can conduct transfers, initiate crowdfunding, build virtual currency exchanges, and even implement regulatory-compliant black/white lists on the BitShares platform.

BitShares designed a novel freely tradable digital asset: BitShares market-pegged assets [29], which can be exchanged for USD, euros, or gold. For example, the BitUSD asset can be exchanged for an equivalent USD amount. These assets typically use twice their value in BitShares as collateral, with smart contracts automatically executing liquidation to prevent default risk, ensuring value stability and creating a virtuous ecosystem cycle.

BitShares uses DPoS, granting all BitShares holders voting rights, with the top 101 vote-getting nodes earning transaction bookkeeping authority. This enables transaction confirmation within three seconds and processing speeds of 100,000 transactions per second—fully meeting typical commercial requirements.

Compared to Bitcoin, BitShares' evolutionary features include:
a) **Commercial-grade transaction/transfer speeds**: DPoS enables three-second confirmation times.
b) **Minimal energy consumption**: The DPoS mechanism requires negligible

energy.
c) **Multi-domain applicability**: Market-pegged assets maintain price stability, enabling applications across multiple fields.

compares the evolutionary improvements of Ethereum, Cardano, Dash, and BitShares across transaction speed, energy consumption, application diversity, storage security, regulation, and decentralization.

3 Future Research Trends in Digital Currencies

Blockchain' s disruptive innovation over traditional centralized technologies provides decentralized application models for finance, food safety, species conservation, IoT, and numerous other industries. Although blockchain has existed for less than a decade and remains in its infancy with immature standards, many nations have prioritized it as a strategic research technology due to its profound impact on financial sovereignty, social credit, and cross-border transactions. Active participation in blockchain standardization and deep investigation of its innovative value across domains will enhance national discourse and leadership in technology and economics.

Based on blockchain' s characteristics and current application status, the following research directions represent major future trends:

a) **Research on blockchain-based digital currency issuance**: Current digital currency technologies for issuance, circulation, regulation, and control remain immature [30, 31], lacking effective issuance schemes. Future research will address reducing the high costs of traditional paper currency issuance and circulation, enhancing transaction convenience and transparency, reducing crimes like money laundering and tax evasion, and improving central bank control over money supply and circulation.

b) **Research on blockchain-based transaction tracking**: Current research primarily focuses on how blockchain-based digital asset transactions occur [32, 33], with limited investigation into traceability. Future research should design transaction rules and regulatory frameworks to ensure both transaction efficiency and traceability.

c) **Research on massive data analysis in blockchain**: Few studies have addressed analysis of blockchain' s massive datasets [34, 35]. However, blockchain records authentic real-world data with enormous commercial value for user profiling and behavior analysis. Future research will employ intelligent algorithms like machine learning [36] and deep learning [37] to analyze blockchain user data and extract valuable business insights.

4 Conclusion

This paper introduced blockchain technology fundamentals, analyzed the evolution of blockchain-based digital currencies, and examined how Ethereum, Car-

dano, Dash, and BitShares evolved Bitcoin' s functionality. Based on current blockchain applications, the paper analyzed challenges facing digital currency research and projected future trends. Blockchain' s disruptive innovation provides decentralized alternatives for numerous industries. Despite its nascent stage, blockchain' s strategic importance demands active participation in standardization and deep exploration of its technological innovation value to strengthen future leadership across scientific and economic domains.

References

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. (2008-11-01) [2018-05-06]. http://www.bitcoin.org/bitcoin.pdf.
[2] Devine R. Design and implementation of DDH: a distributed dynamic hashing algorithm [C]// Proc of International Conference on Foundations of Data Organization and Algorithms. Berlin: Springer, 1993: 101-114.
[3] Courtois N T, Grajek M, Naik R. Optimizing Sha256 in bitcoin mining [C]// Proc of International Conference on Cryptography and Security Systems. Berlin: Springer, 2014: 131-144.
[4] Ephrati E, Rosenschein J S. The clarke tax as a consensus mechanism among automated agents [C]// Proc of National Conference on Artificial Intelligence. Anaheim: AAAI Press//MIT Press, 1991: 173-178.
[5] Liu Yujia, Liang Changyong, Chiclana F, et al. A trust induced recommendation mechanism for reaching consensus in group decision making [J]. Knowledge-Based Systems, 2017, 119 (C): 221-231.
[6] Kosba A, Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts [C]// Security and Privacy. California: IEEE Press, 2016: 839-858.
[7] Luu L, Chu D H, Olickel H, et al. Making smart contracts smarter [C]// Proc of ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 254-269.
[8] Ron D, Shamir A. Quantitative analysis of the full bitcoin transaction graph [C]// Proc of International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2013: 6-24.
[9] Donet J A D, Pérez-Sola C, Herrera-Joancomartí J. The bitcoin P2P network [C]// Proc of International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2014: 87-102.
[10] Bhattacharya R, White M, Beloff N. A blockchain based peer-to-peer framework for exchanging leftover foreign currency [C]// Proc of Computing Conference. Hangzhou: IEEE Press, 2017: 1431-1435.
[11] Li Hongwei, Lu Rongxing, Zhou Liang, et al. An efficient merkle-tree-based authentication scheme for smart grid [J]. IEEE Systems Journal, 2014, 8 (2): 655-663.
[12] Ahmad A, Alajeely M, Doss R. Establishing trust relationships in OppNets using Merkle trees [C]// Proc of International Conference on Communication Systems and Networks. Beijing: IEEE Press, 2016: 1-6.
[13] Gervais A, Karame G O, Glykantzis V, et al. On the Security and Perfor-

mance of Proof of Work Blockchains [C]// Proc of ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 3-16.
[14] Sleiman M D, Lauf A P, Yampolskiy R. Bitcoin message: data insertion on a proof-of-work cryptocurrency system [C]// Proc of International Conference on Cyberworlds. Chongqing: IEEE Press, 2016: 332-336.
[15] Li Wenting, Andreina S, Bohli J M, et al. Securing Proof-of-Stake Blockchain Protocols [M]// Data Privacy Management, Cryptocurrencies and Blockchain Technology. Cham: Springer, 2017: 297-315.
[16] Bartoletti M, Lande S, Podda A S. A Proof-of-stake protocol for consensus on bitcoin subchains [C]// Proc of International Conference on Financial Cryptography and Data Security. Cham: Springer, 2017: 568-584.
[17] Larimer D. Delegated proof-of-stake (dpos) [EB/OL]. (2013-09-11) [2018-05-06]. https://bitshares.org/technology/delegated-proof-of-stake-consensus.
[18] Zheng Zibin, Xie Shaoan, Dai Hongning, et al. An overview of blockchain technology: Architecture, consensus, and future trends [C]// Proc of IEEE International Congress on Big Data. Honolulu: IEEE Press, 2017: 557-564.
[19] Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery [J]. ACM Trans on Computer Systems, 2002, 20 (4): 398-461.
[20] Distributed Technology Company. Antshares consensus algorithm [EB/OL]. (2016-01-11) [2018-05-06]. http://www.onchain.com/paper/66c6773b.pdf.
[21] Bubi (Beijing) Network Technology Co., Ltd. Bubi blockchain product white paper [EB/OL]. (2016-08-21) [2018-05-06]. http://www.bubi.cn/whitePaper/index.jhtml.
[22] Szabo N. Formalizing and securing relationships on public networks [J]. First Monday, 1997, 2 (9): 1-21.
[23] Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA) [J]. International Journal of Information Security, 2001, 1 (1): 36-63.
[24] Hirai Y. Defining the Ethereum Virtual machine for interactive theorem provers [C]// Proc of International Conference on Financial Cryptography and Data Security. Cham: Springer, 2017: 520-535.
[25] Kiayias A, Russell A, David B, et al. Ouroboros: a provably secure proof-of-stake blockchain protocol [C]// Proc of International Cryptology Conference. Cham: Springer, 2017: 357-388.
[26] Guides T S. Why Cardano ADA Deserves Attention–Cardano Cryptocurrency Strategy [EB/OL]. (2018-01-09) [2018-05-07]. https://cardanodocs.com/introduction.
[27] Vrijders S, Staessens D, Colle D, et al. Experimental evaluation of a Recursive InterNetwork Architecture prototype [C]// Proc of Global Communications Conference. Washington DC: IEEE Press, 2015: 2017-2022.
[28] Robert W. Understanding the Governance and Budget System [EB/OL]. (2008-05-04) [2018-05-07]. https://dashpay.atlassian.net/wiki/spaces/DOC/pages.
[29] Schuh F, Larimer D. BitShares 2.0: Financial Smart Contract Platform [EB/OL]. (2015-12-20) [2018-05-06]. http://docs.pybitshares.com/en/latest.
[30] Aste T, Tasca P, Matteo T D. Blockchain Technologies: The Foreseeable Impact on Society and Industry [J]. Computer, 2017, 50 (9): 18-28.
[31] Spearpoint M. A Proposed Currency System for Academic Peer Review

Payments Using the BlockChain Technology [J]. Publications, 2017, 5 (3): 21.
[32] Godfrey-Welch D, Lagrois R, Law J, et al. Blockchain in Payment Card Systems [J]. SMU Data Science Review, 2018, 1 (1): 3.
[33] Kisore N R, Sagi S. A secure SMS protocol for implementing digital cash system [C]// Proc of International Conference on Advances in Computing, Communications and Informatics. Kerala: IEEE Press, 2015: 1883-1892.
[34] Kuzuno H, Karam C. Blockchain explorer: An analytical process and investigation environment for bitcoin [C]// Electronic Crime Research. Arizona: IEEE Press, 2017: 9-16.
[35] Vo H T, Mehedy L, Mohania M, et al. Blockchain-based Data Management and Analytics for Micro-insurance Applications [C]// Proc of ACM Conference on Information and Knowledge Management. New York: ACM Press, 2017: 2539-2542.
[36] Adoma F. Big data, machine learning and the blockchain technology: an overview [J]. International Journal of Computer Applications, 2018, 180 (28): 1-4.
[37] Gimpel H, Röglinger M. Disruptive technologien: blockchain, deep learning & Co [J]. Wirtschaftsinformatik & Management, 2017, 9 (5): 8-17.

Note: Figure translations are in progress. See original paper for figures.