Blockchain and Cryptocurrencies: Model, Techniques, and Applications

Yong Yuan, *Senior Member, IEEE*, and Fei-Yue Wang, *Fellow, IEEE*

***Abstract*—As an emerging decentralized architecture and distributed computing paradigm underlying Bitcoin and other cryptocurrencies, blockchain has attracted intensive attention in both research and applications in recent years. The key advantage of this technology lies in the fact that it enables the establishment of secured, trusted, and decentralized autonomous ecosystems for various scenarios, especially for better usage of the legacy devices, infrastructure, and resources. In this paper, we presented a systematic investigation of blockchain and cryptocurrencies. Related fundamental rationales, technical advantages, existing and potential ecosystems of Bitcoin and other cryptocurrencies are discussed, and a six-layer reference model of the blockchain framework is proposed with detailed description for each of its six layers. Potential applications of blockchain and cryptocurrencies are also addressed. Our aim here is to provide guidance and reference for future research along this promising and important direction.**

***Index Terms*—Bitcoin, blockchain, consensus algorithm, cryptocurrency, smart contract.**

I. Introduction

BLOCKCHAIN is the fundamental technology underlying the emerging cryptocurrencies including Bitcoin [1]. The key advantage of blockchain is widely considered to be decentralization, and it can help establish disintermediary peer-to-peer (P2P) transactions, coordination, and cooperation in distributed systems without mutual trust and centralized control among individual nodes, based on such techniques as data encryption, time-stamping, distributed consensus algorithms, and economic incentive mechanisms. As such, blockchain can offer a novel solution to the long-standing problems of high operation costs, low efficiency and potential security risks of data storage in traditional centralized systems.

With the rapid development and popularization of Bitcoin and other cryptocurrencies in the recent years, blockchain research and applications have also been witnessed to showcase an unprecedented trend of explosive increase. In [2], blockchain is widely recognized to be in position to become the fifth disruptive innovation of computing paradigm after mainframe, personal computer, Internet, and mobile/social networks. Blockchain can be considered as the next generation of cloud computing, and is expected to radically reshape the behavior model of individuals and organizations, and thus realize the transition from the Internet of Information today to the future Internet of Value [3], [4].

The fast-growing trend of blockchain has attracted a wide spectrum of interests from governments, financial institutions, high-tech enterprises, and also the capital markets. The history of blockchain can be traced back to the late 2008, when Bitcoin was first invented by a researcher with the pseudonym of "Nakamoto" [5] posting in a cryptography mail group, an article entitled "Bitcoin: A peer-to-peer electronic cash systems." Technically speaking, blockchain can be narrowly defined as a kind of decentralized shared ledger that uses chronological, encrypted and chained blocks to store verifiable and synchronized data (e.g., transactions, states, behaviors, decisions, etc.) across a P2P network. Broadly speaking, blockchain can be viewed as a novel decentralized architecture and distributed computing paradigm, which stores data with encrypted chained blocks, verifies data with distributed consensus algorithms, guarantees security and privacy in data access and transmission with cryptography, and manipulates data with self-executed program scripts (i.e., smart contracts) [3], [6].

Blockchain has many desirable features in both its technical and organizational aspects, which can be summarized as "TRUE" and "decentralized autonomous organization (DAO)" [7]. The former denotes trustable, reliable, usable, and efficient, while the latter denotes distributed and decentralized, autonomous, and automated, as well as organized and ordered. More specifically, blockchain is a distributed shared ledger, in which the recording, verification, storage, maintenance, and transmission of blockchain data are all based on the distributed architecture, and the mutual trust among distributed nodes is established via mathematical algorithms instead of centralized third-party authorities. Transaction data is stored on the blockchain in the form of chained blocks with time stamps, which can endow blockchain data with a temporal dimension

Manuscript received February 22, 2018; accepted June 8, 2018. Date of publication July 25, 2018; date of current version August 16, 2018. This work was supported in part by the National Natural Science Foundation of China under Grant 71472174, Grant 71702182, Grant 61533019, Grant 71232006, and Grant 61233001, and in part by the Qingdao Think-Tank Foundation on Intelligent Industries. This paper was recommended by Associate Editor H.-X. Li. *(Corresponding author: Yong Yuan.)*

Y. Yuan is with the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China, and also with the Innovation Center on Parallel Blockchain, Qingdao Academy of Intelligent Industries, Qingdao 266109, China (e-mail: yong.yuan@ia.ac.cn).

F.-Y. Wang is with the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China, also with the Research Center of Military Computational Experiments and Parallel System, National University of Defense Technology, Changsha 410073, China, and also with the Center of China Economic and Social Security, University of Chinese Academy of Sciences, Beijing 100049, China (e-mail: feiyue.wang@ia.ac.cn).

Digital Object Identifier 10.1109/TSMC.2018.2854904

and in turn strong verifiability and traceability. Various kinds of economic incentive mechanisms are designed so as to crowd-source the mining process of blockchain to large numbers of blockchain miners, so that these miners are willing to contribute their computing power and participate in verifying the data blocks in the distributed shared ledger, as well as compete in the consensus process with the aim of winning the opportunity of creating the next data block and appending it to the main chain. Blockchain can also be empowered by programmable chain-codes and scripts, so that users can create high-level smart contracts, cryptocurrencies, or other decentralized applications (DApps). For instance, Ethereum (ETH) platform can offer Turing-complete script language and enable users to design any arbitrary smart contracts or transactions that can be precisely defined. Finally, blockchain data will be encrypted using asymmetric cryptography, and secured via the computing power collected from the consensus algorithms among large numbers of nodes in the distributed systems. As such, blockchain can be considered as a secured framework against outside attacks, and thus ensuring strong unforgeability and untemperability.

Blockchain is a novel and fundamental technical framework, and is expected to bring profound influence to the finance, economics, science and technology, and even politics areas. According to the development trend of blockchain technology, it is widely believed that blockchain will experience three types of application patterns, i.e., blockchain 1.0 featuring programmable cryptocurrencies, blockchain 2.0 featuring programmable financial systems, as well as blockchain 3.0 featuring programmable societies [2]. These patterns evolves synchronously rather than progressively.

The remainder of this paper is organized as follows. In Section II, we discuss the rationale of Bitcoin and other cryptocurrencies. Section III proposes the six-layer reference model for blockchain, and discusses the detailed model and techniques in each layer. In Section IV, we present several illustrative application scenarios of blockchain. Section V concludes this paper.

II. Bitcoin and Cryptocurrency

Bitcoin is one of the most successful application scenarios of blockchain so far. According to the latest statistics reported in the monitoring website Blockchain.info [8], more than 120 000 transactions, with $75 million transferred, were written into the Bitcoin blockchain ledger on daily average, and currently more than 500 000 blocks have been created. It is also reported by the website coinmarketcap.com that there are currently more than 1500 types of cryptocurrencies in the blockchain-powered markets with the total market cap of more than $500 billion, in which Bitcoin stands in the dominant position with a market cap accounting for more than 37% of the total, and the ETH and Ripple stand in the second and third places, respectively [9]. Currently, the number of bitcoins that have been mined and in circulation is approximately 17 million, and the global Bitcoin economy has been $185.8 billion, about the size of the GDP of New Zealand in 2016. In other words, the decentralized Bitcoin has created a global economy with the size of a mid-size developed country based merely on algorithm-endorsed trust and consensus. As such, it is estimated that about 10% of global GDP will be stored on blockchain by 2027 [10].

Bitcoin and most other cryptocurrencies differ from the traditional electronic cash in the following five aspects. First, Bitcoin is completely decentralized without central control or hierarchical structure. Actually, Bitcoin is controlled by distributed consensus algorithms running among computing nodes in P2P networks. The traditional electronic cashes, however, typically need centralized service providers, and thus are centrally controlled by governments or specific companies. Second, Bitcoin is pseudo-anonymous like e-mail. One might know the address of a Bitcoin user, but cannot know exactly who he or she is. On the contrary, most traditional electronic cashes is nonanonymous, and the users identities will be recorded by the centralized service providers. Third, Bitcoin has a limited currency issuance with a cap of about 21 million bitcoins. While most traditional electronic cashes have unlimited currency issuance. The centralized service provider can make their decision to increase or decrease the supply of cashes, which might possibly cause inflation or deflation. Fourth, Bitcoin is open-source to the public. Everyone can check the source code of Bitcoin, and thus each and every one of them will understand the underlying mechanisms of Bitcoin issuance. However, most traditional electronic cashes are closed-source, and the critical business logic is always kept as secret to the users. Finally, Bitcoin itself has no value, it is only a sequence of zeros and ones. However, Bitcoin can gain value by increasing users. The more users trust and use Bitcoin, the more value Bitcoin will have. In contrast, almost all traditional electronic cashes are endorsed by fiat money.

The first block of Bitcoin blockchain, also known as, the genesis block, was created on January 4, 2009 by Nakamoto, who sent 10 bitcoins to a crptographer Finney one week later. This is widely considered as the first transaction in the Bitcoin history. In May 2010, a programmer in Florida bought two pizzas worth $25 using 10 000 bitcoins, resulting in the initial exchange rate of Bitcoin to U.S. dollars. Since then, the price of Bitcoin raises rapidly, and peaked at $1242 each bitcoin, exceeding the price of gold, that is, $1241 per ounce at that time. It is estimated by CoinDesk that there are more than 60 000 of merchants in the world accepting Bitcoin transactions, and China is among the most fast-growing countries in Bitcoin transactions [11].

Bitcoin is in essence an electronic cash generated in the distributed systems. The issuance of Bitcoin relies on a consensus competition among distributed network nodes, known as proof-of-work (PoW)-based mining, instead of a specific centralized authority. In the PoW-based consensus process, each and every computing node in the P2P network contributes its computing resource (CPU) and competes to solve a mathematically hard puzzle with dynamically adjustable difficulties. More specifically, in each round of the consensus process, new Bitcoin transactions will be broadcasted to the P2P network. Each node keeps listening to the network, and adds the received transactions to a memory pool. Every node is competing to compute a nonce satisfying certain requirements.

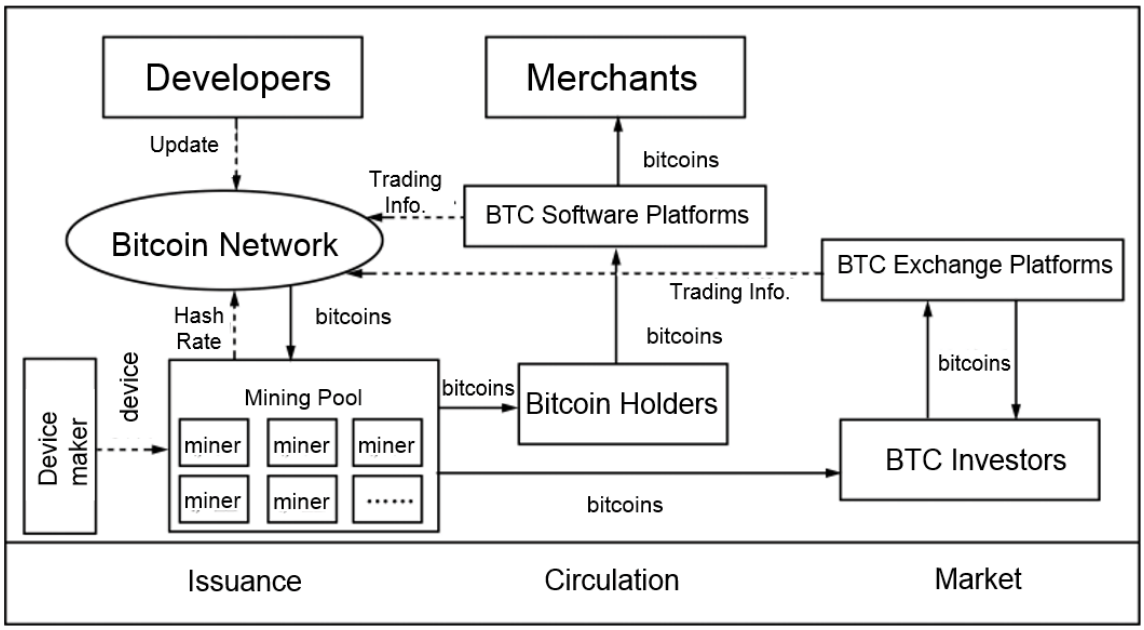

Fig. 1. Bitcoin ecosystem.

The miner who first successfully find such a correct nonce will win the consensus competition, and also win the right of creating the next new block. The winner will package transactions in the memory pool into a new block, partly according to a decreasing order of their associated transaction fees, and then broadcast this new block into the entire blockchain network. The block will be accepted by other nodes if and only if the transactions in it is valid and not received before. Finally, other nodes append this block into the main chain, and start the next round of consensus process competing for the right of packaging new transactions. In this process, the Bitcoin system will generate a specific amount of bitcoins as a reward to the winning miner, and also as an incentive to encourage other miners to continue contribute their computing power. The circulation process of Bitcoin will be secured by cryptography, with each Bitcoin transaction being hashed, encrypted and written into blockchain ledger after validation from all miners. Meanwhile, the transaction can be programmed and controlled by algorithm-driven scripts and non-Turing complete smart contracts, so as to realize the programmable and automatic circulation for Bitcoin. To sum up, we can conclude that Bitcoin blockchain typically has the following five key components, i.e., a public shared blockchain ledger, a distributed P2P networking system, a decentralized consensus algorithm, a well-designed economic incentive mechanism, and programmable smart contracts.

Bitcoin, like most other cryptocurrencies, is a self-contained ecosystem consisting of the issuance, circulation and the exchange market of bitcoins, as is depicted in Fig. 1 [3]. In the issuance part, the Bitcoin network is maintained and updated by the developers, and the network receives hash-based computing power from the mining pool or individual miners, and generates bitcoins as rewards to these miners. The miners can participate in the mining process individually, and can also cooperate by joining the mining pool so as to increase the possibility of successfully creating a block. The device maker produces and sells mining computers to the miners. In the circulation part, Bitcoin holders or users buy specific types of goods or services from the merchants via the Bitcoin software platforms, such as Bitcoin wallets. The trading information will be broadcast to the Bitcoin network and also validated by the miners. In the exchange market part, since Bitcoin price fluctuates frequently, which results in a good investment opportunity for the investors. So they will buy and sell bitcoins from the Bitcoin exchange platform, and the trading information will also be broadcast to the Bitcoin network, and validated by the miners.

Inspired by the great success of Bitcoin, thousands of other blockchain-powered cryptocurrencies emerge and develop rapidly in this novel market. Most of these cryptocurrencies, also known as altcoins, are invented with the aim of improving the performance of the Bitcoin system. Currently, there are six major dimensions and directions in the innovation of altcoins, as can be seen in Fig. 2. The first dimension focuses on the scalability. For instance, Bitcoin cash, forked from the Bitcoin blockchain, extends the block size from 1 to 8 MB. This allows more transactions packaged into a single block in each round of consensus competition, and thus results in improved capability of transaction processing and reduced time in transaction confirmation. Zilliqa can improve the throughput using the network sharing technique, which can automatically divide the blockchain network into multiple shards that validate transactions in parallel. The second dimension aims to improve the security and privacy protection with cryptographic techniques including zero-knowledge proof and homomorphic encryption. Examples include ZCash (ZEC) and Monero (XMR), among others. The third dimension is enhancing the programmability of blockchain systems, and the most

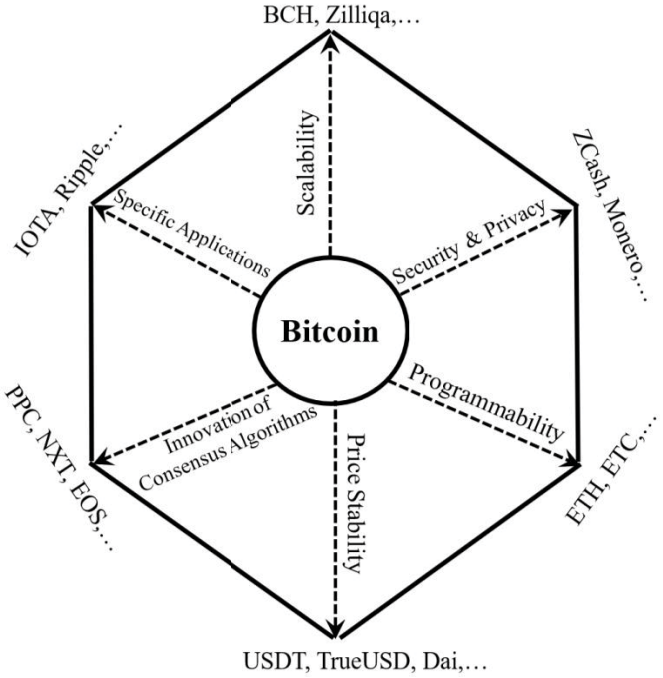

Fig. 2. Six dimensions in cryptocurrency innovation.

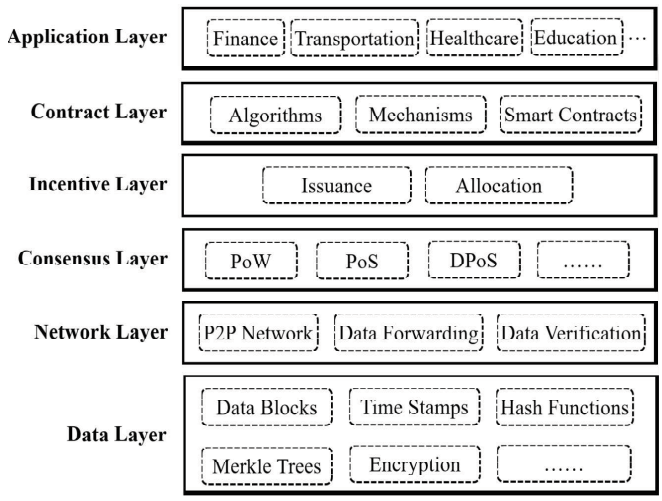

Fig. 3. Reference model of blockchain.

well-known example is ETH, which supports Turing complete smart contracts and in turn DApps. The forth dimension is targeted at the price stability. For instance, USDT and other Tether currencies are endorsed by and equivalent in value to U.S. dollar, and can help facilitate the transfer of national currencies, provide users with a stable alternative to Bitcoin. The fifth dimension is based on the innovation of consensus algorithms, such as PeerCoin and EOS. Finally, the sixth type of crypt-currencies are devoted to specific application scenarios, such as the IOTA oriented to Internet of Things, Ripple used for global financial settlement, as well as Augur created for prediction market applications.

III. Reference Model and Techniques of Blockchain Technology

Although blockchain has imposed significant impacts on cryptocurrency, finance, and even socio-economic activities, it is not a new technology invented from scratch. Actually, blockchain can be considered as an ensemble innovation combining a group of extant technologies in cryptography, economics, and computer sciences fields. In this section, we will propose a six-layer reference model for characterizing and standardizing the typical architecture and major components of blockchain systems, and discuss the key techniques in each layer. Similarly as the well-known open system interconnection reference model of the Internet [12], a complete blockchain system can also be decoupled into six layers stacked as is shown in Fig. 3 [3], [6].

A. Data Layer

This layer provides the key techniques for manipulating a variety of data collected from cyber, physical, and social spaces [13]–[15]. These data will be bundled into chained blocks, stored on all the full nodes in the blockchain network using the data structure of asymmetrically encrypted, hashed, and time-stamped Merkle trees. More specifically, each node, once winning the consensus competition, will be empowered to package all data generated in the period (typically a regular interval, e.g., 10 min in the Bitcoin system) of the competition into a new block with a time-stamp indicating its creating time. If there are conflicting data such as Bitcoin's double spending, only one agreed version to all or a majority of nodes will be selected and appended into the block. As is shown in Fig. 4 [6], a typical Bitcoin block consists of a header and a body part. The former contains all the meta-information while the latter stores a Merkle tree of verified and hashed data (e.g., via double SHA256 algorithm). The blocks are chained one by one in chronological order, forming the entire history from the genesis block to the newly generated one. In this layer, Merkle tree and time stamp can be considered as two important components for the blockchain ledger. The former helps realize rapid, efficient, and secured verification of the existence and integrity of blockchain data, while the latter enables the traceability and precise positioning of blockchain data. As such, blockchain is expected to be widely used in time-sensitive application scenarios. More importantly, time-stamp has the potential of endowing blockchain data with a time dimension, and thus makes it possible to recur the past data history.

B. Network Layer

This layer specifies the decentralized communication models and the related mechanisms of distributed networking, data forwarding, and verification. In most cases, blockchain application scenarios involves an open and dynamic environment with large number of distributed and connected devices or vehicles. The blockchain focuses on the important part of decentralized environments that can be topologically modeled as P2P networks. All participating nodes in the network are equally privileged without central authorities or middle-mans,

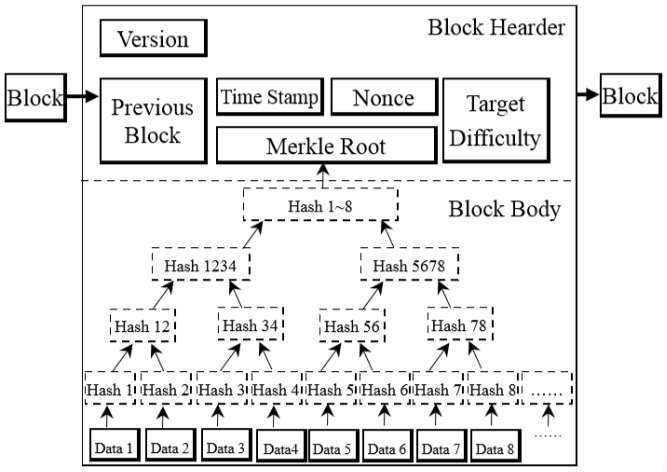

Fig. 4. Data layer of blockchain.

so that the blockchain system is under decentralized, emergent, and bottom-up control. These nodes keep listening to the network, verifying the broadcasted data or blocks according to predefined check lists. Invalid blocks will be discarded and others will be forwarded to neighboring nodes. This way, only one block accepted by the majority will be appended into blockchain. It is worth noting that this P2P-based decentralized network makes blockchain a potential architecture for the next generation of cloud computing. Blockchain data is stored on each and every node, and can be synchronized and restored even in the worst case of failure in all but one nodes. This evolves the cloud model with multiple central servers to a completely decentralized model, which is particularly useful in communication and interaction among decentralized entities [3].

C. Consensus Layer

Blockchain uses a variety of consensus algorithms to guarantee the data consistency and the fault-tolerant ability of the shared ledger among distributed nodes [16], [17]. Traditional application scenarios typically are relatively closed ecosystems with entities trusting in each other, where early algorithms such as PAXOS might be sufficient to reach consensus efficiently. Blockchain models, however, mainly focus on open and dynamic environments with a large number of trustless entities with possible Byzantine failures [18], so that more complex algorithms are needed, such as practical Byzantine fault tolerance for semiopen environments and proof-of-X (POX) type consensus for open environments (e.g., the cryptocurrency markets). For instance, PoW is the most widely used algorithm, which asks nodes to compete repeatedly to do a mathematically difficult computation to validate the data [19]. The winning node will be allowed to append its block on the ledger; proof-of-stake (PoS) requires the node with the largest amount of predefined stakes (e.g., coins) to create the new block; Other POX algorithms include delegated PoS (DPoS), proof-of-movement, etc. Among all POX algorithms, noncompute-intensive algorithms such as PoS and DPoS are particularly suitable for most lightweight systems in blockchain ecosystems.

D. Incentive Layer

This layer incorporates economic rewards into blockchain systems. In essence, the data verification and block creation process driven by consensus competitions can be considered as a crowdsourcing task to participating nodes that contribute their computing power. These nodes are actually self-interested agents, so that incentive compatible mechanisms must be designed to make individual behavior of revenue maximization aligned with the system-wide target of guaranteeing a secured and trusted ecosystem [20]–[22]. Toward this end, cryptocurrencies such as Bitcoin and ETH can serve as a natural form as motivating reward. Its issuance mechanism is simple: once a new block is created, a certain amount of cryptocurrencies will be issued as reward and allocated to the winning node to motivate the entire network continuing their efforts in data verification and block creation. This incentive layer is a key component and the main driving force for blockchain, especially for those based on public blockchains. It cannot only serve as the engine for powering blockchain, but also establish an imbedded, cryptocurrency-based financial system in blockchain, so that disintermediated trading and real-time micro-payment can be easily supported. It is worth noting that, however, this layer is optional for some partially centralized blockchain applications, typically called private blockchain for closed environments and consortium blockchain for semiopen scenarios, where trusted entities participate mandatorily without payment and financial requirements.

E. Contract Layer

In this layer, various smart contracts, mechanisms, and algorithms are packaged, and can serve as the high-level business logics to activate the static data, money, or assets stored on blockchain. Smart contracts can be narrowly defined as a group of self-verifying, self-executing and self-enforcing state-response rules that are stored and secured by the blockchain. Once a group of parties consent to a set of predefined terms or rules, they can codify them as a smart contract, cryptographically sign it, and broadcast it to the P2P network for verification. The verified contract will be packaged into a block on the ledger. Once one or more preconditions are triggered, the stipulations and associated actions will be activated and self-executed without human interventions, as is shown in Fig. 5. This self-execution feature has the potential of transforming physical or digital assets into smart properties, which can be controlled and managed in an automatic and programmable fashion, thus significantly reducing the social complexity. In a broader sense, scripts and algorithms can also be viewed as dynamically decision-making rules (instead of the static rules in contracts), and thus can be written as smart contracts on the ledger, resulting in improved autonomy and programmability [3], [6], [23], [24].

F. Application Layer

This layer packages all possible application scenarios and use cases of blockchain. Although blockchain technology is still in its infancy, it has witnessed a tremendous growth in recent years in both research and industrial applications.

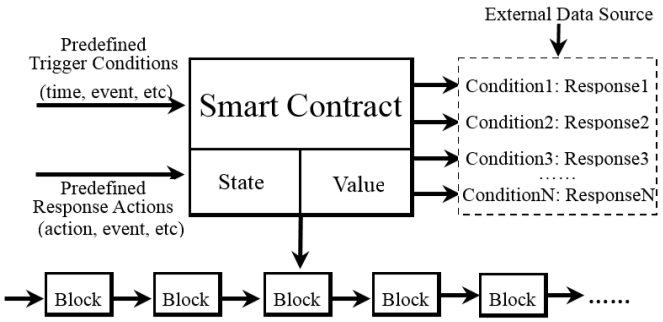

Fig. 5. Blockchain-enabled smart contracts.

Large numbers of novel business models and use cases have emerged, aiming at building a decentralized, disintermediated system with data security. In Section IV, we will present several typical application scenarios for blockchain.

IV. Application Scenarios of Blockchain

Due to its advantages of TRUE and DAO, blockchain has the potential of reshaping many traditional applications. In this section, we briefly discuss four typical application scenarios, each attracting many startup companies and investors.

A. Blockchain-Powered Smart Devices

Blockchain, when integrated with smart contracts and Internet of Things (IoT) technologies, has the potential of transforming devices into automatic "smart properties," and in the future establishing an ecosystem and economy of autonomous agents [25]. Three levels of intelligence, namely data-level, individual-level, and social-level intelligence, may emerge in the life-time management and control of devices or vehicles.

First, the data-level intelligence basically takes advantages of the techniques in the data layer in Fig. 3, and helps maintain a globally shared and secured ledger. The data in life-time events including manufacturing, registration, sales, leasing, maintenance, and insurance, as well as real-time sensor data including position, speed, and mileage, can be perceived and recorded in the blockchain ledger and synchronized to all stakeholders. This can radically reduce costs in device management, for instance, for used car sale and leasing industries.

Second, mobile devices or vehicles, especially driverless cars or drones, may become autonomous and adaptive agents that possess individual intelligence, and interact and trade with other devices without intermediation [26], [27]. Thanks to the contract layer, we can imagine that vehicles are controlled by a cyber driver, which is an intelligent agent equipped with various algorithms and strategies, acting according to globally agreed mechanisms, protocols and rules written as smart contracts on the blockchain ledger. This cyber driver manages, controls, and even own a physical vehicle, constituting a parallel driverless vehicle [23], [28]. Also, the cryptocurrency in the incentive layer makes it possible for vehicles to trade and pay for services such as self-parking, tolls, Wi-Fi hotspots, radars, laser rangefinders, among others. Using blockchain-based E-wallets, vehicles can send and receive bitcoin-like cryptocurrencies in a disintermediated fashion, and maximize its revenue on behalf of its human owner, or even itself.

Third, in the consensus and network layers, the P2P consensus-based control makes it possible to apply blockchain idea in swarm robotic systems with social intelligence. Generally speaking, one of the striking features of swarm robots is lacking of global knowledge, explicit communication models and central authorities, and relying on local communication among neighboring robots. Using blockchain, the globally shared ledger can serve as a good solution to decentralized control problem. The robots, such as a fleet of unmanned vehicles, vessels, or drones, can reach a decentralized consensus by competing for the right of encapsulating their beliefs, desires, or intentions in blocks on the shared ledger, using specific consensus algorithms ranging from the inefficient but secured PoW to the simple majority voting. Meanwhile, the self-executing smart contracts agreed among robots can help reduce the social complexity caused by human interventions to the systems, and thus evolve the swarm system from a complex Merton system to a predictable and tractable Newton system. This blockchain-based swarm robotics idea is particularly effective for dynamic and open systems, and can help realize the so-called device democracy and decentralized robot autonomy [24].

B. Decentralized Sharing Economy

Blockchain can serve as a key enabling technology for the next generation of sharing economy. Although representing an important step toward economic disintermediation, most of sharing economy applications including Uber and Lyft are essentially centralized with online platforms serving as middle-mans, resulting in unsatisfactory centralized decisions or risks such as surge pricing and privacy leaks. Blockchain-powered sharing economy can be considered as a completely decentralized and disintermediated model, which offers secured, immutable, and P2P-stored shared ledgers for all those transactions, representing the future shared economy 2.0.

One of the most successful application scenarios, so far, is real-time ride-sharing. As illustrated in [6], Lazooz, widely publicized as the blockchain version of Uber, aims to build an open-source, worldwide, and decentralized social transportation network. Lazooz enables private car owners to share their empty seats with others traveling the same route.

The underlying operation mechanism of Lazooz basically follows our six-layer blockchain model. Any device running the DApp [29] of Lazooz, e.g., smartphones, wearable devices, and computers of its community of users, can be registered as a "road miner" in the Lazooz blockchain network. The realtime data generated in the network will be verified and stored in a community-maintained crypto-ledger, through which all ride-sharing behavior, schedules, and payments are coordinated and executed (the data layer). Road miners are interconnected in a P2P fashion without any central authority (the network layer). Rather than the commonly used consensus algorithms such

as PoW, PoS, and DPoS, Lazooz designed a novel consensus algorithm called "proof-of-movement," which encourages road miners to drive with Lazooz's DApp running on their devices. This way, road miners can contribute to the community by sharing their data along the way and helping Lazooz weave the local social transportation Web (the consensus layer). As reward, Lazooz automatically generates new tokens called zooz to road miners, and these tokens can be used to pay for ride-sharing and other transportation services (the incentive layer). Furthermore, various algorithms are designed and integrated into Lazooz's DApp. These algorithms can be used to make specific decisions without human intervention, e.g., detecting the usage rate of specific geographic region and activating the service in the region where the number of active users exceeds the "critical mass," and so on (the contract layer). To summarize, Lazooz can be viewed as a decentralized, self-managed DAO. Its formal decisions are collectively made by the community according to each users weight, which represents the users contribution to the community and will be updated via public voting process. In our viewpoint, Lazooz, together with Arcade City and other companies with the similar business model, represent the future trend of blockchain-enabled social transportation and will reshape the sharing economy [6], [30], [31].

C. Blockchain-Powered Freight Transportation

Freight transportation, especially the global shipping industry, plays a vital role in modern transportation systems and international economy. However, many long-standing problems, especially the undesirable operational costs, efficiency, and data interoperability, remain open in this area. Blockchain can serve as a potential solution to tackling these problems. Using blockchain, service providers can create a permanent digital shared ledger of transactions, on which a distributed network of stakeholders can communicate and coordinate with each other according to unified standards and procedures. Designated parties can cryptographically add record to and retrieve data from the ledger using any devices including mobile phones, tablets, and personal computers, eliminating the need for costly and proprietary infrastructure and radically reducing the complexities. To sum up, this blockchain-based solution has the potential of evolving traditional freight transportation to better track orders and assets, reduce errors and frauds, increase operational transparency ,and offer greater security.

As an illustrative example, we here briefly introduce Blockfreight, a startup aiming at designing open-source, immutable, and distributed end-to-end blockchain solution specifically for the shipping industry. Technically, the primary payload of transactions is the important commercial documents including electronic bill of landings, stored using the InterPlanetary File System protocol. The blockchain network runs with the P2P gossip protocol for broadcasting and transmitting unconfirmed transactions, which will be validated using the Tendermint consensus. Blockfreight issues tradeable tokens, typically worth $1 each, to be used to pay for the transaction and network fees and eliminate spam on the decentralized systems. Finally, in the contract layer, customers can use smart contracts to permanently and securely define the bill of lading, payment terms, and other elements to a completed cargo shipment, built on the ETH blockchain.

D. Blockchain-Based Enterprise Management and Knowledge Automation

Blockchain, together with blockchain-powered smart contracts, have the potential of reshaping traditional enterprise management process, especially in its knowledge automation workflows including modeling, validation, integration, and implementation. Knowledge automation can be considered as a novel research direction for further development of artificial intelligence technology, and also a general framework for dealing with management of complex business processes. The goal of knowledge automation is from UDC to AFC, that is, dealing with complex management issues of uncertainty, diversity, and complexity with capacity of agility, focus, and convergence [24].

More specifically, blockchain can be integrated into enterprise business process in the following aspects. First, blockchain-powered smart contracts can help automate the rules and regulations predefined by enterprise managers, so as to reduce the operation costs and the human intervention. Second, internal tokens or coins can be designed and issued as incentives to help improve the employees' performance. Third, enterprise data can be stored in a decentralized and secured fashion, and validated using a consortium blockchain by all departments in the enterprise. Finally, employees can cooperate with each other on a specific task, forming various DAOs. This can help flatten the organization structure, and improve the management efficiency and effectiveness.

V. Conclusion

As fundamental technologies with transformative potentials, blockchain and cryptocurrencies have found a wide spectrum of application scenarios in various types of industries, ranging from the underlying techniques of data storage, encryption, and verification, to the middle level of finance and asset management, and to a variety of high-level business models. In this paper, we present the technical details of Bitcoin and other cryptocurrencies, propose a six-layer reference model for the blockchain framework, and discuss several potential application scenarios. The main aim of this paper is to stimulate more detailed investigation and innovative research in this new direction.

References

[1] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Sebastopol, CA, USA: O'Reilly Media, 2015.
[2] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.
[3] Y. Yuan and F.-Y. Wang, "Blockchain: The state of the art and future trends," *Acta Automatica Sinica*, vol. 42, no. 4, pp. 481–494, 2016.
[4] C. L. P. Chen and C.-Y. Zhang, "Data-intensive applications, challenges, techniques and technologies: A survey on big data," *Inf. Sci.*, vol. 275, pp. 314–347, Aug. 2014.
[5] S. Nakamoto. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[6] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, Rio de Janeiro, Brazil, 2016, pp. 2663–2668.
[7] F.-Y. Wang, "Blockchain intelligence: Cornerstone of the future smart economy and smart societies," in *Proc. 2nd World Intell. Congr.*, Tianjin, China, 2018.
[8] *Blockchain Monitoring Website*. Accessed: Jan. 8, 2016. [Online]. Available: https://blockchain.info/
[9] *Cryptocurrency Monitoring Website*. Accessed: Nov. 24, 2015. [Online]. Available: http://coinmarketcap.com/
[10] *World Economic Forum Survey*. Accessed: Feb. 21, 2016. [Online]. Available: http://www.coinfox.info/news/3184-world-economic-forum-survey-10-of-global-gdp-may-be-stored-with-blockchain-technology-by-2027
[11] *CoinDesk Report*. Accessed: Feb. 21, 2016. [Online]. Available: http://www.bitcoin86.com/news/3527.html
[12] N. Modiri, "The ISO reference model entities," *IEEE Netw. Mag.*, vol. 5, no. 4, pp. 24–33, Jul. 1991.
[13] X. Wang, L. X. Li, Y. Yuan, P. J. Ye, and F.-Y. Wang, "ACP-based social computing and parallel intelligence: Societies 5.0 and beyond," *CAAI Trans. Intell. Technol.*, vol. 1, no. 4, pp. 377–393, 2016.
[14] X. Wang, X. H. Zheng, X. Z. Zhang, K. Zeng, and F.-Y. Wang, "Analysis of cyber interactive behaviors using artificial community and computational experiments," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 6, pp. 995–1006, Jun. 2017.
[15] F.-Y. Wang, Y. Yuan, X. Wang, and R. Qin, "Societies 5.0: A new paradigm for computational social systems research," *IEEE Trans. Comput. Social Syst.*, vol. 5, no. 1, pp. 2–8, Mar. 2018.
[16] T. V. Lakshman and A. K. Agrawala, "Efficient decentralized consensus protocols," *IEEE Trans. Softw. Eng.*, vol. SE-12, no. 5, pp. 600–607, May 1986.
[17] C. L. P. Chen, G.-X. Wen, Y.-J. Liu, and F.-Y. Wang, "Adaptive consensus control for a class of nonlinear multiagent time-delay systems using neural networks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 25, no. 6, pp. 1217–1226, Jun. 2014.
[18] J. Fan, L. T. Yi, and J. W. Shu, "Research on the technologies of Byzantine system," *J. Softw.*, vol. 24, no. 6, pp. 1346–1360, 2013.
[19] D. Kraft, "Difficulty control for blockchain-based consensus systems," *Peer-to-Peer Netw. Appl.*, vol. 9, no. 2, pp. 397–413, 2016.
[20] Y. Yuan, F.-Y. Wang, and D. Zeng, "Competitive analysis of bidding behavior on sponsored search advertising markets," *IEEE Trans. Comput. Social Syst.*, vol. 4, no. 3, pp. 179–190, Sep. 2017.
[21] Y. Yuan, D. Zeng, H. M. Zhao, and L. J. Li, "Analyzing positioning strategies in sponsored search auctions under CTR-based quality scoring," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 45, no. 4, pp. 688–701, Apr. 2015.
[22] J. J. Li, X. C. Ni, and Y. Yuan, "The reserve price of ad impression in multi-channel real-time bidding markets," *IEEE Trans. Comput. Social Syst.*, vol. 5, no. 2, pp. 583–592, Jun. 2018.
[23] F.-Y. Wang, Y. Yuan, C. M. Rong, and J. J. Zhang, "Parallel blockchain: An architecture for CPSS-based smart societies," *IEEE Trans. Comput. Social Syst.*, vol. 5, no. 2, pp. 303–310, Jun. 2018.
[24] Y. Yuan, T. Zhou, A. Y. Zhou, Y. C. Duan, and F.-Y. Wang, "Blockchain technology: From data intelligence to knowledge automation," *Acta Automatica Sinica*, vol. 43, no. 9, pp. 1485–1490, 2017.
[25] S. Li, L. D. Xu, and S. Zhao, "The Internet of Things: A survey," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, 2014.
[26] K. Dorling, J. Heinrichs, G. G. Messier, and S. Magierowski, "Vehicle routing problems for drone delivery," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 1, pp. 70–85, Jan. 2017.
[27] H. Li, D. H. Pan, and C. L. P. Chen, "Intelligent prognostics for battery health monitoring using the mean entropy and relevance vector machine," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 44, no. 7, pp. 851–862, Jul. 2014.
[28] D. Wen, Y. Yuan, and X.-R. Li, "Artificial societies, computational experiments, and parallel systems: An investigation on a computational theory for complex socioeconomic systems," *IEEE Trans. Services Comput.*, vol. 6, no. 2, pp. 177–185, Apr./Jun. 2013.
[29] M. Swan, "Blockchain thinking: The brain as a decentralized autonomous corporation [commentary]," *IEEE Technol. Soc. Mag.*, vol. 34, no. 4, pp. 41–52, Dec. 2015.
[30] *La'zooz Website*. Accessed: Feb. 2, 2018. [Online]. Available: http://www.lazooz.org/
[31] *Arcade City Website*. Accessed: Feb. 2, 2018. [Online]. Available: http://arcade.city/

Yong Yuan (M'15–SM'17) received the B.S., M.S., and Ph.D. degrees in computer software and theory from the Shandong University of Science and Technology, Shandong, China, in 2001, 2004, and 2008, respectively.

He is an Associate Professor with the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing, China, and the Vice President of the Qingdao Academy of Intelligent Industries, Qingdao, China. He has authored over 90 papers published in academic journals and conferences. His current research interests include blockchain, cryptocurrency, and smart contract.

Dr. Yuan is currently an Associate Editor of the IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS, and *Acta Automatica Sinica*. He is the Chair of the IEEE Council on RFID Technical Committee on Blockchain, the Co-Chair of the IEEE SMC Technical Committee on Blockchain, and the Director of the Chinese Association of Automation Technical Committee of Blockchain. He is the Secretary General of the IEEE SMC Technical Committee on Social Computing and Social Intelligence, the Vice Chair of the IFAC Technical Committee on Economic, Business and Financial Systems (TC 9.1), and the Chair of the ACM Beijing Chapter on Social and Economic Computing. He is also the Secretary General of the Chinese Association of Artificial Intelligence Technical Committee on Social Computing and Social Intelligence, and the Vice Director and the Secretary General of the Chinese Academy of Management Technical Committee on Parallel Management.

Fei-Yue Wang (S'87–M'89–SM'94–F'03) received the Ph.D. degree in computer and systems engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 1990.

He joined the University of Arizona, Tucson, AZ, USA, in 1990 and became a Professor and the Director of the Robotics and Automation Laboratory and Program in Advanced Research for Complex Systems. In 1999, he founded the Intelligent Control and Systems Engineering Center, Institute of Automation, Chinese Academy of Sciences (CAS), Beijing, China, under the support of the Outstanding Oversea Chinese Talents Program from the State Planning Council and the 100 Talent Program, and in 2002, he was appointed as the Director of the Key Laboratory of Complex Systems and Intelligence Science and became the State Specially Appointed Expert and the Director of the State Key Laboratory of Management and Control for Complex Systems in 2011. His current research interests include methods and applications for parallel systems, social computing, and knowledge automation.

Dr. Wang was a recipient of the Second Class National Prize in Natural Sciences of China, in 2007, the Outstanding Scientist by ACM for his work in intelligent control and social computing in 2007, the IEEE ITS Outstanding Application and Research Awards in 2009 and 2011, respectively, and the IEEE SMC Society Norbert Wiener Award in 2014. He was the Founding Editor-in-Chief of the *International Journal of Intelligent Control and Systems* from 1995 to 2000, and the Editor-in-Chief of the IEEE Intelligent Systems from 2009 to 2012 and the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS. He is currently the Editor-in-Chief of the IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS. Since 1997, he has served as the General or the Program Chair of over 20 IEEE, INFORMS, ACM, and ASME conferences. He was the President of the IEEE ITS Society from 2005 to 2007, the Chinese Association for Science and Technology, USA, in 2005, and the American Zhu Kezhen Education Foundation from 2007 to 2008. Since 2008, he has been the Vice President and the Secretary General of Chinese Association of Automation. He is elected as a fellow of INCOSE, IFAC, ASME, and AAAS.