How does the blockchain technology affect finance and economy?

Boyang, Tang ID:6429449 UPI:btan766

I. Introduction

Motivation

According to recent statistics, approximately 90% of banks around the world are investing in blockchain solutions by 2018, and about 14% of financial market institutions plan to go into blockchain production in 2017. Before discussing the underlying technology of the blockchain and its potentials in finance and economy, it is good to look through some top issues among current financial services, digital economics, industries or enterprises, etc.

Intuitively, security is the object that the most necessary in every aspect of the society. There is no doubt that security issues are still the most significant challenge remains in traditional and emerging areas of finance. One of the most dangerous areas for financial institutions for some time will be cybersecurity risk [7]. The core fundamental of transactions is the security, which protects businesses and allows them to innovate or build new products and services. Although the rapid digital disruption on a massive scale, which enhances efficiency, flexibility and unlimited customization. But meanwhile, it drives an ever-evolving and dynamic threat landscape. The digital security risk is traditionally regarded as a technical problem since the growth of digitization, while achieving an effective security approach is complicate and not that easy.

In addition to above concerns, another risk is the data breach incident, which affects financial or personally identifiable information that calls for specific actions on the part of financial institutions. A considerable amount of personal data can be easily collected from various sources since the number of entities such as online retailers, Internet Service Providers, financial service providers (banks, credit card companies, etc.) and governments are increasingly growing up [9]. Economic can get benefits of reusing and sharing of data, however, the disclosure of personal data and privacy would cause some sensitive information and hidden patterns to be misused in illegal ways. In the current situation, it is not easy for regulators to achieve a good trade-off between standards for protecting sensitive data and sharing information.

Moreover, in the current network-centric business model, it is becoming increasingly difficult to validate a personal identity, control an access, and maintain integrity and privacy of data. It is mostly due to the transparency of transactions is not enough [8]. The aim of transparency is trying to enhance reliability by ensuring that information on so-called securities financing transactions is efficiently reported to the trade repositories and investors. For example, transparency could prevent financial middlemen (such as banks) from attempting to circumvent regulations by shifting parts of their activities to less-regulated shadow sector. Although financial services could obtain benefits of transparency, it would lead to time-consuming and extensive cost when implementing technologies to monitor financial systems [6].

Why blockchain?

By summarizing all above concerns in the financial marketplaces, the core idea behinds a successful transaction is the trust [1,4]. Generally, people usually find ways to lower uncertainty about one another so that they can exchange value. In conventional, we are under some institutions that formulated by governments or regulators. As our society grew more complex and our trade routes grew more distant, we built up more formal and powerful institutions, such as banks, governments, corporations. These institutions helped us manage our trade, while some common constraints such as the uncertainty, management complexity, and transparency problems. Our personal control was much lower. Recently, we put these same institutions on the internet. The platform marketplaces like Amazon, eBay, Alibaba, which are faster institutions that act as middlemen to facilitate human economic activities [4].

There is a common among above-mentioned situations, they are centralized, or say, the transactions must rely on the third-party, otherwise we would encounter many risks. Unlike traditional economic institutions, which are promised to lower uncertainty. While we can do it with technology alone, and that is called Blockchain. The blockchain technology is a decentralized database that stores a registry of assets and transactions across a peer-to-peer network [5].

But why blockchain has been viewed as an evolution and so crucial to current financial markets. Basically, this is because of the public registry of who owns what and who transacts what. All transactions are secured through cryptography, there are many chains and each of them is formed by connected blocks. And over time, any transaction history will be locked in a block, whose data that is cryptographically linked together and secured. All the transaction records across the internet are immutable and unforgeable, and each record is replicated so that every computer that uses the same network can access it [1,11]. It seems that we don't need banks, corporations, or other institutions anymore, and everything is secured and reliable, which shows that the blockchain would radically transform the

economy [10]. The rest part of the report will look insight into the details of blockchain technology and illustrate some useful applications that facilitate the understanding of what influences the blockchain has on finance and economy.

II. RELATED WORK

A. Blockchain in real-world scenarios

From the technical point of view, blockchain is a low-level infrastructure. Its scope of application is not limited to the financial industry, just like big data can be used in the financial industry as well as in other sectors [1,12]. For the financial industry, the feasibility of the application of blockchain in many segments has been repeatedly discussed in the past few years. In numerous discussions, people have many misunderstandings about the blockchain, and often portray the blockchain as a concrete technology or concept, such as "distributed ledger", "smart contract", and "cryptography". As in fact, each of them is a branch of the blockchain, but cannot represent the blockchain alone.

In essence, the blockchain is a "consensus system" that involves multiple parties and is a robust security mechanism under an open architecture [14]. As mentioned before, the overview of the blockchain technology talks about establishing a shared and decentralized database that stores a registry of assets and transactions across a peer-to-peer network. Of course, so far people still partially grasp the knowledge about the blockchain. It would be helpful for understanding the blockchain through its mathematical model and some life scenarios.

The blockchain is not mysterious and many similar scenarios really exist in our life. For example, the fruit market is the place that most people visit. It is easy to find that is an open, freely priced market, fruits of the same quality that sold at different booths are always with the same price. It is very interesting to think carefully about this phenomenon because the owner of different booths are not allies and there is no situation of joint pricing. However, in such a decentralized, non-trusty, and price-converging environment, if there is an owner decides to increase prices unilaterally, he/she will undoubtedly face the problem of disappointing sales of goods. If prices are unilaterally reduced, although sales will increase, it means that there is no profit or even a loss of sales. In other words, after a full game of all participants in the market, the price of the commodity will reach a stable state (that is "consensus"), and any participant who attempts to unilaterally changes its pricing strategy and tries to undermine this status will be automatically eliminated.

Thus, the essence of the blockchain is such a "consensus system" that involves multiple parties. From the engineering control point of view, the blockchain is not statically implemented by a control, but by designing a game filed to achieve a virtuous competitive incentive mechanism: that the participants who abide by the rules will gain benefits, and the destruction of the rules will certainly be sanctioned [14].

In addition to above economic example, we can also look at a phenomenon that is very common in social activities. For instance, there are often hidden rules in the workplace. Although there are no express provisions, everyone will follow in unison, when a new person enters the work unit. After a period, whether it is a state-owned enterprise, a foreign enterprise or a national administrative department. The language, dress and work style will gradually merge into the unique culture of the organization. This culture is not a legal or mandatory requirement, but it is recognized by all in that organization and it continues to influence new entrants. From a broader perspective, any community, group, or nation has certain ideologies that have reached a consensus during a long time (such as the Chinese custom of returning from the Spring Festival). We can say this kind of "consensus system" is the mechanism of the blockchain, to a certain extent, enables society to operate in an orderly manner [14,15]. It is a strong security mechanism under an open architecture.

From the perspective of mathematics, the famous American mathematician John Nash proposed an essential concept in his doctoral thesis "Non-Cooperative Games", which was later called Nash-equilibrium game theory [16]. In brief, Nash-equilibrium mathematically proves that in a non-cooperative (non-trusted) gaming environment, each participant makes autonomous decisions that are independent of others. Such a strategic combination will eventually reach a point of equilibrium which makes it impossible for participants to change their strategy alone and increase their earnings. In other words, under the principle of Nash-equilibrium, any participant who wants to change his strategy alone will not obtain benefits any longer. The essence of the blockchain is to achieve a consensus system with Nash-equilibrium. It is a kind of benign game mechanism, rather than pure technological innovation.

B. Lower uncertainties by using blockchain

In this part, we will technically explain how the blockchain achieves this consensus system by reducing uncertainties. The blockchain can be thought of as an open infrastructure, which stores many kinds of assets. More specifically, it stores the history of ownership and the location for assets like digital currency, or other digital assets. Those assets could be a certificate, a contract, real-world objects, or even personally identifiable information [5,17]. But the point is how blockchains lower uncertainty and how they therefore promise to transform our economic systems in radical ways.

As mentioned before, in economics, uncertainty is a significant term that can be briefly concluded into three aspects: not knowing whom we are dealing with, not having visibility into a transaction, and not having records if things go wrong. The first aspect is actually talking about identity management [12,17]. Suppose people who want to buy an iPhone on the internet, the first thing they will do is to look up whom they are buying from. The profiles, great reviews, and ratings may be used as attestations to lower uncertainty when a transaction happens. But the problem is that they are very fragmented. Blockchains allow us to create an open and global platform on which to store any identification about any entity from any place. A user-controlled portable identity can be realized by this

way. Unlike presenting a profile to public, it allows you to selectively reveal the useful attributes about you that help facilitate trade or interaction, and in the meanwhile, it protects personal information that irrelevant [12]. Having this kind of portable identity around the physical world and the digital world, which means it enables to do all kinds of human trade in an entirely new way.

The second aspect of uncertainty we usually face is just not having enough transparency in our interactions [17]. Assuming that the iPhone is sent by mail, people want to know that the product they bought is same on that arrives in the mail and that there is some record for tracking it. As in fact, not just for electronic stuff like iPhones, but for all kinds of goods or assets, any kind of data or product that they don't want tampered with. The problem in many companies, especially those produce complex products such as smartphones, they always manage all different vendors across a horizontal supply chain. All of these people are working on the same product, but they don't have the same database, or they don't use the same infrastructure. In other words, there is an existence of information asymmetry. So, it becomes tough to evolve a product transparently over time. However, using the blockchain that we can create a shared reality across non-trusting entities. Then all of these vendors and companies can interact by using the same database without trusting on one another [17]. Therefore, for consumers, they can have more transparencies. As a real-world object travels along, we can see its digital certificate or track information move on the blockchain.

The last aspect of uncertainty that we often face is one of the most open-ended and it is the reneging on deals. What if suppliers don't send products to their customers? Is there a way that promises to get customers' money back? Blockchains allow to bind contracts between individuals and then guarantee that those contracts will bear out without a third-party enforcer. In other words, when you are financing an iPhone, but you don't need to release the funds until you can verify that all the conditions have been met. This might be one of the most exciting ways that blockchains lower our uncertainties. Since that people can collapse institutions and their enforcements in some degree [18]. Thus, rather than requiring institutions that slow down economic activities, we can harness all of that collective uncertainty by using the blockchain to collaborate and exchange more faster and more open.

III. APPLICATION OF BLOCKCHAIN IN BANKING SERVICES

Blockchain solutions are enhancing banking experiences for customers by considering transaction time from hours to seconds. It removes manual processes and reduces friction in day-to-day trade finance, digital identities, and cross-border payments [20]. With blockchain, you can conduct business more quickly and securely. Transaction records have been moved from paper-based to blockchain-stored, which provides an easier expansion to understand financial markets such as small and medium enterprises [19]. There are several blockchain use cases that are proposed to enhance the banking experience:

A. Bitcoin

The blockchain firstly entered the public view was with Bitcoin together. In fact, the underlying technology of Bitcoin is the blockchain. It would be a good way to figure out what influences that blockchains have on real-world finance and economy by combining the concept of the digital currency with current financial services.

Currently, the internal trade on the internet is naturally subject to the weakness of trust-based model. This weakness is produced in the case of physical cash missing that leads to uncertainties in sale costs and payment issues. The internet trading systems usually use a credit card, electronic transfer or other processes to complete a payment, which makes it impossible to achieve a completely irreversible transaction. The potential refunds may never be excluded. The buyers would always have a doubt about the actual goods that might not be fully satisfied by their expectations, or have a doubt about whether the goods will be transferred on time after payments. At the same time, it is inevitable that a certain percentage of fraudulent customers exist in business activities. They might claim a refund for the loss of goods but indeed they have received the goods already. So, the suppliers must watch out for their customers to prevent an increase in the cost of sales. Therefore, both vendors and purchasers must have to choose a financial institution as a trusted third-party intermediary, which acts as the transaction endorsement and comes forward in the event of a disputation.

However, the existence of financial intermediaries not only increases the cost of the transaction but also limits the practical minimum transaction size, as well as many transactions of goods and services that cannot be returned on their own. This points out the biggest barrier of E-commerce, which is the credit [7]. In fact, the global financial crisis that began in 2008 has been largely due to the inaccurate assessment of credit that obtained from financial institutions.

The Bitcoin technique might be an excellent choice to address the urgent needs of the moment. It introduces a solution that an electronic payment system based on cryptography rather than credit. A purely distributed peer-to-peer system that is arranged to generate and record transaction ledgers in accordance with time sequence, thereby effectively preventing possible rollback payment transactions. Making payments directly between any points that have a common agreement, no third-party intermediary involvement is required [5,17]. This method is designed to endorse the use of a password, which enables to avoid the difficulty of establishing credibility among buyers and sellers. So, the transactions between the two sides will be secured even they do not trust each other.

To be more specific, every single owner of a digital currency must have to add a signature at the end of the currency. The signature is generated by a random hash function, and digital currency is encrypted by using the next owner's public key. And then, adding the signature to the end of this digital cryptocurrency, which will be sent to the next owner. While the recipient can use their unique private key to decrypt the signature, the authenticity of the content will be examined after obtaining the hash value, thereby verifying the identity of the previous owner [21]. As a result, a group of blocks that consists of data will be formed after every transaction.

In fact, there is a fatal weakness within the payment process as described above, it is called Double-Spending problem [22]. Which it is easy for a payment intermediary to solve this problem, as long as dealing with only one transaction at the same time. But the pursuit of the Bitcoin payment system is to be decentralized. To achieve this purpose, a mechanism called Timestamp is proposed into this system. A time stamp is added to every block, and it is still generated by a random hash function, which will be broadcasted across the whole network [21]. Since ensuring that a transaction does not exist, the only way is to know all the transactions that happened.

Moreover, to make sure that the information on the chain cannot be tampered, the Bitcoin payment system introduced the "Proof of Work", which adds a random number to each block. The random number starts with a zero or a range of zeros, as the number of zeros increases, the time required to find the solution grows exponentially, but only one random hash calculation can test the result [21]. When a node wants to generate a block, it must to find this random number by repeated attempts, this will cause a quite high cost of the CPU workload. Before the completion of a considerable amount of work, any information of this block cannot be changed.

B. Legal digital currency

The Bitcoin system has a strong network, whose core idea is trying to get benefits of a distributed peer-to-peer database system. The system is non-unique, since the source of Bitcoin is public. Other virtual currencies are very similar to Bitcoin, they could be created by modifying the parameters [23]. The Bitcoin network is a value transmission protocol. It has at least three attributes, which are finance, technology, and sociology [17, 21]. From the financial point of view, Bitcoin has a fixed number, and it is not necessary to take it with you. And it is highly favored by the public as the transaction cost is very low. Also, the development space is huge, therefore, more and more investors believe that is "electronic gold" and can become a kind of digital investment products or global standardized digital assets [21,23]. Also, Bitcoin is circulated around the world based on the internet, and on specific occasions such as cross-border payment and virtual economic value transmission, it is very efficient to use it for transactions [24]. At the same time, Bitcoin as a kind of currency can be assumed to be a financial instrument, which can be applied in the process of financial globalization to improve the problem of low efficiency, high cost, and other issues.

Money is the foundation of finance and the universal medium for all economic activities based on value exchange. Needless to say, the statutory digital currency scenario will be extremely large, complex, and of important financial strategic significance.

What needs to be emphasized here is that one of the most important implications of using blockchain to advance statutory digital currency is to pre-empt international standards [25]. From the perspective of national strategy, the development of legal digital currency standards, including the development of data structure standards for "basic data units" and consensus protocol standards for "data flow chains". The importance of them in the financial domain is similar to the importance of developing the TCP/IP internet protocol standard in the IT field [23,25].

This looks like a kind of competition of a technical protocol or a commercial standard, which affects the fundamental interests of national security. Imagine that in the future, when the legal digital currency becomes the globally accepted currency, which country has mastered the standards for the issuance and circulation of the legal digital currency, it will have a huge impact, which likes a subtle and profound global financial expansion.

C. Cross-border payments

The blockchain technology can achieve a transaction from point to point, also can share and monitor the transaction data across the whole network. This can effectively enhance the efficiency of traditional banking payment settlements and reduce the transaction cost [24].

Take the cross-border payment for example, if one account holders want to transfer money from a small bank of their country to another small overseas bank, there are usually four steps: 1. account holders make remittances to their small banks; 2. the small banks make an application to the large banks in the same country; 3. the large banks make an electronic transfer to the large overseas banks that they have made an agreement on corporation; 4. The large overseas banks send money to small overseas banks [2,24]. This long process almost takes 3 to 10 days, and the transaction fees are very high. Additionally, the lengthy and complicated intermediate links lead to the high cost of labor.

Adding the blockchain technology into cross-border payment system can make it possible to pending a transaction of remittance directly, and then finding a receiver who has the public key in the bank blockchain system, thereby completing the transaction within a few seconds. Thus, the fundamental pain of the traditional cross-border payment system can be addressed by a join of payment system with the blockchain.
Modern commercial trade transactions are usually liquidated with the help of banks. During the process of cross-border payment, every single institution in the system has its own accounting process. Thus, it is essential to sign a cross-border exchange agreement, which takes a lot of costs and time for reconciliations, payments, and settlements among institutions. The high cost and low efficiency would cause many exchange risks.

First, if the remitting bank or receiving bank does not have the cross-border exchange qualifications, they must have to go through the transit of large banks. It would cause the collection of transit fees, this cost will be priced according to the agreement between those banks. And the sender does not know the exact cost of the transit fees, thus they will generally add fees as necessary to ensure that the recipient can receive the full amount [2].

Second, the safety and convenience are regarded as the core troubles of traditional cross-border payments. The reliability of trade will produce a difference in accordance with the level of development of trade in that country. And the cross-border payment transactions can only be initiated by the bank during working hours. In addition, when account holder wants to make

a payment to abroad, they must make a conversion to foreign currency first, and it must be done online or at a bank counter. The procedure is cumbersome and time-consuming, which make it lacks user-friendliness [20].

Finally, the cross-border payment processes are slow and inefficiency, that is because of the long transit links with a number of banks and payment systems. Generally, the cross-border transfers need to undergo 3 to 10 working days. For the people who are familiar with long-distance transactions, they may not be affected by the delay of payment. While for some manner of time-sensitive recipients, the lag in payment will result in negative effects [20, 24].

Blockchain technology can solve the problem of bank transfer in traditional cross-border payment platforms. The blockchain enables to directly form a peer-to-peer payment, eliminate the tedious aspects of intermediary organizations, and make cost-effective and real-time cross-border payments possible.

The subversive improvement of traditional payment and settlement systems by using the blockchain technology is mainly reflected in the increased safety, high efficiency, and low transaction costs. Since the launch of blockchain technology, the average daily transaction volume, total amount, and average transaction amount for the international payments and settlements have dramatically grown [1,2]. Demonstrating that blockchain technology plays a significant role in the change of payment and settlement services.

Moreover, from the perspective of technical security, the blockchain system does not need users' personal information and bank account information, the system encrypts the information into a hash value and transmits it to the recipients directly. While the traditional payment system needs personal information to confirm the transactions. The gathering of these personal information and bank information can easily become a way for lawless people to obtain illegal gains. Blockchain technology uses the SHA-256 algorithm, which is a type of hash functions, it will map a binary value with arbitrary length to a hash value of a fixed length. Anything different is mapped to the same compact binary form, which can help in verifying data consistency and integrity [4,12,14].

D. Digital identity

Among all industries, the financial sector is subject to the most rigorous supervision. And the verification of customer identities (KYC) is the prior focus of financial supervision [12]. Traditionally, requiring clients to repeatedly provide identifying information can erode customer satisfaction and cause transaction delays. Onboarding clients for checking accounts or mortgages, or migrating them from one bank to another requires strict compliance with KYC standards. The current status is that financial institutions generally have redundant information collection in the KYC process, and the inefficiency and huge compliance costs that caused by delay in information flow. Blockchain-based digital identities can transfer data between organizations across regions, increase efficiency, and reduce costs. This is the value that blockchain can be brought to various scenarios of traditional banking services.

But more importantly, blockchain-based digital identities can be used as a basic protocol for implementing digital inclusive finance. At present, the pain point of inclusive finance lies in the high cost of users and the difficulty in risk control. While currently digital inclusive finance is using digital technology such as big data that can only be confined to the ecological system of a specific organization in some scenarios (such as mobile payments). And the real cross-organizational, cross-national digital financial architecture and cooperation has not yet been achieved. The fundamental reason is that the cross-organizational, cross-national data (especially sensitive data involving national security and economic livelihoods) cannot be safely shared through traditional methods.

The blockchain is a kind of strong security mechanism under open architecture. The digital identities built on the basic data units and data links of its two core modules, which enable that the identity information, historical activity records, and other identity-related attribute information covered by digital inclusive finance to be securely transferred between institutions and individuals across countries and regions [2,13]. Thereby enabling open and secure sharing of sensitive data.

E. Broader financial security (regulatory) infrastructure

In a sense, the blockchain can be viewed as a new type of security infrastructure. Unlike traditional defensive security technologies based on cryptography, blockchain does not focus on sensitive data that needs protection in the "cloud" or then attempts to build a "safety wall" that resists external intrusions. From the various security incidents that have occurred in recent years, it is not difficult to find that even if there is a solid "city wall", hackers may pass it by constantly trying to find a security hole, since the target data is stored centrally in a fixed location (such as a server). So that breaking into the wall is ultimately only a matter of time. In contrast, the security infrastructure represented by blockchain is a kind of global security. The data in the blockchain is collectively managed and co-existent, the location of the storage is changed at any time; only real and effective data will be connected into the chain, and the forged data will be automatically discarded by the system [4,46].

Money laundering refers to the income generated by illegal ways, which can be covered up through various means such as concealing the source and nature of money, thus formally legalizing the behaviors. The fundamental purpose of money laundering is to change the original form of the proceeds of crime and erase the records of funding sources by converting the assets through multi-channel and multi-mode ways [27]. In order to make the proceeds of crime to become legalized, forcing the criminals to take more extreme and complex tools to achieve their own ends by sacrificing the interests of innocent individuals. The criminals take advantage of the time lag in international transactions, as well as the characteristics of complex operating procedures of the non-uniform system, and then developing the transnational money laundering as an important way to transfer funds. It leads a large span of crimes and serious damages to the international economic system.

Blockchain can be used to optimize the anti-money laundering (AML) process of financial institutions. First, it is possible to track every financial transaction that is mainly due

to the untampered timestamp of a distributed ledger and the characteristics of public autonomy of the entire network [26]. So that it can prevent illegal money flows that caused by regulatory loopholes and inadequate laws, and then significantly reducing the social and economic losses. Second, the credit records and transaction information of all participants are stored in the general ledger of the blockchain system, and shared by each node. Information sharing will reduce the duplication of audit work, thus all new customer data can be quickly located, thereby dramatically reducing time cost and improving efficiency [20]. Moreover, there is an achievement of enhancing the system security and transparency. Since the blockchain is a decentralized database, then no single node can control the entire system, thereby increasing the difficulty of leaking data on a single node. In the meanwhile, the operation of data on any node will be observed by other nodes in the first place, thus strengthening the monitoring of data leakage [23]. In addition, the fundamental identity of the node in the blockchain exists as a private key, which is used for signature verification during the transaction. Only the owner of the information knows the private key. Even if other information is leaked out, as long as the private key is not revealed and the leaked information cannot be matched with the node identity, thus losing the use value [12,27].

IV. APPLICATION OF BLOCKCHAIN IN SECURITIES INDUSTRY

A. Securities market

In traditional securities areas, the initial public offerings (IPO) and securities transactions require financial intermediaries to participate in a long process, which is high-spending and inefficient. While using blockchain allows enterprises and investors to autonomously complete the IPO on a multicenter trading platform, and freedom to make a transaction without any intervention of the financial intermediaries. Once this idea is verified, strengthening the capability of securities consulting, weakening the capability of resource acquisition and underwriting will be a transformation direction of the securities services in the future [3].

With the accelerating innovation in the widespread use of information technology, the internal issuance system of stock exchange corporations has begun to gradually extend to the internet, thus changing the way of issuing and trading traditional securities. However, there also has drawbacks in online securities issuance and trading. First, it only moves the program of issuance and trading to the network, while the preparatory process of issuance and trading, as well as the approval process, have not been simplified [30]. Although online transaction speed has been significantly improved compared to paper-based era, it still needs at least five to six months to approve the issue after a company passing the first trial of IPO. Most of the time spent on a lengthy process of declaration, feedback, and reply. Second, due to the development of network technology is imperfect and inadequate, the transaction processes and the completion of settlement procedures still require third-party intermediaries to be involved [30,31]. Therefore, there is a risk of being hacked on the network, and transaction security is not effectively protected. Securities trading involves a lot of property delivery and privacy information, once a security incident happens such as data leakage, it will cause huge losses to the people.

The blockchain technology greatly simplifies the securities issuance process and enables peer-to-peer direct transactions. Blockchain technology can help in building a market for private equity, then there can be many start-up companies that put their equity systems in this framework and trade them in the future [31]. In addition, as in fact, that the blockchain is an open and transparent database, it includes all past transaction records and other related information which are securely stored in a string of data, where the data is encrypted in a chain of blocks. Moreover, the blockchain technology greatly promotes the development of non-standardized and personalized securities trading. Today, most of the securities that traded on the floor are standardized securities. While for non-standardized securities, especially for the complex financial derivate products which must be intervened by lawyers or other intermediaries to complete the transaction [23,31]. Thus, it takes a lot of labor power, material resources, financial capacity with respect to need. While the combination of blockchain and smart contracts can completely replace the complicated processes of non-standardized securities trading, and can automatically execute complex securities settlements and delivery orders.

B. Smart contracts

Nick Szabo's work theory on smart contracts has not been implemented, one important reason is the lack of digital systems and technologies that can support programmable contracts [28]. The emergence of blockchain technology solves this problem. It can not only support programmable contracts, but also has the advantages of decentralization, non-disruption, and transparent traceability. It is naturally suitable for smart contracts [18,28]. As the examples mentioned in banking services, the blockchain solves the problem of decentralization of currency and payment instruments. But more than that, blockchain makes it possible to convert many different things by using a smart contract. Almost all types of financial transaction can be transformed by binding a contract on the blockchain system, including stocks, private equity, bonds, and other types of financial derivatives such as futures, options, and so on [18,28].

In essence, the smart contract works automatically as an "if-then" programming statement, and it is adopted in this way to interact with real-world assets. When a pre-written condition is triggered, the system automatically executes the corresponding contract terms [28]. The smart contract must first meet the general contract conditions when designing, such as payment methods, liens, confidentiality, and enforcement rights. So that it can minimize the occurrence of malicious attacks or accidents, and reduce the dependence on credit intermediaries. In addition, other relevant economic goals such as reducing fraud losses; controlling arbitration costs, execution costs, and other transaction costs should also be reflected in the smart contracts [28].

In the blockchain system, only the parties of a contract can make an operation on the money, once the contract is

confirmed, the funds involved in the contract would be allocated in accordance with the pre-written conditions of the contract, the funds can only be re-used until the contract expires. During the contractual period or after the contract is entered into force, either party to the contract cannot control or misappropriate the funds [28].

Thus, the smart contracts based on blockchain technology cannot only exert the advantages of smart contracts in terms of cost efficiency but also avoid the interference of malicious behaviors on the normal execution of contracts. The smart contract is written into the blockchain in a digital form, and the features of the blockchain technology ensure that the whole process of storage, reading, and execution is transparent and traceable [20].

V. LIMITATIONS AND CHALLENGES

Although blockchain technology has a widespread application in the financial sector and other domains, most of them are still being conceived and tested, and only a few projects have been implemented. As an emerging technology, the use of blockchain in economic and social production still has a long way to go, and there exists many challenges in the practical applications.

First, the authority of government supervision is being challenged by the blockchain technology, whose development is constrained by the current institutions. More specifically, the leading position of the central banks is challenged by the characteristics of public autonomy and decentralization of the blockchain system. The existing monetary system, bank supervision mechanism, and the function of regulators will be subversively changed by this revolution [31]. For example, the digital currency represented by Bitcoin that not only challenges the national coin-building rights but also influences the formulation and transmission of monetary policy. Weakening the central bank's centralization position and its ability to control the economy will lead to the high cautions about digital currencies. Second, the establishment of laws and regulations for the blockchain technology is lagging, leading the testing and promotion of this new technology to be hampered [33]. In the future, the development and promotion of the blockchain must be bound to the improvement of regulatory mechanism as well as a sound economic environment.

In addition, the blockchain technology faces technical limitations, since the blockchain network is built on a large number of trusted computing nodes. An important issue of maintaining the development of blockchain is to ensure that a large number of trusted nodes are not destroyed by hacking or data corruption [33]. Especially for improving financial services, which requires participants to share data and resources, thereby jointly building a distributed ledger. Thus, the issue of trust among cooperation agencies is also an important cornerstone for the development of the blockchain [29,33].

Finally, the development of blockchain is constrained by block capacity. As we known, the Bitcoin is the most discussed use case of blockchain in the financial market, its daily transaction volume can reach 200,000 and the capacity of general ledger is around 50GB, while that is only a fraction of traditional bank transaction volume. However, under the premise that the blockchain system has not been widely used by the entire financial industries, there already has a problem of slow transaction aging [5,29]. A large amount of unprocessed and unconfirmed transactions occupies cache space, which severely hampers the system speed. Moreover, the blockchain system has a high requirement on the computer configuration of the server, which intensifies the investment in equipment costs and resources [26,33].

VI. FUTURE WORK

In order to ensure a stable development of the digital money market and blockchain financial system, the supervisory departments not only need to learn from the experience of foreign policy and system construction, but also have to design a system that around the reform of financial industries.

At the national level, the current blockchain and other new technologies will have a major impact on monetary system and financial market. The original economic and financial policy framework will not keep up with the changes in the technological situation. Regulatory authorities should keep pace with the times and cooperate with commercial banks and securities companies in the financial sector, making full use of financial technologies to enhance supervision methods and regulatory measures. The trend shows that there might have three major directions:

1. Open the market access restrictions. Take the digital currency as an example, to lower the threshold for the issuance of digital currency licenses, gradually allowing digital currency issuers to participate in or engage in more economic and financial activities. And encouraging the blockchain start-ups to join the financial market, thereby promoting the competition in the entire market.
2. It is time to develop international standards of the blockchain. At present, the blockchain regulatory framework has not yet been published in the global scope, and there are no specific laws to restrict the blockchain financial behaviors. Therefore, the regulatory authorities should seize the opportunities brought by the blockchain and encourage financial institutions to actively prepare for the development of international standards. Furthermore, the alliance made among financial technology companies would be very helpful to make breakthroughs in technical bottlenecks.
3. The last is to strengthen the effective supervision of the blockchain financial institutions. It is essential to scientifically classify the blockchain financial institutions, in order to carefully understand the dynamics of the real-time blockchain financial industries. Thus, making the real needs of the financial markets as the basis for regulation. In addition, it is urgent to strengthen the trial of blockchain financial applications and step up the development of blockchain financial infrastructure.

VII. CONCLUSION

With the application of blockchain technology in many fields, especially in the banking services and financial industries, this has caused the boom in blockchain technology to get hotter.

People have a higher expectation for the blockchain technology, more and more companies are beginning to join the field of the blockchain, thus being able to put the blockchain to use in the first place. Although the blockchain technology has its own charm, and it is also regarded as the key of the next-generation technology revolution, but the blockchain still faces many problems and challenges.

The core idea behind the blockchain is the consensus mechanism, whose characteristic is that when a transaction occurs, it can only be completed in the place of acquiring all nodes' confirmations. However, the consensus is prone to fail when the blockchain is applied in a large-scale area with many transactions occurring at the same time, it may due to some misleading factors.

In addition to the problems faced by the operating mechanism, the blockchain technology also faces other difficulties, such as the gradual increase of blockchain size, long validation time, and low transaction frequency. The future development is constrained by the current regulations, and the problem of high integration costs also needs to be considered.

In the near future, when the application of blockchain technology in the financial industry becomes increasingly popular, the organizational structure of financial regulation will face a round of profound adjustments. From the perspective of macroeconomic, once a new financial infrastructure and ancillary infrastructure have been constructed by using blockchain technology, the currency creation mechanism may be changed in the future. Traditionally, the connotation of money is the measure of value, the medium of exchange, and the storage of value. But a new proposition of the currency will be redefined by the blockchain since the real demand of commercial business is going to create credit rather than merely creating money. From the perspective of microeconomic, with the strong impact of technology finance and internet finance, the application of blockchain technology is expected to integrate finance and business organically, and it is bound to exceed the boundary of current financial industries [32].

In conclusion, the blockchain has not been established as a mature solution on the technology platform, the problems such as netting, extensible capacity, privacy protection and other technical issues remain to be resolved. And, the construction of large-scale blockchain financial infrastructure needs to rebuild IT architecture and re-engineer financial business process. Moreover, the acceptance of regulatory institutions to the technological innovation that brought about by blockchain is also very important. Lastly, the open-source code without geographical constraints is the advantage that enables the true global interconnection of the entire world network, thereby laying a solid technical foundation for the globalization of inclusive finance.

REFERENCES

[1] Fanning, K., & Centers, D. P. (2016). Blockchain and its coming impact on financial services. *Journal of Corporate Accounting & Finance*, *27*(5), 53-57.

[2] Holotiuk, F., Pisani, F., & Moormann, J. (2017). The impact of blockchain technology on business models in the payments industry.

[3] Lee, L. (2015). New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market. *Hastings Bus. LJ*, *12*, 81.

[4] Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications*.

[5] Swan, M. (2015). *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".

[6] Allen, Franklin, and Douglas Gale. "Innovations in financial services, relationships, and risk sharing." *Management Science* 45.9 (1999): 1239-1253.

[7] Turban, Efraim, et al. "E-Commerce Security and Fraud Issues and Protections." *Electronic Commerce*. Springer, Cham, 2015. 457-518.

[8] Akkermans, H., Bogerd, P., van Doremalen, J. 2004. Travail, transparency and trust: A case study of computer-supported collaborative supply chain planning in high-tech electronics. European Journal of Operational Research, 153: 445-456

[9] Sen, Ravi, and Sharad Borle. "Estimating the contextual risk of data breach: An empirical approach." *Journal of Management Information Systems* 32.2 (2015): 314-341.

[10] Tapscott, D., & Tapscott, A. (2017). How blockchain will change organizations. *MIT Sloan Management Review*, *58*(2), 10.

[11] Woodside, J. M., Augustine Jr, F. K., & Giberson, W. (2017). Blockchain Technology Adoption Status and Strategies. *Journal of International Technology and Information Management*, *26*(2), 65-93.

[12] Shrier, D., Wu, W., & Pentland, A. (2016). Blockchain & infrastructure (identity, data security). *MIT Connection Science*, 1-18.

[13] Collomb, A., & Sok, K. (2016). Blockchain/Distributed Ledger Technology (DLT): What Impact on the Financial Sector?. *Communications & Strategies*, (103), 93.

[14] Baliga, A. (2017). Understanding blockchain consensus models. Tech. rep., Persistent Systems Ltd, Tech. Rep.

[15] Kwon, Jae. "Tendermint: Consensus without mining." *Retrieved May* 18 (2014): 2017.

[16] Myerson, Roger B. "Refinements of the Nash equilibrium concept." *International journal of game theory* 7.2 (1978): 73-80.

[17] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*, 6-10.

[18] Yasin, A., & Liu, L. (2016, June). An online identity and smart contract management system. In *Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual* (Vol. 2, pp. 192-198). IEEE.

[19] Larios-Hernández, G. J. (2017). Blockchain entrepreneurship opportunity in the practices of the unbanked. *Business Horizons*, *60*(6), 865-874.

[20] Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. Financial Innovation, 2(1), 24.

[21] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[22] Karame, Ghassan O., Elli Androulaki, and Srdjan Capkun. "Double-spending fast payments in bitcoin." *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012.
[23] Chuen, David Lee Kuo, ed. *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data*. Academic Press, 2015.
[24] Holotiuk, F., Pisani, F., & Moormann, J. (2018, January). Unveiling the Key Challenges to Achieve the Breakthrough of Blockchain: Insights from the Payments Industry. In *Proceedings of the 51st Hawaii International Conference on System Sciences*.
[25] Plassaras, Nicholas A. "Regulating digital currencies: bringing Bitcoin within the reach of IMF." *Chi. J. Int'l L.* 14 (2013): 377.
[26] Pinna, A., & Ruttenberg, W. (2016). Distributed Ledger Technologies in Securities Post-Trading Revolution or Evolution?.
[27] Moser, Malte, Rainer Bohme, and Dominic Breuker. "An inquiry into money laundering tools in the Bitcoin ecosystem." *eCrime Researchers Summit (eCRS), 2013*. IEEE, 2013.
[28] Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and smart contracts for the internet of things." *IEEE Access* 4 (2016): 2292-2303.
[29] Urquhart, A. (2016). The inefficiency of Bitcoin. Economics Letters, 148, 80-82.
[30] Mainelli, Michael, and Alistair Milne. "The impact and potential of blockchain on securities transaction lifecycle." (2016).
[31] Micheler, Eva, and Luke von der Heyde. "Holding, clearing and settling securities through blockchain technology Creating an efficient system by empowering asset owners." (2016).
[32] Freixas, Xavier, and Jean-Charles Rochet. *Microeconomics of banking*. MIT press, 2008.
[33] Blockchain and Construction - Virginia Tech Blockchain nichb15https://blogs.lt.vt.edu/blockchain/2017/12/23/blockchain-and-construction/