Contemporary Social Sciences

2022 | Number 2 Article 2

2022

A Preliminary Study of Embedded Supervision Thoughts: Based on a Distributed Financial System

Wu Xiangyi
Sichuan Academy of Social Sciences

Du Kunlun
Sichuan Academy of Social Sciences

Tang Zhou
Sichuan Academy of Social Sciences

Li Xianbin
Sichuan Academy of Social Sciences

Recommended Citation

Xiangyi, Wu; Kunlun, Du; Zhou, Tang; and Xianbin, Li (2022) "A Preliminary Study of Embedded Supervision Thoughts: Based on a Distributed Financial System," *Contemporary Social Sciences*: No. 2, Article 2.
DOI: http://dx.doi.org/10.19873/j.cnki.2096-0212.2022.02.002
Available at: https://css.researchcommons.org/journal/vol2022/iss2/2

A Preliminary Study of Embedded Supervision Thoughts: Based on a Distributed Financial System

Wu Xiangyi, Du Kunlun, Tang Zhou, and Li Xianbin*

Sichuan Academy of Social Sciences

Abstract: Regulation of technology has been a hot issue in the financial field in recent years. Traditional financial regulation is constructed by a centralized account system, which relies on ex-ante regulation. Embedded supervision, which relies on regulation during and after the matter, operates in a decentralized and trusted environment and has the characteristics of high efficiency, transparency, and safety. It provides a breakthrough to solve the lag of traditional financial supervision. This paper clarifies the concepts and theoretical basis of embedded supervision, constructs the embedded supervision model with a lag, and analyzes the feasibility of embedded supervision with a lag. This research can promote scientific exploration and method innovations in the domestic finance field, enrich China's financial discipline system, and provide decision-making references for practical financial supervision innovation.

Keywords: blockchain, embedded supervision, distributed financial system

DOI: http://dx.doi.org/10.19873/j.cnki.2096-0212.2022.02.002

* Wu Xiangyi, Institute of Finance and Trade, Sichuan Academy of Social Sciences;
Tang Zhou, Institute of Finance and Trade, Sichuan Academy of Social Sciences;
Du Kunlun, Institute of Finance and Trade, Sichuan Academy of Social Sciences;
Li Xianbin, Institute of Finance and Trade, Sichuan Academy of Social Sciences.

Correspondence concerning this article should be addressed to Wu Xiangyi, Institute of Finance and Trade, Sichuan Academy of Social Sciences, Chengdu. Email: wxiangyi@outlook.com

Overview of Blockchain Technology

Since Satoshi Nakamoto proposed the concept of blockchain in his *Bitcoin: A Peer-to-Peer Electronic Cash System* in 2008, blockchain, encrypted assets, and smart contracts have become hot research areas in academic fields and practice fields, which have penetrated many industries. There are four main trends in the development of blockchain, including new infrastructure, government affairs, supply chain, finance, and other sectors.

How to combine and implement blockchain technology with multiple fields has become the main direction of academic and practical exploration. In the beginning, blockchain technology was mainly used in the currency field, as it can make trading affairs more secure and convenient. Then blockchain technology gradually entered the financial field after Ethereum (Ethereum is a platform powered by blockchain technology that is best known for its native cryptocurrency, called Ether or ETH, or simply Ethereum) became the first public blockchain embedded in a Turing-complete programming language, when the concept of smart contracts was proposed (Ouyang et al., 2019). After that, blockchain technology gradually entered the financial field and the application of blockchain is mainly focused on "Blockchain + Bank" (Ba, 2020; Zhang, 2019; Hu et al., 2017). As for the research framework and basic theory of blockchain supervision, it is in its infancy, and there are still many problems and ideas to be demonstrated and solved. Current blockchain policy is mainly based on encouragement, and partially based on implementation, 80 percent of which are guiding policies, while regulatory filings accounted for just 7.6 percent. So, there is an urgent need to supplement and improve the regulations related to blockchain.

The *Guiding Opinions of the State Council on Strengthening and Standardizing the Interim and Ex-post Regulation* states that,[①] "Giving full play to the roles of modern technologies in the interim and ex-post regulation, promoting regulatory innovations by depending on such new technologies as the Internet, big data, the Internet of Things, cloud computing, AI, and blockchain, and making efforts to achieve maximum regulatory effectiveness, optimized regulatory costs, and minimum interference to market players."

Blockchain technology has been further developed and applied in the field of financial regulation, such as smart contracts and smart regulatory reports. Blockchain is seen as an adjunct rather than an alternative to existing regulations. For instance, one of the Financial Conduct Authority (FCA)'s[②] planned future projects, Blockchain Technology for Algorithmic Regulation and Compliance (BARAC), aims to investigate the potential use of blockchain technology for automated regulation and compliance. IBM has partnered with CLS Group, a foreign exchange market infrastructure company, to create a platform called Ledger Connect. Deloitte used blockchain technology to help

[①] http://www.gov.cn/zhengce/content/2019-09/12/content_5429462.htm

[②] The Financial Conduct Authority (FCA), the UK's financial markets regulator.

Northern Ireland Bank integrate its business data onto the chain and establish a blockchain distributed financial report system. Blockchain technology establishes linkages among the bank's departments and realizes cross-bank supervision.

With the advent of blockchain, regulatory technology can fall into two categories, which refer to traditional regulatory technology and new regulatory technology. Traditional financial regulation mainly relies on pre-project approval and post-project regulation. But considering the institutional design and cost-effectiveness, the government is unable to do real-time supervision. So, with the financial products becoming increasingly complex and the transactions increasingly frequent, the existing problems and risks are gradually exposed and negative externalities to society are increasing (Feng, 2012). Embedded supervision is a kind of whole-process, full coverage supervision, before the event, at present, and after the event. Under embedded supervision, the regulatory process is no longer just running on the backend supervision system, but on the trading system. This means that every single transaction is monitored, at the time of trading.

The concept of embedded supervision is a comparatively novel concept; both domestic and foreign research on it mostly focus on its concept. An algorithm for embedded supervision is still being explored. How to use engineering thinking to learn the economic connotations and utility of embedded supervision is also an urgent problem and needs to be solved. In this paper, the model was optimized and deduced more accurately based on Raphael Auer (2019), and its technical feasibility was examined by combining the current situation with monitoring technologies. It also enriches the research content of embedded supervision.

Embedded Regulatory Literature Review

The embedding theory emerged in the middle and late 20th century and was then widely used in economics and sociology. The theory emphasized that "behavior and institutions are deeply conditioned by social relations." Therefore, it can be seen that even if the assumption of rational economic man is satisfied, rational economic behavior will be restricted by social relations. As a kind of social activity, economic behavior is embedded in various social relations and generates economic order. In a dialogue with Oliver E. Williamson (Nobel Prize Winner in Economics in 2009, majoring in New Institutional Economics), Mark Granovetter proposed "embedding," the core concept of new economic sociology (Granovetter, 2015) and Su Chunyan (2004) analyzed the embeddedness of the social construction of economic action. The application of embeddedness in the financial field can be divided into two levels: one is the application of embedded supervision in the field of centralized finance; the other is the application of embedded supervision in the field of distributed finance. Embedded supervision means automatically monitoring the issuance and trading of digital assets such as digital securities and cryptocurrencies for compliance with regulatory objectives by reading distributed ledgers, and reducing the need to proactively collect, verify and deliver data. Embedded supervision will further facilitate the compliant trading of digital assets and make decentralized financial engineering possible by self-executing smart contracts.

Research on Centralized Financial Embedded Supervision

Taking the legal supervision of private lending as an example, Feng Hui (2012) discussed the concept of innovation and system application of "embedded supervision" in financial supervision. He proposed that the supervision of private lending should be guided by the embedded supervision concept, with equal emphasis on blocking and dredging, strict reform, and strict law enforcement to comprehensively improve the performance of the financial regulatory system from the perspectives of illegal borrowing in accordance with laws and regulations, risk warning and information supply, interest rate liberalization, and promotion of cooperative finance. Tang Hongxia (2014) put forward the idea of implementing embedded supervision on the operation of private capital, and suggested adopting embedded supervision of both dredging and blocking, establishing, and improving private financing and lending service platforms and credit guarantee mechanisms, dredging private investment financing channels, and timely disclosure of relevant information. He Haifeng (2018) and others proposed that regulatory technology should be applied to the entire chain of financial supervision, and that cooperation between the regulatory end and the compliance end will become the main path of regulatory technology. Blockchain technology is becoming an important part of regulatory technology, and the process of institutionalization of regulatory technology is accelerating. Yang Dong (2018) defines RegTech as a means of "technology-driven supervision." "Technology-driven supervision" refers to the two-dimensional supervision system formed by adding a technological dimension to the traditional financial supervision dimensions such as prudential supervision and behavior supervision under the current situation of disintermediation and decentralization of financial transactions. Xia Shiyuan et al. (2020) developed a preliminary outlook on the application of blockchain technology as a typical technology of regulatory technology.

However, the reasons why it is difficult to implement embedded supervision for centralized financial institutions are as follows: First, the interests of regulators and regulated parties differ substantially, and there is a lack of consensus on the implementation of embedded supervision; Second, the accounting system construction logic of centralized financial institutions is enclosed, and it is difficult for the supervisory methods to be embedded into the whole process of the business operation system. Only off-site and non-real-time supervision and punishment with per-object indicator settings, and post-project reports can be achieved.

Research on Distributed Financial Embedded Supervision Innovation

As artificial intelligence, big data, blockchain, and other high and new technologies continue to expand their influence on the traditional financial industry, the integration of fintech and financial business has been promoted to a great extent. At the same time, a new challenge to traditional financial supervision is posted. The risks posed by fintech are disruptive and insidious; therefore, the efficiency of financial supervision may be reduced if the regulatory ideas and methods are not improved.

The Regulatory Sandbox, which originated in the UK, realized real-time, information-based, and panoramic supervision. In the supervision practice, the supervision effect should be investigated continuously and fully, and the supervision measures should be revised flexibly and improved according to the supervision effect (Wilkinson, 2007). In 2016, Aegean University proposed a plan to apply blockchain technology to financial markets, allowing simultaneous transactions and financial supervision. The Federal Reserve Bank of Boston (2019) proposed a design idea for the regulatory node architecture based on blockchain technology. The Federal Reserve and the Bank of England believe that distributed ledger technology can control financial risks not only by analyzing traditional financial statements but also by monitoring data through real-time supervision.

Raphael Auer (2019), chief economist of the Bank for International Settlements, built an innovative implementation of embedded supervision in blockchain finance. This article offers a regulatory framework for reading the distributed ledger information in the market and then analyzes the data to automatically monitor the compliance of the generalized market, thereby reducing the need and cost of passive collection, verification, and delivery of data by the regulated object. Ji Jia (2019) supposed that embedded supervision could simplify the audit procedures, reduce the fixed cost of establishing the regulatory system, and improve the efficiency of financial supervision. Ba Shusong et al. (2020) looked forward to blockchain-based financial supervision from the perspective of data-driven embedded supervision. Shusong's article focused on the potential risks brought by blockchain applications, analyzed how to use blockchain and other new technologies to strengthen financial supervision, and conducted theoretical explorations for improving blockchain supervision mechanisms. Douglas Arner et al. (2020) conducted research on the risks, potential, and regulation of stablecoins, and proposed that from a regulatory perspective, one possible option should be to embed regulatory requirements into the stable-coin system itself. Dirk A. Zetzcher et al. (2020) conducted an in-depth study of distributed finance in the context of traditional economics and finance and proposed that a brand-new regulatory design method, "embedded supervision" and "embedded regulation" be developed. The idea is to build the supervision method into the system of distributed finance and incorporate both finance and supervision into supervision technology. The financial regulation in the US mainly adopts functional regulation and classifies financial business with blockchain, big data, and other technologies. Li Xiaonan (2020) proposed that embedded regulation should be introduced based on the decentralized characteristics of blockchain technology itself. Li believes that access for regulators should be provided in blockchain financial infrastructure to allow them to supervise the safe operation of the system. Li put forward a feasible scheme: to set up a super-node in the blockchain as the regulatory node, which is able to meet micro and macro-prudential requirements and adapt to different regulatory requirements according to changing application scenarios. For instance, this node could be given the power to access and supervise financial transactions between different nodes in the blockchain. Wu Xiaoling (2021) also proposed a new construction method for the supervision of data and algorithms of platform financial technology (fintech) companies. Wu suggested that the behavior supervision of algorithms be strengthened and a compliance audit framework for algorithms and the regulatory requirements be constructed, as well as embedding social ethics and anti-monopoly reviews into the behavior monitoring algorithm. Cheng Xuejun et al. (2021) conducted research on the operation mechanisms of regulatory technologies and recommended comprehensive solutions for efficient supervision, relying on cutting-edge technologies such as blockchain and artificial intelligence. He found that the regulation technology ecology is constructed by supervisors, financial institutions, and regulation technology companies, and the application of transaction behavior monitoring, customer identification, financial stress testing, submission of compliance data, and tracking of laws and regulations is widespread. In order to balance the dual goals of promoting the development of fintech and preventing financial risks, the concept of financial supervision needs to be changed.

However, the current limitations of research on distributed financial embedded supervision innovation center on two points: one is that most studies only give a conceptual framework; the other is that some studies give financial cases, but they lack systematic theoretical construction.

Embedded Supervision Model Building

According to the paper of Raphael Auer (2019), which establishes a general model for distributed markets, the difference lies in that the utility of each party is clearer and the calculation formula is corrected. This paper also optimizes results and the related parameters of embedded supervision with a lag.

Assumption

In a market under embedded supervision, participants are free to trade during the duration, and all contracts are forced to clear when they expire. The transaction process is verified by the verifiers, and the transaction can be added to the chain only after being verified. At the same time, the transaction information will be transferred to the supervisors, who have the right to view the information in real time. Under real-time embedded supervision, the supervision system will be continuously monitored, while under embedded supervision with a lag, regulatory measures are taken only “once in a while,” which introduces the risk that losing parties among the market participants will have incentives to bribe the verifiers to reduce trading losses. The regulatory system must assess the risks of the transactions, and if it finds that there may be risks, in-depth risk research will be needed. If a significant risk is found, the transaction will undo the chain and the verifiers will be punished. According to the situations above, we put forward the following assumptions:

a. Before the deal, participants must have enough margin in the distributed ledger to meet the potential net payoff of the contract on the chain, thereby avoiding settlement risk.

b. Assume that the contracts are added to the blockchain at time $t=b_i=0$. And the service charge is only paid once, at the beginning of contract signing.

c. Participants know the set of verifiers for each block before they assign a transaction contract to the blockchain.

d. Rational economic assumption. The losing parties have an incentive to bribe the verifiers to revoke the block to cut a loss. If the verifiers receive a bribe greater than the sum of verification capital and commission income ($f + s$), the verifiers have an incentive to participate in a "blockchain history reversion" attack.

e. If two or more competitive blockchains emerge, market participants will only assign their blocks to the blockchain with the highest cumulative verification capital. This means that the chain is unique.

f. The verifiers verify the contracts of market participants to the chain only if the verification capital is high enough that the block will not be revoked.

g. Maximum contract loss within the extension is $\bar{C}_i=P_{i,0}\underline{c}$, part of the initial value of the contract.

The definition of these variables is shown in Table 1:

Table 1 Variable Definitions

Variable	Description	
b, t	Block number, time	Time is discrete, and is indexed by t; b is normalized, so that t and b can represent each other
b_i	The block into which contract i is assigned	The set of contracts is indexed by i. b_i is added to the chain at time $t = b_i$
L	The length of the contract	Each contract expires after a period of L
$N_{i,t}$	The number of contracts live at time t	The number of contracts assigned at the beginning is $N_{i,0}$, $N_{i,t}$ contracts i are still live at time t
v_i	Number of verifiers	During the duration of contract i, the number of verifiers remains the same
s	Verification capital	In each block, each verifier is required to deposit a verification capital worth s
δ	Risk-free rate	Verifiers can validate the blocks, or they can invest their capital elsewhere to earn a return of δ
f	The verifier's commission	In each block, each verifier will receive a commission income f at the end of the contract
$\underline{\pi}$	Transaction rate	$\pi = \underline{\pi} P_0$
π	Service charges	Participants pay a charge at the beginning of the period
$C_{i,t}$	Profit loss ratio	The total profit and loss ratio at time t: $C_{i,t} \in [-\underline{c}, \underline{c}]$
$P_{i,t}$	The price of contract i at time t	
$r_{i,t}$	Supervision profit and loss ratio	The total profit and loss ratio of supervision at time t: $r_{i,t} \in [-\underline{r}, \underline{r}]$
D	The number of days of delay in regulation	

Simplified Model Construction

Three parties are involved in this model. Respectively, the supervisor's utility refers to U_R, the utility of financial market participants refers to U_c, and the utility of market verifiers can be expressed as U_v. The objective function is expressed as follows:

$\max E\,(\,U_R + U_c + U_v\,)$

According to the specific situation of this paper, for supervisors, the revenue relates to the regulatory fees, which refers to $R_{i,t}$, usually negative. Then the utility of supervisors is represented as $U_R = -R_{i,t}$. While the contracts remain on the blockchain, contracts generate losses or gains. Martet participants are divided into the ones with losses or gains. The behaviors of the ones with a positive payoff can be predicted, as they are sure to be willing to sell off. But the losing side has incentives to bribe verifiers in order to minimize the loss, of which the greatest value is $C_{i,t}$. So, the utility of market participants can be represented as $U_c = -C_{i,t}$. The utility of verifiers is the sum of commissions and security deposits, which refers to $U_v = v_i L\,(v + f)$. The specific model is derived as follows:

In this model, time is discrete and indexed by t, and at each time period, a new block is added to the blockchain, labeled b. The number b is normalized so that b can be viewed as t. Assume that the current block number at time t_1 is b, block b_i was added to the chain at time $t_2 = b_i$, then $t_1 - t_2 = b - b_i$ corresponds to the time that has elapsed since block b_i was written into the blockchain.

In each block b, the set of newly generated contracts is represented as i, then the number of contracts on the block b_i at the beginning is $N_{i,0}$. Each contract has a buyer and a seller, and the participants of each contract pay a service charge and a settlement fee totaling π for the right to assign and clear a financial contract on the block.

When a financial contract i is assigned to block b_i, it generates a series of net gains or losses as the price of the asset fluctuates. These financial contracts can be considered as any type of financial transaction in which the future net gain or loss is uncertain. Contracts are zero-sum, where the changes in the losing side and the gains side are negative of each other, and the absolute values are equal.

Participants can freely enter and exit the market. And if they decide to exit the market, they can cash out of the market, that is, settle the contract with off-book funds: the negative balance party transfers the off-chain funds to the positive balance party, and then both parties dissolve the contract on the blockchain. All contracts in set will not be clear until $t - b_i = L$.

The verifier acts as a third party, assigning the block containing the new contract into the blockchain. The system randomly assigns enough verifiers to validate the contracts on the block, to perform customer identification, anti-money laundering, and other legal background checks. On each block, if the verifiers use their verification capital for block verification, they will earn verification income f at the end of the contract. But if the verifiers do not verify the block or invest the capital elsewhere instead, such as capital markets or money markets, they will get a return of δ at the expiration of the contract, which is the opportunity cost of the verifiers participating in the verification of the block. Once the verifier uses his verification capital to validate a block, his verification capital will be locked throughout the duration of the contract for the period of L time. It cannot be withdrawn until the contract expires. If the verifier validates a block that is reversed at some time in the future, the verifier will suffer a loss.

On each block, we assume that the net loss parties to the contract can form an alliance. If the net loss party, or parties, wants to undo the gains and losses on the current block, which is to say that they want to co-fund the abolition of blocks on the blockchain, a certain amount of money is required to bribe the verifier. The verifiers will only suffer a financial loss, called verification capital s, when the blocks are found to be reversed afterwards.

To simplify the derivation, we assume that the number of contracts to be cleared each day over the life of the contract varies proportionally in the simplified model and in each block, there is a share $(1 - \beta)$ of contracts that are netted. Netting means to net on-chain positions via off-chain payments and then void the contract on the chain. Then we know that: $N_{i,t} - N_{i,t-1} = -(1-\beta)N_{i,t-1}$.

First of all, we define the cumulative rate of return of contract i at time point t ($t > b_i$) as $C_{i,t}$. There will be losses and gains while the contract is still on the blockchain, like stock accounts. The net present value of the profits and losses is distributed over time:

$$\begin{cases} c_{i,t}b_i \in \left[-\underline{c}, \underline{c}\right], 0 < t < L \\ c_{i,t}b_i = 0, t \geq L \end{cases}$$

In the general model, the number of reductions in valid contracts is in a geometric sequence. Then the number of live contracts at the end of each period can be expressed as:

$$N_{i,t} = \begin{cases} \beta^t N_{i,m}, 0 \leq t \leq L \\ 0, t \geq L \end{cases}$$

The number of new contracts cleared per day is:

$$-\Delta N_{i,t} = (1-\beta) N_{i,t-1}, 0 < t \leq L$$

For the verifier's account, during the term of this contract $1 \leqslant t \leqslant L$, the validator needs to validate the contracts on each block at each time period. Set $N_{i,0} = N_m$, then we have:

$$v_i\left[s(1+\delta)^{L-1} + s(1+\delta)^{L-2} + \mathrm{L} \ + s\right] = Lv_i(f+s)$$

$$N_m\pi(1+\delta)^L = Lv_i f$$

Obtained from the above equation, we can get:

$$f = s \cdot \left[\frac{(1+\delta)^L - 1}{L \cdot \delta} - 1\right]$$

Substitute the above equations into the formula for calculating the procedure rate $\underline{\pi} = \frac{\pi}{P_{i,0}}$, then we have:

$$\underline{\pi} = \frac{Lv_i f}{N_m P_{i,0}}$$

An expansion of the service charge rate can be obtained in the general model:

$$\underline{\pi} = \frac{v_i s}{N_m P_{i,0}} \left[\frac{(1+\delta)^L - 1}{L \cdot \delta} - L \right]$$

The sufficient and necessary condition for the economic finality is: at the end of time point *t*, no strategy to undo the last 0~X ($X < L$) blocks can ever be profitable, even under the most adverse realization of payoffs.

We use $C_{i,t}$ to denote the maximum gain $C_{i,t}$ of abolishing block $b_{i,t}$ in the chain at time *t*.

$$C_{i,t} = \beta N_{i,t} P_{i,0} \underline{c}, 0 < t < L$$

In the situation without supervision, the total utility function is E ($U_c + U_v$). We can define it as economic finality, which can be expressed as:

$$E\left\{ \max_{X<L} \left\{ \sum_{k=0}^{X} \left[C_{i,t} - v_i (s+f) \right] \right\} \right\} \leq 0$$

To satisfy the following conditions:

$$\overline{C_i} = \max_{0<t<L} \left(C_{i,t} \right) = \max_{0<t<L} \left(N_{i,t} P_{i,t-1} \underline{c} \right)$$

The expanded form of $\bar{C}_i$ can be obtained in the general model:

$$\overline{C_i} = N_m P_{i,0} \underline{c}$$

Assertion 1: The necessary and sufficient conditions of the economic finality of the general model can be simplified as:

$$\overline{C_i} \leq v_i L(s+f), 0 < t < L$$

So that:

$$\beta N_m P_{i,0} \underline{c} \leq v_i L(s+f)$$

Proof:

For contracts generated at time point $b_{i,0} = t = 0$, as long as $0 < t < L$:

We know one of the necessary and not sufficient conditions for an economic finality is: it is unprofitable to abolish the current block $b_{i,t}$ of the chain at time *t*, that is:

$$N_{i,t}P_{i,0}\underline{c}-v_iL\left(s+f\right)\le 0,0<t<L$$

Then one of the necessary (but alone not sufficient) conditions needed for economic finality can be obtained: at time t, for $X < t$, it is uneconomical to abolish blocks $b_{i,t\text{-}X}$ to $b_{i,t}$ in the chain, because: when $0 < t < L$:

$$\begin{aligned}&N_{i,t}P_{i,0}\underline{c}-v_iL\left(s+f\right)\\&\quad\le \beta N_{i,m}P_{i,0}\underline{c}-v_iL\left(s+f\right)\\&\quad=\overline{C}_i-v_iL\left(s+f\right)<0\end{aligned}$$

$$\begin{aligned}&\left[N_{i,t}P_{i,0}\underline{c}-v_iL\left(s+f\right)\right]+\left[N_{i,t\text{-}1}P_{i,0}\underline{c}-v_iL\left(s+f\right)\right]\\&\quad\le\left[\beta N_{i,t}P_{i,0}\underline{c}-v_iL\left(s+f\right)\right]+\left[\beta N_{i,t-1}P_{i,0}\underline{c}-v_iL\left(s+f\right)\right]\\&\quad\le 2\left[\overline{C}_i-v_iL\left(s+f\right)\right]<0\end{aligned}$$

Then we can get additional necessary (but alone not sufficient) conditions needed for economic finality, that at any time during the duration of the contract, it is an unwise choice to undo the last X consecutive blocks.

$$\begin{aligned}&\sum_{k=0}^{X}\left[C_{i,t}-v_iL\left(s+f\right)\right]\\&\quad\le\sum_{k=0}^{X}\left[\overline{C}_i-v_iL\left(s+f\right)\right]\\&\quad=X\left[\overline{C}_i-v_iL\left(s+f\right)\right]\le 0\end{aligned}$$

And this is a sufficient condition, for undoing the last X consecutive blocks can be avoided at each time period/block. To sum up, the above equation is not only sufficient but also necessary, which means financial finality:

$$\sum_{k=0}^{X}\left[\overline{C}_i-v_iL\left(s+f\right)\right]\le 0$$

So that:

$$\overline{C}_i-v_iL\left(s+f\right)\le 0\,,0<t<L$$

More specifically, for the situation in which the number of reductions in valid contracts is in a geometric sequence, the necessary and sufficient condition for financial finality is:

$$\beta N_mP_{i,0}\underline{c}-v_iL\left(s+f\right)\le 0\,,0<t<L$$

$$\beta N_mP_{i,0}\underline{c}\le v_iL\left(s+f\right),0<t<L$$

Therefore, the number of verifiers can be obtained:

$$v_i = \frac{\overline{C}_i}{L\left(s+f\right)}$$

Substitute it into the general model:

$$v_{i1} = \frac{N_m\delta}{s\left[\left(1+\delta\right)^L - 1\right]} \times \beta \times P_{i,0}\underline{c}$$

According to the calculation formula of the fee rate, the fee rate is $\underline{\pi}_1$:

$$\underline{\pi}_1 = \frac{Lv_i f}{N_m P_{i,0}} = \delta\left[1 - \frac{L\delta}{\left(1+\delta\right)^L - 1}\right] \times \beta \times \underline{c}$$

Lemma 1: Fee rate for market participants $\underline{\pi}$ is independent of verification capital s, as well as the initial number of contracts.

Lemma 2: Fee rate for market participants $\underline{\pi}$ is in positive correlation with the maximum loss rate $\underline{c}$ and the contract length L, and is in negative correlation with the rate at which the contracts decrease (1 - β).

Proof of Lemma 2:

Obviously, the fee rate $\underline{\pi}$ is in positive correlation with the maximum loss rate $\underline{c}$, and is in negative correlation with the rate at which the contracts decrease (1 - β).

$$\frac{\partial \underline{\pi}}{\partial \underline{c}} = \delta\left[1 - \frac{L\delta}{\left(1+\delta\right)^L - 1}\right] \times \beta > 0$$

$$\frac{\partial \underline{\pi}}{\partial \beta} = \delta\left[1 - \frac{L\delta}{\left(1+\delta\right)^L - 1}\right] \times \underline{c} > 0$$

Then we prove that the fee rate $\underline{\pi}$ is in positive correlation with the contract length L.

We set $f\left(L\right) = \frac{L}{\left(1+\delta\right)^L - 1}$

Then we know that the monotonicity of $f(L)$ is different from that of $\underline{\pi}(L)$.

$$\frac{\partial f}{\partial L} = \frac{\left(1+\delta\right)^L - 1 - L\cdot\left(1+\delta\right)^L \cdot \ln\left(1+\delta\right)}{\left(1+\delta\right)^L - 1}$$

We set $g\left(L\right) = \left(1+\delta\right)^L - 1 - L\cdot\left(1+\delta\right)^L\cdot\ln\left(1+\delta\right)$

$$\frac{\partial g\left(L\right)}{\partial L} = -L\left(1+\delta\right)^L\left[\ln\left(1+\delta\right)\right]^2 < 0$$

So we can get: $g(L) < g(0) = 0$,

So $f(L)$ is monotonically decreasing in our domain, then we have $\underline{\pi}(L)$ increases monotonically with respect to L, the length of contract duration.

Next, to better analyze the embedded supervision model, let us introduce the concept of redundant validation capital RVC. As $v_i(s+f) \geq \overline{C}_i \geq C_{i,1<t<L}$, excess verification capital starts to accumulate over time. Expanded to the general case, the residual verification capital accumulated in contract from time $t=1$ to $t=X<L$ is:

$$RVC_{1,X(X>0)} = \sum_{k=1}^{X}\left[v_i L(s+f) - C_{i,t}\right]$$

Real-Time Embedded Supervision Model

If market participants know that regulators are going to use information from the blockchain, they may have an incentive to report false information in order to deceive regulators.

In order to consider the influence of regulators on the market in the model, extra gains and losses of each contract $r_{i,t} < b_i$ are assumed to occur before the expiry date.

$$\begin{cases} r_{i,t} \in \left[-\underline{r}, \underline{r}\right], 0 < t < L \\ r_{i,t} = 0, t \geq L \end{cases}$$

$$R_{i,t} = N_{i,t} P_{i,t-1} \underline{r}, 0 < t < L$$

$$\overline{R}_i = \max_{0<t<L}\left(R_{i,t}\right) = N_m P_{i,0} \underline{r}$$

Furthermore, when considering the case of real-time supervision, the total utility of regulators, market participants and verifiers is $E(U_R + U_c + U_v)$. So, the necessary and sufficient conditions of the economic finality is:

$$E\left\{\max_{X<L}\left\{\sum_{k=0}^{X}\left[C_{i,t} + R_{i,t} - v_i L(s+f)\right]\right\}\right\}$$

Which can be simplified as:

$$\overline{C}_i + \overline{R}_i \leq v_i L(s+f),\ 0 < t < L$$

That is:

$$N_m P_{i,0}\left(\underline{c} + \underline{r}\right) \leq v_i L(s+f)$$

Then the number of verifiers in the real-time supervisory model is:

$$v_{i2} = \frac{\overline{C}_i + \overline{R}_i}{L(s+f)}$$

Substitute the above equation into the real-time supervisory model and we get:

$$\begin{aligned} v_{i2} &= \frac{\overline{C}_i + \overline{R}_i}{L\left(s+f\right)} \\ &= \frac{N_m\delta}{s\left[\left(1+\delta\right)^L - 1\right]} \times \beta \times P_{i,0} \times \left(\underline{c} + \underline{r}\right) \end{aligned}$$

According to the equation, the fee rate is:

$$\begin{aligned} \underline{\pi}_2 &= \frac{Lv_i f}{N_m P_{i,0}} \\ &= \delta\left[1 - \frac{L\delta}{\left(1+\delta\right)^L - 1}\right] \times \beta \times \left(\underline{c} + \underline{r}\right) \end{aligned}$$

When the number of verifiers and the fee rate meet the above equation, regulators can read the books in real time to achieve automatic market regulation, but this situation means that higher verification capital is required than the simplified model.

Embedded Supervision with a Lag

Because real-time regulation is more expensive, we introduced delayed compliance regulation. Suppose the regulator allows the use of compliance regulation every *D* time period. Then the redundancy verification capital in the lagging *D* period satisfies the following equation:

$$RVC_{2,D(D>0)} \geq R_{i,D}$$

Under the embedded supervision with a lag, supervisors' costs will be less than those under real-time supervision. This cost can be specified as $R_{i,D}$, and then the total utility of the supervision model with a lag is $E\ (\ U_{RD} + U_c + U_v\ )$. Then the sufficient and necessary condition of embedded supervision with a lag is:

$$E\left\{\max_{X<L}\left\{\sum_{k=0}^{X}\left[v_i(s+f) - C_{i,k}\right]\right\}\right\} \leq R_{i,D}$$

Finally, the number of verifiers and the fee rate required can be expressed as follows:

$$\sum_{k=1}^{D}[\ v_i L\ (s+f)\text{-}C_{i,k}\ ]=R_{i,d}$$

$$\begin{aligned} v_{i3} &= \frac{1}{L\left(s+f\right)} \times \frac{1}{D} \times \left[\sum_{k=1}^{D} C_{i,k} + R_{i,D}\right] \\ &= \frac{\beta N_m \delta}{s\left[\left(1+\delta\right)^L - 1\right]} \times \frac{1}{D} \times P_{i,0} \times \left(\frac{1-\beta^D}{1-\beta} \times \underline{c} + \beta^{D-1}\underline{r}\right) \end{aligned}$$

$$\begin{aligned} \underline{\pi}_3 &= \frac{\pi_3}{P_{i,0}} = \frac{Lv_i f}{N_m P_{i,0}} \\ &= \delta\left[1 - \frac{L\delta}{\left(1+\delta\right)^L - 1}\right] \times \beta \times \frac{1}{D} \times \left(\frac{1-\beta^D}{1-\beta} \times \underline{c} + \beta^{D-1}\underline{r}\right) \end{aligned}$$

More strictly:

$$\sum_{k=1}^{D}[\ v_i L\ (s+f)\text{-}\overline{C}_i\ ]=\overline{R}_i$$

Therefore, the necessary and sufficient condition for the embedded supervisory model with a lag can be simplified as:

$$v_{\mathrm{i}} L(s+f)-\overline{C}_{i,k}<\frac{\overline{R}_i}{D}$$

The number of verifiers for the embedded supervisory model with a lag is:

$$v_{i3}=\frac{\overline{C}_i+\frac{\overline{R}_i}{D}}{L(s+f)}$$

The fee rate of the embedded supervisory model with a lag refers to equation:

$$\underline{\pi}_3=\frac{\pi_3}{P_{i,0}}=\frac{L v_{i3} f}{N_m P_{i,0}}$$

The expansion is:

$$v_{i3}=\frac{N_m\delta}{s\left[(1+\delta)^L-1\right]}\times\beta\times P_{i,0}\times\left(\underline{c}+\frac{\underline{r}}{D}\right)$$

$$\underline{\pi}_3=\delta\left[1-\frac{L\delta}{(1+\delta)^L-1}\right]\times\beta\times\left(\underline{c}+\frac{\underline{r}}{D}\right)$$

In conclusion, for $0<D<L$, we have:

$$v_{i2}=v_{i1}\cdot\left[1+\frac{\underline{r}}{\underline{c}}\right]$$

$$v_{i3}=v_{i1}\cdot\left[1+\frac{\underline{r}}{D\underline{c}}\right]$$

$$\underline{\pi}_2=\underline{\pi}_1\cdot\left[1+\frac{\underline{r}}{\underline{c}}\right]$$

$$\underline{\pi}_3=\underline{\pi}_1\cdot\left[1+\frac{\underline{r}}{D\underline{c}}\right]$$

In all existing regulations, there is a great time lag in the delivery of data from the regulated to the regulators. But in this model, the verifiers have immediate access to certain data, and only take regulatory action after a certain period of time.

Conclusion

The sufficient and necessary condition for the economic finality is: at the end of time point *t*, no strategy to undo the last 0~X ($X < L$) blocks can ever be profitable, even under the most adverse realization of payoffs. And it can be expressed as an inequality:

$$\begin{cases} E\left\{\max\limits_{X<L}\left\{\sum\limits_{k=0}^{X}\left[C_{i,t}-v_i\left(s+f\right)\right]\right\}\right\}\leq 0, & \text{Non-Regulation} \\ E\left\{\max\limits_{X<L}\left\{\sum\limits_{k=0}^{X}\left[C_{i,t}+R_{i,t}-v_i\left(s+f\right)\right]\right\}\right\}\leq 0, & \text{Real-time Regulation} \\ E\left\{\max\limits_{X<L}\left\{\sum\limits_{k=0}^{X}\left[v_i\left(s+f\right)-C_{i,t}\right]\right\}\right\}\leq R_{i,t}, & \text{Regulation with a lag} \end{cases}$$

According to the equations above, the number of verifiers and transaction fee rates of participants is:

$$v_i = \begin{cases} \dfrac{\overline{C}_i}{L\left(s+f\right)}, & \text{Non-Regulation} \\ \dfrac{\overline{C}_i+\overline{C}_i}{L\left(s+f\right)}, & \text{Real-time Regulation} \\ \dfrac{\overline{C}_i+\dfrac{\overline{R}_i}{D}}{L\left(s+f\right)}, & \text{Regulation with a lag} \end{cases}$$

$$\underline{\pi} = \frac{Lv_i f}{N_m P_{i,0}}$$

The embedded supervisory model with a lag works better than the real-time embedded supervisory model, and it satisfies the relationships of the analysis in the previous section

$$v_{i2} = v_{i1}\cdot\left[1+\frac{r}{\underline{c}}\right];\quad v_{i3} = v_{i1}\cdot\left[1+\frac{r}{D\underline{c}}\right];$$

$$\underline{\pi}_2 = \underline{\pi}_1\cdot\left[1+\frac{r}{\underline{c}}\right];\quad \underline{\pi}_3 = \underline{\pi}_1\cdot\left[1+\frac{r}{D\underline{c}}\right].$$

It will cost more to take regulatory measures than not, but it takes less to take regulatory measures with a lag as the number of verifiers and the transaction fees required by embedded supervision decrease.

By observing the calculation results, we can see that the smart contract based on the distributed ledger is Villefredo Pareto improved compared with the traditional contract, and the cost of delayed supervision is lower than that of real-time supervision. In addition, with the development and application of distributed ledgers in the blockchain industry, as well as the low fixed cost of compliance of distributed ledgers, the decentralized financial system has the foundation to take root and acquire effective support from the legal system and registered rating agencies and other supporting institutions. In the current traditional financial market, centralized finance is still the mainstream. Despite great technological progress, the price of financial services is still high due to information asymmetry even though the distributed ledger market can effectively reduce the costs of compliance with financial regulation and reduce the entry threshold. At the same time, regulators can write their own regulatory ideas, methods, and standards into the contract, to achieve embedded supervision, reduce regulatory costs and ensure a level playing field for participants.

For market participants, traditional financial markets generate commissions and fees when buying and selling contracts. However, in the distributed market with embedded regulation, the fee rate is low, which encourages participants to enter this emerging market. For the verifiers, the profit and loss of the participant must be verified by the verifier. If the block is proved invalid, the existing transaction will be regarded as invalid, and the verifier will lose a given amount of verification capital, which controls the illegal operation of the verifier and establishes the relevant criterion. For regulators, they can carry out embedded supervision through distributed ledgers at any time and take delayed regulatory measures to ensure the normal operation of the market while improving efficiency without reducing profits.

Until now, newly issued tokens known as block rewards in blockchain have accounted for the majority of mining revenues. As new block rewards are phased out, crypto transaction liquidity will decline significantly, which may require social coordination or institutionalized support. Regulators also need to develop complementary frameworks for managing distributed markets and their infrastructure, such as burden-sharing for decentralized market crime, to deliver higher quality and more efficient compliance at a lower cost.

Future Expectations for Embedded Supervision

The application of embedded supervision requires not only strict demonstration of rationality and feasibility through mathematical models but also top-level design from the systematic aspect to ensure the completeness of its internal logic. Here we give a vision of an embedded future system.

Regulatory technology based on distributed ledger blockchain will be the mainstream in the future, and it will no longer just be based on big data platforms. In 2020, Travel Rule Information Sharing Architecture (TRISA) put forward the concept of a supervision network, a network of interconnected regulatory systems, where trading and regulation go on at the same time. Facebook's Libra system also has embedded supervision, and the Bank for International Settlements, the Bank of England and several foreign research institutions are proposing the same concept. For these and similar systems, the embedded supervision algorithms would be confidential. Under embedded supervision with a lag, the information is verified by the verifiers, and the transaction information will be delivered to the transaction monitoring system at the same time. This supervision system has access to information all the time but only takes regulatory measures every once in a while. The regulatory system will check some information to assess the risks of the deal, such as trading volume, exchange risk, trading speed, and personal information. The deal will trigger in-depth risk research if it is found to be risky. And if there is a significant risk, the transaction will be interrupted, and the examiner will be punished.

Embedded supervision based on blockchain requires multi-party simultaneous online collaborative interactive regulation. Embedded supervision promotes sector-specific supervision and institutional supervision of traditional financial supervision in the form of technology and underlying logic. It is based on on- and off-site inspection and swift multi-party online and collaborative supervision. Compliance blockchain led by regulatory authorities gathers the central bank, banking, and insurance regulatory systems as well as the systems for securities, public security, industry and commerce, and other governmental regulatory departments onto the blockchain. At the same time, embedded supervision can open interface access to all types of licensed and unlicensed financial institutions, including consumer groups, urging financial institutions to share data and transaction operations. Regulators' regulatory policies and compliance guidelines, as well as financial institutions' daily data, will be packaged and integrated into the chain, forming individual nodes. Thus a multi-party online, point-to-point interconnection interactive structure will be formed.

As a brandnew supervision method, embedded supervision should be put into official use after sandbox experiments are carried out as the operation mode and errors need to be observed during the sandbox experiments. The continuous debugging and evolution of a supervision system will improve the incompatibilities between the embedded supervision and the distributed financial systems so that it can carry out real-time supervision in distributed financial application scenarios. Globally, many countries are open to regulating technology, and some are already developing regulatory sandboxes. For instance, the Lithuanian bank is carrying out a blockchain sandbox that aims to embed regulatory infrastructure in a market based on distributed ledgers. The Federal Reserve Bank of Boston is studying the possibility of establishing a regulatory node and plans to create mock transactions to try to keep depository balances under the Federal Reserve Bank of Boston's blockchain supervision. Drawing on the practices of regulatory sandboxes in the UK, Singapore, Australia, and the US, compliance blockchain is an indispensable part of the regulatory sandbox, and it is also the trend of the optimization of the regulatory sandbox system of the future. Regulators, financial institutions, and fintech start-ups can conduct flat peer-to-peer and interoperable communication in the real test scenario of the regulatory sandbox.

Cross-border cooperation needs to be promoted. In today's globalization networks and information transfers, financial elements and technological elements are moving more frequently around the world. Financial institutions and fintech companies carry out business across countries. All these exacerbate the transmission and cross-diffusion of financial risks and the regulatory technology is attracting more attention around the world. Several countries such as the UK, Australia, Singapore and the

US have already started the research and deployment of regulatory technology and compliance blockchain. China is a late starter in regulatory technology, but it is growing fast. In addition, for enterprises themselves, the compliance risk of global operations is increasing, and penalties caused by compliance problems are also increasing. So, it is an important part of regulatory science and technology cooperation to strengthen international cooperation on compliance blockchain. It can effectively improve the prevention and governance of cross-border risks to strengthen international cooperation on compliance blockchain, and have an inhibitory effect on anti-money laundering (AML), anti-terrorist financing, and other dark web transactions. Compliance blockchain cooperation among international stock exchanges is also conducive to strengthening the ability of front-line supervision. The establishment of compliance blockchain among various countries is conducive to coordination, interaction, information sharing, and the development of regulatory technology.

As for new technological innovations, cloud computing can provide an effective solution for the storage of blockchain nodes. Node data is stored and backed up in the cloud. Data on a single node does not need to be stored on local hardware devices, which helps save space. The development of 5G will be able to expand blockchain bandwidth and increase the speed at which transactions can be processed and transmitted. For the privacy protection of data, a variety of encryption technologies and blockchain privacy protection safety valve mechanisms will enhance the privacy protection capability of compliance blockchain.

A consensus mechanism should be established among regulators, participating agencies, and verification agencies. In the original blockchain system, consensus mechanisms such as PoW and PoS allow verifiers in the block to reach a consensus on the distributed database, thereby ensuring the uniqueness and completeness of the database. When third-party regulators are introduced, it is one of the core elements of embedded regulatory applications that the basic elements of the regulatory concept, principles, and standards are written into the blockchain network. Low cost is needed for distributed financial services under the introduction of embedded supervision. If not, it will be difficult to attract more participants and verifiers to participate in the maintenance of the blockchain system. When designing embedded supervision, the derivation of mathematical models should be used to strictly prove that under supervision, participants will have lower as well as maintain. Also, it is supposed that under embedded supervision, distributed financial services can maintain their economic effectiveness. In the top-level design of embedded supervision, we need to accurately quantify the participants' service charge, the verifier's verification capital, and the regulator's cost and other parameters. The effectiveness of distributed financial operations is ensured from the aspects of system design and parameter optimization.

REFERENCES

Ba, S. S., Wei, W., & Bai, H. F. (2020). Financial regulation based on blockchain: From data-driven to embedded regulation. *Journal of Shandong University (Philosophy and Social Sciences Edition)*. 4, 161—173.

Cheng, X. J, Yin, Z. T., & Li, X. H. (2021). Fintech innovation and regulatory path search: Based on regulatory technology research perspective. *E-Government*. 1, 43—56.

Dirk, A. Z., Douglas, W. A., & Ross, P. B. (2020). Decentralized finance. *Journal of Financial Regulation*, 2, 172—203.

Douglas, A., Raphael, A., & Jon. F. (2020). Stablecoins: Risks, potential, and regulation. *Basel: BIS working paper.* 905.

Federal Reserve Bank of Boston. (2019). Beyond theory: Getting practical with blockchain: The Federal Reserve Bank of Boston learns by doing with blockchain technology. *Boston: Federal Reserve Bank of Boston*.

Feng, H. (2012). On "embedded regulation": Concept innovation and system application of financial regulation: Taking legal regulation of private lending as an example. *Politics & Law*, 8, 30—38.

He, H. F., Yin, D. N., & Liu, Y. X. (2018). Research on Sptech: Conception, application and development trend. *Journal of Financial Regulation*, 10, 65—79.

Hu, Z. J., & Chang, Y. (2017). Application and prospect of blockchain in commercial banks. *New Finance*. 10, 44—48.

Ji, J. (2019). Make good use of blockchain technology to reduce the cost of financial regulation. *China Securities News*. p. 3.

Li, X. N. (2020). Regulatory response to financial infrastructure based on blockchain. *Financial Regulation Research*. 10, 85—97.

Mark, G. (2015). *Social network and economic action*. Luo, J. D., et al (trans.). Beijing: Social Sciences Academic Press.

Melanie, S. (2015). Blockchain: Blueprint for a new economy. *O'Reilly Media*.

Ouyang, L. W., Wang, S., & Yuan, Y., et al. (2019). Smart contract: Architecture and progress. *Acta Automatica Sinica*, 45(03), 445—457.

Raphael, A. (2019). Embedded supervision: how to build regulation into blockchain finance. *Basel: BIS working paper.* 811.

Shang, H. X. (2014). Embedded regulation of private capital operation. *Special Zone Economy*, 5, 55—57.

Su, C. Y. (2004). The social construction of economic action: An analysis of the embeddment of economic action in new economic sociology. *Journal of Shanghai University (Social Science Edition)*, 11(6), 22—25.

Wilkinson, M. (2007), Between constitutionalism and democratic experimentalism: New governance in the EU and the US. *Modern Law Review*, 70, 680—700.

Wu, X. L. (2021). Research on regulation of platform fintech companies. *TSINGHUA Financial Review*. 7, 14—15.

Xia, S. Y., & Tang, L. (2020). Research on theoretical framework and perfection path of regulatory technology. *Southwest Finance*, 11, 86—96.

Yang, D. (2018). Regulatory technology: The regulatory challenges and dimensions of financial technology. *Social Sciences in China*, 5, 69—91+205—206.

Zhang, T. (2019). Applications and prospects of blockchain technology in Commercial Banks of China. *New Finance*. 7, 50—57.

(Editor: Xu Huilan)