Columbia University Press
Columbia Business School Publishing

Chapter Title: Risks of Fintech and Regulatory Technology

Book Title: China's Fintech Explosion
Book Subtitle: Disruption, Innovation, and Survival
Book Author(s): Sara Hsu and Jianjun Li
Published by: Columbia University Press, Columbia Business School Publishing. (2020)
Stable URL: https://www.jstor.org/stable/10.7312/hsu-19656.12

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at https://about.jstor.org/terms

Columbia University Press, Columbia Business School Publishing are collaborating with JSTOR to digitize, preserve and extend access to *China's Fintech Explosion*

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

CHAPTER EIGHT

Risks of Fintech and Regulatory Technology

Overview

Many risks are associated with fintech, particularly risks related to fraud and security. Regulators must pay attention to these risks as well as to business compliance. Although use of technology increases the spectrum of risks it also can help to reduce and control risks.

Just as fintech firms have had to cope with risks, the fintech industry has presented a serious challenge to Chinese regulators. Most of the existing regulations pertain to the traditional financial industry rather than to fintech per se. Many of the characteristics of these new fintech firms are unprecedented and thus are not covered by current rules.[1] Before 2015, regulators allowed the fintech industry to develop without substantial regulation; however, because of the growing size of the industry, this is no longer possible. Therefore, additional regulations have been made, as laid out in the previous chapters.

Compliance with regulations can be costly, but regulatory technology (regtech) reduces these costs and ensures that complex regulations are fully implemented and also can be applied in real time to financial

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

market changes. Using the definition of the UK Financial Conduct Authority (FCA), regtech refers to the adoption of new technology to serve financial regulation and business compliance, and regtech is an important part of fintech. The technology can boost consumer protection and enhance business insight.

Currently, the global regtech industry is only in its beginning stages. An increasing number of firms, however, are aimed at improving the process of regulatory reporting, risk management, compliance, transaction monitoring, due diligence tools, and financial crime control.

Risks of Fintech

Fintech has raised several challenges to regulation, including mixed industry operation risks, compliance risks, associated risks, volatility and procyclicality risks, and technology risks. We discuss these challenges in the following sections.

Mixed Industry Operation Risks

Financial technology has broken through the boundaries of traditional financial industries. Cross-industry, cross-institutional, and cross-sector financial products have emerged in an endless stream, breaking the time and space restrictions of risks and increasing the possibility of the rapid spread of financial risks and cross-border contagion. In addition, innovative products often run through multiple levels of financial markets, blurring the underlying assets and ultimate investors, increasing the concealment of risks, and making it difficult to identify and measure risk. These risks place higher demands on the technical level of financial supervision.

Compliance Risks

Fintech has reconstructed many of its financial trading habits and methods. The emerging financial formats and new financial trading behaviors are difficult to effectively regulate within the existing legal framework, and compliance risks are prevalent. For example, the current legal rules cannot clearly define the legal nature of smart contracts in which blockchain is applied. Whether the existing legal

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

norms, such as the Contract Law, are applicable to smart contracts remains unclear, and the disputes that arise are difficult to accurately characterize and regulate.

Associated Risks

The development of financial technology links financial institutions at home and abroad. This had led to a sharp increase in the incidence and spread of financial risks.

Volatility and Procyclicality Risks

Although financial technology is improving the efficiency of financial services, the risk transmission speed is becoming faster and faster. As the behavior of participants in the financial market converges, financial market volatility is amplified. Financial institutions now use intelligent systems to provide customers with programmatic asset management recommendations. In the case of these smart investment consultants, when similar risk indicators and trading strategies are adopted across investors, they may lead to overall riskier behavior in purchases and sales in the market, since this phenomenon will aggravate market volatility.

Technology Risks

At present, financial business increasingly relies on technological innovation, and technology risks inevitably will spread to the financial sector and evolve into financial risks. Some organizations have weak security awareness, and the safety of the production system is not standardized. Additionally, some criminals may take advantage of the system to exploit fraud.

Big data can be used to combat fraud in online banking.[2] As internet banking has expanded, this has facilitated the innovation of bank financial services. The use of internet technology in banks, however, also has provided lawless elements with new opportunities to commit fraud. Third-party payment, peer-to-peer (P2P), and crowdfunding apps have introduced great challenges to traditional banking services, as banks must continuously improve their service quality to meet the development needs of modern society. Although people have become

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

increasingly accustomed to the convenience of online services, internet financial fraud continues to threaten the safety of online property and thus has received a lot of attention. Relevant fraud departments should increase the attention given to targeted attacks, as criminals increasingly use big data as a tool for committing online fraud. Through such attacks, criminals can obtain information from unsuspecting victims, including their names, consumption habits, and so on. Criminals may design appropriate fraudulent links according to the purchase habits of the victims to commit illegal and criminal activities. Therefore, fintech firms must use various means and technologies to establish a safety shield for consumers to prevent internet fraud and better protect people's property.

Common forms of fraud include customer identity theft, transaction fraud, and mobile terminal fraud. Identity theft occurs through two primary methods. The first is to make fraudulent applications—that is, to obtain customer information through the network and apply for the financial business using someone else's customer information. The second is account theft. This theft includes the illegal acquisition of a customer's account information through a Trojan virus or other means and the use of the customer's account to conduct fraudulent transactions to obtain financial or material benefits. This transaction fraud also has two types: (1) the pseudo-card transaction, in which the criminal copies the card through illegal channels and makes transactions using the copied card; and (2) the fraudster obtains customer cards through illegal channels and conducts transactions through online payment and other noncard transactions.

Fraud may occur through mobile banking or personal computer clients through the webpage login. It is easy to affect transaction security by pushing computer and mobile phone viruses, causing loopholes in transactions. In recent years, as smartphones are updated rapidly, the frequency of customers changing mobile phones has increased, and the use of mobile banking has become more frequent. These trends have combined to provide an important channel for fraudsters. Compared with the risk defense line of traditional bank offline business, internet finance business has added many more risks, including both network risks and traditional risks.

Security risks brought about by banks' emerging internet business applications also have risen in recent years.[3] The emergence of new applications, such as mobile finance, network finance, third-party

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

payment, corporate network financing, and direct banking, has extended banks' online business chain. The hidden dangers have increased, not only introducing technical security problems but also creating potential security risks. The most significant security vulnerabilities of a bank's internet financial system include business design flaws, cross-site scripting attacks, mobile phone SMS verification defects, login function defects, SQL injection attacks, and sensitive information disclosure. In addition to the traditional vulnerability scanning, SQL injection attacks, web backdoors, false webpages, unauthorized access, and brute force attacks, internet financial platforms face the prospect of false registration and malicious swipes. Security risks for fintech also include collision attacks, in which an attacker repeatedly tries to log in to the website through an automated tool. To accomplish this, a large number of valid usernames and passwords are collected or illegally purchased, and automated tools are used for continuous login attempts. Customers often use the same username and password combination on different websites, which makes it easier for an attacker to impersonate the user to log onto an internet financial platform for illegal activities, resulting in extensive economic losses.

Although the bank currently deploys firewalls, intrusion protection and intrusion detection systems, web application framework application firewalls, anti–distributed denial of service (DDoS), and malware protection, traditional security technologies, whether based on signatures or rules, can combat known malicious behavior. Applications can analyze and write behavior rules for protection. Automated attacks that simulate legitimate operations, such as collision-causing attacks, however, may not be identified as malicious attacks under the existing security software. If system usernames and passwords are leaked online, attackers can easily access accounts in other systems as well. Therefore, new security protection technologies are needed for these new types of security threats. To combat these threats, new security technologies have been created. These include camouflage technology and remote-browser technology. The essence of camouflage technology is to target the attacker's network, application, terminal, and data to make the hacker's tools invalid and disrupt the attacker, thus creating the need for Remote-browser technology addresses the fact that browsers are gateways to attacks, some people use a remote browser server pool. Users access the web using these remote browsers, which

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

means that the servers on which these browsers reside are isolated from the terminals and networks in the user's environment.

Yao Junxian proposes a dynamic method of interrupting hackers' intrusions.[4] These include dynamic encapsulation, dynamic verification, dynamic confusion, and dynamic tokens. Dynamic encapsulation encapsulates the underlying code of a web page. It encapsulates sensitive portals, URLs, and online forms that may be attacked on a web page, thereby hiding the entrance to the attack and preventing the attacker from predicting server behavior. Dynamic verification prevents dynamic terminals from being accessed through dynamic two-way authentication of the client and server. This form of verification randomly selects the detected items and quantities each time to increase the unpredictability of the application and greatly increase the attack cost. Dynamic confusion obscures sensitive data transmission on web pages, including cookies, post data, and URLs, to prevent forgery requests, malicious code injection, eavesdropping, or tampering with transaction content. Dynamic tokens grant one-time tokens for legitimate requests, ensuring the appropriate execution of business logic and effectively defending against automated attacks, such as web content search, web backdoors, advanced persistent threat attacks, and application-layer DDoS. Compared with the traditional security protection technology, dynamic camouflage security protection technology uses the concept of dynamic protection as its guiding ideology.

Dynamic security protection systems prevent the abuse of normal functions, such as account access, and can prevent malicious hacking, false registration, and bulk account opening using automated tools. These systems can address the defects that are difficult to identify using traditional security methods. This type of security also can prevent users from experiencing cross-site forgery attacks, fraudulent transactions, and business fraud. In this way, sensitive information can be protected from attacks such as SQL or command injection, effectively preventing attackers from accessing sensitive data.

Regulatory Technology

In 2014, the UK FCA first proposed the concept of regtech, which was defined as "using new technologies to promote financial institutions to achieve regulatory requirements more effectively."[5] Since then, the International Finance Association has defined regtech as

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

"a new technology that can efficiently and effectively address regulatory and compliance requirements."[6] These new technologies include machine learning, artificial intelligence, blockchain, biometrics, digital encryption technology, and cloud computing.

The international mainly examines regtech from the perspective of financial institutions. The Chinese government attaches great importance to the application of regtech, and defines regtech from a broader perspective, combining it with prevention and control of financial risks. The People's Bank of China's Financial Science and Technology Committee has proposed "to strengthen RegTech and actively use big data, artificial intelligence, cloud computing and other technologies to enrich financial supervision methods and improve the ability to identify, prevent and resolve financial risks across industries and markets."[7]

Guofeng Sun, director of the People's Bank of China Financial Research Institute, wrote in *Contemporary Financiers* magazine in April 2018 that regtech is an emerging technology represented by big data, cloud computing, artificial intelligence, blockchain, and other technologies.[8] Regtech is used to maintain the security and stability of the financial system, to achieve the stable operation of financial institutions, and to protect the rights of financial consumers. From the perspective of the body applying such technology, regtech includes both "compliance" and "regulation." On the one hand, financial institutions use regtech as an important tool to reduce compliance costs and adapt to regulation. From this dimension, regtech can be understood as compliance technology (comptech). On the other hand, regtech can help financial regulators to enrich regulatory tools, improve regulatory efficiency, and reduce regulatory pressure. This is an important way to maintain the security and stability of the financial system, prevent systemic financial risks, and protect the rights of financial consumers. In this way, regtech can be understood as supervised technology (suptech)—that is, regtech = suptech + comptech.[9]

From a regulator's perspective, regtech applies technology to carry out regulatory duties. The rapid development of financial technology has introduced changes in the existing financial business, and financial industry risks have revealed characteristics that are reflected primarily in the reduction of financial entry barriers, the high frequency of financial transactions and big data, and ongoing emergence of cross-industry financial products that break through the boundaries of traditional financial industries. Thus, the prediction and identification of

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

financial risks have become increasingly difficult. Although the application of financial technology brings a wide range of financial service innovations, it also generates a series of new risks, which introduce new challenges to the supervision of the financial industry. Financial regulators urgently need to improve their regulatory capabilities and reduce regulatory costs. With the development of new technologies, such as big data, cloud computing, blockchain, and artificial intelligence, conditions have been created to improve regulatory measures and reduce compliance costs.

From the perspective of financial regulatory reform, the rapid rise of regtech is a rational response to lowering the compliance costs of financial institutions and addressing the latest round of financial regulatory reforms. Since the international financial crisis in 2008, the regulatory systems of major global economies have undergone profound changes, regulatory requirements have escalated, and regulatory measures have become more complicated. The cost of regulatory compliance to meet requirements has increased, leading to the further development of regtech.

According to a study by the Boston Consulting Group, global financial institutions suffered fines of $321 billion between 2009 and 2016 because of regulatory noncompliance.[10] At the same time, the rapid development of financial technology has led to an increase in the relevance of financial services worldwide, and the differences in financial regulatory frameworks across countries also have increased the compliance costs of multinational financial institutions. The principle of unification and standardization of regtech as an emerging technology framework can resolve financial regulatory differences and conflicts between countries.

Relationship Between Regtech and Fintech

The Financial Stability Board defines financial technology as "a financial innovation brought about by technology that creates new business models, applications, processes or products. This has a major impact on the way financial markets, financial institutions, or financial services are provided."[11] The essence of financial technology is to use emerging information technology to transform and innovate financial products and services. It is to optimize, upgrade, and reshape the financial

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

industry from the perspective of technology research and development and application.

Financial technology has brought about financial innovation and injected new vitality into the financial industry. At the same time, it has ushered in new challenges to financial security. To better prevent and respond to financial technology risks, regtech has emerged. Because of the increasingly virtual service mode of fintech, along with blurred business boundaries and the continuous opening of the business environment, the financial risk situation is becoming increasingly complicated. Although the application of financial technology introduces a wide range of financial service innovations, it also generates a series of new risks, which in turn raise difficulties to supervise the financial industry.

First, cross-border financial services across industries and markets are increasingly enriched. Different businesses are becoming interrelated. Financial risks are complex and potentially contagious. Second, financial technology uses information technology to transform business flow into information flow. Although improving the efficiency of capital financing, it breaks the time and space restrictions of risk transmission, making the risk spread faster. Third, the correlation of financial products is increasing, risks are difficult to identify and measure, and risks are more concealed. Traditional regulatory measures are difficult to work. In this context, the financial management department builds a modern financial regulatory framework through regtech and develops financial regulatory platforms as well as tools based on artificial intelligence, big data, and application programming interfaces (APIs). Regtech thereby effectively enhances the accuracy, traceability, and nonrepudiation of financial regulatory information, identifying and defusing financial risks and rectifying financial chaos.

In contrast, in the context of financial technology, the financial industry, as a typical data-intensive industry, generates and processes massive amounts of data resources every day. The huge amount of financial data with scattered sources and diverse formats exceeds the processing power of traditional regulatory methods. In the face of the massive data submitted by financial institutions, the regulatory authorities need to use technology to improve processing efficiency and regulatory effectiveness. The China Finance and Technology Commission noted the necessity to strengthen regtech and proposed the use of financial technologies such as big data, artificial intelligence, and cloud

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

computing to enrich financial supervision. Financial regulators and financial institutions are aware of the important driving role of technology, thus accelerating the emergence and development of regtech.

Regtech has emerged in recent years to cope with the challenges brought about by the development of financial technology. It has become an important research field to improve the technical level and regulatory efficiency of the regulatory system and to build a new paradigm of technology-driven regulation.

Regtech is used to regulate the entire financial industry, including traditional financial and financial technology, rather than being limited to regulating the financial technology industry. That is, regtech is not just the application regulation in the fintech field but rather encompasses a comprehensive technology of regulation. The effective use of technology in the financial sector and the risks exposed by financial technology have made financial regulators and financial institutions aware of the important driving role of technology, thus accelerating the emergence and development of regtech.

Fintech promotes the development of regtech. Financial institutions use financial technology to meet compliance requirements. The UK FCA considers regtech to be a part of financial technology and has proposed that regulatory technology can ensure that regulatory requirements are met in an efficient way. The concept is narrowly defined as regtech (compliance technology), in which financial institutions use new technologies to more effectively meet regulatory compliance issues and reduce rising compliance costs. After the 2008 financial crisis, the need for financial regulation was elevated to unprecedented heights. Regulators are eager to obtain more comprehensive and accurate data. The increasingly strict supervision and intensive laws and regulations have increased the compliance costs of financial institutions. In response, the development of financial technology has enabled financial institutions to use new technologies to save compliance costs, meet regulatory requirements, and promote the development of regtech.

Regtech is used not only in the financial industry but also in all industries that are involved in compliance, especially in highly regulated industries, such as medical and health, food safety, environmental monitoring, and safe production. Therefore, the regtech industry is not limited to the financial industry but will also expand horizontally to other industries.

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

Operation Mechanism of Regtech

Compared with European and American countries, China's regtech started relatively late, and the gap remains. Table 8.1 shows that no major Chinese companies currently rank among the global regtech firms. The recent development of China's regtech, however, has been highly motivated, and the application needs are quite broad.

At the policy level, the state gives strong support to the development of regulatory science and technology. In May 2017, the People's Bank of China established the Financial Science and Technology Committee and proposed to strengthen the supervision and application of science and technology as an important means to enrich financial supervision. In June 2017, the People's Bank of China issued the Thirteenth Five-Year Development Plan for China's Financial Industry Information Technology, proposing to strengthen the research and application of fintech and regtech. In May 2018, the China Securities and Regulatory Commission (CSRC) Science and Technology Supervision Expert Advisory Committee, composed of academicians from the two academies, university scholars, and experts from the business community, was established. In August 2018, the CSRC issued the China Securities Regulatory Commission to Supervise the Overall Construction of Science and Technology notice, marking the completion of the top-level design of the supervision of science and technology construction work and the start of the full implementation stage.

Table 8.1 shows the distribution by country of major regtech companies in 2017.[12] The table shows that the United Kingdom and United States lead the world in the number of large regtech companies,

TABLE 8.1
National Distribution of Major Global Regulatory Technology Companies in 2017 (percent)

Country	United Kingdom	United States	Ireland	Luxembourg	Australia	Israel	China
Number	42	41	13	12	6	6	0

Source: China Institute of Information and Communications (CAICT), *Internet Investment and Financing in the Second Quarter of 2018* (in Chinese), CAICT, 2018, http://www.caict.ac.cn/kxyj/qwfb/qwsj/201807/P020180720343745695019.pdf.

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

whereas China had none. This likely will become an area of intense focus in the coming years.

Specific Application of Compliance Technology

Regtech can help to ensure compliance with regulations. It also acts as an early warning system for fintech companies. Dagong Credit Data Co., for example, has a list of indicators used at the provincial level to screen online loan platforms for risks and fraud. This technology was applied early on, in 2014, and found that nearly half of the 1,395 companies screened did not meet basic viability standards. Warnings arose because of a lack of information disclosure, insufficient cash flow to cover costs, situations in which a promised rate of return was higher than the actual rate of return, fraud involving false guarantees, and the possibility for other credit risk events to emerge.[13]

Specific Regtech Applications

Government Applications

Chinese financial regulators are constantly exploring the application of regtech. The Anti-Money Laundering Monitoring Center of the People's Bank of China is building a comprehensive analysis platform for the second generation of anti-money-laundering monitoring and analysis; the China Banking and Insurance Regulatory Commission will apply the distributed architecture to EAST data, combining on-site inspection programs with big data.

In August 2018, the CSRC issued the China Securities Regulatory Commission RegTech Overall Construction Plan, marking the completion of the regtech top-level design by the CSRC and entering the full implementation stage. This plan clearly defines the needs and work contents of various informatization construction work for supervising Regtech 1.0, 2.0, and 3.0. The main content of Regtech 1.0 is designed to improve the digitalization, electronification, automation, and standardization of supervision work by purchasing or developing mature and efficient software and hardware tools or facilities to meet the information needs of the basic office and specific work of

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

the departments and agencies. The content of Regtech 2.0 is to continuously enrich and improve the functions of the central regulatory information platform, optimize the construction of business systems, and realize the online operation of the entire process of cross-departmental supervision services. This will establish a good foundation for the application of technologies, such as big data, cloud computing, and artificial intelligence in Regtech 3.0.

The core of Regtech 3.0 is to build a highly efficient and effective big data supervision platform and to comprehensively use electronic evidence, statistical analysis, data mining, and other technologies to conduct comprehensive monitoring and data analysis around the main business activities of the capital market. This will enable supervisors to discover insider trading, market operations, and other violations in a timely manner.

In December 2018, the CSRC issued the Measures for the Management of Information Technology of Securities Fund Operating Agencies to guide the securities fund–operating institutions, to continuously strengthen the supporting role of modern information technology in their business activities, and to improve legal compliance and prevent risks. The management approach comprehensively covers all types of entities; clarifies the three main lines of governance, security, and compliance; strengthens the main responsibility of information technology management; and supports the application of information technology to improve service efficiency. The measures also clarify the corresponding penalties for various market entities that fail to fulfil their information technology management responsibilities.

In October 2018, the first phase of the Corporate Portrait project, which was independently developed by the Shenzhen Stock Exchange, was officially launched. The project application functions include locating information about a company's quick view, company label, equity shareholder, restructuring review assistance, and relationship map. By using text mining, cloud computing, and other information technologies, it is possible to automatically extract and intelligently prompt different means of monitoring high-frequency information, thereby effectively helping first-line supervisors to improve the ability to detect illegal activities and prevent and resolve risks.

In 2016, the Beijing Financial Work Bureau began to build a network loan risk monitoring system based on the blockchain as the underlying technology, which enables the regulatory authorities to

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

record the data reported by all online lending platforms and quickly identify and respond to abnormal transactions.

Corporate Applications

Typical corporate applications in China include the Risk Brain System of Ant Financial, the financial risk monitoring platform of Tencent Financial, and the Rubik's Cube security products of Jingdong Financial.

THE RISK BRAIN SYSTEM OF ANT FINANCIAL PROFILE

The Ant Risk Brain System has four core segments: risk detection warning, risk identification decision, risk intelligence optimization, and risk analysis insight. These four parts work together to make up a comprehensive risk control system.[14]

The risk warning system is equivalent to the eyes of the risk control system and is used to sense and predict risks. Risk groups are identified through risk anomaly identification, which are presented graphically and visually, and risk experts are used to judge risks and anomalies. This process will push the necessary model and strategy adjustments in real time to form a closed-loop optimization of the risk control system.

The risk identification system is at the core of risk prevention and control. The process must be comprehensive and three-dimensional. This means that it is necessary to build a comprehensive risk-scanning system based on people, environment, network, equipment, blacklists, and conflicts. The most worrying aspect of risk prevention and control is that the system will default when one layer is broken. To address this issue, the Ant Risk Brain presents a three-dimensional risk control system with five layers. If a single layer is broken, the next layer will take over, which is more secure and reliable than the traditional risk prevention and control system.

Behind the risk identification is a security policy model. If a customer is identified as posing a risk, the final judgment needs to be intelligently analyzed from multiple dimensions, considering the availability and applicability of the actual environment and risk preferences to make intelligent and personalized decisions based on risk control and user experience.

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

Ant Financial also practices faster and more effective control of risks through human-computer collaboration. It does so in three main ways. First, it analyzes user tags based on a single case and connects time, space, and behavior to restore the whole process of a case, locating missing points (such as missing customer income) and risk points in the risk control system. Second, it analyzes the knowledge map and uncovers fraudulent rings and their characteristics. Third, it makes a strategically intelligent recommendation, combining intelligent algorithms and expert experience and using it to adjust the risk prevention and control system. In addition, Ant Financial's risk control system can self-optimize and self-evolve, making timely and effective adjustments and optimizations for new risk situations.

The Ant Risk Brain System has extended its risk security capabilities to three areas. The first is in the field of government and people's livelihood, including areas of aviation, taxation, and railway. Ant Financial offers six core competencies: account protection, marketing protection, channel protection, transaction protection, mobile protection, and content protection. Taking the Eastern Airlines app as an example, the Ant Risk Brain provides China Eastern Airlines with a full risk control solution to prevent user points from being stolen and to prevent mistakes in customer seating.

The second area of security capabilities is applied to the banking sector. Under the background of digital banking transformation, Ant Financial has exported risk prevention and control programs and infrastructure for banks to help banks transform. On April 9, 2018, Ant Financial Services Group signed a cooperation agreement with Chongqing Three Gorges Bank Co., Ltd. The two parties will establish a joint venture innovation laboratory for financial technology to explore and practice the implementation of new financial technology in the banking business. The Ant Risk Brain will help construct the Three Gorges Bank's risk control system and enhance the ability of the Three Gorges Bank to prevent and control risks and serve the real economy.

The third field of risk security capability is in regtech. The Ant Risk Brain uses advanced technologies such as big data, cloud computing, blockchain, and artificial intelligence to build a more efficient intelligent monitoring system. The system enables financial regulators to realize real-time, intelligent, and visualized financial risk monitoring. The Ant Risk Brain can help local regulatory authorities

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

conduct multidimensional risk investigations of financial institutions and achieve dynamic scanning of all risk areas, including stakeholder, operational, and compliance risks. Through knowledge map mining, regulatory authorities can identify potential risks among affiliates in a timely manner and identify suspected financial fraud rings at their root. It also helps regulators build regional and industry-wide risk indices, quickly identify regional and industry risks, and detect macrofinancial risk trends.

Regtech Core Technologies

The core technologies of regtech are cloud computing, big data, artificial intelligence, blockchain, and API. Cloud computing provides low-cost computing and storage resources for regtech and provides large-scale data resources through centralized data aggregation to enhance the sharing of regulatory tools. Big data enables large-scale data mining and analysis capabilities as well as efficient real-time processing capabilities. Artificial intelligence further enhances the intelligent analysis capabilities of data and enhances customer interaction capabilities. The blockchain guarantees the authenticity and efficiency of the acquired basic information, ensures business compliance, and improves the efficiency of business processing. The API helps to effectively enforce regulatory policies and compliance guidelines, improve the regulatory nature of regulation, and conduct supervision in a minimally disruptive manner.

Regtech Application Scenarios

To date, regtech's basic application has been to electronically report paper regulatory processes, reduce regulatory human resource costs, and effectively reduce compliance costs. The high-level regtech application utilizes advanced technologies to program regulatory policies and directives, embed them in various business systems, and verify and alert to risks in a timely manner. The five main applications for the use of regtech are data processing and reporting, customer identification, financial institution stress testing, market behavior monitoring, and legal and regulatory information tracking.

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

The first application is in the field of compliance data processing and reporting. After the financial crisis, the requirements of regulatory agencies for the reporting of financial institutions' data were constantly increasing. Financial institutions needed to submit data of different structures and different statistical dimensions to multiple regulatory agencies, which greatly increased the compliance costs of financial institutions. Financial institutions can improve compliance data-reporting capabilities through data asset management and reduced compliance costs. The underlying technologies involved in this area include big data, cloud computing, and digital encryption technologies. Compliance data reporting is achieved mainly by acquiring and processing a large amount of structured data, establishing standardized data reports, improving the convenience of data sharing, and achieving rapid generation of compliance data reports. With this encryption technology, the security of data sharing is improved simultaneously and data integrity and privacy are guaranteed.

The second application is in the field of customer identification. Regulators have clear regulatory requirements for financial institutions to "know your customers" (KYC) to avoid illegal business practices that are not operated by customers, such as credit card theft and opening of accounts with false documents. The process uses intelligent biometric technology and big data comparison technology to automate the KYC procedure and integrate multiple KYC data sources into one application through an API to improve customer identification ability and intercept abnormal account operations.

The third application is in the field of stress testing for financial institutions, to simulate real trading scenarios in a virtual environment and to test the stability and security of financial institutions. This application mainly uses technologies such as big data, artificial intelligence, and cloud computing to quickly process large amounts of data, analyze many data variables, reduce scene distortion, improve the accuracy of scenario testing, realize the dynamics of stress testing, and help financial institutions maintain stability. Timely discovery of risks and related measures are used to effectively prevent risk accumulation. It also is possible to reduce the cost of stress testing through cloud computing and to help financial institutions achieve self-compliance.

The fourth application is in the field of market behavior monitoring. Regulators and financial institutions need to take effective measures to identify violations of internal transactions, money laundering,

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

fraud, illegal fundraising, and multiaccount manipulation. Monitoring is mainly applied to big data processing, artificial intelligence, and machine learning and is accomplished through the multidimensional, high-frequency, full-dynamic real-time analysis of transaction data, mining the subject relationship and deep information from large amounts of information on trading behavior.

The fifth application is in the field of legal and regulatory information tracking. With the continuous tightening of financial supervision and the intensive introduction of regulatory laws and regulations, financial institutions need to keep track of current rules every day and compare the similarities and differences between old and new documents. This application primarily uses artificial intelligence technology to quickly identify and learn the latest laws and regulations, promptly remind the financial institutions of relevant regulatory changes, and reduce the legal compliance risks of financial institutions. It also analyzes and compares the similarities and differences between regulatory documents in different countries, helps to achieve global requirements, conducts risk assessment, and provides guarantees for financial institutions to achieve legal cross-border business.

Regulatory Sandbox

Some experts have recommended a regulatory sandbox, which would allow small-scale, live testing by small firms under government supervision. This is in use in many industrial countries, including the United States, Canada, Thailand, Australia, and the United Kingdom.

In the United Kingdom, a regtech sandbox has enabled startup fintech firms to create applications for compliance, data analysis, and risk evaluation. The UK's regtech sandbox is for institutions engaged in financial innovation, under the premise of ensuring consumer rights, following the FCA's simplified approval procedures, submitting applications and obtaining limited authorizations, and conducting financial product or service innovation tests within the scope of application. The FCA monitors the testing process and evaluates the situation to determine whether formal regulatory authority is granted and can be promoted outside of the sandbox.

Other economies, such as Abu Dhabi, Singapore, Australia, Hong Kong, China, and Taiwan, also have implemented a regulatory sandbox

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms

plan or proposed similar regulatory measures. The regulatory sandbox has relaxed regulatory restrictions for financial technology innovation, will not have an impact on the current legal framework, and also can serve as a decision-making system in which the legal regulation may be difficult to adjust quickly during the rapid emergence of innovation.[15]

The regulatory sandbox concept is similar in its implementation to China's regional financial reform pilots. Both concepts reflect the fact that in the process of reform, the government allows local areas to take the first step, carry out institutional innovations, summarize the pilot experience and lessons learned, and then push the new system to the greater economy. Therefore, from the perspective of the financial reform in mainland China, a basis already exists for adopting a regulatory sandbox for financial technology supervision.

As the wave of financial technology sweeps around the globe, increasing numbers of countries and regions have joined the ranks of regulatory sandboxes. Compared with other countries and regions, the regulatory sandbox is still in the conceptual stage in China. Chinese regulators can learn from the practices followed in the United Kingdom, Singapore, and other countries: adjust regulatory objectives and responsibilities in a timely manner; enhance forward-looking thinking; and study the applicability to China. Regulators also can explore the creation of a regulatory tool that applies financial innovation in order to reduce risks.

Fintech incubators and accelerators have been set up to test the risk properties of innovative firms. China's city of Ganzhou in Jiangxi Province, as well as the National Internet Emergency Center and Xinhua Net, already have set up the first regulatory sandbox. This sandbox is exploring the role of regtech in the fintech industry and aims to identify and resolve financial risks of internet finance companies operating in the sandbox to improve risk control technology and further develop the regtech industry.

This content downloaded from 157.253.50.50 on Sun, 23 Aug 2020 23:25:46 UTC
All use subject to https://about.jstor.org/terms