Finance Research Letters 65 (2024) 105533

Contents lists available at ScienceDirect

Finance Research Letters

journal homepage: www.elsevier.com/locate/frl

Cybersecurity governance and digital finance: Evidence from sovereign states

Shihui Cheng [a,1], Jing Li [b,*,2], Lai Luo [c,3], Yumin Zhu [d,4]

[a] College of Public Administration, Huazhong University of Science and Technology, China
[b] School of Economics, Minzu University of China, China
[c] School of History and Culture, Hubei University, China
[d] School of International Trade and Economics, University of International Business and Economics, China

ARTICLE INFO

Keywords:
Cybersecurity
Digital finance
Double fixation models

ABSTRACT

Digital finance provides unprecedented development opportunities for countries, especially in times of epidemic, and digital transformation has become an important means of accelerating economic development and maintaining social stability. However, digital finance relies on Internet infrastructure, and cybersecurity challenges have increased, bringing severe security risks to digital finance. Therefore, safeguarding network security has become a key cornerstone for the development of digital finance. This paper analyzes and explores the main cybersecurity problems faced in the era of big data from the perspective of the current development status of digital finance, and at the same time shows some new initiatives currently underway in the international arena in order to meet the challenges posed by cybersecurity and to help navigate the sustainable development of global digital finance.

1. Introductory

With the digital transformation of industries taking place on a large scale, digital finance has become one of the main engines driving economic growth in countries around the world. Many new industrial models during the epidemic have further accelerated the digitalization of human society. In the era of digitization, the rapid development and deep integration of big data technology with artificial intelligence, cloud computing and other new-generation communication technologies have led to rapid changes in all aspects of social life and government management. On the one hand, big data technology can rapidly obtain data and facilitate the dissemination and analysis of data, which brings great convenience to government management (Wang, 2023), daily life and work and study; on the other hand, there are risks of illegal theft of personal information, illegal trafficking in confidentiality leaks for improper

* Corresponding author.
E-mail address: 20400027@muc.edu.cn (J. Li).
[1] Postdoctoral fellowInstitutional email : arc_csh@hust.edu.cnResearch interests: Global Digital Governance, International Cooperation of Digital Economy, Global Issue, International Law
[2] Institutional email:20400027@muc.edu.cnHomepage: NoneEducation Background: PhD in Chinese Ethnic Economics, Minzu University of China (2020 to present)Career history: NoneResearch interests: National Economy, Digital Economy and Agricultural Modernization, Digital transformation
[3] Research interests: National Culture and National Communication, Intercultural Communication, Global Issue
[4] Institutional email: 202000182007@uibe.edu.cn

https://doi.org/10.1016/j.frl.2024.105533
Received 22 December 2023; Received in revised form 11 May 2024; Accepted 12 May 2024
Available online 13 May 2024

interests, and cyber-attacks are becoming increasingly severe, with the Internet healthcare industry, telecommuting, and online education becoming the focus of the attack, and cyber rumors rising in all directions (Zhou, 2023). The Internet has become a key target of attacks in the medical industry, telecommuting, online education, etc., and cyber rumors have been spreading, seriously affecting the normal operation of society and the development of digital finance (Xu, 2024).

The new round of technological and industrial revolution is changing rapidly, and the application scenarios of digital finance are becoming more and more rich and complex (Tian et al., 2022). Accompanied by the new industry and new fields spawned in the epidemic period, the development of digital finance is faced with more severe cybersecurity challenges, and the problem of cybersecurity should not be ignored (Wang, 2023). The main purpose of this paper is to provide the following theoretical foundation and reference experience for the green development of enterprises in China: firstly, to explore the impact of cybersecurity on digital finance by constructing a double fixed effect model; secondly, to solve the problem of endogeneity among variables by using the two-stage least squares method; and lastly, to study the difference of cybersecurity on digital finance under different samples from the perspectives of developed countries and developing countries in separate samples. Guaranteeing cybersecurity is the cornerstone of digital finance development. This paper analyzes the cybersecurity risks and challenges faced in digital finance from the current situation, and explores the corresponding countermeasures and suggestions, aiming to contribute to the navigation of global digital finance development.

2. Literature review

2.1. Research related to digital finance

Digital finance refers broadly to the use of modern digital technology to complete the customer development and screening of financial and financial institutions, traditional and other new types of financial business services operation mode (Huang Yiping, 2018). Hao (2018) combed and summarized the development of China's digital finance in recent years, and found that the operation mode of financial services and the way to complete the service, etc. changed with the development of digital finance, but the combination of finance and digital technology did not affect the core connotation of finance. Haizhang et al. (2020) believe that traditional finance through the combination of a new generation of digital technology makes the massive generation of data, rapid collection, efficient processing, and low-cost sharing a reality, and will gradually transform the traditional financial framework based on "credit" into a digital realization based on "data". The combination of data generation, rapid collection, efficient processing, and low-cost sharing has made the traditional financial framework based on "credit" into a "data"-based digital realization. Hui et al. (2021) believe that digital finance relies on modern digital technology to make business breakthroughs in the traditional financial "credit" framework and geographical and spatial limitations, greatly expanding and enhancing the scope and depth of traditional financial services, and effectively improving the efficiency of China's financial services and the degree of service to the real economy. Ozili (2017) believes that compared with the traditional financial model, digital finance is characterized by convenience and security. Song et al. (2020) believe that the development of financial technology will force the transformation and upgrading of the traditional financial sector, and realize the "superiority and elimination" of the financial industry. Dong et al. (2018) believe that the new financial industry generated by the combination of modern technology and traditional finance is an important engine for human society to move forward to the digital economy and information civilization. Yiping et al. (2018) found that compared with other countries, China has the advantage of digital technology, relatively loose policies and the lack of formal financial services, and other factors have jointly promoted the rapid development of digital finance.

2.2. Research related to cyber security

In the field of cybersecurity, foreign studies focus on the importance of cybersecurity and the way it is protected. Anderson and Moore (2006) argue that cybersecurity is a great incentive for economic development and that the economics of information security is becoming a thriving discipline. In it, the reliability of cybersecurity is crucial. Norbekov (2020), from an ideological perspective, states that cybersecurity involves customs, traditions, and historical cultures and proposes relevant countermeasures. AlGhamdi et al. (2020), on the other hand, point out that cybersecurity plays an important role in the protection of an organization's business and suggests ways of aligning cybersecurity policies with the organization's goals as a Solution. Thus, from macro to micro, from economic base to superstructure, cybersecurity has been a hotly debated issue. Most of the literature has approached it from the perspectives of law and computer science.

Dengguo et al. (2014) summarized the connection between big data security and privacy protection and cybersecurity, and explained the key technologies related to cybersecurity protection. Xiaying (2019) explains the rationale for data control from four aspects: personal information protection, corporate data interests, undue competition regulation, and cybersecurity protection, and proposes the theoretical structure of "sharing-control". Shen Satellite (2020) points out that the biggest institutional obstacle to the development of digital finance is the problem between data ownership and distribution rules, and calls for the construction of a binary rights structure of data ownership and data use rights, so as to protect data security and fully utilize the value of data.

From the perspective of national network security, Na et al. (2004) put forward the "5432" strategy, which takes into account the basic attributes, basic capabilities, basic elements and construction aspects of national network security, and builds an effective theoretical framework for China's national network security protection system. Wenchao et al. (2013) discuss the protection measures of national cybersecurity from the three major aspects of the construction of information infrastructure, the enhancement of information warfare capability, and the exertion of public diplomacy. Aimin and Gaofeng (2016), on the other hand, start from the theory of

data sovereignty and suggest establishing a data sovereignty system and strengthening the improvement of the network security law at the same time.

2.3. Correlation studies between cybersecurity and digital finance

Obviously, there is a close link between digital finance and cybersecurity. Without the development of information technology, digital finance can only remain in theory. With the progress of science and technology, Internet technology has penetrated into various industries, giving rise to a new form of development of digital finance. Cybersecurity is no longer a proper noun, but is gradually integrated into the digital financial industry, and the scope of subjects involved is also expanding, showing a trend of diversified development.

In addition, we can observe that well-known domestic leading digital finance companies, such as Ali, Baidu, Meituan and Tencent, are listed on the NASDAQ in the United States or the Hong Kong Stock Exchange in China, without choosing to list on the domestic stock market. The vast majority of investors in these companies come from outside the country and are also subject to foreign laws. U.S. securities regulators have been trying to obtain the audit transcripts of these listed companies, and have even introduced the Foreign Corporation Accountability Act, which puts some Chinese concept stocks on the pre-demonetization list to warn other companies. It is evident that cybersecurity is directly related to the healthy development of the digital finance industry. Therefore, network security is an issue that cannot be ignored in the development of digital finance.

According to Guokai (2021), the importance of cybersecurity in the context of digital finance is mainly reflected in the three aspects of preventing infringement, promoting the healthy development of digital finance and promoting the construction of digital China. Bing and Zhen (2021) pointed out that in digital finance, there are problems such as the risk of citizens' personal property security, unclear data ownership and national security risk. At the same time, China is also facing a rule of law dilemma when dealing with the protection of network security under digital finance. However, it would be detrimental to the country's development to have reservations about digital finance just because it may bring cybersecurity problems. License (2019) points out that one year after the implementation of the General Data Protection Regulation (GDPR) in the European Union (EU), mature Internet businesses, emerging industries, and economic innovations in EU countries have suffered some damage. At the same time, the GDPR focuses too much on personal data protection, instead weakening cybersecurity. It can be seen that the disorderly development of digital finance will certainly jeopardize the cybersecurity of citizens and even the country, while too harsh cybersecurity protection will limit the development of digital finance.

Therefore, how to reconcile the relationship between digital finance and cybersecurity is an issue to be considered. Qingxin and Kai (2017) argued that in the era of digital finance, the government should innovate the supervision method, improve the supervision system, and strengthen the cybersecurity supervision of key digital industries. Yue (2018) explains the three major principles of network information security in the era of digital finance from the perspective of the Network Security Law, and proposes a path strategy for China's participation in international data privacy governance. Jianbo and Danhui (2019), on the other hand, argue that a multi-party collaborative governance mechanism is an indispensable part of safeguarding cybersecurity under the development of digital finance, which involves the construction of government legislation and standards, as well as the self-discipline and preventive supervision of enterprises. Yihua et al. (2019) constructed an evolutionary game model and analyzed it through MATLAB, pointing out that government regulation, internal governance mechanism and judicial liability system are conducive to the protection of personal information security in the era of digital finance. Jing and Taixuan (2020) focus on the coupling of public and private law right rules, liability system, regulatory model and safeguard methods for personal information security protection in the context of digital finance.

3. Modeling and study data

3.1. Modeling

The three main approaches to panel data modeling are fixed effects models, difference-in-differences models, and random effects models. Fixed-effects models cover individual fixed-effects models, time fixed-effects models, and point-in-time individual fixed-effects models, which model changes in the intercept at the individual, time, and point-in-time levels, respectively. When selecting the optimal model, model complexity and likelihood function need to be balanced, and commonly used selection methods include the Akaike Information Criterion (AIC) and the Bayesian Information Criterion (BIC), which avoid the overfitting problem by introducing a penalty term, where the BIC is more stringent in considering the number of samples, and helps to prevent overfitting due to excessively complex models.

Therefore, based on the results obtained, this paper concludes that the dual fixed effects model is superior to the single fixed effects model. Therefore, we believe that the double fixed effects model is more reliable. In order to conduct a more intuitive analysis of the impact of cybersecurity on the digital economy, the model is constructed as follows on the basis of the existing literature:

$$Fin_{it} = \alpha_0 + \alpha_1 network_{it} + \alpha_3 control_{it} + \varepsilon_{it}$$

In the above equation, i denotes the individual, t denotes the year, digital finance (Fin) is the explanatory variable, cybersecurity (network) is the core explanatory variable, control is the relevant control variables: per capita GDP (gdp), stable server (internet), mobile cellular subscription per 100 people (iphone), consumer price index (cpi), foreign direct investment (fdi), with δ_i are individual fixed effects, the ρ_t are time fixed effects, and ε_{it}. is a randomized disturbance term.

3.2. Description of variables

This paper is selected for 2018–2021, 42 countries, totaling 168 observations. The size of the digital economy is from the Global Digital Economy White Paper by the China Academy of Information and Communication Research, and the cybersecurity index is from the e-Governance Academy (https://ncsi.ega.ee/). All other data in this paper come from the World Bank, and data processing and regression analysis was done through Stata17.0.

3.3. Descriptive statistical results

In this paper, descriptive statistical analysis was first conducted to show the basic characteristics of the selected data, and the results are shown in Table 1. It can be seen that the digital finance index in the sample does not change much, and the range of fluctuation is relatively small, with a mean value of 0.567. The average level of the cybersecurity index is higher, but with greater fluctuations, which may have greater changes at different times, with a mean value of 0.688. The average level of GDP per capita is high and relatively stable, indicating relatively stable economic development, with an average value of 10.300. The Consumer Price Index has a wide range of fluctuations, and there may be a greater risk of inflation, with an average value of 1.760. There are greater fluctuations in OFDI, indicating that there may be greater changes in the inflows or outflows of foreign capital, with an average value of 1.668. The Stable Web Server Index has a high average level but with a stability that may have greater fluctuations, with an average value of 9.758. Mobile communications penetration is low, and there may be some degree of digital divide, with an average value of 1.056. (Table 2)

3.4. Multiple covariance analysis and correlation analysis

3.4.1. VIF multicollinearity test

The variance inflation factor (VIF) is a measure of the severity of multicollinearity in a multiple linear regression model. It represents the ratio of the variance of the regression coefficient estimates compared to the variance when no linear correlation is assumed between the independent variables. Multicollinearity refers to the existence of a linear correlation between independent variables, i.e., one independent variable can be a linear combination of one or more other independent variables. The test usually uses 10 as the judgment boundary. When VIF < 10, there is no multicollinearity; when $10 <= \text{VIF} < 100$, there is strong multicollinearity; when VIF $>= 100$, there is serious multicollinearity.

The values of VIF for all the above variables are <10 and the result of 1/VIF is also greater than 0.1, Mean VIF of 1.77 is also <10, thus indicating that the covariance between the variables is not strong. (Table 3)

3.4.2. Correlation analysis

After obtaining the relevant data information, we have to analyze these data and study the relationship between the variables. Correlation analysis is a very widely used method. It is a statistical analysis method that does not consider the causal relationship between the variables but only studies and analyzes the correlation between the variables, and the commonly used correlation analysis includes simple correlation analysis, partial correlation analysis and so on.

Therefore, this paper carries out a simple correlation analysis on the data of digital finance (Fin), network security (network), GDP per capita (gdp), stable network server (internet), mobile penetration (iphone), consumer price index (cpi), foreign direct investment (fdi) and other variables, and the results are shown as follows, from which the correlation coefficients between the various correlation coefficients between the variables, in which the correlation coefficient between the digital financial index (Fin) and cybersecurity (network) is 0.356 and positively significant at the 1 % level. Because of the large number of variables, only correlation variables with an absolute value greater than 0.5 are now selected for interpretation. The larger the absolute value of this correlation coefficient indicates a closer relationship between the two variables, meaning that the variables are more highly correlated. The correlation coefficient between stable web servers (internet) and GDP per capita (gdp) is significant at 0.673. This may indicate that in countries or regions with a higher level of economic development, there are usually more stable and reliable web servers. Higher GDP per capita means more investment and resources for building and maintaining network infrastructure, including web servers. This investment improves the performance, stability, and security of web servers, which reduces the risk of network outages and failures and ensures that users can access Internet services more smoothly. The correlation coefficients of the variables as a whole are not close to -1 or 1, and are overall in the range of -0.5 to 0.5, indicating that the variables are better independent and less likely to have a negative impact

Table 1
Description of variables.

	Variable name	Variable letter	Variable description
explanatory variable	digital finance	Fin	Scale of the digital economy
Core explanatory variables	network security	network	Network Security Index
control variable	GDP per capita	gdp	Natural logarithm of GDP per capita
	Stable Web Server Index	internet	Secure Internet servers (per 1 million people)
	Mobile penetration rate	iphone	Mobile cellular subscriptions (per 100 population)
	consumer price index CPI	cpi	price and consumption levels
	external direct investment (OFDI)	fdi	Foreign direct investment, net inflows (percentage of GDP)

Table 2
Descriptive statistics.

Variable	*N*	Mean	p50	sd	Min	Max
Fin	168	0.567	0.569	0.0870	0.370	0.789
network	168	0.688	0.705	0.143	0.320	0.920
gdp	168	10.30	10.530	0.805	8.092	11.520
cpi	168	1.760	1.709	1.352	−1.139	6.694
fdi	168	1.668	1.938	7.748	−37.68	29.699
internet	168	9.758	9.921	1.402	5.435	12.530
iphone	168	1.056	1.168	0.380	0.292	1.862

Table 3
VIF multicollinearity analysis.

Variable	VIF	1/VIF
gdp	2.54	0.394077
internet	2.26	0.44254
iphone	1.62	0.618159
cpi	1.4	0.715353
fdi	1.02	0.979801
Mean VIF	1.77	

on the subsequent regression analysis. It shows that the data selected in this paper are overall reliable, alleviating the problem of covariance of the regression equation to a certain extent, and the subsequent regression analysis can be carried out. (Table 4)

4. Empirical analysis

4.1. Benchmark regression

Through the selection of indicators and model setting and testing in the above subsections, the double fixed effect model is selected for empirical analysis based on panel data and the results shown in the table below are obtained: (Table 5)

In the regression process, we use cybersecurity as the base variable and then add other control variables to the regression, which will make the results more stable. In the estimation results of the table, the first column is regressed only on cybersecurity (x) as an explanatory variable, and from the regression results, it can be seen that cybersecurity (x) passes the test of significance at the 1 % level, with a coefficient of 0.406. That is to say, for every unit increase in cybersecurity, digital finance (Fin) will increase by 0.406 units correspondingly, which indicates that as cybersecurity proceeds it will promote the improvement of digital finance (Fin). Fin) enhancement. In the second column, after the inclusion of control variables, the regression coefficient of cybersecurity (x) is 0.114 and is significantly positive at the 10 % level. It can be seen that after the inclusion of each of the above variables, there is a small increase in the magnitude of the coefficient values of the explanatory variables, which are the most important concern of this paper, and their positive correlation with digital finance (Fin) remains unchanged, i.e., cybersecurity has a significant positive impact on digital finance (Fin). This may be due to the fact that cybersecurity is one of the basic prerequisites for the development of digital finance. With the popularization of digital financial services, users' online transactions and information transmission become more and more frequent, so the guarantee of cybersecurity is crucial for users to trust and use digital financial services. Second, a higher level of cybersecurity can reduce risks such as cyberattacks and fraud, further enhancing users' confidence in digital finance. This explains to some extent the robustness of the above estimation results.

In terms of control variables, GDP per capita (gdp): the regression coefficient is 0.005 and is significant at 1 % level of significance. This indicates that there is a positive relationship between high GDP per capita and larger digital finance, i.e., the higher the level of economic development, the larger the digital finance. This may be due to the fact that higher levels of economic development are usually accompanied by greater wealth accumulation and consumption power. Higher GDP per capita means that more people have the economic power to use digital financial services, which in turn promotes the development of the digital finance market. Second, a

Table 4
Correlation analysis of variables.

	Fin	Network	gdp	cpi	fdi	internet	iphone
Fin	1						
network	0.356***	1					
gdp	0.401***	0.326***	1				
cpi	−0.213**	−0.0170	−0.270***	1			
fdi	0.0310	−0.0580	−0.0940	0.0840	1		
internet	0.270***	0.422***	0.673***	−0.233**	−0.0880	1	
iphone	−0.00100	−0.232**	−0.171*	−0.389***	−0.0870	0.188**	1

Table 5
Benchmark regression results.

	(1) Fin	(2) Fin
network	0.406***	0.393***
	(5.76)	(5.23)
gdp		0.005***
		(5.25)
cpi		−0.006
		(−1.05)
fdi		0.001
		(1.13)
internet		0.042***
		(6.26)
iphone		−0.040***
		(−5.86)
_cons	0.294***	−0.095
	(6.55)	(−0.08)
N	168	168
R^2	0.492	0.519
Year	Yes	Yes
FE	Yes	Yes

Note: Values in parentheses are standard errors. "***", "**", "*" indicate that the indicator is significant at the 1 %, 5 % and 10 % levels, respectively.

relatively high level of economic development can also provide broader business opportunities and an innovative environment for digital finance. The regression coefficient of stable web server index (internet) is 0.042 and is significant at 1 % significance level. This implies that stable web servers can provide high-quality and reliable services and provide users with a good experience. In digital finance, real-time and security of transactions are very important, and a stable network server can safeguard these needs, thus increasing users' trust in digital finance and promoting the development of digital finance. Mobile penetration rate (iphone): the regression coefficient is −0.040 and is significant at 1 % significance level. Lower mobile penetration means fewer people are able to use mobile devices for digital finance transactions and services. Mobile devices play an important role in digital finance and the lack of penetration may limit the popularity of digital finance and the expansion of the user base. And consumer price index (cpi) and foreign direct investment (fdi) are not significant.

4.2. Endogeneity test

First, in the analysis of the impact of cybersecurity on digital finance, it is crucial to ensure that cybersecurity has a substantial impact on digital finance. Existing research shows that there is an endogenous relationship between network security and digital finance that influences each other: on the one hand, network security affects the development of digital finance; on the other hand, digital finance also has an impact on network security. This paper argues that while network security has an impact on digital finance, changes in digital finance may also have an impact on network security. Therefore, there may be a mutual causal relationship between cybersecurity and digital finance, which leads to endogeneity problems. In addition, the regression analysis of panel data using a fixed effects model may lead to bias problems due to endogeneity.

Table 6
Endogeneity test.

	(1) 'One period behind'	(2) 'Mean value'
network	0.134*	0.323***
	(1.73)	(5.24)
gdp	0.051***	0.001***
	(3.09)	(5.17)
cpi	−0.004	−0.004
	(−0.55)	(−1.45)
fdi	0.001	0.002
	(0.65)	(1.03)
internet	−0.009**	0.025***
	(−2.86)	(5.26)
iphone	0.034*	−0.048***
	(1.75)	(−5.76)
_cons	0.014	−0.035
	(0.09)	(−0.05)
R^2	0.249	0.519
N	126	126

Therefore, in order to estimate the above model, the instrumental variable two-stage least squares method is used here to re-estimate the role of cybersecurity on the impact of digital finance in order to avoid estimation bias arising from the empirical regression. The selection of instrumental variables is subject to certain conditions: instrumental variables are correlated with endogenous variables, uncorrelated with the random disturbance term, uncorrelated with the rest of the explanatory variables, and uncorrelated between multiple instrumental variables when more than one instrumental variable exists. The core explanatory variables with one period lag and taking the mean were selected as instrumental variables. (Table 6)

In the table, network as the core explanatory variable is regressed, and the results show that network security still has a significant positive effect on digital finance, and every unit increase in network security leads to a 0.134 increase in digital finance. The above results show that the positive effect of network security on digital finance is still significant in the 2SLS regression. Therefore, there is no substantial difference in the conclusions obtained compared to the previous paper.

4.3. Heterogeneity analysis

The study conducted a regression analysis of the different samples, taking into account country characteristics, in order to obtain more focused conclusions. Given the differences in the level of impact between developed and developing countries, the study divided the total sample into two groups and tested for heterogeneity. We applied the fixed effect model to analyze the heterogeneity of the relevant data. The specific regression results are shown in the table below: (Table 7)

The coefficient of the impact of cybersecurity (NETWORK) on digital finance is positive in both types of firms, but the coefficient is larger in developing country firms, indicating that the impact of cybersecurity on the digital finance of developing country firms is more significant. The possible reason for this is that developing country firms face more cybersecurity challenges and risks in the process of digital transformation, so the impact of cybersecurity on their digital finance is more prominent.

Second, GDP per capita (gdp) GDP per capita has a positive impact on the development of digital finance in both developed and developing countries, but its impact is more significant in developed countries. This may be due to the fact that in developed countries with higher economic power and spending power, people are more likely to use digital financial services. In developing countries, on the other hand, although an increase in GDP per capita also leads to the development of digital finance, the impact of other factors may be more prominent. Thus an increase in GDP per capita has a more significant impact on digital finance. Consumer price index (cpi) In developed countries, the effect of cpi on digital finance is positive while in developing countries it is negative. This may be due to the fact that lower inflation and stable price environment in developed countries makes people more willing to use digital financial services. Whereas in developing countries, higher inflation rate may have reduced people's trust and willingness to use digital finance. Stable Web Server Index (internet): There are differences in the impact of the stable web server index on digital finance in developed and developing countries. In developed countries, the effect of the Stable Web Server Index on digital finance is not significant, while in developing countries, its effect on digital finance is significantly positive. This may be due to the fact that in developing countries, stable web servers can provide better service quality and user experience, which can promote the development of digital finance. Mobile penetration (iphone) is significantly negative in both developed and developing countries, and the negative impact coefficient is larger in developing countries, which may be due to the fact that in developed countries, the digital finance market is already relatively mature, and there are many competitive digital finance service providers and products, which may also lead to the relatively small impact of mobile penetration on digital finance. In developing countries, on the other hand, mobile penetration may reflect the current state of the digital divide. While cell phone and smartphone penetration is increasing in developing countries, many people still

Table 7
Heterogeneity analysis by nature of subnationality.

	(1) 'Developed countries'	(2) 'Developing countries'
network	0.434***	0.520***
	(3.35)	(4.77)
gdp	0.064***	0.052*
	(3.42)	(1.88)
cpi	0.001***	−0.009***
	(3.13)	(−4.76)
fdi	0.001	−0.001
	(0.64)	(−0.82)
internet	0.004	0.086*
	(0.08)	(1.83)
iphone	−0.024*	−0.122*
	(−1.37)	(−1.97)
_cons	0.878	0.127
	(0.55)	(0.08)
N	92	71
R^2	0.519	0.797
Year	Yes	Yes
FE	Yes	Yes

Note: Values in parentheses are standard errors. "***", "**", "*" indicate that the indicator is significant at the 1 %, 5 % and 10 % levels, respectively.

have no exposure to digital financial services or do not trust them. This may lead to a relatively low take-up of digital financial services, which in turn affects the development of digital finance.

4.4. Robustness tests

4.4.1. Reduction of the sample

Since when we analyze within the whole range of the obtained data set, we often find that the conclusions obtained by changing different time periods may be completely different. Therefore, in order to test whether the empirical results of the fixed-effects regression model constructed in the previous section are robust and to ensure the rigor of the research results, we further, by reducing the sample data to conduct the first robustness test results are shown in the table below. (Table 8)

Network security (NETWORK) passed the significance test at the 1 % level, with a coefficient of 0.520 in the regression. which is basically consistent with the empirical results in the previous section. The significance and positive and negative correlation of the core explanatory variables also did not change significantly, proving that the establishment of the previous model is reasonable and the regression results are stable.

4.4.2. Replacement regression methods

Meanwhile, the regression of fixed effects was replaced with OLS for testing, and the regression results are shown in the table (Table 9).

Network security (network) passed the test of significance at the 1 % level, with a coefficient of 0.213 in the regression. The results of the test of the robustness of the replacement method remain basically the same as the regression results above, and the robustness is verified. The results are also similar to the base regression results, again indicating that the findings of this paper are highly robust.

Finally, a robustness test replacing the double fixed effects with only fixed individuals yielded the following results (Table 10):

In this study, the core explanatory variables passed the significance test. This result is basically consistent with the empirical results in the previous section, in addition, it is also noted that the significance and positive and negative correlations of the other control variables did not change significantly, indicating that the previously established model is reasonable and the regression results are stable and reliable.

5. Conclusions and policy recommendations

Based on the previous analysis, this study chooses cybersecurity as the core explanatory variable, digital finance as the explanatory variable, and considers seven control variables under the macro perspective: per capita GDP, stable web server index, mobile penetration rate, consumer price index, and outward foreign direct investment. The empirical regression of the panel data using the double fixed effects model shows that the double fixed effects model is more effective in avoiding the overfitting problem than the single fixed effects model. The study draws the following conclusions: cybersecurity has a significant positive impact on the development of digital finance. Controlling for other factors, GDP per capita and stable web server index positively affect the development of digital finance, while mobile penetration negatively affects the development of digital finance. Meanwhile, the relationship between consumer price index and outward foreign direct investment and digital finance development is less pronounced. These findings expand our understanding of the factors influencing the development of digital finance and provide an important reference basis for relevant decision-making. Based on the above findings, the following important policy insights are provided.

(1) In the context of digital finance, the occurrence of cybersecurity incidents damages the legitimate rights and interests of the public and negatively affects the relevant companies, impedes the long-term development of the digital finance industry, and may jeopardize national security. It can be seen that the improvement of the performance of digital financial companies and the healthy development of the digital financial industry cannot be separated from the protection of cybersecurity. And to realize the protection of network security, it requires the joint efforts of all parties.

(2) For digital finance companies, first, at the institutional level, companies should establish a set of proven internal control regulations to standardize the scope of use and authority of customer information and to clarify the company's cybersecurity protection measures. At the same time, it should formulate punitive measures in the event of a cybersecurity incident. Second, at the technical level, the company should adopt systems with appropriate cybersecurity protection capabilities and personalize them according to the company's needs to address cybersecurity vulnerabilities in the system. In addition, at the supervisory level, the Company shall regularly investigate potential cybersecurity risks and deficiencies, including but not limited to systems, systems and employee operations, and disclose cybersecurity operations in a timely manner. Lastly, at the public relations level, the Company should establish a pre-plan so that it can reduce or even stop losses in a timely manner in the event of an information leakage incident, as well as appease the emotions of product users, restore investor confidence, handle public opinion appropriately, and effectively prevent the incident from expanding.

(3) As far as the government is concerned, legal protection is the basic premise for realizing cybersecurity. Attempts can be made to improve the construction of the credit collection system by including companies that cause serious cybersecurity incidents in the credit collection system and restricting their business and development, in order to deter companies from abusing citizens' information and jeopardizing national cybersecurity, so as to achieve the goal of "punishing the former and preventing the latter" and to promote the healthy development of digital finance. At the same time, attention should also be paid to the role of small and medium-sized enterprises (SMEs) in promoting the development of digital finance, and instead of adopting a "one-

Table 8
Reduced sample robustness tests.

	(1) Digital-big
network	0.520***
	(4.77)
gdp	0.052*
	(1.89)
cpi	−0.009
	(−1.26)
fdi	−0.001
	(−0.82)
internet	0.086*
	(1.83)
iphone	−0.122*
	(−1.97)
_cons	0.127
	(0.08)
R^2	0.797
N	71

Note: Values in parentheses are standard errors. "***", "**", "*" indicate that the indicator is significant at the 1 %, 5 % and 10 % levels, respectively.

Table 9
Robustness test for substitution into OLS regression.

	(1) 'OLS'
network	0.213***
	(4.10)
gdp	0.050***
	(3.84)
cpi	−0.005
	(−0.68)
fdi	0.001
	(1.03)
internet	−0.014*
	(−1.73)
iphone	0.042*
	(1.87)
_cons	0.006
	(0.04)
R^2	0.267
N	168

Note: Values in parentheses are standard errors. "***", "**", "*" indicate that the indicator is significant at the 1 %, 5 % and 10 % levels, respectively.

size-fits-all" legislative approach to overprotect cybersecurity, it is necessary to understand the difficulties faced by enterprises in the application of data and information, and to target legislation and law enforcement efforts accordingly.

CRediT authorship contribution statement

Shihui Cheng: Writing – original draft, Resources, Methodology, Formal analysis, Conceptualization. **Jing Li:** Software, Data curation. **Lai Luo:** Supervision, Investigation. **Yumin Zhu:** Supervision, Investigation.

Declaration of competing interest

This study is the result of a collaborative team effort, with all authors making significant contributions to the study design, data collection, analysis, and paper writing.

Author Shihui Cheng played a key role in the overall study design, data collection and analysis, as well as undertaking the main

Table 10
Robustness test for substitution into fixed individuals only.

	(1) ''Fixed individuals
network	0.113***
	(4.14)
gdp	0.040***
	(3.74)
cpi	−0.001
	(−0.42)
fdi	0.003
	(1.23)
internet	−0.017*
	(−1.63)
iphone	0.052*
	(1.77)
_cons	0.002
	(0.05)
R^2	0.237
N	168

Note: Values in parentheses are standard errors. "***", "**", "*" indicate that the indicator is significant at the 1 %, 5 % and 10 % levels, respectively.

paper writing.

Author Jing Li was responsible for conducting the literature review, constructing the theoretical framework, and played an important role in the interpretation of results and discussion sessions.

Author Lai Luo was responsible for the design of the research methodology, the concrete implementation of the empirical analysis, the production of graphs and charts, and the revision of the paper.

Author Yumin Zhu was responsible for the section on interpretation and discussion of results.

All authors had thorough discussions and exchanges during the research process to ensure the rigor and credibility of the study.

Thanks are due to all the individuals and organizations that provided help and support during the research process.

Data availability

The data that has been used is confidential.

Acknowledgments

We thank all parties for their support and help in completing this study.

References

Aimin, Q., Gaofeng, Z., 2016. On the establishment and improvement of national data sovereignty system. J. Soochow Univ. (Philosophy and Social Science Edition) 37 (01), 83–88.
AlGhamdi, S., Win, K.T., Vlahu-Gjorgievska, E, 2020. Information security governance challenges and critical success factors: systematic review. Comput. Secur. 99, 102030.
Anderson, R., Moore, T, 2006. The economics of information security. Science 314 (5799), 610–613.
Bing, C., Zhen, H., 2021. Rule of law path to integrate data security and development under digital finance. Changbai J. (05), 84–93. +2.
Dengguo, F., Min, Z., Hao, L., 2014. Big data security and privacy protection. J. Comput. 37 (01), 246–258.
Dong, Y., 2018. Regulatory technology: regulatory challenges and dimensional construction of fintech. China Soc. Sci. (5), 69–91.
Guokai, F., 2021. The importance and practical path of personal information protection in the context of digital finance. J. Changjiang Normal Univ. 37 (06), 102–107.
Haizhang, Q., Yunqing, T., Songwei, C., et al., 2020. Theoretical and empirical evidence on digital financial development and economic growth in China. Res. Quant. Tech. Econ. 37 (06), 26–46.
Hao, Huang, 2018. Formation and challenges of digital financial ecosystem - experience from China. Economist (04), 80–85.
Hui, Q., Dandan, J., Qian, W., 2021. Digital finance, resource allocation efficiency and financial services. Wuhan Finance (11), 61–70.
Jianbo, Z., Danhui, Y., 2019. Accelerating the innovation and standardized development of digital finance. J. Beijing Inst. Technol. (Social Science Edition) 19 (06), 71–79.
Jing, Y., Taixuan, W., 2020. Public law protection of personal information in the era of digital finance–an overview of the coupling of public and private law protection. J. Theory (03), 86–92.
License, 2019. Anniversary review and reflection on the EU general data protection regulation. Electronic Intellectual Property (06), 4–15.
Mei, X.-Y.. Private law limitations and public order construction of data protection between sharing and control. Chinese and Foreign Law, 2019, 31(04):845–870.
Na, W., Binxing, F., Jianzhong, L., Yong, L., 2004. "5432 strategy": a study on the framework of national information security guarantee system. J. Commun. (07), 1–9.
Norbekov, J, 2020. Ensuring information security as an ideological problem. Mental Enlightenment Sci.-Methodol. J. 2020 (1), 56–65.
Ozili, P.K., 2017. Bank profitability and capital regulation: evidence from listed and non-listed banks in Africa. J. Afr. Bus. 18, 143–168.

Qingxin, L., Kai, D., 2017. Development trend and counter measures of digital economy in sharing era. J. Theory (06), 55–61.
Shen, Satellite, 2020. On the right to data usufruct. China Social Sci. (11), 110–131. +207.
Song, T., Xuchuan, W., Jia, Z., 2020. Digital finance and corporate technological innovation - structural characteristics, mechanism identification and effect differences under financial regulation. Manage. World 36 (05), 52–66. +9.
Tian, G., Li, B., Cheng, Y., 2022. Does digital transformation matter for corporate risk-taking? Financ. Res. Lett. 49, 103107.
Wang, A., Han, R., 2023. Can digital transformation prohibit corporate fraud? Empirical evidence from China. Appl. Econ. Lett.
Wang, N., et al., 2023. How digital platform capabilities improve sustainable innovation performance of firms: the mediating role of open innovation. J. Bus. Res. 167, 114080.
W Wenchao, S. Haiming, Z. Huafeng. Ruminations on national information security in the era of big data. National Defense Science and Technology, 2013,34(02):1–5.
Xu, D., et al., 2024. Household green consumption: does digital inclusion matter? Int. Rev. Financ. Anal. 91, 102977.
W. Yihua, C. Xulin, Z. Xiaofeng. Research on the evolutionary game of personal information protection in the era of digital finance. Exploration of Economic Issues, 2019(12):79–88.
Yiping, Huang, Zhuo, Huang, 2018. Digital financial development in China: present and future. Economics(Quarterly) 17 (04), 1489–1502.
Yue, P., 2018. Conflict and resolution of data privacy protection under the perspective of trade regulation. Comp. Law Res. (04), 176–187.
Zhou, L., et al., 2023. Explainable artificial intelligence for digital finance and consumption upgrading. Financ. Res. Lett. 58, 104489.