Manuscript submitted to *Security and Safety*, For Peer Review Only, Vol. x, xxxxxxx (2025)
https://doi.org/10.1051/sands/xxxxxxx
sands.edpsciences.org

Review **Open Access**

Digital Finance

$\mathcal{F}$AMEπ: A Practical Full-Stack System Architecture for Empowering Secure Digital Finance

Cheng Wang[1,2,3,*], Wenjing Yang[1,2], Hao Tang[1,2], Xue Chen[1,2], and Changjun Jiang[1,2,3,*]

[1] *School of Computer Science and Technology, Tongji University, Shanghai 201804, China*
[2] *Key Laboratory of Embedded System and Service Computing, Ministry of Education, Shanghai 201804, China*
[3] *Shanghai Artificial Intelligence Laboratory, Shanghai 200030, China*

Received: xx xxxxx 2025 / Revised: xx xxxxx 2025 / Accepted: xx xxxxx 2025 / Published online: xx xxxxx 2025

Abstract The rapid advancement of digital technologies and the growing complexity of financial systems have amplified the uncertainty, heterogeneity, and interconnectedness of modern financial problems. Traditional digital finance methods, which typically focus on single scenarios, isolated user groups, or narrowly defined tasks, struggle to address today's hybrid financial environments characterized by cross-scenario demands, multi-stakeholder interactions, and tightly coupled functional and security requirements. To bridge this gap, we first propose a novel taxonomy of digital finance research encompassing five macro perspectives (Application, Model, Element, Platform Infrastructure, and Facility), providing a systematic coordinate system for positioning and analyzing existing studies. Building on this foundation, we introduce $\mathcal{F}$AMEπ, a practical full-stack system architecture designed to empower secure, scalable, and holistic digital finance. $\mathcal{F}$AMEπ co-designs and integrates diverse financial applications, a broad spectrum of models, theories of full-element aggregation optimization and trustworthy computation, and a unified intelligent computing platform. Unlike fragmented or patchwork solutions, $\mathcal{F}$AMEπ achieves cross-layer interoperability and system-level optimization, enabling resilient, robust, and inherently secure digital finance across all major scenarios. This work thus establishes both a conceptual blueprint and an architectural path toward next-generation full-stack digital finance systems.

Keywords Secure Digital Finance, Full-Stack Architecture, Behavioral Simulation, Cabin Computing, Intelligent Computing Element

Citation Wang C, Yang WJ, Tang H, Chen X and Jiang CJ. $\mathcal{F}$AMEπ: A Practical Full-Stack System Architecture for Empowering Secure Digital Finance. Security and Safety 2025; **x**: xxxxxxx. https://doi.org/10.1051/sands/xxxxxxx

1 Introduction

Digital finance is profoundly reshaping the operation of the modern economic system, serving as a vital vehicle for financial innovation, resource allocation, and inclusive growth [1, 2]. Empowered by technologies such as big data [3], artificial intelligence [4], cloud computing [5], and blockchain [6], financial services are achieving unprecedented levels of scale, speed, and personalization [7–9]. From payment processing and credit evaluation to asset management and market microstructure analysis, digital tools not only enhance efficiency and user experience but also generate new business models and regulatory demands [10, 11]. Therefore, constructing systems that can stably and securely support these tasks holds both theoretical significance and practical importance for maintaining financial stability, strengthening market confidence, and promoting high-quality economic development [12, 13].

---

[*] Corresponding authors (email: `cwang@tongji.edu.cn (Cheng Wang); cjjiang@tongji.edu.cn (Changjun Jiang)`)

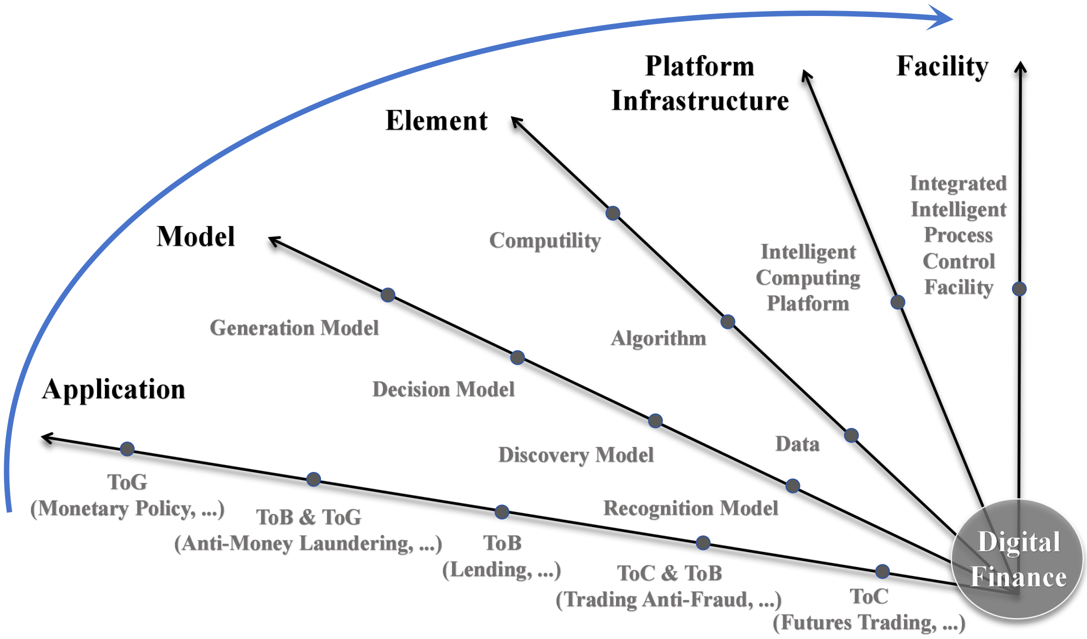


Figure 1. A Novel Taxonomy of Digital Finance Research. The novel taxonomy comprises five dimensions: Application, Model, Element, Platform Infrastructure, and Facility.

In the ecosystem of digital finance, tasks span a broad spectrum of objectives. On one hand, digital finance emphasizes functional development, namely leveraging data intelligence to enhance business efficiency and value creation. Applications such as time series forecasting for prices or risks, credit scoring for decision support, personalized recommendation, and asset pricing exemplify how data-driven models reshape financial operations and market behavior [14, 15]. On the other hand, the security and reliability of financial systems are equally critical. Advanced analytics and artificial intelligence play essential roles in ensuring robustness and regulatory compliance through mechanisms such as fraud detection, risk warning, anti-money laundering, and anomaly monitoring [16, 17]. In practice, these functional and security dimensions are deeply intertwined: Predictive and recommendation models often serve to anticipate potential defaults or liquidity threats [18], while the systems that neglect embedded security safeguards may inadvertently magnify systemic risks [19]. Therefore, security considerations inherently shape the design and deployment of digital finance functions, forming a fundamental layer beneath the apparent pursuit of efficiency and innovation [20].

Despite rapid progress in recent years, current research on digital finance tasks remains fragmented and constrained [21]. First, most existing studies focus on single financial application scenarios (such as stock prediction, credit scoring, or fraud detection) without achieving cross-scenario generalization. Second, research efforts are often oriented toward specific user groups, such as governments (prioritizing interpretability and compliance), businesses (emphasizing profitability and customer retention), or individual consumers (focusing on privacy and experience), thereby limiting interoperability across stakeholders. Third, the majority of works concentrate on single-type problems, addressing either functional or security objectives in isolation. In practice, the financial system involves heterogeneous data sources (structured tables, textual reports, behavioral logs), strong temporal dependencies, multi-party interactions, and stringent compliance requirements. These characteristics impose high demands on model robustness, scalability, privacy preservation, and adaptability [22, 23]. Fragmented approaches often fail when faced with cross-scenario, cross-user, or cross-task integration, revealing a gap between theoretical research and real-world engineering deployment [24]. To the best of our knowledge, there is currently no solution capable of establishing a full-stack system architecture to empower secure digital finance.

In this work, we first propose a novel taxonomy of digital finance research respectively from five perspectives (application, model, element, platform infrastructure and facility, as shown in Figure 1) to conduct a literature review on existing typical financial studies. The purpose of proposing this taxonomy is not to analyze the limitations of existing research or outline future directions, as other reviews

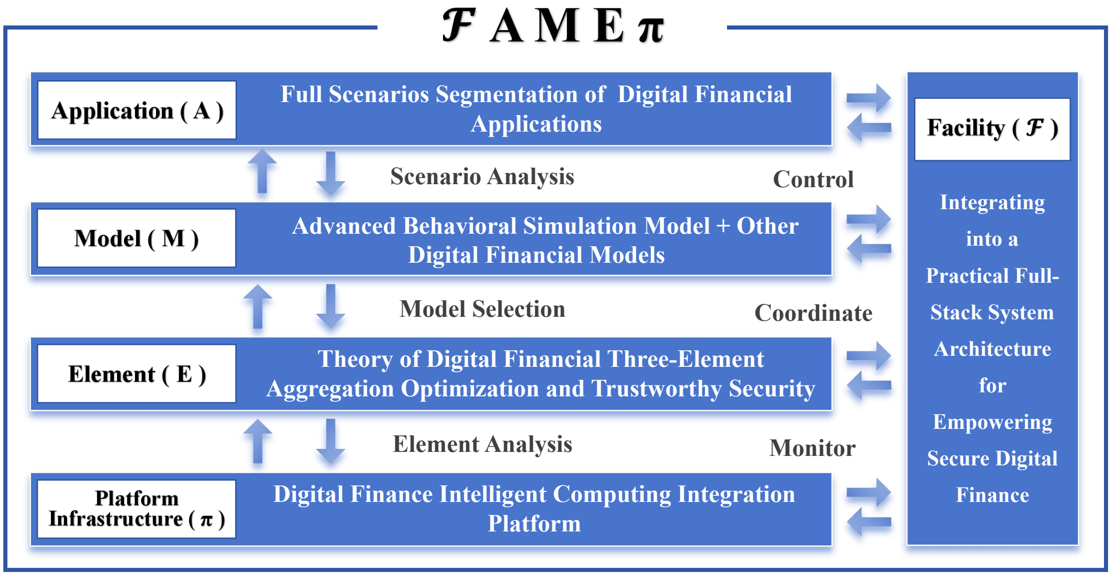


Figure 2. The Overall Structure of $\mathcal{F}$AMEπ. $\mathcal{F}$AMEπ consists of five modules: A (Application), M (Model), E (Element), π (Platform Infrastructure), and $\mathcal{F}$ (Facility).

have done, but rather to conduct essential research on how to construct a system architecture capable of empowering secure digital finance. This classification approach is based on the perspectives of architectural modules and system processes, providing complete insights into the essential modules required for exploring a digital finance system architecture. On this basis, we then propose **$\mathcal{F}$AMEπ**, a practical full-stack system architecture for empowering secure digital finance. $\mathcal{F}$AMEπ draws inspiration from the above taxonomy to guide its construction. The overall structure of $\mathcal{F}$AMEπ is presented in a “4+1” architecture, comprising a total of five parts. The “4” refers to four components arranged from top to bottom: **A (Application)**, **M (Model)**, **E (Element)**, and **π (Platform Infrastructure, PI)**. The “1” denotes the single component **$\mathcal{F}$ (Facility)**. Each module contributes unique capabilities: Module A categorizes digital finance applications across full scenarios from the perspective of digital finance business modes, providing user requirement analysis capabilities for $\mathcal{F}$AMEπ. Module M integrates numerous digital finance models, including our Advanced Behavioral Simulation Model, to deliver suitable functional models for addressing user needs. Module E proposes the theory of full-element aggregation optimization and trustworthy security based on the three elements of intelligent computing, providing theoretical support for $\mathcal{F}$AMEπ’s efficient and secure resolution of user problems. Module π denotes the digital finance intelligent computing platform infrastructure. It leverages financial cabin computing [25, 26] technology to deliver foundational services for $\mathcal{F}$AMEπ’s secure and intelligent resource allocation. Module $\mathcal{F}$, as the system architecture entity, integrates the above four modules and coordinates their operation as a cohesive, functional whole. The overall structure of $\mathcal{F}$AMEπ is shown in Figure 2.

Crucially, $\mathcal{F}$AMEπ is not merely an assembly of innovative components. It is a co-designed full-stack architecture, where internal dependencies between modules are intentionally constructed to support unified, cross-layer optimization. Module A drives the understanding of user needs, determining the types of models required from Module M. Module M interacts with Module E to ensure that modeling processes adhere to trustworthy, full-element optimization principles. Module E guides Module π in orchestrating secure and dynamic resource allocation. Module $\mathcal{F}$, the core execution facility, completes the loop by coordinating interactions across all modules. This interdependent structure distinguishes $\mathcal{F}$AMEπ from prior patchwork systems, where researchers combine the best available model, the most suitable feature engineering pipeline, and an independent computing backend. In such systems, local optimality does not translate to global optimality, because digital finance requires coherent optimization across layers rather than isolated module excellence.

The value of a full-stack architecture becomes clear: It enables system-level intelligence, where the interactions among applications, models, theoretical elements, and platform infrastructure are optimized jointly. Constructing such an architecture is difficult due to the need to unify heterogeneous objectives, reconcile conflicting requirements, and ensure interoperability under strict security and regulatory constraints. Yet this is precisely the advantage $\mathcal{F}$AMEπ offers. In brief, **$\mathcal{F}$AMEπ transforms digital finance research from single-point optimization to whole-system intelligence, providing a principled and extensible full-stack architecture where every module is co-designed for both functional performance and inherent security**.

Beyond its architectural benefits, $\mathcal{F}$AMEπ also provides a standardized coordinate system for future digital finance research. Because each scholarly contribution naturally maps to one or more modules of the architecture, researchers can precisely locate their work within the broader ecosystem, identify cross-module dependencies, and uncover opportunities for integrated optimization. $\mathcal{F}$AMEπ thereby serves not only as a system design but also as a conceptual foundation and methodological benchmark for the next generation of secure, scalable, and intelligent digital finance systems.

The main contributions of this work are as follows:

- For existing research on digital finance, we propose a novel taxonomy of digital finance research. It reviews the literature from the perspectives of application, model, element, platform infrastructure, and facility. This novel taxonomy can cover all research in digital finance and provide a coordinate for each study, facilitating a comprehensive review of the research.
- Based on the taxonomy, we introduce $\mathcal{F}$AMEπ, a practical full-stack system architecture designed to empower secure digital finance. Unlike patchwork solutions, $\mathcal{F}$AMEπ is a co-designed architecture in which internal modules are intentionally interconnected to support cross-layer collaboration and system-level optimization. It delivers a global optimal solution addressing diverse user needs across all financial application scenarios.
- We have made innovative contributions across all dimensions of $\mathcal{F}$AMEπ. For Module A, we introduce five typical financial application scenarios based on three business modes (ToC, ToB, and ToG). For Module M, we propose the Advanced Behavioral Simulation Model. For Module E, we introduce the theory of full-element aggregation optimization and trustworthy security. For Module π, we establish the digital finance intelligent computing integration platform. For Module $\mathcal{F}$, we define the four essential functions it must possess.

2 A Novel Taxonomy of Digital Finance Research

Most existing surveys on digital finance aim to summarize the current state of research on existing technologies and propose potential future development directions [27, 28]. However, none have been conducted from the perspective of critical system modules and the entire process to construct a system architecture capable of providing full-stack services for digital finance. To fill this research gap, we propose a novel taxonomy of digital finance research, comprising five dimensions: application, model, element, platform infrastructure, and facility (as shown in Figure 1). The dimension of application delineates the application scenarios of the research, categorizing digital finance applications into five distinct segments: **ToC**, **ToC & ToB**, **ToB**, **ToB & ToG**, and **ToG**. The dimension of model indicates the functional aspects of the model under research, including **Recognition Model**, **Discovery Model**, **Decision Model**, and **Generation Model**. The dimension of element specifically refers to the three core elements of intelligent computing in the computer science field: **Data**, **Algorithm**, and **Computility** [29]. The dimension of platform infrastructure reflects whether a study constructs a digital finance **intelligent computing platform** from the perspective of platform infrastructure. The dimension of facility reflects whether a study has been constructed as a full-stack system architecture by an **integrated intelligent process control facility**. Each digital finance research will have a value on each dimension of this taxonomy, indicating the point studied by the research from the corresponding perspective. This novel taxonomy offers a comprehensive and complete perspective for examining digital finance research, providing valuable support for constructing full-stack digital finance system architectures.

Next, we will separately take each dimension as the main index to conduct a literature review on existing research of digital finance. (Since there is no research on the dimension of facility, it will not be included in the review.) After the literature review of each dimension, we will present the values of the research on this dimension in other dimensions, so as to comprehensively and completely locate the content of the research (as shown in Table 1, 2, 3, and 4).

2.1 Digital Finance Application

Digital finance application delineates the application scenario targeted by a digital finance research. In the financial services system, business modes are generally classified into three categories according to the characteristics of their target clients: **ToC (To Consumer)**, **ToB (To Business)**, and **ToG (To Government)**. The ToC mode emphasizes the financial needs of individual users, such as investment, payments, and wealth management, and is characterized by high transaction frequency, large user scale, and a strong dependence on user experience and security. By contrast, the ToB mode primarily addresses enterprises, encompassing financing, risk management, and cash flow operations, with a focus on stability, scalability, and regulatory compliance. The ToG mode serves governments and regulatory agencies, concentrating on macroeconomic governance, policy analysis, and financial supervision, with strong regulatory attributes and a public-interest orientation. These three modes reflect the stratification and differentiation of financial service targets and provide the theoretical foundation for categorizing typical financial application scenarios.

Within this framework, we primarily introduce five representative digital finance applications: ToC, ToC & ToB, ToB, ToB & ToG, and ToG. These correspond to five typical application scenarios: Futures Trading, Trading Anti-Fraud, Lending, Anti-Money Laundering, and Monetary Policy (as illustrated in Figure 3). First, futures trading primarily targets individual investors, whose core demands lie in transaction transparency and timeliness, thereby corresponding to the ToC mode. Second, fraud detection in trading systems simultaneously involves the protection of personal users' account security and the prevention of risks in enterprise-level trading systems, thus representing an intersection of ToC and ToB. Third, lending focuses predominantly on enterprises, with large-scale financing needs and stringent compliance requirements, making it a typical ToB application. Fourth, AML embodies both the compliance obligations of financial institutions and the enforcement responsibilities of government regulators, and thus spans both ToB and ToG. Finally, monetary policy serves exclusively governmental actors, aiming to support macroeconomic management and policy adjustments, and is therefore a representative ToG application. Viewed through the lens of service-object classification, this typology not only clarifies the functional positioning and regulatory logic of different financial applications but also provides a structured analytical framework for subsequent systematic research.

2.1.1 Futures Trading

Futures trading enables investors to profit from predicting asset price fluctuations through standardized contracts [30]. Featuring high-frequency trading, strong leverage, and heavy data dependence, it offers high potential returns but also substantial risks, placing stringent demands on system performance, data analytics, and risk management [31]. In practice, futures trading scenarios face multiple challenges. First, fraudulent behaviors such as false orders and illegal flow of funds threaten the fairness of trading [32]. Second, market manipulation risks disrupt the market order through coordinated trading or abnormal price fluctuations [33]. In addition, the lack of risk awareness of individual investors may lead to blind operations, and trading platforms need to help users improve their capabilities through simulated trading tools. Meanwhile, the technical requirements of high-frequency trading have raised higher standards for system reliability and low-latency performance.

To cope with these challenges, futures trading scenarios can enhance efficiency and security through a variety of technological means. Li *et al.* [34] proposed a prediction framework that extracts internal factors and patterns in the gold futures market movements, decomposes their correlations with external markets and detects changes in market conditions to accurately predict the price movements in the gold futures market. Gong *et al.* [35] conducted a study on the dynamic volatility spillover among four major energy commodities-crude oil, gasoline, heating oil and natural gas-in futures markets. The results of the study are of great significance for practical issues such as hedging, portfolio optimization and risk management. Gu *et al.* [36] proposed a hybrid method in order to improve the accuracy of futures price prediction and applied it to predict the London Metal Exchange (LME) nickel settlement price. The experimental results show that the proposed method is a useful algorithm for predicting the settlement price of LME nickel. Liu *et al.* [37] examined the impact of economic policy uncertainty (EPU) on the price volatility of carbon futures in the EU and whether it has the ability to predict the price volatility of carbon futures. Deng *et al.* [38] proposed a price direction fused forecasting and trading method for high-frequency forecasting of Chinese crude oil futures. In addition, Liu *et al.* [39] and Du *et al.* [40] explored

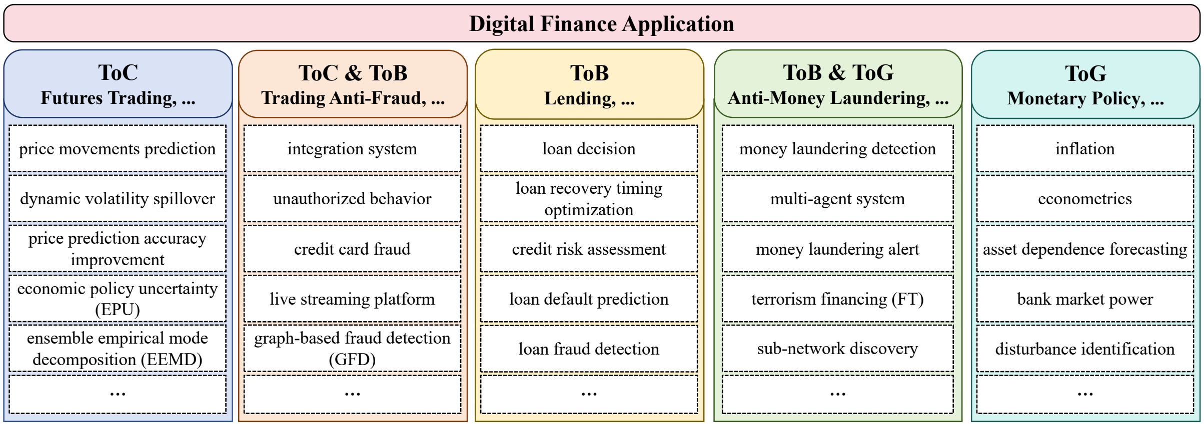


Figure 3. Digital Finance Application. Digital finance applications can be categorized into five types based on their business modes: ToC, ToC & ToB, ToB, ToB & ToG, and ToG. These correspond to five typical application scenarios: futures trading, trading anti-fraud, lending, anti-money laundering, and monetary policy.

futures trading strategies from the theoretical point of view, Huang *et al.* [41] analyzed EU futures trading from a data point of view, Liwang *et al.* [42] studied the futures resource trading mechanism from the point of view of arithmetic resources, and Xu *et al.* [43] investigated whether the ensemble empirical mode decomposition (EEMD) can really improve the prediction of crude oil futures prices from both theoretical and experimental perspectives. A similar financial scenario to futures trading is equities, where Duan *et al.* [44] studied the asset pricing problem in the stock market. Yang *et al.* [45] studied stock forecasting from the perspective of digital data.

Based on the above and Table 1, the research on futures trading (Application=1) prediction has increasingly focused on capturing complex market dynamics through algorithm-driven (Element=2) approaches, mainly relying on discovery and decision models (Model=2, 3). Current studies reveal a trend toward integrating internal and external market factors, enhancing volatility modeling, and combining multiple predictive techniques (matching multi-model application) to improve forecasting accuracy. Notably, these studies lack support from intelligent computing platforms (Platform Infrastructure=0) and full-stack system architectures (Facility=0); the analytical scope has expanded from price prediction to include risk management, resource allocation, and strategy optimization, aligned with decision model application. Looking ahead, futures trading is expected to evolve toward more intelligent systems that leverage multi-source data while also needing to supplement infrastructure support. This will enhance prediction precision and strengthen market resilience in a digital financial ecosystem.

2.1.2 Trading Anti-Fraud

Trading anti-fraud aims to safeguard the security and stability of the trading system, and prevent the loss of funds and system risks caused by fraud [46]. In this scenario, the financial trading system often involves a large number of high-frequency and high amount of money flow, fraud may be manifested in the form of false trading, account hijacking, programmed manipulation of market prices, abnormal fund flows and other forms [47]. These fraudulent behaviors will not only directly threaten the safety of user funds, but may also disrupt market order, bringing compliance risks and reputational loss to financial institutions [48].

The core of the trading anti-fraud is to use technical means to identify, prevent and control abnormal trading behaviors in real time. Wang *et al.* [49] pointed out that integrating appropriate functional modules in data-driven online payment anti-fraud engineering is an effective way to further improve the detection performance and overcome the shortcomings of a single-function approach that is unable to cope with complex and diverse fraud behaviors. However, it is difficult to realize a qualified integration under several demanding requirements such as improving detection performance, ensuring decision interpretability, and limiting processing latency and computational consumption. For this reason they proposed that a qualified integration system can fulfill all the above requirements at the same time. It is often taken for granted that the occurrence of unauthorized actions is a necessary condition for

Table 1. Research on Digital Finance Application

Research	**Application**[a]	**Model**[b]	**Element**[c]	**Platform Infrastructure**[d]	**Facility**[e]
Li *et al.* 2021 [34], Gu *et al.* 2021 [36], Deng *et al.* 2023 [38], Liu *et al.* 2020 [39], Huang *et al.* 2022 [41], Duan *et al.* 2022 [44]	**1**	3	2	0	0
Gong *et al.* 2021 [35], Liu *et al.* 2021 [37], Du *et al.* 2020 [40], Xu *et al.* 2022 [43]	**1**	2	2	0	0
Liwang *et al.* 2021 [42]	**1**	3	3	0	0
Yang *et al.* 2022 [45]	**1**	1	1	0	0
Wang *et al.* 2022 [49]	**2**	3	3	1	0
Wang 2021 [50], Lai *et al.* 2023 [51], Hu *et al.* 2023 [52], Li *et al.* 2021 [53], Liu *et al.* 2021 [54], Zheng *et al.* 2021 [55], Cheng *et al.* 2020 [56], Xiang *et al.* 2023 [57], Xu *et al.* 2024 [58]	**2**	1	2	0	0
Cheng *et al.* 2020 [59]	**2**	1	2	1	0
Abi *et al.* 2021 [60]	**2**	1	3	1	0
Chen *et al.* 2022 [61], Botha *et al.* 2021 [62]	**3**	3	2	0	0
Song *et al.* 2020 [63], Song *et al.* 2023 [64], Xu *et al.* 2021 [65], Błaszczyński *et al.* 2021 [66], Lu *et al.* 2024 [67]	**3**	1	2	0	0
Yang *et al.* 2023 [68], Cheng *et al.* 2023 [69], Jensen *et al.* 2023 [70], Segovia *et al.* 2021 [71], Li *et al.* 2020 [72], Song *et al.* 2024 [73], Du *et al.* 2022 [74]	**4**	1	2	0	0
Alexandre *et al.* 2023 [75]	**4**	1	2	1	0
Chai *et al.* 2023 [76]	**4**	2	2	0	0
Altman *et al.* 2024 [77]	**4**	0	1	0	0
Li *et al.* 2024 [78]	**5**	4	2	0	0
Aras *et al.* 2022 [79], Miranda *et al.* 2021 [80], Gorodnichenko *et al.* 2023 [81], Jordà *et al.* 2020 [82], Wang *et al.* 2022 [83]	**5**	2	2	0	0
Zhu *et al.* 2022 [84]	**5**	1	2	0	0
Shah *et al.* 2023 [85]	**5**	0	1	0	0

[a] The Application dimension has five values ranging from 1-5. 1: ToC, 2: ToC & ToB, 3: ToB, 4: ToB & ToG, and 5: ToG.
[b] The Model dimension has four values ranging from 1-4. 1: Recognition Model, 2: Discovery Model, 3: Decision Model, and 4: Generation Model.
[c] The Element dimension has three values ranging from 1-3. 1: Data, 2: Algorithm, and 3: Computility.
[d] The Platform Infrastructure dimension has two values: 1 and 0, respectively indicating the presence or absence of an intelligent computing platform.
[e] The Facility dimension has two values: 1 and 0, respectively indicating the presence or absence of a full-stack system architecture by an integrated intelligent process control facility.

fraud detection in online payment services. However, Wang [50] sought to break this stereotype. He strove to devise an ex-ante anti-fraud approach that works before unauthorized behavior occurs. Credit card fraud is a significant problem that can impose considerable costs on cardholders and issuing banks. Contemporary approaches use machine learning based methods to detect fraud from transaction records. However, manual generation of features requires domain knowledge and may be hidden behind the modus operandi of the fraud. Cheng *et al.* [59] focused on automatically focusing on the most relevant patterns of fraudulent behaviors in an online detection system, thus proposing a spatial-temporal attention based graph network for credit card fraud detection. Lai *et al.* [51] proposed an effective framework to integrate fraudster detection into recommender systems for adversarial robustness. Hu *et al.* [52] suggested that graph-based fraud detection methods are not suitable for dealing with highly repetitive, unevenly distributed and heterogeneous Ether transactions problem, so they conducted anti-fraud research on Ether transactions based on Transformer. Li *et al.* [53] proposed that live streaming platforms which are similar to traditional online shopping platforms such as Taobao also suffer from malicious online frauds and many transactions are not genuine. They proposed an approach based on graph neural network for live commerce anti-fraud research. Liu *et al.* [54] addressed the problem of e-commerce fraudulent transaction detection by considering the user transaction behavior and transaction intent into the graph network. Zheng *et al.* [55] proposed that different banks are usually not allowed to share their transaction datasets due to data security and privacy concerns. This makes it difficult for traditional models to learn fraud patterns and detect them. They studied the problem from a federated learning perspective. Cheng *et al.* [56] pointed out that contemporary approaches apply machine learning based methods to detect fraud from transaction records. However, manual generation of features requires domain knowledge and may be hidden behind the modus operandi of the fraud. It means that we need to automatically focus on the most relevant patterns in the fraudulent behavior. They investigated the problem from the perspective of attention mechanisms. Xiang *et al.* [57] investigated how to utilize a small amount of labeled data for high quality credit card fraud detection. Xu *et al.* [58] addressed the problem of heterogeneity and label utilization in graph-based fraud detection (GFD). In addition, Abi *et al.* [60] studied the anti-fraud security problem from the perspective of system hardware and operational speed.

On the basis of the above and Table 1, recent research on trading anti-fraud (Application=2) has evolved from traditional rule-based and single-function models toward more intelligent systems, mainly relying on recognition models (Model=1). Current studies emphasize combining modules, leveraging advanced architectures, and incorporating behavioral features with a focus on algorithm-driven (Element=2) approaches to capture hidden fraud patterns. Notably, some studies now adopt intelligent computing platforms (Platform Infrastructure=1) (though all lack full-stack system architectures, Facility=0), while emerging methods like federated learning enhance generalization across heterogeneous environments. The scope has expanded from post-event detection to proactive prevention and cross-party collaboration. Looking ahead, trading anti-fraud is expected to develop unified, low-latency frameworks that integrate multi-source data and real-time learning while supplementing infrastructure support. This will balance detection performance, interpretability, and efficiency in complex digital transaction ecosystems.

2.1.3 Lending

Lending covers multiple key aspects including enterprise financing, credit management and risk control. It is widely present in commercial banks, microfinance companies, fintech platforms and other institutions [86]. As an important means for enterprises to obtain financial support, the core of lending is to realize the efficient allocation of funds, help enterprises solve their liquidity needs, and support their business expansion and development [87]. However, this scenario is also accompanied by complex credit risk, fraud risk and capital flow risk. It puts high demands on the risk control ability and technical level of lending institutions [88].

Loan decisions are usually made using proprietary models that provide users with minimally acceptable explanations. However, the economy has changed dramatically due to the epidemic and a large number of new loans are needed in the short term. What decision support tools would one want to use to make sound loan decisions in this situation? Chen *et al.* [61] proposed a framework for such decisions. In order to objectively compare and evaluate banks' decision rules in terms of optimizing the timing of loan recovery, Botha *et al.* [62] proposed a novel procedure. The procedure can better inform the quantitative aspects of a bank's collection policy rather than relying solely on arbitrary judgments. Credit risk assessment is an important task in the peer-to-peer (P2P) lending industry. In recent years, ensemble learning methods have been shown to perform better than individual classifiers and statistical techniques for default prediction. Real-world lending datasets are unbalanced. However, most research has focused on improving overall prediction accuracy rather than improving the identification of real defaulted loans. In addition, some features that are significantly correlated with default rates have not been emphasized in the model construction of previous studies. To fill these gaps, Song *et al.* [63] proposed an ensemble learning approach to predict default risk in P2P lending. Most of the existing studies on loan default prediction analyze loans with different credit ratings as a whole, ignoring the important relationship between category imbalance and specific credit rating categories. Further considering the different risk preferences of lending companies in reviewing loan applications, Song *et al.* [64] proposed a rating-specific multi-objective ensemble learning framework. Xu *et al.* [65] stated that loan fraud detection is particularly important for lenders to avoid financial losses. Previous methods focus on loan fraud detection using applicants' attributes and historical behaviors. However, the performance of these methods deteriorates when multiple people with different roles (e.g., sellers, intermediaries) conspire to apply for fraudulent loans. To address this challenge, they considered the problem of detecting loan fraud by utilizing users' roles and multiple types of social relationships among users. Błaszczyński *et al.* [66] pointed out that auto loans are an important financial product that, unlike the misuse of credit cards, has not yet been explored in the literature. Given the recent increase in fraudulent transactions regarding auto loan applications, they developed a technique that has not yet been explored for financial fraud prediction to conduct a study of fraudulent auto loan application transactions. Lu *et al.* [67] suggested that Small and Medium-sized Enterprises (SMEs) in interconnected internet lending are vulnerable to chain debt crises, and they investigated this issue based on the financial shock factors triggered by social media.

In view of the above and Table 1, recent research on lending (Application=3) decision-making and risk management has increasingly focused on enhancing accuracy, relying on recognition models and decision models (Model=1,3). Traditional proprietary models are being replaced by algorithm-driven approaches (Element=2) that better capture complex borrower behaviors and risk preferences. Notably, these studies lack intelligent computing platforms (Platform Infrastructure=0) and full-stack system architectures (Facility=0). Advances in multi-objective optimization have expanded the analytical scope from individual borrower assessment to interconnected financial ecosystems, while simulation-based evaluation has improved the rigor of lending and recovery strategies. Looking ahead, lending is expected to move toward holistic, real-time decision frameworks that integrate algorithmic insights while supplementing infrastructure support. This will enable financial institutions to make sound, fair, and resilient lending decisions amid economic uncertainty and evolving credit environments.

2.1.4 Anti-Money Laundering

Anti-Money Laundering (AML) aims at identifying, preventing and combating illegal money flow activities through the financial system [89]. Money laundering usually involves the process of concealing the source of funds, disguising the nature of transactions and converting illegal proceeds into legal assets. It not only threatens the stability of the financial system, but also provides financial support for criminal activities [90]. Therefore, AML has become a key area of concern for financial institutions and government regulators.

The introduction of technological tools has led to the gradual intelligence and automation of AML scenarios. As global AML protocols and technologies are strengthened, traditional money laundering methods face increasing scrutiny. At the same time, the attractiveness of virtual currencies for money laundering has increased due to their freedom from seizure, difficulty in tracking and seamless cross-border transactions. This requires the design of specialized AML strategies for virtual currencies. To this end, Yang *et al.* [68] introduced a groundbreaking two-tier algorithm designed to enable risk-based detection of virtual currency money laundering. In recent years, more and more money laundering activities are carried out by organized criminal groups, while most existing studies still consider the behavior of each account as an independent identity behavior without considering the group-level conspiratorial interactions. Therefore, Cheng *et al.* [69] proposed an organized money laundering detection method. Complex legislation, coupled with an increase in the volume of financial transactions involved in money laundering schemes, has led to research into improving and automating the key processes for detecting, signaling and communicating suspicious customers. AML activities are strongly influenced by and dependent on this process. It has been slow to evolve, partly due to its subjectivity and complexity. Alexandre *et al.* [75] integrated machine learning and risk-based strategies into AML, building a multi-agent system for the study. For money laundering alerts, traditional systems may exhibit very high false alarm rates and waste resources. In order to qualify and issue AML alerts for banks, Jensen *et al.* [70] proposed a deep learning approach that replaces predefined rules with potential features automatically extracted from transaction sequences. Segovia-Vargas [71] proposed an integrated model to help improve customer self-comparisons and group comparisons to detect suspicious transactions related to money laundering and terrorism financing (FT) in the financial system. Li *et al.* [72] pointed out that for the problem of money laundering detection, existing graph fraud detection methods focus on dense subgraph detection and do not take into account the fact that money laundering involves a large amount of money flow through a chain of bank accounts. It reduces the detection accuracy. Therefore, they suggested using multipartite graphs to model transactions. Chai *et al.* [76] pointed out that existing rule-based money laundering sub-network discovery methods rely heavily on domain knowledge and may lag behind the modus operandi of money launderers. Therefore, they firstly used neural network based approach to solve the money laundering sub-network discovery problem. Song *et al.* [73] studied the AML problem of blockchain based on the account graph perspective. Du *et al.* [74] investigated the malicious transaction problem from the perspective of combining federated learning and graph neural networks. In addition, Altman *et al.* [77] created a new set of AML datasets from a data perspective.

From the above and Table 1, the research on AML (Application=4) has evolved toward more intelligent, algorithm-driven methodologies, mainly relying on recognition models (Model=1). To address complex financial crimes such as virtual currency laundering, recent studies emphasize risk-based detection and adaptive learning. These approaches are centered on algorithms (Element=2) and supplemented by data (Element=1) to uncover hidden patterns in heterogeneous datasets. Machine learning and graph analysis are integrated to enhance precision, while most studies lack intelligent computing platforms (Platform Infrastructure=0, with only 1 case recording a value of 1) and all lack full-stack system architectures (Facility=0). Advances in automation are transforming AML from rule-based compliance to proactive systems. Looking forward, AML research is expected to move toward unified frameworks that combine explainable AI and cross-platform fusion, helping regulators combat sophisticated schemes in decentralized financial ecosystems.

2.1.5 Monetary Policy

As an important tool of national macroeconomic management, monetary policy mainly influences economic activities and inflation by regulating money supply, interest rate level and credit scale, thus realizing the goals of economic growth, price stability and full employment [91]. Monetary policy analysis is designed to provide science-based decision support for governments and central banks, thereby safeguarding economic stability and ensuring the healthy operation of financial systems [92]. The construction of models is an important part of monetary policy analysis. Commonly used economic models include dynamic stochastic general equilibrium (DSGE) model [93], vector autoregressive (VAR) model [94], etc. These models can simulate the dynamic relationship between different variables in the economic system. Meanwhile, machine learning algorithms and reinforcement learning techniques have been introduced into monetary policy analysis for uncovering complex nonlinear relationships and optimal decisions in dynamic environments.

For the inflation problem, Li *et al.* [78] investigated it using agent-based modeling (ABM) approach, while Aras *et al.* [79] used machine learning models to forecast inflation. Commonly used tools for identifying monetary policy disturbances are likely to combine real policy shocks with information about the state of the economy as reflected in the information disclosed through policy actions. Miranda-Agrippino *et al.* [80] showed that such signaling effects of monetary policy may lead to empirical difficulties reported in the literature. For this reason, they proposed a new instrument for high-frequency monetary policy shocks that takes into account information rigidity. Gorodnichenko *et al.* [81], after conducting experiments using a deep learning model, found that a positive tone in the Fed Chairman's voice leads to a significant increase in stock prices after controlling for sentiment in the Fed's actions and policy texts. Other financial variables also respond to the chairman's voice cues. Thus, the way a policy message is communicated can influence financial markets. Zhu *et al.* [84] stated that financial assets exhibit a dependence structure, i.e., movements in their prices or returns exhibit a variety of correlations. Understanding asset price dependence can help investors create diversified portfolios aimed at reducing portfolio risk due to high volatility in financial markets. Therefore, they conducted a study for asset dependence forecasting. Monetary policy statements by the Federal Open Market Committee (FOMC) are a major driver of financial market returns. For this reason, Shah *et al.* [85] constructed the largest tokenized and annotated dataset of FOMC speeches, minutes, and press conference transcripts to understand how monetary policy

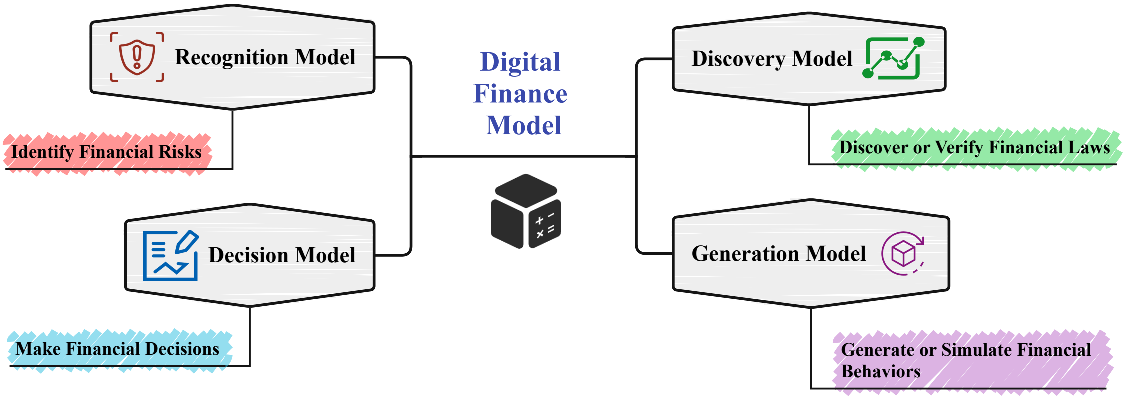


Figure 4. Digital Finance Model. Digital finance models can be classified into four types: recognition model, discovery model, decision model, and generation model.

affects financial markets. In addition, Jordà *et al.* [82] studied monetary shocks from an econometric perspective. Wang *et al.* [83] estimated a dynamic banking model that quantifies the impact of bank market power on the transmission of monetary policy through banks to borrowers.

In light of the above and Table 1, the research on monetary policy (Application=5) analysis has progressively integrated data-driven and econometric approaches, with discovery models (Model=2) being the most widely adopted, while recognition models (Model=1) and generation models (Model=4) are less common. Traditional econometric models are complemented by agent-based simulations and machine learning, where algorithms (Element=2) serve as the core in most cases, with data (Element=1) used only in a small share of works. All relevant research lacks both intelligent computing platforms (Platform Infrastructure=0) and full-stack system architectures (Facility=0). Recent studies highlight that central bank communication tone shapes market expectations, and network analysis deepens insights into systemic risk under policy shocks. Looking ahead, monetary policy analysis is expected to move toward explainable, multi-modal frameworks integrating textual and quantitative signals, enhancing policy evaluation precision amid global financial complexity.

2.2 Digital Finance Model

Digital finance model specifies the function of the model developed by digital finance research. For the research on models oriented to the digital finance domain, we categorize the existing digital finance models into **Recognition Model**, **Discovery Model**, **Decision Model**, and **Generation Model** (as shown in Figure 4).

2.2.1 Recognition Model

In the field of digital finance, the function of recognition models is to recognize financial risks. Ye *et al.* [95] pointed out that earnings conference calls are the most significant factor affecting financial risk (volatility of stock returns over a certain period of time). Previous work mainly focuses on word-level or document-level feature extraction, and the structure of alternate conversations of the conference is neglected. To this end, they proposed a multi-round Q&A attention network. It extracts each round of dialog features and combines the multi-round features to predict financial volatility through Reinforced Sentence Selector (RSS) and Reinforced Bidirectional Attention Network (RBAN). Sun *et al.* [96] investigated how to efficiently construct dynamic financial distress prediction models based on category-imbalanced data streams. They proposed two category-imbalanced dynamic financial distress prediction methods based on synthetic minority oversampling technique (SMOTE) and the Adaboost support vector machine ensemble integrated with time weighting (ADASVM-TW). Experiments show that both models greatly improve the identification of minority financial distress samples. Previous studies have shown that textual information in a company's financial statements can be used to predict the risk level of its stock. For this reason, Qin *et* *al.* [97] developed a multimodal deep regression model (MDRM). The model focuses on the multimodal semantic analysis of the content of earnings calls to predict the risk of future stock price volatility of the company concerned. Lu *et al.* [67] developed a lending risk assessment model named RisQNet in order to combat the debt crisis problem in financial networks. The model uses a time graph network to integrate various cascading risks, including real-time media influences, and social network sentiment content. Wang *et al.* [98] proposed that earnings conference calls summarize the financial performance of the company and are an important indicator of the company's future financial risk. For this purpose, they proposed the copula statistical model. The model quantitatively investigates the relationship between earnings conference calls and financial risk. Chen *et al.* [99] proposed the FA-PSO-LSTM neural network deep learning model based on factor analysis (FA), particle swarm optimization (PSO), and long short-term memory (LSTM) neural network. The model is able to dynamically predict the financial risk of e-commerce companies.

To sum up, as shown in Table 2, the research on financial risk recognition (Model=1) applies to scenarios like futures trading, trading anti-fraud, and lending (Application=1-3). It has primarily focused on leveraging multi-source data, with algorithms (Element=2) as the core support, while exhibiting methodological trends in multimodal fusion, dynamic modeling, and handling class imbalance. Overall, the field is evolving toward a more comprehensive and multi-level approach. In terms of data, the focus has shifted from single financial indicators to integrating multimodal sources for holistic risk feature representation. In feature utilization, structured information like financial network relationships gains increasing attention. In modeling, deep learning integration with optimization algorithms enhances predictive accuracy and stability. All these studies lack both intelligent computing platforms (Platform Infrastructure=0) and full-stack system architectures (Facility=0). In terms of value orientation, efforts balance predictive performance with risk factor interpretation, enhancing applicability in real-world financial scenarios.

2.2.2 Discovery Model

In the field of digital finance, the function of discovery models is to discover or verify financial laws. Park *et al.* [100] proposed a machine learning model based on bubble analysis for the Bitcoin market crash problem. Through experiments, it is found that factors such as rising interest rates and bubble persistence greatly increase the probability of future crashes in the Bitcoin market. Bubble phenomena lasting longer than 14 days significantly increase the probability of a crash. This proves the rule that herd behavior and price crashes in the bitcoin market are highly correlated. Ozgur *et al.* [103] used the Generalized Supremum Augmented Dickey-Fuller (GSADF) test and the machine learning method of random forest to investigate the factors influencing the formation of price bubbles in precious and industrial metals. It was found that monetary policy rates and production indices are important in predicting industrial metal price bubbles and that speculative activities may not adequately predict metal price bubbles. Lee *et al.* [101] designed the fuzzy candlestick patterns to model the market based on the Japanese candlestick theory. This modeling can be viewed as an expert knowledge model derived from the summary of existing market knowledge. Through this model, past market patterns can be represented to summarize investment decision patterns. Chauhan *et al.* [104] used a multiple regression model based on firm characteristics and model changes, and a two-stage least-square (2SLS) type procedure to estimate the effect of leverage changes on stock returns. Claassen *et al.* [105] proposed a continuous time stochastic Ramsey model. The model is capable of generating a variety of established patterns of stock returns in both time series and cross sections. Using the model, it is possible to discover how traditional securities market lines should incorporate changes in stock premiums and time-varying beta coefficients. In addition, Lux *et al.* [102] described a multi-agent model of financial markets that supports the idea that scaling stems from participant interactions. They investigated the scaling laws in financial markets.

All in all, as shown in Table 2, discovery model research (Model=2) in the financial domain applies to scenarios like futures trading, lending, and monetary policy (Application=1,3,5). It primarily focuses on leveraging statistical analysis, machine learning and other methods, with algorithms (Element=2) as core support, to extract underlying financial patterns from vast, multi-source data. These models aim to transform market behavior, macro variables and other elements into interpretable patterns, uncovering driving factors behind price formation, risk accumulation and other phenomena. Current research shows a trend toward diversification and integration: methodologically, it shifts from single statistical models to

Table 2. Research on Digital Finance Model

Research	**Application**[a]	**Model**[b]	**Element**[c]	**Platform Infrastructure**[d]	**Facility**[e]
Ye *et al.* 2020 [95]	2	**1**	2	0	0
Sun *et al.* 2020 [96], Lu *et al.* 2024 [67], Wang *et al.* 2014 [98], Chen *et al.* 2023 [99]	3	**1**	2	0	0
Qin *et al.* 2019 [97]	1	**1**	2	0	0
Park *et al.* 2024 [100], Lee *et al.* 2006 [101], Lux *et al.* 1999 [102]	1	**2**	2	0	0
Ozgur *et al.* 2021 [103]	5	**2**	2	0	0
Chauhan *et al.* 2024 [104], Claassen *et al.* 2023 [105]	3	**2**	2	0	0
Sawhney *et al.* 2021 [106], Gan *et al.* 2023 [107]	1	**3**	2	0	0
Ye *et al.* 2020 [108], Liang *et al.* 2020 [109]	2	**3**	2	0	0
Li *et al.* 2023 [110]	2	**3**	2	1	0
Rivera *et al.* 2021 [111]	3	**3**	2	0	0
Yu *et al.* 2025 [112], Amrouni *et al.* 2021 [113], Shavandi *et al.* 2022 [114], Huang *et al.* 2024 [115]	1	**4**	2	0	0
Li *et al.* 2024 [78], Wang *et al.* 2023 [116], Nokhiz *et al.* 2024 [117]	5	**4**	2	0	0

[a] The Application dimension has five values ranging from 1-5. 1: ToC, 2: ToC & ToB, 3: ToB, 4: ToB & ToG, and 5: ToG.
[b] The Model dimension has four values ranging from 1-4. 1: Recognition Model, 2: Discovery Model, 3: Decision Model, and 4: Generation Model.
[c] The Element dimension has three values ranging from 1-3. 1: Data, 2: Algorithm, and 3: Computility.
[d] The Platform Infrastructure dimension has two values: 1 and 0, respectively indicating the presence or absence of an intelligent computing platform.
[e] The Facility dimension has two values: 1 and 0, respectively indicating the presence or absence of a full-stack system architecture by an integrated intelligent process control facility.

fusion approaches to improve pattern discovery accuracy; in terms of data, the scope expands to multi-modal information for comprehensive market signal capture. All these studies lack intelligent computing platforms (Platform Infrastructure=0) and full-stack system architectures (Facility=0). Moreover, there is growing emphasis on model interpretability, aligning discovered patterns with financial theory to support risk warning, strategy optimization and policy-making.

2.2.3 Decision Model

In the field of digital finance, the function of decision models is to make financial decisions. Sawhney *et al.* [106] viewed the stock selection problem as a ranking learning problem based on scale-free graphs. They proposed the Hyperbolic Stock Graph Attention Network (HyperStockGAT). The complex, scale-free nature of the relationships between stocks is modeled through hyperbolic graph learning on Riemannian manifolds. It allows for a more accurate representation of the spatial correlations between stocks. Portfolio management (PM) is a fundamental financial planning task aimed at achieving investment goals such as maximizing profit or minimizing risk. For this purpose, Ye *et al.* [108] presented SARL, a novel State-Augmented RL framework for PM. Experimental results show that SARL outperforms existing PM methods in terms of cumulative profit and risk-adjusted profit. Liang *et al.* [109] proposed a neural hierarchical multi-label text classification method, namely F-HMTC. It considers the classification of financial events as a hierarchical multi-label text classification problem and uses a tree structure to represent event classification. The method can perform hierarchical multi-label text classification more accurately, which in turn can better support event-based investment decisions. Li *et al.* [110] proposed that automated intelligent rule systems with rule learning and rule management functions are needed in order to make decision rules simpler and widely used in financial scenarios. To this end, they developed the Rule-based Decision System (RDS). It covers the entire life cycle of decision rules and provides an interactive interface that allows users to incorporate expert experience into decision rules, realizing human-computer interaction. Gan *et al.* [107] developed a novel Multi-granularity Graph Disentangled Learning framework called MGDL to efficiently perform intelligent matching of fund investment products and help people make investment decisions. Rivera-Castro *et al.* [111] presented an algorithm, CAUSALYSIS, that combines unsupervised machine learning and predictive model checking. CAUSALYSIS performs causal reasoning in environments with multiple causes, providing financial scenario planning supported by Causal Machine Learning for small and medium businesses.

In summary, as shown in Table 2, the research on financial decision models (Model=3) applies to scenarios like futures trading, trading anti-fraud, and lending (Application=1-3), with algorithms (Element=2) as core support. It primarily focuses on leveraging advanced machine learning and reinforcement learning techniques to enhance the accuracy, robustness, and interpretability of financial decisions. Methodologically, these works exhibit diverse characteristics: graph-based approaches capture complex asset relationships, hierarchical classification supports fine-grained analysis, and rule-based systems integrate expert knowledge for controllable decision-making. Most studies lack intelligent computing platforms (Platform Infrastructure=0), though one case is equipped with such a platform, and all lack full-stack system architectures (Facility=0). Overall, the trend is toward multi-modal integration and complex network modeling to capture high-dimensional correlations in financial systems, while increasingly incorporating causal reasoning and explainable AI to enhance decision reliability under uncertainty. This shift is driving financial decision-making from being primarily “prediction-driven” to becoming more “explanation- and planning-driven”.

2.2.4 Generation Model

In the field of digital finance, the function of generation models is to generate or simulate financial behaviors. Yu *et al.* [112] proposed FinCon, a LLM-based multi-agent framework. The framework uses a manager-analyst hierarchy to facilitate collaboration and monitors market risk through a two-tier risk control component. FinCon is capable of performing customized simulations of various financial tasks. Li *et al.* [78] proposed the EcoAgent based on LLMs with human-like macroeconomic simulation characteristics. EcoAgent simulated a hundred human economic system, which emerged more stable and realistic classical macroeconomic phenomena compared to traditional ABM simulations. Wang *et al.* [116] studied the behavior of economic platforms under shocks such as the COVID-19 blockade and the impact of different regulatory considerations. For this purpose, they developed a multi-agent simulation environment to model the shocks and regulatory trade-offs that may occur in a multi-period environment for platform economies. Amrouni *et al.* [113] designed ABIDES-Gym, a simulator specifically designed for multi-agent discrete event simulation. The environment is intended to be applied to financial markets, providing a simulation environment. Its simulation of daily investors is capable of generating complex interactive market behavior. Shavandi *et al.* [114] proposed a multi-agent deep reinforcement learning framework in order to generate trading behaviors using the collective intelligence of multiple agents to simulate the fractal market hypothesis. Nokhiz *et al.* [117] developed an agent-based behavioral simulation framework. The framework allows attempts to generate different strategies to mitigate financial instability and evaluate their effectiveness. Huang *et al.* [115] proposed the Multi-Agent Double Deep Q-Network (MADDQN) in order to allow agents to effectively learn profitable trading strategies from financial market data. The network allows the agents to reasonably balance the pursuit of maximizing returns with risk avoidance.

To sum up, as shown in Table 2, the research on financial generation models (Model=4) applies to scenarios like futures trading and monetary policy (Application=1, 5), with algorithms (Element=2) as core support. It primarily focuses on constructing multi-agent collaborative frameworks, employing hierarchical structures to generate and simulate complex financial behaviors. Researchers aim to replicate macroeconomic systems and market dynamics to capture realistic economic phenomena and patterns. Integration of risk control and regulatory mechanisms has become a key direction, enabling models to monitor risks while simulating policy impacts on financial behaviors. Advanced techniques like deep reinforcement learning are applied to generate agent behavior strategies, helping balance return maximization

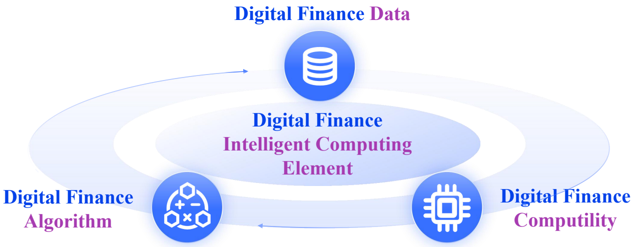


Figure 5. Digital Finance Intelligent Computing Element. Digital finance intelligent computing elements consist of three components: digital finance data, digital finance algorithm, and digital finance computility.

and risk avoidance to enhance trading strategy efficacy. All these studies lack both intelligent computing platforms (Platform Infrastructure=0) and full-stack system architectures (Facility=0).

In prospect, the development trends of financial generation models manifest in more refined multi-agent hierarchical collaboration and integration of dynamic risk regulation mechanisms. They not only enhance model realism and interaction complexity but also improve the precision of risk warning and policy simulation.

2.3 Digital Finance Intelligent Computing Element

Digital finance element specifically refers to the three elements of intelligent computing: **Data**, **Algorithm**, and **Computility**. These elements define the empowering direction of digital finance research within the computer science domain. In the field of digital finance, many researchers often tend to conduct research from the perspective of three intelligent computing elements (as shown in Figure 5).

2.3.1 Digital Finance Data

Digital finance data contains a wealth of valuable information, and how to leverage its value to empower digital finance is a key focus for researchers.

In research related to digital finance data, Kaur *et al.* [118] pointed out that many datasets for Relation Extraction (RE) fail to capture the challenges specific to the financial domain. For this reason they propose REFinD, the first large-scale annotated relational dataset. This provides a data base for the practical advancement of deep learning models in the financial world. The Chinese Financial Language Understanding Evaluation (CFLUE) benchmark proposed by Zhu *et al.* [119] provides a tailored dataset for evaluating the ability of LLM on various dimensions of finance. Considering the lack of multimodal information in previous financial datasets beyond price data, Li *et al.* [120] compiled a new, large-scale multi-modal, text-audio paired earnings-call dataset called MAEC. Chen *et al.* [121] in order to address the lack of scope diversity and question complexity in current financial question answering (QA) datasets, proposed a new dataset for financial long text QA named FinTextQA. Chen *et al.* [122] pointed out that the financial domain includes complex numerical reasoning and understanding of heterogeneous representations. To facilitate analytical progress, they proposed a new large dataset, FinQA. It contains financial reporting question-and-answer pairs written by financial experts. This dataset provides support for numerical reasoning on financial data. After that, Reddy *et al.* [123] introduced a long-document financial QA dataset named DocFinQA to compensate for the missing data problem of LLM in dealing with long financial documents. Zhao *et al.* [124] introduced a novel benchmark, FinanceMath, in order to advance future research on LLM knowledge retrieval and reasoning tasks in the financial domain. FinanceMath contains 1,200 problems with a mixture of textual and tabular content. These problems require college-level knowledge of the finance domain to be solved effectively. Lyua *et al.* [125] proposed a new methodology that combines IoT data and clustering algorithms to optimize household financial asset allocation (FAA) and develop scientific risk control strategies. The methodology utilizes IoT technology to collect real-time data, including macroeconomic indicators, market dynamics, and investor behavior. In addition, in order to facilitate conversational question answering (CQA) in hybrid contexts in the financial domain, Deng *et al.* [126] proposed a new dataset called PACIFIC. Compared to existing CQA

Table 3. Research on Digital Finance Intelligent Computing Element

Research	**Application**[a]	**Model**[b]	**Element**[c]	**Platform Infrastructure**[d]	**Facility**[e]
Kaur *et al.* 2023 [118], Zhu *et al.* 2024 [119], Chen *et al.* 2024 [121], Reddy *et al.* 2024 [123], Zhao *et al.* 2023 [124], Deng *et al.* 2022 [126]	1 2 3 4 5	0	**1**	0	0
Li *et al.* 2020 [120]	3	0	**1**	0	0
Chen *et al.* 2021 [122]	3	0	**1**	0	0
Lyua *et al.* 2024 [125]	1	3	**1**	0	0
Luo *et al.* 2024 [127]	2	1	**2**	0	0
Hou *et al.* 2025 [128], Sang 2021 [129]	3	1	**2**	0	0
Tran *et al.* 2018 [130], Blasco *et al.* 2024 [131]	1	2	**2**	0	0
Liu *et al.* 2022 [132], Yang *et al.* 2023 [133]	3	2	**2**	0	0
Ge *et al.* 2022 [134]	2	2	**2**	0	0
Nazareth *et al.* 2023 [135][*]	1 2 3 4 5	1 2 3 4	**2**	0	0
Mandal *et al.* 2024 [136]	1	3	**2**	0	0
Olorunnimbe *et al.* 2023 [137][*]	1	1 2 3 4	**2**	0	0
Tetlock 2014 [138], Monteiro *et al.* 2023 [139], Inggs *et al.* 2016 [140]	2	2	**3**	0	0
Zhu *et al.* 2023 [141]	1	1	**3**	0	0
Herman *et al.* 2023 [142][*]	1 2 3 4 5	1 2 3 4	**3**	0	0
Orús *et al.* 2019 [143][*]	1 2 3 4 5	1 2 3	**3**	0	0
Saba *et al.* 2023 [144]	2	1	**3**	0	0
Li *et al.* 2016 [145], Mann *et al.* 2022 [146]	3	3	**3**	0	0

[a] The Application dimension has five values ranging from 1-5. 1: ToC, 2: ToC & ToB, 3: ToB, 4: ToB & ToG, and 5: ToG.

[b] The Model dimension has four values ranging from 1-4. 1: Recognition Model, 2: Discovery Model, 3: Decision Model, and 4: Generation Model.

[c] The Element dimension has three values ranging from 1-3. 1: Data, 2: Algorithm, and 3: Computility.

[d] The Platform Infrastructure dimension has two values: 1 and 0, respectively indicating the presence or absence of an intelligent computing platform.

[e] The Facility dimension has two values: 1 and 0, respectively indicating the presence or absence of a full-stack system architecture by an integrated intelligent process control facility.

[*] Reference marked with an asterisk (*) indicates that the research is a review.

datasets, PACIFIC possesses three key characteristics: (i) proactivity, (ii) numerical reasoning, and (iii) hybrid context of tables and text.

All in all, as shown in Table 3, the research on digital finance data (Element=1) spans multiple application scenarios, including futures trading, trading anti-fraud, lending, anti-money laundering, and monetary policy (Application=1-5). Most of these studies use no specific model (Model=0). It primarily focuses on developing diverse, high-quality datasets to support deep learning and large model applications in finance, addressing challenges like data heterogeneity and long-document processing across tasks such as relation extraction and numerical reasoning. Some works integrate IoT data with traditional financial data to optimize risk control, while all these studies lack intelligent computing platforms (Platform Infrastructure=0) and full-stack system architectures (Facility=0). The development trend emphasizes larger, multimodal datasets and cross-modal integration, driving large models' capabilities in financial knowledge retrieval and reasoning. Future research is expected to focus more on scenario-based applications, promoting intelligent, data-driven financial analysis and decision support.

2.3.2 Digital Finance Algorithm

The purpose of digital finance algorithm is to seek a method for extracting useful value from digital finance data. This constitutes the primary focus of digital finance research.

In research related to digital finance algorithm, Luo *et al.* [127] provided a comprehensive survey of AI-driven fraud detection methods in the Decentralized Finance (DeFi) ecosystem, introducing a new taxonomy of DeFi frauds based on the project lifecycle, covering development, introduction, growth, maturity, and decay stages. The effectiveness of methods including tree-based models, graph-based approaches and statistical methods to detect fraud at each stage is evaluated. Hou *et al.* [128] suggested that previous studies have applied a series of machine learning algorithms to predict the credit risk of SMEs in supply chain finance. However, these methods are deficient in terms of prediction efficiency and accuracy. For this reason, they proposed a new method based on the Improved Sparrow Search Algorithm (ISSA) and Light Gradient Boosting Machine (LightGBM) from the mathematical perspective. This provides an important reference for predicting the credit risk of SMEs and reducing the loss of financial institutions. Tran *et al.* [130] proposed a neural network layer architecture for the financial time series forecasting problem that combines the bilinear projection idea and the attention mechanism. The resulting network is highly interpretable as it highlights the importance and contribution of each time instance. Sang [129] used genetic algorithm combined with support vector machine and BP neural network to assess the credit risk of supply chain finance. Sang mainly discussed the risk assessment of SME supply chain finance from the bank perspective. The research results can provide theoretical support for reducing the probability of bank profit damage and improving bank profitability. Liu *et al.* [132] proposed that in financial credit scoring, missing data from rejected loan applications leads to selection bias, making machine learning models unreliable. For this reason, they proposed a novel Reject-aware Multi-Task Network (RMT-Net). It learns to control the task weights for information sharing from rejection/approval tasks to default/non-default tasks via a gating network based on rejection probabilities. Blasco *et al.* [131] systematically reviewed existing research on deep learning methods for uncertainty quantification in financial time series forecasting. This has unearthed some research gaps for deep learning in financial forecasting. After studying the more recent literature on neural network-based financial volatility prediction, Ge *et al.* [134] found a huge gap between modern machine learning models and those applied to volatility prediction. For this reason, they proposed several promising approaches to bridge the gap. The literature review by Nazareth *et al.* [135] analyzes recent advances in machine learning and deep learning in finance. They concluded by pointing out possible new directions of inquiry for machine learning algorithms in finance. Mandal *et al.* [136] comprehensively reviewed the research related to higher-order moments based portfolio selection models. They summarized the potential application of higher-order moments in portfolio optimization, in particular how the limitations of traditional models can be improved by considering skewness and kurtosis. Olorunnimbe *et al.* [137] systematically investigated various scenarios for employing deep learning in financial markets (especially stock markets). Their study shows that existing models, despite improvements in reproducibility, still have a lot of work to do in terms of model interpretability. In terms of algorithmic evaluation, Yang *et al.* [133] proposed an evaluation tool named FinTrust for assessing the logical consistency of financial texts. This evaluation tool evaluates the consistency of each language model in analyzing financial text data and thus predicting relevant financial indicators.

To sum up, as shown in Table 3, current research on digital finance algorithms (Element=2) spans diverse application scenarios: futures trading, trading anti-fraud, lending, anti-money laundering, and monetary policy (Application=1-5). It corresponds to multiple models, including recognition models, discovery models, decision models, and even a mix of all model types (Models=1-4). The research focuses on methodological innovations across fraud detection, credit risk prediction, time series forecasting, and portfolio optimization, emphasizing algorithmic performance, interpretability, and practicality. Methodologically, it has evolved from traditional machine learning to deep learning and hybrid models integrating evolutionary algorithms, while addressing financial data characteristics like missing value handling has become a core concern. All these studies lack intelligent computing platforms (Platform Infrastructure=0) and full-stack system architectures (Facility=0). In evaluation, systematic assessment of models' logical consistency and interpretability is increasingly emphasized, aiming for both high accuracy and transparency. Overall, future trends lean toward multi-source data integration, enhanced explainability, dynamic adaptability, and efficient risk management, driving algorithms from theory to broad financial applications.

2.3.3 Digital Finance Computility

Digital finance places high demands on real-time processing of massive data and rapid computation of complex algorithms. Research on digital finance computility is crucial for ensuring its security and efficiency.

In research related to digital finance computility, Tetlock [138] suggested that continued improvements in computational power may drive the development of a rapidly growing subfield of information in financial markets in the coming years. Option pricing is one of the most active research areas in financial economics. More realistic assumptions impose a huge computational burden on computing the option pricing function and there is a huge computational challenge in determining the optimal kernel bandwidth. For this reason, Monteiro *et al.* [139] addressed this challenge through a parallel computational algorithm executed using graphical processing units. Inggs *et al.* [140] proposed a high-performance computing method for financial derivative pricing problems. They experimentally tested the performance of their high-performance computing algorithm executed on CPU, GPU, and FPGA platforms, and verified the feasibility of applying the algorithm on various high-performance computing platforms. Large-scale crowdsourced credit collection with guaranteed low latency has become a common demand in financial-level Artificial Intelligence of Things (AIoT) environments. In the face of limited computing resources, there is a lack of effective computation offloading methods to guarantee low latency. To solve this problem, Zhu *et al.* [141] introduced the edge computing model and proposed a low-latency edge computing offloading scheme for financial AIoT trust assessment. The study by Herman *et al.* [142] points out that the application of quantum computing in the financial sector is still in its early stages, but it has the potential to bring about significant changes in the financial industry, especially in terms of improving computational efficiency, solving large-scale complex problems, and reducing computational costs. Orús *et al.* [143] discussed how quantum computing can be applied to financial problems. They revealed how quantum annealers can be used to optimize portfolios, find arbitrage opportunities and perform credit scoring. In addition, Saba *et al.* [144] proposed a blockchain-based intelligent IoT protocol for high-performance and secure financial big data transactions. Li *et al.* [145] investigated the profit-maximizing fund-constrained investment scheme in cloud computing. Mann *et al.* [146] explored the cost-optimization, data-protection-aware offloading problem between the edge data centers and the cloud.

On the whole, as shown in Table 3, the research on computility in digital finance (Element=3) spans diverse application scenarios: futures trading, trading anti-fraud, lending, anti-money laundering, and monetary policy (Application=1-5). It corresponds to multiple models, including recognition model, discovery model, decision model, and generation model (Model=1-4). This research primarily focuses on enhancing computational efficiency to meet financial markets' informational demands and complex tasks: High-performance computing is applied to intensive tasks like option pricing via parallel computing, while edge computing strategies support low-latency processing for scenarios like crowdsourced credit evaluation. Quantum computing shows potential in optimizing portfolio management, and blockchain integrates with IoT protocols to secure financial big data transactions. All these studies lack intelligent computing platforms (Platform Infrastructure=0) and full-stack system architectures (Facility=0). The synergistic optimization of cloud and edge computing also helps reduce costs and enhance data protection. Overall, developmental trends highlight heterogeneous platform fusion, high-performance/low-latency coordination, and integration of emerging paradigms like quantum computing, driving financial computational capabilities toward greater efficiency, intelligence, and security.

2.4 Digital Finance Intelligent Computing Platform

With the rapid advancement of the digital economy, financial services are undergoing a profound transformation toward intelligent, platform-based, and highly collaborative architectures. In this transition, digital finance intelligent computing platforms serve as core infrastructures that integrate high-performance computing, artificial intelligence, privacy-preserving technologies, and cloud-edge collaborative frameworks to enable efficient data processing, secure data sharing, and intelligent decision-making. Existing research has systematically enriched the theoretical foundations and technical frameworks of digital finance platforms from multiple perspectives. Concurrently, numerous achievements have further advanced the intelligent, trustworthy, and efficient delivery of financial services.

Based on the evolutionary logic of financial risk identification, assessment, and control, Deng [147] summarized the most suitable feature processing algorithm workflow for visual processing technologies

Table 4. Research on Digital Finance Intelligent Computing Platform

Research	**Application**[a]	**Model**[b]	**Element**[c]	**Platform Infrastructure**[d]	**Facility**[e]
Deng 2022 [147], Shi *et al.* 2024 [148]	3	1	2	**1**	0
Zhang *et al.* 2024 [149]	1	1	1	**1**	0
Abgaryan *et al.* 2024 [150]	2	2	3	**1**	0
Luo 2023 [151]	3	0	1 3	**1**	0
Wang *et al.* 2025 [152]	3	1	2 3	**1**	0
Chen 2022 [153]	2	4	1 2	**1**	0
Liao *et al.* 2024 [154]	2	1 2	2	**1**	0
Yu 2025 [155]	3	0	3	**1**	0
Li 2024 [156]	2	3	1 2 3	**1**	0

[a] The Application dimension has five values ranging from 1-5. 1: ToC, 2: ToC & ToB, 3: ToB, 4: ToB & ToG, and 5: ToG.

[b] The Model dimension has four values ranging from 1-4. 1: Recognition Model, 2: Discovery Model, 3: Decision Model, and 4: Generation Model.

[c] The Element dimension has three values ranging from 1-3. 1: Data, 2: Algorithm, and 3: Computility.

[d] The Platform Infrastructure dimension has two values: 1 and 0, respectively indicating the presence or absence of an intelligent computing platform.

[e] The Facility dimension has two values: 1 and 0, respectively indicating the presence or absence of a full-stack system architecture by an integrated intelligent process control facility.

applicable to corporate financial management systems. Subsequently, he constructed a digital platform for corporate financial management, providing risk management strategies and implementation plans across six dimensions. Zhang *et al.* [149] pointed out that in the digital economy era, the ease of data replication has led to information leakage issues. To address this, they constructed a secure, efficient, active, and mature industrial-grade digital finance application platform for privacy computing. Employing a low-coupling, modular design approach, the platform enables data to be usable yet invisible, ensures clear and unambiguous data ownership, and facilitates secure data sharing while preserving privacy. Shi *et al.* [148] aimed to explore risk management on inclusive digital finance platforms. To this end, they constructed the BP-KMV model based on the KMV framework using a backpropagation (BP) neural network. The BP-KMV model was applied to analyze credit risk and risk management for non-listed enterprises on inclusive digital finance platforms. Results indicate a negative correlation between R&D expenditure ratio and default rate for these enterprises. This work can enrich theoretical research on comprehensive risk control in inclusive finance. Abgaryan *et al.* [150] proposed an innovative framework called IntraLayer, designed to achieve comprehensive interconnectivity within the digital finance sector. This framework comprises a core underlying infrastructure and an overarching strategy aimed at creating a groundbreaking "platform of platforms" serving as an algorithmic trustee. The infrastructure is engineered to optimize transaction efficiency for diverse participants, thereby fostering the sustainable creation of intrinsic economic value. Luo [151] primarily investigated financial data management methods and edge computing platforms based on intelligent edge computing and big data processing. This work analyzes the collaborative model between edge computing and cloud computing while exploring cloud data storage solutions. Subsequently, an edge computing platform was constructed, primarily deploying EC Master and a Docker private image repository within the data center. The designed financial data management edge computing platform effectively manages financial data, making significant contributions to enterprise data management. Wang *et al.* [152] developed a machine learning-enhanced collaborative system specifically designed for digital finance platforms, aiming to integrate theoretical advances in human-machine collaboration with practical applications in financial process optimization. The system constructs a complex multi-layer architecture that integrates machine learning capabilities with human decision-making processes, employing advanced ensemble algorithms, multi-objective optimization techniques, and adaptive learning mechanisms. This learning-collaboration approach effectively combines human knowledge with artificial intelligence, outperforming conventional computer methods and purely human strategies while enabling long-term system improvement through its adaptive learning capabilities. Chen [153] designed a digital finance talent development platform based on Java and MySQL. This platform aims to cultivate students' ability to apply mathematics and statistics to solve economic and financial problems within their specialized courses. It also vigorously promotes seminar-based instruction, laboratory-based instruction, and practice-oriented instruction, thereby achieving the goal of cultivating applied finance professionals for the financial industry. Liao *et al.* [154] designed a financial management platform based on cloud-edge collaboration technology and service-oriented architecture to help financial institutions achieve cross-regional interconnectivity and assist investors in breaking down information silos. This work proposes a cloud-edge collaboration-based financial wealth management service theory and model. The model provides personalized experiences for users through optimized collaborative filtering algorithms while protecting user privacy. Yu [155] constructed a cloud-based financial shared services platform to optimize resource allocation and decision-making efficiency in corporate financial management. Employing a modular architecture design and multi-dimensional performance simulation methods, the study analyzed the platform's technical capabilities in data processing, process automation, and security assurance. Findings indicate that cloud computing integration provides technical support for the platform's intelligence and stability, laying a theoretical foundation for future multi-scenario adaptive expansion. Li [156] addressed data security concerns in intelligent financial digital sharing platforms by proposing a data sharing framework based on blockchain and edge computing. Building upon this framework, an inseparable task allocation algorithm for data sharing was developed. This algorithm employs multi-node collaborative data storage to alleviate data storage pressure on central servers, thereby resolving the challenge of inseparable task allocation.

In summary, as shown in Table 4, the development of digital finance intelligent computing platforms (Platform Infrastructure=1) applies in scenarios like futures trading, trading anti-fraud, and lending (Application=1-3). It is evolving from single-function systems toward integrated, multi-technology architectures. These platforms match diverse models, including recognition, discovery, decision, and generation models (Model=1-4). They also combine elements like data, algorithms, and computility (Element=1-3). Research across risk management, privacy computing, edge computing, and blockchain trust mechanisms has provided technical solutions to enhance financial operation safety, efficiency, and intelligence. All these platforms lack full-stack system architectures (Facility=0). Looking ahead, these platforms are expected to deepen capabilities in high-throughput data processing, trusted data circulation, and cross-entity collaboration, while achieving better explainability, security, and scalability in complex scenarios. As the technological framework matures, digital finance intelligent computing platforms will become vital infrastructure for digital finance innovation, delivering high-quality intelligent services and strategic support to financial institutions, enterprises, and regulators.

3 $\mathcal{F}$AMEπ

3.1 The Overview of $\mathcal{F}$AMEπ

From the above literature reviews, it can be seen that existing research on digital finance exhibits a certain degree of one-sidedness: (1) a single financial application scenario oriented; (2) a single functionality of the developed financial model; (3) no comprehensive consideration of data, algorithms, and computility; and (4) the developed platform infrastructure does not closely integrate with the characteristics of digital finance. If the findings from the above research can be integrated, a full-stack system architecture can be constructed. This architecture would serve all scenarios in digital finance, incorporate various digital finance model functionalities, and provide users with diverse services securely and efficiently. So, what modules are required to build this system architecture? The novel taxonomy proposed in the literature review above demonstrates that application, model, intelligent computing element, and platform infrastructure are all indispensable. Furthermore, to ensure that all modules within this system architecture can be seamlessly integrated and operate securely and efficiently, support from additional module (i.e., facility) is also required. For this reason, we propose $\mathcal{F}$AMEπ, a practical full-stack system architecture for empowering secure digital finance. Its complete architecture and the details of each part are shown in Figure 6. The core innovation of the $\mathcal{F}$AMEπ architecture design is that it can parse and categorize the financial application requirements proposed by different types of users into corresponding financial application scenarios. After selecting the model corresponding to the demand in the application scenario, $\mathcal{F}$AMEπ will analyze the resource-related theory according to the application demand and the financial model. Then, $\mathcal{F}$AMEπ rationally allocates the corresponding computational resources and runs the model

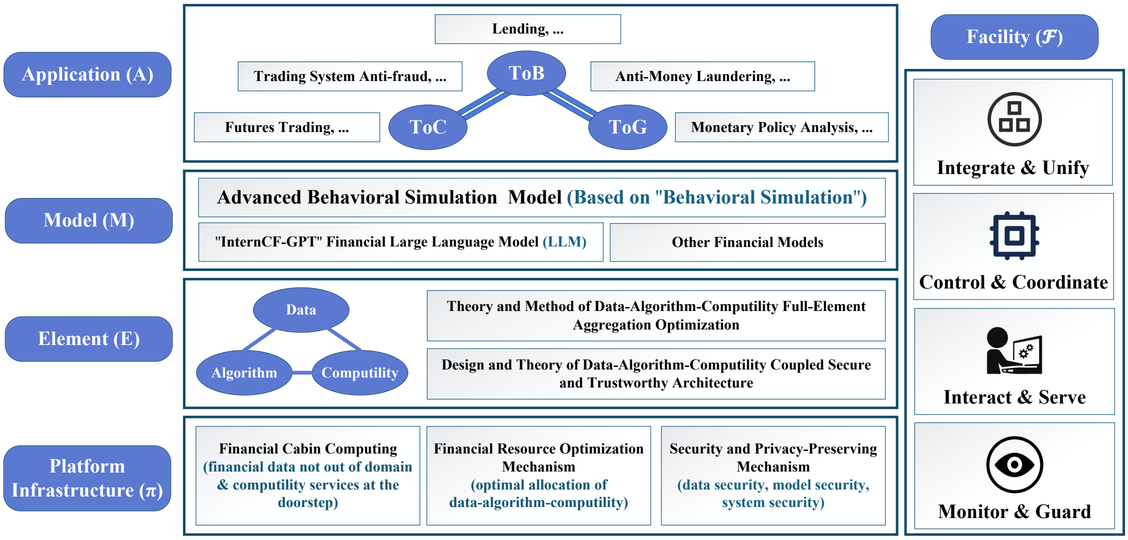


Figure 6. The Complete Architecture of $\mathcal{F}$AMEπ.

through the integrated network scheduling platform. After the computation is completed, the results are presented to the user through the user interaction interface.

3.2 A: Application

Application (A) handles the task of receiving user inquiries and analyzing requirements within the system architecture. This poses a challenge to its ability to categorize user inquiries appropriately into different digital finance applications. To address this, we have equipped Module A with a novel approach to segmenting digital finance application scenarios, enabling it to intelligently analyze user needs.

Module A categorizes digital finance applications based on three business modes: ToC, ToB, and ToG. Here we list five representative digital finance applications: ToC, ToC & ToB, ToB, ToB & ToG, and ToG. These correspond to five typical application scenarios: Futures Trading, Trading Anti-Fraud, Lending, Anti-Money Laundering, and Monetary Policy. This innovative division based on the three business modes of ToC, ToB and ToG can clearly reflect the multi-dimensional needs of the financial sector, cover the entire scenarios of financial business and provide customized financial task solutions for different user groups. Most importantly, this segmentation approach is extensible for financial entire scenarios, i.e., it provides a complete segmentation approach for financial application entire scenarios. Although we only list one application scenario for each type of user here, in fact, when $\mathcal{F}$AMEπ receives demands for application scenarios that it has never encountered before, such as central bank digital currencies (CBDCs), DeFi, and other emerging domains, it can also categorize them according to this segmentation approach. For example, the application requirement for stocks is solved in a manner similar to futures trading.

In addition, Module A is domain-knowledge-based in its implementation, meaning that its accurate classification of user requirements relies on its own professional domain knowledge. This domain knowledge mechanism can change continuously depending on the application domain of system architecture, which means it can be transferred to professional domains other than finance. This demonstrates extremely strong scalability.

3.3 M: Model

M (Model) is a crucial module within the system architecture. It serves to provide suitable digital finance models to address user problems for $\mathcal{F}$AMEπ. It is worth noting that the model referred to here is not limited to a single financial-related model. Module M we propose integrates numerous algorithms, models,

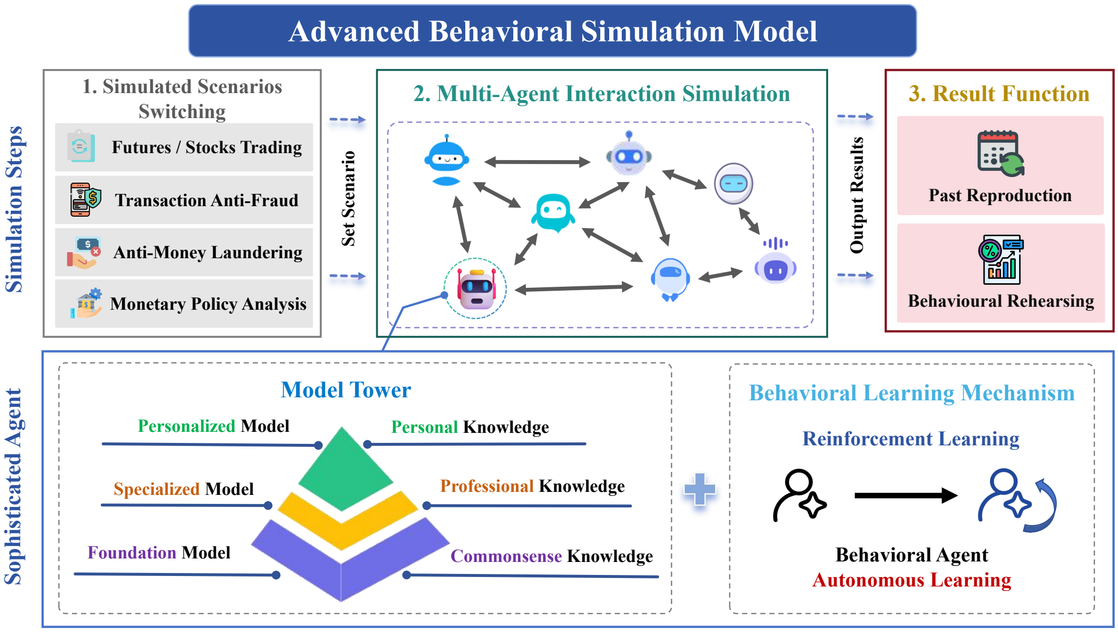


Figure 7. Advanced Behavioral Simulation Model [157]. The main focus of the advanced behavioral simulation model is on model tower-driven agents and their behavioral learning mechanism, which can be used to simulate multi-agent interactions in different simulated scenarios.

and frameworks that can serve digital finance scenarios. These models include the aforementioned digital finance models (recognition models, discovery models, decision models, and generation models), as well as model frameworks designed and developed independently by our team. Here we focus on the **Advanced Behavioral Simulation Model** we built (as shown in Figure 7). It is designed based on the concept of "**Behavioral Simulation**" [158], and uses the **"InternCF-GPT" financial large language model (LLM)** developed by our team.

The shortcomings of the existing four scientific paradigms have led us to propose the next generation of simulation: Behavioral Simulation [158]. Behavioral Simulation organically integrates the previous four paradigms and solves the problem of model training in the case of insufficient data and low quality. Behavioral Simulation technology is mainly composed of two aspects: a model tower with a multi-layered knowledge system and a behavioral learning mechanism. The model tower simulates the multi-layered knowledge structure of human beings. It is divided from the bottom upwards into basic model, specialized model and personal model, which carry basic knowledge, specialized knowledge and personal knowledge of human beings respectively. The basic model can be a general LLM, the specialized model refers to a domain-specific LLM (e.g., our self-developed financial LLM "InternCF-GPT"), and the personal model is a more individual-oriented mental model. Human behavior is the result of the joint influence of knowledge and learning, so behavioral learning mechanism is essential. When a model tower with a multi-layer knowledge structure introduces a behavioral learning mechanism, it can evolve its own knowledge system through interaction with the outside world, in order to make a more rational behavior in line with its own personality.

The Advanced Behavioral Simulation Model can simulate various adversarial scenarios in the financial field, such as futures trading [157], trading anti-fraud, anti-money laundering, and monetary policy analysis. Within the framework, the actors include real users and virtual users simulated by the model tower, who can be cross-combined to form a hybrid human-machine attacking party and a hybrid human-machine defending party to carry out attack and defense drills in the corresponding scenarios.

3.4 E: Element

E (Element) provides the model with appropriate data, algorithms, and computility allocation schemes [159], determines the feasibility of resource allocation plans, and guides the operation of Module π. Module

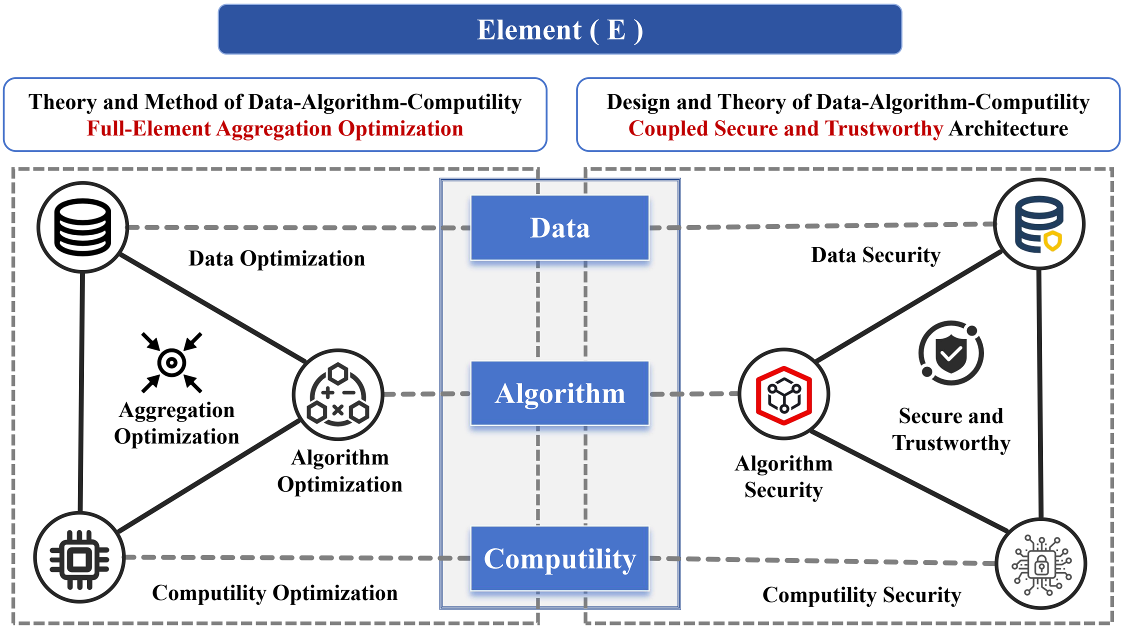


Figure 8. E (Element). Element consists of two parts: Theory and Method of Data-Algorithm-Computility Full-Element Aggregation Optimization, Design and Theory of Data-Algorithm-Computility Coupled Secure and Trustworthy Architecture.

E includes **Theory and Method of Data-Algorithm-Computility Full-Element Aggregation Optimization** and **Design and Theory of Data-Algorithm-Computility Coupled Secure and Trustworthy Architecture** (as shown in Figure 8).

3.4.1 Theory and Method of Data-Algorithm-Computility Full-Element Aggregation Optimization

Theory and Method of Data-Algorithm-Computility Full-Element Aggregation Optimization serves as the foundational basis for achieving efficient resource utilization and collaborative computation in $\mathcal{F}$AMEπ. This theory emphasizes the dynamic adaptation among the three core elements (data, algorithms, and computility). It asserts that only when data characteristics, algorithmic mechanisms, and computility structures are deeply aligned can the intrinsic value embedded in data be fully exploited. It not only focuses on maximizing efficiency in resource allocation but also highlights the coupling relationships and co-optimization pathways among different elements, offering a systematic methodological framework for complex financial computing scenarios.

In the financial domain, data, algorithms, and computility jointly constitute the infrastructure of intelligent computation. Financial data are diverse in form, encompassing structured transaction records, unstructured textual information, and real-time streaming data. Each data type imposes distinct requirements on algorithm design and computility configuration. For example, high-dimensional and nonlinear datasets are better suited for deep learning models such as Transformer or GNN, whereas real-time transactional streams demand low-latency support from edge computility resources. Thus, the nature of data determines the selection of algorithms and computility allocation, while the complexity and computational patterns of algorithms, in turn, influence how computility is scheduled and distributed. Theory and Method of Data-Algorithm-Computility Full-Element Aggregation Optimization is established precisely within this interactive triadic logic.

The core of this theory includes element co-optimization, dynamic adaptation mechanisms, and an aggregation optimization model. In terms of data optimization, it focuses on refining cleaning, compression, transmission, and storage strategies according to data structures and access characteristics, thereby achieving efficient data flow and computational adaptability. For algorithm optimization, it dynamically selects or combines algorithmic models based on data properties and task objectives, enhancing adaptiveness and performance through model integration and online learning. In computility optimization, it employs elastic scheduling and distributed computation techniques in accordance with task features and algorithmic demands, realizing dynamic expansion and load balancing. By establishing a multi-objective aggregation optimization model, this theory comprehensively balances time, cost, accuracy, and energy consumption, seeking global optima through heuristic algorithms and reinforcement learning techniques.

The distinct advantages of this theory and method lie in its adaptivity-driven full-element optimization, achieving global coordination, flexible scheduling, and cost-effective resource utilization while maintaining privacy protection and real-time responsiveness. Nonetheless, challenges persist, including cross-modal adaptation for heterogeneous data, scalability to complex environments, and the integration of self-evolving intelligent optimization algorithms. Future research will further explore self-adaptive mapping mechanisms among elements, standardized interface frameworks, and generative AI-driven self-optimization paradigms, aiming to transition from static configuration to intelligent evolution.

In summary, Theory and Method of Data-Algorithm-Computility Full-Element Aggregation Optimization elucidates the intrinsic matching logic and collaborative dynamics among the three elements (data, algorithms, and computility) establishing a closed-loop optimization system that is data-driven, algorithm-guided, and computility-supported. This theory provides a solid theoretical and technological foundation for $\mathcal{F}$AMEπ to achieve efficient computation and intelligent decision-making in complex financial scenarios.

3.4.2 Design and Theory of Data-Algorithm-Computility Coupled Secure and Trustworthy Architecture

Design and Theory of Data-Algorithm-Computility Coupled Secure and Trustworthy Architecture is the important technical foundation of $\mathcal{F}$AMEπ system. It aims to ensure the security and data trustworthiness of the system in highly sensitive scenarios such as finance through comprehensive protection and trustworthy guarantee. Its core objective is to realize the robustness, transparency and reliability of the system operation, and to provide strong security for complex financial applications.

Data in the financial domain is highly sensitive, involving transaction records, account information, etc., and any data leakage or tampering may cause serious consequences. In addition, the complexity of deep learning algorithms (e.g., GNN, Transformer) increases the difficulty of algorithm credibility verification, while the diversity and heterogeneity of nodes in distributed computility networks make them vulnerable to malicious attacks. Therefore, current financial scenarios urgently need to solve the problems of insufficient data security, lack of algorithmic transparency, and hidden dangers of computility resources, and build a secure and trustworthy system architecture by establishing a mechanism to protect data integrity and confidentiality, improving the transparency and fairness of algorithmic decision-making, and ensuring the trustworthy interaction of computility resources.

The core architecture design includes three major parts: data security and trustworthiness design, algorithm security and trustworthiness design, and computility security and trustworthiness design. In terms of data security, differential privacy [160], homomorphic encryption [161], and federated learning [162] techniques are used to protect privacy, and the data processing process is recorded through the blockchain. It is combined with hash checking to guarantee data integrity, while zero-trust architecture and dynamic access control are used to prevent unauthorized access. In algorithmic security, interpretable AI technology is used to enhance transparency, and anti-jamming ability is improved through adversarial sample detection and model robustness training, while fairness is guaranteed using debiasing algorithms and model auditing. In the computility security design, virtualization technology and sandbox mechanism are used to achieve resource isolation, computility trustworthiness is guaranteed by Trusted Execution Environment (TEE) and Remote Proof, and fault-tolerance capability and resource allocation efficiency are improved by distributed consensus algorithm and dynamic trust assessment.

The architecture has a wide range of application scenarios in the financial field. For example, in anti-money laundering, differential privacy is used to protect data privacy, combined with interpretable AI to analyze money laundering patterns, and distributed computing security is guaranteed through TEE; in high-frequency trading, order data integrity is verified in real time, model fairness is audited, and high-trust computility nodes are dynamically assigned to handle critical tasks. Through the all-round synergy of data, algorithms and computility, the architecture realizes full-process protection, balances security and efficiency, and improves the overall credibility of the financial system.

In the future, the architecture design will further explore security in the quantum computing environment, develop anti-quantum cryptography and stronger privacy protection mechanisms, as well as optimize security policies using generative AI to improve real-time response capabilities. Design and

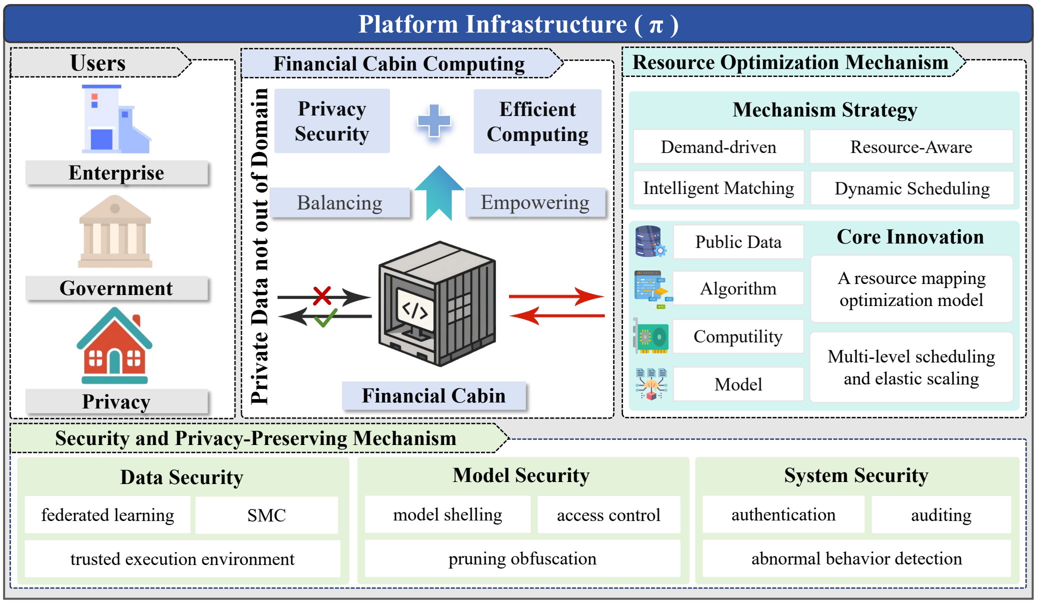


Figure 9. π (Platform Infrastructure). Module π consists of three parts: Financial Cabin Computing, Computing Resource Optimization Mechanism, and Security and Privacy-Preserving Mechanism.

Theory of Data-Algorithm-Computility Coupled Secure and Trustworthy Architecture not only adapts to the current needs of complex financial scenarios, but also provides a solid technical foundation for future application scenarios with higher challenges.

3.5 π: Platform Infrastructure

π (Platform Infrastructure) refers to the digital finance intelligent computing integration platform in the architecture. When a user request from outside the system is judged by Module E to be able to provide services for it, the data, algorithms, and computility needed to solve the user request will be deployed by Module π. Reasonable and even optimal resource deployment is the problem that Module π needs to solve, for which we have pioneered three core technologies of digital finance intelligent computing integration platform: **Financial Cabin Computing** [25, 26], **Computing Resource Optimization Mechanism**, and **Security and Privacy-Preserving Mechanism** (as shown in Figure 9). These technologies support Module π in securely delivering computing resources to users.

3.5.1 Financial Cabin Computing

Financial Cabin Computing is one of the most representative and innovative core technologies in Module π. It is initially proposed to solve the contradiction between "data security" and "efficient computing" in the highly sensitive financial field. Financial data is often highly private and important, especially core business data of enterprises, personal transaction data of users, and macroeconomic regulation data of the government, whose leakage may lead to significant security risks or legal problems. Therefore, the traditional mode of sending data to computing centers for processing can no longer meet the current reality of financial data security compliance needs. Financial Cabin Computing is a new computing paradigm of "data not out of the domain, computility services at the doorstep" proposed in this context.

In terms of specific implementation, Financial Cabin Computing emphasizes the flexible migration of computing resources rather than the centralized aggregation of data. In other words, the user's data can always be stored locally (e.g., enterprise intranet, government data centers, etc.), while the models, algorithms, and necessary computility resources in Module π are "moved" to the region where the data is located through virtual migration, container deployment, edge scheduling, and other technologies to locally complete the whole process of model loading, computation execution, and result generation. In this way, it not only guarantees in-situ storage of data and controlled access, but also realizes “zero leakage” of sensitive data, completely solving the security risks brought by data out of the domain.

At the same time, Financial Cabin Computing is not a single hardware device, but a network of intelligent computing power formed by Module π through the network and dynamic collaboration with multiple forms of “mobile computing cabins”. These “cabins” can be deployed locally in the user’s trusted execution environment, containerized computing nodes, a combination of hardware and software lightweight equipment, etc., with elasticity of expansion, rapid deployment, remote scheduling, so as to meet the flexible computility requirements of ToC, ToB, ToG and other types of financial users in different scenarios.

In addition, Financial Cabin Computing also embeds secure privacy computing mechanisms, such as federated learning, homomorphic encryption, and secure multi-party computation (SMPC), which further enhances the data protection capability during local operation. The structure and parameters of the model ontology can also be encrypted transmission and encapsulation techniques to prevent model theft or attack during the cabin computing process.

To summarize, Financial Cabin Computing provides Module π with an innovative “security-as-a-service” capability. It guarantees the real-time, high efficiency and reliability of computation without touching the core data assets of users, and provides a strong technical support for the data security application in financial scenarios for multiple types of users, such as governments, enterprises and individuals. This mechanism is not only in line with the national data security policy guidance, but also provides a paradigm guide for the credible evolution of future financial technology infrastructure.

3.5.2 Computing Resource Optimization Mechanism

Computing Resource Optimization Mechanism is one of the core capabilities of Module π to achieve intelligent scheduling and fine-grained management of computility, and its goal is to intelligently match and optimally allocate resources such as data, algorithms, and computility dynamically according to the task characteristics, model requirements, and resource status of different financial application scenarios. In the diversified and fast-response financial business environment, the tasks proposed by different users (ToC, ToB, ToG) have significant differences in computational intensity, data sensitivity, model complexity, and time requirements, etc. The traditional static resource allocation mode can no longer meet the dynamic changes and highly concurrent requests of such scenarios, and a more flexible and intelligent resource management mechanism is urgently needed.

Computing Resource Optimization Mechanism in Module π adopts the strategy of “demand-driven, resource-aware, intelligent matching, dynamic scheduling”. First, the system forms a resource demand list through semantic parsing and model dependency analysis of the user’s task, specifying the specific requirements of the task in terms of data size, algorithm type, computational intensity, latency tolerance, etc. Then, the platform performs real-time sensing and load evaluation of the currently available heterogeneous computing resources (including GPUs, CPUs, FPGAs, etc.), and searches for the most matching computing nodes and service capabilities in the global resource pool.

The core innovation of the mechanism is reflected at two levels. The first is the introduction of a resource mapping optimization model. In the process of computility allocation, not only the current load and processing capacity are considered, but also the financial domain attributes of the task, such as transaction frequency, risk level, timing sensitivity, etc., are combined to realize the financial semantic awareness of resource scheduling. Secondly, it supports multi-level scheduling and elastic scaling. The resource optimization mechanism can be combined with edge arithmetic, cloud arithmetic, local arithmetic, etc. for hierarchical management, and automatic elastic deployment is carried out when resources are tight or sudden high concurrency, so as to guarantee the continuous and stable operation of the task.

At the same time, in order to enhance the security and transparency of resource allocation, Computing Resource Optimization Mechanism also integrates a security monitoring system based on verifiable computation and resource usage traceability to ensure the compliance and traceability of resource invocation, and to meet the requirements of high security and high credibility in financial scenarios.

Overall, Computing Resource Optimization Mechanism effectively bridges the gap between the model execution demand and the computing network resources, so that Module π has the ability to respond quickly, schedule reasonably, and optimize execution under complex application scenarios such as financial transactions, anti-fraud, lending and borrowing risk control, and policy analysis. This not only significantly improves the operation efficiency of financial models and the overall throughput of the system, but also provides a solid foundation for realizing green, intelligent and efficient operation of resources in financial scenarios.

3.5.3 Security and Privacy-Preserving Mechanism

Security and Privacy-Preserving Mechanism is the key support part of Module π in ensuring the compliant use of financial data and preventing model leakage and system attacks. Currently, the financial industry is facing multiple challenges of "high data value, high privacy risk, and strict compliance requirements", especially in the ToB and ToG scenarios, and many organizations have a growing demand for "data not out of the domain". Therefore, Module π innovatively integrates a variety of cutting-edge security computing technologies to create a "data security, model security, system security" trinity of security and privacy computing system. It supports the efficient operation of the entire financial intelligent computing network platform under the premise of security and control.

In terms of data security, the platform focuses on adopting technologies such as federated learning, secure multi-party computing, and trusted execution environment, realizing the computing paradigm of "data available but not visible". By sending algorithms to the domain where the data is located for local training or reasoning, sensitive data is avoided to be transmitted in the network, which fundamentally avoids the risk of data leakage. Meanwhile, combining with differential privacy mechanism, it effectively suppresses the exposure of user's privacy due to the leakage of statistical features during the training process.

In terms of model security, Module π has built-in model encryption and reverse engineering defense mechanisms, supporting strategies such as model shelling, pruning obfuscation, and access control to prevent models from being reverse cracked or illegally invoked during operation or delivery. In addition, the platform also supports dynamic monitoring of model behavior to identify potential abnormal output, backdoor attacks, or model drifting behavior, thus guaranteeing the stability and controllability of financial models in real running scenarios.

In terms of system security, Module π has constructed a deep defense system for the financial intelligent computing network, including an authentication mechanism, an access control mechanism, a resource usage auditing mechanism and an abnormal behavior detection mechanism, forming a closed loop of security links from access, scheduling to execution. This mechanism ensures that every resource call, model operation and data transmission is carried out within the authorized scope and regulatory framework, and that threats can be quickly responded to and isolated when they are detected.

In summary, Security and Privacy-Preserving Mechanism of Module π not only provides a diversified service mode of "data not moving but computility moving, data not moving but models moving, data not moving but Facility moving" for business and government users, but also builds a set of sustainable evolutionary security defenses in the highly sensitive business scenarios of financial risks. The mechanism effectively guarantees the compliance of model operation, the trustworthiness of platform resources and the privacy of financial information, escorting the digital and intelligent development of the financial industry.

With the support of the above technologies, Module π has the ability to strengthen the reconfiguration capability of the computility network to adapt to the ever-changing demands and diverse resources in the financial market, and to enhance the maneuverability of the computility network to respond to the instantaneous financial transactions and complex requests. All in all, the resource optimization realized by Module π can effectively support the model running requirements of different financial scenarios of ToC, ToB and ToG.

3.6 $\mathcal{F}$: Facility

$\mathcal{F}$ (Facility) is not merely a conceptual aggregator of Module A, M, E, and π, but an operational execution entity instantiated as an intelligent agent ($\mathcal{F}$-Agent). This agent-based design provides a concrete and implementable mechanism for achieving cross-layer integration, coordination, and control in practice. Concretely, Module $\mathcal{F}$ is implemented as a stateful, policy-driven intelligent agent that maintains a global view of system states across all four modules and orchestrates their interactions through standardized interfaces and decision policies. Its operation can be formally characterized by the following components:

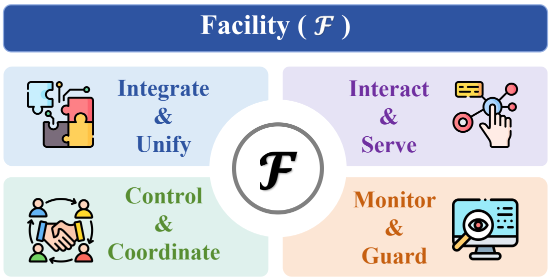


Figure 10. $\mathcal{F}$ (Facility). Module $\mathcal{F}$ has four functions: integrate and unify, interact and serve, control and coordinate, and monitor and guard.

Module $\mathcal{F}$ maintains a unified system state:

$$S_{\mathcal{F}} = \{S_A, S_M, S_E, S_\pi\},$$

where each sub-state corresponds to the real-time status of application requirements, model availability and readiness, element-level constraints, and platform resource conditions. This shared state enables Module $\mathcal{F}$ to reason holistically rather than react locally.

Module $\mathcal{F}$ is equipped with a policy function:

$$\pi_{\mathcal{F}} : (S_{\mathcal{F}}, R, C) \rightarrow \mathcal{A},$$

where R denotes user requests and C denotes security, compliance, and optimization constraints. The output action set ($\mathcal{A}$) includes actions such as model selection, resource orchestration, execution approval, interaction termination, or fallback negotiation. This transforms Module $\mathcal{F}$ from a passive router into an active decision-maker.

Integration is achieved through explicit interface contracts rather than implicit coupling. Module $\mathcal{F}$ enforces standardized message schemas (e.g., requirement descriptors, model capability profiles, element-resolution reports, and resource manifests), ensuring that heterogeneous modules can interoperate without tight dependency binding.

With this agent-based instantiation, the four functions of Module $\mathcal{F}$ are realized through concrete mechanisms:

Integrate and Unify: On the one hand, Module $\mathcal{F}$ serves as an organizer that integrates the other four layers of architecture and ensures that the entire system operates in an orderly manner as a whole.

Interact and Serve: On the other hand, Module $\mathcal{F}$ is the interface that separates the internal and external parts of the system. It is like the “front office” of an enterprise, which needs to receive different requests from outside the system, convey the requirements to the system, and after the system operation, return the request results to the outside of the system through the Application’s interactive interface.

Control and Coordinate: The most important point is that Module $\mathcal{F}$ acts as a controller during the entire operation of the system, and the synergistic work of the various other modules will be controlled and coordinated by Module $\mathcal{F}$. This will be reflected in the next workflow description of $\mathcal{F}$AMEπ.

Monitor and Guard: In addition, Module $\mathcal{F}$ plays a monitoring and guard role in controlling the operation of the whole system and coordinating the work between its components. Specifically, direct interactions between Module A, M, E, and π are monitored by Module $\mathcal{F}$, which has the power to terminate the interaction if there is a security risk in the interaction between them. This is reflected in the description of the workflow of $\mathcal{F}$AMEπ that follows.

This agent-based operationalization clarifies that Module $\mathcal{F}$ is not an abstract glue layer, but a centralized yet intelligent execution authority that enables $\mathcal{F}$AMEπ to function as a coherent full-stack system. Without Module $\mathcal{F}$, Module A, M, E, and π would degrade into a loosely coupled toolkit; with Module $\mathcal{F}$, they form a closed-loop, policy-governed, and self-coordinating system. In this sense, Module $\mathcal{F}$ provides the missing architectural mechanism that bridges conceptual taxonomy and engineering realizability, transforming $\mathcal{F}$AMEπ from a descriptive framework into a deployable and extensible full-stack digital finance system.

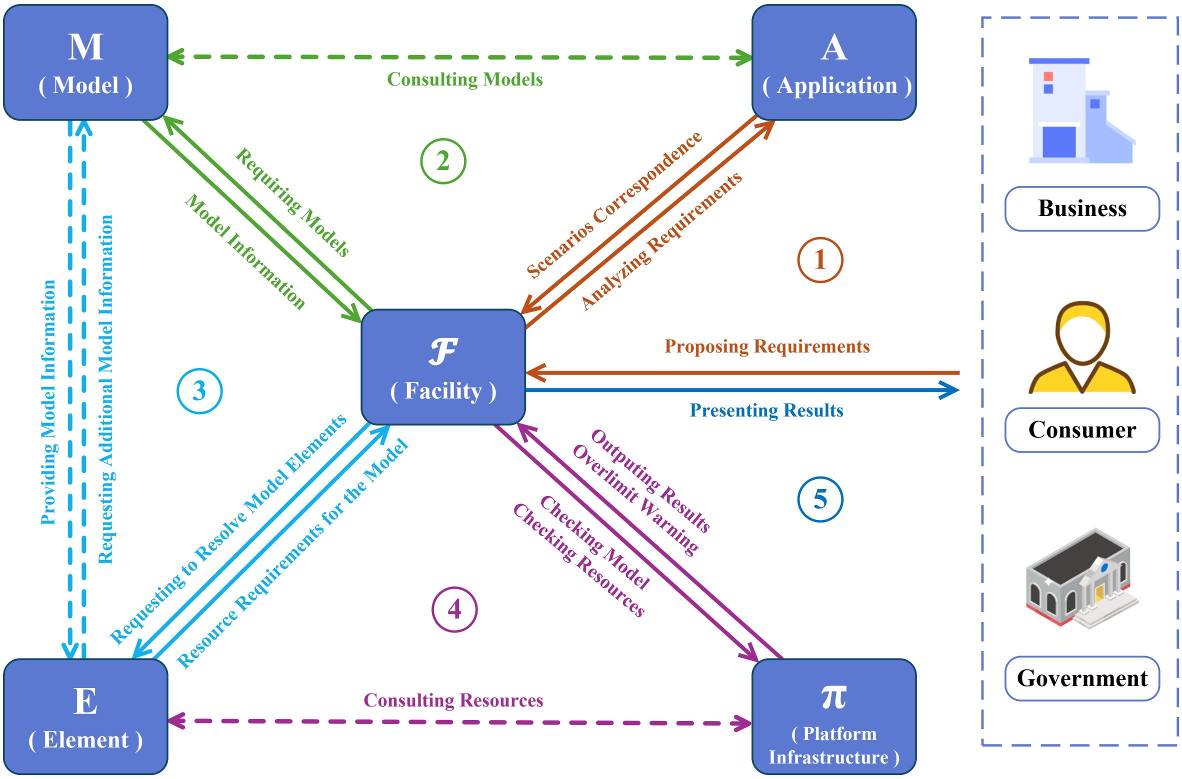


Figure 11. The Workflow of $\mathcal{F}$AMEπ. Module $\mathcal{F}$ is responsible for receiving user requirements and coordinating interactions among other modules, and finally presenting the results to users; Module A is responsible for analyzing user requirements; Module M is responsible for selecting models suitable for addressing user requirements; Module E is responsible for analyzing the three elements of training and running the selected models; Module π is responsible for scheduling the resources required for the models and for training and running the models.

3.7 The Workflow of $\mathcal{F}$AMEπ

The workflow of $\mathcal{F}$AMEπ is shown in Figure 11: Module $\mathcal{F}$ acts as a service frontend between the device and the users, and the users inputs their financial requirements through the interaction interface of Module $\mathcal{F}$. Module $\mathcal{F}$ receives the requirements from the users and passes them to Module A for requirement analyzing, and after analyzing, Module A returns the information of the financial application scenario that corresponds to the requirements to Module $\mathcal{F}$. Based on the analyzing results, Module $\mathcal{F}$ requests the required financial model from Module M and sends a checklist of the models that should be provided to Module π. Module M receives the request and provides the required model to Module π. If Module M is unable to provide the corresponding model (e.g., the model is missing), it negotiates with Module A directly and provides a substitute model (The interactions between Module A, M, E and π are under the supervision of Module $\mathcal{F}$ to ensure framework security. This is shown as the dotted lines in Figure 11). After that, Module $\mathcal{F}$ sends a model element resolution request to Module E, and Module M provides the required financial model information to Module E. Module E receives the model element resolution request from Module $\mathcal{F}$ and performs element resolution on the model information sent by Module M. If Module E lacks model-related information during the analyzing process, it will directly send a request to Module M to supplement the model information. After Module E finishes analyzing the model elements, it sends a list of resources required for model operation to Module $\mathcal{F}$. After Module $\mathcal{F}$ finishes organizing the model elements, it sends a checklist of resources required for model operation to Module π. Module π, after receiving the checklist, will check the model sent by Module M and reasonably allocate the resources (e.g., data, arithmetic power, etc.) required for model operation according to the resource checklist. If there is any problem with the resource allocation in this process, then Module π will negotiate with Module E and adjust the resources accordingly. When the model is finished running on Module π, Module π will return the results to Module $\mathcal{F}$. After that, Module $\mathcal{F}$ will then organize and graphically display that results to the user. This concludes a complete run of the device.

It is worth mentioning that after the completion of each user's request, Module E will summarize the resources according to the financial application scenarios corresponding to this request provided by Module A. On the one hand, this can be shown to the users to help them understand the resources required for the completion of the requirement, so that the users can consider the resource utilization when they puts forward a similar requirement next time. On the other hand, this kind of summary can help Module E to continuously improve its ability to analyze the model elements, so that the architecture can allocate resources more rationally.

3.8 Case Study

3.8.1 Case Study 1: End-to-End Fintech Credit Risk Scoring for SME Lending (ToB Scenario)

Consider a commercial bank providing unsecured or semi-secured loans to SMEs. The core challenge is to perform real-time credit risk scoring by jointly leveraging heterogeneous data sources (transaction records, invoice flows, tax data, and behavioral logs) under strict regulatory and privacy constraints. Traditional pipelines often rely on static scoring models deployed on centralized infrastructure. They suffer from limited adaptability, fragmented security control, and inefficient resource utilization.

To address the above user issue, $\mathcal{F}$AMEπ operates through the following process:

1. User Request and Requirement Analysis (User $\rightarrow \mathcal{F} \rightarrow$ A): A loan officer or an automated lending system submits a request through Module $\mathcal{F}$ interface, specifying the need for credit risk assessment for a target SME. Module $\mathcal{F}$ forwards the request to Module A, which analyzes it and classifies the task as a ToB lending risk scoring scenario, characterized by high data sensitivity, medium-latency tolerance, and strong interpretability requirements.
2. Model Selection and Provisioning ($\mathcal{F} \rightarrow$ M $\rightarrow \pi$): Based on the scenario identified by Module A, Module $\mathcal{F}$ requests suitable risk scoring models from Module M. Module M provides a composite model set, including traditional financial risk models (e.g., gradient boosting or logistic regression for baseline scoring) and an Advanced Behavioral Simulation Model to capture behavioral and interaction-driven risks. The model checklist is then delivered to Module π for execution preparation.
3. Element Resolution and Resource Planning ($\mathcal{F} \rightarrow$ E): Module $\mathcal{F}$ sends a model element resolution request to Module E. Module E analyzes the data-algorithm-computility dependencies, identifying that structured tabular data dominate, interpretability constraints are high, and moderate computational intensity is required. Module E produces a resource requirement list, specifying secure local data access, CPU-dominated computility, and interpretable model components.
4. Secure Execution via Platform Infrastructure (π): Module π deploys the models using Financial Cabin Computing, ensuring that sensitive enterprise data remain within the bank's internal domain. Computility resources are dynamically allocated according to the checklist of Module E. Secure privacy computing mechanisms (e.g., access control and auditable execution) are activated to guarantee compliance.
5. Result Delivery and Feedback ($\pi \rightarrow \mathcal{F} \rightarrow$ User): After execution, Module π returns risk scores and interpretability artifacts (e.g., feature contributions) to Module $\mathcal{F}$. Module $\mathcal{F}$ organizes the outputs and presents them through a graphical interface to the loan officer. The decision rationale is transparent and auditable.
6. Post-Task Resource Summary (E): Upon completion, Module E summarizes the resource usage and model effectiveness for this lending scenario. This summary can inform future lending requests and continuously refine element resolution strategies.

This case demonstrates how $\mathcal{F}$AMEπ enables a secure, interpretable, and adaptive credit risk scoring pipeline, achieving end-to-end integration from user request to decision output while preserving data sovereignty and optimizing resource utilization.

3.8.2 Case Study 2: Transaction Fraud Detection and Risk Alerting in Digital Payments (ToC & ToB Scenario)

A large-scale digital payment platform serves millions of individual users while supporting merchant-side transactions. The platform must detect real-time fraudulent transactions under high concurrency, low latency, and evolving attack strategies. Conventional fraud systems often deploy fixed models with limited adaptability and siloed security mechanisms.

To address the above user requirement, $\mathcal{F}$AMEπ operates through the following process:

1. User/System Trigger ($\mathcal{F} \rightarrow$ A): A suspicious transaction or batch of transactions triggers a fraud detection request through Module $\mathcal{F}$. Module A identifies the task as a hybrid ToC-ToB fraud detection scenario, requiring real-time response and high robustness against adversarial behavior.
2. Adaptive Model Retrieval ($\mathcal{F} \rightarrow$ M): Module $\mathcal{F}$ requests fraud detection models from Module M. Module M supplies a combination of real-time anomaly detection models and an Advanced Behavioral Simulation Model capable of simulating adversarial transaction patterns. If certain models are unavailable, Module M negotiates with Module A to substitute functionally equivalent alternatives.
3. Element Analysis and Optimization ($\mathcal{F} \rightarrow$ E): Module E evaluates the model requirements and identifies streaming data processing, GPU-accelerated inference, and strict latency constraints. It generates a fine-grained resource checklist emphasizing edge computility and fast model switching.
4. Dynamic Resource Allocation (π): Module π allocates edge and cloud computility resources based on the guidance of Module E, deploying models close to transaction sources to minimize latency. Secure privacy computing mechanisms ensure that user transaction data are protected during processing.
5. Fraud Alert and Visualization ($\pi \rightarrow \mathcal{F} \rightarrow$ User): Detection results, including fraud scores and alert levels, are returned to Module $\mathcal{F}$. Module $\mathcal{F}$ visualizes the alerts for platform operators and, if necessary, triggers automated responses such as transaction blocking or secondary verification.
6. Learning and Evolution (E): Module E aggregates post-run statistics on data patterns, model performance, and resource usage, enhancing its future ability to resolve elements under evolving fraud strategies.

This scenario illustrates how $\mathcal{F}$AMEπ supports high-concurrency, low-latency fraud detection with adaptive modeling and secure infrastructure, enabling continuous evolution against emerging financial threats.

Together, these two case studies demonstrate that $\mathcal{F}$AMEπ is not merely a conceptual framework but a practical, end-to-end architecture capable of supporting real-world fintech pipelines. By coordinating Module A, M, E, π through Module $\mathcal{F}$, $\mathcal{F}$AMEπ achieves unified requirement analysis, adaptive model orchestration, principled resource optimization, and secure execution across diverse financial scenarios.

3.9 The Advantages of $\mathcal{F}$AMEπ

Existing digital finance systems are typically constructed following application-driven or technology-driven paradigms, such as microservice-based financial platforms, data-middle-platform architectures, or AI pipeline-centric systems for specific tasks (e.g., fraud detection, credit scoring, or trading) [163–166]. These architectures have proven effective in optimizing individual tasks or isolated scenarios, but they are inherently limited when confronted with cross-scenario, cross-stakeholder, and security-sensitive financial environments.

First, most existing architectures are patchwork solutions, where data management, model execution, security mechanisms, and computing infrastructures are developed and optimized independently. Although modularization improves flexibility, it also leads to local optimality, where improvements in one module do not translate into global system performance or security guarantees. Second, system modules are largely isolated. Application logic, model selection, resource scheduling, and security enforcement are often handled by separate subsystems or even different organizational units. As a result, cross-layer coordination is weak, making it difficult to adapt the system to new financial scenarios or regulatory requirements without extensive re-engineering. Third, security is usually implemented as an add-on rather than an architectural primitive. Privacy protection, trustworthy computation, and compliance auditing are typically appended to existing pipelines, creating trade-offs between efficiency, scalability, and trustworthiness. Importantly, many existing digital finance systems cannot be directly compared one-to-one

Table 5. Comparison Between $\mathcal{F}$AMEπ and Existing Digital Finance Architectures

Dimension	**Existing Digital Finance Architectures**	**$\mathcal{F}$AMEπ**
Architectural Goal	Optimize specific applications or system layers	Achieve system-level optimization across the full stack
Design Paradigm	Patchwork integration of independent modules	Co-designed, tightly coupled full-stack architecture
Application Scope	Single or limited scenarios (e.g., trading, fraud)	Full financial scenarios (ToC, ToB, ToG)
Module Interaction	Loosely coupled, often isolated	Unified and supervised by Module $\mathcal{F}$
Optimization Strategy	Local optimization within modules	Cross-layer full-element aggregation optimization
Security Design	Add-on mechanisms (privacy, encryption, auditing)	Inherent architectural primitive via Module E and Module π
Data Usage Mode	Data-centric (data moved to computility)	Data not moving, computility/model moving
Scalability	Task-level or throughput scalability	Scenario-level and stakeholder-level scalability
Adaptability	Require re-engineering for new scenarios	Naturally extensible via application semantic parsing
Global Optimality	Not guaranteed	Explicitly targeted by architectural design

with $\mathcal{F}$AMEπ, because they do not aim to provide a unified full-stack architecture. Instead, they focus on optimizing specific layers (e.g., data platforms or model services), leaving cross-layer integration largely implicit.

$\mathcal{F}$AMEπ addresses these limitations by proposing a co-designed full-stack system architecture, in which Module A, M, E, π, and $\mathcal{F}$ are explicitly integrated. Rather than assembling independent modules, $\mathcal{F}$AMEπ enables system-level intelligence through intentional cross-layer coupling. Specifically, $\mathcal{F}$AMEπ introduces: Module A as a full-scenario parser for user needs, providing scenario-level semantic understanding rather than task-specific triggers; Module M as a model library, offering suitable model combinations to solve user problems; Module E as an explicit theoretical layer that jointly governs data, algorithms, and computility, enabling full-element aggregation optimization and trustworthy security by design; Module π that executes computation according to element-resolved requirements, rather than static or heuristic resource allocation; Module $\mathcal{F}$ as a unified control and coordination layer, eliminating uncontrolled interactions among modules. As a result, $\mathcal{F}$AMEπ transforms digital finance systems from task-oriented pipelines into a scenario-oriented, security-inherent, and globally optimized architecture, capable of supporting heterogeneous applications across ToC, ToB, and ToG simultaneously.

A comparison between $\mathcal{F}$AMEπ and existing digital finance architectures is shown in Table 5. In short, while existing digital finance systems excel at solving isolated problems, they lack the architectural foundation to support secure, scalable, and cross-scenario digital finance. $\mathcal{F}$AMEπ fills this gap by providing a full-stack, architecture-centric solution, overcoming the intrinsic limitations of patchwork solutions and isolated modules. This positions $\mathcal{F}$AMEπ as a practical and extensible blueprint for next-generation digital finance systems rather than a task-specific platform.

4 Conclusion

We propose a novel taxonomy for digital finance research, comprising five dimensions that can position each digital finance study. Based on this framework, we introduce $\mathcal{F}$AMEπ. The proposed $\mathcal{F}$AMEπ is a practical full-stack system architecture designed to empower intelligent and secure digital finance. It integrates multiple dimensions, including A (Application), M (Model), E (Element), and π (Platform Infrastructure), to deliver powerful capabilities for diverse financial task solving. By supporting both vertical optimization of financial operations and horizontal expansion across multi-scenario applications, $\mathcal{F}$AMEπ enables comprehensive coverage of functional and security needs throughout financial business processes. It provides governments, enterprises, and individual users with full-scene, end-to-end solutions for decision-making, prediction, management, and innovation in finance. Through its full-stack technological framework, $\mathcal{F}$AMEπ realizes accurate task execution, real-time information interaction, and adaptive system optimization, thereby ensuring the efficiency, security, and sustainability of digital finance ecosystems.

Conflicts of interest

The authors declare that they have no conflict of interest.

Data availability statement

No data are associated with this article.

Author contribution statement

Cheng Wang and Changjun Jiang designed the research. Cheng Wang and Wenjing Yang constructed the system architecture of $\mathcal{F}$AMEπ and wrote the paper. Hao Tang and Xue Chen provided valuable suggestions for revising the paper. All authors read and approved the final manuscript.

Acknowledgments

We thank the anonymous reviewers for their helpful comments.

Funding

This work was supported in part by the National Key Research and Development Program of China under Grant 2025YFB3003502, in part by the National Natural Science Foundation of China (NSFC) under Grant 62372328 and Grant 72342026, in part by the Fundamental Research Funds for the Central Universities under Grant 22120240357 and Grant 2024-1-ZD-04, in part by the Key Laboratory of Computing Power Network and Information Security, Ministry of Education under Grant 2024ZD001, and in part by the Leadership Project under the Eastern Talent Program.

References

[1] Arner D W, Barberis J, Buckley R P. The evolution of fintech: A new post-crisis paradigm. Geo. J. Int'l L., 2015. **47**: 1271.

[2] Philippon T. The fintech opportunity. Technical report, National Bureau of Economic Research, 2016.

[3] Hasan M M, Popp J, Oláh J. Current landscape and influence of big data on finance. Journal of Big Data, 2020. **7**: 21.

[4] Milana C, Ashta A. Artificial intelligence techniques in finance and financial markets: a survey of the literature. Strategic Change, 2021. **30**: 189–209.

[5] Nutalapati P. A review on cloud computing in finance-transforming financial services in the digital age. International Research Journal of Engineering & Applied Sciences| Irjeas. org, 2024. **12**: 35–45.

[6] Javaid M, Haleem A, Singh R P, et al. A review of blockchain technology applications for financial services. BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 2022. **2**: 100073.

[7] Chen M, Mao S, Liu Y. Big data: A survey. Mobile Networks and Applications, 2014. **19**: 171–209.

[8] Karnati R. Ai-driven financial innovation: Trends, challenges, and opportunities. International Journal on Science and Technology. https://doi.org/10.71097/ijsat. v16. i2, 2025. **4935**.

[9] Swan M. Blockchain: Blueprint for a new economy. O'Reilly Media, Inc., 2015.

[10] Gomber P, Kauffman R J, Parker C, et al. On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. Journal of Management Information Systems, 2018. **35**: 220–265.

[11] Melnychuk A. Features of the financial mechanism of the enterprise in the conditions of digital transformation. Ekonomichnyy Analiz, 2024. **34**: 106–114.

[12] Risman A, Mulyana B, Silvatika B, et al. The effect of digital finance on financial stability. Management Science Letters, 2021. **11**: 1979–1984.

[13] Allen F, Gu X, Jagtiani J. A survey of fintech research and policy discussion. Review of Corporate Finance, 2021. **1**: 259–339.

[14] Khattak B H A, Shafi I, Khan A S, et al. A systematic survey of ai models in financial market forecasting for profitability analysis. Ieee Access, 2023. **11**: 125359–125380.

[15] Moro S, Cortez P, Rita P. Business intelligence in banking: A literature analysis from 2002 to 2013 using text mining and latent dirichlet allocation. Expert Systems with Applications, 2015. **42**: 1314–1324.

[16] West J, Bhattacharya M. Intelligent financial fraud detection: a comprehensive review. Computers & Security, 2016. **57**: 47–66.

[17] Ngai E W, Hu Y, Wong Y H, et al. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 2011. **50**: 559–569.

[18] Cochrane J H, Piazzesi M. Bond risk premia. American Economic Review, 2005. **95**: 138–160.

[19] Lee C, Huang S H, Chen C T. Poisoning attacks against security-aware federated recommendation system. In: International Conference on Machine Learning and Soft Computing. Springer, 301–313.

[20] Ye C, Ou H, Basile V, et al. The effect of uncertainty index based on sparse method on volatility prediction of stock market. Expert Systems with Applications, 2025: 128208.

[21] Lee I, Shin Y J. Fintech: Ecosystem, business models, investment decisions, and challenges. Business Horizons, 2018. **61**: 35–46.

[22] Xu R, Baracaldo N, Joshi J. Privacy-preserving machine learning: Methods, challenges and directions. arXiv preprint arXiv:2108.04417, 2021.

[23] Xu L D, Duan L. Big data for cyber physical systems in industry 4.0: a survey. Enterprise Information Systems, 2019. **13**: 148–169.

[24] Pum M. Bridging the gap data engineers and ai model deployment, 2025.

[25] Jiang C, Ding Z, Yu J, et al. Cabin computing (in chinese). Sci Sin Inform, 2021. **51**: 1233–1254.

[26] Jiang C. Computing power network and trading risk control. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2023. **35**: 1–7.

[27] Gomber P, Koch J A, Siering M. Digital finance and fintech: current research and future research directions. Journal of Business Economics, 2017. **87**: 537–580.

[28] Ozili P K. Digital finance research and developments around the world: a literature review. International Journal of Business Forecasting and Marketing Intelligence, 2023. **8**: 35–51.

[29] Sun N, Zhang Y, Zhang F. How to translate "computility" into english? Communications of China Computer Federation (CCCF), 2022. **18**: 87.

[30] Silber W L. The economic role of financial futures. Salomon Brothers Center for the Study of Financial Institutes, Graduate School of Business Administration, 1985.

[31] Balaji K. Revolutionizing high-frequency trading: The impacts of financial technology and data science innovations. Machine Learning and Modeling Techniques in Financial Data Science, 2025: 103–124.

[32] Dunbar F C, Dunbar F C. Fraud on the market meets behavioral finance. Del. j. Corp. L., 2006. **31**: 455.

[33] Fletcher G G S. Macroeconomic consequences of market manipulation. Law & Contemp. Probs., 2020. **83**: 123.

[34] Li Y, Wang S, Wei Y, et al. A new hybrid vmd-icss-bigru approach for gold futures price forecasting and algorithmic trading. IEEE Transactions on Computational Social Systems, 2021. **8**: 1357–1368.

[35] Gong X, Liu Y, Wang X. Dynamic volatility spillovers across oil and natural gas futures markets based on a time-varying spillover method. International Review of Financial Analysis, 2021. **76**: 101790.

[36] Gu Q, Chang Y, Xiong N, et al. Forecasting nickel futures price based on the empirical wavelet transform and gradient boosting decision trees. Applied Soft Computing, 2021. **109**: 107472.

[37] Liu J, Zhang Z, Yan L, et al. Forecasting the volatility of eua futures with economic policy uncertainty using the garch-midas model. Financial Innovation, 2021. **7**: 1–19.

[38] Deng S, Zhu Y, Duan S, et al. High-frequency forecasting of the crude oil futures price with multiple timeframe predictions fusion. Expert Systems with Applications, 2023. **217**: 119580.

[39] Liu M, Liu X, Jia W, et al. The trading strategy of inflection point futures analysis based on afs theory. In: 2020 39th Chinese Control Conference (CCC). IEEE, 2170–2175.

[40] Du Y, Liu X, Jia W, et al. A new construction method of futures trading strategy construction based on afs theory. In: 2020 39th Chinese Control Conference (CCC). IEEE, 6420–6425.

[41] Huang W, Wang H, Qin H, et al. Convolutional neural network forecasting of european union allowances futures using a novel unconstrained transformation method. Energy Economics, 2022. **110**: 106049.

[42] Liwang M, Gao Z, Wang X. Let's trade in the future! a futures-enabled fast resource trading mechanism in edge computing-assisted uav networks. IEEE Journal on Selected Areas in Communications, 2021. **39**: 3252–3270.

[43] Xu K, Niu H. Do eemd based decomposition-ensemble models indeed improve prediction for crude oil futures prices? Technological Forecasting and Social Change, 2022. **184**: 121967.

[44] Duan Y, Wang L, Zhang Q, et al. Factorvae: A probabilistic dynamic factor model based on variational autoencoder for predicting cross-sectional stock returns. In: Proceedings of the AAAI Conference on Artificial Intelligence. **volume 36**, 4468–4476.

[45] Yang L, Li J, Dong R, et al. Numhtml: Numeric-oriented hierarchical transformer model for multi-task financial forecasting. In: Proceedings of the AAAI Conference on Artificial Intelligence. **volume 36**, 11604–11612.

[46] Han K M, Park S W, Lee S. Anti-fraud in international supply chain finance: Focusing on moneual case. Journal of Korea Trade, 2020. **24**: 59–81.

[47] Alexander C, Cumming D. Corruption and Fraud in financial markets: Malpractice, Misconduct and Manipulation. John Wiley & Sons, 2022.

[48] Karpoff J M. The future of financial fraud. Journal of Corporate Finance, 2021. **66**: 101694.

[49] Wang C, Chai S, Zhu H, et al. Caesar: An online payment anti-fraud integration system with decision explainability. IEEE Transactions on Dependable and Secure Computing, 2022. **20**: 2565–2577.

[50] Wang C. The behavioral sign of account theft: Realizing online payment fraud alert. In: Proceedings of the Twenty-Ninth International Conference on International Joint Conferences on Artificial Intelligence. 4511–4618.

[51] Lai Y, Zhu Y, Fan W, et al. Towards adversarially robust recommendation from adaptive fraudster detection. IEEE Transactions on Information Forensics and Security, 2023.

[52] Hu S, Zhang Z, Luo B, et al. Bert4eth: A pre-trained transformer for ethereum fraud detection. In: Proceedings of the ACM Web Conference 2023. 2189–2197.

[53] Li Z, Wang H, Zhang P, et al. Live-streaming fraud detection: A heterogeneous graph neural network approach. In: Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining. 3670–3678.

[54] Liu C, Sun L, Ao X, et al. Intention-aware heterogeneous graph attention networks for fraud transactions detection. In: Proceedings of the 27th ACM SIGKDD conference on knowledge discovery & data mining. 3280–3288.

[55] Zheng W, Yan L, Gou C, et al. Federated meta-learning for fraudulent credit card detection. In: Proceedings of the Twenty-Ninth International Conference on International Joint Conferences on Artificial Intelligence. 4654–4660.

[56] Cheng D, Xiang S, Shang C, et al. Spatio-temporal attention-based neural network for credit card fraud detection. In: Proceedings of the AAAI Conference on Artificial Intelligence. **volume 34**, 362–369.

[57] Xiang S, Zhu M, Cheng D, et al. Semi-supervised credit card fraud detection via attribute-driven graph representation. In: Proceedings of the AAAI Conference on Artificial Intelligence. **volume 37**, 14557–14565.

[58] Xu F, Wang N, Wu H, et al. Revisiting graph-based fraud detection in sight of heterophily and spectrum. In: Proceedings of the AAAI Conference on Artificial Intelligence. **volume 38**, 9214–9222.

[59] Cheng D, Wang X, Zhang Y, et al. Graph neural network for fraud detection via spatial-temporal attention. IEEE Transactions on Knowledge and Data Engineering, 2020. **34**: 3800–3813.

[60] Abi Din Z, Venugopalan H, Lin H, et al. Doing good by fighting fraud: Ethical anti-fraud systems for mobile payments. In: 2021 IEEE Symposium on Security and Privacy (SP). IEEE, 1623–1640.

[61] Chen C, Lin K, Rudin C, et al. A holistic approach to interpretability in financial lending: Models, visualizations, and summary-explanations. Decision Support Systems, 2022. **152**: 113647.

[62] Botha A, Beyers C, De Villiers P. Simulation-based optimisation of the timing of loan recovery across different portfolios. Expert Systems with Applications, 2021. **177**: 114878.

[63] Song Y, Wang Y, Ye X, et al. Multi-view ensemble learning based on distance-to-model and adaptive clustering for imbalanced credit risk assessment in p2p lending. Information Sciences, 2020. **525**: 182–204.

[64] Song Y, Wang Y, Ye X, et al. Loan default prediction using a credit rating-specific and multi-objective ensemble learning scheme. Information Sciences, 2023. **629**: 599–617.

[65] Xu B, Shen H, Sun B, et al. Towards consumer loan fraud detection: Graph neural networks with role-constrained conditional random field. In: Proceedings of the AAAI Conference on Artificial Intelligence. **volume 35**, 4537–4545.

[66] Błaszczyński J, de Almeida Filho A T, Matuszyk A, et al. Auto loan fraud detection using dominance-based rough set approach versus machine learning methods. Expert Systems with Applications, 2021. **163**: 113740.

[67] Lu Z, Li T, Zhang J, et al. Risqnet: Rescuing smes from financial shocks with a novel networked-loan risk assessment, 2024.

[68] Yang G, Liu X, Li B. Anti-money laundering supervision by intelligent algorithm. Computers & Security, 2023. **132**: 103344.

[69] Cheng D, Ye Y, Xiang S, et al. Anti-money laundering by group-aware deep graph learning. IEEE Transactions on Knowledge and Data Engineering, 2023. **35**: 12444–12457.

[70] Jensen R I T, Iosifidis A. Qualifying and raising anti-money laundering alarms with deep learning. Expert Systems with Applications, 2023. **214**: 119037.

[71] Segovia-Vargas M J, et al. Money laundering and terrorism financing detection using neural networks and an abnormality indicator. Expert Systems with Applications, 2021. **169**: 114470.

[72] Li X, Liu S, Li Z, et al. Flowscope: Spotting money laundering based on graphs. In: Proceedings of the AAAI Conference on Artificial Intelligence. **volume 34**, 4731–4738.

[73] Song J, Zhang S, Zhang P, et al. Illicit social accounts? anti-money laundering for transactional blockchains. IEEE Transactions on Information Forensics and Security, 2024.

[74] Du H, Shen M, Sun R, et al. Malicious transaction identification in digital currency via federated graph deep learning. In: IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 1–6.

[75] Alexandre C R, Balsa J. Incorporating machine learning and a risk-based strategy in an anti-money laundering multiagent system. Expert Systems with Applications, 2023. **217**: 119500.

[76] Chai Z, Yang Y, Dan J, et al. Towards learning to discover money laundering sub-network in massive transaction network. In: Proceedings of the AAAI Conference on Artificial Intelligence. **volume 37**, 14153–14160.

[77] Altman E, Blanuša J, Von Niederhäusern L, et al. Realistic synthetic financial transactions for anti-money laundering models. Advances in Neural Information Processing Systems, 2024. **36**.

[78] Li N, Gao C, Li M, et al. Econagent: large language model-empowered agents for simulating macroeconomic activities. In: Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers). 15523–15536.

[79] Aras S, Lisboa P J. Explainable inflation forecasts by machine learning models. Expert Systems with Applications, 2022. **207**: 117982.

[80] Miranda-Agrippino S, Ricco G. The transmission of monetary policy shocks. American Economic Journal: Macroeconomics, 2021. **13**: 74–107.

[81] Gorodnichenko Y, Pham T, Talavera O. The voice of monetary policy. American Economic Review, 2023. **113**: 548–584.

[82] Jordà Ò, Singh S R, Taylor A M. The long-run effects of monetary policy. Technical report, National Bureau of Economic Research, 2020.

[83] Wang Y, Whited T M, Wu Y, et al. Bank market power and monetary policy transmission: Evidence from a structural estimation. The Journal of Finance, 2022. **77**: 2093–2141.

[84] Zhu H, Liu S Y, Zhao P, et al. Forecasting asset dependencies to reduce portfolio risk. In: Proceedings of the AAAI Conference on Artificial Intelligence. **volume 36**, 4397–4404.

[85] Shah A, Paturi S, Chava S. Trillion dollar words: A new financial dataset, task & market analysis. arXiv preprint arXiv:2305.07972, 2023.

[86] Omowole B M, Urefe O, Mokogwu C, et al. Integrating fintech and innovation in microfinance: Transforming credit accessibility for small businesses. International Journal of Frontline Research and Reviews, 2024. **3**: 090–100.

[87] Aripin Z, Wibowo L A, Ariyanti M. Funding liquidity dynamics and its influence on bank lending growth: A review of the indonesian banking context. Journal of Economics, Accounting, Business, Management, Engineering and Society, 2024. **1**: 1–18.

[88] Van Gestel T, Baesens B. Credit Risk Management: Basic concepts: Financial risk components, Rating analysis, models, economic and regulatory capital. OUP Oxford, 2008.

[89] BK M, Ramasubramanian V. Anti money laundering system in detecting and preventing money laundering activities: A systematic review. Journal of Money Laundering Control, 2025. **28**: 385–407.

[90] Levi M, Reuter P. Money laundering. Crime and justice, 2006. **34**: 289–375.

[91] Kumar R. The impact of monetary policy on economic growth. International Journal of Exploring Emerging Trends in Engineering, 2023. **9**: 30–38.

[92] Dexu H, Wenlong M. Fiscal decentralization, financial decentralization and macroeconomic governance. China Economist, 2022. **17**: 84–105.

[93] Dilaver Ö, Calvert Jump R, Levine P. Agent-based macroeconomics and dynamic stochastic general equilibrium models: Where do we go from here? Journal of Economic Surveys, 2018. **32**: 1134–1159.

[94] Lütkepohl H, et al. Econometric analysis with vector autoregressive models. Wiley Online Library, 2009.

[95] Ye Z, Qin Y, Xu W. Financial risk prediction with multi-round q&a attention network. In: IJCAI. 4576–4582.

[96] Sun J, Li H, Fujita H, et al. Class-imbalanced dynamic financial distress prediction based on adaboost-svm ensemble combined with smote and time weighting. Information Fusion, 2020. **54**: 128–144.

[97] Qin Y, Yang Y. What you say and how you say it matters: Predicting stock volatility using verbal and vocal cues. In: Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics. 390–401.

[98] Wang W Y, Hua Z. A semiparametric gaussian copula regression model for predicting financial risks from earnings calls. In: Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers). 1155–1165.

[99] Chen X, Long Z. E-commerce enterprises financial risk prediction based on fa-pso-lstm neural network deep learning model. Sustainability, 2023. **15**: 5882.

[100] Park S, Yang J S. Machine learning models based on bubble analysis for bitcoin market crash prediction. Engineering Applications of Artificial Intelligence, 2024. **135**: 108857.

[101] Lee C H L, Liu A, Chen W S. Pattern discovery of fuzzy time series for financial prediction. IEEE Transactions on Knowledge and data Engineering, 2006. **18**: 613–625.

[102] Lux T, Marchesi M. Scaling and criticality in a stochastic multi-agent model of a financial market. Nature, 1999. **397**: 498–500.

[103] Ozgur O, Yilanci V, Ozbugday F C. Detecting speculative bubbles in metal prices: Evidence from gsadf test and machine learning approaches. Resources Policy, 2021. **74**: 102306.

[104] Chauhan G S. Mediating role of profitability relating financial leverage and stock returns. International Journal of Emerging Markets, 2024. **19**: 3459–3482.

[105] Claassen B, Dam L, Heijnen P. Corporate financing policies, financial leverage, and stock returns. The North American Journal of Economics and Finance, 2023. **68**: 101992.

[106] Sawhney R, Agarwal S, Wadhwa A, et al. Exploring the scale-free nature of stock markets: Hyperbolic graph learning for algorithmic trading. In: Proceedings of the Web Conference 2021. 11–22.

[107] Gan C, Hu B, Huang B, et al. Which matters most in making fund investment decisions? a multi-granularity graph disentangled learning framework. In: Proceedings of the 46th International ACM SIGIR Conference on Research and Development in Information Retrieval. 2516–2520.

[108] Ye Y, Pei H, Wang B, et al. Reinforcement-learning based portfolio management with augmented asset movement prediction states. In: Proceedings of the AAAI Conference on Artificial Intelligence. **volume 34**, 1112–1119.

[109] Liang X, Cheng D, Yang F, et al. F-hmtc: Detecting financial events for investment decisions based on neural hierarchical multi-label text classification. In: IJCAI. 4490–4496.

[110] Li M, Zhou J, Yu L, et al. A rule-based decision system for financial applications. In: 2023 IEEE 39th International Conference on Data Engineering (ICDE). IEEE, 3535–3548.

[111] Rivera-Castro R, Burnaev E. Causalysis: Causal machine learning for real-estate investment decisions. In: 2021 IEEE 8th International Conference on Data Science and Advanced Analytics (DSAA). IEEE, 1–3.

[112] Yu Y, Yao Z, Li H, et al. Fincon: A synthesized llm multi-agent system with conceptual verbal reinforcement for enhanced financial decision making. Advances in Neural Information Processing Systems, 2025. **37**: 137010–137045.

[113] Amrouni S, Moulin A, Vann J, et al. Abides-gym: gym environments for multi-agent discrete event simulation and application to financial markets. In: Proceedings of the Second ACM International Conference on AI in Finance. 1–9.

[114] Shavandi A, Khedmati M. A multi-agent deep reinforcement learning framework for algorithmic trading in financial markets. Expert Systems with Applications, 2022. **208**: 118124.

[115] Huang Y, Zhou C, Cui K, et al. A multi-agent reinforcement learning framework for optimizing financial trading strategies based on timesnet. Expert Systems with Applications, 2024. **237**: 121502.

[116] Wang X, Ma G Q, Eden A, et al. Platform behavior under market shocks: A simulation framework and reinforcement-learning based study. In: Proceedings of the ACM Web Conference 2023. 3592–3602.

[117] Nokhiz P, Ruwanpathirana A K, Patwari N, et al. Agent-based simulation of decision-making under uncertainty to study financial precarity. In: Pacific-Asia Conference on Knowledge Discovery and Data Mining. Springer, 43–56.

[118] Kaur S, Smiley C, Gupta A, et al. Refind: Relation extraction financial dataset. In: Proceedings of the 46th International ACM SIGIR Conference on Research and Development in Information Retrieval. 3054–3063.

[119] Zhu J, Li J, Wen Y, et al. Benchmarking large language models on cflue–a chinese financial language understanding evaluation dataset. arXiv preprint arXiv:2405.10542, 2024.

[120] Li J, Yang L, Smyth B, et al. Maec: A multimodal aligned earnings conference call dataset for financial risk prediction. In: Proceedings of the 29th ACM International Conference on Information & Knowledge Management. 3063–3070.

[121] Chen J, Zhou P, Hua Y, et al. Fintextqa: A dataset for long-form financial question answering. arXiv preprint arXiv:2405.09980, 2024.

[122] Chen Z, Chen W, Smiley C, et al. Finqa: A dataset of numerical reasoning over financial data. arXiv preprint arXiv:2109.00122, 2021.

[123] Reddy V, Koncel-Kedziorski R, Lai V D, et al. Docfinqa: A long-context financial reasoning dataset. arXiv preprint arXiv:2401.06915, 2024.
[124] Zhao Y, Liu H, Long Y, et al. Financemath: Knowledge-intensive math reasoning in finance domains. arXiv preprint arXiv:2311.09797, 2023.
[125] Lyua S, Jiao Z. Optimization of financial asset allocation and risk management strategies combining internet of things and clustering algorithms. IEEE Internet of Things Journal, 2024.
[126] Deng Y, Lei W, Zhang W, et al. Pacific: towards proactive conversational question answering over tabular and textual data in finance. arXiv preprint arXiv:2210.08817, 2022.
[127] Luo B, Zhang Z, Wang Q, et al. Ai-powered fraud detection in decentralized finance: A project life cycle perspective. ACM Computing Surveys, 2024. **57**: 1–38.
[128] Hou L, Bi G, Guo Q. An improved sparrow search algorithm optimized lightgbm approach for credit risk prediction of smes in supply chain finance. Journal of Computational and Applied Mathematics, 2025. **454**: 116197.
[129] Sang B. Application of genetic algorithm and bp neural network in supply chain finance under information sharing. Journal of Computational and Applied Mathematics, 2021. **384**: 113170.
[130] Tran D T, Iosifidis A, Kanniainen J, et al. Temporal attention-augmented bilinear network for financial time-series data analysis. IEEE Transactions on Neural Networks and Learning Systems, 2018. **30**: 1407–1418.
[131] Blasco T, Sánchez J S, García V. A survey on uncertainty quantification in deep learning for financial time series prediction. Neurocomputing, 2024. **576**: 127339.
[132] Liu Q, Luo Y, Wu S, et al. Rmt-net: Reject-aware multi-task network for modeling missing-not-at-random data in financial credit scoring. IEEE Transactions on Knowledge and Data Engineering, 2022. **35**: 7427–7439.
[133] Yang L, Ma Y, Zhang Y. Measuring consistency in text-based financial forecasting models. arXiv preprint arXiv:2305.08524, 2023.
[134] Ge W, Lalbakhsh P, Isai L, et al. Neural network–based financial volatility forecasting: A systematic review. ACM Computing Surveys (CSUR), 2022. **55**: 1–30.
[135] Nazareth N, Reddy Y V R. Financial applications of machine learning: A literature review. Expert Systems with Applications, 2023. **219**: 119640.
[136] Mandal P K, Thakur M. Higher-order moments in portfolio selection problems: A comprehensive literature review. Expert Systems with Applications, 2024. **238**: 121625.
[137] Olorunnimbe K, Viktor H. Deep learning in the stock market—a systematic survey of practice, backtesting, and applications. Artificial Intelligence Review, 2023. **56**: 2057–2109.
[138] Tetlock P C. Information transmission in finance. Annu. Rev. Financ. Econ., 2014. **6**: 365–384.
[139] Monteiro A M, Santos A A. Parallel computing in finance for estimating risk-neutral densities through option prices. Journal of Parallel and Distributed Computing, 2023. **173**: 61–69.
[140] Inggs G, Thomas D B, Luk W. A domain specific approach to high performance heterogeneous computing. IEEE Transactions on Parallel and Distributed Systems, 2016. **28**: 2–15.
[141] Zhu X, Ma F, Ding F, et al. A low-latency edge computation offloading scheme for trust evaluation in finance-level artificial intelligence of things. IEEE Internet of Things Journal, 2023. **11**: 114–124.
[142] Herman D, Googin C, Liu X, et al. Quantum computing for finance. Nature Reviews Physics, 2023. **5**: 450–465.
[143] Orús R, Mugel S, Lizaso E. Quantum computing for finance: Overview and prospects. Reviews in Physics, 2019. **4**: 100028.
[144] Saba T, Haseeb K, Rehman A, et al. Blockchain-enabled intelligent iot protocol for high-performance and secured big financial data transaction. IEEE Transactions on Computational Social Systems, 2023. **11**: 1667–1674.
[145] Li K, Mei J, Li K. A fund-constrained investment scheme for profit maximization in cloud computing. IEEE Transactions on Services Computing, 2016. **11**: 893–907.
[146] Mann Z Á, Metzger A, Prade J, et al. Cost-optimized, data-protection-aware offloading between an edge data center and the cloud. IEEE Transactions on Services Computing, 2022. **16**: 206–220.
[147] Deng Y. Construction of a digital platform for enterprise financial management based on visual processing technology. Scientific Programming, 2022. **2022**: 7666110.
[148] Shi W, Long S q, Li Y. The risk analysis of digital inclusive financial platform using deep learning approach. Journal of Information Science & Engineering, 2024. **40**.
[149] Zhang X, Chen P, You C, et al. An industrial digital financial application platform based on privacy computing. In: Proceedings of the 2024 the 12th International Conference on Information Technology (ICIT). 25–30.
[150] Abgaryan A, Sharma U. Intralayer: A platform of digital finance platforms. arXiv preprint arXiv:2412.07348, 2024.
[151] Luo Y. Financial data security management method and edge computing platform based on intelligent edge computing and big data. IETE Journal of Research, 2023. **69**: 5187–5195.
[152] Wang T, Tobias G R. Research on intelligent optimization mechanisms of financial process modules through machine learning-enhanced collaborative systems in digital finance platforms. Future Technology, 2025. **4**: 240–254.
[153] Chen H. Construction of a novel digital platform for smart financial talent training under the big data environment. In: 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS). IEEE, 569–572.
[154] Liao Y, Gou Y, Liu Z, et al. Analysis and design of financial wealth management platform based on cloud edge collaboration. In: 2024 3rd International Conference on Artificial Intelligence, Internet of Things and Cloud Computing Technology (AIoTC). IEEE, 165–168.
[155] Yu H. Research on the construction of enterprise financial sharing platform in the background of cloud computing. In: Proceedings of the 2025 4th International Conference on Cyber Security, Artificial Intelligence and the Digital Economy. 9–13.
[156] Li Q. Design of intelligent financial sharing platform driven by consensus mechanism under mobile edge computing and accounting transformation. International Journal of Data Mining and Bioinformatics, 2024. **28**: 426–438.

[157] Wang C, Wang C, Zeng S, et al. Advanced digital simulation for financial market dynamics: A case of commodity futures. arXiv preprint arXiv:2503.20787, 2025.

[158] Wang C, Wang C, Zhang W, et al. Next-generation simulation illuminates scientific problems of organised complexity. arXiv preprint arXiv:2401.09851, 2024.

[159] Wang C, Wang Y, Li Z, et al. Scaling laws of data-driven machine learning models: A survey and taxonomy. Authorea Preprints.

[160] Wu Z, Zhang Z, Zhao Q, et al. Privacy-preserving financial transaction pattern recognition: A differential privacy approach, 2025.

[161] Dhiman S, Nayak S, Mahato G K, et al. Homomorphic encryption based federated learning for financial data security. In: 2023 4th International Conference on Computing and Communication Systems (I3CS). IEEE, 1–6.

[162] Liu T, Wang Z, He H, et al. Efficient and secure federated learning for financial applications. Applied Sciences, 2023. **13**: 5877.

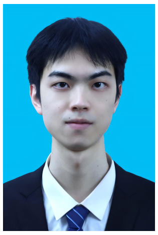
[163] Pamisetty V, Dodda A, Singireddy J, et al. Optimizing digital finance and regulatory systems through intelligent automation, secure data architectures, and advanced analytical technologies. Jeevani and Challa, Kishore, Optimizing Digital Finance and Regulatory Systems Through Intelligent Automation, Secure Data Architectures, and Advanced Analytical Technologies (December 10, 2022), 2022.

[164] Bhatia R. The convergence of cloud and digital financial architecture in enterprise systems. In: International Conference of Global Innovations and Solutions. Springer, 637–656.

[165] Kim K j, Hong S p. Study on digital finance secure architecture based on blockchain. Journal of Advanced Navigation Technology, 2021. **25**: 415–425.

[166] Bhatia R. Digital finance architecture for the public sector: Redesigning us tax and fund distribution systems with fast™ and dfra™. Journal of Computer Science and Technology Studies, 2025. **7**: 1174–1183.

Cheng Wang received a master's degree from the Department of Applied Mathematics at Tongji University, Shanghai, China, in 2006 and a Ph.D. degree from the Department of Computer Science at Tongji University in 2011. He is currently a Professor and the Vice Dean of the School of Computer Science and Technology at Tongji University. His research interests include distributed learning, mobile social networks, and cyberspace security.



Wenjing Yang received a bachelor's degree in Data Science and Big Data Technology at the College of Artificial Intelligence from Nanjing Agricultural University in 2024. He is currently pursuing a Ph.D. degree at the School of Computer Science and Technology at Tongji University in Shanghai, China. His research interests include LLM-based agent and multi-agent simulation.

Hao Tang received his bachelor degree of engineering in the Department of Computer Science and Technology from Chongqing University of Posts and Telecommunications, in 2020, and the Ph.D. degree at the School of Computer Science and Technology at Tongji University, in 2025. He received the Best Paper Award from Security and Safety (S&S) 2024. His research interests include privacy-preserving learning and distributed computing.

Xue Chen received Ph.D. degree in the Department of Computer Science and Technology at Tongji University in 2023. She is currently a postdoctoral researcher at the School of Computer Science and Technology at Tongji University and Brunel University of London. Her research interests include data privacy and machine learning.

Changjun Jiang received a Ph.D. degree from the Institute of Automation, Chinese Academy of Sciences, Beijing, China, in 1995. He is currently the Leader of the Key Laboratory of the Ministry of Education for Embedded System and Service Computing, Tongji University, Shanghai, China. He is also an Honorary Professor with Brunel University London, Uxbridge, England. Dr. Jiang is also an IET Fellow. He is an Academician of the Chinese Academy of Engineering. His research interests include concurrence theory, Petri nets, formal verification of software, cluster, grid technology, intelligent transportation systems, and service-oriented computing.