ISSN: 1813-4890

Research on the application practice of financial digital resilience -- taking Ant Group as an example

Xue Zhou

Management Engineering Department, Anhui Industry Polytechnic, Anhui, China

Abstract

The development of financial technology has accelerated the digital transformation of finance, injected abundant impetus for the high-quality development of the financial industry, and at the same time, it is necessary to prevent possible risks. The intensification of system uncertainty risks will affect business continuity, which puts forward higher security requirements for fintech development and digital transformation. Digital resilience reflects the ability of information systems to continue to operate in a changing environment, continue to withstand threats and shocks, and maintain growth. This paper starts from the definition and characteristics of digital resilience, studies the evaluation and construction of digital resilience system, and looks forward to the development trend, in order to provide reference for financial institutions to ensure the stable operation of information system.

Keywords

Digital toughness, stability, anti-interference.

1. Introduction

The development of financial technology in China is at the leading level in the world, especially the transaction scale of mobile payment and the user scale of online lending, which are in the forefront of the world. Fintech is also an intensive business model. By opening up the internal system process of financial institutions, it simplifies business processes, improves operational efficiency, and reduces the cost of financial services. Combined with big data and operation promotion, it further expands the scope of users and creates more business value. With the increasing scale of sensitive IT support such as "cloud-native and microservices" of financial institutions, and the problems of complex business architecture, high transaction reliability requirements, and long transaction links, whether the facilities of distributed systems can effectively match and interact has become a key factor affecting the stable operation of the system. The continuous guarantee of service delivery under complex IT architecture is faced with great challenges, which puts forward higher requirements for the construction of operation and maintenance platform.

In the past, the disaster recovery capacity building of financial institutions mainly focused on the response to major disaster events and major shutdown events. Today, in complex sensitive architectures, the root causes and points of failure of business disruptions are not as clear as in traditional architectures. Due to the service engine and componentization, the failure of a certain fault is likely to cause secondary disasters that interrupt other services, and the causes of system service interruption become more complex. Traditional emergency and disaster recovery mechanisms, methods and tools are increasingly unable to meet the requirements of continuous service delivery in the cloud native era. Financial institutions hope that the information system can be continued and restored in the "low-frequency and high-loss" major disaster events and major shutdown events, and the service level is not seriously affected in the "high-frequency and low-loss" daily operation and maintenance events, and can ensure that the system continues to update and grow in the changing environment to meet the needs of business development. As a result, the concept of digital resilience has been continually put forward by institutions or organizations to illustrate the capabilities that information systems should have in response to such requirements.

2. Definition and characteristics of digital toughness

2.1. The definition of digital toughness

Digital resilience refers to the ability of information systems to continue to operate in a changing environment, continue to withstand threats and shocks, and maintain growth. Digital resilience is one of the data center business capabilities related to continuous service delivery, built on basic operational capabilities such as configuration management, service governance, state awareness and observability, operational automation, and emergency response. Digital resilience includes the stability of the ability to remain robust, the robustness to external threats, and the ability to adapt to changes in the external environment and keep learning and growing.

2.2. Characteristics of digital toughness

(1) Stability. Stable operation means that the information system can continue to operate when the system internal failure occurs under the condition that the system structure and external environment remain unchanged, that is, the internal anomaly of the system should not cause an unacceptable decline in service quality. To this end, we should identify the weak links in the system, formulate and implement the corresponding strengthening program, and test the strengthening effect. Improved system stability can avoid single point of failure, resist system aging, reasonable inter-service dependency, and elastic scaling based on access pressure.

Since hardware failure is inevitable, the system operating environment should be able to quickly detect, isolate, and replace failed components with redundant capabilities to ensure that component failure does not cause an unacceptable and persistent impact on the service capability of the information system. System aging refers to the gradual decline in the performance of a system over time. In order to ensure the continuous and stable operation of the system, anti-aging tests should be carried out before the information system goes online to check whether the system will be aging under a certain comprehensive operating pressure. Reasonable dependencies between services should be considered in system design. For example, develop emergency plans or disaster recovery plans to reduce losses in the event of service quality decline or service interruption. The information system should be able to fully perceive the change of business or service access pressure, and quickly adjust the resource capacity to realize the elastic scaling of resources.

Robustness. Shock resistance means that the information system can quickly perceive, make decisions and deal with external disturbances, shocks, and even serious catastrophic events while keeping the system structure unchanged, so that the system can maintain a certain quality of service or restore service within the agreed time. At the beginning of the system design, we should analyze the interference that the system may encounter, and make corresponding preparations in advance, take the necessary means to maintain the necessary service capability when the interference occurs, and restore the full service capability of the system after the interference disappears. The application system should have the operation protection ability to sense and respond to external shocks, so as to reduce the impact of external shocks on system operation. These impacts range from cyber attacks or unfriendly access to sudden spikes in traffic to legitimate services.

Adaptability. Adaptability refers to the ability of information systems to adapt to differences in operating environments and deployment configurations in order to operate effectively under different support capabilities and access pressures. To improve the adaptability of application systems to the environment, you can adapt to changes in service requirements, adapt to technological environment upgrades, and provide resources reasonably.

Changes in business requirements are usually the main reason for application system upgrade or reconstruction. Large-scale system upgrade will have a significant impact on system stability, but the change of business environment is usually relatively slow. Organizations should make medium - and long-term plans based on changes in business environment, formulate targeted application system life cycle plans, and complete application system upgrade and reconstruction as planned. The upgrade of the organization's technical architecture directly affects the technical environment in which the application system operates. For the information system, in its life cycle of more than 5 years, the upgrade or replacement of the technical environment is often inevitable. Substitution testing is required when adjusting or changing the technical environment of the application system. Check not only the functional consistency or compatibility of the application system, but also the adaptability of the operation and maintenance capabilities, including monitoring and awareness capabilities, automatic execution capabilities, rights management capabilities, data backup and disaster recovery capabilities, and the support capabilities of the operation and maintenance team. To ensure the service quality of the system during the daily access peak hours, you must determine the service capacity and service capacity of the system, and plan the resource component capacity of the system based on this.

3. Industry practice

Traditional system testing has been difficult to meet the various requirements for the digital resilience of the system. Increasingly complex IT systems and rapid iterative software delivery have brought many challenges and uncertainties to ensure the stability of the system. In order to make the cloud infrastructure better adapt to the complex and changeable operating environment, and continue to provide ultra-large scale and ultra-stable operating performance.

The system stability and anti-interference ability can be guaranteed by introducing the abnormal state (disturbance) of software or hardware into the system actively, creating fault scenarios and determining optimization strategies according to the behavior of the system under various pressures. The application of chaos engineering can verify and evaluate the ability of the system to resist disturbances and maintain normal operation, identify unknown hidden dangers in advance and repair them, so as to ensure the system can better resist out-of-control conditions in the production environment and improve the overall digital toughness of the application system.

Ant Group's business is mostly related to finance, such as Alipay, Huabai and Yu 'e Bao, etc. The amount of funds flowing through Ant's application system every day is very large, and the accuracy of funds (also known as fund security within Ant) has a very high requirement of zero errors. Therefore, the Technical risk Department of Ant Group has built a second-level verification ability of trillions of funds. Be able to spot and stop losses when there is a problem with the correctness of funds online.

In terms of offensive and defensive drills, based on JAVA bytecode technology, it can tamper with the incoming data of a node (application) in the fund link in real time, such as tampering with the amount of the bill paid by Huabai, resulting in the failure phenomenon of inconsistent upstream and downstream fund data (the upstream payment core documents are inconsistent with the downstream payment bill data). In this way, whether the system can find faults in real time is checked. This way is called lossy injection. After finding faults, the fault data needs to be recovered through data correction. In the context of large-scale normal offensive and defensive drills, high-cost lossy injection (high cost of data correction) cannot meet the needs of high-frequency fault injection in normal drills. Therefore, Ant Chaos engineering team innovatively proposed the idea of lossless injection. Lossless injection is designed for the fund prevention and control system, which can effectively test the verification rules without affecting the real data. Currently, lossless injection is one of the core technologies in the normal offensive and defensive drills of fund security.

In addition to offensive and defensive drills, another important practice is financial risk mining, in the ant's huge system scale and complex business logic, there must be a lot of unknown risks, chaos engineering should be able to help the business to discover these unknown risks in advance. To this end, the risk mining capability is built. Based on key technologies such as program analysis, the risk of capital table and capital service can be automatically mined on a large scale, and the data level can be revealed in normal drills, such as how many capital table and capital service there are in a certain business line, how many risk points have been covered by drills, and what is the discovery rate of drills covering these risk points.

4. Conclusion

Under policy guidance and regulatory guidance, the construction standards of data centers in the financial industry are constantly improving. Although large-scale natural disasters remain a major threat to the continuous operation of data centers, the increasing risks of network interruption, cloud service interruption, or local IT failure also pose a serious threat to the ability of data centers to provide continuous services. The concept of digital resilience is aimed at addressing the threats and risks faced during system operation, continuously improving and perfecting various system stability assurance measures, strengthening and continuously verifying the effectiveness of solutions, so that most threats and risks can be resolved through the system's own capabilities, thereby reducing pressure during system operation, reducing reliance on frontline personnel operations, and ensuring the continuous operation of business activities. The gradual improvement and development of the digital resilience thinking system have made the resilience requirements of information systems equally important as their functional requirements.

References

[1] Do FinTech trigger renewable energy use? Evidence from OECD countries[J]. Croutzet Alexandre;Dabbous Amal.Renewable Energy,2021

[2] On the Rise of FinTechs: Credit Scoring Using Digital Footprints[J]. Berg Tobias;Burg Valentin; Gombović Ana;Puri Manju.The Review of Financial Studies,2020

[3] Does bank FinTech reduce credit risk? Evidence from China[J]. Maoyong Cheng;;Yang Qu.Pacific-Basin Finance Journal,2020

[4] Do fintech lenders penetrate areas that are underserved by traditional banks?[J]. Julapa Jagtiani;;Catharine Lemieux.Journal of Economics and Business,2018

[5] Digital Finance and FinTech: current research and future research directions[J]. Peter Gomber;; Jascha-Alexander Koch;;Michael Siering.Journal of Business Economics,2017

[6] Where the Risks Lie: A Survey on Systemic Risk[J]. Benoit Sylvain;Colliard Jean-Edouard;Hurlin Christophe; Pérignon Christophe.Review of Finance,2017

[7] Inclusive finance for inclusive growth and development[J]. Germana Corrado;;Luisa Corrado.Current Opinion in Environmental Sustainability,2017

[8] A financial network perspective of financial institutions' systemic risk contributions[J]. Wei-Qiang Huang;; Xin-Tian Zhuang;;Shuang Yao;;Stan Uryasev.Physica A: Statistical Mechanics and its Applications,2016

[9] The Impact of Internet Banking on the Performance of Romanian Banks: DEA and PCA Approach[J]. Ovidiu Stoica;;Seyed Mehdian;;Alina Sargu.Procedia Economics and Finance,2015

[10] Financial inclusion in India: An axiomatic approach[J]. Satya R. Chakravarty;;Rupayan Pal.Journal of Policy Modeling,2013