University of Amsterdam
Informatics Institute

From Empowering to Motivating

Enhancing Policy Enforcement through Process Design and Incentive Implementation

Xin Zhou

From Empowering to Motivating: Enhancing Policy Enforcement through Process Design and Incentive Implementation

Xin Zhou

Informatics Institute

University of Amsterdam

February, 2024

From Empowering to Motivating: Enhancing Policy Enforcement through Process Design and Incentive Implementation

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
prof. dr. ir. P.P.C.C. Verbeek
ten overstaan van een door het College voor Promoties
ingestelde commissie,
in het openbaar te verdedigen in de Agnietenkapel
op vrijdag 16 februari 2024, te 16.00 uur
door

Xin Zhou
geboren te Hubei, China

Promotiecommisie

Promotors:	Prof. dr. ir. C.T.A.M. de Laat	Universiteit van Amsterdam
	Prof. dr. T.M. van Engers	Universiteit van Amsterdam
Co-promotors:	Dr. A.S.Z. Belloum	Universiteit van Amsterdam
	Prof. dr. S. Klous	Universiteit van Amsterdam
Overige leden:	Prof. dr. R.V. van Nieuwpoort	Universiteit van Amsterdam
	Prof. dr. F. Squazzoni	University of Milan
	Prof. dr. H. Haned	Universiteit van Amsterdam
	Dr. M.H. Lees	Universiteit van Amsterdam
	Dr. Z. Zhao	Universiteit van Amsterdam

Faculteit der Natuurwetenschappen, Wiskunde en Informatica

SIKS Dissertation Series No.2024-08

The research reported in this thesis has been carried out under the auspices of SIKS, the Dutch Research School for Information and Knowledge Systems.

The work described in this thesis has been supported by the Netherlands Organization for Scientific Research in the project Data Logistics for Logistics Data (Grant No.628.009.001); the Dutch Top consortia for Knowledge and Innovation; the Dutch Institute for Advanced Logistics; the Dutch Ministry of Economic Affairs; and the Dutch Commit-to-Data initiative.

Printed and bound by Ridderprint.

ISBN: 978-94-6483-733-9

Abstract

The enforcement of policies plays a crucial role in our daily life, from protecting rights to promoting collaborations. In practice, policies are enforced through designed processes and institutional incentives. Given the distinct focuses and technologies of these two methods, this thesis delves into policy enforcement from a practical and a theoretical dimension respectively.

Part I, which centers on the practical dimension, focuses on empowering (resp. prohibiting) compliant (resp. non-compliant) behaviors through process design, and leveraging appropriate technologies for process realization. This part starts by proposing an approach for enforcing environmental adaptive data sharing policies. This approach is implemented through an integrated environmental adaptive auditing process and an execution process within an infrastructure. Further, to enforce cross-domain workflows, a prototype that employs Petri nets and blockchain technology to orchestrate both on-chain and off-chain tasks is presented. Specifically, this solution incorporates an incentive mechanism via a peer auditing process, enhancing parties' adherence when executing unenforceable off-chain tasks.

Part II, from the theoretical dimension, focuses on motivating (resp. deterring) compliance (resp. non-compliance) through implementing designed institutional incentives. First, for the incentive design stage, a set of comprehensive evaluation criteria are proposed, which consider factors including the promotion of cooperation, sustainability of incentive implementation, and the affluence of both participants and the implementing institution. Subsequently, in the incentive implementation stage, pervasive corruption can significantly hinder the effectiveness of incentives. Real-world solutions often involve external supervision services, such as certification services for validation. To study anti-corruption in incentive implementa-

tion, this thesis develops a game model to analyze how effective external supervision services are in tackling corruption and aiding the implementation of incentives. From these explorations, management suggestions regarding institutional incentive design and implementation are drawn.

Samenvatting

Het handhaven van beleid speelt een cruciale rol in ons dagelijks leven, van het beschermen van rechten tot het bevorderen van samenwerking. In de praktijk wordt beleid gehandhaafd via ontworpen processen en institutionele stimuli. Gezien de verschillende focus en technologieën van deze twee methoden, onderzoekt dit proefschrift de handhaving van beleid vanuit een respectievelijk praktische en theoretische dimensie.

Deel I, gericht op de praktische dimensie, richt zich op het versterken (of verbieden) van conforme (of niet-conforme) gedragingen via procesontwerp en het benutten van geschikte technologieën voor procesrealisatie. Dit deel begint met het voorstellen van een aanpak om situatie-afhankelijke maatregelen over gegevensuitwisseling te handhaven, gerealiseerd door middel van het geïntegreerde, situatie-afhankelijke auditproces en het uitvoeringsproces binnen een infrastructuur. Verder wordt voor het handhaven van inter-domein workflows een prototype gepresenteerd die Petri-netten en blockchaintechnologie inzet om zowel on-chain als off-chain taken te orchestreren. Specifiek omvat deze oplossing een stimuleringsmechanisme via een peer auditproces, wat de naleving van partijen verbetert bij het uitvoeren van niet-afdwingbare off-chain taken.

Deel II daarentegen, vanuit de theoretische dimensie, richt zich op het motiveren (of ontmoedigen) van naleving (of niet-naleving) door de implementatie van ontworpen institutionele stimuli. In dit deel worden eerst uitgebreide evaluatiecriteria voorgesteld voor het ontwerpen van stimuli, die factoren overwegen zoals de bevordering van samenwerking, duurzaamheid van de implementatie van stimuli en de welvaart van zowel deelnemers als de implementerende instelling. Vervolgens kan in de implementatie-stap van stimuli wijdverbreide corruptie de effectiviteit van stimuli aanzienlijk belemmeren. Oplossingen in de echte wereld betrekken vaak externe toezichtdiensten, zoals certificeringsdiensten voor validatie. Om anti-co-

rruptie in de implementatie van stimuli te bestuderen, ontwikkelt dit proefschrift een spelmodel om te analyseren hoe effectief externe toezichtdiensten zijn bij het bestrijden van corruptie en het ondersteunen van de implementatie van stimuli. Uit deze onderzoeken worden managementaanbevelingen afgeleid over ontwerp en implementatie van institutionele stimuli.

Acknowledgments

I never anticipated that the long journey of a PhD could be accomplished so swiftly. When looking backward at the traveled rough road, a profound sense of gratitude wells up. I would like to express my genuine appreciation to all those who have been part of this journey. They have been like gentle candlelight, illuminating the four-year exploration.

I first would like to thank my supervisors, Cees de laat, Tom van Engers, Adam Belloum, and Sander Klous, who granted me the opportunity to pursue my PhD at the University of Amsterdam. Over the past four years, your support and trust gave me the courage to confront challenges. The lessons I learned from you extend beyond knowledge itself; they encompass how to be an honest and independent researcher. For this, I hold deep and enduring sense of gratitude towards you.

I would also like to express special gratitude to my co-authors Reginald Cushing, Ralph Koning, and Mike Lees for our published works; and to my collaborators Fernando Santos and Vítor Vasconcelos for the upcoming works. It is gratifying to work with you. Your exciting insights upon the interconnected knowledge and your open and sincere minds greatly nourished and motivated young researchers. I will always remember the fervor of our discussions and the pure joy of doing research I obtained from them.

To my dear colleagues, Tanjina, Tim, Marco, Damian, and all my peers from CCI group, your staunchest support and encouragement are the best remedy for the inevitable and unbearable delays of positive feedback during a PhD. Your generous praise and triumphant high-fives, whether for a well-prepared presentation, an intricately designed figure, or even a successful formula derivation, wiped off the anxieties and soothed the exhaustion. Reflecting on these moments, even the most resolute heart would soften and feel a sense of warmth.

Of course, I must also acknowledge my amiable friends, Daniela and Mary. Your hospitality has made Amsterdam feel like a second home to me. Hanyu, Wanfang, and Zhijun, thank you for accompanying me through the ups and downs; your empathy doubled the joy and halved the pain. To my cherished family, your unwavering support provided the foundation for my entire PhD journey. Lastly, I want to express my heartfelt gratitude to my partner, Mr. Ling, for healing me with your unconditional acceptance and profound understanding.

I hereby especially thank the entire crew of "Yes Minister". This remarkable sitcom has been my companion over the past four years. The meaningful and humorous dialogues aroused endless joy and resonance. While there are many other artists and writers whose work has touched me deeply, I can hardly list all their names, I truly want to express my appreciation for them. I perceive immense comfort from their splendid works, and gather deep strength from the great deal of effort and dedication invested behind. They prove to me that readers would not only grasp the ideas delivered by the work itself, but also, in a tacit manner, would comprehend all the persistent dedication and absolute sincerity in attaining excellence and beauty, which is the spiritual beacon lighting up paths.

Xin

September 2023

Amsterdam, Netherlands

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Policies have a pervasive influence on all aspects of our daily lives, ranging from international regulations like the General Data Protection Regulation (GDPR) regulating countries and organizations, to community standards of platforms like Weibo or Facebook restricting the behaviors of individual users. These policies establish clear rights and obligations, regulate operations, and clarify prohibitions. However, for policies to be truly effective, proper enforcement is crucial. Without enforcement, policies cannot adequately protect rights, promote trust, or facilitate collaborations.

The enforcement of policies typically involves both constraining operations through process design and encouraging compliant behaviors through institutional incentives [40, 89]. For example, when enforcing community standards, online forums usually design the posting process that leverages machine learning technologies to detect fraudulent or inauthentic accounts, automatically blocking them from posting inappropriate content. At the same time, despite technological advancements, violations can still occur. Various incentives thereby play an important complementary role to technologies in enforcing policies [68], such as warnings, text removal, or even accounts bans [49].

Drawing on this leveraged practical experience, this thesis aims to promote policy enforcement through the combination of technologies and incentives. Leveraging and embedding appropriate technologies helps in designing and realizing processes that enforce operational regulations by constraining non-compliant operations and empowering compliant ones. Meanwhile, employing appropriate incentives can effectively motivate participants to adhere to policies by adjusting the payoff associated with compliant and non-compliant behaviors. Together, these two approaches enhance the overall enforcement of policies.

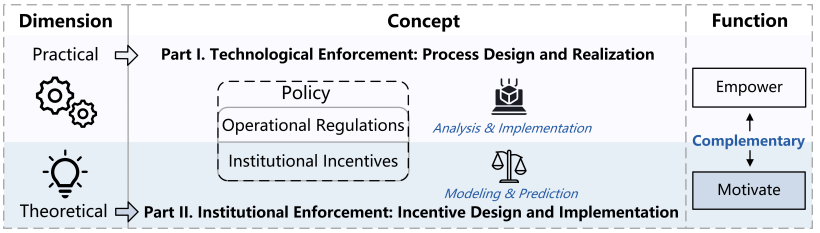


Figure 1-1: The research outline of policy enforcement. This thesis aims to explore measures for enforcing policies from both practical and theoretical dimensions. The practical aspect of this thesis focuses on designing processes to enact the enforcement of operational regulations using technologies. These processes empower compliant behaviors and constrain non-compliant behaviors through the examination of conditions and constraints. Whereas the theoretical aspect focuses on designing and implementing institutional incentives to adjust the expected payoff of compliant and non-compliant behaviors. The goal is to motivate participants towards compliance. These two dimensions are functionally complementary to each other in promoting desired behaviors, including cooperation and compliance.

As Figure 1-1 presents, institutional incentives can be categorized as a distinct class of policies, separate from operational regulations [106, 179]. Operational regulations highlight the procedures, conditions, and explicit constrains for operations, while institutional incentives focus on the consequences of compliant or non-compliant behaviors, which are typically in the form of rewards or punishments [157]. Additionally, it is important to note that the enforcement of institutional incentives relies on human inter-

vention in terms of monitoring and adjudicating, whereas the enforcement of operational regulations can be automated through carefully designed processes.

Given the differences in content focus and implementation formats, the challenges of enforcing these two types of policies are distinct. For operational regulations, the challenge lies in designing appropriate processes that effectively empowers (resp. prohibits) compliant (resp. non-compliant) operations, and subsequently realizing these designed processes by technologies; whereas for institutional incentives, the challenges are designing appropriate incentives to effectively motivate compliance, and overcoming potential obstacles caused by self-interested rule enforcers in incentive implementation.

Thereby, notwithstanding the fact that both types of policies can benefit from the design and realization of comprehensive processes[1], this thesis takes a focused approach for better capturing the main challenges. When referring to process design and realization, the enforced objects focus on the operational regulations. Conversely, when it comes to incentive design and implementation, the emphasis shifts to institutional incentives.

In this focused approach, as summarized in Figure 1-1, the explorations of process design and institutional incentives are identified as two dimensions: the practical dimension and the theoretical dimension. Process design and realization involve engineering analysis and the integration of suitable technologies to effectively meet practical requirements in enforcing operational regulations. In contrast, institutional incentive design and implementation rely on theoretical modeling participants' interaction considering self-interested behaviors, and predicting expected outcomes to ensure that incentives can effectively promote desired behaviors or deter non-compliant behaviors. Based on these two dimensions, this thesis

[1]For instance, to enforce tax policies, tax reporting and payment processes can be designed, empowering companies to comply with tax obligations. Simultaneously, fine process can also be designed to enforce penalties by deducting money from the accounts of tax-evading companies.

develops measures to enhance policy enforcement.

Part I. Technological enforcement: process design and realization

Various technologies have been applied to implement designed processes aimed at enforcing operational regulations. For example, authorization protocols are extensively used to realize the designed data access process which enforces permission-related policies [33]; blockchain and smart contract technologies are employed to realize execution and recording processes when enforcing contractual policies [131, 187]; digital signatures and key management are commonly utilized in the cryptography process to enforce secure communication-related policies [180]; and the previously mentioned machine learning is widely applied in the process of detecting abnormal behaviors to enforce user behavior-related policies [85]. The utilization of these technologies enhances policy enforcement across different fields.

The design of processes and the corresponding selection of technologies depend on the functional requirements of the policies being enforced. For instance, when enforcing data sharing policies, it is necessary to facilitate data sharing among the parties stipulated in the agreement. Consequently, processes such as request checking and execution should be designed. To realize these processes, access control, key management, and technologies related to networking and communication need to be integrated for users identification, request auditing, and compliant requests execution. Hence, analyzing the operational regulations to clarify the concrete functional demands is indispensable for designing necessary processes [134]. This analysis guides the subsequent selection of technologies that shall be embedded. For the convenience of description, the designed processes and their supportive technologies together are denoted as an approach or a solution, which actually enforces the operational regulations.

For this reason, the explorations within Part I are demand-oriented. This

thesis starts from proposing an approach to enforce environmental adaptive data sharing policies that require authorizations for concurrent data requests based on the current environmental condition. It then moves on to developing a solution for enforcing workflows that require a proper choreography of sequential operations/activities involving multiple parties. Since operations in workflows can extend beyond those in data sharing, this workflow enforcement solution expands the scope of enforced operations, and can therefore be regarded as an extension of the approach for data sharing.

Part II. Institutional enforcement: Incentive design and implementation

Incentives can effectively promote compliant behaviors, when they are employed correctly; successful incentives require proper design and rigorous implementation, challenges in these two stages are covered in Part II. Proper design of incentives requires a procedure for modeling the scenario, predicting the outcomes, and evaluating the impact. However, designing scientific evaluation criteria is not easy, any oversight can lead to undesired outcomes. For example, if the cost of the rule enforcer is not considered, over-subsidising might occur, leading to fiscal haemorrhaging to the executor [30]. If the cost of participants is not considered, excessive punishment might be carried out, causing a negative impact on participants and hindering the long-term development of the market [50]. Accordingly, designing comprehensive criteria is critical in designing sustainable and reasonable incentives.

In the implementation stage, there are potential problems that can undermine the effectiveness of incentives. One significant example is pervasive corruption [110, 101]. When incentives are carried out by institutions, participants who engage in non-compliant behaviors may be motivated to bribe the rule enforcers to evade punishment [91, 26]. This can lead to a situation in which participants learn to break rules, and engage in non-compliant behaviors, ultimately leading to the collapse of social norms and

collaborations [91]. Consequently, it is necessary to address corruption to ensure the rigorous implementation of incentives.

Part II of this thesis aims to address problems that arise in both the design and implementation stages of incentives. It first discusses the critical criteria that should be considered in the design stage; and then explores the effects of external supervision services as a possible measure to combat corruption and to ensure effective incentive implementation.

To summarize, the features of the operational regulations and incentives determine their challenges in enforcing. For explicit operational regulations, the hardship lies in designing appropriate processes and selecting the proper technologies to successfully to form a comprehensive solution that empowers compliant operations and restricts non-compliant ones; whereas for human-involved institutional incentives, the difficulties are designing scientific incentives and implementing them rigorously to effectively motivate participants adhering to the policies. Considering these differences, this thesis separately explores the design and realization of processes, and that of incentives. These explorations are correspondingly classified as practical dimension for empowering and theoretical dimension for motivating. These two dimensions are functionally complementary to each other, the combination of which serves for better policy enforcement. The following section lists the concrete research questions in these two dimensions and the leveraged methods for addressing the challenges.

1.1 Research questions and roadmap

This section begins with the introduction of the research questions of Part I and Part II, and their corresponding research methods, followed by an elaboration on the relationship between the research questions. The main information is summarized in Figure 1-2.

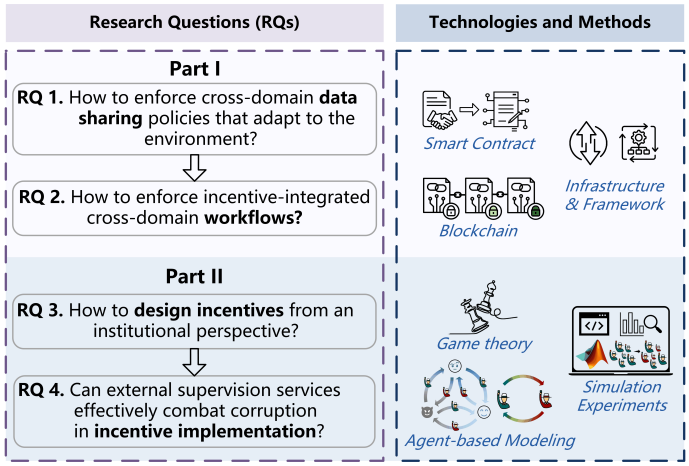


Figure 1-2: Research questions and research roadmap. Part I covers the research questions of how to enforce environmental adaptive data sharing policies, and how to enforce more general operational regulations for cross-domain workflows. The technologies involved in Part I include smart contracts and blockchain. In Part II, issues related to the design and implementation of institutional incentives are discussed. Game theory is applied for modeling, while agent-based modeling and simulation experiments are leveraged for predicting.

The starting point of Part I is to enforce data sharing policies among multiple domains (also known as parties). One of the challenges in data sharing is the trade-off between security and flexibility [125]. While limiting data access as much as possible can enhance security, it may also diminish the value of data sharing and introduce risks. For example, in public incidents, such as fires or stampedes, overly strict or static data sharing policies might hinder the enforcing agency from accessing criti-

cal datasets, which might impede rescue [7]. This highlights the need for flexible and dynamic data sharing policies that can adapt to the actual environment. The enforcement of such environmental adaptive policies calls for an approach that supports environmental sensing in the request checking process and empowers compliant requests in the execution process. This practical demand gives rise to the first research question:

> **RQ 1.** How to enforce cross-domain data sharing policies that adapt to the environment?

By solving **RQ 1**, an approach featuring an auditing layer and a control layer is proposed. The auditing layer handles the request checking process, while the control layer manages the request execution process. These two layers are operationalized by components integrated in a decentralized infrastructure, supporting functions such as environment sensing, broadcasting, communication, and application running.

Moving on from data sharing policies, this thesis further explores the solution for enforcing workflows which contains a sequential tasks with higher variety. One example is the workflows in a supply chain [88, 27], other than the on-chain tasks like data access or data transfer, which can be enforced by blockchain-based smart contracts [98], workflows also involve tasks like product delivery, that must be executed off-chain. This inherent feature of workflows creates opportunities for fraud and undermines trust among parties.

In addition to the challenge brought by the variety of tasks, the designed order of tasks in workflows requires task choreography. This choreography is essential for supporting participants' execution of specified operations at appropriate times. In light of these challenges, the question arises: how to design and realize a comprehensive solution that integrates incentives into workflows to motivate parties to adhere to workflows including off-chain tasks; and meanwhile choreographing such incentive-integrated workflows

among multiple parties? These challenges are solved in the second research question:

> **RQ 2.** How to enforce incentive-integrated cross-domain workflows?

The proposed solution for **RQ 2** leverages smart contracts and hyperledger technology to enforce workflows and integrates peer audit process as incentives. The ordered tasks are choreographed by a designed three-layer architecture. Up to this point, the two research questions and related technologies of Part I have been introduced, and they are summarized in Figure 1-2.

In Part II, there are two research questions that arise in the design and implementation stages of incentives. When designing incentives, determining comprehensive evaluating criteria is challenging. The requirement of effectively promoting compliant behaviors [51] are typically considered. Additionally, when the incentives are executed by a third-party institution, ensuring the sustainable execution of the incentives is vital. As can be expected, if the costs of execution are too high, the institution may face bankruptcy [120]. Furthermore, the affluence of the participants is another important outcome to consider. Excessive punishment may result in the elimination of participants, which is not constructive to the long-term development of the system. The third research question aims to compare incentives based on these aforementioned criteria:

> **RQ 3.** How to design incentives from an institutional perspective?

By addressing **RQ 3**, theoretical analysis and agent-based modeling are applied to predict the outcomes. Specifically, a game model is constructed to predict the cooperation level in the stable state, which contains an incentive executing institution and compliant/non-compliant participants.

Through simulation experiments, the outcomes related to the affluence of the institution and the participants are tracked. By comparing the results of various incentives, management suggestions are derived for incentive design from an institutional perspective.

When incentives are being carried out by institutions, pervasive corruption can impede the successful implementation of incentives[2]. Combating corruption and ensuring rigorous conduction of punishment or reward is important. In the real world, countermeasures such as complaining [159, 13], whistle-blowing, or reporting [185] are provided. These measures serve as an external supervision over the institution, aiming at preventing the potential corruption. Nevertheless, the engagement of these external supervision services are always at a cost, they might consume time, energy, or even financial expenses [159, 44, 118]. Intuitively, such costs can influence the engagement of external supervision services, and the consequent effectiveness on combating corruption.

These facts raise questions about the successful implementation of incentives facing corruption: to what extent can external supervision services combat corruption, and how do other key factors, such as the cost of service, influence the effectiveness of corruption combating? What lessons shall be taken in incentive implementation? All these questions are encompassed in the forth research question:

> **RQ 4.** Can external supervision services combat corruption in incentive implementation?

To address **RQ 4**, an evolutionary game theory framework is used to estimate the effectiveness of external supervision services on combating corruption and predict the eventual collaboration level of the participants. Additionally, stochastic simulation experiments are designed to explore

[2]Institutions usually delegate to rule enforcers who actually conduct supervision, rewarding and punishing activities; and it is usually the rule enforcers who directly accept bribes.

the influence of key factors. The results provide some insights into better introducing external supervising services to combat corruption and ensuring rigorous implementation of incentives.

In summary, **RQ 1** and **RQ 2** within Part I have a progressive relationship, while **RQ 3** and **RQ 4** within Part II have a sequential relationship. Part I proceeds from enforcing data sharing policies that involve concurrent data access or transfer operations to enforcing cross-domain workflows that encompass various sequential operations. In part II, **RQ 3** addresses the evaluation problem in the design stage of incentives, while **RQ 4** deals with the corruption issue in the subsequent implementation stage. These four research questions aim at improving the enforcement of policies, yet Part I and Part II approach this common aim from different dimensions. In Part I, the efforts focus on the practical dimension, empowering (resp. prohibiting) compliant (resp. non-compliant) behaviors at the appropriate time through technologies. In Part II, the efforts concentrate on the theoretical dimension, motivating participants to adhere to the policies based on game theories. The main contributions of these efforts are listed in the next section.

1.2 Main contributions

This thesis contributes to the following aspects: **new solutions** for enforcing operational regulations and **new models** for predicting the outcomes of institutional incentives, thereby facilitating their design and implementation. The contributions related to new solutions include:

- Proposing an approach that enables requests auditing and executing within an extendable infrastructure, supporting environment sensing, broadcasting, and application execution.
- Designing a flexible solution for choreographing incentive-integrated workflows, facilitating peer auditing, and eliminating untrustworthy

parties.

The main contributions in new models are:

- Constructing a model for comprehensive incentive design, predicting the effects of incentives in terms of promoting cooperation (compliance), the affluence of participants, and sustainability on execution.
- Developing a game model to study the influence of external supervision services on combating corruption in incentive implementation

The repositories containing the infrastructure/framework and models can be accessed through the following links:

- `https://github.com/dl4ld`
- `https://zenodo.org/record/8341111`
- `https://bitbucket.org/uva-sne/simulation-experiment-code-of-rspa-2022-0393/src/master/`
- `https://www.comses.net/codebase-release/539df5b3-f302-4ffd-bf60-762c79782722/`

1.3 Thesis overview

The main body of this thesis encompasses the following two parts, each of which can be comprehended independently, without either serving as a prerequisite for the other.

Part I tackles **RQ 1** and **RQ 2**. In **RQ 1**, the demand is to audit and execute data access requests adapting to the environment. Chapter 2 introduces a concrete approach that realizes the environmental adaptive auditing and execution process within an infrastructure to fulfill this demand. Moving on to **RQ 2**, the goal is to integrate incentives into workflows to motivate parties to adhere to regulated off-chain operations. Chap-

ter 3 presents a solution that integrates peer audit process as incentives to enhance compliance, and designs an architecture to coordinate such incentive-integrated cross-domain workflows.

Part II covers **RQ 3** and **RQ 4**. In Chapter 4, **RQ 3** is addressed through a constructed model that considers factors such as the execution cost of incentives and participants' wealth. This model facilitates tracking the impact of incentives on the system's affluence and facilitates a comparison of the sustainability of incentives from an institutional perspective. Turning to **RQ 4**, Chapter 5 proposes a game model that captures the interaction between participants and rule enforcers. This model enables participants to make choices between cooperation (compliant) while trusting the rule enforcers, cooperation without trusting the enforcer and engaging external supervision services, or defecting (non-compliant) with an attempt to bribe the rule enforcers. Meanwhile, rule enforcers can opt for honesty or corruption. With this model, we can study the effectiveness of external supervision services in combating potential corruption.

In the end, conclusions are offered in Chapter 6.

1.4 Origins

Part I builds on work presented in:

- **Xin Zhou***, Reginald Cushing, Ralph Koning, Adam Belloum, Paola Grosso, Sander Klous, Tom van Engers, and Cees de Laat: Policy enforcement for secure and trustworthy data sharing in multi-domain infrastructures, appeared in *The fourteenth IEEE International Conference on Big Data Science and Engineering* (BigDataSE) in 2020.
- Reginald Cushing, **Xin Zhou***, Adam Belloum, Paola Grosso, Tom van Engers, and Cees de Laat: Enabling Collaborative Multi-Domain Applications: A Blockchain-Based Solution with Petri Net Workflow

Modeling and Incentivization, accepted by *The Fifth IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications* (TPS) in 2023.

Part II builds on work presented in:

- **Xin Zhou***, Adam Belloum, Michael H. Lees, Tom van Engers, and Cees de Laat: Costly incentives design from an institutional perspective: cooperation, sustainability and affluence, appeared in *Proceedings of the Royal Society A* (IF: 3.5, **JCR Q2**) in 2022.
- **Xin Zhou***, Adam Belloum, Michael H. Lees, Tom van Engers, and Cees de Laat: The dynamics of corruption under an optional external supervision service, appeared in *Applied Mathematics and Computation* (IF: 4.397, **JCR Q1**) in 2023.

Chapter 2

The enforcement of data sharing policies that adapt to the environment

Abstract: This chapter addresses **RQ 1, "How to enforce cross-domain data sharing policies that adapt to the environment?"** Given that different situations require the application of different policies, there is a practical demand for enforcing environmental adaptive data sharing policies. This chapter presents an approach to meet this demand through a request auditing and a request execution process. These two processes are actualized within a designed infrastructure.

A version of the work in this chapter is published as "Policy enforcement for secure and trustworthy data sharing in multi-domain infrastructures" in *The fourteenth IEEE International Conference on Big Data Science and Engineering (BigDataSE)*, 2020.

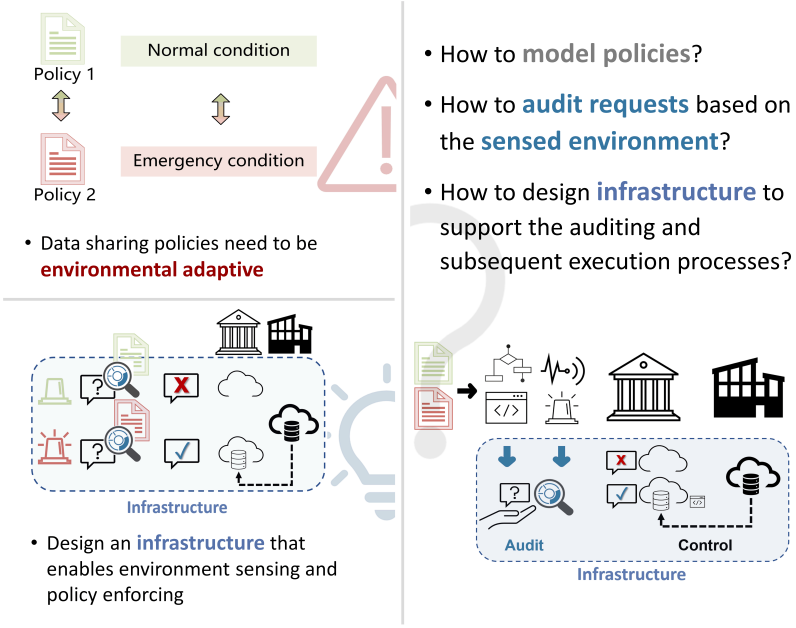


Figure 2-1: Graphical abstract of Chapter 2

2.1 Introduction

The security of data transfer has become a critical topic due to the significant value associated with data, leading to increasing concerns about unauthorized access [183, 39]. To guarantee data safety, many policies and regulations have been designed to govern data collection, sharing, and transfer. Nevertheless, in collaborations involving different individuals, departments, or organisations [84], there is often a need for the free exchange of data. This is particularly crucial in high-timeliness scenarios, for example emergency management, where effective crisis response relies on efficient information sharing among involved parties.

However, policies that aimed at data protection can sometimes impede the effective transmission of information [7]. On the one hand, limiting data access as much as possible can be the safest approach to protect data. On the other hand, these stringent policies can simultaneously diminish the value of data sharing and, in some cases, introduce risks. For example, during public incidents, such as fires or stampedes, strict data sharing policies may prevent the police from accessing critical datasets [7]. While strict policies work well under normal circumstances, they can become obstacles during emergencies. Accordingly, policies are supposed to be dynamically adaptable to the environment.

The enforcement of these flexible data sharing policies then poses a practical demand for an approach that supports sensing the environment, applying the corresponding proper data sharing policy in the request auditing process; and empowering the compliant operations in the execution process. To realize such an approach, several challenges must be addressed: 1) How to model policies to map the operational regulations into executable statements or commands? 2) How to audit[1] requests applying the proper policies based on the sensed environment? 3) How to design an infrastruc-

[1]In this chapter, when referring to "audit", it specifically denotes pre-audit, which is conducted prior to the final settlement of a transaction.

ture that supports the auditing and subsequent execution processes?

This chapter addresses these questions comprehensively. Firstly, in Section 2.2, a conceptual framework is proposed to model policies, which enables mapping the operational regulations into executable statements. Section B.2 then elaborates how to use Jason, a belief-desire-intention (BDI) based AgentSpeak language, for request verification and authorization. This auditing process and the subsequent execution process are supported by the designed infrastructure in Section 2.4, which hosts distributed collaborative applications. Finally, a use-case that involves environment adaptive policies is given to explain how data sharing policies are enforced by the proposed approach.

2.2 Data manifest and conceptual model of policies

In this section, two key concepts are introduced aiming at ensuring proper audit of data access requests: the dataset manifest and the conceptual model of policies.

For each specific dataset, data access or processing requests must adhere to policies set by the data controller who has the sovereignty over the dataset. Consequently, datasets must be lined with relevant policies, which serve as references during the subsequent auditing process. The dataset manifest acts as metadata, informing auditors about the policies that should be referred to.

During the auditing process, natural language policies need to be structured and mapped into executable statements, whose realization is based on the proposed conceptual model of policies. Structuring policies enables their further automatic enforcement through designed components. The following parts of this section delve into the details of these two concepts.

2.2.1 Data manifest

A data manifest encompasses essential information of the dataset, including the domain of the data controller, the corresponding applied policies, the sender's domain, the authorized recipient's domain, and a timestamp linked to the dataset. A data manifest is generated either by the data controller or by the sender (if not the controller) while transferring the dataset to its legitimate recipient.

The data manifest serves the dual purpose of specifying the policies that need to be checked in the auditing process and facilitating traceability of data transferring through recording transfer history. To ensure the integrity of the manifest, it must be signed by the cryptographic key of the data controller or legitimate sender, preventing any unauthorized alteration of the policies or other values contained within the manifest. Table 2.1 displays the data structure of a data manifest, presenting its items and providing examples of their respective values.

Table 2.1: Data manifest

Item	**Value**
Datasets	Set of files {Name of the file} Eg: {$File_1$,$File_2$}
Controller domain	The domain name of the data controller Eg: Alice
Policies	Set of policies {Name of the policy} Eg: {$Policy_1$, $Policy_2$}
Sender domain	The domain name of the data sender Eg: Alice
Recipient domain	The domain name of the recipient Eg: Bob
Timestamp	The timestamp of the manifest generation Eg: 20161206 9:34:10

2.2.2 Conceptual model of policies

Policies that apply to a dataset are regulated by the controller who controls its access and usage [109, 78]. Based on these regulated policies, auditors can verify the compliance of data operation requests. Authorization for these requests is granted only when they align with the policies, after which they are authorized with the cryptographic keys of the pointed auditors before being executed.

Consequently, natural language policies need to be structured to encompass crucial information. Figure 2-2 presents the conceptual model of policies, composed of authorisations, obligations, and environmental conditions [117, 82].

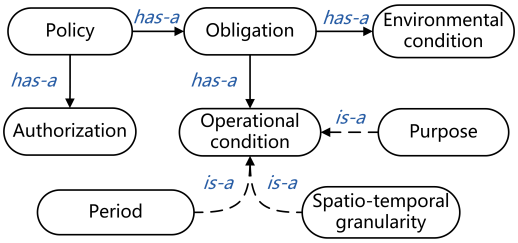


Figure 2-2: Conceptual model of policies. It regulates the required auditors for giving "Authorisation" to certain requests. The compliant data operation is described within the "Obligation". Since "Obligation" can vary under different "Environmental conditions", the latter is also specified in the policy. The purpose, period, and spatio-temporal granularity in the "Operational condition" clarify the rights and duties in a fine-grained manner.

These elements are defined and explained as follows:

(1) Authorisation

The component of authorisation regulates the auditors that are needed for checking the plan or request of data operations. For instance, the data controller may designate $Auditor_1$ and $Auditor_2$ as authorized auditors for

$Dataset_1$. This implies that any requests involving operations on $Dataset_1$ must contain the signatures of both these two auditors for subsequent execution.

(2) Obligation

The component of obligation delineates mandatory requirements that subjects must adhere to. For example, consider a scenario where a data controller, named "Alice", is obligated to transfer "Dataset_1" to the designated receiver, "Bob". Obviously, except for transferring, many other data operations can be described here.

(3) Environmental condition

The environmental condition specifies contextual prerequisites that must be met for a particular obligation to come into effect. For instance, consider the scenario where an obligation for "Alice" to transfer "Dataset_1" to "Bob" only arises in the event of a fire catastrophe. When this specific environmental requirement is fulfilled, the corresponding obligation is activated, enabling auditors to authorize the associated data operation requests.

(4) Operational condition

The operational conditions encompass three key aspects:

- **Conditions by purpose** [21]: This refers to the specific circumstances that define the purpose or intention of the data operation. For instance, the purpose could be "commercial use" "public safety use" or "research use", etc.
- **Spatio-temporal granularity (S-T granularity)** [21]: It determines the temporal scale of conducting the operation, such as "sec-

ondly", "minutely", "hourly", or "daily", etc.

- **Time Period**: It specifies the duration of the data operation can be executed, indicating the time span during which the operation remains active.

An example of structuring a policy with the proposed conceptual model is presented in Table 2.2. In this policy, "Alice" is obliged to transfer the dataset to "Bob" upon "Bob"'s request during an emergency. Operations on this dataset require the authorizations from "Auditor$_1$" and "Auditor$_2$". The "Operational condition" limits the usage of this dataset to research, and temporal scope of the operation is limited to the year 2020.

Table 2.2: An example of a policy

Components	**Value**
<Authorization>	*Auditor$_1$ and Auditor$_2$*
<Obligation>	*Alice is obliged to send dataset to Bob*
<Environmental condition>	*With the request from Bob*
<Operational condition>	<***Purpose***> *Research* <***Period***> *In 2020* <***S-T granularity***> *By default*

The conceptual model can structure policies for their mapping into executable statements, automating the following enforcement[2]. Specifically, the enforcement process of structured natural language policies is as following: according to the manifest, the planner sends operation requests with the domain name of the designated auditors and the corresponding policies. Subsequently, the appointed auditors response, by granting authorization to requests aligned with the respective policies. Consequently, compliant requests with requisite auditor signatures are executed.

[2]It is worth noting that this conceptual model primarily focuses on the expressivity of the normative concept of "obligation", while the concept of "Hohfeldian power" [158] is not included. There are various alternative conceptual models for representing different norms [25, 162, 146, 42]. Due to the limitations of space and the specific focus of the research question, the expressiveness of the conceptual model is not discussed in detail here.

Through this approach, the operational regulations set by the data controllers are enforced. In the following sections, Section 2.3 elaborates on the realization of audit function, and Section 2.4 describes the infrastructure that supports the entire requests auditing and execution processes, enabling cross-domain data sharing.

2.3 Auditing process

2.3.1 Fulfill audit function with Jason

The function of audit is realized by auditors. The concept of an "**auditor**" in this dissertation shares functional similarities with real-life auditors, yet with certain distinctions. In terms of functionality, both types of auditors assess whether specific operations adhere to compliance and determine whether certain activities should be approved. However, it is important to note that real-life auditors are humans, whereas here auditors are designed components that automatically execute the auditing responsibilities through programmed code. To achieve this, an AgentSpeak language, Jason [15, 144], is employed to implement the audit function.

Jason is primarily employed for modeling multi-agent systems based on belief-desire-intention (BDI) framework [86, 116]. The BDI framework equips agents with information about their environment as beliefs; their potential activities as desires; and the specific actions they choose to undertake as intentions. Therefore, the embedding of the BDI framework allows Jason to effectively capture interactions among agents. To bridge the gap between desires and intentions, agents require a reasoning system. This approach uses the procedural reasoning system (PRS) [182, 31] to facilitate agents in selecting and carrying out appropriate activities. The combination of the BDI framework and PRS enables agents created by Jason to effectively realize the audit function.

When employing Jason with a embedded designed PRS to fulfill the role of auditors, auditors are modeled as agents. For each request, the necessary auditors respond with an assessment of compliance and a subsequent authorization decision, which is facilitated by a reasoning process. This process is guided by their beliefs and predefined reasoning rules. For instance, the referenced policies and the sensed environmental condition are beliefs; how to grant authorizations based on these beliefs are predefined reasoning rules. The reasoning rule is straightforward: auditors compare the requests with the policies, if no conflicts arise, they assign authorisations, otherwise they refuse. In this way, Jason effectively realizes the audit function.

While it is true that the audit function can be implemented by other alternative programming languages, the utilization of Jason offers several distinct advantages. These advantages include, but are not limited to the following:

- **Reactive pattern**: Jason supports agents with a reactive pattern. This proves advantageous for auditors, as it enables them to remain responsive to requests.
- **Autonomy of auditors**: Jason empowers auditors with autonomy. Auditors can independently reason and evaluate requests, then generate appropriate authorization outputs. This active decision-making ability aligns well with the role of auditors in assessing compliance.
- **Java-based extensibility**: Developed in Java, Jason boasts inherent extensibility. This feature proves valuable for the auditing process as it facilitates seamless communication between the auditing component and the external environment. This means that auditors can readily update their environmental beliefs through sensors and transmit authorized requests to servers for execution.

In all, the combination of these features of Jason effectively addresses the specific requirements of modeling auditors for the auditing process. In the following, a concrete example is given to elaborate on how to use Jason to realize the auditing process.

2.3.2 An example of requests auditing in Jason

To reduce the cognitive load for readers, we directly use the auditing process in the ArenA use-case as an example to explain how the audit function can be realized by Jason, in the context of enforcing data sharing policies that adapt to the environment. In this part, the background information about the ArenA use-case is first presented, followed by structuring the involved policies by the data manifest and conceptual model proposed in Section 2.2. Finally, the automatic auditing process on data operation requests is exhibited.

(1) Background information about the ArenA use-case

The Johan Cruijff ArenA, the main stadium of Amsterdam, witnessed a tragic incident during an outflow of over 60,000 visitors in 2018. This accident occurred near a pedestrian bridge and necessitated urgent and coordinated response tasks, including dispatching ambulances, directing traffic, guiding visitors, and cleaning the scene. Multiple departments, including the police, traffic management, fire department, and the ArenA Operational Mobility Center (OMC), were involved in this complex emergency situation, demanding rapid information exchange.

In this case, one task for the traffic coordinators from Traffic Management Operations Amsterdam (VMCA[3]) was to divert traffic away from the incident. During this process, VMCA sent requests to OMC, asking for the necessary dynamic parking lot data from the OMC.

[3]https://nonoa.nl/projecten/verkeersmanagement-centrale-amsterdam

(2) Environment adaptive data sharing policy

To ensure privacy and safety, the data sharing process is expected to adhere to the policy:

> *Under normal conditions, the parking data is private to the OMC (data controller). However, when an emergency occurs, OMC has the obligation to share parking data with VMCA for traffic diversion.*

By applying the policy concepts in Section 2.2, this policy can be represented as shown in Table 2.3.

Table 2.3: An environment adaptive data sharing policy

Components	Value
<Authorisations>	*$Auditor_1$ and $Auditor_2$*
<Obligation>	***OMC** is obliged to send dataset to the **VMCA***
<Environmental Condition>	*Emergency*
<Operational Conditions>	<***Purpose***> *Traffic diversion* <***Period***> *During the diversion task* <***S-T granularity***> *By default*

(3) Data sharing requests auditing by Jason

The structured policy can then be saved as a belief for auditors, and meanwhile the requests containing the intended operations on the data objects:

```
1 //Policies – policy(Policy_name, Auditor, Dataset, Sender, Receiver, Purpose,
      Environmental Condition)
2 policy(policy1, auditor1, parking1, omc, vmca, traffic_diversion,
      emergency_condition).
3 policy(policy1, auditor2, parking1, omc, vmca, traffic_diversion,
      emergency_condition).
```

```
//Pending request − request(Dataset, Sender, Receiver, Purpose, Time)
request(parking1,omc,vmca,traffic_diversion,2020,07,06,23,45,0);
```

In this provided code snippet, policies are saved as beliefs of auditors. These policies contain the obligations and the information of which auditors are required to give authorisations. In the given example, "$Policy_1$" specifies that "$Auditor_1$" and "$Auditor_2$" are tasked with auditing requests related to the dataset "parking1". Regarding the pending **request**, it represents a data operation that "*OMC transfer the dataset 'parking1' to VMCA for traffic diversion*", and this request was generated at 23:45:00 on July 6th, 2020.

Additionally, considering the environmental condition is a determinant in the authorization decision, the sensed environmental condition is also included in auditors' beliefs. When under normal condition, the related belief is:

```
// When the environmental condition is normal condition or non−emergency
    condition
+~emergency_condition
```

However, when emergency happens, the auditor can "sense" the change:

```
// Check if the received message contains the emergency event
public static boolean eventsubset(String argv){
    String regex = "EVENT_EMERGENCY_ON";
    Pattern pattern = Pattern.compile(regex);
    Matcher matcher = pattern.matcher(argv);
    if (matcher.find()){
        return true;
    }
    return false;
}

// Read messages from rabbitmq queue "sensor.event"
public static void receiveEnv() throws Exception {
    ...
    DeliverCallback deliverCallback = (consumerTag, delivery) -> {
```

```
        if(delivery != null){
            String message = new String(delivery.getBody(), "UTF-8");
            if(eventsubset(message)){
                Literal emerCon = Literal.parseLiteral("~
    emergency_condition");
                addPercept(emerCon);
                System.out.println("Received alarm.");
            }
        }
    }
    ...
}
```

Correspondingly, the auditors' belief about the environmental condition in Jason will be updated as:

```
// When the environmental condition is emergency condition
+emergency_condition
```

For auditors, their reasoning rule is to check the components within the requests, including the dataset, the sender, the recipient, purpose, and so on; then they authorize if there are no conflicts.

```
// Reasoning rule - Authorisation
authorisation(Dataset_r,Sender_r,Recipient_r,Policy_m,Purpose_r,auditor)
     :-
    emergency_condition & policy(Policy_id,Pointed_auditor,Data_object,
     Sender,Recipient,Purpose, Environment_Condition) & Policy_m ==
     Policy_id & auditor == Pointed_auditor & Dataset_r == Data_object &
     Sender_r == Sender & Recipient_r == Recipient & Purpose_r == Purpose.

// Reasoning rule- Refuse
refuse(Dataset_r,Sender_r,Recipient_r,Policy_m,Purpose_r,auditor) :-
    policy(Policy_id,Pointed_auditor,Data_object,Sender,Recipient,Purpose
     , Environment_Condition)
    & Policy_m == Policy_id & auditor == Pointed_auditor
    & (~emergency_condition | Dataset_r \== Data_object | Sender_r \==
     Sender | Recipient_r \== Recipient | Purpose_r \== Purpose).
```

Finally, the auditors will authorize compliant requests and broadcast the

auditing results:

```
// Output − Authorisation
+request_auditors(Dataset,Sender,Recipient,Policy,Purpose)[source(Agent)
    ]:
    .my_name(Auditor_Name)
    & permission(Dataset,Sender,Recipient,Policy,Purpose,Auditor_Name)
        <- .print("This request has been authorised by ", Auditor_Name);
      !authorised(Dataset,Sender,Recipient,Policy,Purpose,Auditor_Name).
+!authorised(Dataset,Sender,Recipient,Policy,Purpose,Auditor_Name)
    <- .broadcast(tell, authorised(Dataset,Sender,Recipient,Policy,
    Purpose,Auditor_Name)).

// Output−Refuse
+request_auditors(Dataset,Sender,Recipient,Policy,Purpose)[source(Agent)
    ]:
    .my_name(Auditor_Name)
    & refuse(Dataset,Sender,Recipient,Policy,Purpose,Auditor_Name)
        <- .print("This request has been refused by ", Auditor_Name);
        !refused(Dataset,Sender,Recipient,Policy,Purpose,Auditor_Name).
+!refused(Dataset,Sender,Recipient,Policy,Purpose,Auditor_Name)
    <- .broadcast(tell, refused(Dataset,Sender,Recipient,Policy,Purpose,
    Auditor_Name)).
```

Here is an example of reported log:

```
    [auditor1] This request has been authorised by auditor1
    [auditor2] This request has been authorised by auditor2
    [Planner] Request: Transfer parking1 from omc to vmca for
    traffic_diversion is authorised by auditor1
    [Planner] Request: Transfer parking1 from omc to vmca for
    traffic_diversion is authorised by auditor2
    [Planner] Request: transfer parking1 from omc to vmca for
    traffic_diversion can be executed.
    [Planner] No requests need to be audited.
```

In this manner, the audit function is realized by Jason, ensuring that the authorized data operation requests adhere to the policies associated with the dataset. Subsequently, authorized requests can be executed within the proposed infrastructure.

2.4 Infrastructure

In order to operationalize the environmental adaptive data sharing policies, a multi-domain infrastructure is required to integrate all the necessary components for realizing data auditing, data transfer, networking, and more. This section provides an introduction to the essential functional components within this infrastructure.

This infrastructure consists of functionally independent components that can communicate with each other through a built network. Each component has its own set of functions, with some parts exposed and available for invocation by other components. This enables effective collaboration between components from different domains, such as OMC and VMCA in the ArenA use-case, for accomplishing complex tasks.

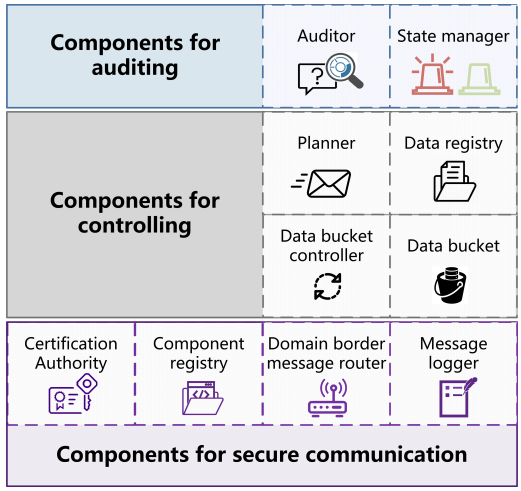


Figure 2-3: The infrastructure components are categorized into three groups based on their functions. 1) Components for auditing, this category includes the "Auditor" and "State manager" components, which form the "auditing layer". 2) Components for controlling, these components are managed by the "Planner" which collects necessary information from the "Data registry". Data requests are then executed by the "Data bucket controller" which initiates the "Data bucket". 3) Components for secure communication, the four components at the bottom guarantee within and cross-domain communication among components.

Based on their functions, these components can be categorized into three groups: 1) components for auditing; 2) components for controlling; and 3) components for secure communication, as illustrated in Figure 2-3. The first category is responsible for realizing the auditing function, constituting the "auditing layer". The second category focuses on coordinating components and executing data requests, forming the "controlling layer". The last category supports communication among components and play a crucial role throughout the entire request sending, auditing, and execution processes. The following of this section dives into the details of these components.

2.4.1 Components for auditing

This subsection introduces two essential components responsible for realizing the auditing process: the auditor and the state manager.

(1) Auditor

The auditor component serves the purpose of listening to requests from the message queue, examining these requests, and authorizing those that comply with the defined policies. Auditor components function autonomously, and organizations possess the liberty to appoint their trusted auditors to oversee operation requests concerning specific datasets. This decentralized distribution of auditors ensures a level of authority distribution, and augments the overall security of data sharing.

(2) State manager

As previously mentioned, auditors need to perceive changes in the environment. The state manager plays a pivotal role in this by broadcasting the updated environmental condition network-wide. To illustrate, within the ArenaA use-case, an emergency triggers a front application. Conse-

quently, the state manager undertakes the responsibility of broadcasting this event via the message queue. Then auditors can update their beliefs by listening to the message queue.

2.4.2 Components for controlling

This subsection delves into the crucial components that handle the orchestration and execution of data operations.

(1) Planner

Planners play the role as a coordinator of actions that have to be taken in order to realize some predefined goals. A planner broadcasts requests on a message queue, and waits for authorized requests. Once a planner receives authorized requests, it subsequently contacts the related components to execute the approved operation. For instance, if a data transfer request is authorized, then the planner contacts the corresponding data bucket controller to enforce the transfer process.

The planner, acting as a coordinator, fulfills the role of broadcasting data operation requests on the message queue. It awaits the authorization of these requests. Once authorized, the planner triggers a series of actions. It contacts the relevant components to execute the approved operations. For instance, if an authorized data transfer request surfaces, the planner communicates with the corresponding data bucket controller to initiate the transfer process.

(2) Data registry

A vital role of the data registry is to facilitate the publication and maintenance of data catalogues. It serves as a query endpoint for the discovery of new datasets and the provision of infrastructural details. These details may include information about which bucket controller is tasked

with overseeing a particular dataset. Therefore, data registry ensures that the planner effectively connects with the appropriate bucket controller.

(3) Data bucket controller

Initiated by the planner, the data bucket controller ensures again the requests are with all the required signatures from auditors. It then establishes Virtual Private Network (VPN) tunnels, and subsequently, launches data buckets. These data buckets function as endpoint containers, executing the actual transfer operations. Importantly, the bucket controller dynamically links the tunnel interfaces to the data bucket containers during runtime.

(4) Data bucket

Data buckets are transient and only generated by the bucket controller. This approach minimizes data exposure and thereby mitigates potential security vulnerabilities. The network interface of data buckets remains under the strict control of the bucket controller. Through dedicated VPN connections, the bucket controller establishes links between the sender and receiver buckets.

Notably, data buckets do not have any network connectivity or associated interfaces by default. When a request triggers bucket controllers, the controllers configure encrypted VPN connections between buckets using Wireguard [43]. Furthermore, controllers save the VPN interfaces into the network namespace [34] of the respective buckets.

The VPN encryption keys are request-specific, ensuring distinct keys for each operation. Once a request is completed, the network interfaces are removed from the containers to avert unauthorized communication.

It's important to note that while our current use-case focuses on enforcing data sharing policies, the system can be extended to involve data com-

puting. For such scenarios, analogous mechanisms can be established. By creating compute interfaces responsible for executing computations, and compute interface controllers for launching these interfaces, more complex requests could be executed effectively.

2.4.3 Components for secure communication

This subsection elaborates on the essential components that facilitate secure and authenticated communication within the multi-domain infrastructure.

(1) Certification Authority (CA)

The Certification Authority (CA) plays a crucial role in assigning cryptographic public/private keys to components within its domain. These keys enable secure communication among domains and components. A public key serves as the unique address of a component, while the corresponding private key facilitate identifying the sender of messages. Communications between components are signed using their private keys, and these signatures can be verified by any node in the network through the public key. Notably, these cryptographic addresses are non-transferable, enhancing traceability. This aspect is pivotal for auditing, as it ensures that actions signed by a component can always be traced back to the source. This feature further enables the auditing process by allowing verification of the sender of requests or messages. The translation of public key addresses to IP endpoints is achieved through name services.

Under this cryptographic addressing scheme, functions within components can be invoked using routes, designated as "hDPK/hCPK/mN/fN". Here, **hDPK** represents the hashed public key of the domain root level certificate[4], **hCPK** signifies the hashed address of a specific component, **mN**

[4]This certificate is used to sign component addresses, and its hashing minimizes address length, an advantage in most message queue systems

corresponds to the module name within the component, and **fN** signifies the function name. To enable the identification of modules and functions, "Component registry" is introduced to store these details, rendering these names discoverable.

(2) Component registry

Serving as an address book, the component registry plays a pivotal role in exposing the names of components, modules, and functions. These exposed addresses enable accurate and effective connections to be established.

(3) Domain border message router

The domain border message router serves as a point of contact between domains. This router utilizes the hashed public key of the receiver domain to forward messages. In scenarios where messages are received from other trusted domains, the router places these messages in the local message queue. This function ensures secure and seamless inter-domain communication.

(4) Message logger

The message logger maintains an immutable and tamper-proof database of messages. Given the absence of a central authority controlling the logs, each domain is responsible for capturing sufficient logging information from other domains. A policy decision might entail cross-logging with another domain, minimizing the potential for tampering with one's own logs. The primary purpose of this message record is to facilitate the postmortem analysis[5] of policy violations. Such violations could arise from incorrect policy implementation or from malicious attempts to subvert the policy.

[5]Also known as post-audit. This chapter primarily focuses on pre-auditing and enabling the execution of compliant operations.

Putting it all together, the components designed for auditing constitute the auditing layer, while those for controlling constitute the controlling layer. The former assesses the compliance of operation requests, and the latter carries out the execution of compliant requests. These layers are interconnected and facilitated by communication components. The process within the auditing layer has been detailed in Section 2.3. Moving to the controlling layer, approved requests are executed as depicted in Figure 2-4: pending requests trigger data bucket controllers to initiate data buckets, which are interconnected via VPN. Data transfer occurs through this VPN tunnel. The execution of each request is recorded in the message logger component, ensuring a record for future reference or post-auditing purposes. As a result, data operational policies are enforced through the combined efforts of the auditing and controlling layers[6].

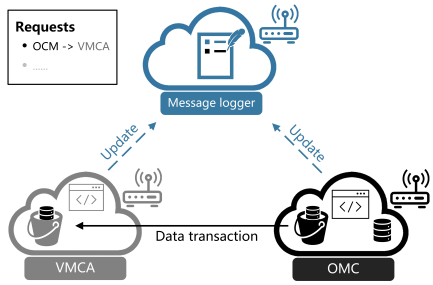


Figure 2-4: Data transfer between domains. There are two domains in the figure running controllers, OMC and VMCA. The domains are executing the requests list presented on the top left. When executing the request of transferring dataset from OMC to VMCA, data bucket controllers of OMC and VMCA create their data buckets, and these two buckets are connected via VPN. The message logger component located at the top right is updated with the occurred transfer.

[6]It is worth mentioning that the approach presented in this chapter may remind our readers of a rule-based data access control model. However, there are some essential differences between them. Firstly, the enforced objects here are obligations, which involve proactive initiations of data operations and require passive pre-auditing of these operations. In contrast, a rule-based data access control model primarily focuses on passive permissions or rejections upon received requests. Therefore, they differ functionality. Additionally, in this approach, each party can choose its trusted domains to manage the auditing responsibility. This decentralization feature distinguishes this approach from access control models which typically rely on a centralized authority at the data controller's end.

2.5 A concrete application of the approach in the ArenA use-case

This section demonstrates the application of our approach to the ArenA use-case, enforcing the environmental adaptive data sharing policy. The section begins by outlining the information flow within the infrastructure relevant to the use-case, and then presents a concise overview of the policy enforcement process. It's worth to mention that while the use-case primarily focuses on data sharing, this proposed approach is also applicable to data access and to managing algorithms or application permissions related to protected datasets.

2.5.1 Information flow of the ArenA use-case

In the use-case, the two parties OMC and VMCA maintain their own administrative domain and host necessary components that facilitate the auditing and controlling layers. The coordination of data operation requests is encoded and managed by the planner component. Note that the planner can technically reside in either domain, and the decision on its hosting depends on mutual agreement between the parties involved. Figure 2-5 illustrates the complete information flow and component interactions involved in enforcing the environmental adaptive policy in the ArenA use-case. These interactions are presented in chronological order in the subsequent paragraphs.

When an emergency occurs, the front application sends relevant information to the OMC's state manager. This event is then broadcasted across the network and captured by auditors from both OMC and VMCA, leading to an update of their respective beliefs about the environmental condition. The state managers in each domain also register this event in the message logger.

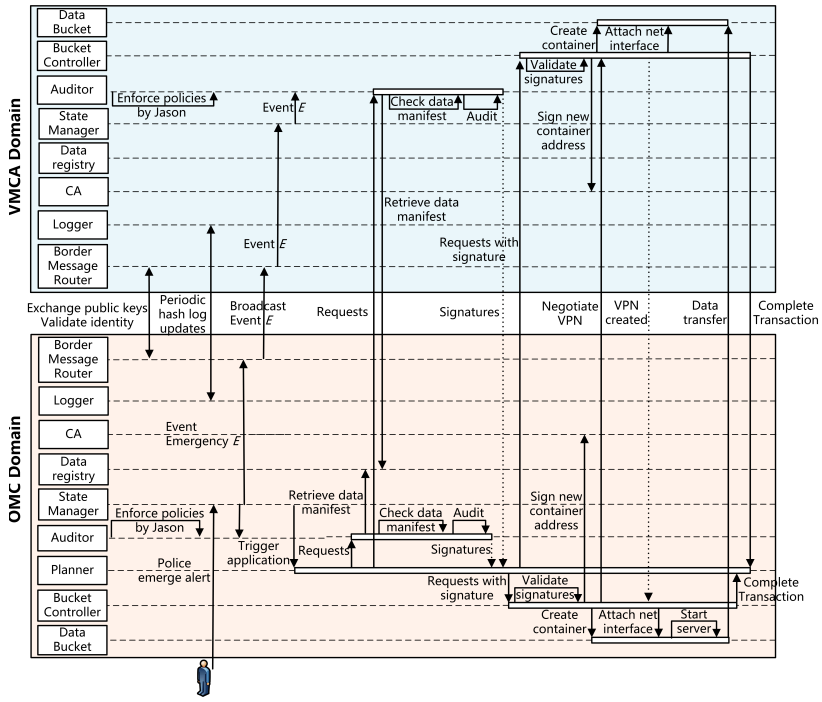


Figure 2-5: Information flow in the ArenA use-case. Components are listed on the left side. The broadcasting of the data operation request is triggered by the alarm of emergencies. Subsequently, auditor components of each domain fulfill the auditing responsibility and send the signed request back to the planner. The planner then forwards the authorized request to the bucket controllers of OMC and VMCA, who establish the VPN tunnel between endpoints for data transfer.

Following this, the planner is activated by the event trigger, sending the request that awaits authorizations to the auditors of both OMC and VMCA domains. These auditors assess the requests using the manifest, engage in reasoning, and return the signed request, either authorized or rejected, to the planner who initiated the request. Subsequently, the planner issues the controllers on both domains to initiate the transfer if the request is approved.

In the controlling layer, the controllers of both OMC and VMCA validate the signatures and establish dedicated VPNs along with containerized services to host the requisite server/client programs for data transfer. Once

the authorized request is successfully executed, the controllers remove the connections and services. Henceforth, the entire process of triggering, auditing, and executing is successfully accomplished.

2.5.2 Demonstrating approach applicability

This section demonstrates the applicability of the proposed approach in the use-case. The demonstration illustrates how the same data operation request is processed under different environmental conditions. To better simulate the scenario, a front-end application is designed to trigger the occurrence of an emergency, as shown in Figure 2-6. The complete version of the demonstration is accessible through this link: https://bitbucket.org/uva-sne/demonstration-ieee-bigdatase2020/downloads/, and the corresponding source code can be found in https://github.com/dl4ld.

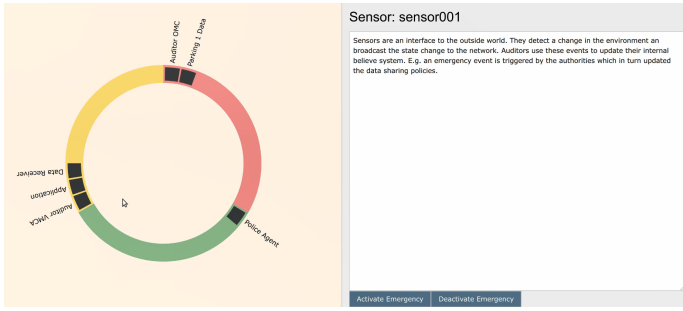
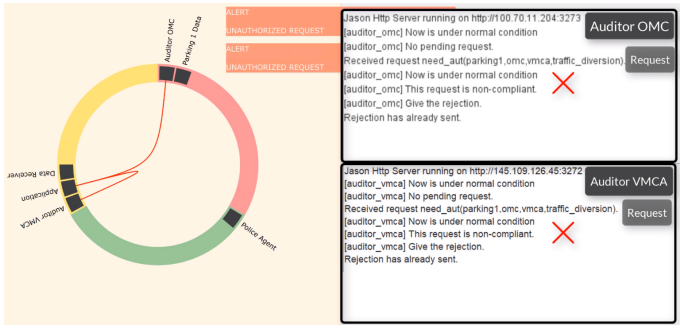
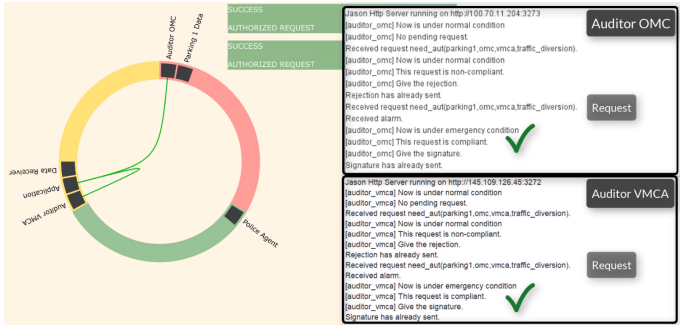


Figure 2-6: The front-end application of the demonstration. The left panel includes involved domains and their components. The right panel shows the application of triggering the emergency, where the "Activate Emergency" button triggers the state manager component to broadcast the emergency condition; the "Deactivate Emergency" button corresponds to lifting the emergency condition.

Figure 2-6 presents a working prototype of the ArenA use-case. The left panel features a three-color ring representing the OMC, VMCA, and police domains. The black blocks within the rings represent domain components. The right panel shows the designed front-end application for triggering emergencies.



(a)



(b)

Figure 2-7: The auditing process of the same data operation request under different environmental conditions. Communications among domains and their components are displayed on the left panel, while the auditing process of auditors from OMC and VMCA is depicted on the right panel. Figure 2-7(a) illustrates auditors rejecting the request under normal conditions, while Figure 2-7(b) depicts auditors authorizing the request under emergency conditions.

Figure 2-7(a) and (b) illustrate the auditing process of the same data operation request under normal and emergency conditions, respectively. The left panel outlines domains and their components, the links between components represent their communication. The right panel provides details of the request auditing process at the auditors of OMC and VMCA.

As observed, under normal conditions, auditors reject the data request, as depicted in Figure 2-7(a). However, when an emergency occurs, auditors' belief about the environmental condition changes upon receiving an alarm

from the police agent. Consequently, under emergency conditions, the same data operation request receives authorization from the auditors.

This demonstration showcases how the proposed approach enforces the environmental adaptive policy in the ArenA use-case. It's important to note that, for enhanced reader comprehension, only certain auditing and controlling components are visible, while other necessary components are operational in the background without explicit representation in the demonstration.

2.6 Concluding remarks

This chapter aims to enforce environmental adaptive data sharing policies. To achieve this goal, three concrete challenges proposed in Section 2.1 need to be addressed. This section briefly summarizes the answers to the questions, and discusses the advantages and limitations of the proposed approach.

- **Policy modeling**: A conceptual model of policies (illustrated in Figure 2-2) has been proposed to structure natural language policies for subsequent mapping to executable programming language.
- **Audit function**: The audit function has been realized using Jason, a belief-desire-intention framework based on Java. Auditor agents created by Jason can store policies, environmental conditions, and pending requests as beliefs, enabling them to reason and make authorization or refusal decisions. The detailed auditing process is provided in Section 2.3.
- **Infrastructure**: The infrastructure comprises an auditing layer and a controlling layer to realize the designed auditing and execution processes, supporting request transmission and coordination, environmental condition broadcasting and updating. More details are

available in Section 2.4.

The proposed approach offers several features in enforcing data sharing policies. Firstly, its decentralization eliminates the need for a single controlling party. Each party can choose its trusted domains to manage the auditing responsibility for requests involving their datasets. This decentralized approach enhances flexibility and autonomy in cross-domain cooperation.

Secondly, its supportive infrastructure is highly extensible in both the auditing and controlling layers. In the auditing layer, while our use-case enforces a single data operational policy, real-world scenarios often involve the need to enforce multiple policies simultaneously. This can be accommodated by adjusting the "Policies" item value in the data manifest (see Table 2.1) and updating auditors' beliefs about policies.

In the controlling layer, although the executed operation in the ArenA use-case involves a simple data transfer between domains (achieved through data bucket controllers and data buckets), the infrastructure can be expanded to handle other data operations, such as data computation. This can be effectively achieved by designing compute interface controller components to manage compute interface components.

However, the proposed approach does have certain limitations. Since involved parties retain control over their own administrative domains, there remains the possibility for malicious domains to privately share data with other parties. For instance, the infrastructure may not be able to prevent VMCA from discreetly sharing OMC's data with an external party. Counteracting such potential non-compliant behaviors requires additional efforts, such as introducing dataset tracking process by incorporating data watermarking technologies or implementing incentive mechanisms to discourage potential malicious actions.

Chapter 3

Coordinating incentive-integrated multi-domain workflows

Abstract: This chapter addresses **RQ 2, "How to enforce incentive-integrated cross-domain workflows?"** To deter potential non-compliance with unenforceable off-chain tasks, this chapter proposes a solution that integrates a peer auditing process into workflow enforcement, thereby providing additional motivation for parties to fulfill off-chain tasks.

A version of the work in this chapter is accepted as "Enabling Collaborative Multi-Domain Applications: A Blockchain-Based Solution with Petri Net Workflow Modeling and Incentivization" in *The Fifth IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS)*, 2023.

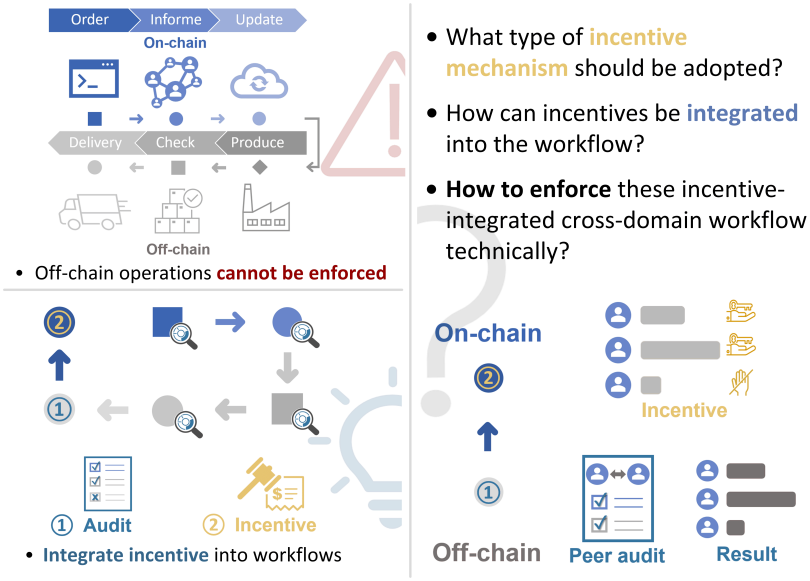


Figure 3-1: Graphical abstract of Chapter 3

3.1 Introduction

Blockchain technology enables the updating of timestamped transaction data on distributed ledgers, offering advantages such as decentralization, transparency, immutability, and auditability [186]. Blockchain offers a programmable environment for the execution of smart contracts, computer protocols specifically designed to facilitate collaborations across multiple domains, eliminating the necessity for trusted third parties [98]. In the past decade, blockchain-based smart contracts have rapidly developed and have been widely applied in industries, varying from finance [139], internet of things (IoT) [170, 124], supply chain [88, 27] to electronic health [24].

To leverage blockchain-based smart contracts for enforcing multi-domain workflows, protocols [97] or policies [190, 135], two requirements are needed. The first one is to model and verify smart contracts at the **contract-level** [155], ensuring that the self-executing programs are properly mapping the designed tasks within the workflow. Secondly, we need to execute the smart contract safely, which requires a collaborative infrastructure that can execute the programs in the workflows (also called applications) at the **program-level**.

However, even if these two requirements are satisfied, non-compliant behaviors can still occur during the execution of the workflow, particularly when the workflow involves tasks that must be executed off-chain, since these off-chain tasks are not visible to all parties involved in the workflow execution. To address this challenge, one approach is introducing triggers to receive and send messages between on-chain smart contract and off-chain interfaces. In this way, triggers connect blockchain to the internal processes of domains and further enforce the regulated workflow [174]. In reality, however, domains may be motivated to deviate from regulations in order to maximize their own utilities. For example, they might skip certain off-chain tasks while claiming that the tasks have been well executed.

Under these circumstances, incentives, which allow punishing or rewarding domains according to their previous performance, have great potential to be deployed into smart contracts. With the complement of incentives at the contract-level, the security of coordinating the on-chain and off-chain workflow in multi-domain scenarios can be enhanced. Hence, the new requirements for blockchain-based smart contract are summarized as follows:

- **Contract-level**: map, encode, verify, and coordinate the tasks within the workflow, while ensuring parties are incentivized to fulfill their tasks, especially the off-chain ones
- **Program-level**: build collaborative infrastructure that is capable of identity management, data-flow management, and control-flow management

To fulfill these requirements at both the contract-level and program-level, three specific questions need to be addressed: 1) What type of incentive mechanism should be adopted? 2) How can incentives be integrated into the workflow? 3) How to technically enforce this incentive-integrated cross-domain workflow? The purpose of this chapter is to shed light on these questions and explore a practical solution.

In this chapter, a solution is proposed that utilizes an incentive-integrated workflow along with blockchain technology to choreograph multi-domain workflows. To provide a comprehensive understanding of the solution, this chapter starts by introducing the fundamental involved concepts in Section 3.2. Following this, the specific implementation details of the blockchain-based Petri nets are elaborated in Section 3.3. To validate the applicability of the proposed solution, a distributed denial-of-service (DDoS) use-case is employed in Section 3.4 to demonstrate the functionality of the approach. This chapter concludes by presenting findings and comparing the solution with related works in Section 3.5.

3.2 Preliminaries

3.2.1 Blockchain and smart contract

Blockchain is a distributed ledger that preserves the integrity and immutability of a series of blocks. Each block in the chain is connected to the previous one through cryptographic hashes, containing information from the prior block, timestamps, and transaction information. This design allows for the creation of a tamper-proof chain of blocks. The fundamental feature of blockchain technology is that every involved party can maintain a synchronized copy of the blockchain, enabling multiple domains to transact without relying on a trusted central server.

The functionality of blockchain is extended and expanded with the emergence and development of smart contracts. As a computer protocol designed for executing applications, smart contracts can maintain the workflow between multiple domains when coupled with blockchain [149]. Consequently, the combination of smart contracts with blockchain technology has made it possible to enforce more complex rules, contracts, and policies among multiple domains meanwhile tracking the progress of execution.

Blockchain-based smart contracts have been widely and rapidly developed [98]. The foundation of blockchain-based smart contracts is built on four key components: 1) **smart contracts**, which enable the execution of complex agreements by automating the processes and enforcing the tasks in the workflow; 2) **ledger**, which provides complete and immutable records shared by all the peers; 3) **wallet**, which utilizes a Public Key Infrastructure (PKI) system to allow users access to the ledger, and assigns "ownership" of ledger records using key signatures; and 4) **consensus**, which ensures the agreement of peers regarding the ledger. These four components work together to create a secure and decentralized system for executing agreements across multiple domains, as exhibited in Figure 3-2.

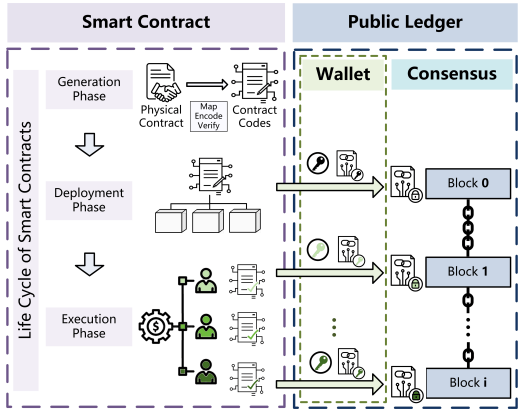


Figure 3-2: Four pillars of the blockchain-based smart contract: smart contracts, public ledger, wallet, and consensus. The life cycle of smart contracts consists of three phases: generation, deployment, and execution. Starting from the deployment phase, the completion of every activity or operation is recorded as a new block on the public ledger. The successful recording relies on wallet and consensus. The wallet uses a public key infrastructure system, enabling the identification of block creator. Meanwhile, the consensus algorithm ensures that all parties agree on the records on the public ledger.

It is worth noting that since all peers update the same ledger, there is a potential risk of breaking consistency. Consensus itself can be an attack vector, for example, in Sybil attack, a peer controlling the ordering can control what gets written. To mitigate the risk, most public blockchain setups apply proof-of-work consensus, which requires an attacker to control more than 50% of the compute power to control the network [55]. Proof-of-work consensus provides higher security at the cost of high computational power. However, in less malicious environments, traditional consensus such as Paxos or Raft can be used [145] to decrease costs. In this study, we consider the scenario that all parties intend to collaborate and have a semi-trustful relationship with other peers. Hence, we apply the Raft consensus algorithm.

3.2.2 Petri net

As Figure 3-2 presented, smart contract generation is the starting point of a smart contract life cycle. At this phase, the physical contract needs to be mapped and encoded into executable codes, where the properties of interactions and the external environment can be expressed and verified. Approaches such as process algebras [127], set-based methods [73], and state-transition systems [75] are commonly used. Considering the aim of this chapter, and the fact that state-transition systems can naturally model the business artifacts in process-oriented contracts, state-transition systems are selected to map and verify the workflow among the domains.

A Petri net is a representative state-transition language proposed by Carl Adam Petri [122]. It consists of four fundamental elements: **places**, **transitions**, **tokens**, and **arcs** that enable Petri nets to model the processes in workflows, policies, or protocols. Figure 3-3 gives an example of a classical Petri net.

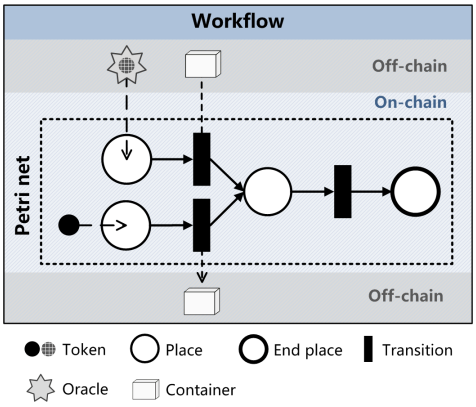


Figure 3-3: The Petri net is a state-transition language used to model workflows, consisting of three fundamental elements: tokens, places, and transitions. Places are connected by transitions, which correspond to tasks or activities in a workflow, while tokens serve as triggers for transitions. Specifically, when all the input places have tokens, the following transition can be fired. Once fired, the transition generates new tokens and places them in the output places of the fired transition. Markings, which record the current distribution of tokens, reflect the state of the Petri net.

A Petri net is essentially a graph composed of places and transitions. Places are token holders, and transitions move tokens from input places to output places. Transitions can be considered as actions and are connected to input/output places by arcs. When all input places of a transition are have tokens, the following transition is fired, during which the action represented by the transition is executed. Subsequently, new tokens are generated by the fired transition, and placed in all the output places of the fired transition. The distribution of tokens among places is called a **marking**, which reflects the current state of the workflow.

Petri nets have the advantage to intuitively represent the entire workflow as well as the real-time process state. Meanwhile, they are adept at detecting and verifying potential logical errors, such as deadlocks or live locks for their mathematical properties [192], enhancing the security of smart contracts. Therefore, Petri nets have been applied in coordinating cross-domain workflows, for example, [81] applied extended Petri nets equipped with interfaces with Oracles that are used to receive external information, in order to cope with workflows that require external data. As Figure 3-3 shows, when the external requirement is satisfied, the Oracle interface can put the token into the place, and trigger the following tasks.

However, off-chain tasks extend beyond mere data transfer; they can involve complex processes that may not always be enforceable. For instance, in a supply chain workflow, a manufacturer may fail to deliver the product to the wholesaler, but falsely declare the task as "accomplished" on the blockchain. Such deviation to the workflow might lead to the collapse of cooperation. Therefore, this solution aims at integrating incentives into classical Petri nets to enhance the enforcement of off-chain tasks in cross-domain workflows. This integration promotes cooperation and reduces the risk of non-compliance among involved parties.

3.2.3 Token economy

A token economy is prevalent in behavior modification programs in social science [83, 77]. These programs typically consist of three essential components: the **target behaviors** that are wished to be reinforced; the **tokens** earned for engaging in those behaviors; and the **back-up reinforcers** that can be obtained by exchanging tokens as rewards. For example, in a supply chain workflow, a wholesaler may incentivize manufacturers to deliver products on time by awarding badges to those who consistently perform the desired behavior. Manufacturers with the highest number of badges are then rewarded the privilege of extending the cooperation period. In this example, the badges are tokens, and the privilege of extending cooperation period is the back-up reinforcer.

It is important to note that the term "token" in the context of a "Token Economy" has a different definition and function than in Petri net. In a token economy, a token is an abstract concept that can take the form of any object or symbol, working as a secondary enforcer. Tokens themselves are worthless, but they can be exchanged for other valuable things. Hence, participants are motivated to engage in desired behaviors to earn tokens. The primary function of tokens in a token economy is serving as a intermediary in enforcing incentives. In contrast, in Petri net, tokens are a fundamental element that triggers the firing of transitions. They do not serve as incentives but are essential for executing tasks. Without tokens, transitions cannot be fired, and tasks cannot be performed. To distinguish these two types of token, the secondary enforcers in a token economy are denoted as E-tokens, and the ones in Petri nets are referred to as tokens.

This solution realizes an E-token economy by employing a peer audit based E-token assignment and aggregation process in the classical Petri nets. Specifically, parties involved in the blockchain are audited by their peers; those who successfully complete both on-chain and off-chain tasks have a higher chance of receiving E-tokens. The results of E-token assignments

are aggregated to determine whether or not **authorization tokens** (auth-tokens) will be assigned for activating the next round of cooperation. For the initial cooperation, each party is automatically assigned one auth-token.

Auth-tokens are essential for authorizing and activating the Petri nets. They allow only parties with auth-tokens to participate in the workflow. Since participation in workflows is valuable to parties, the opportunity for future involvement serves as a backup reinforcer to incentivize party cooperation. Let us refer to such E-token economy implemented workflows as "incentive-integrated workflows".

Incentive-integrated workflows not only encourage parties to fulfill their tasks in the workflow to cooperate, but also enable parties to timely evaluate their peers and select their next round cooperators, which is beneficial for enhancing trust. In the following section, detailed steps are presented for implementing incentive-integrated workflows on Hyperledger.

3.3 Incentive-integrated workflows on Hyperledger

This section first discusses how to integrate the assignment and aggregation processes of E-tokens in Petri nets, and then introduces the three-layer architecture that enables Petri nets to coordinate the on-chain and off-chain tasks involved in incentive-integrated workflows.

3.3.1 Incentive-integrated workflows

A classical workflow outlines the schedule of tasks needed to complete the application. In incentive-integrated workflows, an additional stage "incentive stage" is introduced before the workflow's completion, as depicted in Figure 3-4. The incentive stage encompasses the processes of E-token as-

signment and aggregation, corresponding to "peer audit" transitions and "authorization token assignment" transitions respectively. As illustrated in Figure 3-4, "peer audit" transitions are triggered when generated tokens are placed in "P1" and "P2"[1].

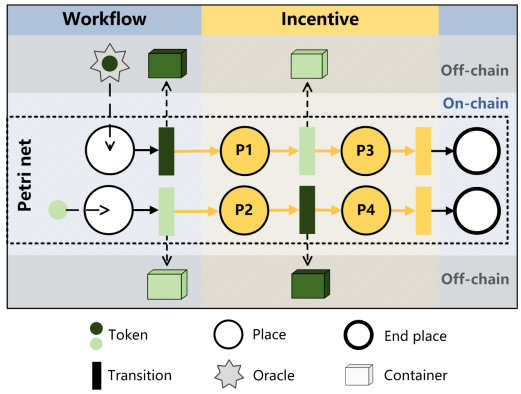


Figure 3-4: An example of incentive-integrated workflows, comprising a "work stage" and an "incentive stage". In the work stage, the first two transitions represent two off-chain tasks executed by two involved parties, distinguished by colors (deep green and light green). Following the execution of these two transitions, tokens are generated and placed in "P1" and "P2". Subsequently, peer audit transitions of the incentive stage are triggered, during which parties decide whether to assign E-tokens to each other. This scenario involves two parties, mutual evaluation occurs: each party evaluates the other. If a party decides to assign an E-token to the other party, a new token is placed at "P3" or "P4", triggering the subsequent on-chain auth-token assignment transitions. Only parties acquiring auth-tokens are able to activate and participant in the next round of the workflow.

In peer audit transitions, parties decide whether to assign an E-token to the party being evaluated based on their own observation of that party's task execution. Distinguished from pre-audit in Chapter 2, peer audit here is a typical post-audit, which analyses outcomes after operations.

[1] In Figure 3-4, there are two involved parties, and each party only requires the evaluation of the other. Therefore, the number of peer audit transitions is two. However, if there are N parties, the maximum number of peer audit transitions is $N^2 - N$, as each party is audited by all other parties. Nevertheless, the required number of peer auditors is configurable. By specifying this number, we can reduce the time complexity in the "incentive-stage".

For example, in a supply chain workflow, when a manufacturer is being evaluated by a wholesaler, the wholesaler can choose not to assign an E-token to the manufacturer if the wholesaler observes that the manufacturer did not deliver the products as regulated.

After peer audit transitions, the subsequent auth-token assignment transition will be fired if all the input places of the assignment transition have tokens. For instance, in Figure 3-4, if place "P3" receives the token generated from the previous peer audit transition, then the following assignment transition (colored yellow) will be fired. In the assignment transition, an auth-token is generated for the party being evaluated. This auth-token is required to activate the same workflow in the next round.

Whether the assignment transition can be fired, allowing a party to obtain the authorization token for the next round of cooperation, depends on both the peer auditing results, and the aggregation algorithm applied to the audit results. Various aggregation algorithms for the final assignment can be implemented, such as "veto power" [18], "majority rule" [16], and more. The chosen aggregation mechanism can be implemented by designing the auth-token assignment process of Petri nets. For example, in both Figure 3-4 and Figure 3-7, the veto power is implemented: the party under evaluation is rewarded with the auth-token only if all other parties have voted in favor of it (by assigning E-tokens). After completing the peer audit and auth-token assignment transitions, the marking of the Petri net finally reaches the end places.

In the first round of the workflow, auth-tokens are automatically assigned to all parties by default. However, for the subsequent rounds of the same workflow, auth-tokens are assigned based on the aforementioned E-token assignment and aggregation process. As a result, parties acquiring auth-tokens can participate in the next round of cooperation, while those not acquiring auth-tokens will be excluded from future rounds of cooperation.

This peer monitoring mechanism ensures that tokens serve as timely feed-

back on the behaviors of involved parties, encouraging them to fully complete their off-chain tasks and contribute to the workflow in an honest manner. Incentives are thereby integrated in the workflows. The following section elaborates on how to deploy and realize such incentive-integrated workflows at the program-level.

3.3.2 Map Petri nets to smart contracts

In this chapter, we utilize Hyperledger[2] as the foundation of our blockchain infrastructure. Hyperledger is an open-source blockchain technology that offers functionalities comparable to other smart-contract capable public blockchains, such as Ethereum. A significant distinction from public blockchains lies in Hyperledger's permission-based nature. It functions as a permissioned blockchain, allowing anyone to establish a private ledger using the concept of channels. This unique feature empowers us to configure private ledgers tailored to consortium collaborations and supports the creation of semi-trusted environments.

The actual Petri net graph is modelled as a set of assets within Hyperledger. These assets include: **tokens**, **places**, **transitions** and **arcs**, as introduced in Section 3.2.2. To map incentive-integrated workflows, two types of tokens are defined: **data-tokens** which are classic tokens carrying data, facilitating data transfer between transitions, and triggering transitions; **auth-tokens** that are designed for authorizing and activating workflows. Due to their distinct functions, data-tokens can be reused in multiple rounds of the workflow, whereas auth-tokens can only be used once; auth-tokens are set to be "USED" after they activate a workflow. Note that data-tokens are usually referred to as tokens in this thesis for simplification.

Correspondingly, places have two types. Certain places in Petri nets are designed to accept auth-tokens for activation, while the remaining places

[2] `www.Hyperledger.org`

can only accept data-tokens. When all the input places of a transition have tokens, the corresponding workflow task associated with this transition is triggered and executed. Following the execution, new tokens are generated and placed in the output places of the fired transition.

To deploy Petri nets on a blockchain (as presented in the Deploy Phase of Figure 3-2), parties need to define the four fundamental elements, places, transitions, tokens and arcs. This is done by a JSON file where each element is defined. These elements are private assets of parties[3]. For instance, an organization can define the required number of input and output places of each transition. This allows complex workflows to be effectively mapped into Petri nets.

Once Petri nets are well defined, they can be deployed on the blockchain. The **activation** step is necessary after deployment, which requires all parties to authorize the deployed Petri nets with auth-tokens. The activation of a workflow indicates a global agreement among parties on the deployed incentive-integrated Petri-net.

However, since workflows can encompass both on-chain and off-chain tasks, coordination between the blockchain layer and the infrastructure layer is required to trigger off-chain applications. To achieve this, a three-layer architecture, as shown in Figure 3-5, is employed to coordinate multi-domain workflows involving both on-chain and off-chain tasks.

3.3.3 Three-layer architecture

Figure 3-5 presents the three-layer architecture composed by the **blockchain layer**, **network layer**, and **infrastructure layer**. The blockchain layer not only records the progress of the incentive-integrated workflows but also facilitates firing transitions at the proper time. Within this layer,

[3]It is important to note that the auth-token assignment process contains an ownership transfer operation, as the auth-tokens are initially generated on-chain by other parties but later need to be assigned to the being evaluated party.

a Petri net is deployed as a smart contract on Hyperledger. Parties with wallets can execute tasks on the Petri net. Function *CompleteTransition()* is invoked after the task completed. This function puts tokens in the output places of the corresponding fired transition, followed by updating the public ledger with the latest markings, recording the current token distribution.

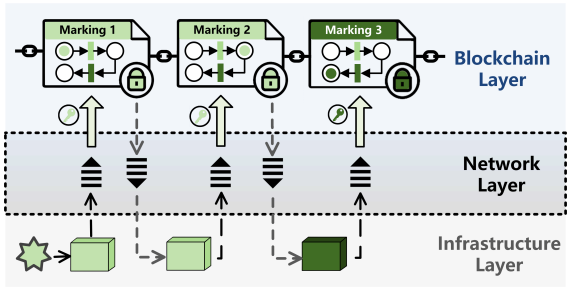


Figure 3-5: The three-layer architecture for coordinating cross-domain workflows using Petri Nets. In this architecture, Petri nets depicting the abstract multi-domain workflows are deployed on the blockchain layer. They can be activated after all parties authorize with their auth-tokens. When executing Petri nets, the completion of each task results in the generation of new tokens, accompanied by the creation and linkage of corresponding markings with existing blocks. When the tasks are executed off-chain, the architecture at the infrastructure layer update the Hyperledger through the network layer. Meanwhile, the network layer allows off-chain architecture components to listen to the latest markings on the blockchain layer, enabling domains to execute tasks at the appropriate time. In this manner, this three-layer architecture realizes a decentralized and transparent choreography of multi-domain workflows.

The network layer serves as a bridge connecting the blockchain layer and the infrastructure layer where off-chain tasks are performed. The network layer enables interaction between the other two layers: containers in the infrastructure layer keep listening to markings on the Hyperledger and execute the off-chain tasks once the marking indicating the input places of the transition receive enough tokens. Upon completion of the off-chain task, the latest marking is recorded as a new block and linked to the Hyperledger on the blockchain layer. A PKI system is used to label and

identify the created block, assigning ownership to a specific party. This tamper-proof synchronization of the markings ensures easy tracking of the workflow's progress for all involved parties. The interaction among these three layers realizes the coordination and monitoring of both on-chain and off-chain tasks in the workflow.

So far, the deployment and execution of incentive-integrated workflows have been discussed. The next section illustrates the application of the proposed in-box solution through a concrete use-case, where an alignment of semi-trust parties cooperate to enforce a designed workflow for mitigating DDoS attacks.

3.4 A DDoS use-case

A distributed denial-of-service (DDoS) attack is a type of services attack that overloads a system by flooding it with requests, preventing legitimate requests from being executed. One of the challenges in containing DDoS attacks is that blocking the detected IP addresses of malicious hosts is never enough for the attacked domains. The illegitimate requests can easily penetrate from those legitimate domains who did not block the malicious host [87]. Therefore, one possible solution is building an alliance where members can share information and block the illegitimate IP addresses at the same time, and dropping malicious traffic closer to the attack sources [62]. In the use-case, we assume there is such an semi-trust alliance to prevent DDoS attacks through the following protocol:

> *When a certain sensor in domain "A" is attacked by an illegitimate IP address, "A" needs to block the IP address and notify other members in the alliance, who have the obligation to block the illegitimate IP address after receiving the notification.*

This protocol outlines the workflow for a semi-trust alliance to mitigate

DDoS attacks. We first map this workflow into an incentive-integrated Petri net, and then simulate its enforcement. In this use-case, the alliance consists of three domains, distinguished by light, medium, and dark green in Figure 3-6.

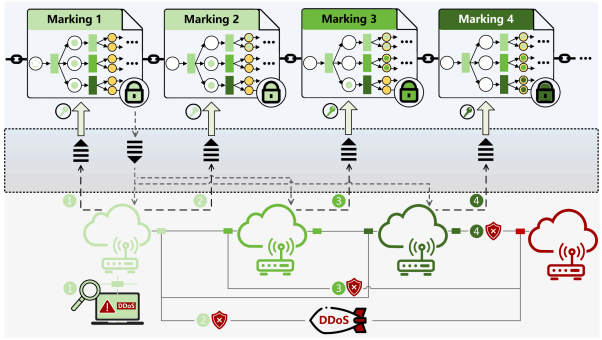


Figure 3-6: The workflow in a semi-trust alliance using a three-layer architecture. The DDoS-resistant protocol workflow is mapped into an incentive-integrated Petri net, and deployed on the blockchain. When a malicious host attacks, a domain triggers the activated Petri net by placing its token, initiating the subsequent transition which notifies alliance members about the illegitimate IP address. Afterwards, tokens are generated and placed at the three output places, the new marking that records this change will be added on the Hyperledger. Alliance members can listen through the network layer and fire the subsequent transitions of blocking the IP address. Each completed transition generates tokens which trigger the follow-up peer audit transitions in the incentive stage.

When a malicious host attacks a domain, the domain triggers the activated Petri net by placing its token at the start place. The subsequent transition, notifying alliance members with the illegitimate IP address, is then fired, followed by the generation of new tokens placed at the output places of the transition. The next three parallel transitions represent the task of blocking the IP address for each domain. Although these transitions are shown firing in sequence in Figure 3-6, in practice, they can be executed in different orders. Each transition results in generated tokens and markings, followed by the incentive stage.

To ensure the successful mitigation of DDoS attacks, it is crucial that all

members of the alliance adhere to the predefined workflow. To motivate semi-trust members to fulfill their obligations, implementing incentives is necessary. In the DDoS use-case, domains can detect the origins of DDoS attacks, allowing them to identify members who have failed to block the illegitimate IP addresses. The peer audit process in our solution offers alliance members the opportunity to evaluate their peers. The subsequent on-chain auth-token assignment transition can be triggered and executed only if all other members assign E-tokens.

Similarly to the blocking transitions, the peer audit transitions of all domains are parallel and can be accomplished in any order in practice. For simplicity, Figure 3-7 only presents the incentive stage of the attacked domain, the incentive stage of the other two domains is analogous. Ideally, dishonest domains receive no auth-tokens after the incentive stage and are excluded from future cooperation. With this timely feedback, the proposed solution motivates domains to be honest and adhere to the protocol.

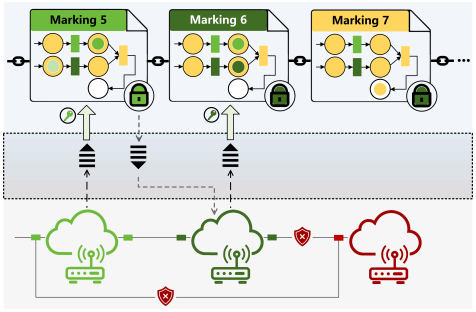


Figure 3-7: The incentive stage of Petri net in the DDoS use-case. Two types of transitions are involved in this incentive stage, 1) peer audit transitions, where parties are evaluated by peers who decide whether to assign E-tokens; 2) Auth-token assignment transitions, in which the outcomes of the audit process are aggregated to determine the assignment of on-chain generated auth-tokens to the evaluated domains. Whether the auth-token assignment transitions are triggered depends on both the audit results and the selected aggregation algorithm. In this particular case, the veto power aggregation mechanism is implemented, requiring two tokens to trigger the auth-token assignment transitions. Only when both of the other two parties assign E-tokens will the evaluated party be assigned an auth-token.

To simulate the enforcement of the protocol in the proposed solution, the Kathara emulator[4] is used to create a hypothetical internet scenario. Kathara emulates a network as a set of Docker containers, where each device is a container, and collision domains are represented by Docker networks. This setup creates a functional network environment, enabling interactions with real devices at the infrastructure layer.

To connect the infrastructure layer to the blockchain layer, we use an MQTT message queue at the network layer. As shown in Figure 3-6, domains use MQTT to create new markings on the Hyperledger, and listen to the latest markings on the blockchain to fulfill their obligations in the workflow.

In our demonstration, the peer audit transitions have not been fully implemented in the emulator, and the evaluation of peers always returns true. As a result, the demonstration presents a scenario where each party assigns E-tokens to others and receives the auth-token after the incentive stage. The source code is available at https://github.com/dl4ld/petrinet.

3.5 Concluding remarks

Lots of explorations have been made in utilizing blockchain in facilitating secure inter-organizational workflows [22]. Since 2016, Weber et al., has proposed an approach that uses Solidity smart contract to execute multi-domain workflows [174, 103], where the smart contract is deployed on-chain and works as a centralized mediator or choreography monitor. Instead of focusing on monitoring and mediating, [36] proposed the framework "ChorChain" for better enforcing and auditing the activities in the workflow through event-based gates to allow only conforming operations being executed, and providing records retrieval interfaces for users. Some other works focus on cross-domain confidential data sharing within a

[4] www.kathara.org/

workflow, for example, [23] proposed an "Encrypter" framework ensuring data integrity and the confidentiality of data exchanged on the blockchain, where data exchange is encrypted and can only be decrypted by authorized organizations. In contrast, [133] addressed the challenge of enforcing access control policies by managing the data access authorizations in the coordination layer implemented on the blockchain framework.

These approaches can handle workflows that involve on-chain tasks, such as data storage and computation, as well as tasks that require off-chain data access. However, some off-chain tasks are difficult to monitor or enforce with these approaches. For example, in the use-case of DDoS attacks, it is challenging to guarantee that domains adhere to the protocol of blocking illegitimate IP addresses, even when domains declare task completion by creating new markings on the Hyperledger. This is an inherent limitation of smart contracts.

To address this issue and facilitate cooperation among such semi-trust domains, a solution that integrates an incentive mechanism is proposed, motivating participants to fulfill their obligations by rewarding them with future cooperation opportunities, specifically:

- A peer audit process is designed to determine whether parties should receive authorization tokens for future cooperation.
- The audit process and authorization token assignment process are integrated into the original workflows, which are referred to as incentive-integrated workflows.
- The incentive-integrated workflows are enforced by a three-layer architecture, where the blockchain layer supports the deployment of smart contracts, the infrastructure layer comprises the parties' system architectures for executing off-chain tasks, and the network layer bridges interactions between these two layers.

Through this solution, the two requirements set at the beginning of this

chapter are met. At the contract-level, workflows are mapped into smart contracts based on Petri nets, offering the benefits of descriptiveness and process logic verification. The integration of peer audit and auth-token assignment processes eliminates non-compliant parties and encourages honesty and compliance, thus enhancing the mutual trust among parties.

At the program-level, the three-layer architecture provides a trusted storage for smart contracts and the execution states of workflows. Both on-chain and off-chain tasks can be triggered at the appropriate time by listening to the markings on the Hyperledger. Consequently, this proposed solution enables timely, tractable, and auditable multi-domain workflow coordination.

To conclude, implementing the incentive-integrated Petri net on the described three-layer architecture can choreograph cross-domain workflow and further enhance the adherence of parties to the predefined tasks. On-chain tasks are enforced by smart contracts, while off-chain tasks are incentivized through peer auditing. To the best of our knowledge, this is the first work that integrates incentives into smart contracts for cross-domain workflow enforcement. This proposed solution is applicable to a range of workflows that involve hard-to-enforce tasks, such as those related to the Internet of Things, supply chain management, and federated learning.

It is important to note that although we use peer auditing to monitor semi-trust parties, this approach relies on the assumption that failures to adhere to the workflow can be observed by the parties. For example, in the DDoS use-case, a domain that fails to block the illegitimate IP address may impact other domains, enabling other domains to observe and evaluate their peers' performance. However, there are instances where non-compliant behaviors may not be immediately recognized due to their high concealment or delayed impact. In such cases, our integrated incentives cannot give effective feedback. To address this limitation, implementing incentives by an external auditing system may be necessary

(This topic will be the focus of the following two chapters). Nevertheless, the Hyperledger which records domains' declared successful activities still benefits the post-auditing process by recording the asserted accomplished activities. Therefore, this solution can be considered as a complementary approach to existing solutions in further enforcing off-chain workflow activities.

Another limitation of this solution is the simplification of the aggregation algorithm in the auth-token assignment, the veto power that we implemented may result in the honest and reliable domains being squeezed out if any of the parties maliciously give poor evaluation. To avoid this risk, future work should explore more comprehensive aggregation algorithms. Additionally, inspired by previous work [173], where a reputation system is built, and only domains with a high reputation are able to build the Hyperledger, another way to address the potential non-compliance could be building an independent reputation chain, and allowing domains to select collaborators based on the reputation chain. This would encourage domains to behave well to maintain their good reputation which increases their chances of future cooperation, meanwhile prevent domains from being completely deprived of the opportunity to collaborate.

Chapter 4

Design incentives from an institutional perspective

Abstract: This chapter addresses **RQ 3, "How to design incentives from an institutional perspective?"** In order to design more comprehensive incentives, this chapter constructs a model to assess incentives from multiple aspects, including their sustainability in execution and their effects on cooperation enhancement as well as market affluence promotion.

A version of the work in this chapter is published as "Costly incentives design from an institutional perspective: cooperation, sustainability and affluence" in *Proceedings of the Royal Society A*, 2022.

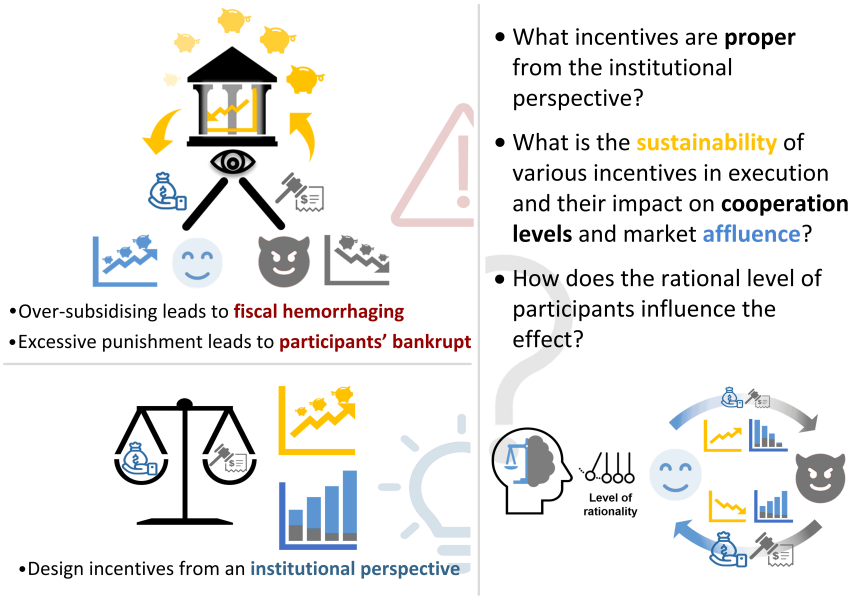


Figure 4-1: Graphical abstract of Chapter 4

4.1 Introduction

In human society, incentives like rewarding norm followers [151, 176] and punishing norm violators [69, 61, 126] are practical instruments for maintaining the order of a market or a community [154, 10]. When participants can gain extra benefits from breaking the norm, self-interests may drive the participants to be a norm violator, and choose to defect or cheat. Incentives, that change the benefits and cost of actions, can largely decrease the rate of non-compliant behaviors and promote collaborations. Because of the important role of incentives in real-world management, experimental and theoretical studies on designing practical and effective proper incentives are raising [156, 115].

Evolutionary game theory (EGT) is an analytical framework widely applied in analyzing and predicting the effect of the incentives [177, 178, 59], which relies on the Darwinian process of natural selection that drives participants toward the optimization of reproductive success [132, 72]. With EGT, the dynamics of participants' population composition under a specific incentive can thus be observed. Previous game-theoretic studies on the design of incentives mainly focused on the dynamics of cooperation, such as the emergence of cooperation [119, 79], the level of cooperation [177], or the sustainability of the cooperation [191], while few of them consider the **sustainability** of incentives, especially when incentives are enforced by an external third-party.

Based on the execution manner of incentives, related studies can be classified into two categories: 1) peer-to-peer incentives executed by participants (also called players) [143, 153, 171, 176]; 2) institutional incentives executed by a **third-party** [37, 121, 140], the third-party can be composed by players [120, 90], or completely external [32]. The enforcement of incentives can be costly [114, 28, 70], and thus the incentive might be terminated if the resources for implementation cannot cover the cost.

While it is reasonable to assume that the resource for implementing incentives is inexhaustible under the peer reward or peer punishment scenarios [111, 54], as volunteer punishment and altruistic rewarding can always emerge [66, 129], this is not the case when incentives are enforced in an institutional manner by the third-party [53, 163]. The cost of incentive enforcement can hardly be ignored [28, 70, 65, 64, 90], as the high cost can potentially lead to the failure in the enforcement process [120].

There are a few works considering minimizing the cost of incentive enforcement from the perspective of optimization, and managing to design cost-effective reward or punishment [63, 166, 45, 113, 169] for an external third-party (or external decision-maker [32]). In these studies, the third-party is composed of rule enforcers that do **not** necessarily belong to the system, and the income of such external third-party was not considered. When incentives are executed by a third-party entirely external to the system, the income of the third-party is often ignored. For instance, when a fraud happens in a market, the income of the judiciary, an institution independent of the market and supported by the nation, is rarely considered in the adjudication and enforcement process. Under these circumstances, prioritizing cost reduction and minimizing expenses holds practical significance. However, if the third-party belongs to the system, but is not composed by players, such as the owner or the maintainer of the market, then not only the costs, but also the income of the third-party need to be considered. Only when the third-party' cash flow is positive, can the incentive be executed sustainably. Hence, from an institutional perspective, an effective incentive needs not only to foster collaboration, but also to be sustainably implemented.

In addition to sustainability, in practice, the influence of incentives on the **affluence** of participants and the third-party is also vital. An incentive that performs well in fostering collaboration may result in undesirable side effects, such as reducing the accumulated wealth of players or shrinking the market size, which conflicts with the affluence growth and the prolonged

development of the market. Therefore, in this study, the evaluating criterion for incentives are extended beyond promoting collaboration to the sustainability and the impact on the market's affluence. Based on these criteria, we try to evaluate incentives from an institutional perspective.

Furthermore, the bounded rationality [35] of participants can be critical for institutional incentive design. Completely irrational participants would choose to cooperate or defect with an equal probability, leading to the failure of incentives. Highly rational participants aim to optimize their own benefits and are more policy-guided; however, their acute strategy selection might cause high incentive enforcement cost for the third-party. Therefore, when predicting the outcome of incentives, the factor of rationality should also be considered.

In all, this chapter aims at exploring the following questions: 1) What incentives are proper from the institutional perspective? 2) What is the sustainability of various incentives in execution, and how are their effects on cooperation levels and market affluence? 3) How does the rational level of participants influence incentive's effects?

To answer these questions, this chapter explores pure reward, pure punishment, and mixed incentives under the framework of EGT, identifying the analytical results of the cooperation dynamics under different incentives. Then, their sustainability in execution is explored by simulation experiments, where the income and cost for the third-party are introduced, and the assumption of an unlimited population [132] in EGT is relaxed by considering a limited market capacity, which might shrink if participants go bankrupt. In the simulation experiments, the cooperation level, sustainability, and the affluence of both players and the third-party are observed.

The remainder of this chapter is organized as follows: Section 4.2 introduces the incentive model, including the cost and income of different parties in the market. Section 4.3 outlines the analytical results derived

by the EGT, with this foundation, the subsequent section elaborates on the design of the simulation experiments. The experimental results are reported and interpreted in Section 4.4. Finally, this chapter concludes with a discussion of the results, and points out some future research directions.

4.2 Model

This section introduces the basic pairwise game played by the participants, and the incentives imposed in the market, followed by the introduction of income and expenditure for the third-party when maintaining the market. With these two parts, the dynamic model involving both the third-party and the participants is defined.

4.2.1 Pairwise game and incentives

Let us consider a market with two parties, N participants that have pairwise interactions, and one independent third-party that implements incentives for promoting cooperation. As players might lack professional regulator training, rarely can players freely switch roles from participant to maintainer. Hence, the third-party is assumed to be independent, rather than composed of players.

For homogeneous participants, each of them has the same strategy space $S = \{C, D\}$, where C and D represent cooperation (also known as compliance) and defection (also known as non-compliance), respectively. Choosing C by both of the participants can bring mutual benefits, whereas each of them has the temptation T to betray the other [112]. Such a situation is quite common in our daily life, and is often characterized using the prisoner's dilemma game (PDG) [54, 108]; PDG is hence selected as the basic game model[1]. The payoff matrix is given by Table 4.1, where the mutual

[1]It is worth noting that in our reality some more complicated scenarios can happen, for example, group interactions can replace the mentioned pairwise ones [121, 150].

cooperation (resp. defection) profit is R (resp. P), and the temptation for defecting is T.

		Player Y	
		C	D
Player X	C	R	$-T$
	D	T	P

Table 4.1: Payoff matrix of the prisoner's dilemma game

Incentives discussed in this chapter include pure reward, pure punishment, and mixed incentives. For pure reward, mutual cooperators will receive reward R_{CC}. The sucker's payoff[2] is R_{CD}, and $R_{CD} \geq R_{CC}$, ensuring that the reward for a sucker will be no less than the reward of a cooperator in a mutual cooperation. As for pure punishment, mutual defectors will receive the fine F_{DD}. The defector who betrays a cooperator will be fined by F_{CD}, and $F_{CD} \geq F_{DD}$. It means that the punishment for a defector in scenario $[D, C]$ will be no less than that for a defector in $[D, D]$. Mixed incentives require $R_{CD} + R_{CC} \neq 0$ and $F_{CD} + F_{DD} \neq 0$.

4.2.2 The income and cost for the third-party

To evaluate whether the incentive can be carried out in a sustainable way, it is assumed that only when the accumulated wealth of the third-party is non-negative, can the incentive be enforced. Hence, the income and cost of the third-party are introduced.

In practice, tax, membership fee, or commission fee are common resources imposed by the third-party for maintaining the order of the community or market [80, 168, 168, 54]. This study assumes the **income** of the third-party is composed of two parts: 1) the basic commission fee c_0 paid by participants in each round [188]; 2) the fine retrieved from the defec-

Meanwhile, participants can be heterogeneous in various features like risk preference or spatial position, etc. But in this dissertation, we start with the most basic homogeneous participants playing pairwise PDG game.

[2]The player who cooperates or acts in a cooperative manner but is taken advantage by the other player who defects is referred to as a sucker.

tors [47, 96]. Let M be the amount of participants in the market, and particularly, $M^{(t)}$ denotes the amount at time t ($M^{(0)} = N, M^{(t)} \leq N$). The concrete income depends on M as well as on the population distribution. The population profile is a vector $\mathbf{x} = \{x, y\}, x + y = 1$, wherein x (resp. y) is the fraction of the cooperators (resp. defectors). Specifically, $\mathbf{x^{(t)}} = \{x^{(t)}, y^{(t)}\}$ denotes the population profile at time t. Hence, the income of the third-party can be expressed as:

$$I^{(t)} = M^{(t)} \left(c_0 + x^{(t)} y^{(t)} F_{CD} + \left(y^{(t)} \right)^2 F_{DD} \right). \tag{4.1}$$

Remark 4.2.1. *When implementing pure reward incentives, $M = N$. However, punishment can eliminate participants who fail to pay the fines or commission fee. Thus, $M \leq N$ when implementing punishment.*

The **cost** of incentives is also composed of two parts: 1) the rewards assigned to the participants [6], 2) the cost for imposing the fine [123]. The reason for not considering the cost for imposing the reward is that, in real-world practice, it is usually the participants self-reporting their good behavior [52], which does not count as the major cost of the third-party. Therefore, the cost of rewarding is simplified as the endowed reward. Whereas the cost of enforcing punishment can be different, relying on detecting and monitoring [10]. This model assumes that the punishment cost is proportional to the probability and the strength of fine [37]. Let α ($\alpha \geq 0$) denote the unit cost of punishment for the third-party. The value of α depends on the specific cost of enforcement. Without loss of generality, we assume $\alpha = 0.3$ [128]. Accordingly, the expenditure of the third-party is defined as:

$$\begin{aligned} E^{(t)} = &\left(x^{(t)} \right)^2 M^{(t)} R_{CC} + x^{(t)} y^{(t)} M^{(t)} R_{CD} \\ &+ \alpha M^{(t)} \left(x^{(t)} y^{(t)} F_{CD} + \left(y^{(t)} \right)^2 F_{DD} \right). \end{aligned} \tag{4.2}$$

The wealth of the third-party at time t, $W_T^{(t)}$ is denoted as:

$$W_T^{(t)} = I^{(t)} - E^{(t)}, \tag{4.3}$$

and the accumulated wealth of the third-party is:

$$W_T = \int W_T^{(t)}\, dt. \tag{4.4}$$

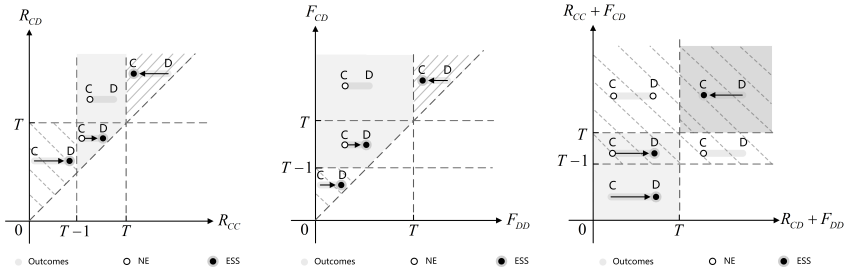
The explicit formula of W_T is given in Appendix A.3. W_T is required to be non-negative for sustainable incentives.

4.3 Analytical results and setup for simulation experiments

Based on the assumptions described in Section 4.2, the population equilibrium with various incentives can be delivered by EGT [38, 58]. This section starts with presenting the evolution of the population under different policies, more concretely, the corresponding thresholds of the incentives for achieving the Nash Equilibrium (NE) and the Evolutionary Stable Strategy (ESS). It then elaborates the design of the simulation experiments based on the derived analytical results.

4.3.1 Analytical results

The three fixed points are $x^* = 0, x^* = 1, x^* = (T - R_{CD} - F_{DD})/(1 + R_{CC} - R_{CD} + F_{CD} - F_{DD})$. In Appendix A.1, Table A.1-A.3 exhibit the requirements for x^* being a NE or ESS under various incentives. Figure 4-2 (a)-(c) visualize the results of the population equilibrium by different incentives, concrete derivations are given in Appendix A.1.



(a) Pure reward (b) Pure punishment (c) Mixed incentives

Figure 4-2: Equilibrium under pure reward, pure punishment, and mixed incentives. The requirement for $x^* = 1$ being a NE is that the strength of incentives (the value of R_{CC}, F_{CD} or $R_{CC} + F_{CD}$) being greater than $T - 1$. Further, when the strength of incentives is greater than T, $x^* = 1$ will be an ESS.

Figure 4-2(a) exhibits the results of pure reward incentives ($R_{CD} \geq R_{CC}$ always exists). It can be observed that if $R_{CC} \geq T$, cooperation ($x^* = 1$) will be the ESS. While given $R_{CC} \leq T - 1$, the ESS will be defection ($x^* = 0$). When $T \geq R_{CC} \geq T - 1$, $x^* = 1$ is the NE, but the strategy is not robust under this circumstance, which means the cooperation strategy can be invaded by mutants.

Figure 4-2(b) shows the results of pure punishment incentives ($F_{CD} \geq F_{DD}$ always exists). When $F_{CD} \geq T - 1$, $x^* = 1$ is always a NE, while $F_{DD} > T$, the $x^* = 1$ becomes an ESS. When the strength of punishment is too light, $F_{CD} \leq T$, then $x^* = 0$ is the ESS. The practical meaning is that the punishment should be at least greater than T which is the temptation can be gained from defection, otherwise the participants will have the motivation to become defectors.

Figure 4-2(c) shows a more complicated scenario where mixed incentive is applied. What matters to the equilibrium is $R_{CC} + F_{CD}$ (resp. $R_{CD} + F_{DD}$), the difference of the expected payoff for cooperators and defectors when facing a cooperator (resp. defector). In Figure 4-2(c), it is clear that as long as $R_{CD} + F_{DD}$ is less than T, then $x^* = 0$ is always an NE,

while only when $R_{CC} + F_{CD}$ is also less than T, $x^* = 0$ can be robust to mutations. This result indicates that only when the payoff differences of being a cooperator and being a defector are both less than T, $x^* = 0$ is the ESS. In addition, if $R_{CC} + F_{CD}$ is greater than $T - 1$, $x^* = 1$ becomes the NE, and when both $R_{CC} + F_{CD}$ and $R_{CD} + F_{DD}$ are greater than T, $x^* = 1$ is the ESS.

4.3.2 Simulation experiment description

As previously stated, in practical markets or communities, the number of participants is always finite. Therefore, in the simulation experiments, the size of the market is initialized as N. Meanwhile, as participants are of bounded rationality in real world, which brings more uncertainties to the effect and the sustainability of the incentives, the results under different level of participants' rationality are analyzed.

(1) Algorithm: the evolution of population

The Monte Carlo simulation experiment is leveraged to observe the accumulated wealth of the third-party and of the participants. This section mainly introduces the algorithm and the design of simulation experiments.

In the market, each of the N participants has an initial wealth $w_A^{(0)}$, the total initial wealth of participants $W_A^{(0)} = N w_A^{(0)}$. Players first pay the commission fee c_0 before playing the PDG pairwisely. Their wealth then gets updated based on the payoff matrix and the implemented incentive. Players who cannot afford the commission fee or fine will be eliminated from the market. Their population profile $\mathbf{x} = \{x, y\}$ will evolve with the following dynamic mechanism: let $\pi(C)$ (resp. $\pi(D)$) denote the average payoff of cooperating (resp. defecting) strategy. Based on the EGT framework, the dominant strategy can have more next generations. With the probability $p_1 = \left[1+\exp^{-\beta(\pi(C)-\pi(D))}\right]^{-1}$, the defector will imitate the co-

operating strategy, and the cooperator with $p_2 = \left[1+\exp^{-\beta(\pi(D)-\pi(C))}\right]^{-1}$ will adopt a defecting strategy [172]. β ($\beta \in [0, \infty)$) denotes the selection intensity, which represents the rational level of participants [148, 152]. A larger β indicates a more rational participant, and if $\beta = 0$, the participant chooses to be a collaborator or defector randomly. Consequently, x will be updated as:

$$x^{(t+1)} = \left(1 - x^{(t)}\right) p_1 + x^{(t)}(1 - p_2). \tag{4.5}$$

Then at time step $t+1$, the new generation of participants will be matched in pairs again to have another round of interaction. In the evolutionary process, we have $x^{(t)}$ to evaluate the cooperation level, the accumulated wealth of the third-party (W_T) to measure the sustainability, and the accumulated wealth of all the participants (W_A) to represent the affluence of the market. The pseudo code of the simulation algorithm is shown in Table 4.2.

Table 4.2: Algorithm for pairwise player stochastic dynamics

Input:	N, c_0, α, β, R, P, T, S, incentive mechanism parameters R_{CC}, R_{CD}, F_{CD}, F_{DD}, initial population profile $\mathbf{x}^{(0)}$, initial accumulated wealth of the third-party $W_T^{(0)}$, initial accumulated wealth of all the participants $W_A^{(0)}$, and the total observation time step $\mathbf{T}$[3].
Output:	Evolution of $x^{(t)}$, W_T, W_A.
Step 1:	If $t < \mathbf{T}$, compute the amount of cooperators and defectors based on $x^{(t)}$, then randomly match individuals in pairs, generate the **pair-wise table**. Else go to **Step 6**.

[3]The termination time is denoted as $\mathbf{T}$, which is distinct from a specific time step t.

Step 2: Based on the pairwise table, calculate the real payoff of each individual, and generate the **payoff table**. If and only if the participant's wealth cannot cover the commission fee c_0 or the fine (F_{CD} or F_{DD}), the participant will be eliminated.

Step 3: Calculate the income and expense of the third-party at time step t, update W_T.
Calculate the average payoff of cooperators, update $\pi(C)$.
Calculate the average payoff of defectors, update $\pi(D)$.

Step 4: Calculate $x^{(t+1)}$ according to eq.4.5.

Step 5: Go to **Step 1**.

Step 6: End.

The settings of the parameters related to the market feature are presented in Table 4.3. With these settings, the population evolving algorithm can be implemented to observe the effect of various incentives.

Table 4.3: Simulation setup for pairwise player stochastic dynamics

Model parameters	**Symbol**	**Value**
Number of initial participants	N	100
Commission fee	c_0	0.5
Cost related coefficient	α	0.3
Rational level of participants	β	[1, 2, 4]
Mutual cooperation payoff	R	1
Mutual defection payoff	P	0
Temptation payoff	T	2
Sucker's payoff	S	-2
Population profile	$\mathbf{x}^{(0)}$	{0.25, 0.75}
Initial wealth of participants	$W_A^{(0)}$	1000
Initial wealth of the third-party	$W_T^{(0)}$	1000

(2) Parameter settings for incentives

For observing the performance of the different incentives, three groups of simulation experiments are designed: pure reward, pure punishment, and mixed incentives.

- **Pure reward**: Based on the analytical results in Section 4.3.1, only when $R_{CC} \geq T - 1$ and $R_{CD} \geq T$, can $x^* = 1$ be a NE or ESS. In simulation experiments with $T = 2$, we set $R_{CC} = 1 + 0.25i$, $R_{CD} = 2 + 0.25i$ where i ($i \in \mathbb{N}, i \leq 8$) represents the strength of the incentive. A higher value of i indicates a stronger incentive.
- **Pure punishment**: Similarly, we set $F_{CD} = 2 + 0.25i$, and $F_{DD} = 0 + 0.25i$ ($i \in \mathbb{N}, i \leq 8$).
- **Mixed**: For mixed incentives, we set both $R_{CC} + F_{CD}$ and $R_{CD} + F_{DD}$ varying from 1 to 3 and 2 to 4 respectively, with the increment of 0.25. There is no unique standard to set the rate of $\mathbf{R_{CC}}$ in $R_{CC} + F_{CD}$ (resp. $\mathbf{F_{DD}}$ in $R_{CD} + F_{DD}$). The rate depends on to what extent the system focuses on positive or negative incentive. In this group of experiments, to guarantee that $R_{CD} \geq R_{CC}$ and $F_{CD} \geq F_{DD}$ while minimizing the difference between the rewarding and the punishment, the rate is set to 0.2 (Related proof and the specific settings of these four parameters are provided in Table A.4 in Appendix A.2).

4.4 Experimental results and interpretation

This section first shows the effect of incentives on promoting cooperation, then elaborates the influence on the wealth of different parties, and finally discusses the sustainability of incentives.

4.4.1 Effect of incentives on cooperators' population and market size

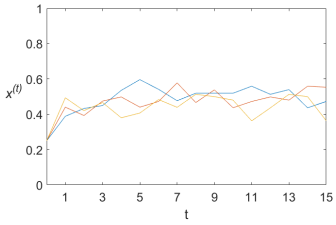


Figure 4-3: The dynamics of $x^{(t)}$ in 15 time steps of three repeating experiments. Parameters, $x^{(0)} = 0.25,\ \beta = 1,\ R_{CC} = 1,\ R_{CD} = 2$.

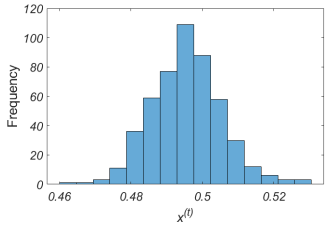
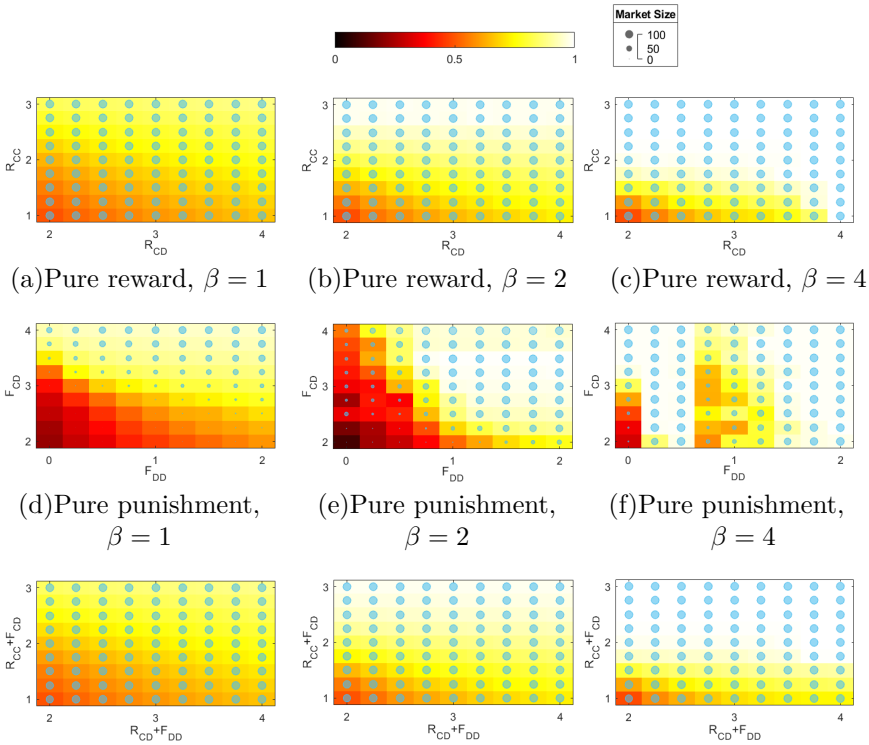


Figure 4-4: The frequency distribution of $x^{(t)}$ from time step 5 to 500. Parameters, $x^{(0)} = 0.25,\ \beta = 1,\ R_{CC} = 1,\ R_{CD} = 2$.

In a market with finite size, with the same population profile $\mathbf{x}$, the expected payoff of different strategies is not entirely fixed, due to the different possible pairs. Thereby, unlike the analytical results shown in Figure 4-2, the dynamics of x exhibits a chaotic behavior, fluctuating over time, and does not reach a fixed value. Figure 4-3 represents the evolution of x in the market contains 100 participants. Notwithstanding the fact that there is no strict "stable state" that can be reached, the determinism of x can be assessed by computational means [94]. With $\mathbf{T} = 500$, $x^{(t)}$ exhibits a normal distribution as shown in Figure 4-4. Since the **expectation of** $x^{(t)}$, $E\left(x^{(t)}\right)$, always exists, and depends on the incentive, the mean value of x^t is chosen to reflect the effect of incentives on the population profile. To determine the termination time, equivalence tests are performed on trials with $\mathbf{T} = [350, 300, 250, 200, 150, 100, 50, 30, 20]$. The goal is to find a termination time $\mathbf{T}$ where the expected value $E\left(x^{(t)}\right)$ for $t \in [5, \mathbf{T}]$ has no statistically significant difference from $E\left(x^{(t)}\right)$ for $t \in [5 : 500]$. After conducting the trials, $\mathbf{T}$ is set to 30.

The heat map in Figure 4-5 shows the expectation of $x^{(t)}$ under various incentives, the heat indicates the expected rate of cooperators in the market. As can be observed, the stronger incentives lead to higher expected $x^{(t)}$.



(a)Pure reward, $\beta = 1$ (b)Pure reward, $\beta = 2$ (c)Pure reward, $\beta = 4$

(d)Pure punishment, $\beta = 1$ (e)Pure punishment, $\beta = 2$ (f)Pure punishment, $\beta = 4$

(g)Mixed, $\beta = 1$ (h)Mixed, $\beta = 2$ (i)Mixed, $\beta = 4$

Figure 4-5: The expectation of $x^{(t)}$ and $M^{(30)}$ under different incentives. The heat represents the value of $x^{(t)}$, the area of the bubble represents the market size. Subplots (a)-(c), (d)-(f), and (g)-(i) represent the results under pure reward, pure punishment, and mixed incentives respectively. Incentives with higher strength are generally corresponding to higher $x^{(t)}$. Exceptions exhibit when the size of the market shrinks, which is caused by too light punishments. A higher rational level of participants also contributes to a higher cooperation level.

In addition, compare plots horizontally, as β increases, the expected $x^{(t)}$ becomes higher with respect to the same strength of the incentive. That is due to the fact that when participants are more rational, the selection will depend more on the payoff.

However, not all the subplots are in line with these rules, in Figure 4-5(f), the outcome of pure punishment with $\beta = 4$ is different. This fact is associated with the size of the market M. To better elaborate this

abnormal phenomenon, a bubble plot is drawn over the heat map to outline $M^{(30)}$. The area of the bubble indicates the value of $M^{(30)}$. From Figure 4-5(a)-(c) and Figure 4-5(g)-(i), it can be observed that under pure reward incentives or mixed incentives, the market size is stable, there are not many participants being eliminated. While under pure punishment incentives, the size of the market changes dramatically, which varies from 0 to 100. The abnormal cells shown in Figure 4-5(f) correspond to the situations where the size of the market shrinks a lot, $x^{(t)}$ is no longer strongly depends on the incentives, but on the choice of few bounded rational participants. An *ad hoc* example would be that a market with $M^{(t)} = 4$, if only one participant chooses defection, $x^{(t)}$ is 75%, then after this participant being eliminated in this round, two of the left ones are selected to interact at time step $t+1$, if only one of them choose to defect, then $x^{(t+1)}$ drops down to 50%, but if this participant chooses to cooperate, then $x^{(t+1)}$ increases to 1. Thus, when M is small, the effect of randomness counteracts the effect of incentives on the results, which leads to the abnormal cells in Figure 4-5(f).

Remark 4.4.1. *Under mixed incentives, the size of the market can also shrink a little bit when the incentive is not strong enough, but this result is not completely visible in Figure 4-5, we adjusted the scale in Figure 4-8 to visualize this pattern in a clearer way.*

The size of the market under various incentives presents some interesting patterns. Since only under pure punishment incentives, M changes a lot, we focus on the result shown on Figure 4-5(d)-(f). Firstly, M gradually becomes larger from the lower triangular part to the upper triangular part in each subplot. It reveals a counter-intuitive phenomenon, that less participants get eliminated under heavier punishment. The explanation is, the heavier punishment increases the payoff difference between cooperators and defectors, hence those bounded rational participants tend to choose cooperation. While under weaker punishment, participants tend to choose

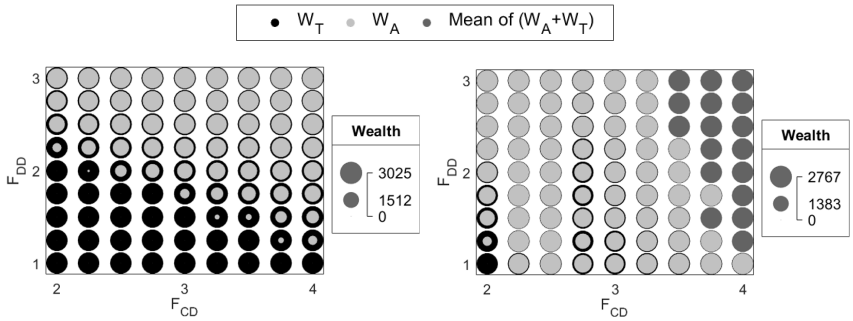
to defect repeatedly, especially when β is low. Hence, participants are easier to be eliminated. Secondly, punishment has a dual effect. On one hand, it reduces the payoff of defectors, increasing the payoff gap between cooperators and defectors, thereby promoting cooperation and maintaining M. On the other hand, if punishment is moderate, it efficiently eliminates participants who repeatedly defect, resulting in a significant drop in M. In Figure 4-5(f), when $F_{DD} \in [0, 0.5]$, the influence of promoting cooperation is dominant, leading to an increase in M as F_{DD} increases. Whereas when $F_{DD} \in [0.75, 1.5]$, the elimination effect becomes dominant, causing a substantial decrease in M. But when F_{DD} becomes even heavier, the cooperative effect regains dominance, resulting in an increase in M.

The experimental results in Figure 4-5 indicate: 1) as a general rule, the expected $x^{(t)}$ increases as the incentive becomes stronger, and this effect is more obvious with higher β. However, under pure punishment incentives, the shrinking market might involve low $x^{(t)}$; 2) in terms of the market size M, under pure reward as well as mixed incentives, M is stable, while under pure punishment incentives, counter-intuitively, M increases as the incentives become heavier.

4.4.2 Effect of incentives on the accumulated wealth of different parties

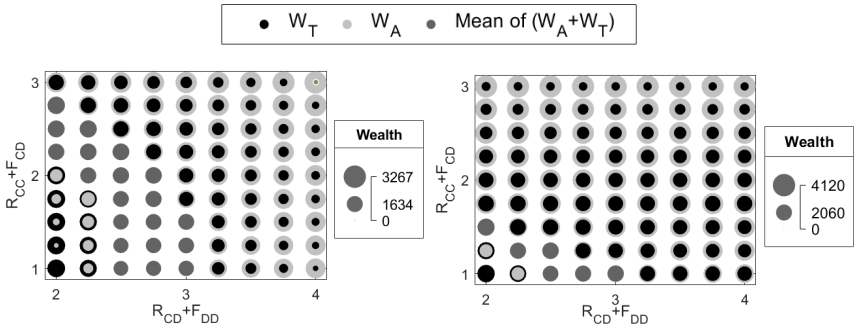
The parties in the market include the third-party who implements the incentives, as well as the participants who join the market. Both of these two parties can gain or lose utilities in the market. This section aims at analyzing the accumulated wealth of these two parties. Under pure reward incentives, the third-party subsidizes cooperators. As a result, it can be expected that the accumulated wealth of the third-party, W_T, decreases monotonically until the third-party goes bankrupt. Simultaneously, the accumulated wealth of the participants, W_A, increases monotonically. In contrast, for pure punishment and mixed incentives, the relative sizes of

W_T and W_A exhibit interesting behaviors, hence, this section focuses on the results of pure punishment and mixed incentive.



(a) $\beta = 1$ (b) $\beta = 4$

Figure 4-6: The accumulated wealth of the third-party (W_T, represented by black bubbles) and of the participants (W_A, represented by light gray bubbles) under **pure punishment** incentives. W_T is always greater than W_A. The difference between W_A and W_T diminishes as the punishment becomes heavier, especially when participants enjoy a higher rational level ($\beta = 4$).



(a) $\beta = 1$ (b) $\beta = 4$

Figure 4-7: The accumulated wealth of the third-party (W_T) and of the participants (W_A) under **mixed incentives**. There is a trade-off between W_A and W_T, W_A decreases while W_T increases as the incentives become stronger. Meanwhile, Pareto optimization space exists for increasing $W_A + W_T$. In addition, When participants are more rational ($\beta = 4$), both the upper limitations of W_A and W_T increase.

The accumulated wealth of the participants W_A and the third-party W_T is represented by bubble plots (Figure 4-6 and Figure 4-7), and bubble areas

represent the amount. Note that the smaller bubbles are drawn over the larger ones, so that the relative difference of the income of the two parties can be observed easily. Different parties are distinguished by colors, black links to W_T and light gray links to W_A. Particularly, when the difference between W_A and W_T is small ($|\log(W_A) - \log(W_T)| \leq 0.35$), the difference is hardly visible, we thus use the gray color to represent $(W_A + W_T)/2$.

Figure 4-6 and Figure 4-7 reveal that W_A increases as the incentives become stronger. As for W_T, **under pure punishment incentives**, W_T is always greater than W_A, as the income of the third-party contains the retrieved fine. Nevertheless, as the incentives become stronger, the population of defector decreases, thus the income of the third-party drops. Accordingly, the difference between W_A and W_T declines as shown in Figure 4-6. This phenomenon becomes more visible as β is greater, that is because having more rational participants means being easier to achieve $x^* = 1$ under the same incentives, which reduces the fine-based income of the third-party. Also, due to this reason, the upper bound of W_T drops down as β increases.

Under mixed incentives, the pattern becomes more complicated as shown in Figure 4-7, W_T declines as the incentives become stronger, while W_A exhibits an opposite trend. It can be observed that W_A catches up with W_T till surpasses it as mixed incentive becomes stronger. In addition, this figure exhibits an obvious trade-off between W_A and W_T. Yet, the Pareto optimization can be observed when incentives have moderate strength, maximizing the sum of the accumulated wealth of both parties.

When comparing the two subplots in Figure 4-7, the relative sizes of W_T with W_A depend on both the strength of the incentives and β. **Under low** β as shown in Figure 4-7(a), when $R_{CD} + F_{DD}$ is small, W_T is much greater than W_A, while as $R_{CD} + F_{DD}$ increases, W_T decreases and W_A increases. When $R_{CD} + F_{DD}$ is greater than 3, W_A becomes obviously greater than W_T. However, **under high** β as shown in Figure 4-7(b), it is

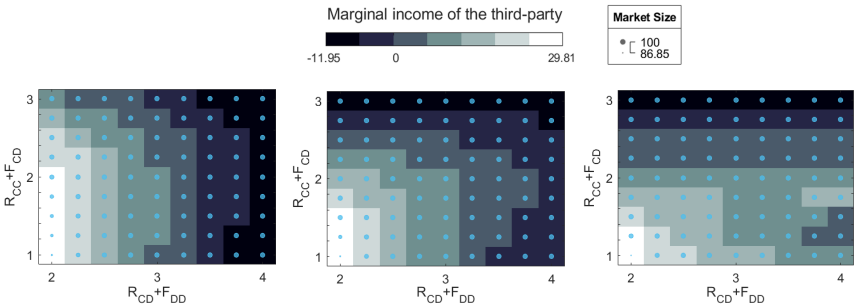
$R_{CC} + F_{CD}$ that mainly influences the trends of W_T and W_A. Especially, when $R_{CC} + F_{CD} \geq 1.75$, W_T becomes less than W_A, and as $R_{CC} + F_{CD}$ increases further, the difference between these two parties enlarges.

This pattern is attributed to β. A higher β value indicates more rational participants. Under the same incentives, it is easier to motivate participants to cooperate. Thus, with high β, as the mixed incentive becomes stronger, more cooperators will be in the market, which leads to a rapid increase in the cost of $R_{CC} + F_{CD}$. That is why W_T decreases dramatically as $R_{CC} + F_{CD}$ increases. However, when β is low, as $R_{CD} + F_{DD}$ becomes stronger, the total amount of compensation for suckers (R_{CD}) increases due to the presence of irrational defectors. Simultaneously, the fine collected from mutual defectors (F_{DD}) decreases because of a lower y induced by the stronger incentive. As a result, with low β, $R_{CD} + F_{DD}$ dominates the change of the wealth.

Summarizing the effect of incentives on W_A and W_T, the findings show that under pure punishment incentives, $W_T > W_A$, but $|W_T - W_A|$ reduces as the punishment become heavier; under mixed incentives, W_T decreases as the mixed incentive becomes stronger, while W_A presents an opposite trend. It is possible to improve $W_T + W_A$ by choosing the moderate strength incentives.

4.4.3 The sustainability of the mixed incentives

In this section, the slope of W_T is applied to evaluate the sustainability, as it can represent the marginal income of the third-party and predict the trend of W_T. An incentive is considered sustainable if this value is positive. For pure reward incentives, the third-party constantly rewards cooperators, making them unsustainable in the long term. In contrast, pure punishment incentives are always sustainable, because the third-part can collect fines from defectors in addition to the commission fee. Therefore, Section 4.4.3 only discusses the result for mixed incentives.



(a) $\beta = 1$ (b) $\beta = 2$ (c) $\beta = 4$

Figure 4-8: Sustainability of mixed incentives, $x^{(0)} = 0.25$. The colors of the cells represent the marginal income of the third-party. The results show that the marginal income decreases as incentives become stronger. Additionally, the sustainability of incentives is also influenced by the rational level of participants, β. Under mixed incentives, the market size is always greater than 86.

Figure 4-8(a)-(c) show that the marginal income of the third-party is negatively related to the strength of the reward or punishment. As mixed incentives become stronger, the slope of W_T changes from positive to negative, indicating that lighter mixed incentives result in a lower implementation cost, leading to a higher marginal income for the third-party, and enabling sustainability. While light mixed incentives can lead to a reduction in the market size M, it consistently remains above 86 under mixed incentives.

When comparing Figure 4-8(a)-(c) horizontally, the value of β has a strong influence on the sustainability of mixed incentives. When $\beta = 1$, participants are less rational, the market is always mixed with defectors, as indicated by Figure 4-5(g). If the incentives become stronger, the cost of R_{CD} will increase. It explains why when $R_{CD} + F_{DD}$ is greater than 3, the slope becomes negative, and incentives become unstable. When $\beta = 4$, more rational participants will choose to be cooperators, this fact increases the cost of R_{CC}. Thus, when $R_{CC} + F_{CD}$ is greater (≥ 2.75), incentives become unsustainable as shown in Figure 4-8(c). For Figure 4-8(b), when $\beta = 2$, it combines the feature of Figure 4-8(a) and Figure 4-8(c).

In summary, the results of the three groups of simulation experiments reveal varying performance of different types of incentives in promoting the cooperation level of participants, influencing the accumulated wealth of both participants and the third-party, and maintaining the market size M. Generally, stronger incentives are more effective in increasing the cooperation level. In terms of wealth accumulation, compared with pure reward incentives, pure punishment incentives ensure the wealth of the third-party is positive, making them constantly sustainable in execution. However, pure punishment also has the potential to eliminate participants and results in the shrinkage of the market size M. Counterintuitively, heavier punishment performs better in maintaining M. Under mixed incentives, the wealth of both parties show opposite trends. Moreover, choosing mixed incentives of the moderate strength can maximize the overall affluence ($W_A + W_T$). Nevertheless, mixed incentives are not always sustainable, their sustainability depends on both their strength and the rational level of participants.

4.5 Concluding remarks

During the last few decades, tremendous efforts have been devoted to designing appropriate incentives. Although the sustainability of incentives is considered a crucial criterion for evaluating real-world incentives and policies in the field of political economics [8], theoretical explorations often overlook the sustainability, especially when incentives are carried out by a third-party (or external decision-maker [32]). This chapter, from an institutional perspective, considers 1) the sustainability of incentives by introducing cost and income of the third-party in incentive execution; 2) the effect of incentives on the market's affluence via a participants elimination mechanism. The motivation for these considerations is twofold. First, we believe that when designing incentives, it is critical to consider their sustainability at the institutional level to ensure the practicality of

incentives. Second, the market is supposed to be viewed as an entire ecological system where its flourishing depends not only on the population of cooperators, but also on the market's size and the accumulated wealth of both parties involved.

Simulation experiments imply that pure reward incentives are unsustainable, given the fact that the third-party has to constantly provide high subsidies. However, this conclusion might be different under different assumptions for the income of the third-party. For example, Sasaki and Uchida proposed a sustainable pure reward incentives based on volunteer reward pool, assuming that the fund in the rewarding pool enjoys an interest rate, and the rewarding pool is shared by rewarders and cooperators [138]. Yet, this chapter focuses on institutional enforced incentives, assuming that the resources for rewarding are purely from commission fees, and with no interests rate. Therefore, the rewarding pool does not increase spontaneously. Meanwhile, to reach a high cooperating level, analytical results show that the reward needs to be greater than the temptation of defection (T), indicating a high cost of rewarding. These two assumptions lead to the opposite conclusion in this chapter, that pure reward incentives are unsustainable. The seemingly contradictory results highlight the subtlety of rewarding incentives, whose sustainability depends on the nature of the specific system.

For pure punishment, several published works have explored the requirements for sustainable pool punishment. For example, Matjaž et al. pointed out that punishing second-order free-riders can lead to sustainable pool-punishment in population-structured public goods games [120, 121]; Sarah et al. relaxed this requirement by introducing the signaling effect of participants knowing whether a punishment institution was established [140]. Different from traditional pool punishment, Lee, Colin, and Szolnoki proposed hiring mercenary punishers from players by the collected tax, to counteract second-order free-riders [90].

The model in this chapter distinguishes itself from these pool or mercenary punishment models by assuming that the third-party cannot be composed of players, considering the rule enforcers of a market is usually fixed by a group of professional managers or regulators. In this study, the punishing pool is composed of commission fee and retrieved fine, with α percent of the retrieved fine allocated to cover enforcement cost ($\alpha = 0.3$ [128]). These settings make the costly punishment sustainable. Additionally, by introducing the elimination mechanism where participants unable to afford the fine or commission fee are removed, the results show that punishment incentives can lead to a reduction of in market size. Light punishments may even lead to the collapse of a market, whereas heavier punishment better maintains the market size. Because heavier punishment improves the cooperation level more effectively. For the same reason, heavier punishment promotes the affluence of participants and the third-party in a long term. The findings further suggest that these positive effects of punishment incentives can be enhanced by more rational participants.

Few previous studies have explored how mixed incentives should be employed. Chen et al. found that the switch of incentive from reward to punishment based on the population of cooperators can effectively promote cooperation [28]. Fang et al. pointed out that mixed incentives which enjoy synergistic effects perform better on promoting cooperation [51]. In this study, we observe that mixed incentives not only lead to a high level of cooperation, but also exhibit advantages in terms of sustainability and affluence, compared with pure incentives. Specifically, compared with pure rewards, mixed incentives perform better regarding the sustainability. In comparison to pure punishment, mixed incentives can better maintain the market size ($M > 86$) and prevent it from collapsing, thereby ensuring the affluence of the market. Furthermore, experimental results reveal a trade-off between the wealth of the third-party (W_T) and that of participants (W_A). As incentives become stronger, W_T decreases while W_A increases. At moderate strength, the overall wealth, $W_T + W_A$, is maximized. Thus,

mixed incentives, to a certain extent, combine the advantages of pure incentives.

Back to the research questions proposed at the beginning of this chapter, we can draw the following insights:

- Evaluation criteria for institutional incentives: effective institutional incentives should consider criteria such as cooperation level, sustainability, and their impact on market affluence.
- Effects of various incentives:
  - Pure reward incentives promote participants' wealth but can hardly be implemented sustainably.
  - Pure punishment is always sustainable. Light punishment may reduce the market size, while heavy punishment helps maintain the market size, and benefits the affluence of both participants and the third-party.
  - Mixed incentives combine the advantages of pure incentives.
- Impact of participants' rationality: the level of participant rationality can significantly influence the effectiveness of incentives in promoting cooperation. Lower rationality necessitates stronger incentives to achieve a high cooperation level.

For future work, some of the assumptions in this study can be relaxed. For example, instead of always implementing punishment or rewards, probabilistic sanctioning can be an alternative way to reduce the cost of incentive implementation [102, 29]. Correspondingly, facing such uncertain punishment or reward, the players might not necessarily be risk-neutral. They can be risk-averse when facing punishments [111] or risk-seeking when facing rewards [181]. Such extensions on assumptions can adjust the third-party's cost in enforcing incentives, and tune the expected payoff of individuals, thereby influencing the effect of incentives. Considering

the constantly evolving environment, flexible incentives are potentially cost-efficient [147, 28, 166], evaluating their effect on affluence and their sustainability is of vital practical importance. By such extensions, more guidance are expected to be drawn in dealing with complicated scenarios.

Chapter 5

Enhancing incentive implementation against corruption

Abstract: This chapter addresses **RQ 4, "Can external supervision services combat corruption in incentive implementation?"** Aiming at improving incentive implementation, this chapter first assesses the impact of bribery collusion resulting from potential corruption, and subsequently explores the effectiveness of external supervision services, such as complaints or reports, in combating corruption.

A version of the work in this chapter is published as "The dynamics of corruption under an optional external supervision service" in *Applied Mathematics and Computation*, 2023.

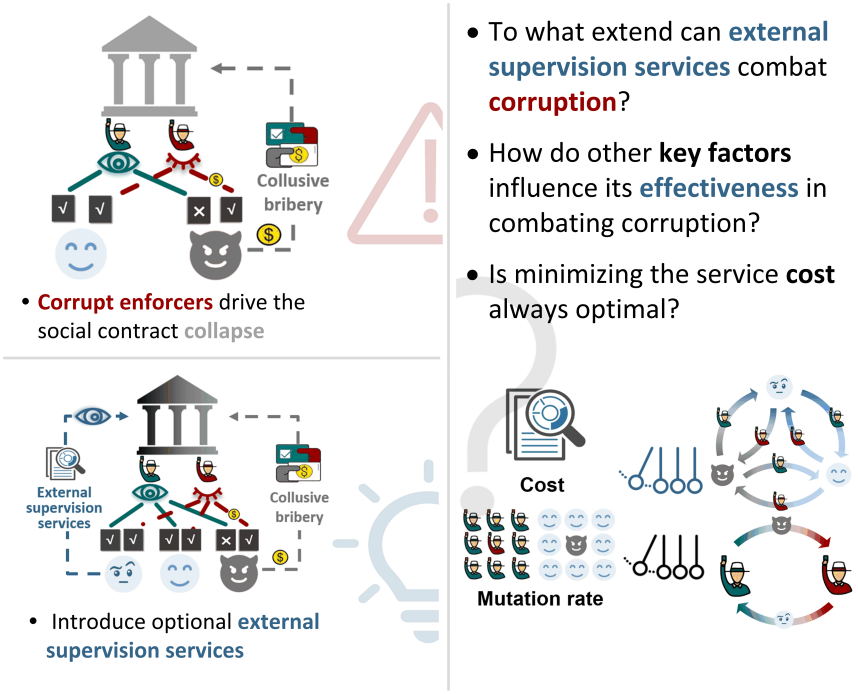


Figure 5-1: Graphical abstract of Chapter 5

5.1 Introduction

From simple groups of individuals to complex alliances of countries, incentives are a common way of constraining behaviors, ensuring interactions are compliant with any specified rules, and a means of promoting cooperative behavior [61]. Incentives are always carried out by an independent rule enforcer [93] who has complete oversight of the participants and executes punishments to the rule-breakers (resp. defectors), or rewards/compensates the rule-obeyers (resp. cooperators) [121]. However, the effectiveness of incentives can be undermined by pervasive corruption, as institutions are still operated by individuals with selfish motives [110, 4, 141, 101]. Corrupt authorities might accept bribes from the defecting participants who intend to escape from the punishment [91, 26] or to get the reward [99]. Such collusive bribery can encourage non-compliant behaviors, erode trust among the participants, and ultimately lead to the collapse of the social contract [91].

Combating pervasive corruption has thus attracted the attention of scholars from different fields. An achieved consensus is that transparency is critical for mitigating corruption. For example, Michael et al. proved the effect of transparency on mitigating corruption in public goods games(PGGs) through experiments as described in [110]; Brusca et al., based on survey data, analyzed the positive effect of transparency on fighting against corruption [19]. Supervision services are effective and common countermeasures in guaranteeing transparency facing corruption: companies can hire independent regulatory authorities to detect potential fraud [107, 175]; citizens can pay for certification [76], appraising or identification service if they suspect fraudulent behavior, and prepare for further available public activities such as complaints [159, 13], whistle-blowing, or reporting [185]. For the sake of brevity, let us refer to such services able to survey the process, assess the value, detect frauds, and provide certifications as **external**

supervision services. These external supervision services provide participants with an opportunity to supervise authorities by reducing the information asymmetry [105], thereby improving the transparency of the system, and ultimately combating collusive corruption.

External supervision services result in extra costs [159, 44, 118], naturally, the level of the cost can influence the participants' willingness to engage such services. If the cost is too high, there might be fewer participants to pay for the service, which makes the collusive bribery still hard to be discovered, and thus corruption can breed. However, not only the cost, but also the environment can influence the engagement strategy, since the benefits of the engagement depends on the probability of discovering the collusive bribery. If the probability of being cheated by peers, and the corruption level of rule enforcers are high, the engagement would be sensible. But if rule enforcers are honest and the participants are all cooperators, engaging the external supervision service is no longer a sensible strategy. Meanwhile, the participants' engagement to the external supervision service in turn shapes the environment. Rule enforcers have to count the extra income from the bribe against the risk of being discovered. As a consequence, when more participants engage the service, rule enforcers would tend to be honest.

Accordingly, the introduction of external supervision services can potentially control the corruption of rule enforcers and subsequently decrease the fraction of defectors among the participants. But these effects can be influenced by other factors, for example, the cost of the external supervision service. This chapter tries to figure out how the paid external supervision service influences the evolutionary dynamics of strategies employed by both rule enforcers and participants. This problem is ideally suited for analysis by evolutionary game theory (EGT), which relies on the Darwinian process of natural selection that drives participants toward the optimization of reproductive success [132, 142]. EGT has been widely applied to analyze and predict the dynamics of strategy profiles during

the evolution process [178, 59, 165, 102].

Recently, a number of papers have applied EGT to explore the key factors that might influence the corruption level of rule enforcers [14, 104], and the evolutionary dynamics of rule enforcers and participants [93, 91]. Additionally, EGT has been used to examine the influence of different anti-corruption controls on the corruption level, including social exclusion [100] and government authority's direct investigation [185]. These anti-corruption controls are of zero cost for the participants. However, it is still not yet fully understood when the control requires a certain cost for the participants [5]. Verma et al. explored how the complaint cost impacts the proliferation of the harassment bribes among varying structured population [159]. They found that with a lower cost of complaining, participants will tend to complain, and the population of honest rule enforcers is proliferated. In harassment bribes, participants are limited to interacting with the rule enforcers and can choose to either bribe or complain. In contrast, collusive bribes involve interactions among participants [3], where their payoff depends not only on the interactions with the rule enforcers, but also on their interactions with peers, deciding whether to collaborate or betray. This is the distinction in the strategy space of participants in collusive bribes and harassment bribes. In addition, considering a lower complaint cost could narrow the payoff difference between participants who complain and those who do not, which may encourage complaint abuse and eventually increase unnecessary cost among the participants. It is hence arguable whether minimizing the complaint cost is the optimized choice within the collusive bribery environment. This chapter thereby aims to answer the following questions: 1) To what extend can the external supervision service combat corruption? 2) How do other key factors, such as the service cost, influence its effectiveness in combating corruption? 3) Is minimizing the service cost always optimal for the market?

To address these questions, let us consider a general market composed of

two parties: rule enforcers who ought to enforce the incentives but face the temptation of bribes, and participants who can play games pairwise. Among the participants, the cooperators are provided with the optional choice of engaging the external supervision service, which can prevent potential loss caused by collusive bribery. To investigate the effect of such external supervision services on combating collusive bribery, we first construct a model to mimic the co-evolution of the strategies in both parties. The evolution of the strategies is then analyzed, using replicator dynamics in an infinite and well-mixed market; furthermore, we apply numerical simulation experiments to study the evolution within different sizes of finite markets. Our analysis reveals several interesting results, and premised on which, we propose a number of strategies to help manage such markets.

The remainder of this chapter is organized as follows: Section 5.2 introduces the basic model composed of the bribery game between rule enforcers and the participants, and the dilemma game played by participants. Section 5.3 provides the analytical results of player-enforcer dynamics with differing service cost in an infinite market, and some robustness analysis when participants can explore different strategies. Section 5.4 discusses the stochastic dynamics within finite markets of various scales. We conclude the findings and compare them with related work in Section 5.5.

5.2 The bribery game model with the external supervision service

Let us first consider a population of participants within a market and assume that interactions within this market operate as a pairwise social dilemma between two participants (also called players). The action space of players is defined as $\mathcal{A}_p = \{C, D\}$, where C is the strategy of the cooperators who obey the market rules, and D is the strategy of the defectors

who break the rules. Table 5.1 presents the payoff matrix of pairwise players. It can be regarded as a classic one-shot prisoner's dilemma where b is the payoff for mutual cooperation, and c is the temptation of choosing to defect [54, 108]. It can also be considered as a donation game where c is the cost for donation, and $b + c$ is the payoff when free-riding [72].

	C	D
C	b	$-c$
D	$b+c$	0

Table 5.1: Original payoff matrix

	C	D
C	$b - c_0$	$-c + f/2 - c_0$
D	$b + c - f - c_0$	$-f - c_0$

Table 5.2: Payoff matrix with rule enforcers implementing incentives

	C	D
C	$b - c_0$	$-c - c_0$
D	$b + c - B - c_0$	$-B - c_0$

Table 5.3: Payoff matrix with corrupt enforcers

Incentives are needed to maintain the order of the market. The payoff matrix shown in Table 5.1 indicates that defecting is the dominant strategy. Without incentives, all self-interested players will choose D, which leads to pure defectors where no one can gain any benefits. Accordingly, rule enforcers need to detect and punish the defectors, and protect the interests of the cooperators, for ensuring the order of the market. Since the implementation of the incentives is usually at a cost [167, 189], we assume that players need to pay c_0 ($c_0 < b$) to rule enforcers as a commission fee for joining this market.

In this model, both negative and positive incentives are considered. Each of the defectors is penalized with a fine f where $f > c$. kf ($k \in (0, 1)$) is used to cover the cost of rule enforcers in monitoring the market and collecting the fine. Each of the cooperators who were cheated by defectors receive a compensation of $(1 - k)f$ from rule enforcers. Without loss of generality, set $k = 0.5$. Under this mechanism, the dominant strategy is

C as shown in Table 5.2, and the market evolves into one that contains only cooperators.

Prevalent symmetric information provides two favorable conditions for collusive bribery. First, the defectors are more likely to bribe as the probability for players to discover the defection is low. As long as the cost of bribe B is less than the profit gained from cheating and less than the fine f, namely, $B < c < f$; bribing is preferable for defectors. Second, rule enforcers also tend to be corrupt, driven by the additional income B and the collusive bribe being unlikely to be detected. Such hidden bribes and corruption can change the payoff matrix completely. Table 5.3 describes the scenario in which bribes and corruption happen. Comparing Table 5.3 to Table 5.2, it can be observed that the existence of a bribe and corruption drives D to become the dominant strategy.

Hence, the strategy of players fully depends on whether the rule enforcers are corrupt or not. Let us denote the action space of enforcers as $\mathcal{A}_u = \{U_h, U_c\}$. For each pair of players, there is one enforcer in charge of incentive enforcement. If the rule enforcer is honest, C is the dominant strategy, otherwise D is the dominant one. Based on these variables, the level of corruption can be represented by the fraction of corrupt enforcers.

If there are no mechanisms to break the information asymmetry, then honest enforcers can become corrupt through social learning or natural selection, because of the additional income from the bribe B. Fortunately, the cooperators can protect their interests through external supervision services at cost a to check the interaction, and subsequently be informed about the existence of non-compliant behavior[1]. Once the collusive bribery between the defector and the corrupt enforcer is exposed, the corrupt enforcer needs to not only return the compensation $f/2$ and the commission fee c_0 but also cover the cost a for the cooperator. In addition, the defector

[1]This model assumes that there are infinite external organizations to offer external supervision services. The defector does not know which organization is hired by the cooperator. Thus, the second order bribe where the defector is able to bribe the hired organization is not considered.

is fined f. Hence, for cooperators, they can choose to engage the external supervision service or not. The strategy in which the service is (resp. not) engaged is denoted as C_a (resp. $C_{\bar{a}}$), and the corresponding cooperators are called cautious cooperators (resp. trusting cooperators). The payoff matrix of C_a, $C_{\bar{a}}$ and D facing an honest enforcer is denoted as A_h:

$$\begin{array}{c} \\ C_a \\ C_{\bar{a}} \\ D \end{array} \begin{array}{c} \begin{array}{ccc} C_a & C_{\bar{a}} & D \end{array} \\ \begin{pmatrix} b-c_0-a & b-c_0-a & -c+f/2-c_0-a \\ b-c_0 & b-c_0 & -c+f/2-c_0 \\ b+c-c_0-f & b+c-c_0-f & -c_0-f \end{pmatrix} \end{array},$$

facing a corrupt enforcer is denoted as A_c:

$$\begin{array}{c} \\ C_a \\ C_{\bar{a}} \\ D \end{array} \begin{array}{c} \begin{array}{ccc} C_a & C_{\bar{a}} & D \end{array} \\ \begin{pmatrix} b-c_0-a & b-c_0-a & -c+f/2 \\ b-c_0 & b-c_0 & -c-c_0 \\ b+c-c_0-f-B & b+c-c_0-B & -c_0-B \end{pmatrix} \end{array}.$$

For the rule enforcers, U_h can get $2c_0$ in all combinations of participants, while U_c can get c_0+B-a in the event (C_a, D), $2c_0+B$ in the event $(C_{\bar{a}}, D)$, and $2c_0+2B$ in the event (D, D). The strategy of rule enforcers is thus decided by the fractions of cautious cooperators (C_a), trusting cooperators ($C_{\bar{a}}$) and defectors (D) in the population. The next section discusses the strategy dynamics of participants and rule enforcers.

5.3 Player-enforcer dynamics in an infinite population

Let the total number of players be N, the number of players who choose strategy C_a, $C_{\bar{a}}$, and D be $\#C_a$, $\#C_{\bar{a}}$, and $\#D$; then the fraction of strategy S_i is $\#S_i/N$, $(S_i \in \{C_a, C_{\bar{a}}, D\})$. The strategy profile is thus denoted as $\mathbf{x} = (x_1, x_2, x_3) = (\#C_a/N, \#C_{\bar{a}}/N, \#D/N)$. Analogously, let M be the total number of rule enforcers, $M = N/2$, the strategy profile of rule enforcers is $\mathbf{y} = (y_1, y_2) = (\#U_h/M, \#U_c/M)$. The initial state of strategy profiles are noted as $\mathbf{x}^{(0)}$ and $\mathbf{y}^{(0)}$. $\mathbf{x}$ and $\mathbf{y}$ evolve within the simplex $\mathrm{S} = \Delta_3 \times [0, 1]$ spanned by the six points (C_a, U_h), ($C_{\bar{a}}$, U_h), (D, U_h), (C_a, U_c), ($C_{\bar{a}}$, U_c), (D, U_c). This section analyzes the dynamics of $\mathbf{x}$ and $\mathbf{y}$ within an infinite and well-mixed population under the framework of EGT [72, 71].

Considering an infinite and well-mixed population, the dynamics of $\mathbf{x}$ and $\mathbf{y}$ follow the replicator equations:

$$\begin{aligned} \dot{x_i} &= x_i\big[\big((A_h\mathbf{x})_i - \mathbf{x}^\top A_h\mathbf{x}\big)y_1 + \big((A_c\mathbf{x})_i - \mathbf{x}^\top A_c\mathbf{x}\big)y_2\big] \\ \dot{y_1} &= y_1(1-y_1)\big(\pi(U_h) - \pi(U_c)\big) \end{aligned}, \tag{5.1}$$

where $\pi(U_h)$ and $\pi(U_c)$ are the payoff of honest enforcers and corrupt enforcers:

$$\begin{aligned} \pi(U_h) &= 2c_0 \\ \pi(U_c) &= 2c_0(x_1^2 + x_2^2 + 2x_1x_2) + (2c_0 + B)2x_2x_3 \\ &\quad + (c_0 + B - a)2x_1x_3 + (2c_0 + 2B)x_3^2 \\ &= 2c_0(1 - x_1x_3) + 2Bx_3 - 2ax_1x_3 \end{aligned}. \tag{5.2}$$

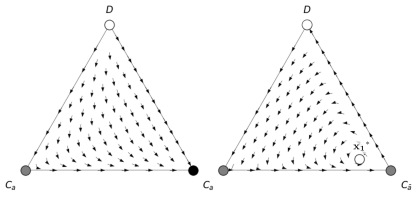
Thereby, we can analyze the dynamics of $\mathbf{x}$ and $\mathbf{y}$, and then discuss the robustness of the results under different exploration rates.

5.3.1 Player-enforcer dynamics without exploration

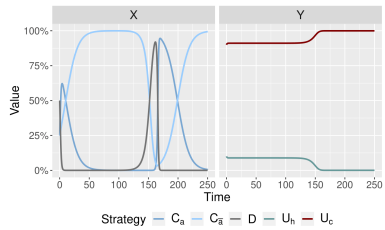
The simplex S in Figure 5-2(a) represents the dynamics of $\mathbf{x}$ with honest enforcers ($y_1 = 1$), while the simplex in Figure 5-2(b) represents the dynamics of $\mathbf{x}$ with corrupt enforcers ($y_1 = 0$). The values of parameters b, c, c_0, B, and f have been set as 0.5, 0.5, 0.2, 0.2, and 2, respectively, based on previous studies [93, 167, 91, 189, 92]. Changing these parameter values can impact the players' and rule enforcers' payoffs, thereby leading to different results. However, this study has opted to use commonly employed values for these parameters and only focuses on varying the level of a and exploration rates.

In the context of the evolutionary game theory framework, the boundary points that span S are invariant states. Therefore, the vertices of Δ_3 are fixed points [72]. In both Figure 5-2(a) and Figure 5-2(b), trusting cooperation ($C_{\bar{a}}$) is the dominant strategy on the edge $C_a C_{\bar{a}}$, the cautious cooperators thus evolve into trusting ones, and $\mathbf{x} = (1, 0, 0)$ is always a saddle point. With pure honest enforcers, $\mathbf{x}^* = (0, 1, 0)$ is the only asymptotically stable fixed point.

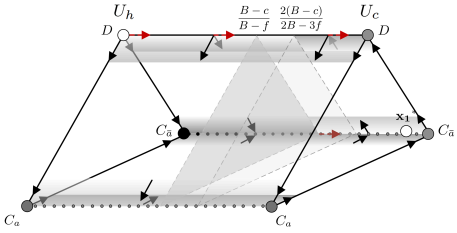
While with pure corrupt enforcers, there are no stable fixed points. The growth of $C_{\bar{a}}$ makes strategy D the dominant one, hence, the players' strategies adapt from $C_{\bar{a}}$ to D. Then, with the increase of x_3, cooperators are motivated to be cautious again. That's why the three fixed points located in the vertices of the simplex Δ_3 are unstable, as Figure 5-2(b) shows. Except for the three vertices, there is one internal fixed point $\mathbf{x_1}^* = \big((c-B)/f, 1-(c-B)/f-2a/(2a+f+2c_0), 2a/(2a+f+2c_0)\big)$. Let us first discuss the existence of $\mathbf{x_1}^*$, and then discuss its stability. Since $B < c < f$, it is easy to tell that $(c-B)/f \in (0,1)$ and $2a/(2a+f+2c_0) \in (0,1)$. Thus, when $x_1 + x_3 \in (0,1)$, namely, $2a + f + 2c_0 < f(f + 2c_0)/(-B + c)$, the interior fixed point $\mathbf{x_1}^*$ exists. Whether $\mathbf{x_1}^*$ is asymptotically stable depends on the real part of the eigenvalues of the Jacobian matrix (eq.B.2 in Appendix B.1.1) at $\mathbf{x_1}^*$. Figure 5-2(b) shows one unstable example



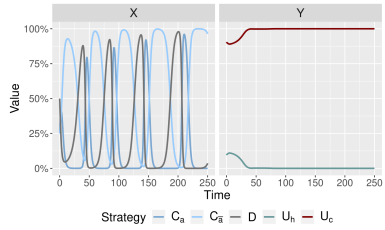
(a) $y_1 = 1$ (b) $y_1 = 0$



(d) $\mathbf{x}^{(0)} = (0.25, 0.25, 0.5)$, $\mathbf{y}^{(0)} = (0.1, 0.9)$, $a = 0.1$



(c) Mixed rule enforcers with $a = 0.1$



(e) $\mathbf{x}^{(0)} = (0.25, 0.25, 0.5)$, $\mathbf{y}^{(0)} = (0.1, 0.9)$, $a = 0.5$

Figure 5-2: Player-enforcer dynamics in an infinite well-mixed population. With the replicator equations (eq.5.1), the dynamics of $\mathbf{x}$ facing honest and corrupt enforcers are shown in Figure 5-2(a) and Figure 5-2(b) ($b = c = 0.5$, $c_0 = B = 0.2$, $f = 2$, $a = 0.1$). The white nodes are unstable fixed points, gray nodes are saddle fixed points, and black nodes are asymptotic stable points. In the simplex $\mathrm{S} = \Delta_3 \times 1$, ($y_1 = 1$), the dominance of pure trusting cooperation ($\mathbf{x}^* = (0, 1, 0)$) is the only asymptotic stable point. In the simplex $\mathrm{S} = \Delta_3 \times 0$, ($y_1 = 1$), there is an unstable interior fixed point $\mathbf{x_1}^*$, and with a lower a, $\mathbf{x_1}^*$ gets closer to the edge $C_aC_{\bar{a}}$. $\mathrm{S} \times [0, 1]$ in Figure 5-2(c) represents the dynamics of $\mathbf{x}$ facing mixed rule enforcers. The horizontal evolution directions of fixed points are shown with dashed arrows. Except for the seven fixed points on the left and right surface, all points on the edge C_aC_a (pure cautious cooperators) are saddle points; points on the edge $C_{\bar{a}}C_{\bar{a}}$ (pure trusting cooperators) are asymptomatically stable when $y_1 > (B - c)/(B - f)$, otherwise, they are saddle points. All points on the edge DD (pure defectors) are unstable, and players evolve from D to C_a or to both C_a and $C_{\bar{a}}$ (if $y_1 > 2(B - c)/(2B - 3f)$); rule enforcers evolve to corrupt ones. Without exploration, $\mathbf{y}^*$ is always reachable, and the equilibrium is decided by $\mathbf{y}^{(0)}$. Figure 5-2(d) and Figure 5-2(e) show the player-enforcer dynamics when $\mathbf{y}^{(0)} = (0.1, 0.9)$, in which $\mathbf{y}^* = (0, 1)$ and $\mathbf{x}$ exhibits cyclic dominance. A higher a has a stronger inhibition effect on cautious cooperators and a heavier punishment effect on corrupt enforcers, which induces the difference of the trajectories of $\mathbf{x}$ and $\mathbf{y}$ in Figure 5-2(d) Figure 5-2(e).

with $a = 0.1$. However, when $a = 0$, $\mathbf{x_1}^*$ is stable, and it is located on the edge $C_aC_{\bar{a}}$. A more elaborate stability analysis of $\mathbf{x_1}^*$ can be found in Appendix B.1.1.

Figure 5-2(a) and Figure 5-2(b) show two extreme scenarios, corresponding to the left and right surface of the triangular prism simplex $\mathrm{S} = \Delta_3 \times [0, 1]$ in Figure 5-2(c). This simplex captures the regime with mixed rule enforcers when $a = 0.1$. There are no interior fixed points inside $\mathrm{S} = \Delta_3 \times [0, 1]$, and neither on the back surface ($x_1 = 0$), the front surface ($x_2 = 0$), nor the bottom surface ($x_3 = 0$). However, all the points on edge C_aC_a and $C_{\bar{a}}C_{\bar{a}}$ are fixed points. In the following analysis, we further analyze $\mathrm{S} = \Delta_3 \times [0, 1]$ from the bottom surface to the upper edge DD.

On the bottom surface where $x_3 = 0$, since honest and corrupt strategies perform equally well for rule enforcers, facing a homogeneous population of cooperators, every fixed point on the edge C_aC_a and $C_{\bar{a}}C_{\bar{a}}$ are fixed points. For fixed points on C_aC_a, they are saddle points and unstable, as for players, C_a is dominated by $C_{\bar{a}}$ facing cooperators. For the fixed points on the edge $C_{\bar{a}}C_{\bar{a}}$, the transversal eigenvalue $\lim_{x_3 \to 0} \hat{x_3}/x_3$ changes sign at $(B - c)/(B - f)$. More specifically, when $y_1 > (B - c)/(B - f)$, the transversal eigenvalue is negative, which indicates that $\mathbf{x}^* = (0, 1, 0)$ is asymptotically stable and D cannot invade this trusting cooperative equilibrium. Whereas when $y_1 \geq (B - c)/(B - f)$, $\mathbf{x}^* = (0, 1, 0)$ is not asymptotically stable and can be invaded by defectors, then the fraction of corrupt enforcers will be aroused by the invading defectors, and finally move towards the right surface of the simplex $\mathrm{S} = \Delta_3 \times [0, 1]$ (Red arrows represent the horizontal evolution directions). Accordingly, all the fixed points on the left side of the dark gray triangle are stable, while those on the right side of the triangle are saddle points. It can be inferred that, in an infinite population, the initial strategy profile of rule enforcers is of vital importance to the evolution direction. If the market initially contains more honest enforcers $\left(y_1^{(0)} > (B - c)/(B - f)\right)$, players have a higher likelihood to evolve into pure trusting cooperators (More analysis

can be found in Appendix B.1.2). Otherwise, the system ends up with pure corrupt enforcers, and the strategy profile of players exhibits stable oscillations, as Figure 5-2(d) and Figure 5-2(e) show.

When $x_3 > 0$, there are no fixed points inside the simplex nor on the edge DD. On the edge DD, all points are unstable. When the market is completely composed of defectors, they eliminate themselves due to the fixed cost c_0, zero gain from the game, and the additional expense of bribing B. This feature of defectors is defined as "**self-inhibiting**" in the remainder of this chapter. The evolution direction at $\mathbf{x} = (0, 0, 1)$ depends on $\mathbf{y}$. As $\lim_{x_2 \to 0} \hat{x_3}/x_2$ changes sign at $2(B - c)/(2B - 3f)$, when $y_1 > 2(B - c)/(2B - 3f)$, both strategies $C_{\bar{a}}$ and C_a can invade, otherwise only C_a can invade. These two parts are segmented by the light gray triangle in Figure 5-2(c).

In order to explore the influence of the cost for engaging the external supervision service a, the player-enforcer dynamics under low cost $a = 0.1$ and high cost $a = 0.5$ are presented in Figure 5-2(d) and Figure 5-2(e), where $\mathbf{x}^{(0)} = (0.25, 0.25, 0.5)$ and $\mathbf{y}^{(0)} = (0.1, 0.9)$. Comparing these two subfigures, it can be observed that the value of a does not change the equilibrium, but it can influence the trajectories to the equilibrium.

For the dynamics of players, when $a = 0.5$, the summit of the fraction of C_a (x_1) is lower in each cycle, compared to when $a = 0.1$. This result is on account of the influence of a on C_a. Since C_a is the dominant strategy when there are enough defectors, once the fraction of defectors decreases below the threshold, $\#C_a$ decreases. A higher a increases the threshold, hence makes x_1 decrease earlier, leading to a lower summit. The other trend of x_1 is the absolute value of its negative gradient is larger. That is because $C_{\bar{a}}$ is dominant to C_a when cooperators are the majority, and a higher a strengthens this dominance. Then players transform from C_a to $C_{\bar{a}}$ faster. We generalize these two influences, reducing the summit and accelerating the elimination of C_a, as the "**inhibition effect**" of a on C_a.

Actually, it is the inhibition effect that accelerates the oscillations of $\mathbf{x}$. The lower summit of x_1 leads to more defectors remaining in the market, the event $(C_{\bar{a}}, D)$ then has a higher chance to happen. Since $\pi(D)$ is the highest in the event $(C_{\bar{a}}, D)$, the higher chance makes it easier for the defectors to invade when $C_{\bar{a}}$ is the majority. $\mathbf{x}$ hence is easier to move away from its unstable fixed point $\mathbf{x} = (0, 1, 0)$, which shortens the time of x_2 staying at the high level. In addition, the faster elimination of C_a also shortens the period. Therefore, the high a reduces the period of $\mathbf{x}$ by its heavier inhibition effect.

For rule enforcers, the fraction of corrupt enforcers (y_2) in the equilibrium is $y_2^* = 1$. Under a low a, y_2 increases monotonically from $y_2^{(0)} = 0.9$; but when $a = 0.5$, y_2 decreases briefly at the beginning. This difference is caused by the influence of a on U_c. In both circumstances, the defectors start with being eliminated by C_a in the event $(C_a, D)|(U_c)$ where $\pi(U_c) = c_0 + B - a$. a then turns out to be a punishment for the corrupt enforcers. Further, a high a means a heavier punishment, which weakens the dominance of U_C and decreases its rate. Let us name this consequence of a on rule enforcers as "**punishment effect**". Due to this punishment effect, $\#U_h$ increases at the beginning when $a = 0.5$.

In summary, from the analytical results, the dynamics of players facing honest enforcers are as one would expect: since $C_{\bar{a}}$ is the strict dominant strategy, $\mathbf{x}^* = (0, 1, 0)$ is the only global evolutionary stable state (ESS). When facing corrupt enforcers, there are no stable fixed points and $\mathbf{x}$ exhibits stable oscillations, with their frequency being higher for larger a. In the case of mixed rule enforcers, the evolution direction strongly depends on $\mathbf{y}^{(0)}$. When $y_1^{(0)} < (B - c)/(B - f)$, $\mathbf{y}^* = (0, 1)$, the dynamics of $\mathbf{x}$ is then the same as when facing corrupt enforcers; otherwise the equilibrium is $\mathbf{x}^* = (0, 1, 0)$, and the higher a is, the longer it takes to reach $\mathbf{y}^*$. Finally, the different levels of a can influence of trajectories of $\mathbf{x}$ and $\mathbf{y}$ through the inhibition effect on cautious cooperators, and the punishment effect on defectors.

5.3.2 Player-enforcer dynamics with exploration

This section analyzes the player-enforcer dynamics when players and rule enforcers explore alternative strategies with a certain probability, denoted as the exploration rate or mutation rate. Let μ and v be the mutation rate of players and rule enforcers. μ means that, in an exploration step, μx_i players from the population of S_i switch to one of the other two strategies, S_j and S_k. Meanwhile, $\mu x_j/2$ players from the population of S_j and $\mu x_k/2$ players from the population of S_k joining the population of S_i. Therefore, the change of x_i caused by mutation is $-\mu x_i + \mu x_j/2 + \mu x_k/2$. Similarly, for rule enforcers, the change of y_i brought by v is $-vy_i + v(1-y_i)$. Thus, the replicator equations with random exploration can be formulated as:

$$\begin{aligned} \dot{x_i} &= x_i\Big[\big((A_h\mathbf{x})_i - \mathbf{x}^\top A_h\mathbf{x}\big)y_1 + \big((A_c\mathbf{x})_i - \mathbf{x}^\top A_c\mathbf{x}\big)y_2\Big] - \mu x_i + \frac{\mu(1-x_i)}{2} \\ \dot{y_1} &= y_1(1-y_1)\big(\pi(U_h) - \pi(U_c)\big) - vy_1 + v(1-y_1) \end{aligned} . \quad (5.3)$$

To analyze the influence of the mutation rates on the player-enforcer dynamics, we first define two groups with two different mutation levels to study the influence of the absolute value of the mutation rates. In the low-level group, the mutation rate is 0.001 or 0.005 [56], and in the high-level group, the rate is 0.01 and 0.05 [91]. To better understand the influence of the relative values of μ and v, asymmetric mutation rates are designed for players and rule enforcers, assuming either $v < \mu$ or $v > \mu$. Accordingly, there are four total combinations of μ and v: $\{(\mu = 0.001, v = 0.005)$, $(\mu = 0.005, v = 0.001)$, $(\mu = 0.01, v = 0.05)$, $(\mu = 0.05, v = 0.01)\}$. The other variables are the same as in Section 5.3.1 ($b = c = 0.5$, $c_0 = B = 0.2$, $f = 2$). Figure 5-3 presents the results under $a = 0.1$ and $a = 0.5$.

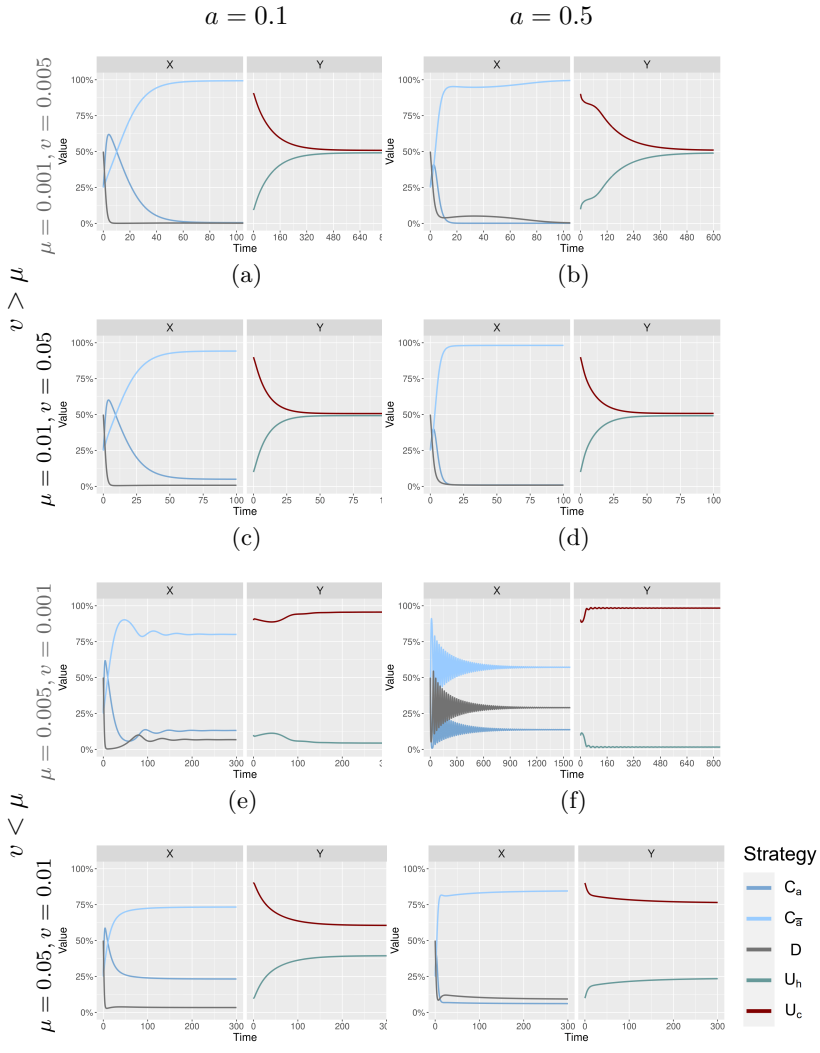


Figure 5-3: Player-enforcer dynamics in an infinite well-mixed population, allowing random exploration ($b = c = 0.5$, $c_0 = B = 0.2$, $f = 2$). With mutation rates μ for players and v for rule enforcers, $\mathbf{x}^*$ and $\mathbf{y}^*$ are always reachable, and the equilibrium of the system is robust to the initial state $\mathbf{x}^{(0)}$ and $\mathbf{y}^{(0)}$. When $v > \mu$, $\mathbf{x}^* \approx (0, 1, 0), \mathbf{y}^* \approx (0.5, 0.5)$ (Figure 5-3(a)-(d)). A higher μ leads more $C_{\bar{a}}$ to explore C_a, x_2 then increases; while this increment of x_2 can be offset by the stronger inhibition effect of a on C_a: when $a = 0.5$, the fraction of trusting cooperators is increased, which reduces the unnecessary supervision cost. For rule enforcers, a higher v almost does not influence $\mathbf{y}^*$ because $\mathbf{y}^* \approx (0.5, 0.5)$. When $v < \mu$, corrupt enforcers are always the majority, as Figure 5-3(e)-(h) show. Hence, a higher v means more U_c explore U_h, which improves the fraction of honest enforcers. For players, more honest enforcers corresponds to a lower frac-

tion of defectors. Nevertheless, the fraction of cautious cooperators (x_1) is not necessarily decreasing, because a higher μ and a lower a can lift x_1^* as Figure 5-3(g) shows.

In contrast to the results in Section 5.3.1, with exploration, $\mathbf{x}^*$ and $\mathbf{y}^*$ are always reachable. Furthermore, the equilibrium is independent of the initial state (See Appendix B.1.2). The equilibrium of the system as well as the time required to reach it are decided by a combination of the mutation rate and the cost a. From Figure 5-3, we observe that the relative value of μ and v are critical for $\mathbf{y}^*$. More concretely, when $v > \mu$, $\mathbf{y}^* \approx (0.5, 0.5)$ (Figure 5-3(a)-(d)), otherwise U_c is the majority (Figure 5-3(e)-(h)). The following discusses the results under $v > \mu$ and $v < \mu$.

(1) The mutation rate of rule enforcers is higher than that of players

When $v > \mu$, the equilibrium of players is $\mathbf{x}^* \approx (0, 1, 0)$[2], and the equilibrium of rule enforcers is $\mathbf{y}^* = (0.5, 0.5)$. In the low mutation group, players always reach equilibrium faster than rule enforcers, as Figure 5-3(a) and Figure 5-3(b) show. According to the analysis in Section 5.3.1, when the market is composed of pure trusting cooperators, $\mathbf{y}$ has no motivation to move, as strategies U_c and U_h perform equally well; but when $v \neq 0$, $\mathbf{y}$ continues evolving after $\mathbf{x}^*$ is already reached. The majority U_c mutates to U_h since $\pi(U_c) \approx \pi(U_h)|(x_2 \to 1)$, until $\mathbf{y}^* \approx (0.5, 0.5)$ is reached.

In the high mutation group, the time required to reach $\mathbf{y}^*$ is significantly shortened. This is because a higher v leads to more corrupt enforcers mutating into honest enforcers. The influence of higher μ is also applicable to $\mathbf{x}$: with a higher μ, the system reaches $\mathbf{x}^*$ faster. It is worth noting that the combination of μ and a decides the fraction of trusting cooperators in the stable state (x_2^*). Generally, a higher μ leads to a lower x_2^*, as more $C_{\bar{a}}$ can explore C_a. However, when $a = 0.5$, the strengthened inhibition

[2]Due to the mutation rate, x_2^* can approach but not reach 1. For instance, in Figure 5-3(a), $\mathbf{x}^* = (0.001000472, 0.9981471, 0.000852428) \approx (0, 1, 0)$. Identically, $\mathbf{y}^* \approx (0.5, 0.5)$ in Figure 5-3(a)-(d).

effect of a on C_a offsets the raise brought by the high μ, and lifts x_2^*. Accordingly, $x_2^*|(\mu = 0.01, a = 0.1) < x_2^*|(\mu = 0.01, a = 0.5)$ as Figure 5-3(c) and Figure 5-3(d) show. The fact that a higher a is associated with more trusting cooperators indicates that a lower a is not always better. A lower a might encourage more cooperators to seek the external supervision service spontaneously, which is unnecessary when facing cooperators; we call it as "**unnecessary supervision cost**" in the rest of the chapter.

(2) The mutation rate of rule enforcers is lower than that of players

When $v < \mu$, players have a higher mutation rate, and both players and rule enforcers reach a mixed strategy equilibrium. Within the low mutation group, $\mathbf{y}^* \approx (0, 1)$, $\mathbf{x}^*$ depends on a. In Figure 5-3(a), the fraction of defectors in the equilibrium is 0.068, rather 0.001 (when $v > \mu$). The persistent existence of D stimulates the growth of U_c, hence instead of $(0.5, 0.5)$, $\mathbf{y}$ evolves to $\mathbf{y}^* = (0.044, 0.956)$, where U_c is the majority, and the corresponding equilibrium of players is $\mathbf{x}^* = (0.132, 0.801, 0.068)$.

In the high mutation group, the fraction of honest enforcers in the equilibrium increases a lot compared to in the low mutation group. Because U_c is the absolute majority, with a higher mutation rate, more U_c explore strategy U_h, and y_1^* increases. For players, with more honest enforcers in the market, the fraction of defectors is lower. Although the remaining cooperators are surrounded by more U_h and fewer D, the fraction of C_a is not necessarily lower. This is because a higher mutation rate also means more $C_{\bar{a}}$ explore strategy C_a, which then raises x_1^*.

As for the influence of a, its inhibition effect of a on $C_{\bar{a}}$ decreases x_1^* in both low and high mutation groups. With less external supervision, the corresponding rate of U_c and D are higher.

In summary, the relative value of the mutation rates determines if rule enforcers can reach the equal dominance ($\mathbf{y}^* \approx (0.5, 0.5)$) where players

are of trusting cooperation dominance ($\mathbf{x}^* \approx (0, 1, 0)$). Only when $v > \mu$, $\mathbf{y}^* \approx (0.5, 0.5)$, and $\mathbf{x}^* \approx (0, 1, 0)$. Under this circumstance, a higher a corresponds to a higher fraction of the trusting cooperators, which reduces the unnecessary supervision cost. However, when $v < \mu$, the cost a together with the absolute value of the mutation rate determine $\mathbf{x}^*$ and $\mathbf{y}^*$; reducing a or increasing the mutation rate is beneficial in reducing the fraction of corrupt enforcers and promoting cooperation. We draw the following conclusions: increasing the mutation rate of v is always favorable for combating bribery corruption; the optimal a depends on whether $x^* \approx (0, 1, 0)$ is reached.

5.4 Stochastic dynamics in a finite population

5.4.1 Simulation experiments design

This section discusses the stochastic dynamics in a finite population. Three sets of experiments with different market sizes are designed: small scale with $N = 10$, medium scale with $N = 100$, and large scale with $N = 1000$. For exploring the effect of introducing the external supervision service and the related key factors on the stochastic dynamics, we first vary the level of a from 0.1 to 0.5; whereof 0.1 indicates low cost and 0.5 indicates high cost. In place of the replicator equations 5.3 that are applied in an infinite population, in a finite population, we assume players update their strategy from S_i to S_j with the likelihood $\left[1 + \exp\big(\mathbf{S}(\pi(S_i) - \pi(S_j))\big)\right]^{-1}$. Similarly, for rule enforcers, the likelihood of switching from U_h to U_c is $\left[1 + \exp\big(\mathbf{S}(\pi(U_h) - \pi(U_c))\big)\right]^{-1}$, and vice versa. The random exploration strategy is also adapted in the simulation experiments. The complete algorithm of the stochastic dynamics is listed in Appendix B.2.2. Table 5.4 shows the complete setup for the experiments.

Table 5.4: Simulation setup for player-enforcer stochastic dynamics

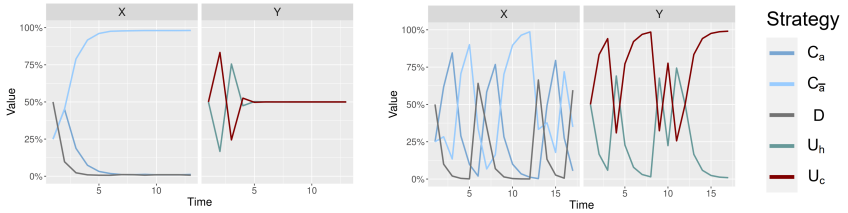
Model parameters	**Symbol**	**Value**
Number of players [167, 14]	N	$\{10, 100, 1000\}$
Payoff of mutual collaboration [91]	b	0.5
Cost of donation [91]	c	0.5
Commission fee [91, 189]	c_0	0.2
Fine [93, 91]	f	2
Cost of the bribe [91]	B	0.2
Cost of hiring an auditor [5]	$\mathbf{a}$	$\{0.1, 0.2, 0.3, 0.4, 0.5\}$
The mutation rate of players [91, 56]	$\boldsymbol{\mu}$	{0.001, 0.005, 0.01, 0.05}
The mutation rate of rule enforcers [56]	$\boldsymbol{v}$	{0.005, 0.001, 0.05, 0.01}
Selective strength	$\mathbf{S}$	10^{10}
Initial population of participants	$\mathbf{x}^{(0)}$	(0.25,0.25,0.5)
Initial population of rule enforcers	$\mathbf{y}^{(0)}$	(0.5,0.5)

In the simulation experiments, the termination time step $\mathbf{T}$ varies for different market sizes: $\mathbf{T} = 1000$ for $N = 10$, $\mathbf{T} = 2000$ for $N = 100$, and $\mathbf{T} = 5000$ for $N = 1000$. These time steps are adjusted and fixed after trials to ensure that the evolution time is sufficient to reveal the patterns of evolution and provide relatively accurate results in the presence of randomness.

5.4.2 Results of simulation experiments

For the evolution of $\mathbf{x}$ and $\mathbf{y}$, there are two possible patterns that can emerge: 1) the strategy profiles eventually evolve to stable states; 2) the strategy profiles show stable oscillations. Figure 5-4(a) shows an example of reaching a stable state, where $N = 10$. As can be observed, for players, the number of defectors decreases while the number of cooperators increases. The trusting cooperators eliminate cautious ones until they dominate the market ($\mathbf{x}^* = (0, 1, 0)$). For rule enforcers, as discussed in

the analytical results, when $\mathbf{x}^* = (0, 1, 0)$, any $\mathbf{y}$ can be a fixed point. In Figure 5-4(a), $\mathbf{y}^* = (0.5, 0.5)$, where the rule enforcers choose U_h or U_c with an equal probability.



(a) $N = 10, \mu = 0.01, v = 0.05, a = 0.1$

(b) $N = 1000, \mu = 0.001, v = 0.005, a = 0.5$

Figure 5-4: Stochastic dynamics in a finite population. The population profiles can either evolve into stable states or exhibit oscillations. Figure 5-4(a) shows the stochastic dynamics of $\mathbf{x}$ and $\mathbf{y}$ in a small scale market ($N = 10$), where $\mathbf{x}^* = (0, 1, 0)$ and $\mathbf{y}^* = (0.5, 0.5)$. Figure 5-4(b) shows an example of stable oscillations in a large scale market ($N = 1000$), where strategies exhibit cyclic dominance.

Figure 5-4(b) shows an example of stable oscillations in a large scale market. This phenomenon essentially comes from players' and rule enforcers' adaptation to the environment. Since the market scale is large, defectors cannot be completely removed. As the fraction of $C_{\bar{a}}$ grows, the occurrence of $(D, C_{\bar{a}})|(U_c)$ increases. When this event takes place, x_3 rises and x_2 falls, since $\pi(D) > \pi(C_{\bar{a}})$. Therefore, x_2 cannot reach 1. However, the increase of x_3 is constrained by the self-inhibiting nature of defectors: the flourish of defectors triggers the emergence of cautious cooperators, which in turn eliminate defectors. As a result, the fraction of cooperators increases, leading to a renewed rise in x_2 as the cycle repeats. Regarding $\mathbf{y}$, the high fraction of cautious cooperators hampers the growth of U_c by reducing $\pi(U_c)$ from $2c_0 + B$ to $c_0 + B - a$. Consequently, y_2 decreases after x_1 climbs up. However, y_2 cannot decrease to 0 because the persistent presence of defectors can stimulate the growth of U_c. The oscillatory pattern hence emerges.

In the simulation experiments, whether the oscillatory pattern occurs de-

pends on the market size N, the mutation rates (μ and v), and the cost of the external supervision service a. In a small scale market where $N = 10$, both $\mathbf{x}$ and $\mathbf{y}$ can always reach a stable state. In a large scale market where $N = 1000$, the strategy profiles always show stable oscillations. The most complicated case is the medium scale market, where $N = 100$, the strategy profiles can evolve into one of the two patterns, depending on the mutation rates and the external supervision cost a. For convenience, the results of experiments are reported in the order of $N = 10$, $N = 1000$, and $N = 100$. In each set of experiments, we elaborated on the influence of the cost a and the mutation rate on the stochastic dynamics.

(1) Stochastic dynamics in a small scale market: N = 10

When $N = 10$, since the number of players in the market is small and the low mutation rate does not influence the stochastic dynamics, only the results of the high mutation rate group ($\mu = 0.01, v = 0.05$ and $\mu = 0.05, v = 0.01$) are reported. For each set of parameters, the experiments are repeated 500 times.

In a small scale market, the strategy profile of rule enforcers eventually evolve to one of the stable states $\{(0.015, 0.985), (0.065, 0.935), (0.5, 0.5), (0.935, 0.065), (0.985, 0.015)\}$. The stable states with a small fraction of honest or corrupt enforcers are caused by the mutation rate v (Detailed proof is in Appendix B.3.1), i.e., $\mathbf{y}^* = (0.015, 0.985)$ and $\mathbf{y}^* = (0.065, 0.935)$ are equivalent to $\mathbf{y}^* = (0, 1)$ when $N = 10$. In the remainder of this chapter, for simplification, if the population evolves to a pure strategy equilibrium, $\mathbf{y}^*$ is written as $(0, 1)$. Hence, $\mathbf{y}$ evolves to one of the three equilibria: the dominance of honest enforcers ($\mathbf{y}^* = (1, 0)$), equal dominance ($\mathbf{y}^* = (0.5, 0.5)$) and the dominance of corrupt enforcers ($\mathbf{y}^* = (0, 1)$). The fraction of simulations (of the 500 repetitions) that reach these equilibria are shown in Figure 5-5. For players, when $\mu = 0.01$, $\mathbf{x}^* = (0, 1, 0)$ is always reachable (Details can be found in Appendix B.3.2), but when

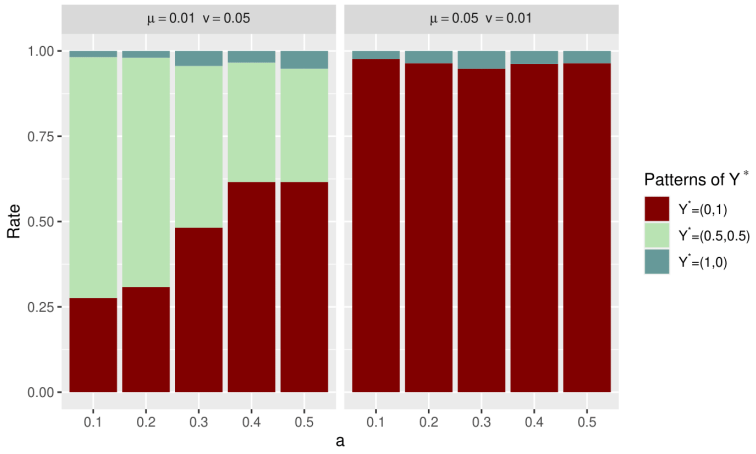


Figure 5-5: The relative frequency of specific equilibrium of rule enforcers among the 500 repetitions with $N = 10$. The combination of the mutation rate and a determines the dynamics of $\mathbf{y}^*$: when $v > \mu$ ($v = 0.05$), the probability of more than half of the rule enforcers being honest ($y_1^* \geq 0.5$) in the stable state is greater than 38.4%, whereas when $v < \mu$ ($v = 0.01$), the probability of evolving into pure corrupt enforcers ($y_2^* = 1$) is almost certain. In the former situation, the chance of $y_1^* \geq 0.5$ decreases with a higher a due to the inhibition effect of a on C_a; and in the latter situation, the punishment effect of a on U_c makes the relative frequency of $y_2^* = 1$ slightly decreases as a increases.

$\mu = 0.05$, $\mathbf{x}^*$ is only reachable when $\mathbf{y}^* = (1, 0)$; otherwise $\mathbf{x}$ presents stable oscillations.

For rule enforcers in an infinite market, we have discussed that $\mathbf{y}^* \approx (0.5, 0.5)$ when $v > \mu$, otherwise, rule enforcers evolve into a highly corrupt group where $y_2^* > y_1^*$. Within a small scale market, we also observe from Figure 5-5 that when $v > \mu$, the probability of $y_1^* \geq 0.5$ is much higher than when $v < \mu$. That is to say, when v is high, the market is more likely to evolve to the state where at least half of the rule enforcers are honest; whereas when $v < \mu$, the probability of evolving into corrupt dominance is greater than 94.8%, although evolving into honest dominance is still possible.

For players, $\mathbf{x}$ eventually evolves to a stable state that is composed of pure

trusting cooperators when $\mu = 0.01$. However, when $\mu = 0.05$, $\mathbf{x}$ might never reach a stable state. Considering $N = 10$, the average number of exploring players is 0.5, which means C_a or D can easily sneak in. Hence, when $\mathbf{y}^* = (0, 1)$, which is the most frequent outcome when $\mu = 0.05$, $\mathbf{x}$ presents a cyclic pattern as the left panel of Figure 5-4(b) shows.

The external supervision cost a can influence $\mathbf{y}^*$'s value. From Figure 5-5, it can be observed that the chance of $y_1^* \geq 0.5$ decreases as a increases when $v > \mu$. This phenomenon is caused by the inhibition effect of a on strategy C_a. With a lack of the external supervisions, the probability of $\mathbf{y}^* = (0, 1)$ is higher. However, when $v < \mu$, the relative frequency of extreme fixed points $\mathbf{y}^* = (1, 0)$ is also increasing. This counter-intuitive conclusion that rule enforcers have a higher probability to evolve to an honest equilibrium with the increase of a, is owing to the punishment effect of a on U_c. Increasing a induces a heavier punishment on U_c, and strengthens the dominance of U_h in the event (C_a, D), and therefore $\mathbf{y}^* = (1, 0)$ increases as a increases.

In summary, in small scale markets, the equilibrium of the rule enforcers' strategy profile is always reachable. In the stable state, enforcers can be composed of pure U_h, half U_c and half U_h, or pure U_c. The probability of a specific equilibrium depends on the relative value of exploration rates and a. When $v > \mu$, the probability of $y_1^* \geq 0.5$ decreases from 72.4% to 38.4% as a increases from 0.1 to 0.5; when $v < \mu$, the chance of $y_1^* = 0$ is more than 94.8%. For players, $\mathbf{x}^* = (0, 1, 0)$ is only reachable when $\mu = 0.01$ (Proved in Appendix B.3.2) or when $y_1^* \geq 0.5$ (Proved in Appendix B.3.2). Otherwise, it exhibits a pattern of cyclic dominance.

(2) Stochastic dynamics in a large scale market: N = 1000

In a large scale market, cyclic dominance emerges among different strategies for both participants and rule enforcers. The strategy profiles $\mathbf{x}$ and $\mathbf{y}$ can never reach equilibria because the large population makes it

more likely for rare mutations to occur and potentially lead to the emergence and spread of less dominant strategies. Nevertheless, the mean value of the fraction of corrupt enforcers or bribery defectors is critical to evaluate the corruption level of the market. Ergo, this subsection discusses the influence of the two key factors, the external supervision cost and mutation rate, on the mean value of the fraction of strategies, $E(\#S_i/N) = \sum_{t=1}^{t=5000}(\#S_i/N)^{(t)}/5000$, $S_i \in \{C_a, C_{\bar{a}}, D, U_h, U_c\}$. In addition, inspired by the results from the numerical experiments, the oscillation frequency (Figure 5-2(d) and Figure 5-2(e)) or the speed of fluctuations (Figure 5-3) can also be impacted by these two factors. We thus count the average cycle length of strategies $\mathscr{C}(S_i)$ and analyze the results. Experiments under each set of parameters are repeated 200 times. All the results are the average of the 200 repeated experiments.

Figure 5-6 shows the mean value of the fraction of specific strategies among the population. The mutation rates are distinguished by the line type, and the strategies are distinguished by the color. The results show that the mutation rate does not bring too much difference to $E(\#S_i/N)$; nevertheless, with higher values of μ, $E(x_1)$, $E(x_3)$, and $E(y_2)$ are higher. The influence of the service cost a is that a higher a induces more trusting cooperators and more honest enforcers, leading to higher $E(x_2)$ and $E(y_1)$.

When there is no exploration, it has been proven that players will evolve into homogeneous trusting cooperators ($\mathbf{x}^* = (0, 1, 0)$). However, in finite markets, although this trend still persists, the equilibrium is not reachable, because random exploration allows D to invade. The greater the μ is, x_2 is more likely to drop before it approaches one. This fact leads to the result that $E(x_2)|(\mu) < E(x_2)|(\mu')$ when $\mu > \mu'$. For the fraction of the other two strategies, C_a and D, they are more likely to rise before they approach zero, and thus have higher mean values as μ increases.

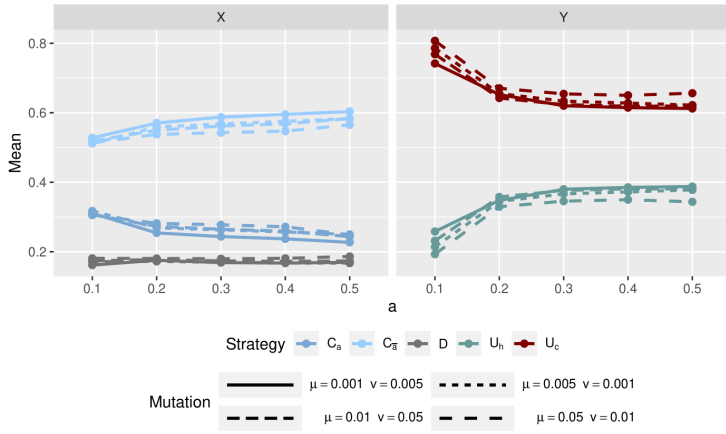


Figure 5-6: The mean value of the fraction of specific strategies ($E(\#S_i/N)$) in large scale markets where $N = 1000$. The influence of different mutation rates on $E(\#S_i/N)$ is as follows: $E(x_2)|(\mu) < E(x_2)|(\mu')$ when $\mu > \mu'$. A higher mutation rate makes C_a and D easier to sneak in before x_2 reaching 1, and hence decreases $E(x_2)$ and increases $E(x_1)$ and $E(x_3)$. $E(y_2)$ depends on both the relative value and absolute value of μ and v. $E(y_2)$ is higher when $v > \mu$ than when $v < \mu$. When the relative value is controlled, a higher mutation rate leads to a larger $E(y_2)$. Additionally, a higher value of a has an inhibiting and punishing effect on C_a and U_c, resulting in more trusting cooperators and honest enforcers.

For rule enforcers, $\mathbf{y}^*$ exists when the population is infinite, and the equilibrium depends on the relative value of μ and v: when $v > \mu$, $y_2^* \approx 0.5$, otherwise $y_2^* > 0.5$. However, in a finite market, $\mathbf{y}^*$ is not reachable due to the mutation rate. The cyclic pattern can be viewed as a series of reaching to and moving away from the potential equilibrium. Since the potential equilibrium of $y_2^*|(v > \mu)$ is approximate to 0.5, but when $v' < \mu'$, y_2^* is greater than 0.5, $E(y_2)|(\mu, v) < E(y_2)|(\mu', v')$ when $v > \mu, v' < \mu'$. Furthermore, the absolute level of mutation rate also has an influence on $E(y_2)$. Because a higher μ brings more remaining defectors, which induces a higher chance of the event $(C_{\bar{a}}, D)|(U_c)$, this fact leads U_c easier to invade. It explains $E(y_2)|(\mu) > E(y_2)|(\mu')$ if $\mu > \mu'$.

The influence of a on the mean value is, with the increase of the external supervision cost a, the fraction of C_a decreases, induced by the stronger

inhibition effect of a on C_a; meanwhile $E(y_1)$ increases, for the heavier punishment effect of a on U_c. Hence, a higher a introduces more honest enforcers and more trusting participants to the market.

To sum up, in a large scale market, the strategy profiles show cyclic dominance patterns. A lower service cost is not necessarily preferable, considering its punishing effect on corrupt enforcers. When a is higher, the punishment effect is strengthened, the average fraction of honest enforcers and trusting cooperators are higher. But such result is at the cost of more $C_{\bar{a}}$ being exposed to and eliminated by defectors.

Inspired by the cyclic pattern of strategies in Figure 5-4(b), we further explore the cycle length of a strategy $\mathscr{C}(S_i)$. $\mathscr{C}(S_i)$ is the time steps that it takes to finish one period, during which the fraction of the strategy S_i grows up from the bottom, reaches its summit and then drops to the bottom again. Results show that the mutation rates influence the cycle length of strategies significantly: $v > \mu$ is always related to a shorter $\mathscr{C}(S_i)$, and when the absolute value of mutation rate is lower, the corresponding $\mathscr{C}(S_i)$ is shorter. In addition to the mutation rate, a also determines the cycle length through its inhibition effect on C_a and punishment effect on D (Analysed in Appendix B.3.3).

(3) Stochastic dynamics in a medium scale market: N = 100

For medium scale markets, experiments under each set of parameters are repeated 500 times. Results show that: 1) in the low mutation rate group, $\mathbf{y}^* \in \{(0,1),(0.5,0.5)\}$, whether $\mathbf{x}^*$ is reachable depends on both the mutation rates and a; 2) in the high mutation rate group, both $\mathbf{x}$ and $\mathbf{y}$ show cyclic dominance patterns.

a. Stochastic dynamics in the low mutation rate group

Table 5.5 shows the relative frequency of $\mathbf{y}^* = (0,1)$ and $\mathbf{y}^* = (0.5,0.5)$ under the low mutation rate. Similar to the results in Section 5.4.2, when

$v > \mu$, the probability of evolving into $\mathbf{y}^* = (0.5, 0.5)$ is greater than when $v < \mu$. When $v > \mu$ ($\mu = 0.001, v = 0.005$), with the increase of a, the probability of $\mathbf{y}^* = (0.5, 0.5)$ decreases from 89.8% to 75%. This result is due to a's inhibition effect on C_a, which makes $C_{\bar{a}}$ eliminates C_a more thoroughly, followed by D's invasion. Then the event $(C_{\bar{a}}, D)|(U_c)$ stimulates the growth of U_c and drives $\mathbf{y}^*$ away from $(0.5, 0.5)$.

However, there are two increases of the relative frequency of $\mathbf{y}^* = (0.5, 0.5)$ when a increases from 0.1 to 0.2, and from 0.3 to 0.4. The first rise if caused by the stronger punishment effect on U_c, which obstacles the growth of U_c, and therefore rises up the probabilities of $\mathbf{y}^*(0.5, 0.5)$. The second rise is more complicated, when a further increases, both the inhibition effect and the punishment effect are stronger. The former drives $\mathbf{y}$ away from $(0.5, 0.5)$, the later drives $\mathbf{y}$ away from $(0, 1)$, which prolongs the required time of reaching the equilibrium (More details can be found in Appendix B.3.4). When $\mathbf{y} = (0.5, 0.5)$, if the event $(C_{\bar{a}}, D)|(U_c)$ never happens until $C_{\bar{a}}$ take over the market, then $\mathbf{y}^* = (0.5, 0.5)$ can be reached. Although such process is unlikely to happen especially when the fraction of $C_{\bar{a}}$ is increasing, the long dynamic time improves its probability.

Table 5.5: The relative frequency of $\mathbf{y}^*$ and $\mathbf{x}^*$ under the low mutation rate group with $N = 100$

a	$\mu = 0.001, v = 0.005$			$\mu = 0.005, v = 0.001$		
	$\mathbf{y}^* = (0, 1)$	$\mathbf{y}^* = (0.5, 0.5)$	$\mathbf{x}^* = (0, 1, 0)$	$\mathbf{y}^* = (0, 1)$	$\mathbf{y}^* = (0.5, 0.5)$	$\mathbf{x}^* = (0.006, 0.991, 0.003)$
0.1	10.2%	89.8%	100.0%	25.8%	74.2%	100.0%
0.2	7.2%	92.8%	100.0%	32.0%	68.0%	100.0%
0.3	26.0%	74.0%	79.6%	100.0%	0	0
0.4	19.6%	80.4%	80.4%	100.0%	0	0
0.5	25.0%	75.0%	75.0%	100.0%	0	0

When $v < \mu$ ($\mu = 0.005, v = 0.001$), the relative frequency of $\mathbf{y}^* = (0, 1)$ is high, and it increases with a higher a. This result is owing to the stronger inhibition effect of a, the lower mutation rate of rule enforcers, and the higher mutation rate of players. When a increases, the inhibition effect on C_a leaves more space for U_c to grow; at the same time, the lower v

makes it harder for U_h to invade. As a result, rule enforcers are less likely to evolve into the equal dominance, but into the corrupt dominance. Furthermore, unlike the scenario under $\mu = 0.001$, when $\mu = 0.005$, defectors can hardly get excluded permanently from the players. The persistent existence of defectors makes the event $(D, D)|(U_c)$ or $(C_{\bar{a}}, D)|(U_c)$ more likely to happen, which stimulates the growth of U_c and drives $\mathbf{y}^*$ to $(0, 1)$

Regarding $\mathbf{x}$, $\mathbf{x}^* = (0, 1, 0)|(\mu = 0.001)$ or $\mathbf{x}^* = (0.006, 0.991, 0.003)|(\mu = 0.005)$ (0.006 is caused by μ), pure cooperators in the stable state is the only reachable equilibrium. The sufficient condition of trusting cooperator dominance is $\mathbf{y}^* = (0.5, 0.5)$ or $a \leq 0.2$. The first sufficient condition is easy to understand, as $\mathbf{x}^* = (0, 1, 0)$ is the only equilibrium when $\mathbf{y}^* = (0.5, 0.5)$. The second sufficient condition comes from the inhibition effect of a. When $a \leq 0.2$, players eventually evolve into pure cooperators ($x_1^* + x_2^* = 0.997$), but if $a \geq 0.3$, the dominance of C_a is further weakened, which arouses the invasion of defectors.

Nevertheless, they are not necessary conditions of trusting cooperator dominance. When $a = 0.3$, there are 28 cases out of the 500 repetitions that $\mathbf{x}^* = (0, 1, 0)$ when $\mathbf{y}^* = (0, 1)$. The average required time for these outliers to reach the stable state is 1123.57, while that for the normal cases when $\mathbf{y}^* = (0.5, 0.5)$ is 28.54. The outliers only happen under a very specific situation where $C_{\bar{a}}$ is the majority and the remaining players are evenly split into C_a and D. Further, the remaining defectors must only be paired with other defectors or cautious cooperators. Then $\#C_a$ and $\#D$ further decrease, meanwhile $\#C_a$ increases until $x_2^* \geq 0.995$ (The detailed elaboration can be found in Appendix B.3.2). This process rarely happens, especially when N is larger; when $N \to \infty$, the chance of cooperation dominance facing corrupt enforcers is zero.

b. Stochastic dynamics under high mutation rate group

Under the high mutation rate group, both $\mathbf{x}$ and $\mathbf{y}$ show stable oscillations. Similar to the analysis in the large scale market, we also focus on

$E(\#S_i/N)$ as well as $\mathscr{C}(S_i)$, and track the influence of the mutation rate and the cost of the external service on them.

Figure 5-7 shows the average fraction of different strategies. We find $E(\#S_i/N)|(\mu) > E(\#S_i/N)|(\mu')$ if $\mu > \mu'$ ($S_i \in \{C_a, D, U_c\}$), and with the increase of a, $E(x_1)$ and $E(y_2)$ decrease monotonically. Compare to the results in a large scale market, the differences are: when $a = 0.1$, $E(y_2)|(N = 100) < E(y_2)|(N = 1000)$, hence, the slop of $E(y_2)$ is more gradual; and when $a \geq 0.2$, $E(x_1)|(N = 100) < E(x_1)|(N = 1000)$, hence the slope of $E(x_1)$ is steeper in medium scale markets.

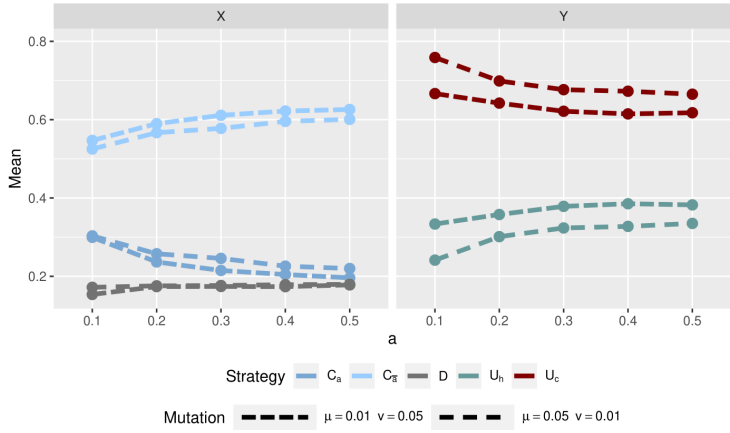


Figure 5-7: The mean value of the fraction of specific strategies ($E(\#S_i/N)$) in medium scale markets where $N = 100$. Comparing to the results obtained in large scale markets, the difference is $E(y_2)|(N = 100) < E(y_2)|(N = 1000)$ when $a = 0.1$. This difference is caused by the higher probability of the event $(C_a, D)|U_c$ which leads $\#U_c$ easier to decline from a high level and consequently reduces $E(y_2)$. However, this influence is offset by the stronger inhibition effect of a on C_a when $a > 0.2$. This stronger inhibition also explains the observation that $E(x_1)|(N = 100) < E(x_1)|(N = 1000)$.

The reason for these results is that when N is smaller, the event $(C_a, D)|(U_c)$ has higher probability to occur under the same $\mathbf{x}$ and $\mathbf{y}$ (Detailed proof is provided in Appendix B.3.5). The occurrence of the event $(C_a, D)|(U_c)$ makes $\#U_c$ more likely to drop from the high level, which reduces $E(y_2)$.

Nevertheless, such consequence is offset by the stronger inhibition effect of a on C_a when a increases from 0.2 to 0.5. That's why $E(y_2)$ has no significant difference in the medium or the large scale market when $a \geq 0.2$. Meanwhile, the heavier inhibition effect of a reduces the summit of x_1, which makes $E(x_1)|(N = 100) < E(x_1)|(N = 1000)$. The large decline of $Var(C_a)$ when $a \geq 0.2$ also confirms this reasoning (More detailed analysis is in Appendix B.3.3).

With regard to the cycle length, the results are almost the same as in large scale markets; the only difference is that the event $(C_a, D)|(U_c)$ is more likely to happen in medium scale markets, which amplifies the punishment effect of a on U_c. Since the punishment effect of a accelerates the elimination of U_c, and eventually shortens $\mathscr{C}(U_c)$, $\mathscr{C}(U_c)$ is monotonically decreasing when a increases (More detailed analysis is provided in Appendix B.3.3).

In summary, in a medium scale market, when the mutation rate of rule enforcers and players are low, keeping the cost of external supervision services no greater than 0.2 is enough to lead the system to evolve into a stable trusting cooperative cooperation. While within the high mutation rate group, similar to in large scale markets, the strategy profiles exhibit stable oscillations. Moderately increasing the cost is beneficial to improve the average fraction of both trusting cooperators and honest enforcers.

These three groups of simulation experiments conducted in small, medium and large scale markets provide representative evolution patterns and demonstrate the mechanism of a and mutation rates influencing the evolution. Despite the designed experiments have answered the research question, the largest scale of market is limited to 1000. Notably, if $N \to \infty$, the evolution of $\mathbf{x}$ and $\mathbf{y}$ will converge to the analytical results in infinite markets. Detailed proofs can be found in Appendix B.3.6. Additionally, it is important to acknowledge that, the assumption of $M = N/2$ simplifies the real-world scenario, as it is possible for one rule enforcer to monitor

multiple pairs of players. Relaxing this assumption may influence whether strategy profiles can evolve to equilibria, but conclusions regarding the effects of a and mutation rates hold. Concrete analysis can be found in Appendix B.3.7.

5.5 Concluding remarks

This study explores the effectiveness of introducing an optional external supervision service to cooperators on combating corruption. Considering that the decisions of players and rule enforcers both depend on and determine the environment [41, 161], a simple model is constructed, where players join in pairs, and each pair of players is assigned a rule enforcer. In this model, players can choose to be a cautious cooperator (C_a), who engages the external supervision service at the cost a; a trusting cooperator ($C_{\bar{a}}$), who does not engage the service; or a defector (D), who bribes the enforcer for escaping from the punishment. At the same time, rule enforcers can choose to be either an honest one (U_h), to enforce the incentives; or a corrupt one (U_c), who exonerates defectors for the bribe. The collusive bribery will be discovered in the event $(C_a, D)|(U_c)$ where C_a is paired with D and assigned U_c.

To better study the consequence of introducing the external supervision option, no additional explicit punishment mechanism is assigned to the corrupt enforcers. Classic explicit punishments for combating corruption include fining corrupt enforcers with a fixed penalty by the right authorities [12, 2] or by other honest enforcers [74]; fining not only bribe-receiver, but also the bribe-givers [161]; social exclusion which ostracizes the corrupt ones out of the system [14, 100], etc. External supervision is different from them, as it is not designed to combat corruption through punishing the corrupt enforcers, but through increasing the transparency of the market, disclosing the collusive bribery, and correcting the participants' payoff

to the level such that they are joining a fair market. Hence, we assume that the defectors only need to pay the fine f for their cheating, but will not receive any additional punishment for conducting the bribery; corrupt enforcers only need to pay the commission fee back to the cautious cooperators and cover their cost on the external supervision services, without any extra punishment for committing the corruption.

The following conclusions are drawn:

- **The effect of external supervision services on combating corruption**: Providing cooperators with the option of engaging external supervision service can reverse the outcome and mitigate corruption. However, the effectiveness of this approach depends on several key factors, including the initial strategy profile of rule enforcers $\left(\mathbf{y}^{(0)}\right)$ and the cost of external supervision service (a). While all the parameters that determine the payoff matrix influence the effectiveness, our specific focus is on a, as it is regulatable and directly affects players' willingness to engage with external supervision services. The remaining parameters are fixed with commonly used values. Note that altering these parameter values may lead to different outcomes.
- **The effectiveness of external supervision services are influenced by several key factors**: Under the framework of evolutionary game theory, we find that $\mathbf{y}^{(0)} = \left(y_1^{(0)}, y_2^{(0)}\right)$ plays a decisive role in the game. $y_1^{(0)} > (B-c)/(B-f)$ results in the dominance of trusting cooperation. Otherwise, players are eventually surrounded by corrupt enforcers, and the strategy profile of players ($\mathbf{x}$) exhibits cyclic dominance. This finding is consistent with previous studies [92, 141]. Furthermore, when cyclic dominance is observed in $\mathbf{x}$, the corresponding oscillation frequency is positively related to a (Figure 5-2(d) and Figure 5-2(e)), a higher value of a leads to higher oscillation frequency.

Other than the mechanism of survival of the fittest, exploration is also a common learning strategy in our real-world. Accordingly, the original model is extended by adding asymmetric mutation rates to the players (μ) and rule enforcers (v). Results show that with the random exploration mechanism, the strategy profile of both players and rule enforcers can reach their equilibrium $\mathbf{x}^*$ and $\mathbf{y}^*$. The relative value of μ and v changes the equilibrium drastically (Figure 5-3). When $v > \mu$, enforcers evolve to an equal dominance (half U_h and half U_c, $\mathbf{y}^* = (0.5, 0.5)$) and players evolve into the dominance of trusting cooperation; further, this result is robust to the initial state of players or enforcers. Lee et al. also noticed the decisive influence of asymmetric mutation rate in dynamics [93], they constructed a harvester–enforcer game in which the enforcer can be honest or corrupt. They pointed out that if the corrupt enforcers have higher mutation rate than the honest ones, the system is more likely to end up with cooperation dominance. In contrast, in our model, it is the bias of the mutation rate between enforcers and players that determines the equilibrium. Such different results illustrate the subtle influence of the random exploration mechanism on the evolution, which depends on the nature of the specific system.

- **The optimal service cost**: The cost of the external supervision service has critical influence on the player-enforcer dynamics through its double effect: the inhibition effect on cautious cooperators decreases the transparency of the system, and breeds corruption; yet the punishment effect on corrupt enforcers deters the corrupt enforcers, and improves the fraction of honest enforcers. Although extra punishments of committing corruption have been excluded for rule enforcers, the assumption that the corrupt enforcer has to cover the cost of engaging external supervision for C_a in the event $(C_a, D)|(U_c)$ turns a into a negative incentive for corruption. Due to these two effects of a, different level of a can change the trajectories

of $\mathbf{x}$ and $\mathbf{y}$ (Figure 5-2(d) and Figure 5-2(e)), and determines $\mathbf{x}^*$ and $\mathbf{y}^*$ if the equilibrium exists (Figure 5-3). It is intuitive that reducing a would be an effective means of reducing corruption [159, 160]. However, in our model, a lower a is not necessarily better. The results reveal that only when $v < \mu$, corrupt enforcers are the majority, is a lower a preferable. Otherwise, $\mathbf{y}^* \approx (0.5, 0.5)$, a lower a in turn decreases the fraction of trusting cooperators but increases that of cautious cooperators. This corresponds to more cooperators engaging in unnecessary external supervision services.

To examine whether the insights of the influence of mutation rates and supervision cost a are also valid in a finite population, simulation experiments are designed to explore the stochastic dynamics within different sizes of markets. We find that in a finite market the conclusions are still valid. Increasing v makes the rule enforcers more likely to evolve into an equal dominance (Figure 5-5 and Table 5.5). Even when the strategy profiles cannot reach any equilibrium, but exhibit cyclic patterns, the average fraction of $C_{\bar{a}}$ ($E(C_{\bar{a}})$) and of U_h ($E(U_h)$) are higher if $v > \mu$ (Figure 5-6 and Figure 5-7).

Furthermore, in finite markets, decreasing a to the utmost is not always beneficial. The optimal value of a depends on the scale of the market. Within a small scale market, reducing a is not necessary, since players eventually evolve into homogeneous trusting cooperators. Within a medium scale market, when the equilibrium is reachable, ensuring $a \leq 0.2$ is meaningful, as it can guarantee the market ends up with trusting cooperator dominance. Whereas when cyclic dominance patterns are observed in $\mathbf{x}$ and $\mathbf{y}$, such as in a large scale market, a higher a arouses a higher $E(U_h)$ and $E(C_{\bar{a}})$ instead (Figure 5-6 and Figure 5-7), as a result of a's punishment effect. However, it does not necessarily mean that a should be increased as much as possible when strategy profiles cannot reach equilibria. After analyzing the average cycle length of strategy C_a and D, we

find that a higher a also leaves $C_{\bar{a}}$ exposed to defectors longer, due to its inhibition effect on C_a. Therefore, considering the trade-off between protecting trusting cooperators and improving the average fraction of honest enforcers, $a = 0.2$ is the most eclectic level. Note that this value is provided with a set of predefined parameters (Table 5.4). When changing the assumptions, the optimal a might also be different.

In all, the conclusions that drawn from the replicator dynamics imply some practical suggestions for platform management. First, since the initial fraction of the honest enforcers is critical, investing in the ethical education for new rule enforcers is a valuable investment, as this measure facilitates the establishment of an honest atmosphere from the beginning, which can effectively prevent corruption. Second, increasing the mutation rate of rule enforcers is always beneficial. Despite v, as a feature of rule enforcers, is challenging to regulate directly, we can indirectly influence it by replacing parts of the rule enforcers with new recruits or through rotation [1]. As long as the new group has a different strategy profile than the original group, it is equivalent to introducing randomly exploring rule enforcers into the system, thereby achieving the effect of increasing v. Third, reducing a is intuitively advantageous, however, it may not always be the case. In our model, we found the optimal cost depends on the scale of market and the exploration rates of enforcers and players.

This work still leaves out certain possibilities for future research. In our model, players and rule enforcers are independent and not structured. However, corruption and bribes are usually not happening independently in real life. The structured social network of players or rule enforcers can influence the bribery and corruption behavior [159, 95]. For example, the honest enforcers may transform into corrupt ones under the peer pressure [104] or social intimidation [14]. Additionally, this research assumes that once the collusive bribery is discovered by the external supervisor,

the loss that the cautious cooperators suffer from the interaction can be covered in time; but in real life, there can be a delay [20] or even subsequent loses (like revenge from the rule enforcers), which can change the payoff matrix and dynamics essentially. It may be interesting to consider these extensions in future researches.

Chapter 6

Conclusions

This thesis revolves around designing processes and incentives to facilitate policies enforcement from both practical and theoretical dimensions. The focuses of these two dimensions include leveraging technologies to empower compliant operations while prohibiting non-compliant ones, and employing incentives to motivate participants' compliance. In Chapter 1, four research questions have been stated to guide the following chapters. This chapter revisits the answers to these research questions, and ends with a discussion on future directions.

6.1 Main findings

RQ 1. How to enforce cross-domain data sharing policies adapting to the environment?

A comprehensive approach is proposed, encompassing an environmental adaptive auditing process and an authorized requests execution process. This approach is implemented within an infrastructure that integrates an audit layer and a control layer to fulfill related functions. In this infrastructure, data

requests are audited, non-compliant requests are prohibited and only compliant ones are empowered in the control layer. Specifically, the auditing process is facilitated by Jason[1], which can store the current policies and environmental condition as beliefs, forming the basis for decision-making. This enables the application of corresponding policies to check requests under different circumstances. In this way, cross-domain data sharing policies can be enforced adapting to the environment. More details can be found in Chapter 2.

Since the execution process of requests is realized by independently developed applications, which are customized and replaceable, the infrastructure used in the proposed approach can be easily generalized and applied to enforce other operational regulations. Nevertheless, the approach is limited in enforcing concurrent operations. For workflows that encompass sequential operations and require choreography, addressing the second research question becomes crucial.

RQ 2. How to enforce cross-domain data sharing policies that adapt to the environment?

A solution that leverages blockchain technology and utilizes Petri nets for workflow modeling is proposed. This solution implements Petri nets on the blockchain and employs a three-layered architecture to choreograph both on-chain and off-chain tasks. An incentive mechanism is integrated into the deployed workflow. Specifically, incentivization is achieved by incorporating a peer audit process, wherein participants are evaluated by their peers. Only those who pass the audit process are granted tokens to activate subsequent rounds of the workflow (as detailed in Chapter 3). This solution motivates parties

[1] Jason is an environment of belief-desire-intention (BDI) based multi-agent system(MAS).

to complete off-chain tasks by future cooperation opportunities. Moreover, it empowers parties to monitor their peers and provide timely feedback in each cooperation. Through this mechanism, untrustworthy parties are eliminated, while collaborative ones will be preserved.

The presented solution leverages the strengths of Petri nets to map and visualize the workflows, allowing real-time monitoring of the execution process through the blockchain. In addition, the integrated incentive mechanism empowers parties to observe their peers' activities and offer feedback, effectively eliminating untrustworthy parties. In this manner, this solution ultimately enhances cooperation and trust among semi-trusted parties.

The proposed solutions to address **RQ 1** and **RQ 2** focus on empowering compliant operations through process design and technological realization. However, as discussed in Chapter 1, violations can still occur despite the development of technologies. Institutional incentives play an important complementary role in policy enforcement. Therefore, in Part II, the focus shifts from empowering to motivating, exploring challenges that arise in incentive design and implementation.

RQ 3. How to design incentives from an institutional perspective?

From the institutional perspective, proper incentives need to effectively promote cooperation while also being sustainable. Sustainability entails two aspects: for the institution, the execution cost of incentives cannot be excessively high, as it would hinder continuous implementation; for participants, the severity of incentives must be manageable while still encouraging cooperation, allowing participants to remain in the market and benefit from it. To design incentives that meet these criteria, the evolutionary game theory framework is applied to compare

the effect of pure reward, pure punishment, and mixed incentives, in terms of the cooperation level, sustainability, and the affluence of both participants and the institution. The results show that: 1) Pure reward incentives promote participants' wealth but can hardly be implemented sustainably. 2) Pure punishment is always sustainable. Mild punishment can lead to the shrinkage of the market due to participants' limited rationality, while strong punishment can maintain the market size, and enhance the affluence for both participants and the institution. 3) Mixed incentives generally lead to different wealth levels for participants and the institution. Moderate strength of mixed incentives maximizes the overall wealth of both parties. Chapter 4 offers a more in-depth analysis.

In **RQ 3**, the evaluation criteria for incentives is extended, highlighting the practicality of institutional-enforced incentives. Incentive design for market management requires viewing the market as an ecological system. The market's flourishing depends not only on the population of cooperators but also on the market's size and the accumulated wealth of both the institutional and participants.

It is worth pointing out that the quantified results are derived based on model-related parameters, which may not entirely coincide with real-world situations. Therefore, these quantified results may not be directly applicable in practice. Nonetheless, the proposed extended evaluating criteria hold broad applicability. By calibrating the model parameters to fit the specific scenario, the model can shed more light on the incentive design process.

In the stage of incentive implementation, pervasive corruption is a recurring challenge that impedes the rigorous execution of incentives. The exploration of **RQ 4** delves into whether this challenge can be mitigated by external supervision services such as complaining, whistle-blowing, or

reporting.

> **RQ 4.** Can external supervision services combat corruption in incentive implementation?

> To study the effectiveness of external supervision services, a game model is constructed to simulate the possible corruption caused by non-compliant participants bribing corrupt enforcers, referred to as "collusive bribery". Under the analytical framework of evolutionary game theory, the findings indicate that introducing external supervision services can contain collusive bribery during incentive implementation and promote cooperation. Additionally, the initial fraction of honest rule enforcers, exploration rates, and the cost of external supervision services can influence the final level of corruption and cooperation. Specifically, when the initial fraction of honest rule enforcers is greater than a certain threshold, the market decisively evolves into a pure cooperation equilibrium. A higher exploration rate of rule enforcers inclines participants towards a dominance strategy of trusting cooperation (with no engagement in external supervision services). Finally, reducing the cost of supervision services is not necessarily beneficial. If a dominance of trusting cooperation is achieved, a higher cost of external supervision services reduces the unnecessary engagements; when strategies exhibit cyclic dominance, the cost of the external supervision services has a trade-off between combating corruption and protecting trusting cooperators. Detailed explanations of these findings are provided in Chapter 5.

These results imply some practical suggestions for facilitating the rigorous implementation of incentives facing potential corruptions. First, since the initial fraction of the honest rule enforcers is critical, investing in ethical

education for new rule enforcers is a valuable investment. This measure facilitates the establishment of an honest atmosphere from the beginning, effectively preventing corruption. Secondly, increasing the exploration rate of rule enforcers is always beneficial. Although directly regulating this rate might be challenging, we can indirectly influence it by replacing parts of the rule enforcers with new recruits or through rotation [1]. For example, introducing new enforcers with a different strategy profile than the original group is equivalent to introducing randomly exploring rule enforcers into the system, achieving the effect of increasing the exploration rate. Thirdly, the optimal cost depends on the scale of the market and the exploration rates of enforcers and players; it should be carefully settled by considering the concrete scenario.

So far, the four research questions proposed in Chapter 1 have been answered, from empowering compliant concurrent or sequential operations through technology to motivating compliance by incentives. Nevertheless, it is essential to acknowledge that there are other challenges that still remain. Due to the scope of the research questions, these challenges are not thoroughly explored in this dissertation, but they cannot be ignored when enforcing complex policies in real-life scenarios. The final part of this chapter uncovers these remaining open issues and discusses the future directions in addressing them.

6.2 Future directions

Indeed, the utilization of technologies or incentives to promote compliance encompass spans a wide spectrum of disciplines and methodologies. Attempting an thorough and comprehensive exploration within the scope of this final section would be unrealistic. In spite of this, it is still feasible to select closely related challenges for discussion. These challenges can be categorized into three main aspects: 1) the challenges in enforcing policies by technologies; 2) the challenges in promoting compliant behaviors by incentives; 3) the potential for a profound integration of technologies and incentives in policy enforcement. The following of this section unfold these three streams.

Aspect I: Challenges in enforcing policies by technologies

When empowering or prohibiting requests to enforce operational policies, it is crucial to ensure the precise identification of compliant or non-compliant operations. The clarity of operations is fundamental for processes design, and the subsequent technologies integration. In **RQ 1** and **RQ 2**, the operational regulations are specific and clear with respect to the activities that need to be executed, making the semantic modeling and mapping of policies easy. However, when policies are abstract, their enforcement through technologies becomes tricky. For example, one rule in the General Data Protection Regulation (GDPR) about transferring personal data is

> *A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection [48].*

This rule uses ambiguous phrase like “adequate level of protection”. The accurate threshold for “adequate” is not given, meanwhile how to estimate or evaluate the level of protection is unspecified.

Undoubtedly, policies cannot be always concrete, the adequate threshold can be higher for more sensitive dataset, and lower for others. But such guideline-formation policies indeed create confusion and challenges when enforcing, due to the lack of explicitness and operability. Additionally, sometimes policies of different level of abstraction might even have conflicts, certain operations under one policy shall be empowered, yet under another one shall be prohibited. Such conflicts might cause the same operation receiving completely different processing outcomes in practice. Therefore, addressing challenges in modelling and mapping policies, as well as in reasoning and coping with conflict rules, is an important future direction in policy enforcement.

Other than that, solutions for enforcing **dynamic policies** have great practical potential [130]. In this thesis, the implemented policies are fixed and static. When answering **RQ 2**, for instance, once the workflow is deployed, involved parties need to execute the agreed sequence of tasks. However, in real life, dynamic workflows are common, with changes in the sequence of tasks or in the concrete functions fulfilled in certain tasks [164]. Solutions that support dynamic policies' enforcement have wide application space for their higher flexibility and reliability.

Lastly, although solutions for policy enforcement are developing, academic research outcomes may not always be perfectly synchronized with industry demands. Developing comprehensive evaluation criteria for proposed solutions is crucial and expected in practice. Managers in companies are always looking forward to understand to what extend can the risk of non-compliance being reduced after applying the solution; they are eager to know the best or the worst cases that can happen if employing the new approach. Most existing evaluations of related works primarily focus on

performance effectiveness, it is imperative to consider security assurance aspects [46, 184].

Aspect II: Challenges in promoting compliant behaviors by incentives

When predicting the effect of incentives, other than factors like the level of rationality, exploration rates, etc., that considered in **RQ 3** and **RQ 4**, there are many other critical factors that can change the results, such as the social network [95], reputation system [137], participants' memory [17], etc. Take the social network as an example, in real life, participants cannot actually get access to anyone in the system. Not considering the interactive network, but assuming that participants are well mixed and their strategies are determined solely by the rest of the peers, might overlook geographical or spatial limitations.

Not only participants, but also rule enforcers have their own relationship networks. The relationship network can potentially influence whether enforcers implement incentives honestly by peer pressure [104]. Surrounded by corrupt rule enforcers, an honest enforcer tends to flip to a corrupt one. Furthermore, the social networks among participants and among rule enforcers might be dynamic and update based on their interaction history. Such co-evolution of strategies and social networks might better reflect the real world.

The inclusion of these factors makes the theoretic model more realistic, and makes the predictions on the performance of incentives more applicable to practice, and therefore strengthening the practical significance. However, these factors can largely complicate the model and might introduce noise, challenging the development of the model. Addressing these challenges requires combining traditional mathematical modeling and agent-based simulations, complemented by laboratory or field experiments. Real data from experiments are valuable in evaluating whether the model captures key factors and calibrating corresponding parameters.

Aspect III: A profound integration of technologies and incentives

There exists a demand for the profound integration of technologies and incentives in policy enforcement. Solely designing and implementing processes cannot fully prevent non-compliance behaviors as discussed in Chapter 1. Chapter 3 takes the initial step in exploring the integration of incentives into the enforcement of workflows by introducing peer auditing. However, it may not suffice. Opportunists could treat collaboration as a one-time shot, and gain benefits from cheating in each new collaboration. Therefore, more powerful incentive mechanisms need to be integrated.

Meanwhile, designing incentives alone is neither enough to exclude non-compliant behaviors. Successful implementation is crucial, and the cost and feasibility of implementing incentives can present practical obstacles. For example, monitoring participants can require significant human and material resources for rule enforcers. Leveraging technologies to reduce the cost and facilitate the implementation of incentives becomes a practical demand.

In summary, a profound integration of technologies and incentives for promoting policy enforcement is an important future direction. How to concretely integrate them poses an open question with a multitude of potential research directions. The following presents two concrete examples as starting points to stimulate readers' further explorations and investigations.

1) **Blockchain based reputation system**

Reputation is a powerful and effective incentive, its significant role in an autonomous society has been proved by studies [137]. A transparent reputation system serves as an indicator for people to select their cooperators, and restricts people's behaviors as an external pressure. Consequently, in such a system, people cherish their reputation for future opportunities and are cautious about their behavior.

Blockchain technology, by its nature, can practically support the estab-

lishment of such reputation system. Its tamper-proof feature enhances the credibility of the reputation by preventing falsification, thereby providing a stronger reference in cooperator selection. In Chapter 3, the blockchain is used to enforce workflows where peer audit is integrated, but the audit results are local information shared only among collaborators. If the results can be recorded on another public reputation chain, the effectiveness of the incentive can be greatly enhanced.

This blockchain based reputation system is promising to be applied in different scenarios, such as data sharing systems, supply chain management, and two-sided market (multi-sided platform) management, etc. Systems in these scenarios can benefit from the transparent and reliable reputation system, where participants can autonomously selecting trust worthy collaborators.

Whereas in practice, autonomy is always complemented by an external central governance that carry out incentives. The following elaborates on how technologies further facilitate the implementation of incentives in central governance.

2) **Transparent and auditable system**

In **RQ 3** and **RQ 4**, the cost of implementing incentives, including monitoring, surveying and verification, is considered by a constant parameter. However, the cost can drastically grow when the interaction history is complex [60], which impedes rule enforcers from carrying out incentives efficiently. Designing processes and automating certain functions with technologies to facilitate enforcers implementing incentives are additional future directions.

There are few studies delicate to utilizing technologies for improving the transparency and audibility of the system. For example, using digital signatures with public keys to confirm the authenticity of operations [9]; using blockchain to record a transparent log of activities, and maintain complete and transparent historical data [11]; and employing data mining

to detect fraud to facilitate post-auditing [57], ect. These efforts underscore the importance and potential of designing transparent and auditable systems, and applying them into the governance of markets, platforms, or even cities.

Overall, a more profound integration of technologies and incentives is meaningful for promoting compliance and fostering a cooperative environment in both autonomous and central governance communities.

Back to the mission of this thesis - enhancing policy enforcement through technologies and incentives - the challenges discussed in this section entail the fact that no perfect solutions or incentives exist to completely eliminate all non-compliant behaviors. Nevertheless, efforts aimed at addressing these challenges pave the way, and illuminate the path toward approaching the ideal destination.

Appendix A

A.1 Population equilibrium

To predict the effect of incentive mechanism, **evolutionary game theory** which describes the population of players engaging in pairwise interaction, has been generally accepted as a common framework to model and interpret the evolution of cooperation in a social dilemma. This part shows the derivation process of the analytical results of the population in equilibrium.

Assume a finite population of size N, M of them participant a market play PDG, two types of strategies for cooperation C and defection D are well mixed. Let $\pi(C)$ denote the expected payoff of strategy C, $\pi(D)$ donate that of strategy D, and $\bar{\pi}(\mathbf{x})$ denote the average payoff of the whole population:

$$\pi(C) = (1 - c_0 + R_{CC})x + (-T - c_0 + R_{CD})y, \tag{A.1}$$

$$\pi(D) = (T - c_0 - F_{CD})x + (0 - c_0 - F_{DD})y, \tag{A.2}$$

$$\bar{\pi}(\mathbf{x}) = \pi(C)x + \pi(D)y. \tag{A.3}$$

The replicator dynamics of cooperators and defectors is:

$$\dot{x} = x(1 - x)[\pi(C) - \pi(D)]. \tag{A.4}$$

With the equations eq.A.1, eq.A.2, eq.A.3, and eq.A.4, let $\dot{x} = 0$,

$$(x^2 - x)[x + xR_{CC} + (1-x)R_{CD} + xF_{CD} + (1-x)F_{DD} - T] = 0. \quad \text{(A.5)}$$

Thus, the fixed points are $x^* = 0$, $x^* = 1$, and $x^* = (T - R_{CD} - F_{DD})(1 + R_{CC} - R_{CD} + F_{CD} - F_{DD})^{-1} = q$.

We next discuss if the fixed point is the Nash equilibrium (NE) and satisfy the requirement of being as the evolutionary stable strategy (ESS).

Let $\mathbf{s}^* = (x^*, 1 - x^*)$, $\mathbf{s} = (p, 1 - p)$, $\mathbf{s} \neq \mathbf{s}^*$, an ESS can be defined as a mixed strategy $\mathbf{s}^*$, such that for any strategy $\mathbf{s}$ and any sufficient small $\epsilon > 0$,

$$\pi[\mathbf{s}^*, (1-\epsilon)\mathbf{s}^* + \epsilon\mathbf{s}] > \pi[\mathbf{s}, (1-\epsilon)\mathbf{s}^* + \epsilon\mathbf{s}]. \quad \text{(A.6)}$$

Using the linearity in probability of expected payoffs reduces A.6 to:

$$(1-\epsilon)\pi(\mathbf{s}^*, \mathbf{s}^*) + \epsilon\pi(\mathbf{s}^*, \mathbf{s}) > (1-\epsilon)\pi(\mathbf{s}, \mathbf{s}^*) + \epsilon\pi(\mathbf{s}, \mathbf{s}). \quad \text{(A.7)}$$

If for all small $\epsilon > 0$ and for all $\mathbf{s}$,

$$\pi(\mathbf{s}^*, \mathbf{s}^*) \geq \pi(\mathbf{s}, \mathbf{s}^*), \quad \text{(A.8)}$$

then $\mathbf{s}^*$ is a symmetric NE. Further, if

$$\pi(\mathbf{s}^*, \mathbf{s}) > \pi(\mathbf{s}, \mathbf{s}), \quad \text{(A.9)}$$

whenever $\pi(\mathbf{s}^*, \mathbf{s}^*) = \pi(\mathbf{s}, \mathbf{s}^*)$, $\mathbf{s}^*$ is an ESS [38].

A.1.1 The sustainability of $x^* = 0$

When fixed point at $x^* = 0$, $\mathbf{s}^* = (0, 1), \mathbf{s} = (p, 1-p)$ $(0 < p \leq 1)$, we have:

$$\pi(\mathbf{s}^*, \mathbf{s}^*) = -c_0 - F_{DD}, \quad \text{(A.8a)}$$

$$\pi(\mathbf{s}, \mathbf{s}^*) = p(-T - c_0 + R_{CD}) + (1-p)(0 - c_0 - F_{DD}), \tag{A.8b}$$

$$\pi(\mathbf{s}^*, \mathbf{s}) = p(T - c_0 - F_{CD}) + (1-p)(0 - c_0 - F_{DD}), \tag{A.9a}$$

$$\begin{aligned}\pi(\mathbf{s}, \mathbf{s}) =& p^2(1 - c_0 + R_{CC}) + p(1-p)(-T - c_0 + R_{CD}) \\ &+ p(1-p)(T - c_0 - F_{CD}) + (1-p)^2(0 - c_0 - F_{DD}).\end{aligned} \tag{A.9b}$$

By A.8a-A.8b, we have

$$\begin{aligned}A.8a - A.8b &= -p(-T - c_0 + R_{CD}) + p(0 - c_0 - F_{DD}) \\ &= p(T - F_{DD} - R_{CD}),\end{aligned} \tag{A.8c}$$

and by A.9a - A.9b, we have

$$A.9a - A.9b = p^2(T - F_{CD} - R_{CC}) + p(1-p)(T - F_{DD} - R_{CD}). \tag{A.9c}$$

The Table A.1 shows the requirements for $x^* = 0$ being a NE or an ESS under different incentive policies.

Table A.1: NE and ESS analysis when $x^* = 0$

Incentive	**Constraints**	**Requirements of NE**	**Requirements of ESS**
Reward	$R_{CC} + R_{CD} > 0$, $F_{CD} = F_{DD} = 0$	$T \geq R_{CD}$, $A.8c \geq 0$	$T > R_{CD}$, $A.9c > 0$
Punishment	$R_{CD} = R_{DD} = 0$, $F_{CD} + F_{DD} > 0$	$T \geq F_{DD}$, $A.8c \geq 0$	$T \geq F_{CD}$, $A.9c > 0$
Mixed incentives	$R_{CD} + R_{CC} \neq 0$, $F_{CD} + F_{DD} \neq 0$	$T \geq R_{CD} + F_{DD}$, $A.8c \geq 0$	$T \geq \max[R_{CD} + F_{DD}, R_{CC} + F_{CD}]$, $A.9c > 0$

A.1.2 The sustainability of $x^* = 1$

Consider the fixed point at $x^* = 1$, $\mathbf{s}^* = (1, 0), \mathbf{s} = (1-p, p)$ $(0 < p \leq 1)$, we have:

$$\pi(\mathbf{s}^*, \mathbf{s}^*) = 1 - c_0 + R_{CC}, \tag{A.8d}$$

$$\pi(\mathbf{s}, \mathbf{s}^*) = (1-p)(1 - c_0 + R_{CC}) + p(T - c_0 - F_{CD}), \tag{A.8e}$$

$$\pi(\mathbf{s}^*, \mathbf{s}) = (1-p)(1-c_0+R_{CC}) + p(-T-c_0+R_{CD}), \tag{A.9d}$$

$$\begin{aligned}\pi(\mathbf{s}, \mathbf{s}) =&(1-p)^2(1-c_0+R_{CC}) + p(1-p)(-T-c_0+R_{CD}) \\ &+ p(1-p)(T-c_0-F_{CD}) + p^2(0-c_0-F_{DD}).\end{aligned} \tag{A.9e}$$

By A.8d - A.8e, we have

$$\begin{aligned}A.8d - A.8e &= p(1-c_0+R_{CC}) - p(T-c_0-F_{CD}) \\ &= p(1-T+R_{CC}+F_{CD}),\end{aligned} \tag{A.8f}$$

and by A.9d - A.9e, we have

$$\begin{aligned}A.9d - A.9e =&p(1-p)(1-c_0+R_{CC}) - p(1-p)(T-c_0-F_{CD}) \\ &+ p^2(-T-c_0+R_{CD}) - p^2(0-c_0-F_{DD}) \\ =&p(1-p)(1-T+R_{CC}+F_{CD}) \\ &+ p^2(R_{CD}+F_{DD}-T).\end{aligned} \tag{A.9f}$$

The Table A.2 shows the requirements for $x^* = 1$ being a NE or an ESS under different incentive policies.

Table A.2: NE and ESS analysis when $x^* = 1$

Incentive	**Constraints**	**Requirements of NE**	**Requirements of ESS**
Reward	$R_{CC} + R_{CD} > 0$, $F_{CD} = F_{DD} = 0$	$R_{CC} \geq T-1$, $A.8f \geq 0$	$R_{CC} \geq T$, $A.9f > 0$
Punishment	$R_{CD} = R_{DD} = 0$, $F_{CD} + F_{DD} > 0$	$F_{CD} \geq T-1$, $A.8f \geq 0$	$F_{DD} > T$, $A.9f > 0$
Mixed incentives	$R_{CD} + R_{CC} \neq 0$, $F_{CD} + F_{DD} \neq 0$	$R_{CC} + F_{CD} \geq T-1$, $A.8f \geq 0$	$\min[R_{CD} + F_{DD}, R_{CC} + F_{CD}] \geq T$, $A.9f > 0$

A.1.3 The sustainability of $x^* = q$

Consider the fixed point at $x^* = q = (T - R_{CD} - F_{DD})(1 + R_{CC} - R_{CD} + F_{CD} - F_{DD})^{-1}$. Let $\mathbf{s}^* = (q, 1-q)$ and $\mathbf{s} = (p, 1-p)$ $(0 \leq p \leq 1, p \neq q)$, we have:

$$\begin{aligned}\pi(\mathbf{s}^*, \mathbf{s}^*) =& q^2(1 - c_0 + R_{CC}) + q(1-q)(-T - c_0 + R_{CD}) \\ &+ q(1-q)(T - c_0 - F_{CD}) - (1-q)^2(c_0 + F_{DD}),\end{aligned} \tag{A.8g}$$

$$\begin{aligned}\pi(\mathbf{s}, \mathbf{s}^*) =& pq(1 - c_0 + R_{CC}) + p(1-q)(-T - c_0 + R_{CD}) \\ &+ (1-p)q(T - c_0 - F_{CD}) - (1-p)(1-q)(c_0 + F_{DD}),\end{aligned} \tag{A.8h}$$

$$\begin{aligned}\pi(\mathbf{s}^*, \mathbf{s}) =& pq(1 - c_0 + R_{CC}) + (1-p)q(-T - c_0 + R_{CD}) \\ &+ p(1-q)(T - c_0 - F_{CD}) - (1-p)(1-q)(c_0 + F_{DD}),\end{aligned} \tag{A.9g}$$

$$\begin{aligned}\pi(\mathbf{s}, \mathbf{s}) =& p^2(1 - c_0 + R_{CC}) + p(1-p)(-T - c_0 + R_{CD}) \\ &+ p(1-p)(T - c_0 - F_{CD}) - (1-p)^2(c_0 + F_{DD}).\end{aligned} \tag{A.9h}$$

By A.8g - A.8h, we have

$$\begin{aligned}A.8g - A.8h =& q(q-p)(1 - c_0 + R_{CC} - T + c_0 + F_{CD}) \\ &+ (1-q)(q-p)(-T - c_0 + R_{CD} + c_0 + F_{DD}) \\ =& (q-p)[q(1 + R_{CC} + F_{CD}) + (1-q)(R_{CD} + F_{DD}) - T],\end{aligned} \tag{A.8i}$$

and by A.9g - A.9h, we have

$$\begin{aligned}A.9g - A.9h =& p(q-p)(1 - c_0 + R_{CC} - T + c_0 + F_{CD}) \\ &+ (1-p)(q-p)(-T - c_0 + R_{CD} + c_0 + F_{DD}) \\ =& (q-p)[p(1 + R_{CC} + F_{CD}) + (1-p)(R_{CD} + F_{DD}) - T].\end{aligned} \tag{A.9i}$$

The Table A.3 shows the requirements for $x^* = q$ being a NE or an ESS under different incentives.

Table A.3: NE and ESS analysis when $x^* = q$

Incentive	**Constraints**	**Requirements of NE**	**Requirements of ESS**
Reward	$R_{CC} + R_{CD} > 0$, $F_{CD} = F_{DD} = 0$	$A.8i = 0$, thus always hold	$A.9i < 0$, thus the ESS is not hold
Punishment	$R_{CD} = R_{DD} = 0$, $F_{CD} + F_{DD} > 0$	$A.8i = 0$, thus always hold	$A.9i < 0$, thus the ESS is not hold
Mixed incentives	$R_{CD} + R_{CC} \neq 0$, $F_{CD} + F_{DD} \neq 0$	$A.8i = 0$, thus always hold	$A.9i < 0$, thus the ESS is not hold

A.2 Rate of R_{CC} (F_{DD}) in $R_{CC} + F_{CD}$ ($R_{CD} + F_{DD}$)

Let α be the rate, $k = R_{CC} + F_{CD}$, to minimize the difference between reward ($R_{CD} + R_{CC}$) and punishment ($F_{CD} + F_{DD}$), meanwhile satisfy the constraints are $R_{CD} \geq R_{CC}, F_{CD} \geq F_{DD}$, we have:

$$\begin{aligned} \min_{\alpha} \quad & k\alpha + (k+1)\alpha - [k(1-\alpha) + (1+k)\alpha] \\ \text{s.t.} \quad & (1-\alpha)2 \geq 3\alpha \\ & (1-\alpha)1 \geq 4\alpha. \end{aligned} \tag{A.10}$$

The solution is $\alpha = 0.2$. Consequently, these four parameters are set as shown in Table A.4.

Table A.4: Mixed incentives setup

$R_{CC} + F_{CD}$	R_{CC}	F_{CD}	$R_{CD} + F_{DD}$	R_{CD}	F_{DD}
1	0.2	0.8	2	1.6	0.4
1.25	0.25	1	2.25	1.8	0.45
1.5	0.3	1.2	2.5	2	0.5
1.75	0.35	1.4	2.75	2.2	0.55
2	0.4	1.6	3	2.4	0.6
2.25	0.45	1.8	3.25	2.6	0.65
2.5	0.5	2	3.5	2.8	0.7
2.75	0.55	2.2	3.75	3	0.75
3	0.6	2.4	4	3.2	0.8

A.3 Accumulated wealth of the third-party

From eq.A.4, we have

$$\begin{aligned} \dot{x} = \frac{dx}{dt} =& (1 + R_{CC} - R_{CD} + F_{CD} - F_{DD})x^3 \\ &+ (2R_{CD} + 2F_{DD} - F_{CD} - R_{CC} - T - 1)x^2 \\ &- (R_{CD} + F_{DD} - T)x. \end{aligned}$$

Let $a = 1 + R_{CC} - R_{CD} + F_{CD} - F_{DD}$, $b = 2R_{CD} + 2F_{DD} - F_{CD} - R_{CC} - T - 1$, $c = T - R_{CD} - F_{DD}$, we have:

$$\frac{dx}{dt} = ax^3 + bx^2 + cx.$$

We can then solve the differential equation:

$$\begin{aligned}
\int \frac{1}{ax^3 + bx^2 + cx} dx &= \int 1 dt \\
&= \int \frac{1}{x(ax^2 + bx + c)} dx \\
&= \int \frac{1}{cx} + \frac{-ax - b}{c(ax^2 + bx + c)} dx \\
&= \frac{1}{c} \int \frac{1}{x} dx - \frac{a}{c} \int \frac{x}{ax^2 + bx + c} dx - \frac{b}{c} \int \frac{1}{ax^2 + bx + c} dx \\
&= \frac{1}{c} \ln x - \frac{b}{c} \frac{2}{a\sqrt{4ac - b^2}} \tan^{-1}\left(\frac{2ax + b}{\sqrt{4ac - b^2}}\right) + C \\
&\quad - \frac{a}{c}\left(\frac{\ln(ax^2 + bx + c)}{2a} - \frac{b}{a\sqrt{4ac - b^2}} \tan^{-1}\left(\frac{2ax + b}{\sqrt{4ac - b^2}}\right)\right) \\
&= t.
\end{aligned} \tag{A.11}$$

$x^{(t)}$ is the inverse function of A.11, let $x^{(t)} := F(t, a, b, c)$. The wealth of the third party at time step t is shown as eq.4.3

$$\begin{aligned}
W_T^{(t)} &= M^{(t)}\Big(c_0 + x^{(t)}\big(1 - x^{(t)}\big)F_{CD} + \big(1 - x^{(t)}\big)^2 F_{DD} \\
&\qquad - \big(x^{(t)}\big)^2 R_{CC} - x^{(t)}\big(1 - x^{(t)}\big)R_{CD} \\
&\qquad - \alpha\Big(x^{(t)}\big(1 - x^{(t)}\big)F_{CD} + \big(1 - x^{(t)}\big)^2 F_{DD}\Big)\Big) \\
&= M^{(t)}\Big(\big(x^{(t)}\big)^2\big((1 - \alpha)(F_{DD} - F_{CD}) - R_{CC} + R_{CD}\big) \\
&\qquad + x^{(t)}\big((1 - \alpha)(F_{CD} - 2F_{DD}) - R_{CD}\big) \\
&\qquad + c_0 + (1 - \alpha)F_{DD}\Big) \\
&= M^{(t)}\Big(F^2(t, a, b, c)\big((1 - \alpha)(F_{DD} - F_{CD}) - R_{CC} + R_{CD}\big) \\
&\qquad + F(t, a, b, c)\big((1 - \alpha)(F_{CD} - 2F_{DD}) - R_{CD}\big) \\
&\qquad + c_0 + (1 - \alpha)F_{DD}\Big).
\end{aligned}$$

Thus,

$$\begin{aligned}
W_T &= \int W_T^{(t)}\, dt \\
&= \big((1-\alpha)(F_{DD}-F_{CD}) - R_{CC} + R_{CD}\big) \int M^{(t)} F^2(t,a,b,c)\, dt \\
&\quad + \big((1-\alpha)(F_{CD}-2F_{DD}) - R_{CD}\big) \int M^{(t)} F(t,a,b,c)\, dt \\
&\quad + \big(c_0 + (1-\alpha)F_{DD}\big) \int M^{(t)}\, dt.
\end{aligned}$$

Appendix B

B.1 Supplement of analytical results

B.1.1 The stability of fixed points

Based on the replicatorequations (eq.5.1), it is easy to write $\dot{x}$ in the formation:

$$\begin{bmatrix} \dot{x_1} \\ \dot{x_2} \\ \dot{x_3} \end{bmatrix} = \begin{bmatrix} x_1((A_c\mathbf{x})_1 - \mathbf{x}^\top A_c\mathbf{x}) \\ x_2((A_c\mathbf{x})_2 - \mathbf{x}^\top A_c\mathbf{x}) \\ x_3((A_c\mathbf{x})_3 - \mathbf{x}^\top A_c\mathbf{x}) \end{bmatrix}, \tag{B.1}$$

the Jacob matrix of (B.1) is,

$$\mathbf{J} = \begin{bmatrix} \frac{tialx\dot{}_1}{tialx_1} & \frac{tialx\dot{}_1}{tialx_2} & \frac{tialx\dot{}_1}{tialx_3} \\ \frac{tialx\dot{}_2}{tialx_1} & \frac{tialx\dot{}_2}{tialx_2} & \frac{tialx\dot{}_2}{tialx_3} \\ \frac{tialx\dot{}_3}{tialx_1} & \frac{tialx\dot{}_3}{tialx_2} & \frac{tialx\dot{}_3}{tialx_3} \end{bmatrix}. \tag{B.2}$$

The real part of the eigenvalues of $\mathbf{J}$ at the fixed point decides the stability of the fixed point. If the eigenvalues have negative real parts, then the fixed point is asymptotically stable [136, 67].

Under heavy punishment, $f = 2$, facing pure corrupt rule enforcers, when

$a = 0.1, b = c = 0.5, c_0 = B = 0.2$, the internal fixed point $\mathbf{x_1}^* = (3/20, 201/260, 1/13)$. The eigenvalue of $\mathbf{J}$ at $\mathbf{x_1}^*$ is $\big(-29/130, (42 - 6\mathrm{i}\sqrt{69631})/10400, (42 + 6\mathrm{i}\sqrt{69631})/10400\big)$. Since the real part of the second and third eigenvalue are positive, $\mathbf{x_1}^*$ is not asymptotically stable.

Keeping the value of all the rest parameters but set a to 0, $\mathbf{x_1}^* = (3/20, 17/20, 0)$, and the eigenvalue of $\mathbf{J}$ at $\mathbf{x_1}^*$ is $(-3/10, 0, 0)$. Since all the real part of the eigenvalues are less than or equal to zero, and with no imaginary parts, $\mathbf{x_1}^*$ is stable. Actually, as Figure B-1 shows, every point on the edge $C_a C_{\bar{a}}$ (represented by a dashed line) is stable.

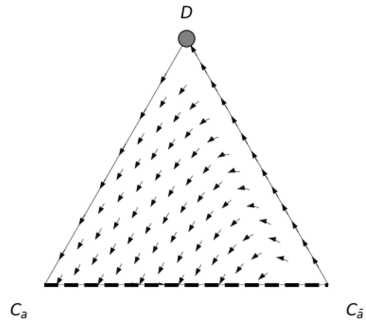
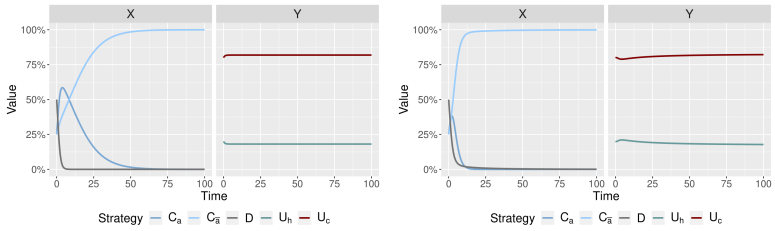


Figure B-1: When $y_1 = 2, b = c = 0.5, c_0 = B = 0.2, f = 2, a = 0$, the original interior fixed point $\mathbf{x_1}^*$ locates on the edge $C_a C_{\bar{a}}$. All points on the dashed edge $C_a C_{\bar{a}}$ are stable.

B.1.2 Player-enforcer dynamics in an infinite and well-mixed population

(1) The equilibrium without exploration



(a) $a = 0.1$ (b) $a = 0.5$

Figure B-2: Player-enforcer dynamics when $y_1^{(0)} > (B-c)/(B-f)$, $\mathbf{x}^{(0)} = (0.25, 0.25, 0.5)$, $\mathbf{y}^{(0)} = (0.2, 0.8)$. Both $\mathbf{y}^*$ and $\mathbf{x}^*$ are reachable, $y_1^* < y_1^{(0)}$, $\mathbf{x}^* = (0, 1, 0)$. Compare Figure B-2(a) with Figure B-2(b), it can be observed that, when a is higher, the stronger inhibition effect of a on the cautious cooperators reduces the summit of the fraction of C_a, and accelerates the elimination of C_a by $C_{\bar{a}}$. Meanwhile, the heavier punishment effect of a on U_c leads to a slight increase of the fraction of honest enforcers at the beginning.

The equilibrium of the population profile of rule enforcers and players depend on the initial state of the enforcers $\mathbf{y}^{(0)}$. When $y_1^{(0)} > (B-c)/(B-f)$, y_1^* decreases slightly from $y_1^{(0)}$ in the equilibrium, and the corresponding equilibrium of players is $\mathbf{x}^* = (0, 1, 0)$. Furthermore, comparing Figure B-2(a) and Figure B-2(b), it can be noticed that the value of a do not change $\mathbf{x}^*$ and $\mathbf{y}^*$.

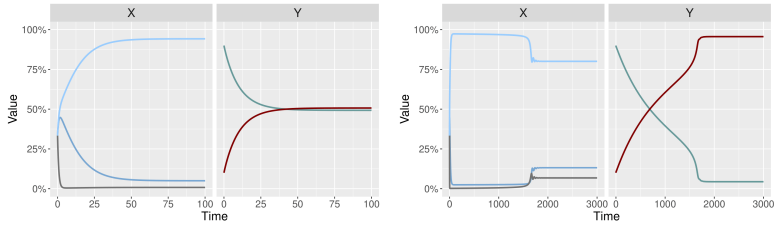
However, a changes the trajectory of $\mathbf{x}$ and $\mathbf{y}$. Due to the inhibition effect of a on C_a, a higher a is accompanied by a lower summit of and a steeper slop of the fraction of C_a. We also note that in Figure B-2(b), the fraction of corrupt enforcers when $a = 0.5$ is not monotonic increasing as in Figure B-2(a), but first decreasing and then increasing. This result attributes to the punishment effect of a on U_c: the higher the a is, the less

$\pi(U_c)$ is in the event $(C_a, D)|(U_c)$.

(2) The equilibrium with exploration

When the players and enforcers are allowed to explore strategies randomly ($\mu \neq 0$ and $v \neq 0$), $\mathbf{x}^*$ and $\mathbf{y}^*$ always exist. In Figure 5-3, we show the player-enforcer dynamics under $\mathbf{x}^{(0)} = (0.25, 0.25, 0.5)$, $\mathbf{y}^{(0)} = (0.1, 0.9)$. For elaborating on the independence of the mixed strategy equilibrium to the initial state, we set a different initial state, $\mathbf{x}^{(0)} = (1/3, 1/3, 1/3), \mathbf{y}^{(0)} = (0.9, 0.1)$, the results are shown in Figure B-3. Compare Figure B-3(a) to Figure 5-3(c), it is easy to tell that $\mathbf{x}^*$ and $\mathbf{y}^*$ are the same with different initial state. Analogously, the equilibrium in Figure B-3(b) and Figure 5-3(e) are the same.

The initial state does not change the equilibrium, but influences the required time of reaching the stable state. When the distance between the initial state and the equilibrium is greater, the required time is longer. For example, the required time in Figure B-3(b) is much longer than in Figure 5-3(e), as $\mathbf{y}^{(0)} = (0.9, 0.1)$ is further from $\mathbf{y}^* \approx (0, 1)$ compared with $\mathbf{y}^{(0)} = (0.1, 0.9)$. In contrast, $\mathbf{y}^0$ in Figure B-3(a) and Figure 5-3(c) are of an equal distance to the equilibrium $\mathbf{y}^* \approx (0.5, 0.5)$, the required time in these two scenarios are hence similar.



(a) $\mu = 0.01, v = 0.05, a = 0.1$ (b) $\mu = 0.005, v = 0.001, a = 0.5$

Figure B-3: Player-enforcer dynamics with the initial state $\mathbf{x}^{(0)} = (1/3, 1/3, 1/3), \mathbf{y}^{(0)} = (0.9, 0.1)$. If players and enforcers are allowed to explore strategies randomly, both $\mathbf{y}^*$ and $\mathbf{x}^*$ are reachable, and they are robust to the initial state.

B.2 Supplement of simulation experiments algorithms

B.2.1 The stochastic replicator dynamics algorithm in a finite population

Assume a transfer matrix $\mathbf{M}$,

$$\mathbf{M} = \begin{bmatrix} P_{1,1} & P_{1,2} & P_{1,3} \\ P_{2,1} & P_{2,2} & P_{2,3} \\ P_{3,1} & P_{3,2} & P_{3,3} \end{bmatrix}, \tag{B.3}$$

$P_{i,j} = \big[1 + \exp\big(\mathbf{S}(\pi(S_i) - \pi(S_j))\big)\big]^{-1}$, which denotes the probability that a player transform from strategy S_i to S_j. The exploration matrix $\mathbf{M_E}$ is:

$$\mathbf{M_E} = \begin{bmatrix} -\mu & \mu/2 & \mu/2 \\ \mu/2 & -\mu & \mu/2 \\ \mu/2 & \mu/2 & -\mu \end{bmatrix}. \tag{B.4}$$

Let $\|\mathbf{M}\|$ be the row normalized matrix of $\mathbf{M}$, in $\|\mathbf{M}\|$, $\sum_{j=1}^{j=3} P_{i,j} = 1$. The population profile at the next time step is:

$$\mathbf{x}^{(t+1)} = \mathbf{x}^{(t)}(\|\mathbf{M}\| + \mathbf{M_E}). \tag{B.5}$$

Thus, if $(\|\mathbf{M}\| + \mathbf{M_E})$ is fixed, meanwhile $\mathbf{x}^{(t+1)} = \mathbf{x}^{(t)}$, then $\mathbf{x}^{(t)}$ reaches $\mathbf{x}^*$.

Theorem B.2.1. *If the stable state exists,* $\mathbf{x}^*$ *and* $\mathbf{y}^*$ *must be the left eigenvectors of the corresponding constant matrix* $\|\mathbf{M}\| + \mathbf{M_E}$.

The exploration matrix for enforcers is analogous, $\mathbf{M_E}$ is adapted to:

$$\mathbf{M_E} = \begin{bmatrix} -v & v \\ v & -v \end{bmatrix}. \tag{B.6}$$

B.2.2 Algorithm for stochastic dynamics in a finite population

Table B.1: Algorithm for player-enforcer stochastic dynamics

Input:	$N, b, c, c_0, f, B, \mathbf{S}$, the cost of external supervision service a, the mutation rate of players μ, the mutation rate of rule enforcers v, the initial population profile $\mathbf{x}^{(0)}$, $\mathbf{y}^{(0)}$, and the termination time step $\mathbf{T}$.
Output:	$\mathbf{x}$, $\mathbf{y}$.
Step 1:	If $t < \mathbf{T}$, compute $\#C_a$, $\#C_{\bar{a}}$, and $\#D$ based on $\mathbf{x}^{(t)}$; compute $\#U_h$ and $\#U_c$ based on $\mathbf{y}^{(t)}$. Generate the pairwise table, each row of which is composed of two players and one random assigned rule enforcer. eg. $(C_{\bar{a}}, C_{\bar{a}}, U_h)$. Else go to **Step 6**.
Step 2:	Based on the pairwise table, calculate the payoff of each player and rule enforcer. Hence, generate the **payoff table**, each row is composed of the payoff of the two players and the enforcer, eg. $(0.3, 0.3, 0.4)$.
Step 3:	Based on the payoff table, calculate the average payoff of strategies: $\pi(C_{\bar{a}})$, $\pi(C_a)$, and $\pi(D)$; $\pi(U_h)$ and $\pi(U_c)$.
Step 4:	Calculate $\mathbf{x}^{(t+1)}$ and $\mathbf{y}^{(t+1)}$ according to the replicator dynamics algorithm in Appendix B.2.1. Update t to $t+1$.
Step 5:	Go to **Step 1**.
Step 6:	End.

B.3 Supplement of simulation experiments results

B.3.1 Proof of y*=(0.065, 0,935) with v = 0.05

Proof. Assume that at time step t, $\mathbf{y} = (0.065, 0.935)$. With $N = 10$, $M = \#U_c + \#U_h = 5$. Among the 5 enforcers, $\#U_h = 5 * 0.065 = 0$, and $\#U_c = 5$. Naturally, $\pi(U_h) = 0$, and $\pi(U_c) = 2c_0(1 - x_1x_3) + 2Bx_3 - 2ax_1x_3 = 0.2214 \geq 0$. According to the stochastic dynamics algorithm in Appendix B.2.1,

$$\mathbf{M} = \begin{bmatrix} 1/2 & 1 \\ 0 & 1/2 \end{bmatrix}. \tag{B.7}$$

Since $\pi(U_h) \equiv 0$ and $\pi(U_h)$ is always greater than 0, $\mathbf{M}$ is constant. Then we have,

$$\|\mathbf{M}\| = \begin{bmatrix} 1/3 & 2/3 \\ 0 & 1 \end{bmatrix}, \tag{B.8}$$

with

$$\mathbf{M_E} = \begin{bmatrix} -0.05 & 0.05 \\ 0.05 & -0.05 \end{bmatrix}, \tag{B.9}$$

Then we have

$$(\|\mathbf{M}\| + \mathbf{M_E}) = \begin{bmatrix} 0.2833 & 0.7167 \\ 0.05 & 0.95 \end{bmatrix}, \tag{B.10}$$

whose left eigenvector is $(0.065, 0, 935)$. According to Theorem B.2.1, $\mathbf{y}^* = (0.065, 0, 935)$ is a stable state. □

B.3.2 The sustainability of players' strategy profile in a finite market

(1) x*=(0, 1, 0) when the fraction of honest enforcers no less than 0.5

Lemma B.3.1. *In a small or medium scale market,* $\mathbf{x}^* = (0, 1, 0)$ *if* $y_1^* \geq 0.5$.

Section 5.3.1 has shown that $\mathbf{x}^* = (0, 1, 0)$ if $y_1^* > 2(B - c)/(2B - 3f)$ in an infinite and well-mixed population. When allowing for random exploration, $\mathbf{x}^*$ cannot reach $(0, 1, 0)$, but $C_{\bar{a}}$ becomes the majority and $x_2^* \approx 1$. If N is finite, the transfer matrix B.3 is uncertain because of the chance event can lead to different $\pi(S_i)$. Thus, it is hard to prove $\mathbf{x}^* = (0, 1, 0)$ by calculating the payoff matrix. Nevertheless, we can prove by reasoning the required condition of reaching $\mathbf{x}^*$. Note that the precondition of reaching an equilibrium is that the mutation rate is low enough such that once the equilibrium has been reached, other strategies cannot invade. Hence, we only consider the low exploration group.

Proof. It is known that homogeneous D or C_a is unstable ($a > 0$), the only possible equilibrium for players is homogeneous $C_{\bar{a}}$. However, the more trusting cooperators existing in the market, the more likely defectors invade, since defectors gains more in the scenario $(C_{\bar{a}}, D)$ than any other scenarios. Therefore, in a finite market that is composed of one defector and $N-1$ trusting cooperators, the expected value of $\pi(D)$ get maximized. $E(\pi(D)) = y_1(b+c-c_0-f)+y_2(b+c-c_0-B)$, and similarly $E(\pi(C_{\bar{a}})) = y_1(-c + f/2 - c_0) + y_2(-c - c_0)$. When $y_1^* \geq 0.5$, we have $E(\pi(D)) < E(\pi(C_{\bar{a}}))$, therefore, x_3 tends to decrease and x_2 tends to increase. As long as $x_2 \geq 0.95$, the market is composed of homogeneous $C_{\bar{a}}$, meanwhile the small mutation rate cannot bring in defectors. $\mathbf{x}^* = (0, 1, 0)$ is then reached. □

(2) Dynamic patterns of x*=(0, 1, 0) when y* = (0,1)

a. $N = 10, \mu = 0.01$

Lemma B.3.2. *In a small scale market,* $\mathbf{x}^* = (0, 1, 0)$ *when* $\mu = 0.01$.

Theoretically, surrounded by corrupt enforcers, $\mathbf{x}^*$ is unreachable, but when the market is small, $\mathbf{x}^* = (0, 1, 0)$ can happen. When $N = 10$ and $\mu = 0.01$, $\mathbf{y}^* \in \{(0, 1), (0.5, 0.5), (1, 0)\}$. It has been proved that when $y_1^* \geq 0.5$, $\mathbf{x}^* = (0, 1, 0)$, now let us prove when $y_1^* = (0, 1)$, $\mathbf{x}^*$ is still reachable.

Proof. Let us assume all rule enforcers are corrupt ($y_1^* = 0$). Still, the fraction of D only increases when the event $(C_{\bar{a}}, D)|(U_c)$ happens. Otherwise, the fraction of defectors tends to decrease, and during which the fraction of cooperators increases. Among the cooperators, the trusting cooperators eliminate the cautious ones, until take over the market ($\mathbf{x}^* = (0, 1, 0)$).

Despite the chance of event $(C_{\bar{a}}, D)$ not happening continuously is low, especially when trusting cooperators are the majority, such low chance event would eventually happen as long as time is long enough. Additionally, the small exploration rate ($\mu = 0.01$) leaves no chance to the defectors to invade once the equilibrium has been reached. Therefore, $\mathbf{x}^* = (0, 1, 0)$ in small scale markets when $\mu = 0.01$. □

b. $N = 100, \mu = 0.001$

Usually, in a medium scale market, $\mathbf{x}^*$ does not exist when $\mathbf{y}^* = (0, 1)$. Table B.2 shows the fraction of cautious cooperators (x_1) and of the defectors (x_3) when the fraction of trusting cooperators (x_2) reaches its summit facing pure corrupt enforcers. The results are the average of the 500 times repeated experiments.

When $a < 0.2$, $x_1 + x_3 < 0.005$, then the population has evolved into $\mathbf{x}^* = (0, 1, 0)$ where $\#C_a = \#D = 0$. However, when $a \geq 0.3$, the minimum fraction of defectors is 0.005. It means that there is at least one defector remains in the market, once the event $(C_{\bar{a}}, D)$ happens, x_2 drops from its summit. Accordingly, $\mathbf{x}^* = (0, 1, 0)$ cannot be reached.

Table B.2: $(x_1, x_3)|\big(x_2 = \max(x_2), \mathbf{y}^* = (0,1)\big)$

	$\mu = 0.001, v = 0.005$		$\mu = 0.005, v = 0.001$	
	x_1	x_3	x_1	x_3
a = 0.1	0.001	0.001	0.006	0.003
a = 0.2	0.001	0.001	0.006	0.003
a = 0.3	0.006	0.005	0.008	0.007
a = 0.4	0.005	0.009	0.008	0.008
a = 0.5	0.006	0.009	0.007	0.009

However, there are 28 cases among the 500 times repeated experiments with $a = 0.3$ unexpectedly reaches $\mathbf{x}^* = (0, 1, 0)$. The 500 repeated experiments are marked from 1 to 500, the numbers of the 28 cases are: 21, 23, 125, 127, 147, 153, 162, 163, 167, 243, 250, 260, 272, 296, 302, 324, 331, 350, 378, 384, 393, 396, 397, 404, 440, 443, 458, 469. Table B.3 presents the stochastic dynamics of $\mathbf{x}$ during time step 1146 to 1151, for elaborating on these uncommon cases.

Table B.3: Stochastic dynamics of $\mathbf{x}$ in the 272^{nd} experiment

Time Step	1146	1147	1148	1149	1150	1151	1152	1153
x_1	0.2828	0.1001	0.0262	0.0198	0.0093	0.0032	0.0021	0.0016
x_2	0.7027	0.8965	0.9474	0.9745	0.9890	0.9935	0.9958	0.9969
x_3	0.0145	0.0034	0.0264	0.0057	0.0016	0.0032	0.0021	0.0016

At step 1147, we notice that the fraction of trusting cooperators (x_2) increases to 89.65%, the rest of the players are cautious cooperators. In the next time step 1148, x_2 further increases to 97.45% after eliminating the cautious cooperators (C_a), but the exploration rate brings a few defectors to the market. From $\mathbf{x}^{(1149)}$, it can be inferred that all the defectors are paired with C_a, which drives x_2 further increases to 97.45%. The market then is composed of 97 $C_{\bar{a}}$, 2 C_a, and 1 D; the only defector is paired with one of the cautious cooperators, namely, the event $(C_{\bar{a}}, D)$ never happens. x_2 hence increases further to 98.9% at time step 1150. At this time step, the market has 99 $C_{\bar{a}}$ and 1 C_a. Since $C_{\bar{a}}$ is the dominant strategy, x_2 increases again at step 1151 to 99.35%, where there are 99 $C_{\bar{a}}$.

The remaining one player theoretically can be either C_a or D with an equal chance. In this experiment, it happens to be C_a, then x_2 increases and finally reaches 99.58%. Henceforth, all the 100 participants are trusting cooperators.

In the whole process, $\#D$ is less than 3, and $\#C_{\bar{a}}$ increases from 90 to 100, none of the defectors is paired with C_a. However, the probability of the event (D, C_a) not happening continuously is quite low, especially when x_2 is high and keeps increasing. Therefore, $\mathbf{x}^* = (0, 1, 0)$ rarely happens when $\mathbf{y}^* = (0, 1)$ in medium scale markets.

B.3.3 Analysis of the cycle length

(1) Cycle length within large scale markets

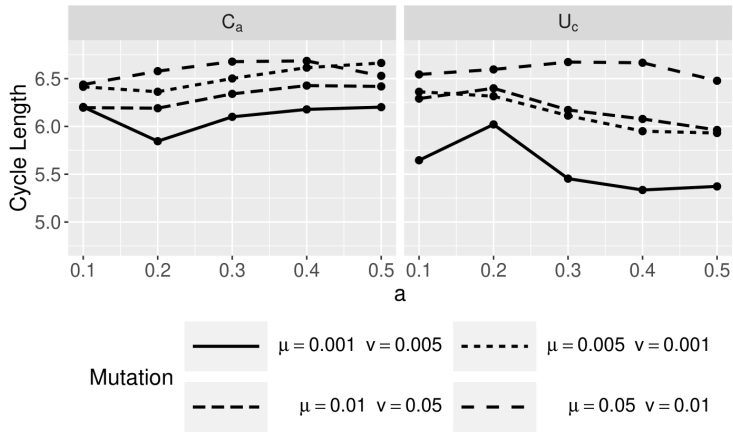


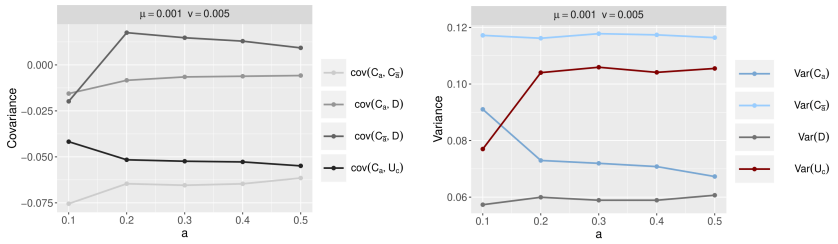
Figure B-4: The cycle length of strategies C_a and D within large scale markets where $N = 1000$. Both the mutation rate and the cost of external supervision services can influence $\mathscr{C}(C_a)$ and $\mathscr{C}(U_c)$. When $v > \mu$, $\mathscr{C}(S_i)$ is larger, since the potential x_1^* is one under $v > \mu$, defectors are more likely to invade, which drives the evolution to move into the next period. The absolute value of exploration rates also changes the cycle length. A high mutation rate decelerates the dynamic process by introducing more irrational agents, which prolongs the cycle length. In terms of a, it changes $\mathscr{C}(S_i)$ indirectly through its inhibition effect on C_a and punishment effect on U_c. Both effects can shorten or prolong the period, the net result of the two effects depends on the value of a. This complicated mechanism leads to a non-monotonic relationship between $\mathscr{C}(S_i)$ and a.

Figure B-4 gives the average cycle length of strategy C_a and U_c. The numerical results provide hints to understand this phenomenon. From Section 5.3.2, we know x_2^* is larger when $v > \mu$ than when $v < \mu$. Namely, when $v > \mu$, $C_{\bar{a}}$ always tends to dominant the market, which makes D more likely to invade, thus the stable oscillation of the system is accelerated; but when $v < \mu$, there are more D and C_a in the market which improves the chance of events (D, D) and (C_a, D), and then delays the growth of D and U_c. That is why when $v > \mu$, $\mathscr{C}(S_i)$ is larger. Holding

the relative value of μ and v, the larger the absolute value of μ is, the larger $\mathscr{C}(S_i)$ will be. The reason for this is that a high mutation rate can cause more irrational agents to choose the less dominated strategies, which decelerates the elimination process.

As to the cost of external supervision services, it has an inhibition effect on C_a and a punishment effect on D, these two effects indirectly change $\mathscr{C}(C_a)$ and $\mathscr{C}(D)$. For C_a, the inhibition effect on the one hand shortens $\mathscr{C}(C_a)$ by 1) terminating the growth of C_a in advance and limiting its summit, or rather that, once C_a eliminates D to a certain level, x_1 stops growing and immediately drops (Compare Figure 5-2(e) with Figure 5-2(d)); 2) strengthening the dominance of $C_{\bar{a}}$ to C_a, $C_{\bar{a}}$ then eliminates C_a earlier and faster. On the other hand, the inhibition effect prolongs $\mathscr{C}(C_a)$ by lifting the required fraction of defectors for C_a to start growing, which delays the growth of x_1. These two conflict consequences make $\mathscr{C}(C_a)$ change non-monotonically as a increases.

When a increases from 0.1 to 0.2, the former consequence is stronger, and $\mathscr{C}(C_a)$ decreases. This result is also confirmed in Figure B-5. In Figure B-5(a), the significant decrease of $Var(C_a)$ when a increases to 0.2 indicates the decrease of the summit of C_a. The increase of $cov(C_a, C_{\bar{a}})$ from -0.0075 to -0.065 in Figure B-5(b) evidences the shorter horizontal phase shift between x_1 and x_2, which is caused by the earlier and faster elimination of C_a by $C_{\bar{a}}$. However, when a further increases, the latter consequence becomes stronger, and $\mathscr{C}(C_a)$ becomes longer (Compare Figure 5-2(e) with Figure 5-2(d)). The decrease of $cov(C_{\bar{a}}, D)$ when a increases from 0.2 to 0.5 is exactly the consequence of x_1 longer staying at a low level, because when the market contains very few C_a, the event $(C_{\bar{a}}, D)$ is more likely to happen, which strengthens the negative correlation between $C_{\bar{a}}$ and D.



(a) $cov(S_i, S_j)$ (b) $Var(S_i)$

Figure B-5: The covariance of the fraction of strategies, $cov(S_i, S_j)$ (S_i and $S_j \in \{C_a, C_{\bar{a}}, D, U_c\}$) in large scale markets where $N = 1000$, with $\mu = 0.001, v = 0.005$. The negative correlation between C_a and $C_{\bar{a}}$ is weakened with the increase of a, due to the inhibition effect of a on C_a, which shortens the horizontal phase shift between x_1 and x_2. $cov(C_a, U_c)$ is also negative, this negative relationship is strengthened as a increases, because of the punishment effect of a on U_c accelerating the elimination of U_c by C_a. $cov(C_{\bar{a}}, D)$ has non-monotonic changes. When a increases from 0.1 to 0.2, the reduced summit of C_a leaves $C_{\bar{a}}$ a higher chance to co-exist with D, $cov(C_{\bar{a}}, D)$ therefore increases to a positive number. As a further increases, $\#C_a$ has a longer time staying at a low level; C_a is more likely to be eliminated by defectors, and $cov(C_{\bar{a}}, D)$ is hence weakened. $Var(C_a)$ drops (resp. $Var(U_c)$ rises) largely as a increase from 0.1 to 0.2, which indicates a smaller (resp. larger) wave height of the fraction of C_a (resp. U_c) and confirms the lower (resp. higher) summit of x_1 (resp. y_2).

The trend of $\mathscr{C}(C_a)$ under $\mu = 0.05, v = 0.01$ is different from under other mutation rates. That is because with the highest μ, the minimum $\#C_a$ and $\#D$ are lifted the most, then the remaining more cautious cooperators contend with the remaining defectors longer, and hence delays the coming of the growth of defectors. Additionally, it is also known that a higher a lifts the required fraction of defectors for C_a to start growing. Because of these two reasons, $\mathscr{C}(C_a)$ is prolonged as a increases. When a further increases from 0.4 to 0.5, the consequence of reducing the summits of C_a plays the main role again, and $\mathscr{C}(C_a)$ drops accordingly.

Another interesting phenomenon is that $\mathscr{C}(U_c)$ is almost the same as $\mathscr{C}(C_a)$ when $\mu = 0.05$. Theoretically, $\mathscr{C}(C_a)$ and $\mathscr{C}(U_c)$ should be similar. However, when μ is small, U_c is more likely to raise up more than

one time as C_a falling down. In Figure 5-4(b), the fraction of trusting cooperators reaches its summit by eliminating cautious cooperators during time step 7 to 13, during which C_a decreases monotonically, but U_c grows up twice at time step 9 and 11 respectively. That is because under lower mutation rate, $\#D$ and $\#C_a$ are less when $C_{\bar{a}}$ reaches its summit; then the few remaining defectors are more likely to be paired with $C_{\bar{a}}$ instead of C_a. Namely, the event $(C_{\bar{a}}, D)|(U_c)$ has a higher chance to happen, which stimulates the growth of U_c. Therefore, the period of $\mathbf{y}$ is not completely in line with the period of $\mathbf{x}$. But when μ is very high, more remaining D and C_a induce a higher probability of the event $(C_a, D)|(U_c)$, which prevents y_2 from growing multiple times when x_2 increases. That is why $\mathscr{C}(U_c)$ and $\mathscr{C}(D)$ in Figure B-4 are more similar to each other when $\mu = 0.05, v = 0.01$.

When $\mu \neq 0.05$, $\mathscr{C}(U_c)$ first climbs up and then goes down. When a increases to 0.2, the inhibition effect plays the main role, it delays the growth of C_a and hence lead to a higher summit of U_c, and indirectly increases $Var(U_c)$, as shown in Figure B-5(b). For rule enforcers, the higher summit of U_c takes longer time to reach, $\mathscr{C}(U_c)$ is then prolonged. As a further increases, $Var(U_c)$ does not change too much, the punishment effect on U_c plays the main role: a heavier punishment accelerates the elimination of U_c by C_a, and henceforth a higher a is accompanied by a shorter $\mathscr{C}(U_c)$ when $a > 0.2$.

(2) Cycle length within medium scale markets

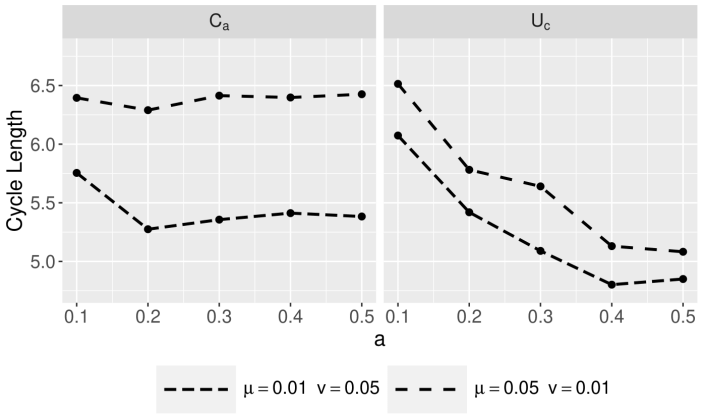


Figure B-6: $\mathscr{C}(C_a)$ and $\mathscr{C}(U_c)$ within medium scale markets where $N = 100$. When $N = 100$, the event $(C_a, D)|(U_c)$ happens with a higher frequency compared with when $N = 1000$. This fact amplifies the punishment effect of a, hence the average fraction of the strategy U_c is lower, and $\mathscr{C}(U_c)$ decreases larger as a increases.

$\mathscr{C}(C_a)$ is similar under different market scales, but $\mathscr{C}(U_c)$ is different. Let $R\big(\mathscr{C}(U_c)|(\mu)\big)$ be the range of the cycle length of strategy U_c under certain μ. When $N = 1000$, $R\big(\mathscr{C}(U_c)|(\mu = 0.01)\big) = 0.44$ and $R\big(\mathscr{C}(U_c)|(\mu = 0.05)\big) = 0.20$, whereas when $N = 100$, $R\big(\mathscr{C}(U_c)|(\mu = 0.01)\big) = 1.27$ and $R\big(\mathscr{C}(U_c)|(\mu = 0.05)\big) = 1.43$. Such results indicate that the punishment effect of a on U_c is amplified in the medium scale market. This result is owing to the higher frequency of the event $(C_a, D)|(U_c)$, through which the punishment effect of a accelerates the elimination of U_c, and eventually shortens $\mathscr{C}(U_c)$.

(3) The variance of the fraction of strategies in medium scale markets

Compared with in large scale markets, $Var(U_c)$ is much lower in a medium scale market. Because the punishment effect of a on U_c is amplified by

the more often event $(C_a, D)|(U_c)$, y_2 is more likely to drop from the high level. With the lower summit in each period, $Var(U_c)$ and $E(y_2)$ are lower.

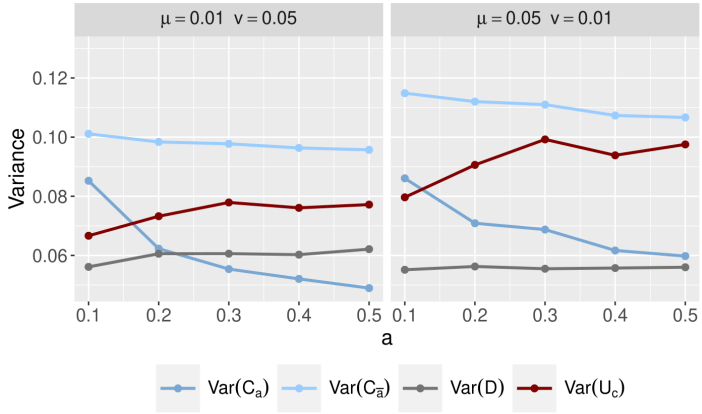


Figure B-7: The variance of the population sizes of the coexisting strategies in medium scale markets where $N = 100$.

But when $a \geq 0.2$ the inhibition effect of a on C_a plays the main role, which offsets the consequence of decreasing $E(y_2)$ brought by the amplified punishment effect. Compare Figure B-7 to Figure B-5(b), it can be observed that when a increases from 0.1 to 0.2, the drops of $Var(C_a)$ within $N = 100$ and $N = 1000$ are similar; but when a further increases, $Var(C_a)$ decreases much more in a medium scale market than in a large scale market. When $N = 100$, $Var(C_a)$ decreases 42.5% ($\mu = 0.01$) or 30% ($\mu = 0.05$), the numbers are 17.9% and 18.4% when $N = 1000$. The reduced $Var(C_a)$ indicates the stronger inhibition effect on C_a, which promotes the growth of U_c and increases $E(y_2)$. That is why $E(y_2)|(a \geq 0.2)$ does not show differences in the medium and the large scale market.

B.3.4 Supplements of y* within a medium scale market

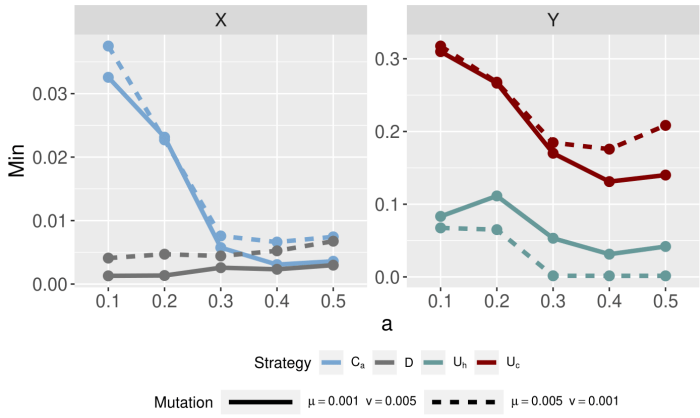


Figure B-8: The minimum fraction of strategies within medium scale markets where $N = 100$. A higher μ lifts the minimum fraction of defectors, which makes the defectors cannot permanently being eliminated. The existence of defectors then stimulates the growth of corrupt enforcers, and thereby leads $\mathbf{y}$ to escape from $(0.5, 0.5)$ and ultimately evolve to $\mathbf{y}^* = (0, 1)$.

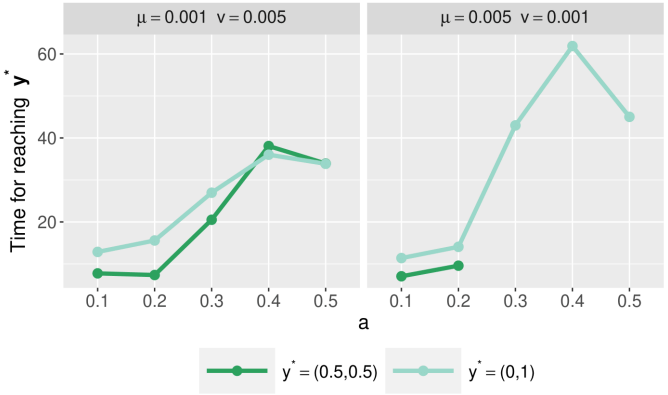


Figure B-9: The average time for reaching $\mathbf{y}^*$ in medium scale markets where $N = 100$. $\mathbf{y}^* \in \{(0.5, 0.5), (0, 1)\}$. The punishment effect of a prevents $y_2^* = 1$, but the inhibition effect of a contributs to $y_2^* = 1$. As a increase, both these two effects become stronger, the time of reaching $\mathbf{y}^*$ is accordingly prolonged. When $a = 0.4$, the time to reach the equilibrium is the longest.

B.3.5 The probability of event $(C_a, D)|(U_c)$

Lemma B.3.3. *Given* $\mathbf{x}$ *and* $\mathbf{y}$*, the event* $(C_a, D)|(U_c)$ *is easier to happen when the scale of the market is smaller, which makes* y_2 *easier to drop from the high level.*

Proof. Without loss of generality, let the size of the two markets be N_1 and N_2 ($N_1 < N_2$), the corresponding number of rule enforcers are $M_1 = N_1/2$ and $M_2 = N_2/2$. The probability of the event $(C_a, D)|(U_c)$ is $P\big((C_a, D)|(U_c)\big)$, we then have:

$$\begin{aligned} P_1\big((C_a, D)|(U_c)\big) &= P_1(C_a, D)P_1(U_c) \\ &= \frac{C^{\ 1}_{x_1 N_1} C^{\ 1}_{y_2 M_1}}{C^2_{N_1}}, \\ P_2\big((C_a, D)|(U_c)\big) &= P_2(C_a, D)P_2(U_c) \\ &= \frac{C^{\ 1}_{x_1 N_2} C^{\ 1}_{y_2 M_2}}{C^2_{N_2}}, \\ \frac{P_1\big((C_a, D)|(U_c)\big)}{P_2\big((C_a, D)|(U_c)\big)} &= \frac{N_1}{N_2}\frac{N_2 - 1}{N_1 - 1} \\ &> 1. \end{aligned} \tag{B.11}$$

Thus, the probability of event $(C_a, D)|(U_c)$ is higher within a smaller scale market, which decreases the payoff of corrupt enforcers and makes their fraction easier to drop from a high level. □

B.3.6 Discussion about convergence

It is worth considering whether the simulation experiment results of finite markets converge to the analytical results of infinite markets as N increases. The answer is positive, because the expected payoff of strategies in infinite markets converges to the payoff of strategies in infinite markets. Additionally, the bias in the actual payoff of finite markets caused by randomness tends to zero as N increases. In the following, we provide the

proof supporting our conclusion.

Lemma B.3.4. *The expected payoff of strategies in finite markets converges to the payoff of strategies in infinite markets as N increases.*

For better elaboration, we take the payoff of U_c as an example to prove Lemma B.3.4. The proof process for other strategies is analogous.

Proof. When $N \to \infty$, the payoff of corrupt enforcers, $\pi(U_c)$, is a function of $\mathbf{x}$ as presented in eq.5.2. However, in finite markets, the expected payoff of U_c is a function of $\#C_a$, $\#C_{\bar{a}}$, and $\#D$. To distinguish between the payoff in finite and infinite markets, we denote the expected payoff in finite markets as π_{U_C}:

$$\begin{aligned}\pi_{U_C} =& P_{(C_a,D)}(c_0 + B - a) + P_{(C_{\bar{a}},D)}(2c_0 + B) + P_{(D,D)}(2c_0 + 2B) + \\ & (1 - P_{(C_a,D)} - P_{(C_{\bar{a}},D)} - P_{(D,D)})2c_0\end{aligned}, \tag{B.12}$$

where $N = \#C_a + \#C_{\bar{a}} + \#D$, $P_{(C_a,D)} = \frac{2\#C_a\#D}{N(N-1)}$, $P_{(C_{\bar{a}},D)} = \frac{2\#C_{\bar{a}}\#D}{N(N-1)}$, and $P_{(D,D)} = \frac{\#D(\#D-1)}{N(N-1)}$.

Since as N grows, $P_{(C_a,D)} \to 2x_1x_3$, $P_{(C_{\bar{a}},D)} \to 2x_2x_3$, and $P_{(D,D)} \to x_3^2$, $\pi_{U_c} \to \pi(U_c)$. Therefore, the expected payoff of U_c in finite markets converges to the payoff of U_c in infinite markets as N increases. □

In finite markets, it is not possible to completely eliminate the randomness that introduces bias to the actual payoff. For example, the chance event that every defector is paired with a trusting cooperator can happen and result in the actual payoff for U_c being higher than π_{U_c}. However, we can prove that the probability of such chance events tends to zero as N increases.

Lemma B.3.5. *The bias in the actual payoff of finite markets caused by randomness tends to zero as N increases.*

We take the aforementioned chance event as an example to prove the Lemma B.3.5. The proof process for other events that can cause bias is analogous.

Proof. Let $P(D \to C_{\bar{a}})$ be the probability of the chance event where every defector is paired with a trusting cooperator:

$$P(D \to C_{\bar{a}}) = \frac{2\#D \cdot A^{\#D}_{\#C_{\bar{a}}} \cdot A^{2}_{\#C_a+(\#C_{\bar{a}}-\#D)} \cdot \left(\frac{N}{2}!\right)}{N!}. \tag{B.13}$$

To better understanding the calculation of formula (B.13), let's imagine that all the players are assigned with an identical number from 1 to N. Then there are $N!$ ways to arrange the N players. Among the players, $\#D$ of them are labeled as D, $\#C_{\bar{a}}$ of them are labeled as $C_{\bar{a}}$.

To calculate the probability, we first select a group of players with label $C_{\bar{a}}$ and pair them with the $\#D$ number of defectors to form sets of $(C_{\bar{a}}, D)$. Since we consider $(C_{\bar{a}}, D)$ and $(D, C_{\bar{a}})$ as different pairs, there are in total $2\#D \cdot A^{\#D}_{\#C_{\bar{a}}}$ arrangement.

Then the number of remaining cautious cooperators is $\#C_a$, and the number of trusting cooperators is $\#C_{\bar{a}} - \#D$, they can pair freely. Therefore the number of arrangement for these remaining player is $A^{2}_{\#C_a+(\#C_{\bar{a}}-\#D)}$.

In total, there are $N/2$ pairs, and these pairs can be in any order, as a result, the total number of arrangements of the N players satisfying the condition that every defector is paired with a trusting cooperator is $2\#D \cdot A^{\#D}_{\#C_{\bar{a}}} \cdot A^{2}_{\#C_a+(\#C_{\bar{a}}-\#D)} \cdot \left(\frac{N}{2}!\right)$. Finally, dividing this value by $N!$ will give the precise probability of $P(D \to C_{\bar{a}})$.

Then through calculations, we can easily find that given a specific $\mathbf{x}$, as N increases, the probability of $P(D \approx C_{\bar{a}})$ decreases rapidly and tends to zero. For example, given $\mathbf{x} = (0.2, 0.6, 0.2)$, $P(D \approx C_{\bar{a}}) = 0.119$ when $N = 10$, but when $N = 50$, the probability decreases to 9.675×10^{-22}. This

fact implies that in finite markets, although randomness always exists and leads to the actual payoff deviating from the expected payoff, the likelihood of such deviations decreases as N increases. □

Accordingly, combining Lemma B.3.4 and Lemma B.3.5, we can conclude that the actual payoff converges to π_{U_c}, and π_{U_c} converges to $\pi(U_c)$ when $N \to \infty$.

In fact, this convergence is already evident in the difference in the cycle length of strategies observed in large and medium scale markets. Comparing Figure B-6 with Figure B-4, it is clear that $\mathscr{C}(S_i)|N1000 < \mathscr{C}(S_i)|N100$. This is because $\mathbf{x}$ and $\mathbf{y}$ can sustain longer at the potential equilibria in larger scale markets. As expected, when further increases N, (S_i) will decrease to a lower level.

B.3.7 When one rule enforcer monitors multiple pairs of players

In our model, we assume that each pair of players is monitored by one rule enforcer, therefore within finite markets $M = N/2$. However, this assumption can be arguable, as in practical life, one rule enforcer can monitor multiple pairs of players. A natural question is how do the original conclusions change when $M < N/2$. There are two ways to achieve $M < N/2$: by reducing the number of rule enforcers or by expanding the market scale to include more players; for the convenience of elaboration, we do not consider changing these two factors at the same time.

In the case of infinite markets, the replicator dynamics solely depend on $\mathbf{x}$ and $\mathbf{y}$, which are unaffected by either of these two ways. Therefore, when $M < N/2$, the player-enforcer dynamics remain unchanged, and the original conclusions still hold. For finite market, however, the evolution of strategies might be affected because of the affected mutation rate and the changed probability of events. Next, we discuss the results arise from

reducing M and increasing N in finite markets respectively.

By reducing M while keeping N constant, the number of pairs of players that one rule enforcer monitors increases. This change itself has no influence the evolution of strategy profiles in a finite population, provided that each rule enforcer is randomly assigned to the same number of pairs. This assumption ensures that the assignment of each rule enforcer to $N/(2M')$ pairs of players produces the same results as the alternative approach: duplicating the M' rule enforcers $(N/2)/M'$ times, thereby expanding the number of rule enforcers to $N/2$, and assigning each of them one pair.

However, the evolution process is influenced if the reduction of M affects the effectiveness of the mutation rate v and impedes the invasions of randomly exploring rule enforcers. To illustrate this, we consider two representative examples: $M = 50$ and $M = 5$, while keeping $N = 1000$. In the former case, under high mutation rates, only the number of monitored pairs changes, while in the latter case, the effect of the mutation rate changes.

Consider a large scale market where $N = 1000$ with 50 rule enforcers. Under high mutation rates, randomly matching 500 rule enforcers with the 500 pairs of players is the same as assigning 10 pairs of players to each of the 50 rule enforcers. In both scenarios, $\mathbf{x}$ and $\mathbf{y}$ exhibit cyclic dominance due to the invasions caused by the mutation rate. The mean value of the fraction of specific strategies under $M = 50$ are presented in Figure B-10, which aligns with the original results under $M = 500$ in Figure 5-6.

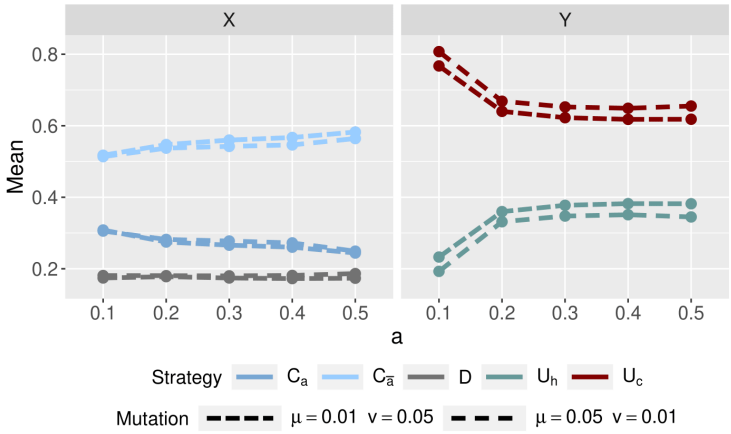


Figure B-10: The mean value of the fraction of specific strategies ($E(\#S_i/N)$) when $N = 1000$, $M = 50$. Since reducing M from 500 to 50 does not change the effects of v, random exploration by rule enforcers can always lead to invasions, resulting in cyclic dominance of $\mathbf{y}$. In each round of evolution, assigning each rule enforcers to 10 pairs of players is equivalent to expanding the 50 rule enforcers to 500 and randomly matching them with the 500 pairs of players. Consequently, the evolution results are the same as those obtained when $M = 500$.

However, under low mutation rates, $M = 50$ leads to $\mathbf{y}^* = (0, 1)$, which is distinct from the cyclic dominance of $\mathbf{y}$ observed in $M = 500$. The reason is that $M = 50$ makes the low mutation rates ($v = 0.001$ and $v = 0.005$) lose their effectiveness, as no randomly exploring rule enforcers can invade once $\mathbf{y}^* = (0, 1)$ is reached. As expected, further reducing M to 5 makes $\mathbf{y}^*$ always reachable under both high and low mutation rates. The relative frequency of $\mathbf{y}^*$ with $M = 5$ among the 500 repeated experiments is presented in Figure B-11. In summary, reducing M alone does not influence the evolution in finite markets unless it affects the mutation rate, as too small M impedes the presence of randomly exploring rule enforcers.

By the other way that increasing N with controlling M, the number of randomly exploring players might increase. For example, Figure B-11 and Figure 5-5 represent the results under $N = 10$ and $N = 1000$ respectively,

while keeping $M = 5$. It can be observed that $\mathbf{y}^* = (0.5, 0.5)$ does not occur when $N = 1000$, in contrast to the results when $N = 10$. This is because the larger N prevents the complete elimination of defectors, which stimulates the growth of corrupt enforcers and leads $\mathbf{y} = (0.5, 0.5)$ to evolve into $\mathbf{y}^* = (0, 1)$. Therefore, the only opportunity for the market to evolve into a desirable state is that each corrupt rule enforcers being matched with the pair (C_a, D) during the early stages of the evolution. This matching drives the rapid evolution of $\mathbf{y}$ towards $\mathbf{y}^* = (1, 0)$.

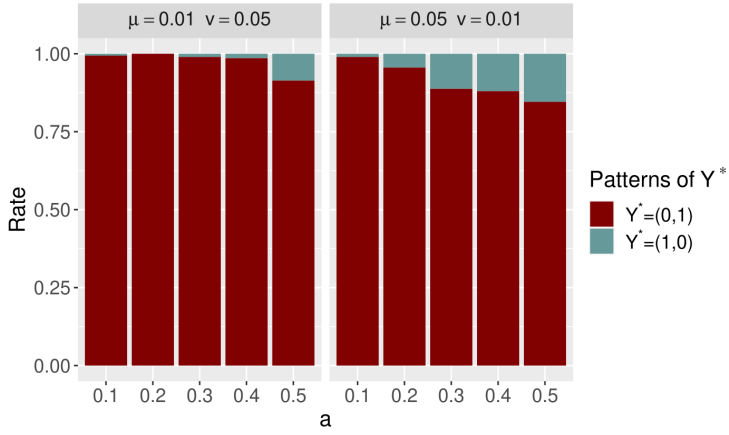


Figure B-11: The relative frequency of specific equilibrium of rule enforcers among the 500 repetitions, with $M = 5$ and $N = 1000$. In contrast to the cyclic dominance observed in Figure 5-7 where $M = 500$, reducing M to 5 actually makes the mutation rate of rule enforcers, v, lose effectiveness. As a result, the equilibrium $\mathbf{y}^*$ is always reachable. Comparing these results to those obtained in small scale markets where M remains but $N = 10$, $\mathbf{y}^* = (0.5, 0.5)$ does not occur when $N = 1000$. This difference results from the persistent presence of defectors, which stimulates the growth of U_c and drives $\mathbf{y} = (0.5, 0.5)$ to $\mathbf{y}^* = (0, 1)$.

In this circumstance, a high v in turn prevents the elimination of corrupt enforcers at the early stages, as it increases the probability of honest enforcers exploring strategy U_c. That is why the probability of evolving into a good market that contains only honest enforcers are even higher when $v < \mu$ in Figure B-11. This result contradicts to our previous conclu-

sion that higher v is always beneficial, since the expanded N essentially prevents the potential equilibrium $\mathbf{y}^* = (0.5, 0.5)$ under $v > \mu$.

The expansion of N also brings another change: the lower probability of event $(C_a, D)|(U_c)$. This results in different mean value of the fraction of strategies between the case of $N = 100$ and $N = 1000$. Since the mechanism behind this difference has been illustrated in Section 5.4.2, we will not delve into it further here.

To summarize, when one rule enforcer monitors multiple pairs of players in infinite markets, all the original conclusions still hold. In finite markets, reducing M and increasing N have different influence. By reducing M, as long as it does not affect the mutation rate of rule enforcers, all the original conclusions hold, otherwise $\mathbf{y}^*$ becomes always reachable. Increasing N can impede $\mathbf{y}^* = (0.5, 0.5)$ and eventually lead to $\mathbf{y}^* = (0, 1)$ when $\mathbf{y}^*$ is reachable; when $\mathbf{y}^*$ is unreachable, increasing N influence $E(\#S_i/N)$, but does not alter the original conclusions regarding the influence of a and v.

Bibliography

[1] Klaus Abbink. Staff rotation as an anti-corruption policy: an experimental study. *European Journal of Political Economy*, 20(4):887–906, 2004.

[2] Klaus Abbink, Utteeyo Dasgupta, Lata Gangadharan, and Tarun Jain. Letting the briber go free: An experiment on mitigating harassment bribes. *Journal of Public Economics*, 111:17–28, 2014.

[3] Klaus Abbink and Kevin Wu. Reward self-reporting to deter corruption: An experiment on mitigating collusive bribery. *Journal of Economic Behavior & Organization*, 133:256–272, 2017.

[4] Sherief Abdallah, Rasha Sayed, Iyad Rahwan, Brad L LeVeck, Manuel Cebrian, Alex Rutherford, and James H Fowler. Corruption drives the emergence of civil society. *Journal of the Royal Society Interface*, 11(93):20131044, 2014.

[5] William C Abram and Kadeem Noray. Political corruption and public activism: an evolutionary game-theoretic analysis. *Dynamic Games and Applications*, 8(1):1–21, 2018.

[6] Peter Alders and Frederik T Schut. The 2015 long-term care reform in the netherlands: Getting the financial incentives right? *Health Policy*, 123(3):312–316, 2019.

[7] Riham AlTawy and Amr M Youssef. Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices. *IEEE Access*, 4:959–979, 2016.

[8] J Andrews and Monique Borgerhoff Mulder. Cultural group selection and the design of redd+: insights from pemba. *Sustainability science*, 13(1):93–107, 2018.

[9] Mourade Azrour, Jamal Mabrouki, Azedine Guezzaz, and Yousef Farhaoui. New enhanced authentication protocol for internet of things. *Big Data Mining and Analytics*, 4(1):1–9, 2021.

[10] Daniel Balliet, Laetitia B Mulder, and Paul AM Van Lange. Reward, punishment, and cooperation: a meta-analysis. *Psychological bulletin*, 137(4):594, 2011.

[11] Masoud Barati, Gagangeet Singh Aujla, Jose Tomas Llanos, Kwabena Adu Duodu, Omer F Rana, Madeline Carr, and Rajiv Ranjan. Privacy-aware cloud auditing for gdpr compliance verification in online healthcare. *IEEE Transactions on Industrial Informatics*, 18(7):4808–4819, 2021.

[12] Karna Basu, Kaushik Basu, and Tito Cordella. Asymmetric punishment as an instrument of corruption control. *Journal of public economic theory*, 18(6):831–856, 2016.

[13] Kaushik Basu. Why, for a class of bribes, the act of giving a bribe should be treated as legal. *Ministry of Finance, Government of India*, 2011.

[14] F Bauzá, D Soriano-Paños, J Gómez-Gardeñes, and LM Floría. Fear induced explosive transitions in the dynamics of corruption. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 30(6):063107, 2020.

[15] Rafael H Bordini, Jomi Fred Hübner, and Michael Wooldridge. *Programming multi-agent systems in AgentSpeak using Jason*, volume 8. John Wiley & Sons, 2007.

[16] Laurent Bouton, Aniol Llorente-Saguer, and Frédéric Malherbe. Get rid of unanimity rule: The superiority of majority rules with veto power. *Journal of Political Economy*, 126(1):107–149, 2018.

[17] Yves Breitmoser. Cooperation, but no reciprocity: Individual strategies in the repeated prisoner's dilemma. *American Economic Review*, 105(9):2882–2910, 2015.

[18] Donald J Brown. Aggregation of preferences. *The Quarterly Journal of Economics*, 89(3):456–469, 1975.

[19] Isabel Brusca, Francesca Manes Rossi, and Natalia Aversano. Accountability and transparency to fight against corruption: an international comparative analysis. *Journal of Comparative Policy Analysis: Research and Practice*, 20(5):486–504, 2018.

[20] Johannes Buckenmaier, Eugen Dimant, Ann-Christin Posten, and Ulrich Schmidt. Efficient institutions and effective deterrence: on timing and uncertainty of formal sanctions. *Journal of Risk and Uncertainty*, 62(2):177–201, 2021.

[21] Quyet H. Cao, Madhusudan Giyyarpuram, Reza Farahbakhsh, and Noel Crespi. Policy-based usage control for a trustworthy data sharing platform in smart cities. *Future Generation Computer Systems*, 107:998 – 1010, 2020.

[22] Barbara Carminati, Elena Ferrari, and Christian Rondanini. Blockchain as a platform for secure inter-organizational business processes. In *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, pages 122–129. IEEE, 2018.

[23] Barbara Carminati, Christian Rondanini, and Elena Ferrari. Confidential business process execution on blockchain. In *2018 ieee international conference on web services (icws)*, pages 58–65. IEEE, 2018.

[24] Roberto Casado-Vara and Juan Corchado. Distributed e-health wide-world accounting ledger via blockchain. *Journal of Intelligent & Fuzzy Systems*, 36(3):2381–2386, 2019.

[25] Núria Casellas. Legal ontologies. *Legal ontology engineering: Methodologies, modelling trends, and the ontology of professional judicial knowledge*, pages 109–169, 2011.

[26] Roy Cerqueti and Raffaella Coppier. Corruption, evasion and environmental policy: a game theory approach. *IMA Journal of Management Mathematics*, 27(2):235–253, 2016.

[27] Shuchih E Chang and Yichian Chen. When blockchain meets supply chain: A systematic literature review on current development and potential applications. *Ieee Access*, 8:62478–62494, 2020.

[28] Xiaojie Chen, Tatsuya Sasaki, Åke Brännström, and Ulf Dieckmann. First carrot, then stick: how the adaptive hybridization of incentives promotes cooperation. *Journal of the royal society interface*, 12(102):20140935, 2015.

[29] Xiaojie Chen, Attila Szolnoki, and Matjaž Perc. Probabilistic sharing solves the problem of costly punishment. *New Journal of Physics*, 16(8):083016, 2014.

[30] Hans Christiansen, Charles P Oman, and Andrew Charlton. Incentives-based competition for foreign direct investment: The case of brazil. 2003.

[31] Ge Chu and Alexei Lisitsa. Poster: Agent-based (bdi) modeling for automation of penetration testing. In *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, pages 1–2. IEEE, 2018.

[32] Theodor Cimpeanu, Cedric Perret, and The Anh Han. Cost-efficient interventions for promoting fairness in the ultimatum game. *Knowledge-Based Systems*, 233:107545, 2021.

[33] Simone Cirani, Marco Picone, Pietro Gonizzi, Luca Veltri, and Gianluigi Ferrari. Iot-oas: An oauth-based authorization service architecture for secure services in iot scenarios. *IEEE sensors journal*, 15(2):1224–1234, 2014.

[34] J. Claassen, R. Koning, and P. Grosso. Linux containers networking: Performance and scalability of kernel modules. In *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, pages 713–717, April 2016.

[35] John Conlisk. Why bounded rationality? *Journal of economic literature*, 34(2):669–700, 1996.

[36] Flavio Corradini, Alessandro Marcelletti, Andrea Morichetta, Andrea Polini, Barbara Re, and Francesco Tiezzi. Engineering trustable and auditable choreography-based systems using blockchain. *ACM Transactions on Management Information Systems (TMIS)*, 13(3):1–53, 2022.

[37] Marta C Couto, Jorge M Pacheco, and Francisco C Santos. Governance of risky public goods under graduated punishment. *Journal of Theoretical Biology*, 505:110423, 2020.

[38] Vincent P Crawford. Learning and mixed-strategy equilibria in evolutionary games. *Journal of Theoretical Biology*, 140(4):537–550, 1989.

[39] Simon Dalmolen, HJM Bastiaansen, EJJ Somers, Somayeh Djafari, Maarten Kollenstart, and Matthijs Punter. Maintaining control over sensitive data in the physical internet: Towards an open, service oriented, network-model for infrastructural data sovereignty. In *6th International Physical Internet Conference (IPIC), London 2019*, 2019.

[40] Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. Personalized privacy assistants for the internet of things: Providing users with notice and choice. *IEEE Pervasive Computing*, 17(3):35–46, 2018.

[41] Domenico De Giovanni, Fabio Lamantia, and Mario Pezzino. Evolutionary dynamics of compliance in a two-population game of auditors and taxpayers. *Communications in Nonlinear Science and Numerical Simulation*, 117:106945, 2023.

[42] R v Doesburg and T v Engers. Perspectives on the formal representation of the interpretation of norms. In *Legal Knowledge and Information Systems: JURIX 2016: The Twenty-Ninth Annual Conference*, volume 294, page 183. IOS Press, 2016.

[43] Jason A Donenfeld. Wireguard: Next generation kernel network tunnel. In *NDSS*, 2017.

[44] Esther Duflo, Michael Greenstone, Rohini Pande, and Nicholas Ryan. Truth-telling by third-party auditors and the response of polluting firms: Experimental evidence from india. *The Quarterly Journal of Economics*, 128(4):1499–1545, 2013.

[45] Manh Hong Duong and The Anh Han. Cost efficiency of institutional incentives for promoting cooperation in finite populations. *Proceedings of the Royal Society A*, 477(2254):20210568, 2021.

[46] Phan The Duy, Hien Do Hoang, Anh Gia-Tuan Nguyen, Van-Hau Pham, et al. B-dac: a decentralized access control framework on northbound interface for securing sdn using blockchain. *Journal of Information Security and Applications*, 64:103080, 2022.

[47] Antonio Estache. 17. institutions for infrastructure in developing countries: What we know... and the lot we still need to know. In *The Handbook of Economic Development and Institutions*, pages 634–688. Princeton University Press, 2020.

[48] European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council.

[49] Facebook. Facebook community standards.

[50] Ruguo Fan, Yitong Wang, Fangze Chen, Kang Du, and Yuanyuan Wang. How do government policies affect the diffusion of green innovation among peer enterprises?-an evolutionary-game model in complex networks. *Journal of Cleaner Production*, 364:132711, 2022.

[51] Yinhai Fang, Tina P Benko, Matjaž Perc, Haiyan Xu, and Qingmei Tan. Synergistic third-party rewarding and punishment in the public goods game. *Proceedings of the Royal Society A*, 475(2227):20190349, 2019.

[52] Lana Friesen and Lata Gangadharan. Designing self-reporting regimes to encourage truth telling: An experimental study. *Journal of Economic Behavior & Organization*, 94:90–102, 2013.

[53] Simon Gächter. Carrot or stick? *Nature*, 483(7387):39–40, 2012.

[54] Shiping Gao and Jinling Liang. Cooperation under institutional incentives with perfect and imperfect observation. *Physics Letters A*, 384(28):126723, 2020.

[55] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In *Advances in Cryptology-EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II*, pages 281–310. Springer, 2015.

[56] Julián García and Arne Traulsen. Evolution of coordinated punishment to enforce cooperation from an unbiased strategy space. *Journal of the Royal Society Interface*, 16(156):20190127, 2019.

[57] Xiuqin Geng and Dawei Yang. Intelligent prediction mathematical model of industrial financial fraud based on data mining. *Mathematical Problems in Engineering*, 2021:1–8, 2021.

[58] Herbert Gintis et al. *Game theory evolving: A problem-centered introduction to modeling strategic behavior*. Princeton university press, 2000.

[59] Cuiling Gu, Xianjia Wang, Jinhua Zhao, Rui Ding, and Qilong He. Evolutionary game dynamics of moran process with fuzzy payoffs and its application. *Applied Mathematics and Computation*, 378:125227, 2020.

[60] Lingling Guo, Jingjing Chen, Shihan Li, Yafei Li, and Jinzhi Lu. A blockchain and iot-based lightweight framework for enabling information transparency in supply chain finance. *Digital Communications and Networks*, 8(4):576–587, 2022.

[61] Özgür Gürerk, Bernd Irlenbusch, and Bettina Rockenbach. The competitive advantage of sanctioning institutions. *Science*, 312(5770):108–111, 2006.

[62] Mehrdad Hajizadeh, Nima Afraz, Marco Ruffini, and Thomas Bauschert. Collaborative cyber attack defense in sdn networks using blockchain technology. In *2020 6th IEEE Conference on Network Softwarization (NetSoft)*, pages 487–492. IEEE, 2020.

[63] The Anh Han and Long Tran-Thanh. Cost-effective external interference for promoting the evolution of cooperation. *Scientific reports*, 8(1):1–9, 2018.

[64] Christoph Hauert, Arne Traulsen, Hannelore Brandt, Martin A Nowak, and Karl Sigmund. Via freedom to coercion: the emergence of costly punishment. *Science*, 316(5833):1905–1907, 2007.

[65] Dirk Helbing, Attila Szolnoki, Matjaž Perc, and György Szabó. Punish, but not too hard: how costly punishment spreads in the spatial public goods game. *New Journal of Physics*, 12(8):083005, 2010.

[66] Joseph Henrich, Richard McElreath, Abigail Barr, Jean Ensminger, Clark Barrett, Alexander Bolyanatz, Juan Camilo Cardenas, Michael Gurven, Edwins Gwako, Natalie Henrich, et al. Costly punishment across human societies. *Science*, 312(5781):1767–1770, 2006.

[67] William GS Hines. Three characterizations of population strategy stability. *Journal of applied probability*, 17(2):333–340, 1980.

[68] Mark Hinnells and Brenda Boardman. Market transformation: innovation theory and practice. *Innovation for a Low Carbon Economy: Economic, Institutional and Management Approaches*, pages 203–229, 2008.

[69] Arend Hintze and Christoph Adami. Punishment in public goods games leads to meta-stable phase transitions and hysteresis. *Physical biology*, 12(4):046005, 2015.

[70] Arend Hintze, Jochen Staudacher, Katja Gelhar, Alexander Pothmann, Juliana Rasch, and Daniel Wildegger. Inclusive groups can avoid the tragedy of the commons. *Scientific reports*, 10(1):1–8, 2020.

[71] Josef Hofbauer and Karl Sigmund. Evolutionary game dynamics. *Bulletin of the American mathematical society*, 40(4):479–519, 2003.

[72] Josef Hofbauer, Karl Sigmund, et al. *Evolutionary games and population dynamics*. Cambridge university press, 1998.

[73] Kai Hu, Jian Zhu, Yi Ding, Xiaomin Bai, and Jiehua Huang. Smart contract engineering. *Electronics*, 9(12):2042, 2020.

[74] Feng Huang, Xiaojie Chen, and Long Wang. Evolution of cooperation in a hierarchical society with corruption control. *Journal of Theoretical Biology*, 449:60–72, 2018.

[75] Richard Hull, Vishal S Batra, Yi-Min Chen, Alin Deutsch, Fenno F Terry Heath III, and Victor Vianu. Towards a shared ledger business collaboration language based on data-aware processes. In *Service-Oriented Computing*, pages 18–36, Cham, 2016. Springer International Publishing.

[76] Eduard Ivanov. Aml/cft and anti-corruption compliance regulation: two parallel roads? *IACA Research Paper Series*, (2), 2018.

[77] Jonathan W Ivy, James N Meindl, Eric Overley, and Kristen M Robson. Token economy: A systematic review of procedural descriptions. *Behavior Modification*, 41(5):708–737, 2017.

[78] Johnson Iyilade and Julita Vassileva. P2u: A privacy policy specification language for secondary data sharing and usage. In *2014 IEEE Security and Privacy Workshops*, pages 18–22, 2014.

[79] Raúl Jiménez, Haydee Lugo, José A. Cuesta, and Angel Sánchez. Emergence and resilience of cooperation in the spatial prisoner's dilemma via a reward mechanism. *Journal of Theoretical Biology*, 250(3):475–483, 2008.

[80] Takafumi Kanazawa, Yasuhiko Fukumoto, Toshimitsu Ushio, and Takurou Misaka. Replicator dynamics with pigovian subsidy and capitation tax. *Nonlinear Analysis: Theory, Methods & Applications*, 71(12):e818–e826, 2009.

[81] Prabhakaran Kasinathan and Jorge Cuellar. Workflow-aware security of integrated mobility services. In *Computer Security: 23rd European Symposium on Research in Computer Security, ESORICS 2018, Barcelona, Spain, September 3-7, 2018, Proceedings, Part II 23*, pages 3–19. Springer, 2018.

[82] Basel Katt, Xinwen Zhang, Ruth Breu, Michael Hafner, and Jean-Pierre Seifert. A general obligation model and continuity: enhanced policy enforcement engine for usage control. In *Proceedings of the 13th ACM symposium on Access control models and technologies*, pages 123–132, 2008.

[83] Alan Kazdin. The token economy: A review and evaluation. 2012.

[84] Florian Kelbert and Alexander Pretschner. Data usage control enforcement in distributed systems. In *Proceedings of the third ACM conference on Data and application security and privacy*, pages 71–82, 2013.

[85] Ashraf Khalil, Hassan Hajjdiab, and Nabeel Al-Qirim. Detecting fake followers in twitter: A machine learning approach. *International Journal of Machine Learning and Computing*, 7(6):198–202, 2017.

[86] Zeshan Aslam Khan, Edison Pignaton de Freitas, Tony Larsson, and Haider Abbas. A multi-agent model for fire detection in coal mines using wireless sensor networks. In *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pages 1754–1761. IEEE, 2013.

[87] Hasan Ali Khattak, Munam Ali Shah, Sangeen Khan, Ihsan Ali, and Muhammad Imran. Perception layer security in internet of things. *Future Generation Computer Systems*, 100:144–164, 2019.

[88] Ravi Chandra Koirala, Keshav Dahal, and Santiago Matalonga. Supply chain using smart contract: A blockchain enabled model with traceability and ownership management. In *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, pages 538–544. IEEE, 2019.

[89] Dimosthenis Kyriazis, Ofer Biran, Thanassis Bouras, Klaus Brisch, Armend Duzha, Rafael del Hoyo, Athanasios Kiourtis, Pavlos Kranas, Ilias Maglogiannis, George Manias, et al. Policycloud: analytics as a service facilitating efficient data-driven public policy management. In *Artificial Intelligence Applications and Innovations*, pages 141–150, Cham, 2020. Springer International Publishing.

[90] Hsuan-Wei Lee, Colin Cleveland, and Attila Szolnoki. Mercenary punishment in structured populations. *Applied Mathematics and Computation*, 417:126797, 2022.

[91] Joung-Hun Lee, Yoh Iwasa, Ulf Dieckmann, and Karl Sigmund. Social evolution leads to persistent corruption. *Proceedings of the National Academy of Sciences*,

116(27):13276–13281, 2019.

[92] Joung-Hun Lee, Marko Jusup, and Yoh Iwasa. Games of corruption in preventing the overuse of common-pool resources. *Journal of Theoretical Biology*, 428:76–86, 2017.

[93] Joung-Hun Lee, Karl Sigmund, Ulf Dieckmann, and Yoh Iwasa. Games of corruption: How to suppress illegal logging. *Journal of Theoretical Biology*, 367:1–13, 2015.

[94] Florin Leon. Design and evaluation of a multiagent interaction protocol generating behaviours with different levels of complexity. *Neurocomputing*, 146:173–186, 2014.

[95] Jingjing Li, Qiangqiang Shen, and Wencan Gao. Characterization of group behavior of corruption in construction projects based on contagion mechanism. *Computational intelligence and neuroscience*, 2022:8456197, 2022.

[96] Juan Li, Yi Liu, Zhen Wang, and Haoxiang Xia. Egoistic punishment outcompetes altruistic punishment in the spatial public goods game. *Scientific reports*, 11(1):1–13, 2021.

[97] Ruinian Li, Tianyi Song, Bo Mei, Hong Li, Xiuzhen Cheng, and Limin Sun. Blockchain for large-scale internet of things data storage and protection. *IEEE Transactions on Services Computing*, 12(5):762–771, 2018.

[98] Shi-Yi Lin, Lei Zhang, Jing Li, Li-li Ji, and Yue Sun. A survey of application research based on blockchain smart contract. *Wireless Networks*, 28(2):635–690, 2022.

[99] Linjie Liu and Xiaojie Chen. The evolution of cooperation and reward in a corrupt environment. *IFAC-PapersOnLine*, 53(2):16938–16945, 2020.

[100] Linjie Liu and Xiaojie Chen. Evolutionary dynamics of cooperation in a corrupt society with anti-corruption control. *International Journal of Bifurcation and Chaos*, 31(03):2150039, 2021.

[101] Linjie Liu and Xiaojie Chen. Effects of interconnections among corruption, institutional punishment, and economic factors on the evolution of cooperation. *Applied Mathematics and Computation*, 425:127069, 2022.

[102] Linjie Liu, Xiaojie Chen, and Attila Szolnoki. Evolutionary dynamics of cooperation in a population with probabilistic corrupt enforcers and violators. *Mathematical Models and Methods in Applied Sciences*, 29(11):2127–2149, 2019.

[103] Orlenys López-Pintado, Luciano García-Bañuelos, Marlon Dumas, and Ingo Weber. Caterpillar: A blockchain-based business process management system. In *Proceedings of the 15th International Conference on Business Process Management*, pages 1–5, 2017.

[104] Dan Lu, F Bauza, D Soriano-Paños, J Gómez-Gardeñes, and LM Floría. Norm violation versus punishment risk in a social model of corruption. *Physical Review E*, 101(2):022306, 2020.

[105] Chongsen Ma, Yun Chen, Wenxi Zhu, and Liang Ou. How to effectively control vertical collusion in bidding for government investment projects-based on fsqca method. *PLoS ONE*, 17(9):1–15, 2022.

[106] Jing Ma and Keith W. Hipel. Exploring social dimensions of municipal solid waste management around the globe – a systematic literature review. *Waste Management*, 56:3–12, 2016.

[107] Ricardo Malagueño, Chad Albrecht, Christopher Ainge, and Nate Stephens. Accounting and corruption: a cross-country analysis. *Journal of Money Laundering Control*, 13(4):372–393, 2010.

[108] Laura Mieth, Axel Buchner, and Raoul Bell. Moral labels increase cooperation and costly punishment in a prisoner's dilemma game with punishment option. *Scientific reports*, 11(1):1–13, 2021.

[109] Andres Munoz-Arcentales, Sonsoles López-Pernas, Alejandro Pozo, Álvaro Alonso, Joaquín Salvachúa, and Gabriel Huecas. An architecture for providing data usage and access control in data sharing ecosystems. *Procedia Computer Science*, 160:590–597, 2019.

[110] Michael Muthukrishna, Patrick Francois, Shayan Pourahmadi, and Joseph Henrich. Corrupting cooperation and how anti-corruption strategies may backfire. *Nature Human Behaviour*, 1(7):1–5, 2017.

[111] Mitsuhiro Nakamura. Rare third-party punishment promotes cooperation in risk-averse social learning dynamics. *Frontiers in Physics*, 6:156, 2019.

[112] John Nash. Non-cooperative games. *Annals of mathematics*, pages 286–295, 1951.

[113] Tetsushi Ohdaira. Cooperation evolves by the payoff-difference-based probabilistic reward. *The European Physical Journal B*, 94(11):1–8, 2021.

[114] Yohsuke Ohtsubo, Fumiko Masuda, Esuka Watanabe, and Ayumi Masuchi. Dishonesty invites costly third-party punishment. *Evolution and Human Behavior*, 31(4):259–264, 2010.

[115] Isamu Okada. A review of theoretical studies on indirect reciprocity. *Games*, 11(3):27, 2020.

[116] Inah Omoronyia. Reasoning with imprecise privacy preferences. In *Proceedings of the 2016 24th ACM SIGSOFT International Symposium on Foundations of Software Engineering*, FSE 2016, page 952–955, New York, NY, USA, 2016. Association for Computing Machinery.

[117] Jaehong Park and Ravi Sandhu. The uconabc usage control model. *ACM Transactions on Information and System Security (TISSEC)*, 7(1):128–174, 2004.

[118] Thomas FJ-M Pasquier and David Eyers. Information flow audit for transparency and compliance in the handling of personal data. In *2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW)*, pages 112–117. IEEE, 2016.

[119] Huayan Pei, Guanghui Yan, and Huanmin Wang. Reciprocal rewards promote the evolution of cooperation in spatial prisoner's dilemma game. *Physics Letters A*, 390:127108, 2021.

[120] Matjaž Perc. Sustainable institutionalized punishment requires elimination of second-order free-riders. *Scientific reports*, 2(1):1–6, 2012.

[121] Matjaž Perc, Jillian J Jordan, David G Rand, Zhen Wang, Stefano Boccaletti, and Attila Szolnoki. Statistical physics of human cooperation. *Physics Reports*, 687:1–51, 2017.

[122] CA Petri. Kommunikation mit automaten (phd thesis). *Institut für Instrumentelle Mathematik, Bonn, Germany*, 1962.

[123] A Mitchell Polinsky and Steven Shavell. The economic theory of public enforcement of law. *Journal of economic literature*, 38(1):45–76, 2000.

[124] Tahmid Hasan Pranto, Abdulla All Noman, Atik Mahmud, and AKM Bahalul Haque. Blockchain and smart contract for iot enabled smart agriculture. *PeerJ Computer Science*, 7:e407, 2021.

[125] Alexander Pretschner, Manuel Hilty, Florian Schütz, Christian Schaefer, and Thomas Walter. Usage control enforcement: Present and future. *IEEE Security & Privacy*, 6(4):44–53, 2008.

[126] Wojtek Przepiorka and Andreas Diekmann. Individual heterogeneity and costly punishment: a volunteer's dilemma. *Proceedings of the Royal Society B: Biological Sciences*, 280(1759):20130247, 2013.

[127] Meixun Qu, Xin Huang, Xu Chen, Yi Wang, Xiaofeng Ma, and Dawei Liu. Formal verification of smart contracts from the perspective of concurrency. In *Smart Blockchain: First International Conference, SmartBlock 2018, Tokyo, Japan, December 10–12, 2018, Proceedings 1*, pages 32–43. Springer, 2018.

[128] Ji Quan, Wei Liu, Yuqing Chu, and Xianjia Wang. Stochastic evolutionary voluntary public goods game with punishment in a quasi-birth-and-death process. *Scientific reports*, 7(1):1–14, 2017.

[129] Daniela Rabellino, Rosalba Morese, Angela Ciaramidaro, Bruno G Bara, and Francesca M Bosco. Third-party punishment: altruistic and anti-social behaviours in in-group and out-group settings. *Journal of Cognitive Psychology*, 28(4):486–495, 2016.

[130] Kaushik Ragothaman, Yong Wang, Bhaskar Rimal, and Mark Lawrence. Access control for iot: A survey of existing research, dynamic policies and future directions. *Sensors*, 23(4):1805, 2023.

[131] Mohammad Saidur Rahman, Ibrahim Khalil, and Mohammed Atiquzzaman. Blockchain-powered policy enforcement for ensuring flight compliance in drone-based service systems. *IEEE Network*, 35(1):116–123, 2021.

[132] Carlos P Roca, José A Cuesta, and Angel Sánchez. Evolutionary game theory: Temporal and spatial effects beyond replicator dynamics. *Physics of life reviews*, 6(4):208–249, 2009.

[133] Christian Rondanini, Barbara Carminati, Federico Daidone, and Elena Ferrari. Blockchain-based controlled information sharing in inter-organizational workflows. In *2020 IEEE International Conference on Services Computing (SCC)*, pages 378–385. IEEE, 2020.

[134] Babak Darvish Rouhani, Mohd Naz'ri Mahrin, Fatemeh Nikpay, Rodina Binti Ahmad, and Pourya Nikfard. A systematic literature review on enterprise architecture implementation methodologies. *information and Software Technology*, 62:1–20, 2015.

[135] Stavros Salonikias, Marie Khair, Theodoros Mastoras, and Ioannis Mavridis. Blockchain-based access control in a globalized healthcare provisioning ecosystem. *Electronics*, 11(17):2652, 2022.

[136] William H Sandholm. Local stability under evolutionary game dynamics. *Theoretical Economics*, 5(1):27–50, 2010.

[137] Fernando P Santos, Simon A Levin, and Vítor V Vasconcelos. Biased perceptions explain collective action deadlocks and suggest new mechanisms to prompt cooperation. *Iscience*, 24(4), 2021.

[138] Tatsuya Sasaki and Satoshi Uchida. Rewards and the evolution of cooperation in public good games. *Biology letters*, 10(1):20130903, 2014.

[139] Fabian Schär. Decentralized finance: On blockchain-and smart contract-based financial markets. *Fed. Reserve Bank of St. Louis Review*, 103(2):153–174, 2021.

[140] Sarah Schoenmakers, Christian Hilbe, Bernd Blasius, and Arne Traulsen. Sanctions as honest signals–the evolution of pool punishment by public sanctioning institutions. *Journal of Theoretical Biology*, 356:36–46, 2014.

[141] Zhenyu Shi, Wei Wei, Baifeng Li, Chao Li, Haibin Li, and Zhiming Zheng. Two-layer network model of public goods games with intervention and corruption. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 32(6):063138, 2022.

[142] Karl Sigmund. *The Calculus of Selfishness*. Princeton University Press, Princeton, 2010.

[143] Karl Sigmund, Christoph Hauert, and Martin A Nowak. Reward and punishment. *Proceedings of the National Academy of Sciences*, 98(19):10757–10762, 2001.

[144] Giovanni Sileno, Alexander Boer, Tom M van Engers, et al. The institutional stance in agent-based simulations. In *Proceedings of the 5th International Conference on Agents and Artificial Intelligence (ICAART)*, pages 255–261, 2013.

[145] Arshdeep Singh, Gulshan Kumar, Rahul Saha, Mauro Conti, Mamoun Alazab, and Reji Thomas. A survey and taxonomy of consensus protocols for blockchains. *Journal of Systems Architecture*, 127:102503, 2022.

[146] Michele Soavi, Nicola Zeni, John Mylopoulos, and Luisa Mich. From legal contracts to formal specifications: a systematic literature review. *SN Computer Science*, 3(5):345, 2022.

[147] Weiwei Sun, Linjie Liu, Xiaojie Chen, Attila Szolnoki, and Vítor V Vasconcelos. Combination of institutional incentives for cooperative governance of risky commons. *Iscience*, 24(8):102844, 2021.

[148] György Szabó and Csaba Tőke. Evolutionary prisoner's dilemma game on a square lattice. *Physical Review E*, 58(1):69, 1998.

[149] Nick Szabo. Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought,(16)*, 18(2):28, 1996.

[150] Attila Szolnoki and Xiaojie Chen. Cooperation and competition between pair

and multi-player social games in spatial populations. *Scientific reports*, 11(1):1–9, 2021.

[151] Attila Szolnoki and Matjaz Perc. Reward and cooperation in the spatial public goods game. *Europhysics Letters*, 92(3):38003, 2010.

[152] Attila Szolnoki, Jeromos Vukov, and György Szabó. Selection of noise level in strategy adoption for spatial social dilemmas. *Physical Review E*, 80(5):056112, 2009.

[153] Hirofumi Takesue. Evolutionary prisoner's dilemma games on the network with punishment and opportunistic partner switching. *Europhysics Letters*, 121(4):48005, 2018.

[154] Fangfang Tan and Erte Xiao. Third-party punishment: Retribution or deterrence? *Journal of Economic Psychology*, 67:34–46, 2018.

[155] Palina Tolmach, Yi Li, Shang-Wei Lin, Yang Liu, and Zengxiang Li. A survey of smart contract formal specification and verification. *ACM Computing Surveys (CSUR)*, 54(7):1–38, 2021.

[156] Arne Traulsen, Torsten Röhl, and Manfred Milinski. An economic experiment reveals that humans prefer pool punishment to maintain the commons. *Proceedings of the Royal Society B: Biological Sciences*, 279(1743):3716–3721, 2012.

[157] Diana Ürge-Vorsatz, LD Danny Harvey, Sevastianos Mirasgedis, and Mark D Levine. Mitigating co2 emissions from energy use in the world's buildings. *Building Research & Information*, 35(4):379–398, 2007.

[158] Tom van Engers. An owl ontology of fundamental legal concepts. In *Legal Knowledge and Information Systems: JURIX 2006: the Nineteenth Annual Conference. Vol*, volume 152, page 101, 2006.

[159] Prateek Verma, Anjan K Nandi, and Supratim Sengupta. Bribery games on inter-dependent regular networks. *Scientific reports*, 7(1):1–12, 2017.

[160] Prateek Verma, Anjan K Nandi, and Supratim Sengupta. Bribery games on interdependent complex networks. *Journal of Theoretical Biology*, 450:43–52, 2018.

[161] Prateek Verma and Supratim Sengupta. Bribe and punishment: An evolutionary game-theoretic analysis of bribery. *PLoS ONE*, 10(7):e0133441, 2015.

[162] Marx Viana, Paulo Alencar, Donald Cowan, Everton Guimarães, Francisco Cunha, and Carlos Lucena. The development of normative autonomous agents: An approach. In *2015 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT)*, volume 2, pages 9–16, 2015.

[163] Daniel Villatoro, Giulia Andrighetto, Jordi Sabater-Mir, and Rosaria Conte. Dynamic sanctioning for robust and cost-efficient norm compliance. In *Proceedings of the International Joint Conference on Artificial Intelligence*, pages 414–419, 2011.

[164] Wattana Viriyasitavat and Danupol Hoonsopon. Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*, 13:32–39, 2019.

[165] Qiang Wang, Nanrong He, and Xiaojie Chen. Replicator dynamics for public goods game with resource allocation in large populations. *Applied Mathematics and Computation*, 328:162–170, 2018.

[166] Shengxian Wang, Xiaojie Chen, and Attila Szolnoki. Exploring optimal institutional incentives for public cooperation. *Communications in Nonlinear Science and Numerical Simulation*, 79:104914, 2019.

[167] Shengxian Wang, Xiaojie Chen, Zhilong Xiao, and Attila Szolnoki. Decentralized incentives for general well-being in networked public goods game. *Applied Mathematics and Computation*, 431:127308, 2022.

[168] Shengxian Wang, Linjie Liu, and Xiaojie Chen. Tax-based pure punishment and reward in the public goods game. *Physics Letters A*, 386:126965, 2021.

[169] Shengxian Wang, Linjie Liu, and Xiaojie Chen. Incentive strategies for the evolution of cooperation: Analysis and optimization. *Europhysics Letters*,

136(6):68002, 2022.

[170] Xu Wang, Xuan Zha, Wei Ni, Ren Ping Liu, Y Jay Guo, Xinxin Niu, and Kangfeng Zheng. Survey on blockchain for internet of things. *Computer Communications*, 136:10–29, 2019.

[171] Zhen Wang, Cheng-Yi Xia, Sandro Meloni, Chang-Song Zhou, and Yamir Moreno. Impact of social punishment on cooperative behavior in complex networks. *Scientific reports*, 3:3055, 2013.

[172] Lucas Wardil and Jafferson KL da Silva. The evolution of cooperation in mixed games. *Chaos, Solitons & Fractals*, 56:160–165, 2013.

[173] Hiroki Watanabe, Shigeru Fujimura, Atsushi Nakadaira, Yasuhiko Miyazaki, Akihito Akutsu, and Jay Kishigami. Blockchain contract: Securing a blockchain applied to smart contracts. In *2016 IEEE international conference on consumer electronics (ICCE)*, pages 467–468. IEEE, 2016.

[174] Ingo Weber, Xiwei Xu, Régis Riveret, Guido Governatori, Alexander Ponomarev, and Jan Mendling. Untrusted business process monitoring and execution using blockchain. In *the 14th International Conference on Business Process Management*, pages 329–347, Cham, 2016. Springer.

[175] Binghui Wu, Jing Yang, Guanhao Fu, and Mengjiao Zhang. The strategy selection in financial fraud and audit supervision: A study based on a three-party evolutionary game model. *Systems*, 10(5):173, 2022.

[176] Yu'e Wu, Shuhua Chang, Zhipeng Zhang, and Zhenghong Deng. Impact of social reward on the evolution of the cooperation behavior in complex networks. *Scientific reports*, 7:41076, 2017.

[177] Yu'e Wu, Bin Zhang, and Shuhua Zhang. Probabilistic reward or punishment promotes cooperation in evolutionary games. *Chaos, Solitons & Fractals*, 103:289–293, 2017.

[178] Yunpeng Yang and Weixin Yang. Does whistleblowing work for air pollution control in china? a study based on three-party evolutionary game model under incomplete information. *Sustainability*, 11(2):324, 2019.

[179] Yao Yin. A socio-political analysis of policies and incentives applicable to community wind in oregon. *Energy Policy*, 42:442–449, 2012.

[180] Sherali Zeadally, Ashok Kumar Das, and Nicolas Sklavos. Cryptographic technologies and protocol standards for internet of things. *Internet of Things*, 14:100075, 2021.

[181] Weijun Zeng, Minqiang Li, and Fuzan Chen. Cooperation in the evolutionary iterated prisoner's dilemma game with risk attitude adaptation. *Applied Soft Computing*, 44:238–254, 2016.

[182] Gulnara Zhabelova, Valeriy Vyatkin, and Victor N Dubinin. Toward industrially usable agent technology for smart grid automation. *IEEE Transactions on Industrial Electronics*, 62(4):2629–2641, 2014.

[183] Lu Zhang, Reginald Cushing, Leon Gommans, Cees De Laat, and Paola Grosso. Modeling of collaboration archetypes in digital market places. *IEEE Access*, 7:102689–102700, 2019.

[184] Lu Zhang, Arie Taal, Reginald Cushing, Cees de Laat, and Paola Grosso. A risk-level assessment system based on the stride/dread model for digital data marketplaces. *International Journal of Information Security*, 27:509–525, 2021.

[185] Yan Zheng and Xiaoming Liao. Corruption governance and its dynamic stability based on a three-party evolutionary game with the government, the public, and public officials. *Applied Economics*, 51(49):5411–5419, 2019.

[186] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. IEEE, 2017.

[187] Huan Zhou, Xue Ouyang, Zhijie Ren, Jinshu Su, Cees de Laat, and Zhiming Zhao. A blockchain based witness model for trustworthy cloud service level agreement enforcement. In *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, pages 1567–1575, 2019.

[188] Xiaoyang Zhou, Kexin Chen, Haoyu Wen, Jun Lin, Kai Zhang, Xin Tian, Shouyang Wang, and Benjamin Lev. Integration of third-party platforms: Does it really hurt them? *International Journal of Production Economics*, 234:108003, 2021.

[189] Xin Zhou, Adam Belloum, Michael H Lees, Tom van Engers, and Cees de Laat. Costly incentives design from an institutional perspective: cooperation, sustainability and affluence. *Proceedings of the Royal Society A*, 478(2265):20220393, 2022.

[190] Xin Zhou, Reginald Cushing, Ralph Koning, Adam Belloum, Paola Grosso, Sander Klous, Tom van Engers, and Cees de Laat. Policy enforcement for secure and trustworthy data sharing in multi-domain infrastructures. In *2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE)*, pages 104–113. IEEE, 2020.

[191] Guang Zhu, Hu Liu, and Mining Feng. Sustainability of information security investment in online social networks: an evolutionary game-theoretic approach. *Mathematics*, 6(10):177, 2018.

[192] Nejc Zupan, Prabhakaran Kasinathan, Jorge Cuellar, and Markus Sauer. Secure smart contract generation based on petri nets. In *Blockchain Technology for Industry 4.0: Secure, Decentralized, Distributed and Trusted Industry Environment*, pages 73–98. Springer, 2020.

SIKS Dissertations

2016

01 Syed Saiden Abbas (RUN), Recognition of Shapes by Humans and Machines
02 Michiel Christiaan Meulendijk (UU), Optimizing medication reviews through decision support: prescribing a better pill to swallow
03 Maya Sappelli (RUN), Knowledge Work in Context: User Centered Knowledge Worker Support
04 Laurens Rietveld (VUA), Publishing and Consuming Linked Data
05 Evgeny Sherkhonov (UvA), Expanded Acyclic Queries: Containment and an Application in Explaining Missing Answers
06 Michel Wilson (TUD), Robust scheduling in an uncertain environment
07 Jeroen de Man (VUA), Measuring and modeling negative emotions for virtual training
08 Matje van de Camp (TiU), A Link to the Past: Constructing Historical Social Networks from Unstructured Data
09 Archana Nottamkandath (VUA), Trusting Crowdsourced Information on Cultural Artefacts
10 George Karafotias (VUA), Parameter Control for Evolutionary Algorithms
11 Anne Schuth (UvA), Search Engines that Learn from Their Users
12 Max Knobbout (UU), Logics for Modelling and Verifying Normative Multi-Agent Systems
13 Nana Baah Gyan (VUA), The Web, Speech Technologies and Rural Development in West Africa - An ICT4D Approach
14 Ravi Khadka (UU), Revisiting Legacy Software System Modernization
15 Steffen Michels (RUN), Hybrid Probabilistic Logics - Theoretical Aspects, Algorithms and Experiments
16 Guangliang Li (UvA), Socially Intelligent Autonomous Agents that Learn from Human Reward
17 Berend Weel (VUA), Towards Embodied Evolution of Robot Organisms
18 Albert Meroño Peñuela (VUA), Refining Statistical Data on the Web
19 Julia Efremova (TU/e), Mining Social Structures from Genealogical Data
20 Daan Odijk (UvA), Context & Semantics in News & Web Search
21 Alejandro Moreno Célleri (UT), From Traditional to Interactive Playspaces: Automatic Analysis of Player Behavior in the Interactive Tag Playground
22 Grace Lewis (VUA), Software Architecture Strategies for Cyber-Foraging Systems
23 Fei Cai (UvA), Query Auto Completion in Information Retrieval
24 Brend Wanders (UT), Repurposing and Probabilistic Integration of Data; An Iterative and data model independent approach
25 Julia Kiseleva (TU/e), Using Contextual Information to Understand Searching and Browsing Behavior

26 Dilhan Thilakarathne (VUA), In or Out of Control: Exploring Computational Models to Study the Role of Human Awareness and Control in Behavioural Choices, with Applications in Aviation and Energy Management Domains
27 Wen Li (TUD), Understanding Geo-spatial Information on Social Media
28 Mingxin Zhang (TUD), Large-scale Agent-based Social Simulation - A study on epidemic prediction and control
29 Nicolas Höning (TUD), Peak reduction in decentralised electricity systems - Markets and prices for flexible planning
30 Ruud Mattheij (TiU), The Eyes Have It
31 Mohammad Khelghati (UT), Deep web content monitoring
32 Eelco Vriezekolk (UT), Assessing Telecommunication Service Availability Risks for Crisis Organisations
33 Peter Bloem (UvA), Single Sample Statistics, exercises in learning from just one example
34 Dennis Schunselaar (TU/e), Configurable Process Trees: Elicitation, Analysis, and Enactment
35 Zhaochun Ren (UvA), Monitoring Social Media: Summarization, Classification and Recommendation
36 Daphne Karreman (UT), Beyond R2D2: The design of nonverbal interaction behavior optimized for robot-specific morphologies
37 Giovanni Sileno (UvA), Aligning Law and Action - a conceptual and computational inquiry
38 Andrea Minuto (UT), Materials that Matter - Smart Materials meet Art & Interaction Design
39 Merijn Bruijnes (UT), Believable Suspect Agents; Response and Interpersonal Style Selection for an Artificial Suspect
40 Christian Detweiler (TUD), Accounting for Values in Design
41 Thomas King (TUD), Governing Governance: A Formal Framework for Analysing Institutional Design and Enactment Governance
42 Spyros Martzoukos (UvA), Combinatorial and Compositional Aspects of Bilingual Aligned Corpora
43 Saskia Koldijk (RUN), Context-Aware Support for Stress Self-Management: From Theory to Practice
44 Thibault Sellam (UvA), Automatic Assistants for Database Exploration
45 Bram van de Laar (UT), Experiencing Brain-Computer Interface Control
46 Jorge Gallego Perez (UT), Robots to Make you Happy
47 Christina Weber (UL), Real-time foresight - Preparedness for dynamic innovation networks
48 Tanja Buttler (TUD), Collecting Lessons Learned
49 Gleb Polevoy (TUD), Participation and Interaction in Projects. A Game-Theoretic Analysis
50 Yan Wang (TiU), The Bridge of Dreams: Towards a Method for Operational Performance Alignment in IT-enabled Service Supply Chains

2017

01 Jan-Jaap Oerlemans (UL), Investigating Cybercrime
02 Sjoerd Timmer (UU), Designing and Understanding Forensic Bayesian Networks using Argumentation
03 Daniël Harold Telgen (UU), Grid Manufacturing; A Cyber-Physical Approach with Autonomous Products and Reconfigurable Manufacturing Machines
04 Mrunal Gawade (CWI), Multi-core Parallelism in a Column-store
05 Mahdieh Shadi (UvA), Collaboration Behavior
06 Damir Vandic (EUR), Intelligent Information Systems for Web Product Search
07 Roel Bertens (UU), Insight in Information: from Abstract to Anomaly
08 Rob Konijn (VUA), Detecting Interesting Differences:Data Mining in Health Insurance Data using Outlier Detection and Subgroup Discovery

09 Dong Nguyen (UT), Text as Social and Cultural Data: A Computational Perspective on Variation in Text
10 Robby van Delden (UT), (Steering) Interactive Play Behavior
11 Florian Kunneman (RUN), Modelling patterns of time and emotion in Twitter #anticipointment
12 Sander Leemans (TU/e), Robust Process Mining with Guarantees
13 Gijs Huisman (UT), Social Touch Technology - Extending the reach of social touch through haptic technology
14 Shoshannah Tekofsky (TiU), You Are Who You Play You Are: Modelling Player Traits from Video Game Behavior
15 Peter Berck (RUN), Memory-Based Text Correction
16 Aleksandr Chuklin (UvA), Understanding and Modeling Users of Modern Search Engines
17 Daniel Dimov (UL), Crowdsourced Online Dispute Resolution
18 Ridho Reinanda (UvA), Entity Associations for Search
19 Jeroen Vuurens (UT), Proximity of Terms, Texts and Semantic Vectors in Information Retrieval
20 Mohammadbashir Sedighi (TUD), Fostering Engagement in Knowledge Sharing: The Role of Perceived Benefits, Costs and Visibility
21 Jeroen Linssen (UT), Meta Matters in Interactive Storytelling and Serious Gaming (A Play on Worlds)
22 Sara Magliacane (VUA), Logics for causal inference under uncertainty
23 David Graus (UvA), Entities of Interest — Discovery in Digital Traces
24 Chang Wang (TUD), Use of Affordances for Efficient Robot Learning
25 Veruska Zamborlini (VUA), Knowledge Representation for Clinical Guidelines, with applications to Multimorbidity Analysis and Literature Search
26 Merel Jung (UT), Socially intelligent robots that understand and respond to human touch
27 Michiel Joosse (UT), Investigating Positioning and Gaze Behaviors of Social Robots: People's Preferences, Perceptions and Behaviors
28 John Klein (VUA), Architecture Practices for Complex Contexts
29 Adel Alhuraibi (TiU), From IT-BusinessStrategic Alignment to Performance: A Moderated Mediation Model of Social Innovation, and Enterprise Governance of IT
30 Wilma Latuny (TiU), The Power of Facial Expressions
31 Ben Ruijl (UL), Advances in computational methods for QFT calculations
32 Thaer Samar (RUN), Access to and Retrievability of Content in Web Archives
33 Brigit van Loggem (OU), Towards a Design Rationale for Software Documentation: A Model of Computer-Mediated Activity
34 Maren Scheffel (OU), The Evaluation Framework for Learning Analytics
35 Martine de Vos (VUA), Interpreting natural science spreadsheets
36 Yuanhao Guo (UL), Shape Analysis for Phenotype Characterisation from High-throughput Imaging
37 Alejandro Montes Garcia (TU/e), WiBAF: A Within Browser Adaptation Framework that Enables Control over Privacy
38 Alex Kayal (TUD), Normative Social Applications
39 Sara Ahmadi (RUN), Exploiting properties of the human auditory system and compressive sensing methods to increase noise robustness in ASR
40 Altaf Hussain Abro (VUA), Steer your Mind: Computational Exploration of Human Control in Relation to Emotions, Desires and Social Support For applications in human-aware support systems
41 Adnan Manzoor (VUA), Minding a Healthy Lifestyle: An Exploration of Mental Processes and a Smart Environment to Provide Support for a Healthy Lifestyle
42 Elena Sokolova (RUN), Causal discovery from mixed and missing data with applications on ADHD datasets
43 Maaike de Boer (RUN), Semantic Mapping in Video Retrieval

44 Garm Lucassen (UU), Understanding User Stories - Computational Linguistics in Agile Requirements Engineering
45 Bas Testerink (UU), Decentralized Runtime Norm Enforcement
46 Jan Schneider (OU), Sensor-based Learning Support
47 Jie Yang (TUD), Crowd Knowledge Creation Acceleration
48 Angel Suarez (OU), Collaborative inquiry-based learning

2018

01 Han van der Aa (VUA), Comparing and Aligning Process Representations
02 Felix Mannhardt (TU/e), Multi-perspective Process Mining
03 Steven Bosems (UT), Causal Models For Well-Being: Knowledge Modeling, Model-Driven Development of Context-Aware Applications, and Behavior Prediction
04 Jordan Janeiro (TUD), Flexible Coordination Support for Diagnosis Teams in Data-Centric Engineering Tasks
05 Hugo Huurdeman (UvA), Supporting the Complex Dynamics of the Information Seeking Process
06 Dan Ionita (UT), Model-Driven Information Security Risk Assessment of Socio-Technical Systems
07 Jieting Luo (UU), A formal account of opportunism in multi-agent systems
08 Rick Smetsers (RUN), Advances in Model Learning for Software Systems
09 Xu Xie (TUD), Data Assimilation in Discrete Event Simulations
10 Julienka Mollee (VUA), Moving forward: supporting physical activity behavior change through intelligent technology
11 Mahdi Sargolzaei (UvA), Enabling Framework for Service-oriented Collaborative Networks
12 Xixi Lu (TU/e), Using behavioral context in process mining
13 Seyed Amin Tabatabaei (VUA), Computing a Sustainable Future
14 Bart Joosten (TiU), Detecting Social Signals with Spatiotemporal Gabor Filters
15 Naser Davarzani (UM), Biomarker discovery in heart failure
16 Jaebok Kim (UT), Automatic recognition of engagement and emotion in a group of children
17 Jianpeng Zhang (TU/e), On Graph Sample Clustering
18 Henriette Nakad (UL), De Notaris en Private Rechtspraak
19 Minh Duc Pham (VUA), Emergent relational schemas for RDF
20 Manxia Liu (RUN), Time and Bayesian Networks
21 Aad Slootmaker (OU), EMERGO: a generic platform for authoring and playing scenario-based serious games
22 Eric Fernandes de Mello Araújo (VUA), Contagious: Modeling the Spread of Behaviours, Perceptions and Emotions in Social Networks
23 Kim Schouten (EUR), Semantics-driven Aspect-Based Sentiment Analysis
24 Jered Vroon (UT), Responsive Social Positioning Behaviour for Semi-Autonomous Telepresence Robots
25 Riste Gligorov (VUA), Serious Games in Audio-Visual Collections
26 Roelof Anne Jelle de Vries (UT), Theory-Based and Tailor-Made: Motivational Messages for Behavior Change Technology
27 Maikel Leemans (TU/e), Hierarchical Process Mining for Scalable Software Analysis
28 Christian Willemse (UT), Social Touch Technologies: How they feel and how they make you feel
29 Yu Gu (TiU), Emotion Recognition from Mandarin Speech
30 Wouter Beek (VUA), The “K” in “semantic web” stands for “knowledge”: scaling semantics to the web

2019

01 Rob van Eijk (UL), Web privacy measurement in real-time bidding systems. A graph-based approach to RTB system classification
02 Emmanuelle Beauxis Aussalet (CWI, UU), Statistics and Visualizations for Assessing Class Size Uncertainty
03 Eduardo Gonzalez Lopez de Murillas (TU/e), Process Mining on Databases: Extracting Event Data from Real Life Data Sources
04 Ridho Rahmadi (RUN), Finding stable causal structures from clinical data
05 Sebastiaan van Zelst (TU/e), Process Mining with Streaming Data
06 Chris Dijkshoorn (VUA), Nichesourcing for Improving Access to Linked Cultural Heritage Datasets
07 Soude Fazeli (TUD), Recommender Systems in Social Learning Platforms
08 Frits de Nijs (TUD), Resource-constrained Multi-agent Markov Decision Processes
09 Fahimeh Alizadeh Moghaddam (UvA), Self-adaptation for energy efficiency in software systems
10 Qing Chuan Ye (EUR), Multi-objective Optimization Methods for Allocation and Prediction
11 Yue Zhao (TUD), Learning Analytics Technology to Understand Learner Behavioral Engagement in MOOCs
12 Jacqueline Heinerman (VUA), Better Together
13 Guanliang Chen (TUD), MOOC Analytics: Learner Modeling and Content Generation
14 Daniel Davis (TUD), Large-Scale Learning Analytics: Modeling Learner Behavior & Improving Learning Outcomes in Massive Open Online Courses
15 Erwin Walraven (TUD), Planning under Uncertainty in Constrained and Partially Observable Environments
16 Guangming Li (TU/e), Process Mining based on Object-Centric Behavioral Constraint (OCBC) Models
17 Ali Hurriyetoglu (RUN), Extracting actionable information from microtexts
18 Gerard Wagenaar (UU), Artefacts in Agile Team Communication
19 Vincent Koeman (TUD), Tools for Developing Cognitive Agents
20 Chide Groenouwe (UU), Fostering technically augmented human collective intelligence
21 Cong Liu (TU/e), Software Data Analytics: Architectural Model Discovery and Design Pattern Detection
22 Martin van den Berg (VUA),Improving IT Decisions with Enterprise Architecture
23 Qin Liu (TUD), Intelligent Control Systems: Learning, Interpreting, Verification
24 Anca Dumitrache (VUA), Truth in Disagreement - Crowdsourcing Labeled Data for Natural Language Processing
25 Emiel van Miltenburg (VUA), Pragmatic factors in (automatic) image description
26 Prince Singh (UT), An Integration Platform for Synchromodal Transport
27 Alessandra Antonaci (OU), The Gamification Design Process applied to (Massive) Open Online Courses
28 Esther Kuindersma (UL), Cleared for take-off: Game-based learning to prepare airline pilots for critical situations
29 Daniel Formolo (VUA), Using virtual agents for simulation and training of social skills in safety-critical circumstances
30 Vahid Yazdanpanah (UT), Multiagent Industrial Symbiosis Systems
31 Milan Jelisavcic (VUA), Alive and Kicking: Baby Steps in Robotics
32 Chiara Sironi (UM), Monte-Carlo Tree Search for Artificial General Intelligence in Games
33 Anil Yaman (TU/e), Evolution of Biologically Inspired Learning in Artificial Neural Networks

34 Negar Ahmadi (TU/e), EEG Microstate and Functional Brain Network Features for Classification of Epilepsy and PNES
35 Lisa Facey-Shaw (OU), Gamification with digital badges in learning programming
36 Kevin Ackermans (OU), Designing Video-Enhanced Rubrics to Master Complex Skills
37 Jian Fang (TUD), Database Acceleration on FPGAs
38 Akos Kadar (OU), Learning visually grounded and multilingual representations

2020

01 Armon Toubman (UL), Calculated Moves: Generating Air Combat Behaviour
02 Marcos de Paula Bueno (UL), Unraveling Temporal Processes using Probabilistic Graphical Models
03 Mostafa Deghani (UvA), Learning with Imperfect Supervision for Language Understanding
04 Maarten van Gompel (RUN), Context as Linguistic Bridges
05 Yulong Pei (TU/e), On local and global structure mining
06 Preethu Rose Anish (UT), Stimulation Architectural Thinking during Requirements Elicitation - An Approach and Tool Support
07 Wim van der Vegt (OU), Towards a software architecture for reusable game components
08 Ali Mirsoleimani (UL), Structured Parallel Programming for Monte Carlo Tree Search
09 Myriam Traub (UU), Measuring Tool Bias and Improving Data Quality for Digital Humanities Research
10 Alifah Syamsiyah (TU/e), In-database Preprocessing for Process Mining
11 Sepideh Mesbah (TUD), Semantic-Enhanced Training Data Augmentation-Methods for Long-Tail Entity Recognition Models
12 Ward van Breda (VUA), Predictive Modeling in E-Mental Health: Exploring Applicability in Personalised Depression Treatment
13 Marco Virgolin (CWI), Design and Application of Gene-pool Optimal Mixing Evolutionary Algorithms for Genetic Programming
14 Mark Raasveldt (CWI/UL), Integrating Analytics with Relational Databases
15 Konstantinos Georgiadis (OU), Smart CAT: Machine Learning for Configurable Assessments in Serious Games
16 Ilona Wilmont (RUN), Cognitive Aspects of Conceptual Modelling
17 Daniele Di Mitri (OU), The Multimodal Tutor: Adaptive Feedback from Multimodal Experiences
18 Georgios Methenitis (TUD), Agent Interactions & Mechanisms in Markets with Uncertainties: Electricity Markets in Renewable Energy Systems
19 Guido van Capelleveen (UT), Industrial Symbiosis Recommender Systems
20 Albert Hankel (VUA), Embedding Green ICT Maturity in Organisations
21 Karine da Silva Miras de Araujo (VUA), Where is the robot?: Life as it could be
22 Maryam Masoud Khamis (RUN), Understanding complex systems implementation through a modeling approach: the case of e-government in Zanzibar
23 Rianne Conijn (UT), The Keys to Writing: A writing analytics approach to studying writing processes using keystroke logging
24 Lenin da Nóbrega Medeiros (VUA/RUN), How are you feeling, human? Towards emotionally supportive chatbots
25 Xin Du (TU/e), The Uncertainty in Exceptional Model Mining
26 Krzysztof Leszek Sadowski (UU), GAMBIT: Genetic Algorithm for Model-Based mixed-Integer opTimization
27 Ekaterina Muravyeva (TUD), Personal data and informed consent in an educational context

28 Bibeg Limbu (TUD), Multimodal interaction for deliberate practice: Training complex skills with augmented reality
29 Ioan Gabriel Bucur (RUN), Being Bayesian about Causal Inference
30 Bob Zadok Blok (UL), Creatief, Creatiever, Creatiefst
31 Gongjin Lan (VUA), Learning better – From Baby to Better
32 Jason Rhuggenaath (TU/e), Revenue management in online markets: pricing and online advertising
33 Rick Gilsing (TU/e), Supporting service-dominant business model evaluation in the context of business model innovation
34 Anna Bon (UM), Intervention or Collaboration? Redesigning Information and Communication Technologies for Development
35 Siamak Farshidi (UU), Multi-Criteria Decision-Making in Software Production

2021

01 Francisco Xavier Dos Santos Fonseca (TUD), Location-based Games for Social Interaction in Public Space
02 Rijk Mercuur (TUD), Simulating Human Routines: Integrating Social Practice Theory in Agent-Based Models
03 Seyyed Hadi Hashemi (UvA), Modeling Users Interacting with Smart Devices
04 Ioana Jivet (OU), The Dashboard That Loved Me: Designing adaptive learning analytics for self-regulated learning
05 Davide Dell'Anna (UU), Data-Driven Supervision of Autonomous Systems
06 Daniel Davison (UT), "Hey robot, what do you think?" How children learn with a social robot
07 Armel Lefebvre (UU), Research data management for open science
08 Nardie Fanchamps (OU), The Influence of Sense-Reason-Act Programming on Computational Thinking
09 Cristina Zaga (UT), The Design of Robothings. Non-Anthropomorphic and Non-Verbal Robots to Promote Children's Collaboration Through Play
10 Quinten Meertens (UvA), Misclassification Bias in Statistical Learning
11 Anne van Rossum (UL), Nonparametric Bayesian Methods in Robotic Vision
12 Lei Pi (UL), External Knowledge Absorption in Chinese SMEs
13 Bob R. Schadenberg (UT), Robots for Autistic Children: Understanding and Facilitating Predictability for Engagement in Learning
14 Negin Samaeemofrad (UL), Business Incubators: The Impact of Their Support
15 Onat Ege Adali (TU/e), Transformation of Value Propositions into Resource Re-Configurations through the Business Services Paradigm
16 Esam A. H. Ghaleb (UM), Bimodal emotion recognition from audio-visual cues
17 Dario Dotti (UM), Human Behavior Understanding from motion and bodily cues using deep neural networks
18 Remi Wieten (UU), Bridging the Gap Between Informal Sense-Making Tools and Formal Systems - Facilitating the Construction of Bayesian Networks and Argumentation Frameworks
19 Roberto Verdecchia (VUA), Architectural Technical Debt: Identification and Management
20 Masoud Mansoury (TU/e), Understanding and Mitigating Multi-Sided Exposure Bias in Recommender Systems
21 Pedro Thiago Timbó Holanda (CWI), Progressive Indexes
22 Sihang Qiu (TUD), Conversational Crowdsourcing
23 Hugo Manuel Proença (UL), Robust rules for prediction and description
24 Kaijie Zhu (TU/e), On Efficient Temporal Subgraph Query Processing
25 Eoin Martino Grua (VUA), The Future of E-Health is Mobile: Combining AI and Self-Adaptation to Create Adaptive E-Health Mobile Applications
26 Benno Kruit (CWI/VUA), Reading the Grid: Extending Knowledge Bases from Human-readable Tables
27 Jelte van Waterschoot (UT), Personalized and Personal Conversations: Designing Agents Who Want to Connect With You

28 Christoph Selig (UL), Understanding the Heterogeneity of Corporate Entrepreneurship Programs

2022

01 Judith van Stegeren (UT), Flavor text generation for role-playing video games
02 Paulo da Costa (TU/e), Data-driven Prognostics and Logistics Optimisation: A Deep Learning Journey
03 Ali el Hassouni (VUA), A Model A Day Keeps The Doctor Away: Reinforcement Learning For Personalized Healthcare
04 Ünal Aksu (UU), A Cross-Organizational Process Mining Framework
05 Shiwei Liu (TU/e), Sparse Neural Network Training with In-Time Over-Parameterization
06 Reza Refaei Afshar (TU/e), Machine Learning for Ad Publishers in Real Time Bidding
07 Sambit Praharaj (OU), Measuring the Unmeasurable? Towards Automatic Co-located Collaboration Analytics
08 Maikel L. van Eck (TU/e), Process Mining for Smart Product Design
09 Oana Andreea Inel (VUA), Understanding Events: A Diversity-driven Human-Machine Approach
10 Felipe Moraes Gomes (TUD), Examining the Effectiveness of Collaborative Search Engines
11 Mirjam de Haas (UT), Staying engaged in child-robot interaction, a quantitative approach to studying preschoolers' engagement with robots and tasks during second-language tutoring
12 Guanyi Chen (UU), Computational Generation of Chinese Noun Phrases
13 Xander Wilcke (VUA), Machine Learning on Multimodal Knowledge Graphs: Opportunities, Challenges, and Methods for Learning on Real-World Heterogeneous and Spatially-Oriented Knowledge
14 Michiel Overeem (UU), Evolution of Low-Code Platforms
15 Jelmer Jan Koorn (UU), Work in Process: Unearthing Meaning using Process Mining
16 Pieter Gijsbers (TU/e), Systems for AutoML Research
17 Laura van der Lubbe (VUA), Empowering vulnerable people with serious games and gamification
18 Paris Mavromoustakos Blom (TiU), Player Affect Modelling and Video Game Personalisation
19 Bilge Yigit Ozkan (UU), Cybersecurity Maturity Assessment and Standardisation
20 Fakhra Jabeen (VUA), Dark Side of the Digital Media - Computational Analysis of Negative Human Behaviors on Social Media
21 Seethu Mariyam Christopher (UM), Intelligent Toys for Physical and Cognitive Assessments
22 Alexandra Sierra Rativa (TiU), Virtual Character Design and its potential to foster Empathy, Immersion, and Collaboration Skills in Video Games and Virtual Reality Simulations
23 Ilir Kola (TUD), Enabling Social Situation Awareness in Support Agents
24 Samaneh Heidari (UU), Agents with Social Norms and Values - A framework for agent based social simulations with social norms and personal values
25 Anna L.D. Latour (UL), Optimal decision-making under constraints and uncertainty
26 Anne Dirkson (UL), Knowledge Discovery from Patient Forums: Gaining novel medical insights from patient experiences
27 Christos Athanasiadis (UM), Emotion-aware cross-modal domain adaptation in video sequences
28 Onuralp Ulusoy (UU), Privacy in Collaborative Systems
29 Jan Kolkmeier (UT), From Head Transform to Mind Transplant: Social Interactions in Mixed Reality

30 Dean De Leo (CWI), Analysis of Dynamic Graphs on Sparse Arrays
31 Konstantinos Traganos (TU/e), Tackling Complexity in Smart Manufacturing with Advanced Manufacturing Process Management
32 Cezara Pastrav (UU), Social simulation for socio-ecological systems
33 Brinn Hekkelman (CWI/TUD), Fair Mechanisms for Smart Grid Congestion Management
34 Nimat Ullah (VUA), Mind Your Behaviour: Computational Modelling of Emotion & Desire Regulation for Behaviour Change
35 Mike E.U. Ligthart (VUA), Shaping the Child-Robot Relationship: Interaction Design Patterns for a Sustainable Interaction

2023

01 Bojan Simoski (VUA), Untangling the Puzzle of Digital Health Interventions
02 Mariana Rachel Dias da Silva (TiU), Grounded or in flight? What our bodies can tell us about the whereabouts of our thoughts
03 Shabnam Najafian (TUD), User Modeling for Privacy-preserving Explanations in Group Recommendations
04 Gineke Wiggers (UL), The Relevance of Impact: bibliometric-enhanced legal information retrieval
05 Anton Bouter (CWI), Optimal Mixing Evolutionary Algorithms for Large-Scale Real-Valued Optimization, Including Real-World Medical Applications
06 António Pereira Barata (UL), Reliable and Fair Machine Learning for Risk Assessment
07 Tianjin Huang (TU/e), The Roles of Adversarial Examples on Trustworthiness of Deep Learning
08 Lu Yin (TU/e), Knowledge Elicitation using Psychometric Learning
09 Xu Wang (VUA), Scientific Dataset Recommendation with Semantic Techniques
10 Dennis J.N.J. Soemers (UM), Learning State-Action Features for General Game Playing
11 Fawad Taj (VUA), Towards Motivating Machines: Computational Modeling of the Mechanism of Actions for Effective Digital Health Behavior Change Applications
12 Tessel Bogaard (VUA), Using Metadata to Understand Search Behavior in Digital Libraries
13 Injy Sarhan (UU), Open Information Extraction for Knowledge Representation
14 Selma Čaušević (TUD), Energy resilience through self-organization
15 Alvaro Henrique Chaim Correia (TU/e), Insights on Learning Tractable Probabilistic Graphical Models
16 Peter Blomsma (TiU), Building Embodied Conversational Agents: Observations on human nonverbal behaviour as a resource for the development of artificial characters
17 Meike Nauta (UT), Explainable AI and Interpretable Computer Vision – From Oversight to Insight
18 Gustavo Penha (TUD), Designing and Diagnosing Models for Conversational Search and Recommendation
19 George Aalbers (TiU), Digital Traces of the Mind: Using Smartphones to Capture Signals of Well-Being in Individuals
20 Arkadiy Dushatskiy (TUD), Expensive Optimization with Model-Based Evolutionary Algorithms applied to Medical Image Segmentation using Deep Learning
21 Gerrit Jan de Bruin (UL), Network Analysis Methods for Smart Inspection in the Transport Domain
22 Alireza Shojaifar (UU), Volitional Cybersecurity
23 Theo Theunissen (UU), Documentation in Continuous Software Development
24 Agathe Balayn (TUD), Practices Towards Hazardous Failure Diagnosis in Machine Learning

25 Jurian Baas (UU), Entity Resolution on Historical Knowledge Graphs
26 Loek Tonnaer (TU/e), Linearly Symmetry-Based Disentangled Representations and their Out-of-Distribution Behaviour
27 Ghada Sokar (TU/e), Learning Continually Under Changing Data Distributions
28 Floris den Hengst (VUA), Learning to Behave: Reinforcement Learning in Human Contexts
29 Tim Draws (TUD), Understanding Viewpoint Biases in Web Search Results

2024

01 Daphne Miedema (TU/e), On Learning SQL: Disentangling concepts in data systems education
02 Emile van Krieken (VUA), Optimisation in Neurosymbolic Learning Systems
03 Feri Wijayanto (RUN), Automated Model Selection for Rasch and Mediation Analysis
04 Mike Huisman (UL), Understanding Deep Meta-Learning
05 Yiyong Gou (UM), Aerial Robotic Operations: Multi-environment Cooperative Inspection & Construction Crack Autonomous Repair
06 Azqa Nadeem (TUD), Understanding Adversary Behavior via XAI: Leveraging Sequence Clustering to Extract Threat Intelligence
07 Parisa Shayan (TiU), Modeling User Behavior in Learning Management Systems
08 Xin Zhou (UvA), From Empowering to Motivating: Enhancing Policy Enforcement through Process Design and Incentive Implementation

Policy enforcement is crucial in our daily life, from protecting rights to promoting collaborations. In practice, designed processes and institutional incentives are two powerful tools in enforcing policies. Processes empower compliance and prevent non-compliance by technology, while incentives motivate adherence through rewards and punishments.

Given the distinct mechanisms of these two methods, this dissertation addresses policy enforcement from the perspectives of empowerment and motivation in Part I and Part II, respectively.

Part I focuses on designing appropriate processes, including pre-audit, operational execution, and post-audit, to empower and terminate compliant and non-compliant behaviors. It further realizes these processes by blockchain and smart contract technologies.

Part II discusses comprehensive criteria for institutional incentive design and potential corruptions in incentive implementation. It predicts incentive effectiveness through mathematical modeling and simulation experiments.

It is worth mentioning that, although the enforced policies in this dissertation are primarily for data governance, the obtained results can be applied to various scenarios.

From Empowering to Motivating

Enhancing Policy Enforcement through
Process Design and Incentive Implementation

University of Amsterdam
Informatics Institute

Xin Zhou

9 789464 837339