Promoting Cyberspace Governance by Developing Cross-domain Collaboration Framework

Tsinghua University

May 2023

Cyberspace Governance

Framework under UN (social and civil issues, multi-stakeholder)

IGF **UN-GGE** **WSIS** **ITU**

Participators: National Government Department, Research Institutions, Private Sector, Civil Society

Military

Network Security

International law

International Politics

Domain name agency, ISP, Telecom company
Managing network infrastructure
Search engines, Self-media platforms, Video sites
Managing Internet content production
Communication software, Travel services
Providing Internet life service

Cyberspace Governance

Framework under UN (social and civil issues, multi-stakeholder)

IGF

UN-GGE

WSIS

ITU

Laws and Regulations

- Intellectual Property
- Privacy Protection

Economic Society

- Digital Currency
- Digital trade

Civil Security

- Internet Crime
- Cyber Terrorism

Culture Media

- Censorship
- Entertainment

Cyberspace Governance

Framework under Technical Community

ISOC

ICANN

IETF

Internet Resources

- Critical Infrastructure Control
- Name / IP Allocation

Standardization

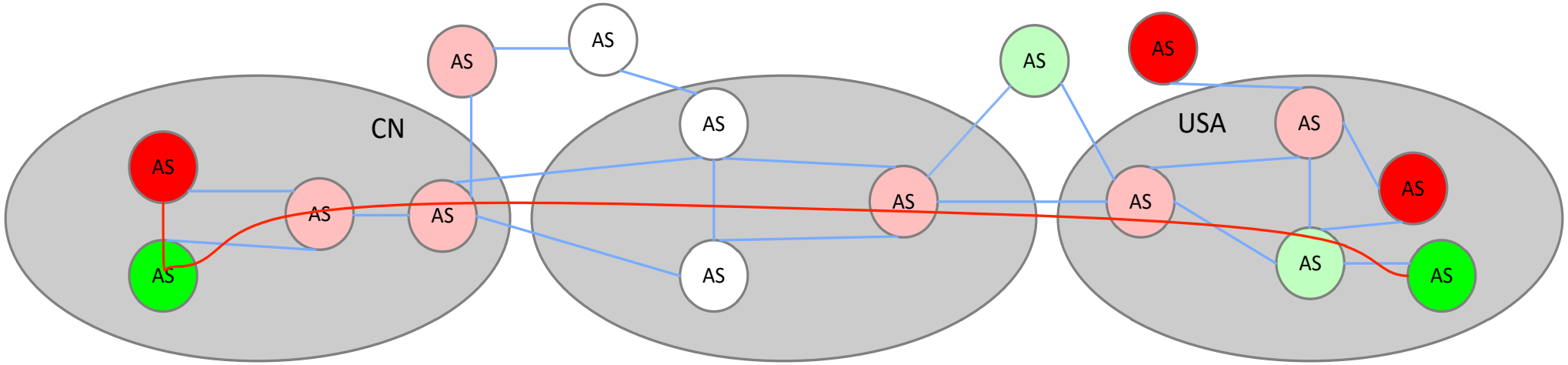
- Networking Protocols

Is it enough for the efficiency, stability and security of the Internet?

Cyberspace Governance: Challenges

Non-technical community produces policy and law, but how to enforce them?

Various Network Security Issues are addressed separately, no platform for all issues.

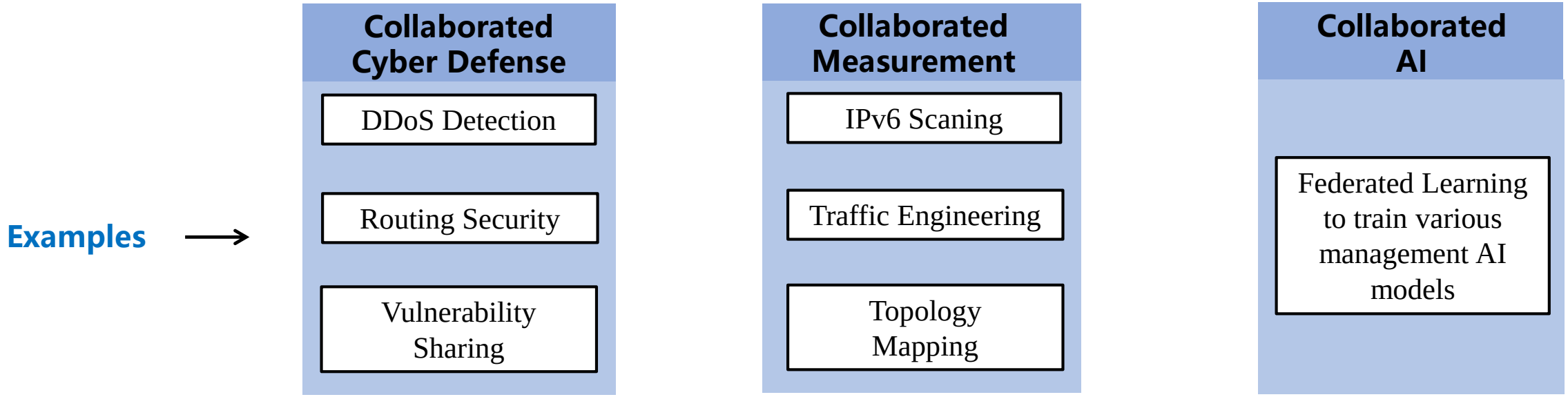


Mutual trust and collaboration between independent governance entities

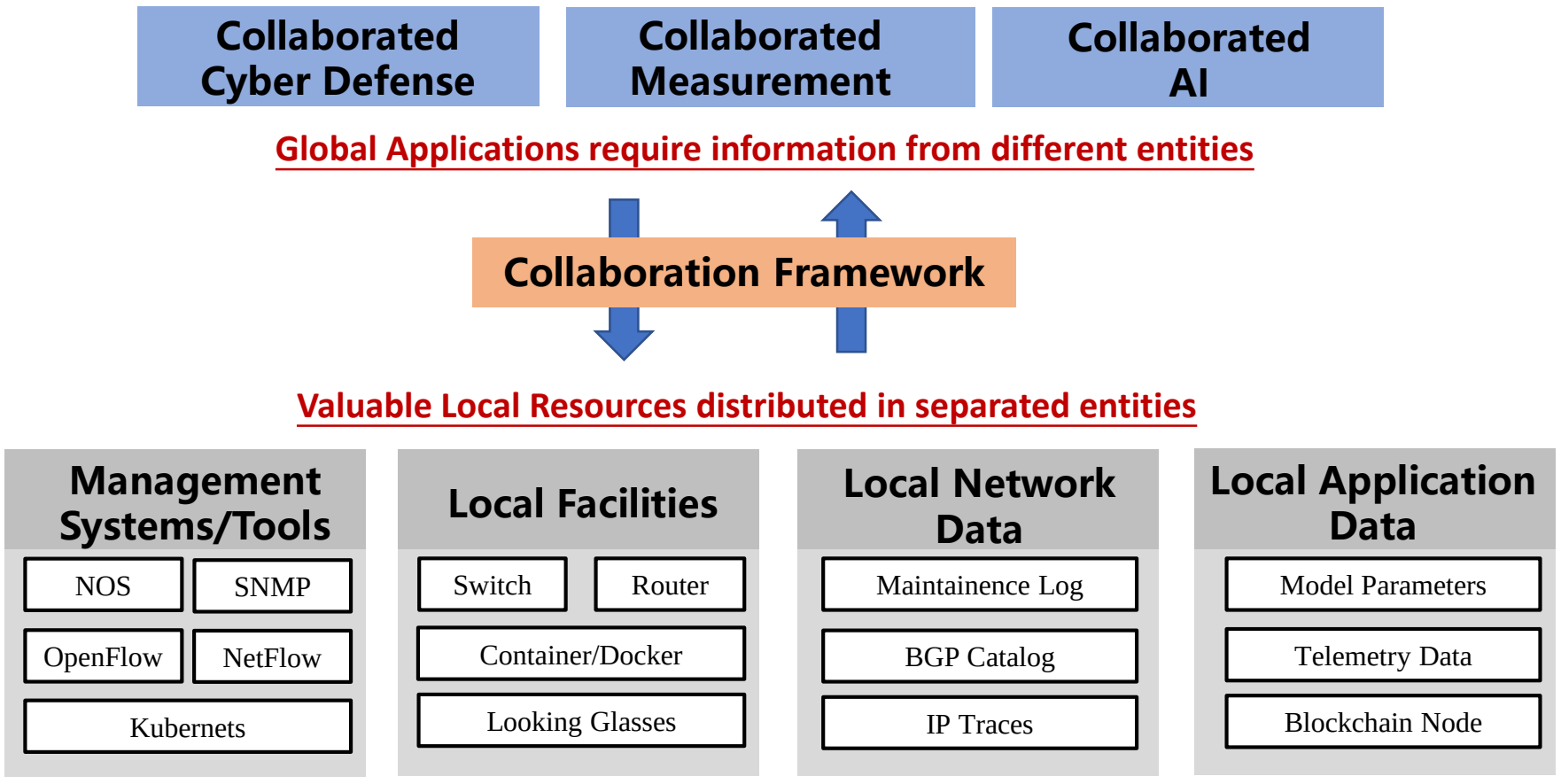
Resolve cyber issues online, real-time, and automatically (according to policy or law).

Collaboration Framework for Technical Issues

Propose an architecture model to help solve the technical challenges of international cyber governance and resolve the conflict between network autonomy and the need for inter-domain governance collaboration.

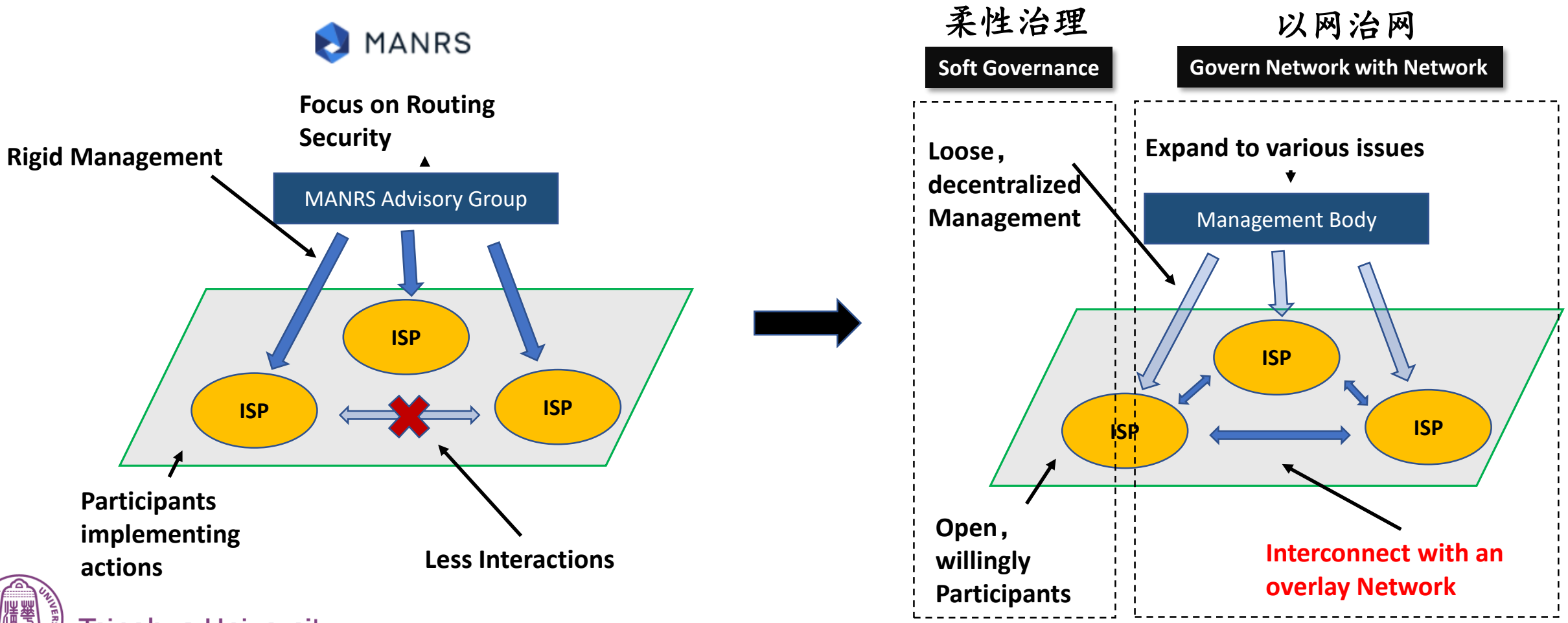


Collaboration Framework for Technical Issues

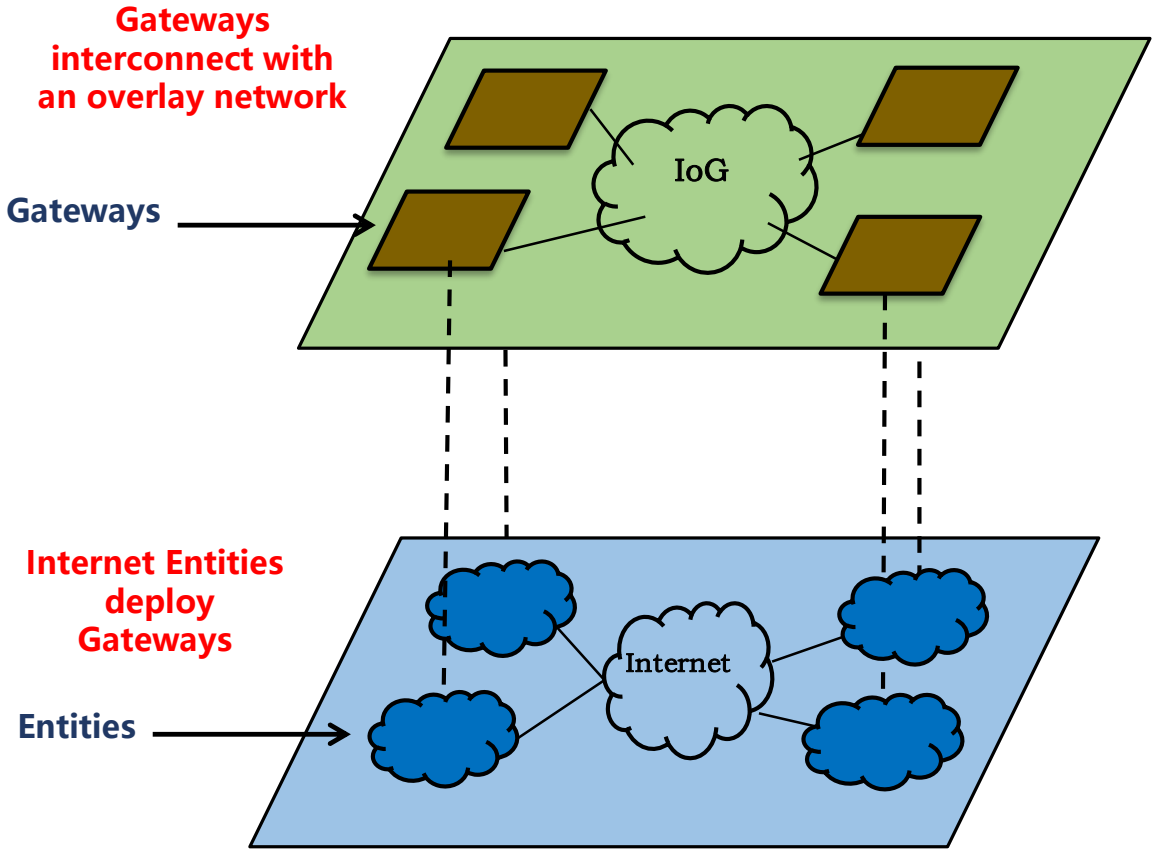


Chief Design Principles

Govern Network with Network; Soft Governance

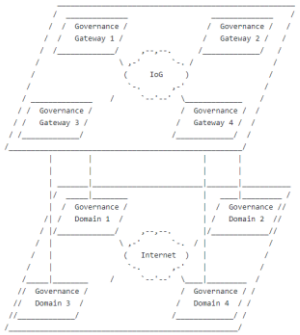


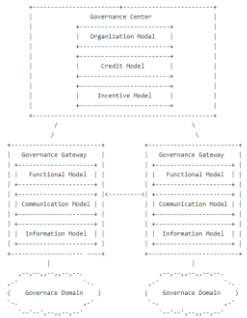
Framework Overview

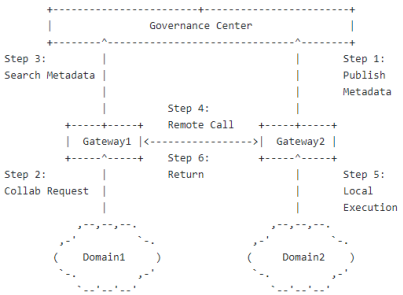


The Internet of Governance (IoG):

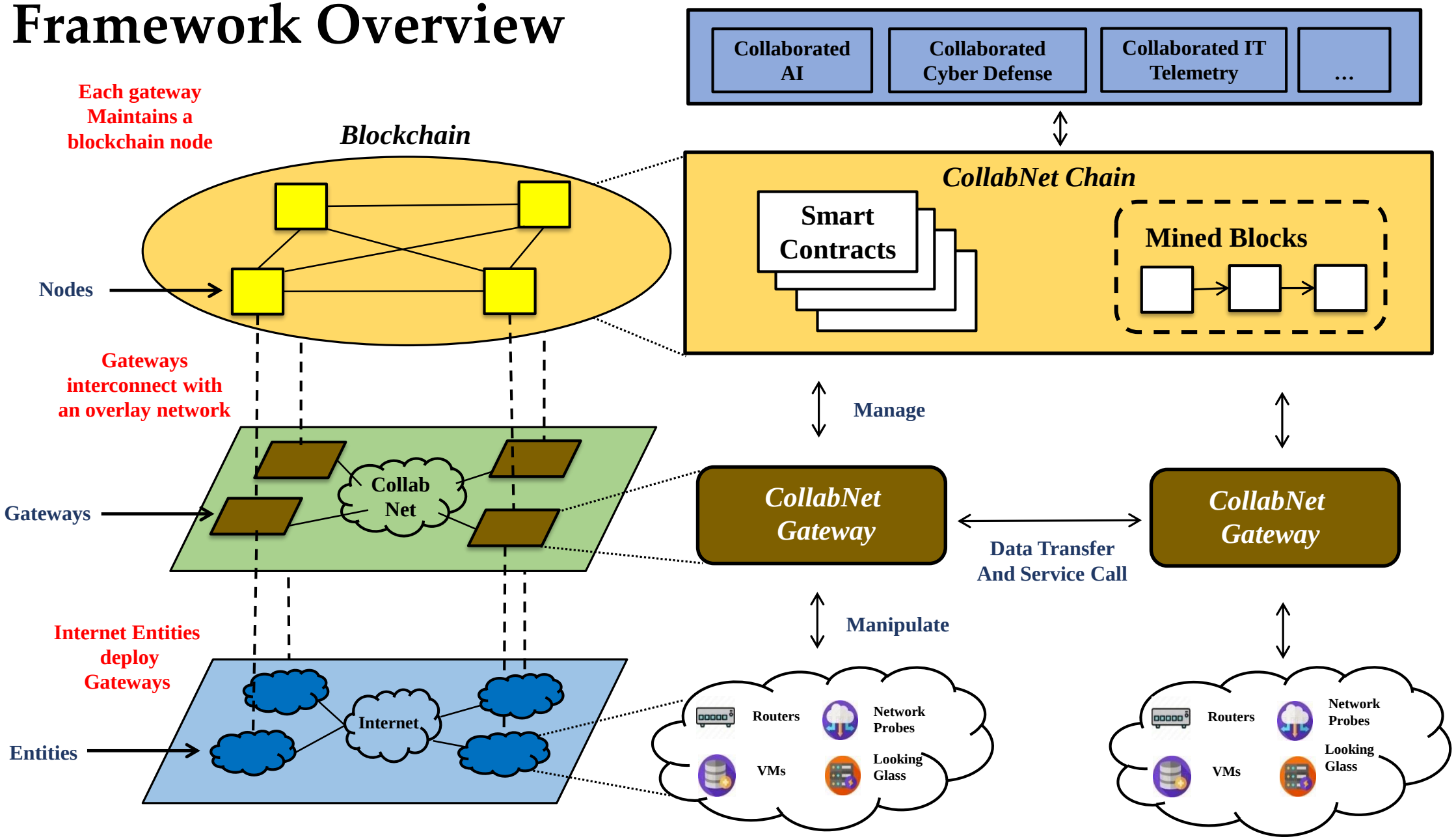
- IoG is an open and interconnected platform that facilitates inter-domain and international collaboration to resolve cyberspace governance issues.
- IoG contains multiple cyberspace governance entities, such as Internet organizations, ISPs and ICPs.
- Detailed in https://datatracker.ietf.org/doc/draft-jilongwang-opsawg-iog/







Framework Overview



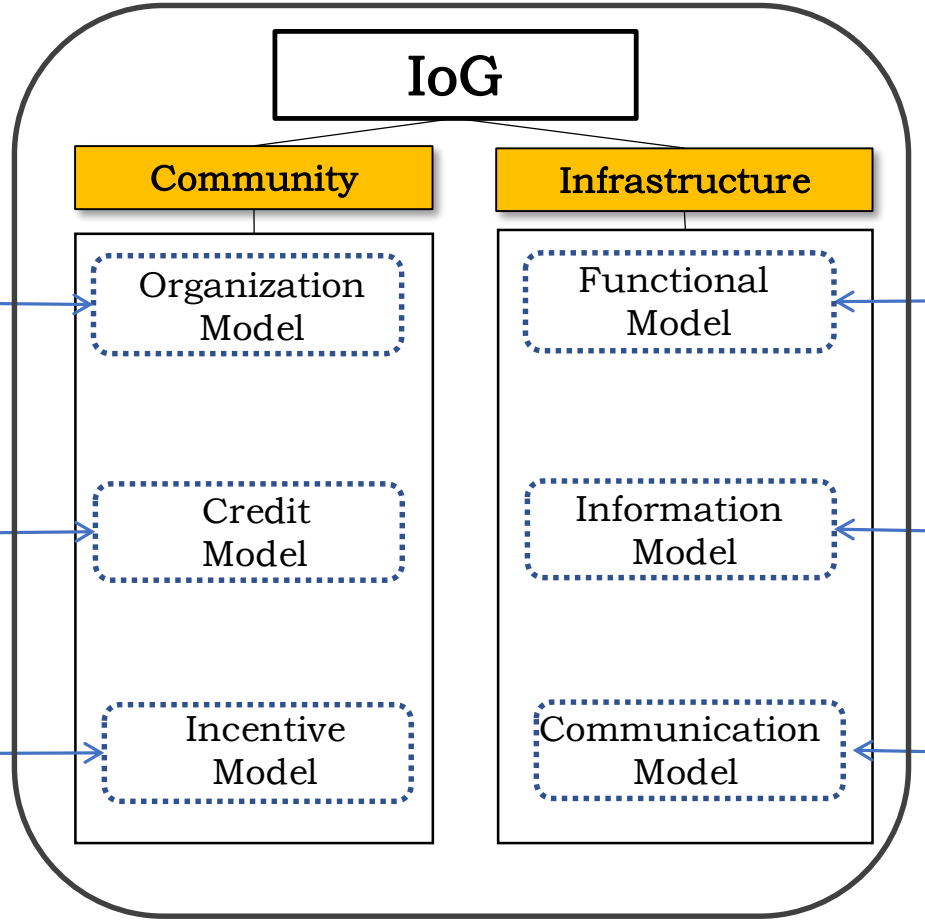
Architectural Model of the Framework

Organizational structure and agenda

defines the organization structure and agenda

defines how to translate participant behaviors and attributes to credits used to evaluate the security and creditability.

defines how to encourage collaboration and how to increase collaboration efficiency and effects



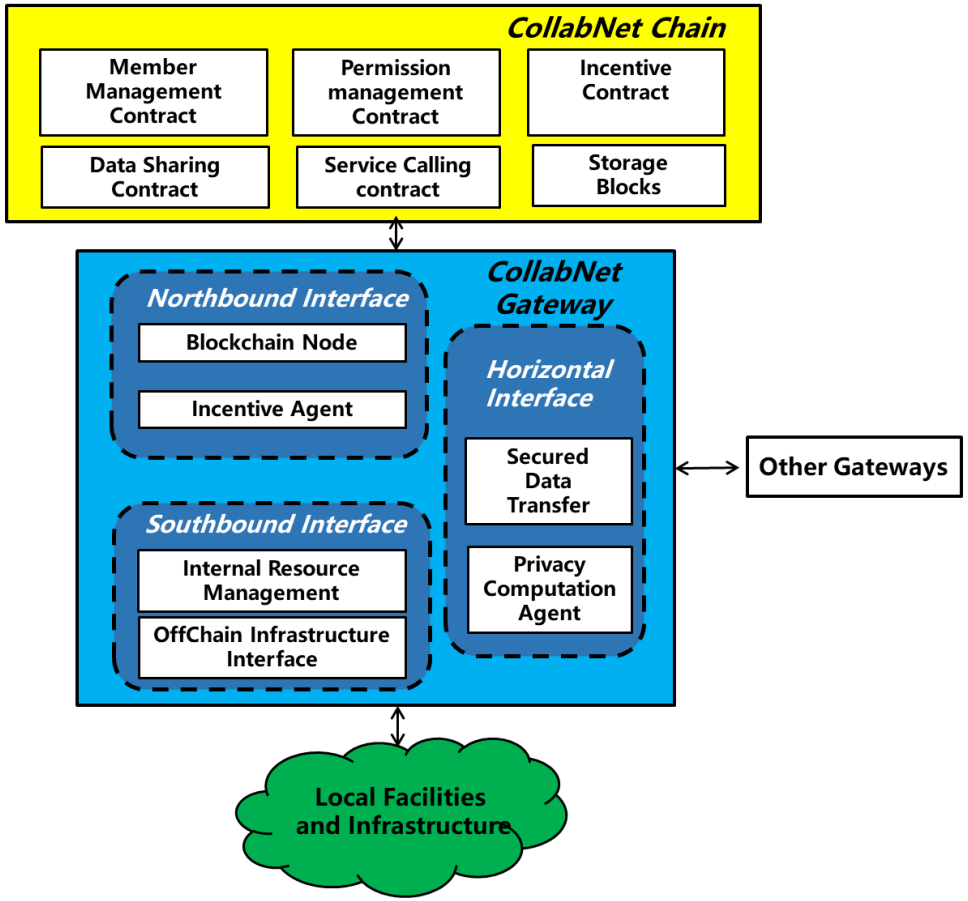
Stream-lined, automated Collaboration Scheme

defines mandatory functionalities that participants need to implement for collaboration

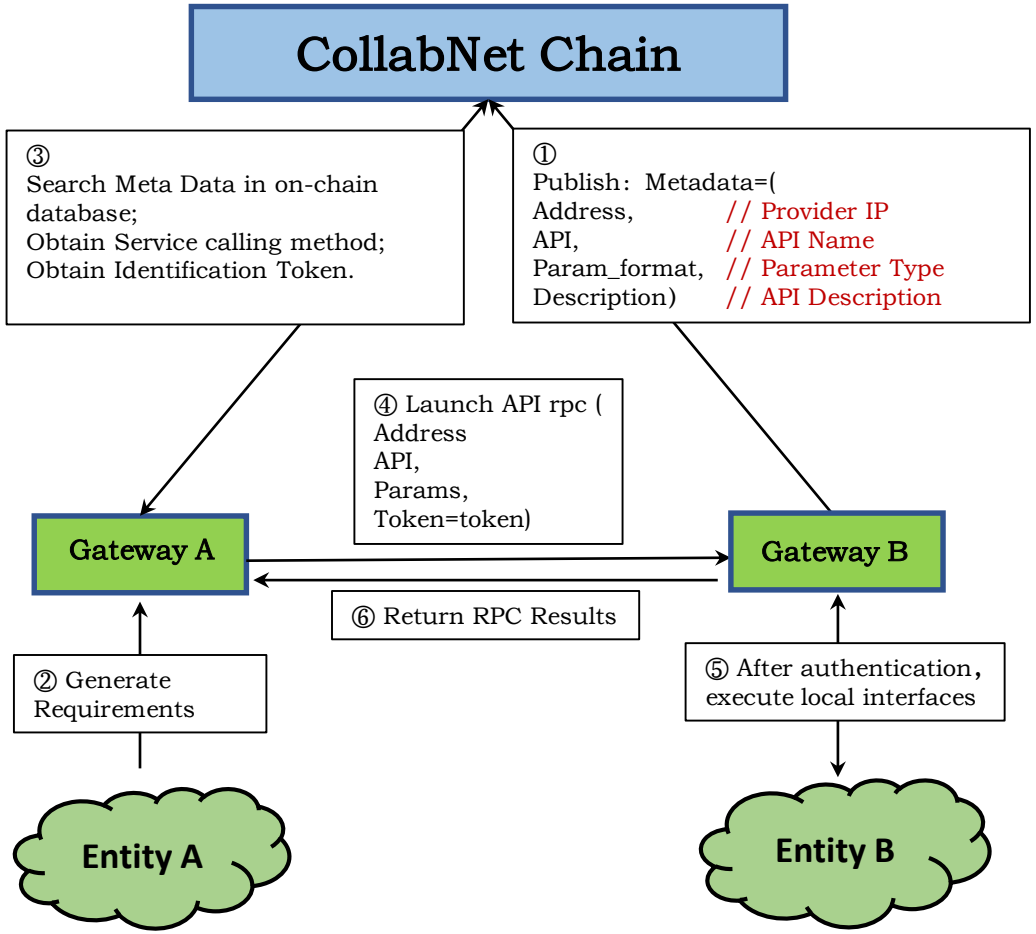
defines homogeneous information structure supporting different underlying local management systems

defines how participants communicate each other and how to publish and access service metadata

Components and Procedures

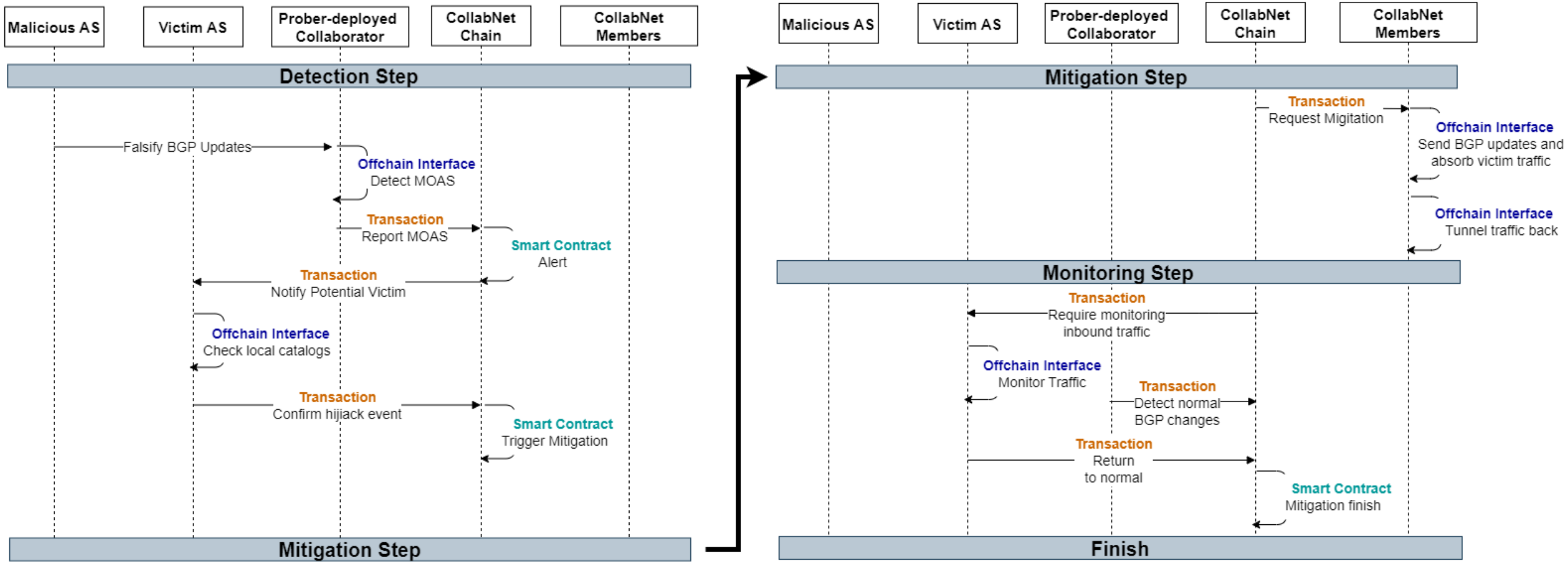


Detailed module design and interfaces between modules



Typical publish/search/submit procedure life-cycle for collaboration

Collaboration Automation via Smart Contract



Incentive Mechanism

Incentivize resources and services sharing among selfish independent ASes

Credit-based

Credit Assignment based on Shapley Value

How to solve?

Multi-agent Reinforcement Learning

Case study

Collaborative DDoS Mitigation

Two Incentive Mechanisms

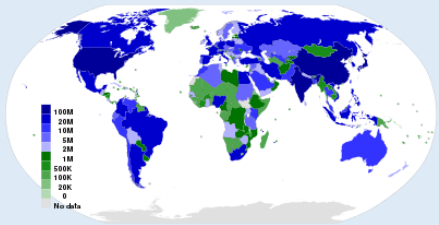
Accurate, Timely, Delicate

Robust, Slowly-evolved

Governance Network

Central Authority: Credit Account

De-Centralized: Reputation



Reputation-based

Reputation Score based on Behavior History

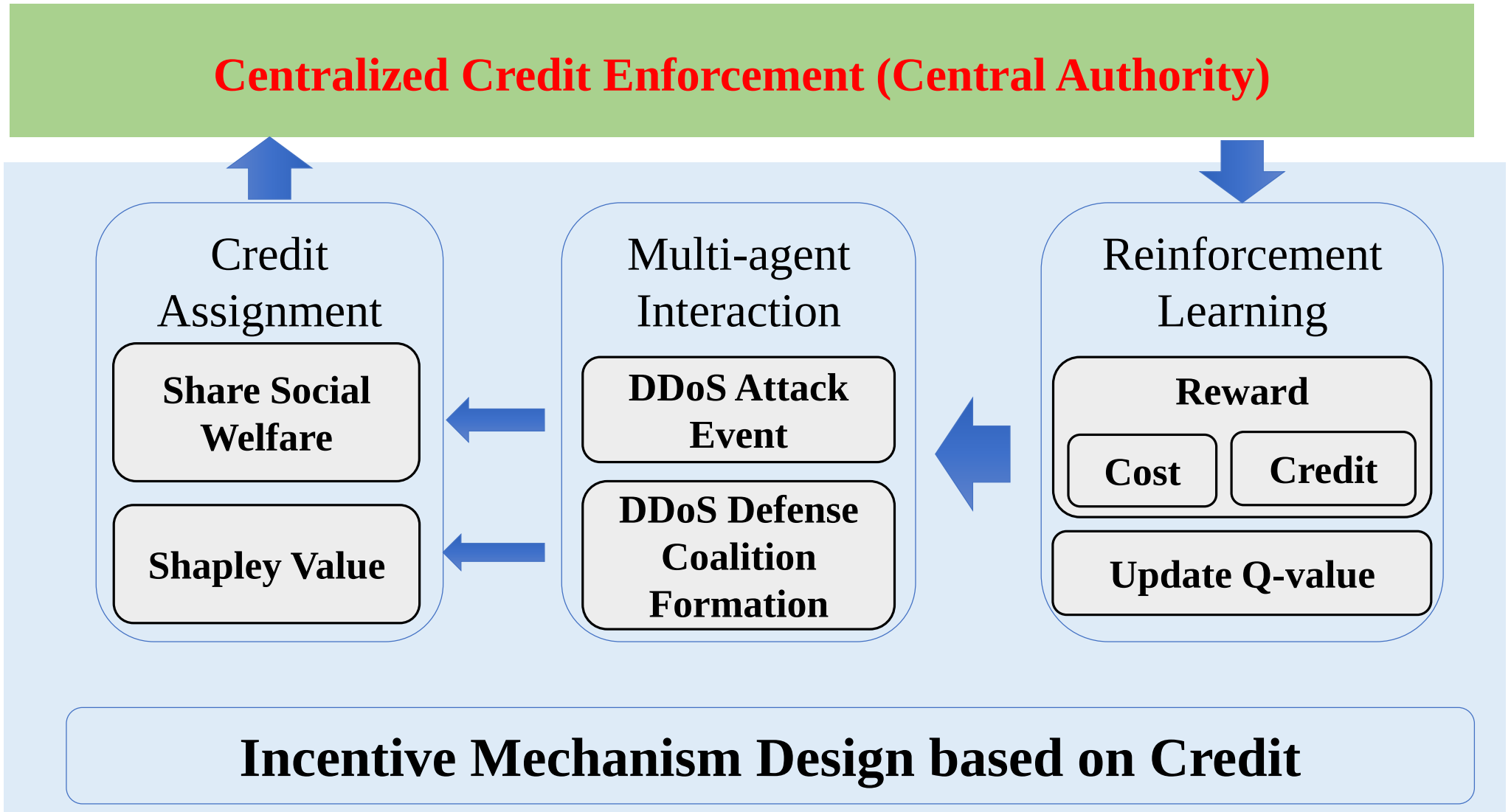
How to solve?

Evolutionary Game Theory

Case study

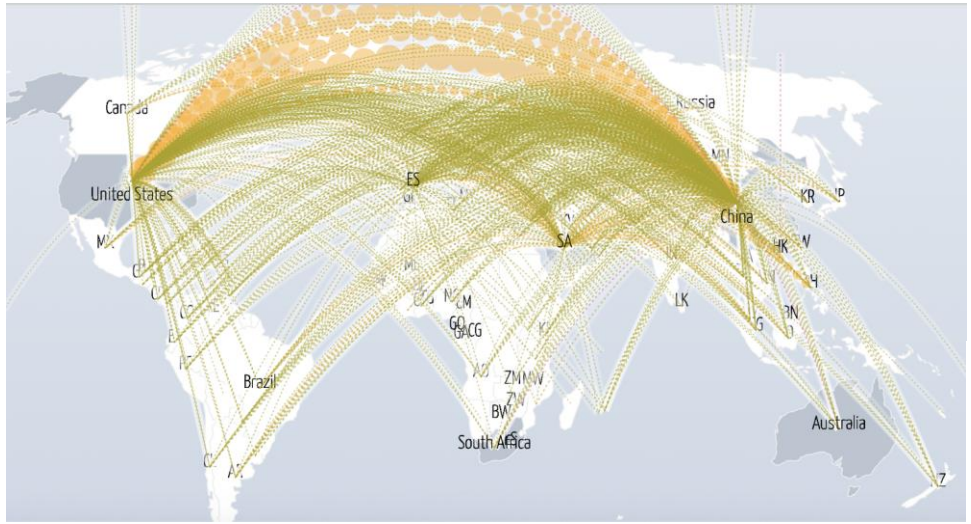
Collaborative Measurement

Incentive Mechanism



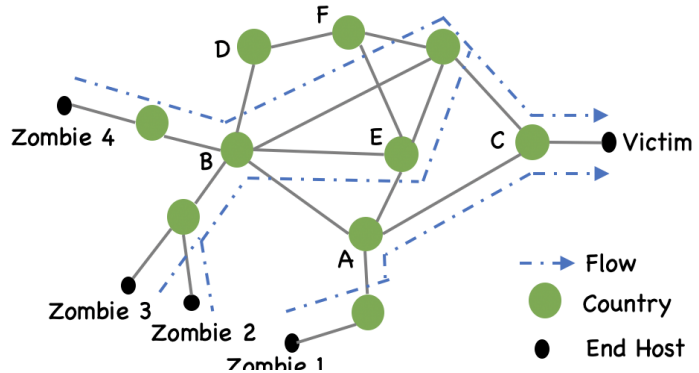
Incentive Mechanism

Collaborative DDoS Defense based on Credit Mechanism

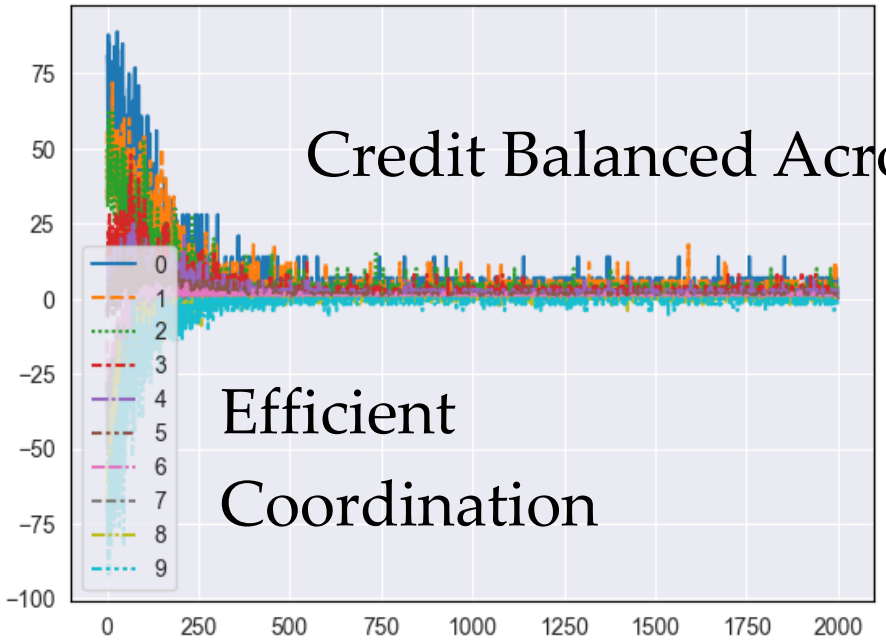


Global DDoS Attack Map

From Jan 1, 2015 to Oct 1, 2022



Collaborative DDoS Defense

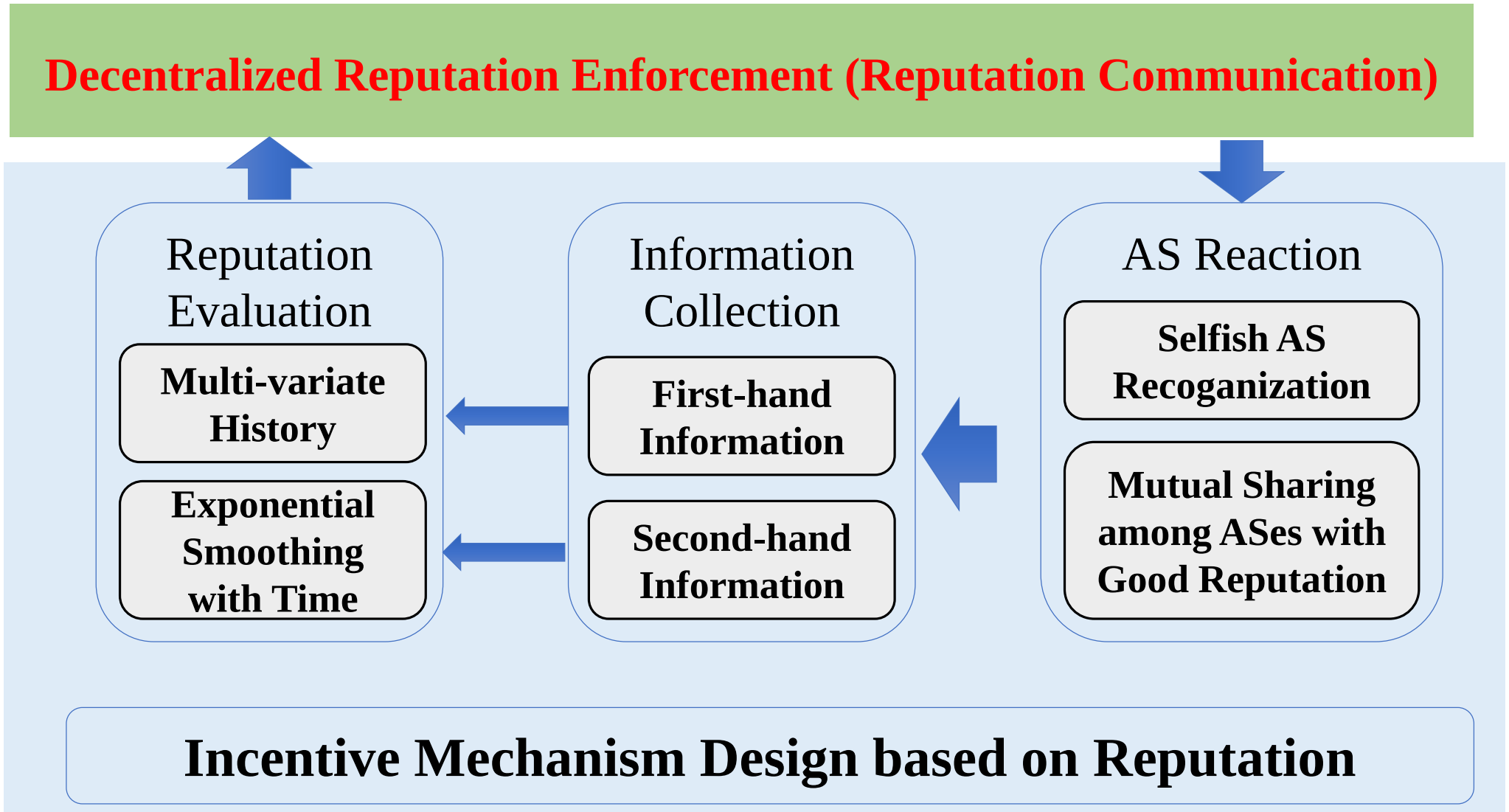


Credit Balanced Across Time & Space

Efficient Coordination

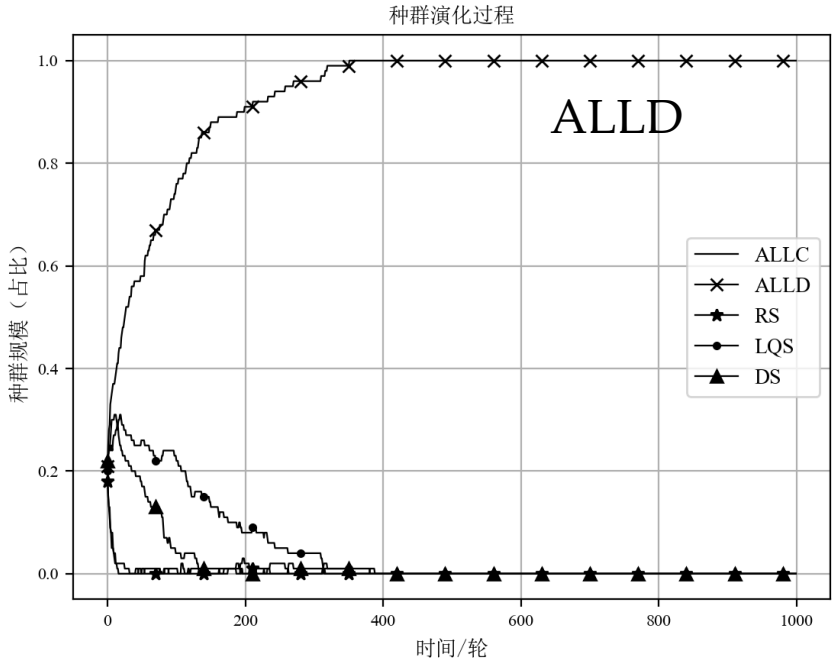
AS Credit Account

Incentive Mechanism

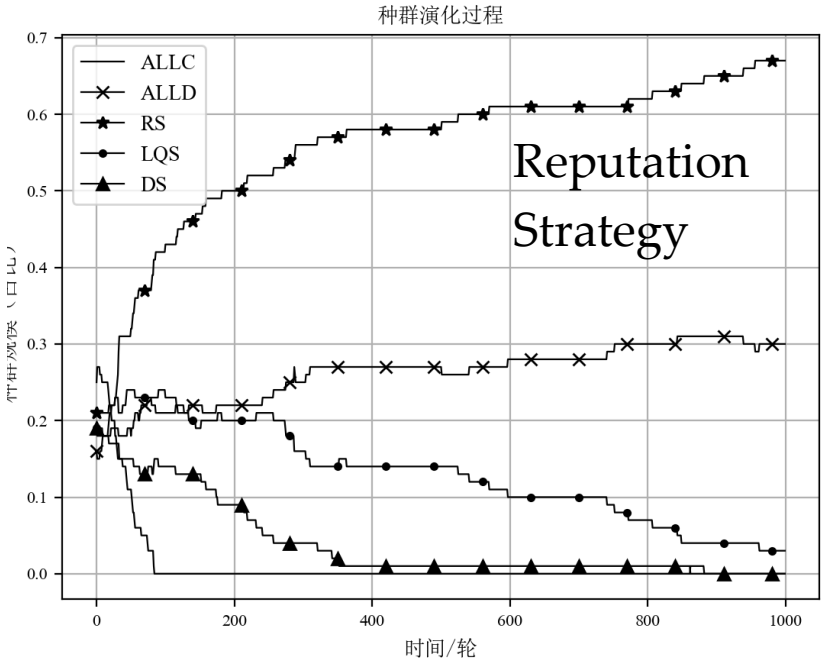


Incentive Mechanism

AS Population Evolution in Simulation based on Reputation Mechanism



No Reputation

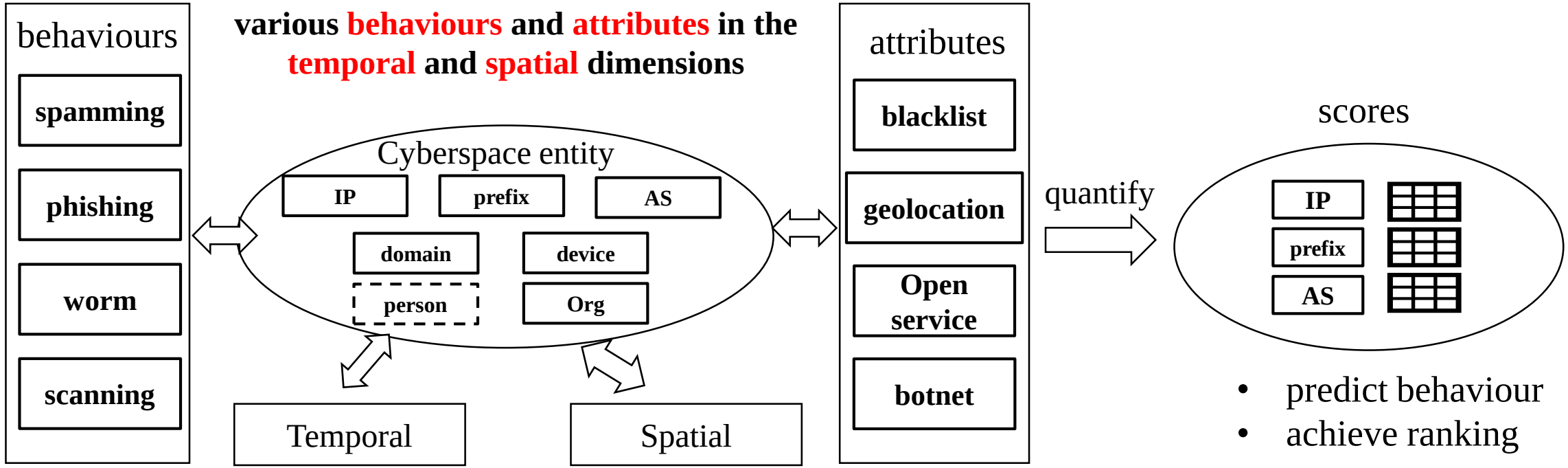


Reputation Mechanism

ALLC
(Always Cooperate)
ALLD
(Always Defect)
RS
(Reputation Strategy)
LQS
(Low Quality Strategy)
DS
(Discrimination Strategy)

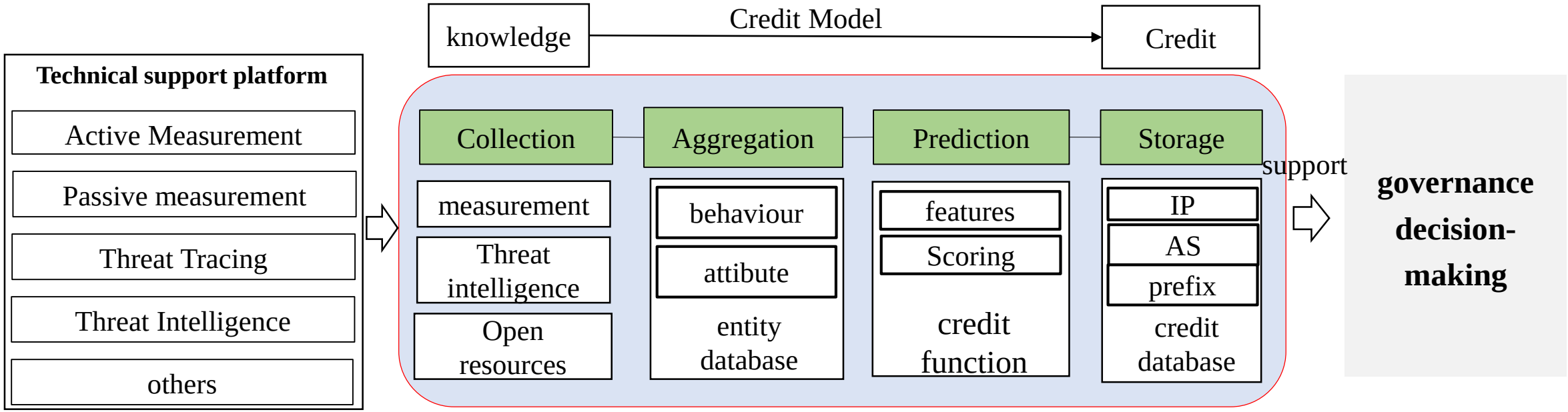
Security Credit of Cyberspace entities

In cyberspace, entities are network objects with network behaviours and attributes, such as IP addresses, IP prefixes, AS numbers, domain names, etc.



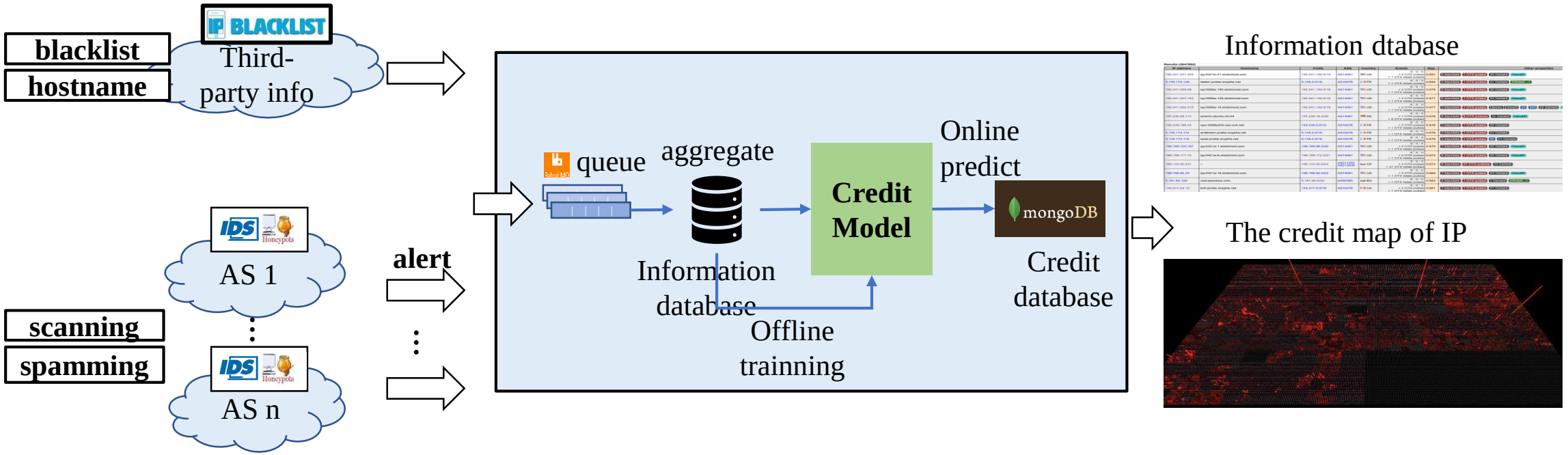
Security Credit Model

The credit is a summary of the past knowledge of a entity and can be used to predict the entity's future. A credit model needs to be designed to quantify the knowledge of a cyberspace entity into credit.



Security Credit of IP address

the credit of an IP address: the likelihood of an IP address performing a malicious act



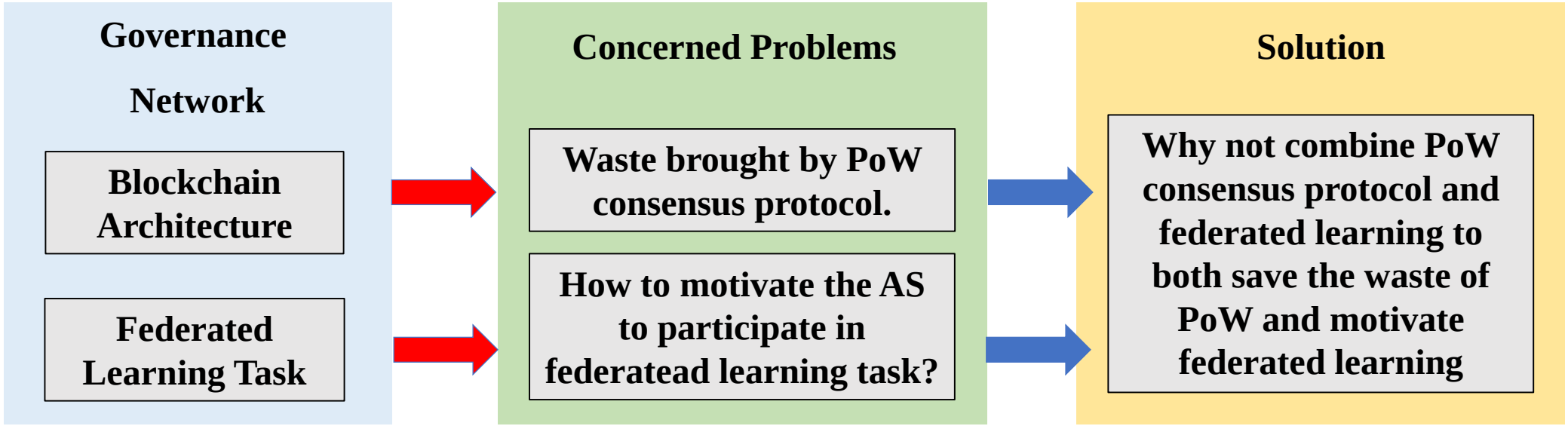
- The Information database: approximately 2.8 million IP addresses, covering 163 countries/regions

The security credits of IP addresses can be used to help network operators understand their security situation.

Build an efficient and effective technical platform to solve cyber issues in cyberspace itself quickly and auto-matically!

Efficient and Secure Consensus Protocol for Blockchain-based Network Governance Architecture

Blockchain-based network governance architecture requires a new designed PoW consensus protocol.



Energy waste brought by PoW **consensus protocol** + **motivation** to participate in **federated learning task**.

FedChain to **combine PoW consensus protocol and federated learning** within governance network.

Efficient and Secure Consensus Protocol for Blockchain-based Network Governance Architecture

Propose a secure and efficient consensus protocol for blockchain-based network governance architecture.

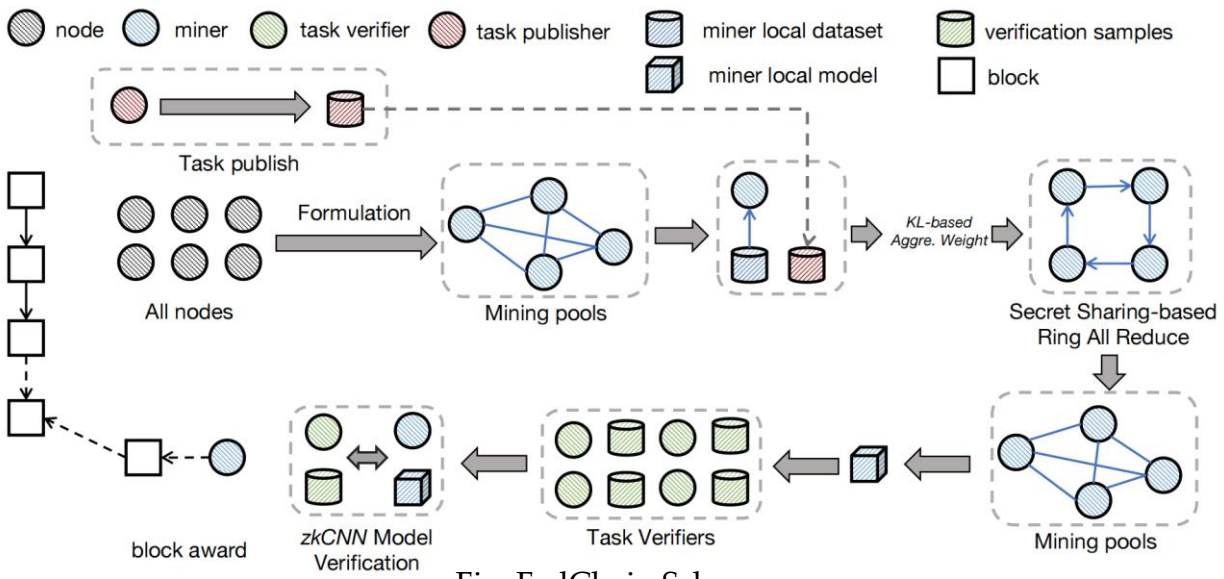


Fig. FedChain Scheme

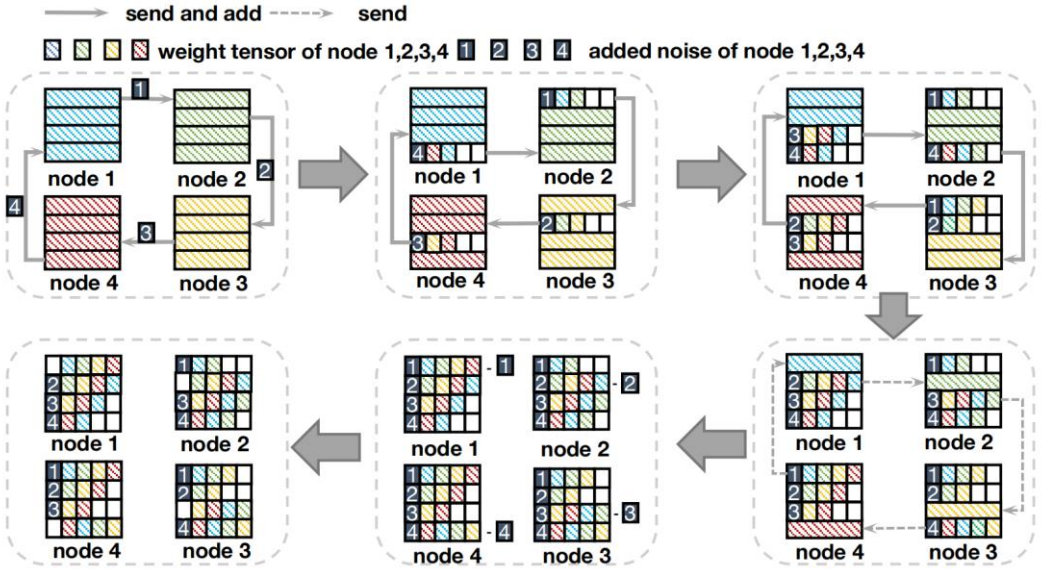
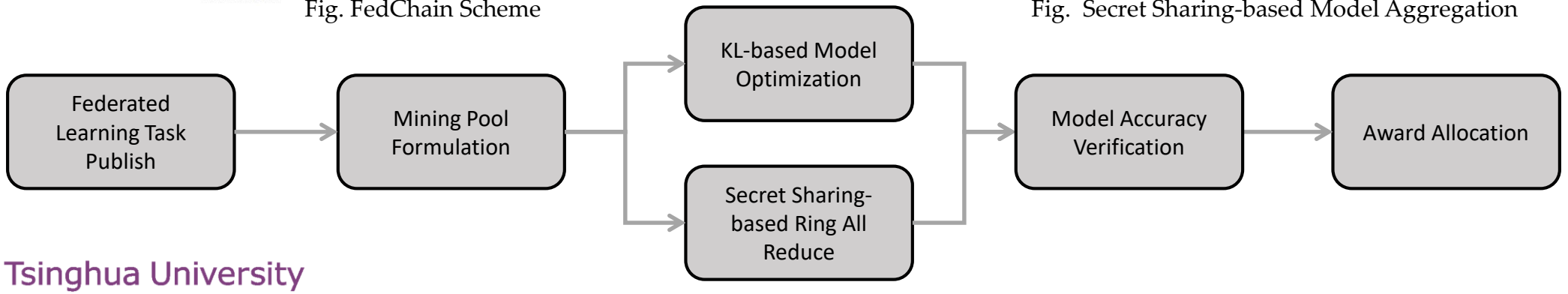


Fig. Secret Sharing-based Model Aggregation



Efficient and Secure Consensus Protocol for Blockchain-based Network Governance Architecture

Our proposed FedChain scheme achieves high performance compared with other schemes.

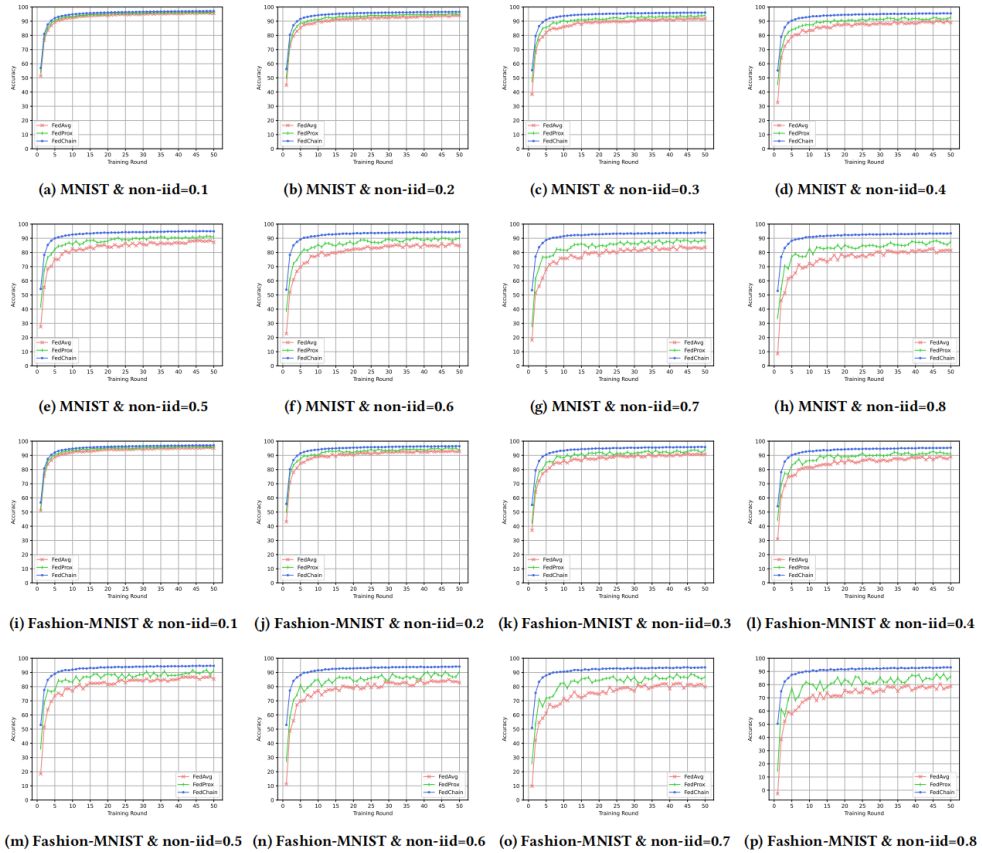


Fig. Accuracy comparison with other schemes

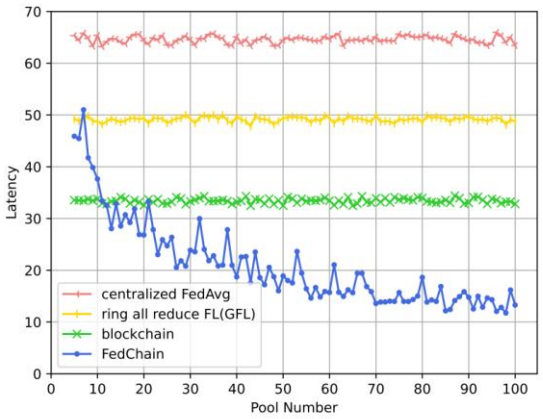


Fig. Latency comparison under different mining pool number

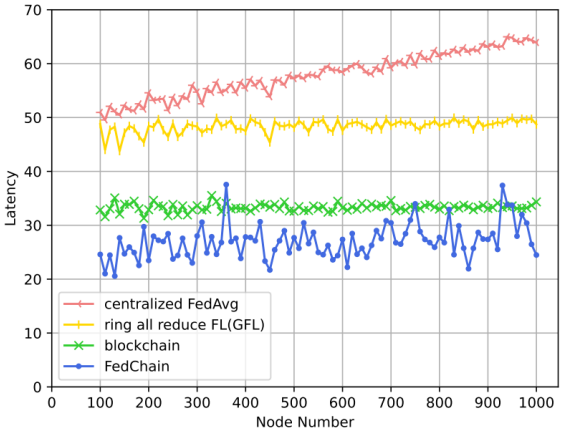


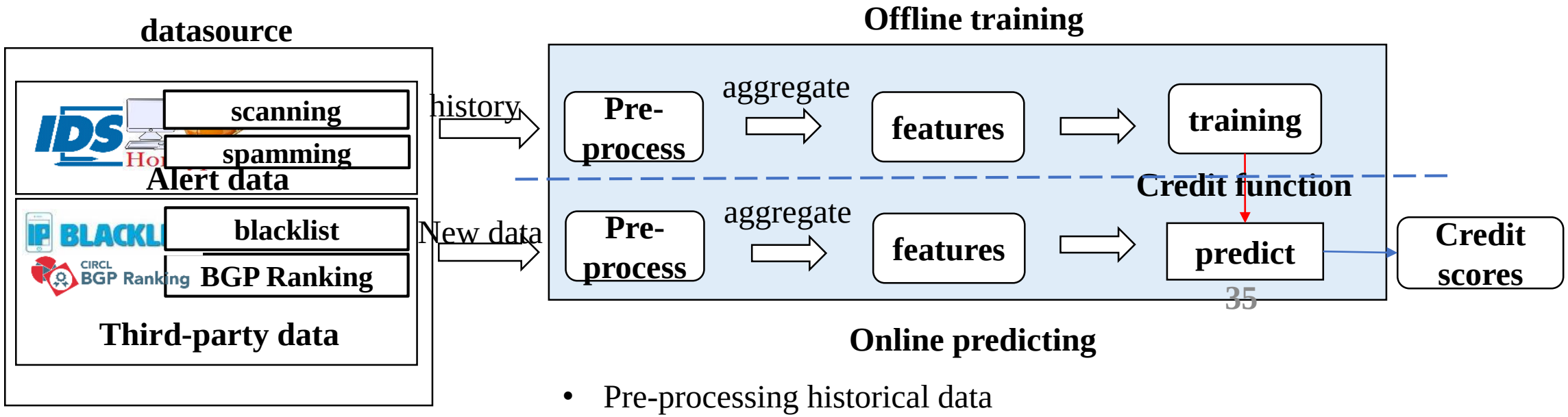
Fig. Latency comparison under different node number

We compare our proposed FedChain with other existing schemes. The results show that our proposed FedChain scheme has better performance in both model accuracy and latency.

Security Credit of IP address

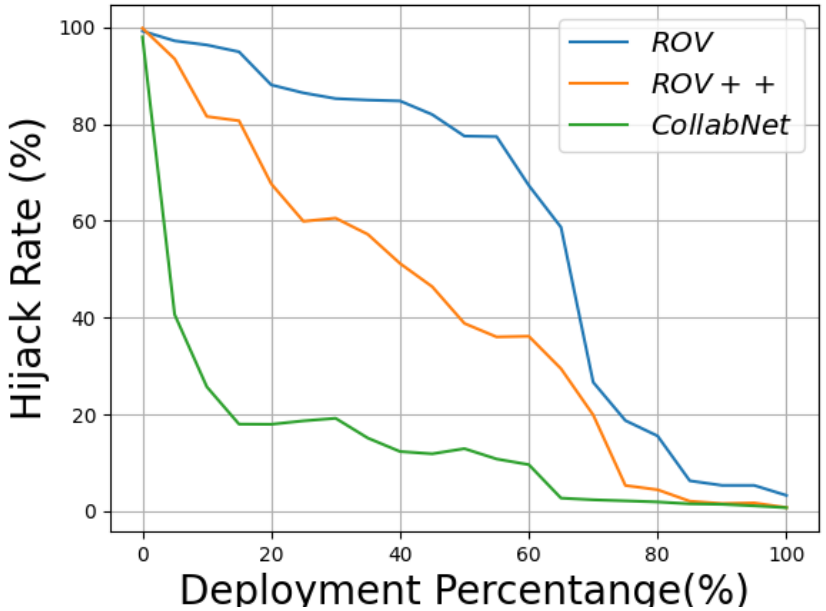
the credit of IP address: the likelihood of an IP address performing a malicious act

The credit model uses IP alert data and third party information as input, and a credit score is generated using a credit function.

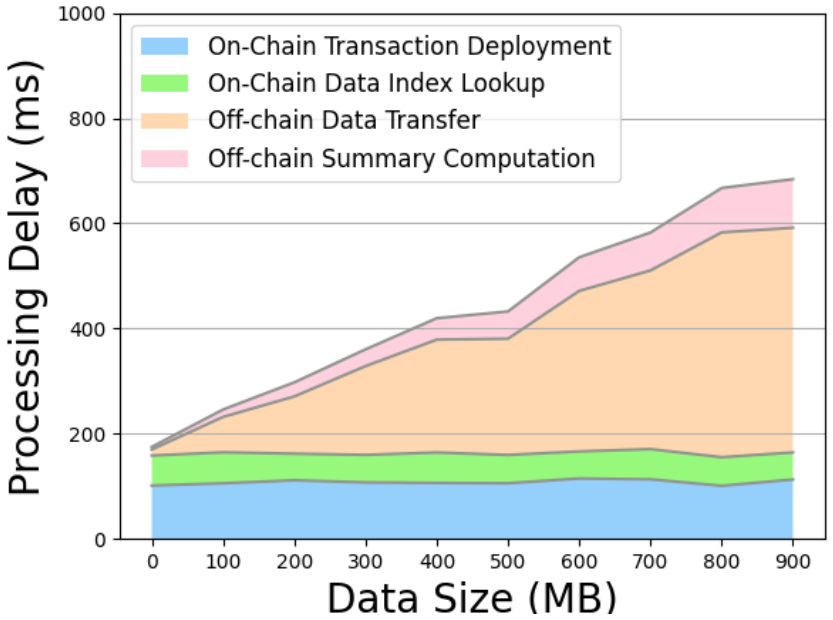


- Pre-processing historical data
- Extract features of aggregate data
- Training and prediction
  - Offline: training credit prediction function
  - Online: calculate the credit score of an IP address

Simulation and Results



We show that our collaboration platform performs better against routing hijacks than state-of-the-art ROV schemes and the recently proposed ROV++ [9], an update version of ROV.



The processing delay of different stages of a newly-deployed data sharing transaction. Introducing blockchain technologies brings negligible performance overhead for collaboration.

Tsinghua University