BEAF: A Blockchain and Edge Assistant Framework with Data Sharing for IoT Networks

Report : Yingxun Hu

Email : hyx@njust.edu.cn

Nanjing university of science and technology

CONTENTS

1

PART ONE

Introduction

▷ Background

An Information Carrier

the fifth generation (5G)

artificial intelligence technology

IoT market has fully exploded

▷ Introduction

- decentralized authentication
- privacy threats and data sharing
- malicious tracking

……

▷Introduction

resource allocation

social cost saving

information resource utilization rate reasonably

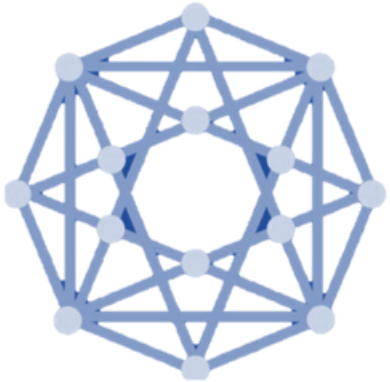
user privacy disclosure

data integrity problem

unauthorized data access

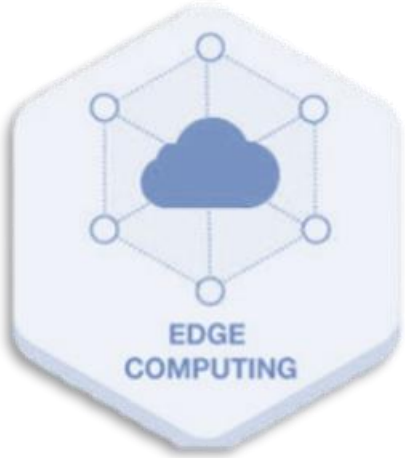
……

▷ Introduction



Blockchain

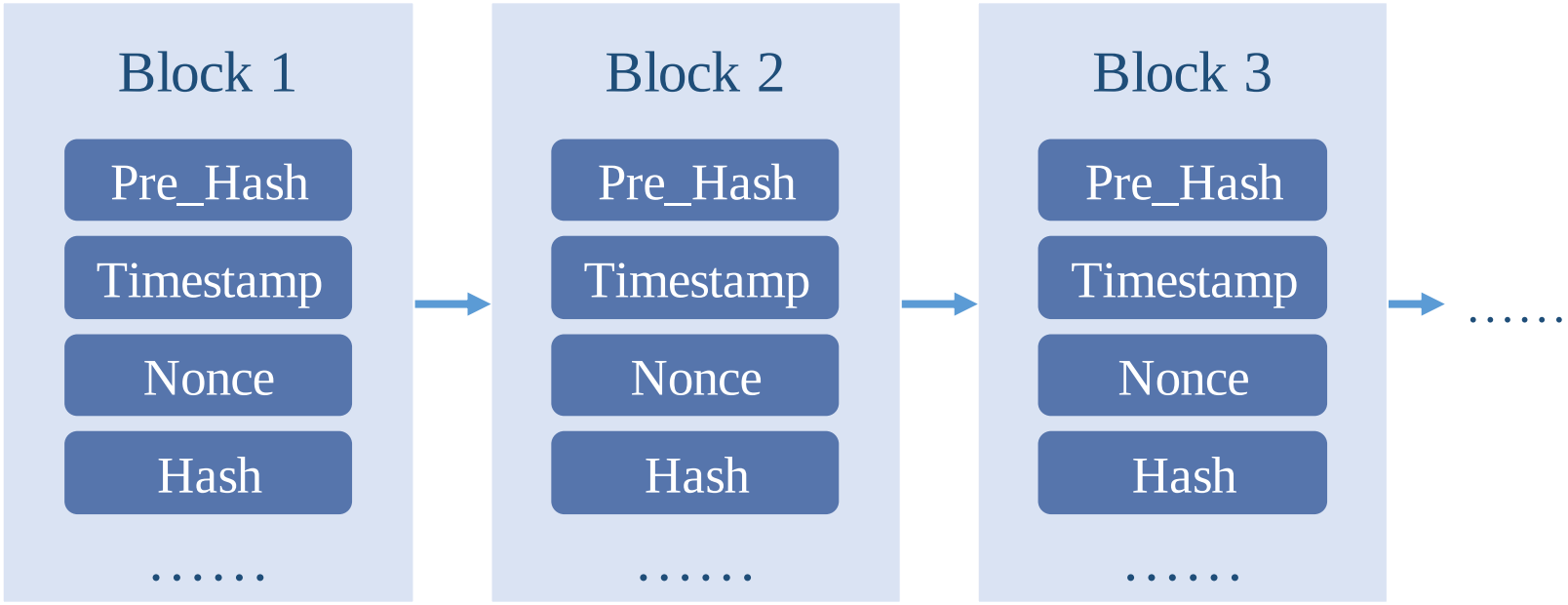
+



Edge Computing

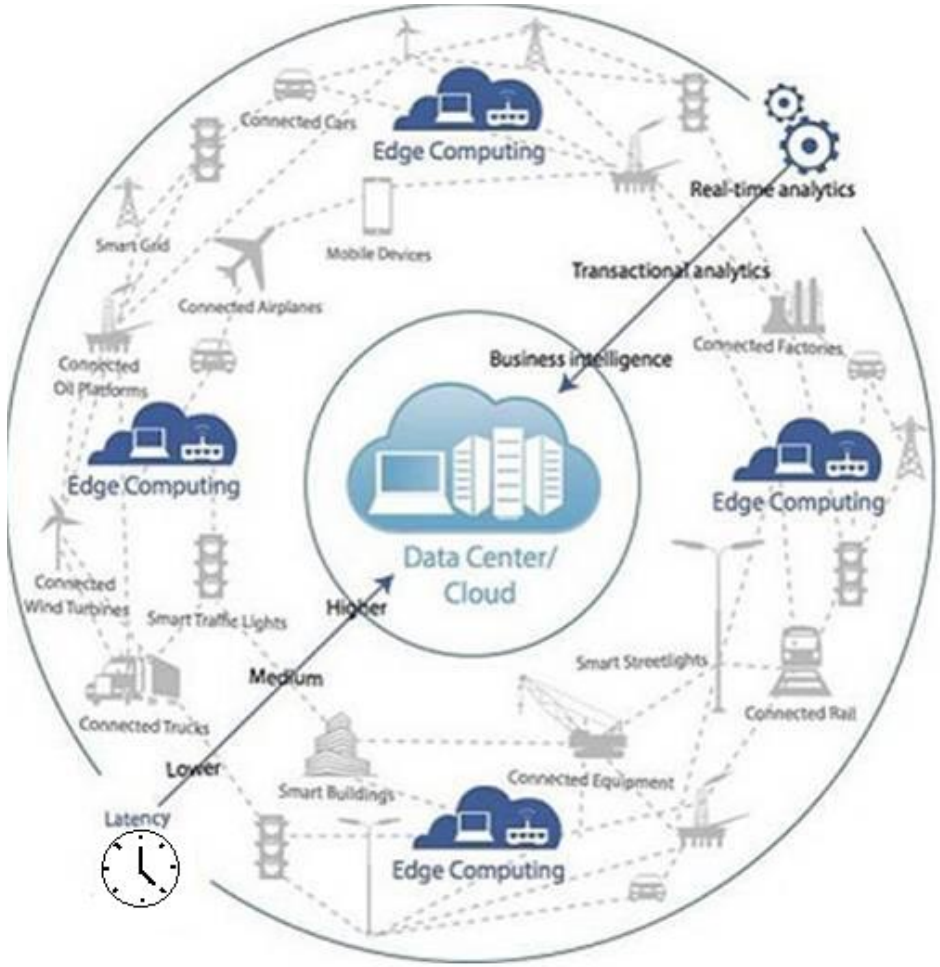
data security
privacy protection

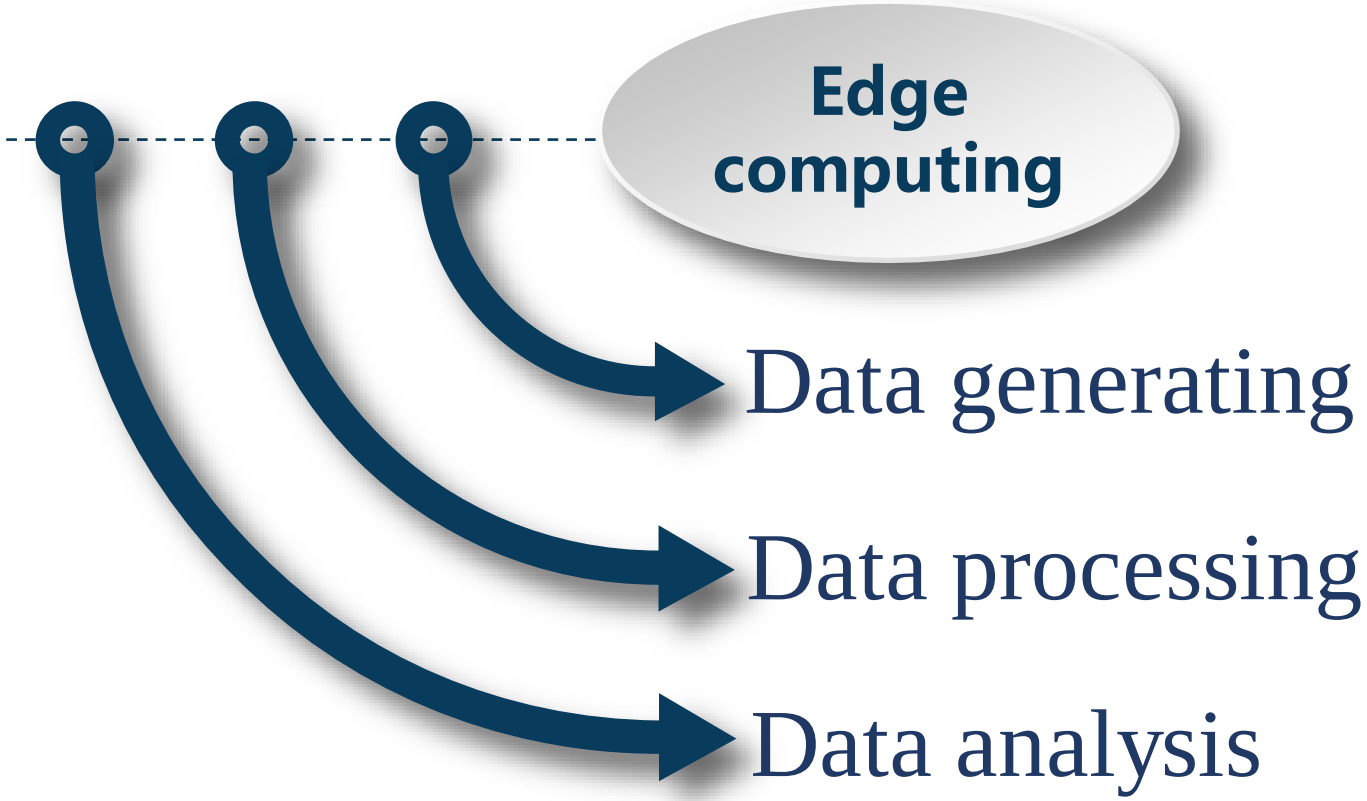
▷ Introduction



Consortium blockchains

▷ Introduction





▷ Literature review

1. a medical data sharing model via blockchain
2. a secured proxy-based data sharing module in IoT environments using blockchain
3. a secure solution for intelligent vehicle data sharing
4. a new mechanism SeShare for data storing based on blockchain
5. the user-controlled privacy-preserving user profile data sharing based on blockchain

---

scheme

- the use of traditional public key infrastructure (PKI)
- a new class of privacy indicators -- Data Controller Indicators (DCIs)
- a public key re-encryption scheme

……

- a cross-domain based data sharing scheme in cooperative edge computing
- a distributed algorithm developed for VNET

2

PART TWO

System Model

▷ System model

traditional centralized cloud architectures

- security
- scalability

BEAF

Edge computing

- computing resources
- data processing

users

Blockchain

the resource allocation of edge networks

▷System model

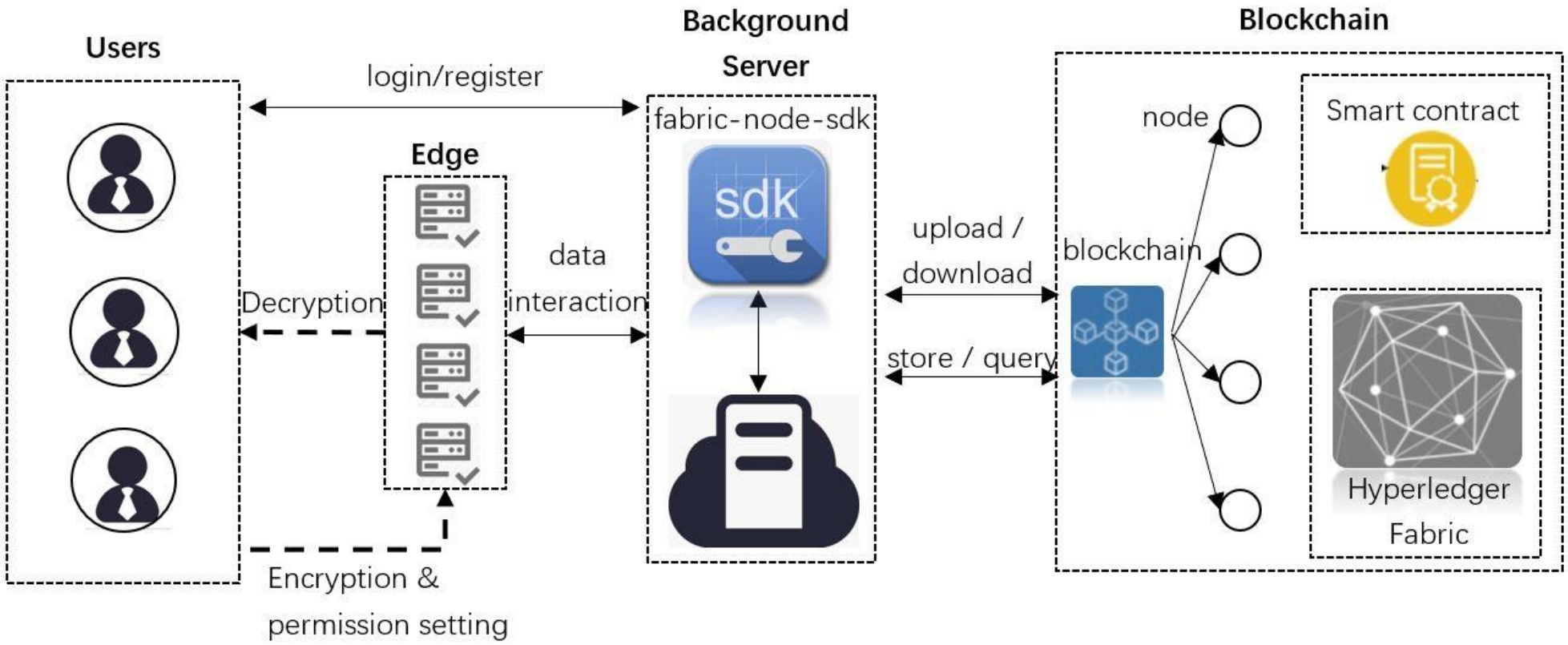
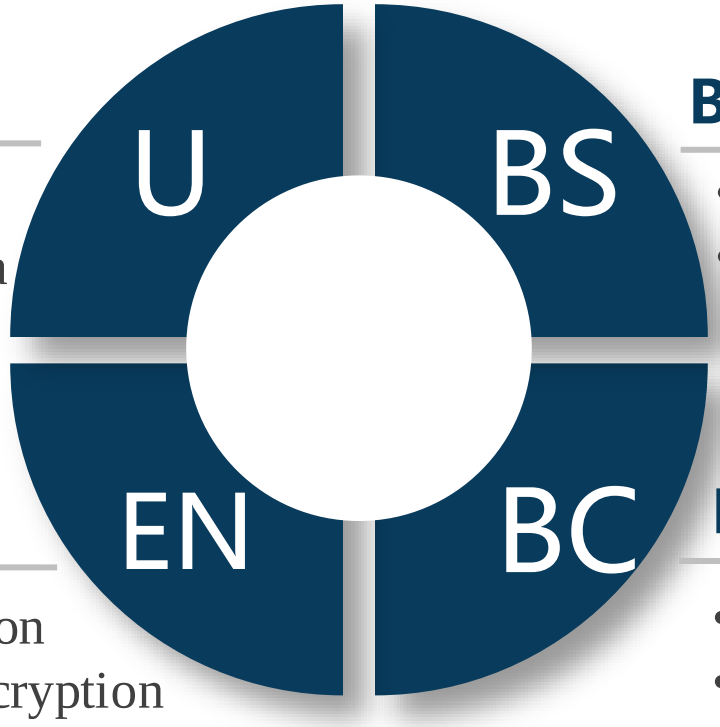


Figure 1

▷ System model



User

- upload data
- query & download data

Background Server

- Syst. Management
- Trace malicious user

Edge Node

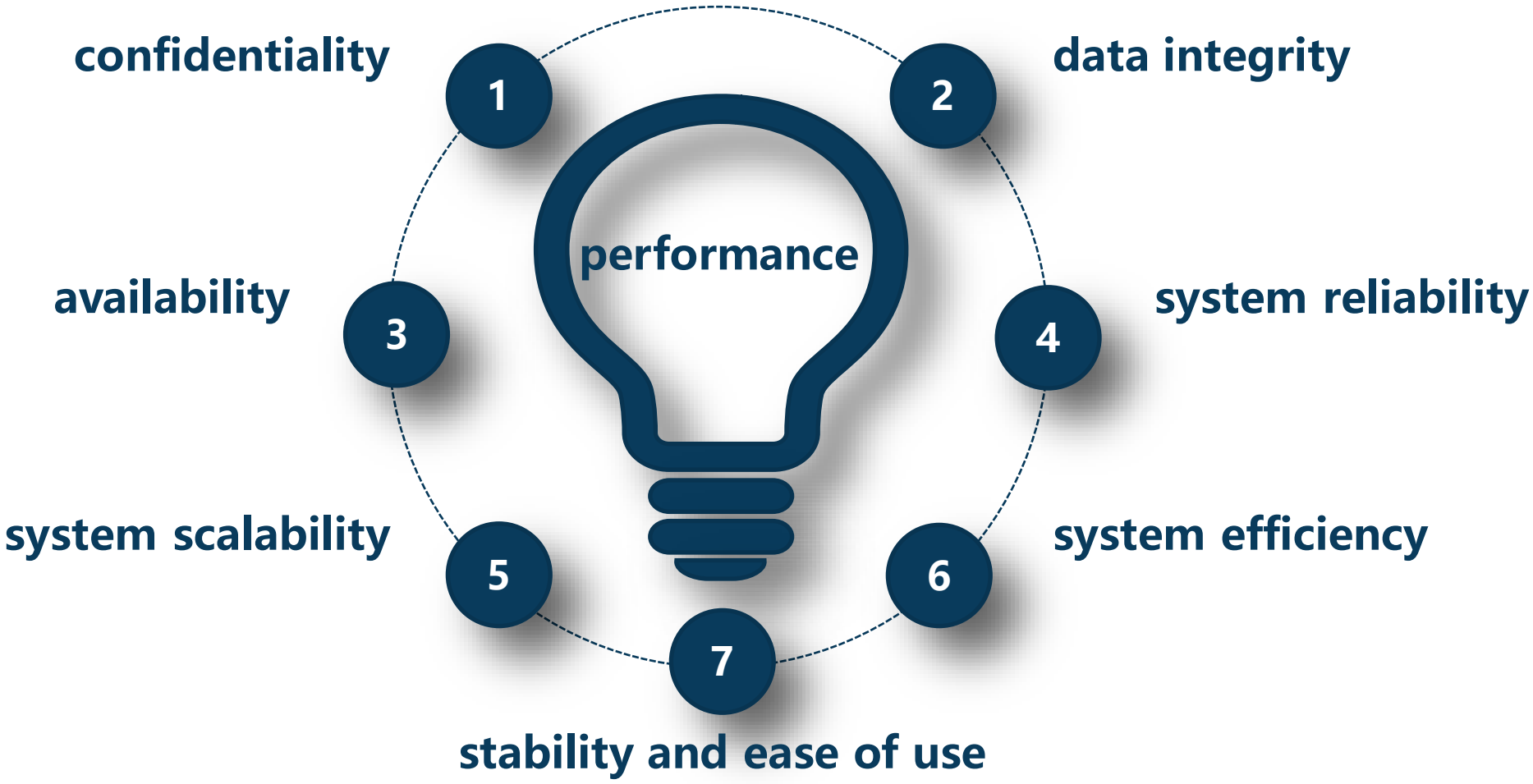
- distribution computation

→ data upload, data encryption and data downloaded

Blockchain

- Data storage
- Tracing

▷ Requirements



3

PART THTEE

The Proposed Framework BEAF

▷ Framework

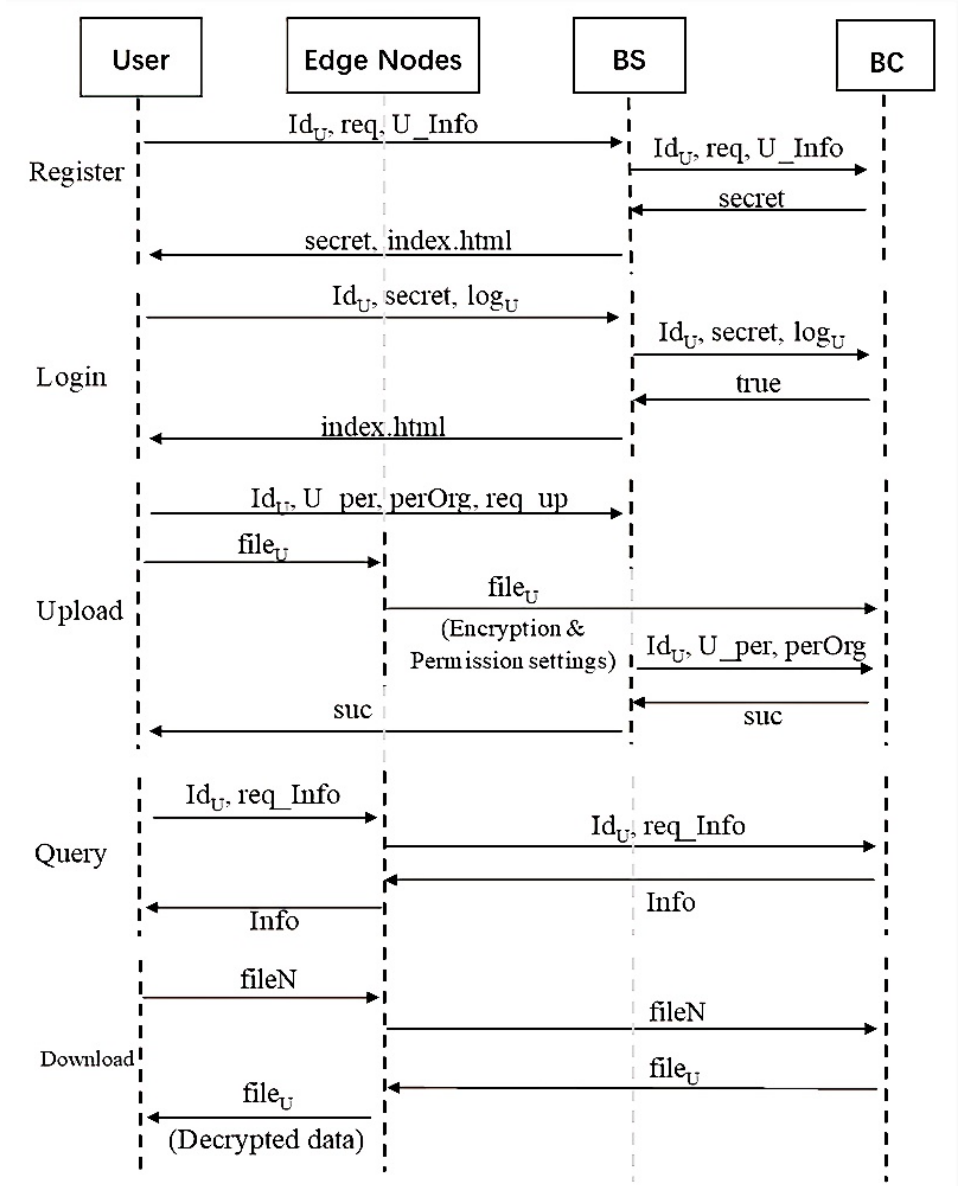
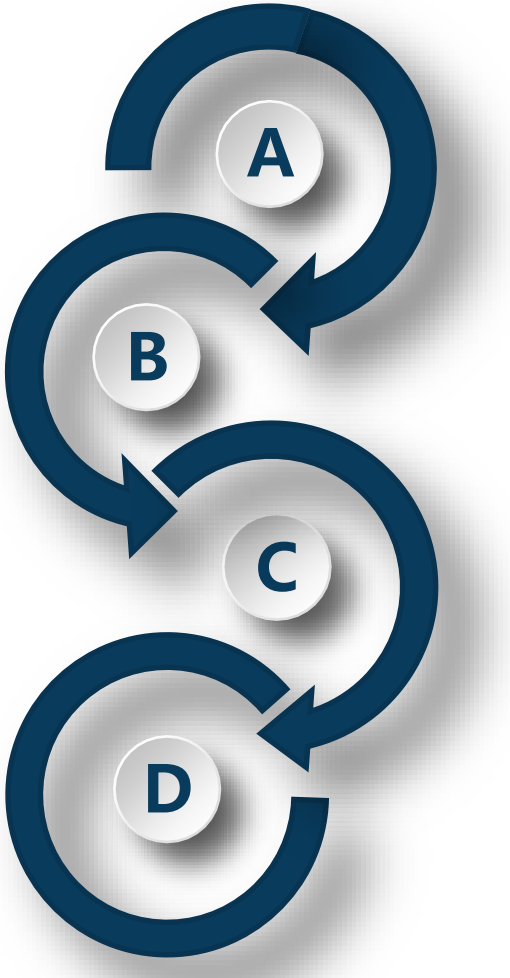


Figure 2

▷ Framework

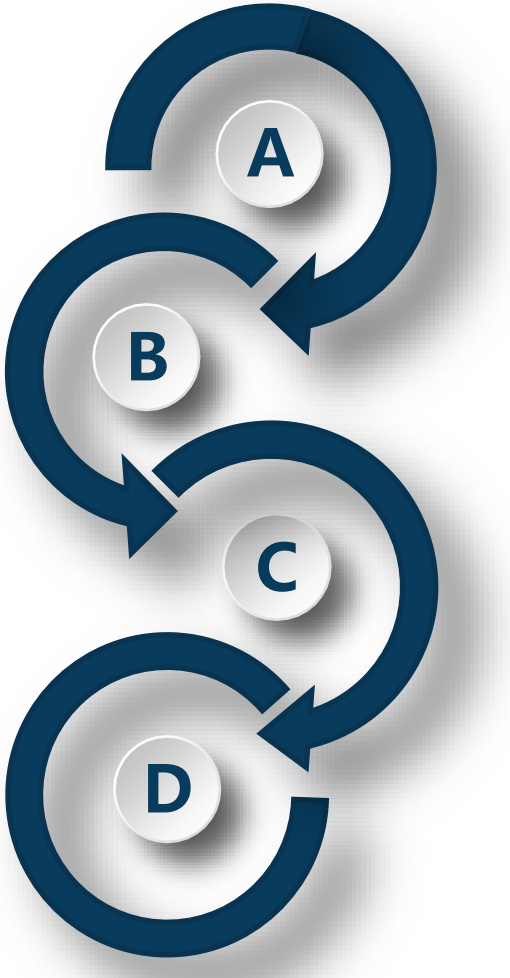
Register :



- **U → BS :** Id_U, reg, U_Info
- **BS → BC :** Id_U, reg, U_Info
- **BC → BS :** secret
- **BS → U :** secret, indel.html

▷ Framework

Login :



- **U** → **BS** : Id_U, secret, $\log_U$
- **BS** → **BC** : Id_U, secret, $\log_U$
- **BC** → **BS** : true
- **BS** → **U** : indel.html

▷ Framework

Upload :

1. **U** → **BS** : Id_U, $file_U$, U_per, perOrg and req_up
2. **U** → **EN** : $file_U$
3. **EN** → **BC** : $file_U$
4. **BS** → **BC** : Id_U, U_per, perOrg
5. **BC** → **BS** : suc
6. **BS** → **U** : suc

▷ Framework

Query :

ONE

U → **EN** : Id_U, req_Info

TWO

EN → **BC** : Id_U, req_Info

THREE

BC → **EN** : Info

FOUR

EN → **U** : Info

Download :

FIVE

U → **EN** : fileN

SIX

EN → **BC** : fileN

SEVEN

BC → **EN** : $file_U$

EIGHT

EN → **U** : $file_U$

4

PART FOUR

Security Analysis

▷ Security analysis

confidentiality

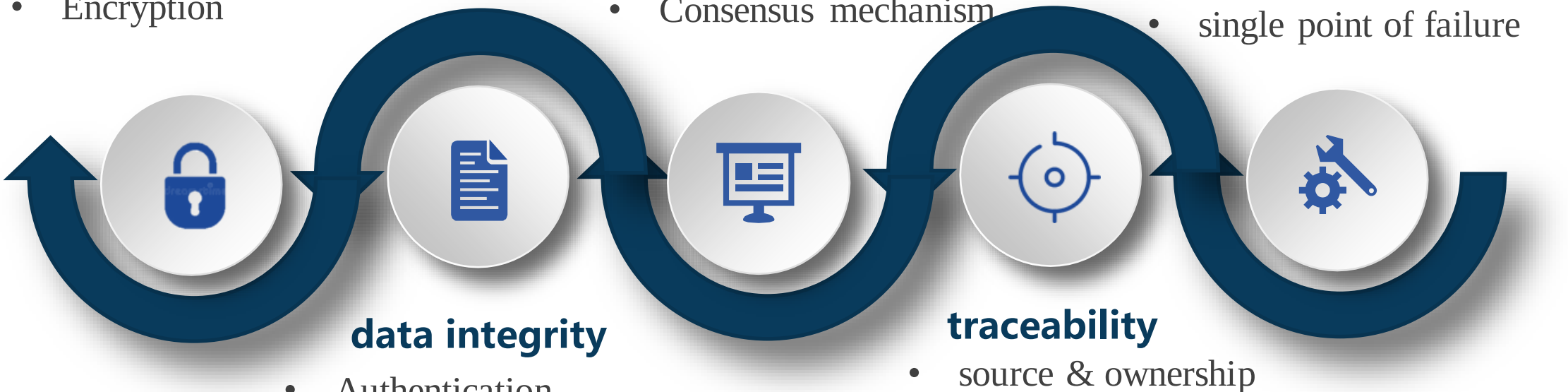
- Registered users
- Encryption

availability

- Monitor
- Consensus mechanism

reliability, stability, and scalability

- illegal / incomplete
- single point of failure



data integrity

- Authentication
- Encryption
- Immutability

traceability

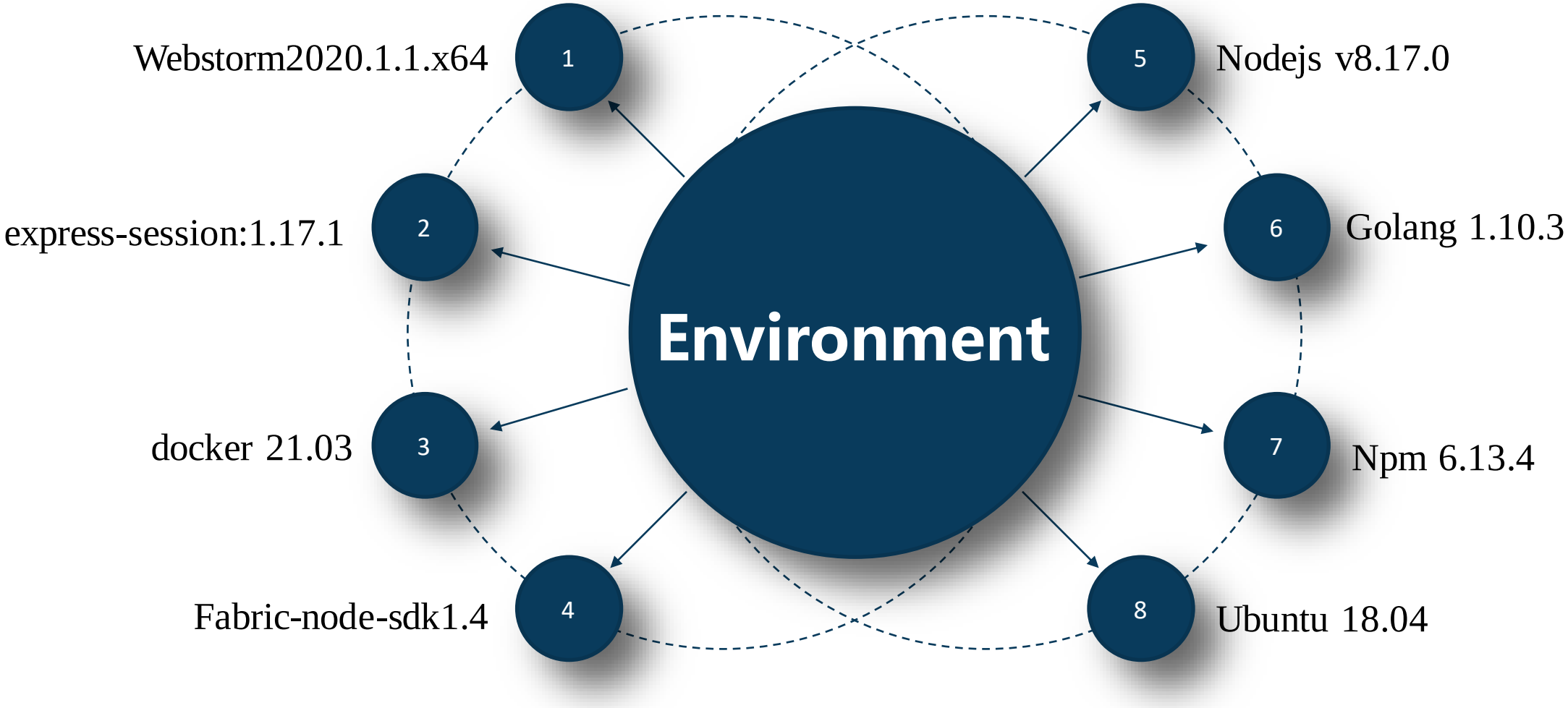
- source & ownership
- other disputes
- liability determinations

5

PART FIVE

Performance Discussion

▷ Performance discussion



▷ Performance discussion

Performance	Specific Indicators	Value
Average Response Time	Query (Single file)	372ms
	Query (All file)	362ms
	Upload	572ms
	Download	291ms
Reliability	System stable (operation duration)	7*24h
	System failure rate	5 times/week

TABLE II. The performance of the proposed BEAF

6

PART SIX

Conclusions

▷ Conclusions

- **Objectives:** secure data sharing and privacy preservation
- **Security:** data security, data authenticity, privacy protection, data tamper resistance, and traceability
- **Performance:** data query efficiency and system reliability.
- **BEAF:** employ blockchain and edge computing paradigms

THANKS!