Research on the Monitoring, Privacy Protection and Application of Blockchain

School of Cyber Science & Engineering,
Southeast University, China
Dr. Xiaoyan Hu

29 October 2020

SOUTHEAST UNIVERSITY

Content

東南大學
SOUTHEAST UNIVERSITY

01

Research on Encrypted Traffic in Ethereum network

止于至善

Research Purposes:

Ethereum uses the private RLPx protocol to encrypt the content. Accurate identification of ethereum encrypted traffic can provide strong support for ethereum network supervision.

Research Contents:

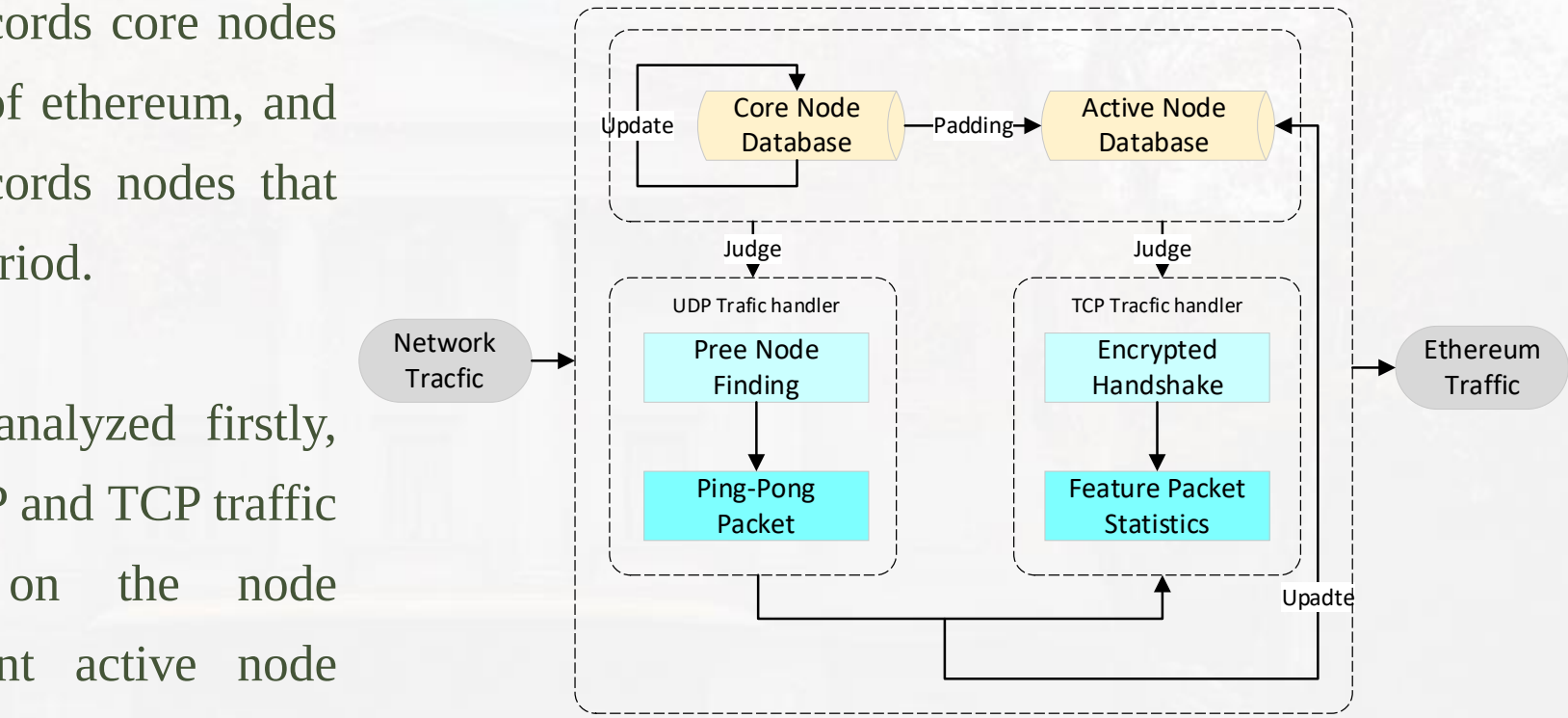
① Analyze ethereum private protocol RLPx.

② Ethereum encrypted traffic identification method based on active node database.

Research Methods:

① The core node database records core nodes that maintain the stability of ethereum, and the active node library records nodes that active in the current time period.

② The RLPx protocol was analyzed firstly, and then, the ethereum UDP and TCP traffic were identified based on the node information in the current active node database.



Research Purposes:

By extracting the characteristics of ethereum encrypted behavior traffic and constructing a behavioral context fingerprint database to realize accurate classification of the ethereum encrypted behavior traffic, which provides a basis for further realizing the traceability of Ethereum or the analysis of abnormal behavior of ethereum.

Research Contents:

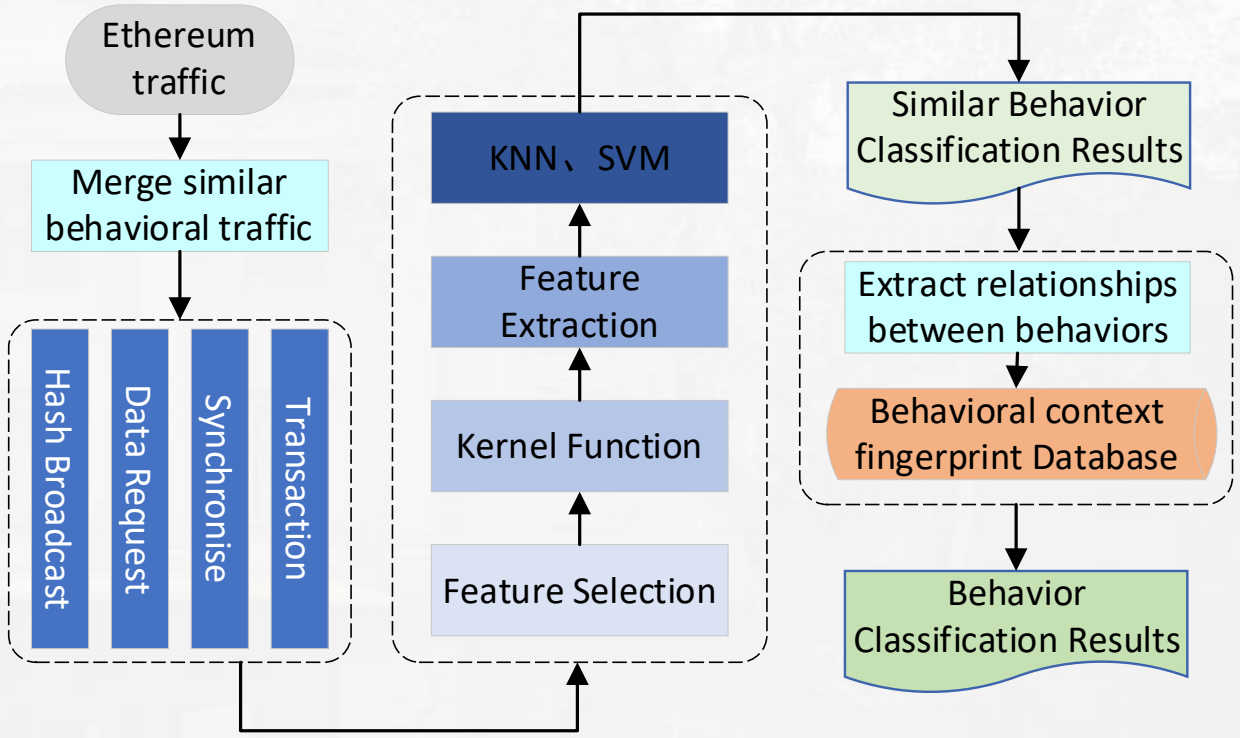
① Feature extraction method of Ethernet encrypted behavior traffic.

② Ethereum encrypted behavior traffic classification method based on correlation analysis between behaviors.

Research Methods:

① Similar behaviors were merged firstly, and then classified by machine learning method after feature extraction and feature selection.

② The correlation between behaviors is analyzed firstly, and then establish a behavior context fingerprint database.



東南大學
SOUTHEAST UNIVERSITY

02

Research on Verifiable and Regulable Encrypted Data in Consortium Chain

止于至善

Research Background:

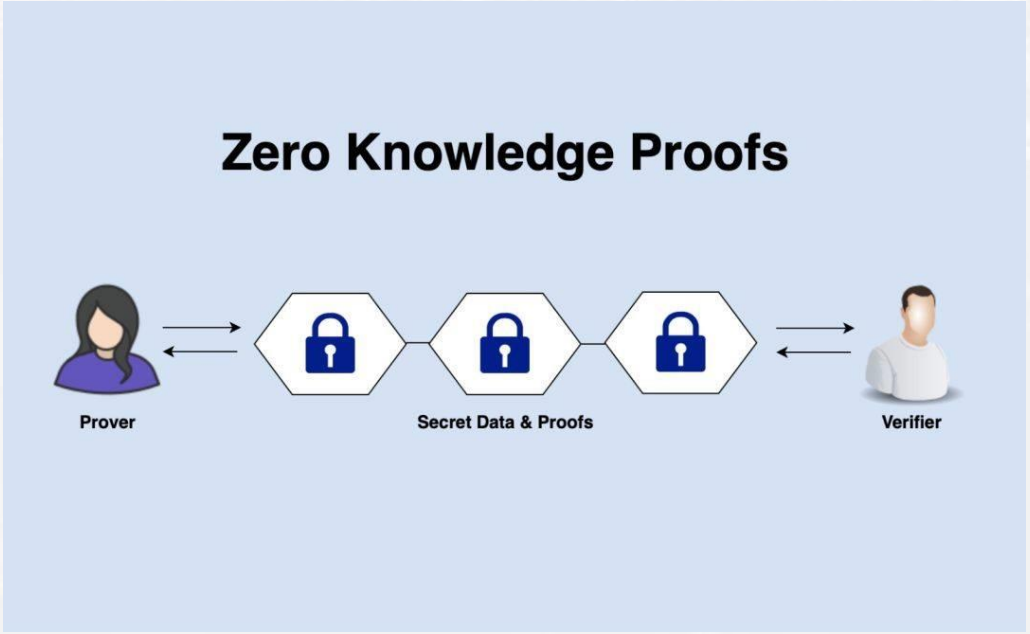
In the consortium blockchains, the transaction information of participants may contain some encrypted sensitive data. However, there will still be a demand for a third party to verify these sensitive data in the case of encryption.

Research Purposes:

How to design a verifiable method for encrypted data under the premise of ensuring data privacy, so that the verifier can verify the consistency of the sensitive protected data, is an urgent problem to be solved.

Research Idea:

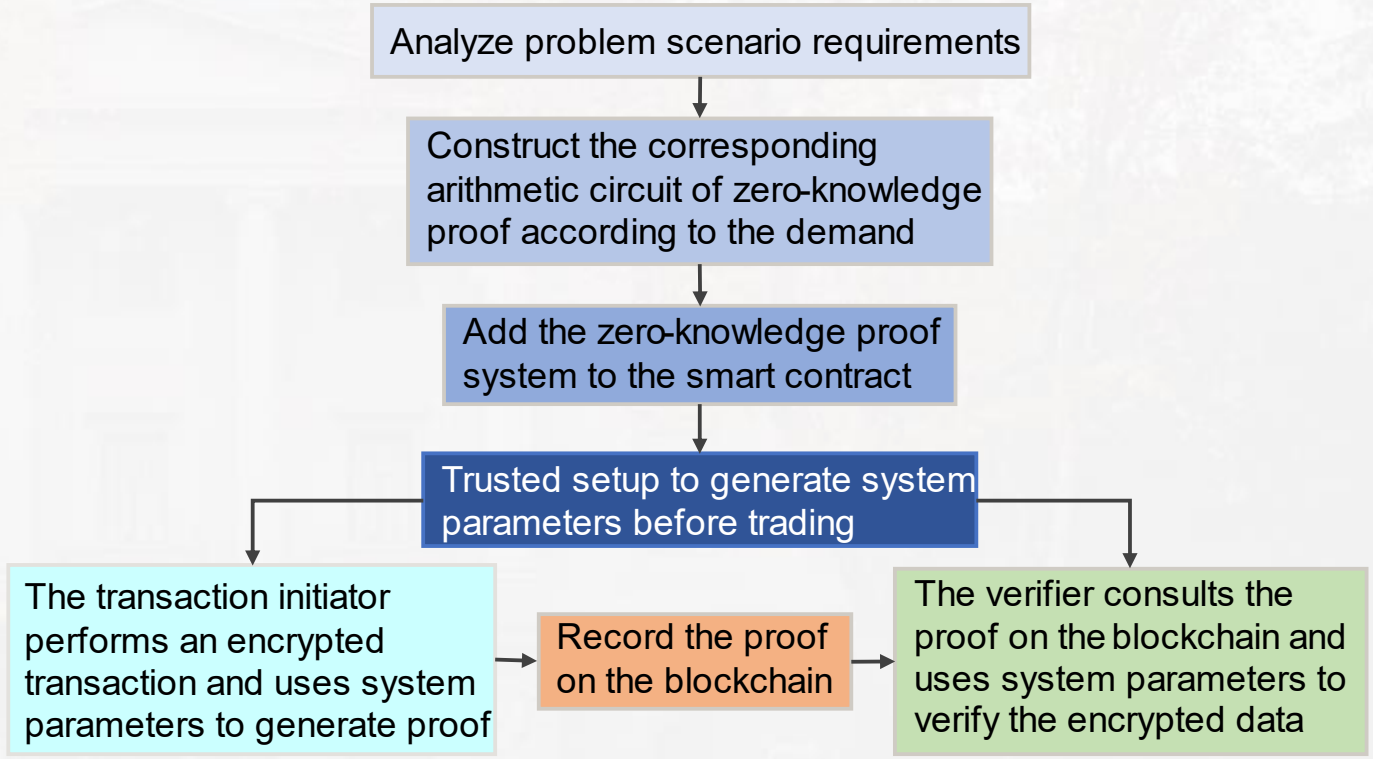
A technology called **“Zero-Knowledge Proof(ZKP)”** can meet the demand well. The Zero-Knowledge Proof is a method by which one party (the prover) can prove to another party (the verifier) that an assertion is true without revealing any useful information apart from the fact.



Research Methods:

① Construct a non-interactive zero-knowledge proof system according to demands and join the consortium blockchain system.

② The third party verifies the encrypted data with proofs generated by the trader recorded on the blockchain.



Research Background:

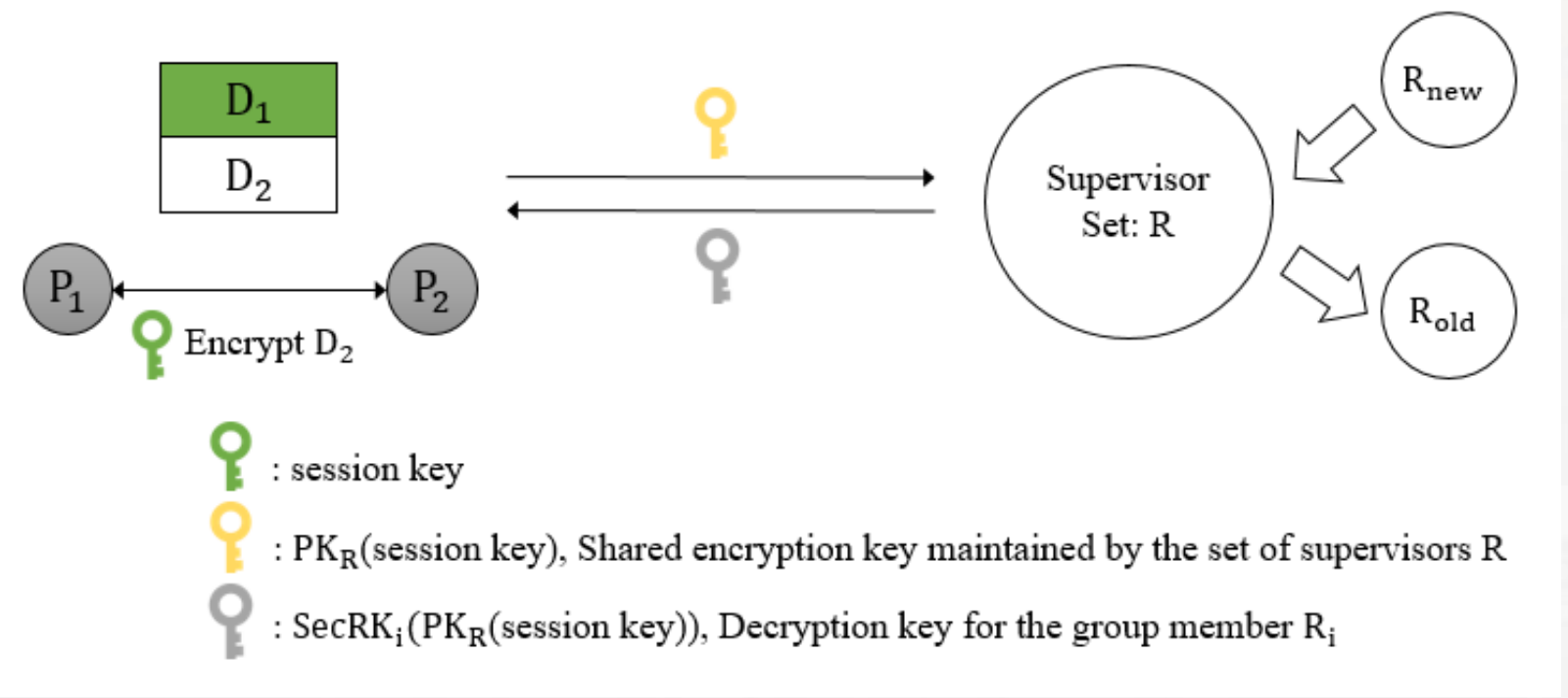
- In the enterprise-level application scenario of the consortium chain, the requirements for data privacy protection are relatively high.
- Transaction data will be stored on the chain in the form of cipher text. The supervisors in the consortium chain should be authorized (to obtain the key to decrypt private data) to decode the encrypted data on the chain.

Research Purposes:

- Simplify the authorization process: The authorization of private data is to send the session key to encrypt the data to the supervisors. Since there may be many supervisors on the alliance chain, if each supervisor is authorized separately, the authorization process will be inefficient and waste resources.

Research Contents:

The supervisors form a group, the group members maintain a common group encryption key for session key encryption, and each group member decrypts the session key using its own unique decryption key. This method avoids the need to encrypt each session key for individual supervisors, thereby improving authorization efficiency. The group is relatively stable and the management of member join and leave is efficient.



Research Methods:

Step 1

- System initialization, generate corresponding system parameters

Step 2

- Supervisor's public and private key generation

Step 3

- Key agreement process: After a series of calculations and broadcasts, a key generation matrix will be obtained.

Step 4

- Verify the identity of the group members and the integrity and correctness of the messages published by the group members. If the verification is successful, the group encryption key is generated. And group members generate their own decryption keys.

Step 5

- Encryption and decryption process

東南大學
SOUTHEAST UNIVERSITY

03

Practice of Developing Blockchain Applications

止于至善

The System Significance:

A. Solve the inconvenience of marriage registration

- When citizens apply for marriage registration, they no longer need to take physical proof materials.

B. Make marriage registration data more reliable

- The use of blockchain technology makes data tamper-proof and traceable, reducing the risk of falsification of documents and modification of data.

C. Solve the data island problem

- It can prevent criminals from using the information barrier of marriage data to cheat marriage and bigamy.

The System Overview:

- This system use the FISCO BCOS underlying platform to build a chain of alliances. It uses WeIdentity to realize distributed identity management, making people's real identity into the identity on the chain. It issues electronic credentials to people, and those credentials can be verified on the blockchain.

- This system simulates the basic process of marriage registration, and has the roles of issuing agency, applicant, verification agency(Marriage Registry), which can form a logical business loop.

Marriage Registration System Based on Blockchain

1. The authoritative issuing agency issues personal identity credentials for citizens
2. The applicants authorize their credentials to the Marriage Registry
3. Marriage Registry verifies the authenticity of credentials on the blockchain
4. Marriage Registry issues marriage credentials to applicants
5. Turn marriage credentials into evidence in the chain
6. The marriage certificates become evidence in the chain that can be used for other purposes

Design Significance:

- Continuous rewards and incentives for positive civilized behaviors, especially small and positive behaviors are valued, recorded, encouraged, and continuously affirmed.

- For example, effective incentives or rewards for collecting money, garbage sorting, and courageous acts can improve society governance level, promote the development of social civilization, and then achieve the goal of sustainable development.

Reward mechanism for righteousness

Design Ideas:

- The roles in the project include: users, auditors, administrators, sponsors, and companies.
- Among them, the auditor is not on the blockchain, and is responsible for reviewing the authenticity of the events submitted by users offline, and feedback to the administrator if it is true.
- All roles on the chain have functions such as registration and login, and the remaining functions are as follows:

User	Admin	Sponsor	Company
Fill in the application, **Q**uery related information.	**D**esign point distribution func, **R**eview events types, **A**ward points, **A**ward related honors.	**C**ontact the administrator offline to obtain information about sponsored users, **C**ontact users offline to invite them to participate in activities and give them relevant rewards, **U**pload related events to the chain.	**P**rovide users services (point cost), **S**ubmit points to admin regularly.

Design Framework:

- The design framework of the project includes the following four points: front-end, back-end, middleware, and smart contract. Its functions are described as follows:

front-end	back-end	middleware	smart contract
Each role obtains data from the blockchain, processes the data, and uploads the data to the chain.	Store data for recall.	Unblock the front end and smart contracts.	Set a set of operating specifications so that all participants in the chain must strictly abide by it.

東南大學
SOUTHEAST UNIVERSITY

04

Prospects for Possible Cooperation Directions of Smart City

止于至善

Prospects for Possible Cooperation Directions of Smart City

Encrypted traffic detection

Privacy data protection

Behavior supervision

Encrypted traffic detection:

- In the process of building the smart city, criminals may use the anonymity and immutability of the blockchain to release harmful information. Therefore, it is necessary to identify and trace the source of on-chain traffic, especially encrypted traffic.

Behavior supervision:

- Supervision must exist in all important links of building the smart city. When the data in the chain is ciphertext, the regulatory agency should consider how to efficiently implement regulatory actions.

Privacy data protection:

- Core sensitive information must be properly protected. This is extremely important for the safe and stable development of smart cities.

Thank you!

School of Cyber Science & Engineering,
Southeast University, China
Xiaoyan Hu

29 October 2020

止于至善