Evaluation Trust Model of Block Chain Information Capacity Based on Subjective Logic

Liu Zhenjun[1], Fan Yaoguo[2], Wang Yong[3], Miao Zengliang[4], Sun Yongjun[5], Miao Xuepei[4]

[1]LuoLong Area Military Civilian Road No.16, Luoyang, China

[2]Zhongshan West Road No.691 10-4-102, Shijiazhuang, China

[3]Greate Wall Street Beautiful Government River, Baoding, China

[4]54 Way No.1705, Baoding, China

[5]Zhongshan West Road No.691 104-1-201, Shijiazhuang, China

375990172@qq.com

Keywords: Block Chain, Distributed Network, Subjective Logic, Privilege Control

Abstract: This paper analyses the technical characteristics and working principle of Block Chain, combines with distributed network nodes and refers to Information Capability Evaluation System, studies the implementation principle and complexity of these methods, summarizes their suitable environment and advantages and disadvantages, and proposes a Evaluation Trust Model of Block Chain Information Capacity Based on Subjective Logic (ETMBCIC-SL). This model introduces Jøsang's Subjective Logic to detect the block chain accounting behavior, so as to solve the dynamic trustworthiness problem of the Block Chain's privilege control, and dynamically detect the Block Chain privilege control through independent viewpoint and dependent viewpoint. The simulation results show that the model has high Completeness, Accuracy and Instantaneity.

1. Introduction

Block Chain is a distributed ledger, which consists of a series of data blocks connected in time-stamp order. Each block of data in the ledger contains information of multiple effective transaction confirmations between network nodes. Through consensus mechanism and cryptography, it is guaranteed that the ledger cannot be changed or forged[1].A Block Chain ledger is maintained by distributed peer nodes that collectively form the Block Chain Network, and each node has a local backup of the ledger[2].Block chain technology had been as the key technical support of the application of the Bitcoin, but the success of the Bitcoin makes Block Chain technology is valued by educational world, now Block Chain technology is extracted from the currency, in the areas outside of the Bitcoin, it has been widely applied[3], and plays an important role in the new field, bring new technology revolution, and it has made some breakthrough.

Information Capability mainly includes three aspects: Information Acquisition Capability(IAC), Information Processing Capability(IPC) and Information Transmission Capability(ITC). Therefore, Information Capability is embodied in the whole process of collection, processing and transmission. As shown in Figure 1.

  DOI: 10.25236/isaicn.2019.083

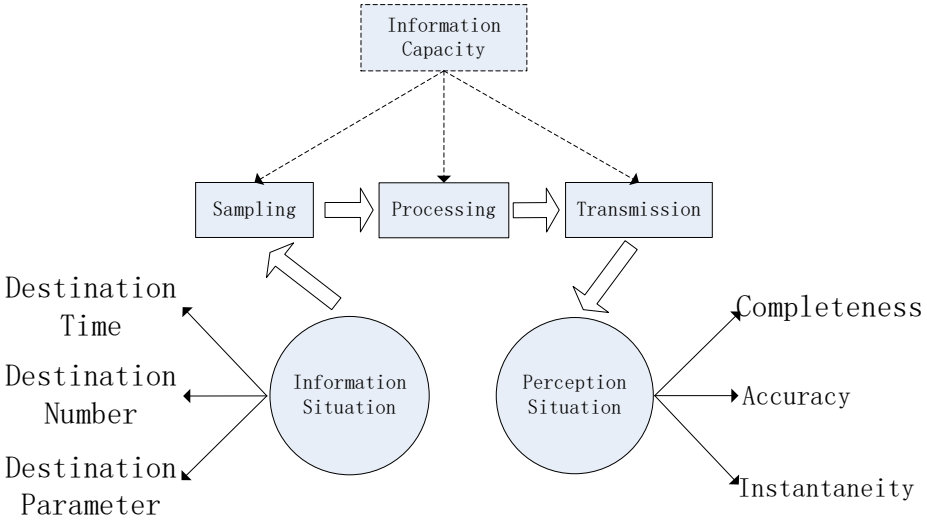

Figure 1 Information Capacity Model

Focusing on these problems, this paper proposed an Evaluation Trust Model of Block Chain Information Capacity Based on Subjective Logic, ETMBCIC-SL.

2. The Key Technology

2.1 The Technology of Block Chain

Block Chain is a kind of special data structure that connects data blocks end to end according to logical order. Encryption algorithm is used to ensure that internal transaction information cannot be tampered with or falsified. It is a decentralized ledger. Block Chain instead of the common key access to the data access mode, but to adopt chain structure and is validated by calculating block data, through consensus and voting mechanism to generate and load the new the block, using encryption algorithm to improve the reliability of message transmission process, intelligent contract can be formed through digital code management data of disruptive distributed control architecture[4]. It can completely store the transaction records of virtual currency or other interactive data, and the relevant data cannot be falsified or altered. Since the Block Chain can automatically execute the contract code, it does not need the intervention of the authoritative and centralized auditing unit. Recorded transaction information can be not only virtual currency like Bitcoin, but also various virtual assets like stocks and cultural interests. Block Chain technology has solved the problem of Byzantine generals, greatly reduced the trust cost and accounting cost in the real economy, and redefined the property rights system in the Internet Ara.

2.1 The Technology of Block Chain

2.1.1 Equality Network

The role of P2P in the Block Chain is to connect all nodes, so that any pair of nodes can establish interconnection communication without relying on a third party, and transmit data and information in the situation of broadcasting, so that the system can operate normally[5].

2.1.2 Encryption Algorithm

Based on the principles of cryptography, Block Chain technology enables communication between any two nodes and solves the problem of communication credit. In the traditional world, it is common to issue e-certs, provide electronic signatures, and hold public keys. The asymmetric encryption algorithms used in Block Chain include elliptic curve encryption algorithm and RSA signature algorithm. The RSA signature algorithm stores the block in a Json file, and then strings it into a string. After segmentation, the data is encrypted with RSA encryption algorithm and sent out one by one, and the generated public key is sent out at the same time when the data is sent out. This design is shown in Figure 2:

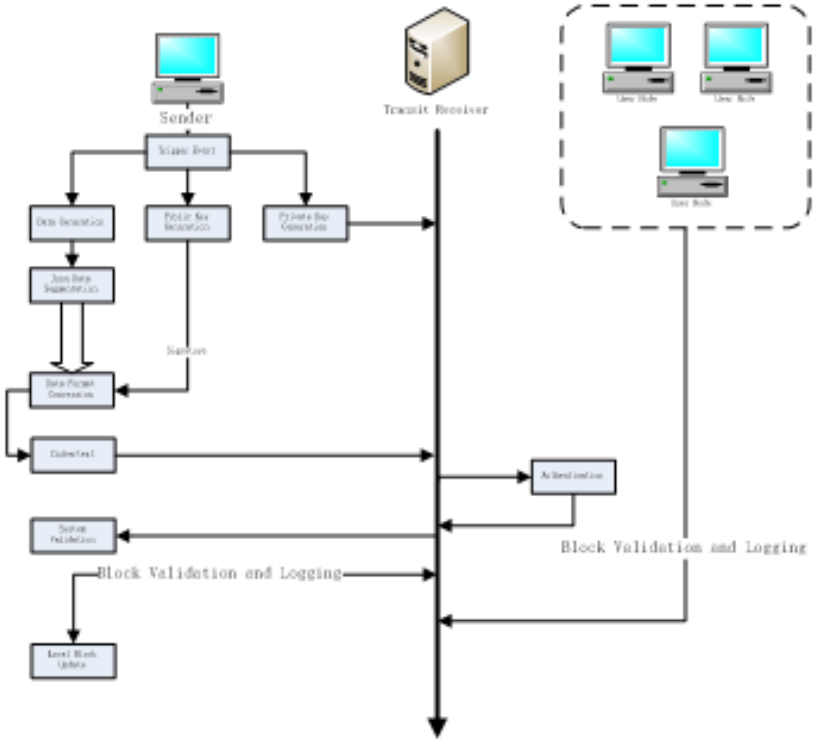

Figure 2 The Signature Process

2.1.3 Hash Algorithm

Secure hash algorithm (SHA) is a commonly used data encryption algorithm. It was published by the national institute of standards and technology (NIST) as a federal information processing standard (sha-0) in 1993. In 1995, its improved version sha-1 was also officially released[7]. SHA algorithm is the most commonly used security hash algorithm and the most advanced encryption technology. The general idea of a hash algorithm is to take a piece of clear text and convert it in an irreversible way to a (usually smaller) ciphertext and convert them into a shorter, fixed-digit output sequence, namely the hash value (called the information digest). The algorithm produces 160-bit message digest output for messages up to 264 in length, and the input is processed in groups of 512 bits.

3. ETMBCIC-SL Trust Model

3.1 Construction of Block Chain Trust Network

Suppose X is a block chain identification framework containing k disjoint propositions $X_i(i=1,2,...,k)$. Firstly, the trust relationship of identification framework X is constructed. As shown in Figure 3, if trust entity A wants to know the trust opinion of identification framework X, then entity A will send A request to entity B who has interacted with it, asking if B has A trust opinion of identification framework X. In order to obtain an accurate view of trust in X, B will also make A request to other n entities a_1, a_2, . . . , a_n that have interacted with it, asking whether they have A view of trust in X. Then entity B will integrate the view of n entities obtained by asking and its view of X and recommend it to entity A.

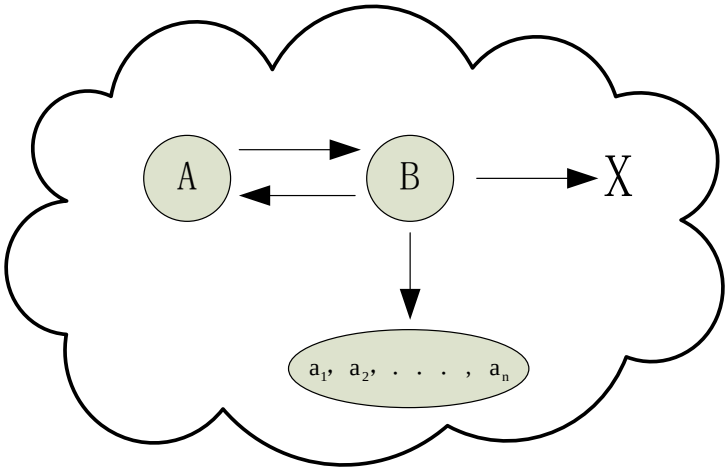

Figure 3 Building a trust relationship

3.2 Independent Opinion

It is assumed that two entities observe the Block Chain identification framework X at different time periods and the viewpoints obtained are mutually independent.

(1) Credibility-based fusion operation for two independent Dirichlet density functions.

Let $\varphi(r_X^A, a_X^A)$ and $\varphi(r_X^B, a_X^B)$ respectively represent the polynomial Dirichlet density function of entity A and entity B for X, rep^A is the reputation value of entity A, rep^B is the reputation value of entity B, the fused Dirichlet density function is $\varphi(r_X^{A\Diamond'B}, a_X^{A\Diamond'B})$, and is defined as:

$$\begin{cases} r_{X_i}^{A\Diamond'B} = R^A r_{X_i}^A + R^B r_{X_i}^B \\ a_{X_i}^{A\Diamond'B} = \dfrac{R^A \sum_{i=1}^{k} r_{X_i}^A}{R^B \sum_{i=1}^{k} r_{X_i}^B + R^A \sum_{i=1}^{k} r_{X_i}^A} a_{X_i}^A + \dfrac{R^B \sum_{i=1}^{k} r_{X_i}^B}{R^B \sum_{i=1}^{k} r_{X_i}^B + R^A \sum_{i=1}^{k} r_{X_i}^A} a_{X_i}^B \end{cases}$$

Where, $R^A = \dfrac{rep^A}{R}$, $R^B = \dfrac{rep^B}{R}$, Dirichlet density function $\varphi(r_X^{A\Diamond'B}, a_X^{A\Diamond'B})$ represents the R of reputation of virtual entity [A,B].The choice of R value is in the initial case, the credit value of each entity is the same base rate credit value of all entities, in this R take 0.5 or the average of two credit values.

(2) A credibility-based fusion operation for independent viewpoints.

Let $\omega_X^A = (b_X^A, u_X^A, a_X^A)$ and $\omega_X^B = (b_X^B, u_X^B, a_X^B)$ represent the trust views of entity A and entity B on X respectively, and view $\omega_X^{A\Diamond'B} = (b_X^{A\Diamond'B}, u_X^{A\Diamond'B}, a_X^{A\Diamond'B})$ represents the credibility-based fusion of ω_X^A and ω_X^B, which can be regarded as the polynomial views of virtual entity [A,B] on x.

$$\begin{cases} b_{X_i}^{A\Diamond'B} = \dfrac{R^A b_{X_i}^A u_X^B + R^B b_{X_i}^B u_X^A}{K} \\ u_{X_i}^{A\Diamond'B} = \dfrac{u_X^A u_X^B}{K} \\ a_{X_i}^{A\Diamond'B} = \dfrac{R^A a_{X_i}^A u_X^B + R^B a_{X_i}^B u_X^A - (R^A a_{X_i}^A + R^B a_{X_i}^B) u_X^A u_X^B}{R^A u_X^B + R^B u_X^A - (R^A + R^B) u_X^A u_X^B} \end{cases}$$

Where, $K = R^B u_X^A + R^A u_X^B + (1 - R^A - R^B) u_X^A u_X^B$, and $K \neq 0$.

When K=0, that is, ω_X^A and ω_X^B are completely certain views, then

$$\begin{cases} b_{X_i}^{A\Diamond'B} = \gamma^A b_{X_i}^A + \gamma^B b_{X_i}^B \\ u_{X_i}^{A\Diamond'B} = 0 \\ a_{X_i}^{A\Diamond'B} = \gamma^A a_{X_i}^A + \gamma^B a_{X_i}^B \end{cases}$$

Where

$$\begin{cases} \gamma^A = \lim\limits_{\substack{u_X^A \to 0 \\ u_X^B \to 0}} \dfrac{R^A u_X^B}{R^A u_X^B + R^B u_X^A + (1 - R^A - R^B) u_X^A u_X^B} \\ \gamma^B = \lim\limits_{\substack{u_X^A \to 0 \\ u_X^B \to 0}} \dfrac{R^B u_X^A}{R^A u_X^B + R^B u_X^A + (1 - R^A - R^B) u_X^A u_X^B} \end{cases}$$

3.3 Dependent Opinion

(1) Credibility-based fusion operation for two completely dependent Dirichlet density functions.

Let $\varphi(r_X^A, a_X^A)$ and $\varphi(r_X^B, a_X^B)$ represent the Dirichlet density function of entity A and entity B on X respectively. These two probability density functions are completely dependent on each other. The fused Dirichlet density function $\varphi(r_X^{A\underline{\Diamond}'B}, a_X^{A\underline{\Diamond}'B})$ is defined as:

$$\begin{cases} r_{X_i}^{A\underline{\Diamond}'B} = \dfrac{R^A r_{X_i}^A + R^B r_{X_i}^B}{2} \\ a_{X_i}^{A\underline{\Diamond}'B} = \dfrac{a_{X_i}^A + a_{X_i}^B}{2} \end{cases}$$

Using the above definition and mapping between the viewpoint space and the fact space, the following operations can be obtained.

(2) For credibility-based fusion operations of dependent viewpoint.

Let $\omega_X^A = (b_X^A, u_X^A, a_X^A)$ and $\omega_X^B = (b_X^B, u_X^B, a_X^B)$ represent the trust viewpoint of entity A and entity B respectively in the block chain observation and identification framework X at the same time, and view $\omega_X^{A\underline{\Diamond}'B} = (b_X^{A\underline{\Diamond}'B}, u_X^{A\underline{\Diamond}'B}, a_X^{A\underline{\Diamond}'B})$ represents the credibility-based fusion of ω_X^A and ω_X^B, which can be regarded as virtual entity [A,B] 's polynomial viewpoint about X.

$$\begin{cases} b_{X_i}^{A\underline{\Diamond}'B} = \dfrac{R^A b_{X_i}^A u_X^B + R^B b_{X_i}^B u_X^A}{K} \\ u_{X_i}^{A\underline{\Diamond}'B} = \dfrac{2u_X^A u_X^B}{K} \\ a_{X_i}^{A\underline{\Diamond}'B} = \dfrac{a_{X_i}^A + a_{X_i}^B}{2} \end{cases}$$

Where, $K = R^B u_X^A + R^A u_X^B + (2 - R^A - R^B) u_X^A u_X^B$, and $K \neq 0$.

When K=0,that is, ω_X^A and ω_X^B are completely specified viewpoint, then

$$\begin{cases} b_{X_i}^{A\underline{\Diamond}'B} = \gamma^A b_{X_i}^A + \gamma^B b_{X_i}^B \\ u_{X_i}^{A\underline{\Diamond}'B} = 0 \\ a_{X_i}^{A\underline{\Diamond}'B} = \gamma^A a_{X_i}^A + \gamma^B a_{X_i}^B \end{cases}$$

Where

$$\begin{cases} \gamma^{A} = \lim\limits_{\substack{u_X^A \to 0 \\ u_X^B \to 0}} \dfrac{R^{A} u_X^B}{R^{A} u_X^B + R^{B} u_X^A + (2 - R^{A} - R^{B}) u_X^A u_X^B} \\ \gamma^{B} = \lim\limits_{\substack{u_X^A \to 0 \\ u_X^B \to 0}} \dfrac{R^{B} u_X^A}{R^{A} u_X^B + R^{B} u_X^A + (2 - R^{A} - R^{B}) u_X^A u_X^B} \end{cases}$$

At a certain moment, the independent viewpoint fusion and dependent viewpoint fusion are used to get the subjective evaluation of ω, which is compared with the critical ω, so as to judge whether the blockchain node is credible. If trusted, record the ledger; Otherwise, abandon the record.

4. Simulation Experiment and Result Analysis

This system uses four physical hosts to build the experimental environment. The specific host information is shown in Table 1:

Table 1 Host Information Table

CPU	Memory	Hard Disk
Intel(R)Core(TM)i5-3470 CPU 3.20GHz	4G	250G
Intel(R)Core(TM)i5-3470 CPU 3.20GHz	4G	250G
Intel(R)Core(TM)i5-3470 CPU 3.20GHz	4G	250G
Intel(R)Core(TM)i5-3470 CPU 3.20GHz	4G	250G

The software is shown in Table 2:

Table 2 Software Usage Table

Purpose	Name	Version
Operation System	Windows7 64 bit	6.1.7601
IDE	Eclipse	4.7.0
DataBase	MySQL	5.5.48
Custom Network	Geth	1.5.9

4.1 Successful Case

Case Input: the device requests the platform to obtain resource information through the gateway, including operation type, device name, platform id of the device, platform id of the device to which the resource is requested, request resource level, request resource start timestamp and request resource end timestamp. The json information is as follows:

```
"inputs":[{
            "opoerate":"query",
             "deviceNmae":"phone_zb",
             "platformId":"QRot0YXxXH0zGynw",
              "queryDevicedId":"I80r2mTUppNk7C78",
             "dataLevel":"",
             "startDate":"1513259100",
             "endDate":"1513259110"

         }]
```

Test results: the platform passed the authorization of the device and sent the resources to the device.After viewing the permission information of the device "QRot0YXrXH0zGynw", the device has the right to read the device "I8O2mTUppNk7C78". After the platform obtains the information of the device "I8O2mTUppNk7C78", it sends the information of the starting and ending time period

to the device requesting the resource.

4.2 Failure Case

Case Input: the device uploads resource request information to the platform through the gateway, including operation type, device name, platform id of the device, platform id of the device to which the resource is requested, request resource level, request resource start timestamp and request resource end timestamp. The json information is as follows:

"inputs":[{
"opoerate":"query",
"deviceNmae":"phone_thq",
"platformId":"hny9dsmOt2Ah2NUu",
"queryDevicedId":" QRot0YXrXH0zGynw",
"dataLevel":"",
"startDate":"1513304925",
"endDate":"1513304935"
}]

Test result: the result of the platform's authorization for the device is not passed, and the platform refuses to issue resources to the device. After checking the permission information of the device "hny9dsmOt2Ah2NUu", the device does not have the right to read the resource of the device "QRot0YXrXH0zGynw". The platform refuses to send the information of the device "I8O2mTUppNk7C78" to the device requesting the resource. The information returned by the platform to the requesting device is as follows: result: failed; The message: "illegal operate".

4.3 Test Conclusion

Considering the influence of independent point of view and dependent point of view, the Information Capacity platform will issue the resource of the requested device to the device with permission, and refuse to return the information resource to the device platform with insufficient permission, and the test passes.

References

[1] Yang Yang, Jing Chun Yu. The prospect of digital currency of China's central bank based on blockchain technology [J].China Market, 2017(14:14-15)

[2] Shen X,Pei Q Q,Liu X F.Survey of block chain[J]. Chinese Journal of Network & Information Security, 2016.

[3] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. https://bitcoin.org/bitcoin.pdf.

[4] Li jun. Technology and law: dual track of blockchain financial development [J]. Journal of Shanghai lixin accounting and finance college, 2017,(03):54-59

[5] Chia-Cheng Hu,Chin-Feng Lai,Ji-Gong Hou,Yueh-Min Huang.Timely scheduling algorithm for P2P streaming over MANETs[J]. Computer Networks, 2017,127.

[6] shen xin, pei qing qi, liu xue feng. Overview of block chain technology [J]. Journal of network and information security, 2016, 2(11):11-20.

[7] Zhang song min, tao rong, yu guo hua. Research on security hashing algorithm sha-1 [J].Computer security, 2010, (10):3-5

[8] Jøsang A. The consensus operator for combining beliefs. Artificial Intelligence Journal, 2002, 142:157-170.