2021 21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter)

2021 21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter) | 978-1-6654-1843-0/20/$31.00 ©2021 IEEE | DOI: 10.1109/SNPDWinter52325.2021.00018

A Decentralized Copyright Protection, Transaction and Content Distribution System Based on Blockchain 3.0

Liming Liu
School of Computer Science and Cybersecurity
Communication University of China, Beijing, China
picpic2019@gmail.com

Wenqian Shang*
School of Computer Science and Cybersecurity
Communication University of China, Beijing, China
shangwenqian@163.com
*corresponding author

Weiguo Lin
School of Computer Science and Cybersecurity
Communication University of China, Beijing, China
linwei@cuc.edu.cn

Wei Huang
Division of Scientific Research
Communication University of China, Beijing, China
huangwei910@cuc.edu.cn

***Abstract*—The current copyright protection and copyright transactions have problems such as high platform fees, opaque transaction information, difficulty in copyright protection, and slow speed. The current interplanetary file system has gaps in file-sharing; Most blockchain frameworks do not use national secret algorithms, which causes security uncertainty. This system uses smart contract accounts to define copyrights, uses multi-person accounts to define cooperation, treats copyright deposits from the perspective of transactions, and uses many fully automatic key "center" to be responsible for the key distribution of encrypted files, which can reduce the single point pressure of the copyright center server, reduce the negative impact of single-point invalidation of the copyright center on transactions and reduce the review time. We also achieved decentralized copyright transactions and secret key transmission. By using national secret algorithms for encryption, signature, and hashing, we can get rid of excessive dependence on foreign algorithms.**

Keywords—Decentralization, secret key transmission, copyright protection, copyright transactions, blockchain

I. Introduction

A. National Secret Algorithm

A cryptographic algorithm is the core technology to ensure information security, and the security of blockchain technology relies on cryptographic security. Blockchain has long used internationally accepted cryptographic algorithm systems and related standards such as SHA and RSA. To fundamentally get rid of the excessive dependence on foreign cryptographic technology and products, the State Cryptography Administration announced the "elliptic curve public key cryptographic algorithm" (SM2) at the end of 2010 which is independently developed by the Chinese government. To ensure the security of cryptographic applications in critical systems, the State Cryptography Administration requires that since July 1, 2011, information systems that are put into operation and use public-key cryptography should use the SM2 algorithm.

SM2 Signature Algorithm Steps [1]:

A1. set $\overline{M} = ZA \,||\, M$

A2. $integer\ e = HV(\overline{M})$

A3. $random\ k \in [1, n-1]$

A4. $(int(x_1), y_1) = kG$

A5. $r = (e + x_1) mod\ n$ if r == 0 || r + k == n then go to A3.

A6. $s = (1 + dA) - 1 \cdot (k - r \cdot dA) mod\ n$ if r == 0 then go to A3.

A7. Signature is (r, s)

For the message M' and its signature (r', s'):

B1. $check\ r' \in [1, n-1]$

B2. $check\ s' \in [1, n-1]$

B3. set $\overline{M'} = ZA \,||\, M'$

B4. $integer\ e' = HV(\overline{M'})$

B5. $s' = integer(s'), r' = integer(r')$
$t = (r' + s') mod\ n$ if t == 0 then fail.

B6. $(x_1', y_1') = s'G + tPA$

B7. $x_1' = integer(x_1'), R = (e' + x_1') mod\ n$ if $R = r'$ then success.

B. Current Status of Blockchain Development

After Bitcoin [2] and Ethereum [3], the blockchain has moved from digital payments and transfers to programmable applications, and extends to asset types such as stocks, bonds, and loans, while developing autonomous organizations and smart contracts. The function is more and more powerful. At this stage, blockchain technology is providing professional and technical program services for all walks of life. As a result, Blockchain as a Service (BaaS)[5] has become an important part of the blockchain economy and can bring more value. BaaS embeds the blockchain architecture into the cloud service platform and uses the deployment and management advantages of cloud services to provide developers with a convenient and high-performance blockchain ecological environment and supporting services. The BaaS platform facilitates the creation, deployment, operation, and monitoring of the blockchain, and can provide a series of operational services such as blockchain-based search queries, task submission, and so on. There are advantages in saving costs, lowering the threshold of use, and improving system security.

C. InterPlanetary File System

Inter-Planetary File System (IPFS) [4] is a peer-to-peer distributed file system that tries to connect the same universal file system for all computing devices. In some respects, IPFS is like the World Wide Web, and it can also be seen as an independent BitTorrent group, exchanging objects in the same

978-1-6654-1843-0/21/$31.00 ©2021 IEEE
DOI 10.1109/SNPDWinter52325.2021.00018

Git repository. In other words, IPFS provides a high-throughput, content-addressable block storage model, and content-related hyperlinks. This forms a generalized Merkle directed acyclic graph (DAG). IPFS combines distributed hash tables, encouraging block exchanges, and self-certified namespace. IPFS has no single point of failure, and nodes do not need to trust each other. Distributed content delivery can save bandwidth and prevent DDoS attacks that HTTP schemes may encounter.

The file system can be accessed in many ways, including FUSE and HTTP. Adding local files to the IPFS file system makes it available to the world. File representation is based on its hash, which is good for caching. The distribution of files uses a BitTorrent-based protocol. Other users who view the content also help provide the content to others on the network. IPFS has a name service called IPNS, which is a PKI-based global namespace used to build a chain of trust, which is compatible with other NSs and can map DNS, .onion, .bit, etc. to IPNS.

D. Verifiable certificates

Verifiable certificates (VC) can establish trust between parties by using a set of tamper-proof statements and metadata, which can be used to cryptographically prove the identity of the holder and the identity of the issuer. More importantly, by using this method, users can retain their data when they receive a request, and it is very easy and simple to share a verified certificate with the other party.

E. Disadvantages of Centralized Copyright Deposit and Trading

Once the center is attacked, it is easy to cause evidence to be lost or tampered with. In the forensics stage, once the evidence leaves the original equipment, it becomes replicable and cannot be a basis for a verdict. Therefore, when obtaining electronic evidence, it is necessary to freeze the computer, hard disk and other equipment and the work itself for inspection, which results in the copyright being locked and the transaction cannot be carried out, which in turn leads to damage to the normal work and interests of the person under investigation. In addition, because electronic evidence can be tampered with and copied easily, the benefits of such electronic evidence are extremely low.

Electronic data is very difficult to identify the evidence due to its large amount, strong real-time, high storage cost, and difficulty in identifying the original. Therefore, it is difficult for such evidence to play a decisive role in supporting the case. And because the depository center needs to store evidence with high reliability, the equipment used by the depository center is specially made and extremely costly. Even far higher than the price of ordinary computer clusters, greatly increasing the cost of deposits.

Centralized transactions are faced with unsupervised data replication. When obtaining data, they are only authenticated by the central node. The security is low and the pressure on the central node is greater. Moreover, the transparency of the central platform to users is limited, and there are problems such as the arbitrary collection of fees, which users have no way of knowing.

Due to the distrust between nodes, the file must be encrypted before being transferred to IPFS. Because of the lack of a secret key transmission mechanism, even if the transaction is successful, it is difficult to transmit works in a decentralized environment without human intervention.

F. Solution

This article aims to introduce an automated and decentralized key "central" node to realize a decentralized key transmission mechanism, and at the same time solve the decentralized copyright storage and transaction issues and enable the copywrite to be traded during the publicity period.

Take the publishing, trading, and reporting of piracy of a work jointly completed by A, B, and C as an example. First, create a multi-person account, which records the creation and division of labor information and profit distribution strategy. Then create a copyright account, which records the author, work citations, etc. At this time, the political review variable of the copyright account is false, which means that the work has not yet passed the political review, and dissemination is prohibited. If A, B, and C only needs to deposit certificates on the chain, then the goal has been achieved. If ABC wants the work to enter the global material library and can be traded and disseminated, it needs to encrypt the work with the key K and upload it to IPFS. Then, encrypt the symmetric key K with the public key of the key "center" that A, B, and C all trusted and write the encrypted key into the relating variable of the copyright account. After that, ABC can initiate a political review application and wait for political review by the Copyright Center. When the political review is passed, the publicity period is entered, the material center will automatically put the work in the library, display and sell the work. When a user purchases this work, a transaction needs to be initiated to this copyright account. The money collection contract will check all cited works of this copyright. If the cited work requires partial income, the copyright account will initiate a transaction to the account of the cited work, giving enough money required by the cited work. After deduction, the remaining income will be locked in the copyright account, waiting for the end of the publicity period. After the publicity period ends, author A can call the withdrawal contract of the multi-person account, and the multi-person account will call the withdrawal contract of the work, transfer the proceeds to the multi-person account, and distribute it proportionally. Finally, a transaction is initiated to A's account, and the amount is all the income that A deserves.

This brings many benefits. If the copyright is reported, the buyer's trading behavior will not be affected when the evidence is locked. If a copyrighted work is reported during the publicity period and the report is successful, the original author can obtain the full revenue of the copyright; if the copyright publicity period has expired, the original author can obtain all the proceeds after the report. The system also has advantages such as obtaining dominant evidence, decentralized identity verification and certificate distribution, peer-to-peer transactions without middlemen, and so on. The system adopts a micro-service architecture, a physical computer can deploy multiple software roles, or a distributed cluster can be used to deploy a single role. It allows users to make full use of idle computing and storage resources to contribute to decentralized copyright transactions; it also allows companies to use only cheap civilian-grade equipment to build a highly reliable and secure transaction network with good nodes fault tolerance, which can greatly reduce the purchase cost of highly reliable equipment. This system uses a basic data structure similar to Ethereum, uses MPT trees to ensure data synchronization between blockchain nodes, and uses PoW [2] or PoS [3] to ensure the security of the blockchain system. At the same time, it supports the alliance chain and private chain protocol, which is more secure and flexible. This system transmits sensitive data through asymmetric encryption, uses threshold signatures for joint reporting of multi-person works, uses verifiable certificates and decentralized identities for authority and identity verification, and stores and distributes copyrighted works through the interplanetary storage file system.

II. Architecture

A. Blockchain layer

This system uses the same data structure and consensus protocol as Ethereum, and accounts are divided into multi-person accounts and copyright accounts. The most important data structure of this system is the account which uses the MPT tree to maintain and organize, and the root hash is stored in the blockchain header. Accounts are divided into external accounts and contract accounts. An external account is also called a single-person account, which maintains the user's balance; the contract account consists of a code segment and a storage segment. The code segment is interpreted and executed by the system virtual machine. Each blockchain node maintains a copy of the state tree, and use the consensus protocol to maintain the consistency of the state tree.

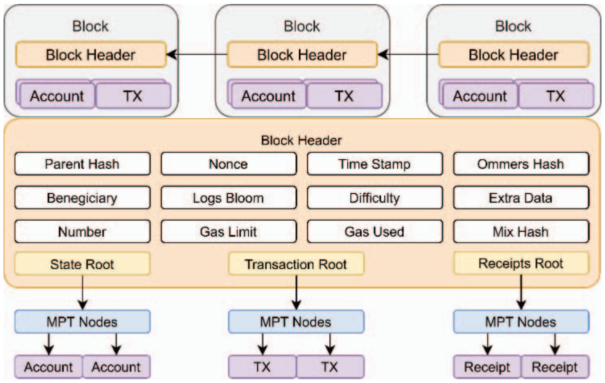

Figure 1. Data Structure Overview

1) Multi-person Account

When work is completed by multiple people, the record of the division of labor and asset allocation are challenging. To unify the data structure of the system, the concept of multi-person accounts is introduced.

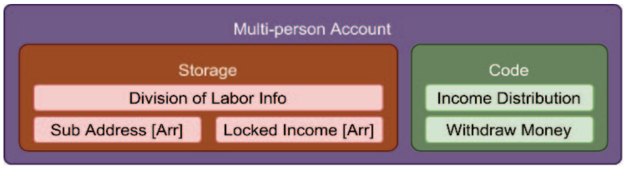

Figure 2. Multi-person Account Data Structure

a) Storage Segment

• **Division of Labor Info**: A string that records the contributions of all authors to the work, used for evidence.

• **Sub Address**: The address of each individual account that makes up this multi-person account.

• **Locked Income**: Record the amount that each sub-author can get from this multi-person account.

b) Code Segment

• **Income Distribution**: the predefined profit distribution method when creating a multi-person account.

• **Withdraw Money**: The contract will take out all the income locked by the copyright, and then call the income distribution contract to split and store the income into the "Locked Income" array corresponding to each sub-account address. Finally, the income of a single author is transferred to the corresponding author's personal address.

2) copyright account

This system uses smart contract accounts to define copyright. The storage part records the copyright owner, usage rights, review status, piracy status, price, etc. When copyright is being preserved as evidence, traded, audited, reported as piracy or it is doing identity verification or certificate verification, the corresponding smart contract will be called to achieve those specific functions.

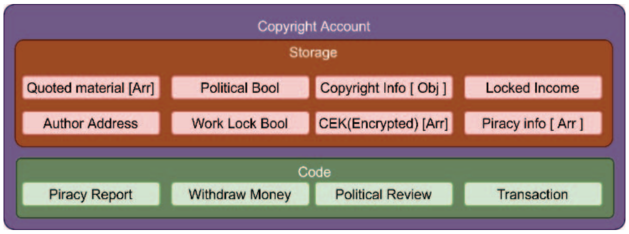

Figure 3. Copyright Account Data Structure

a) Storage Segment

• **Quoted material**: All material addresses cited in this work.

• **Author Address**: Indicates the original author of the work. If it is an individual creator, this variable would be the author account address; if it is a joint creation by multiple people, this variable would be the address of the multi-person account.

• **Political Bool**: When set to false, it means that it has not passed political review and cannot be sold, IPFS cannot provide file streams, and the key center cannot provide secret keys. When set to true, it means that it has passed political review and can be traded freely.

• **Work Lock Bool**: This variable is set to true when the work is just uploaded. After the political review, it enters the publicity period and is still true. At this time, the work can be traded, but all the income obtained by the exchange are locked in the work contract and cannot be withdrawn. When the publicity period expires, the value is set to false by the Copyright Center, and the author can withdraw the proceeds through the withdrawal contract. When the work is reported as piracy, this value is set to true. After the work is reviewed, this value is set to false.

• **Copyright Info**: Including the hash value of the work, the copyright price, the IPFS storage address, the right to use, the right to copy, the right to edit, etc. For example, after work A is quoted by work B when work B obtains income, it needs to be transferred to work A’ s income 10%.

• **CEK(Encrypted)**: The decryption symmetric key of the encrypted file stream in IPFS is encrypted using the asymmetric public key of the key "center". The same symmetric key is encrypted using the public keys of multiple key "centers" and stored in this array respectively. For the use of load balancing and high availability.

• **Locked Income**: Untaken proceeds obtained from the work.

• **Piracy Info**: It is used to store the variables required by the piracy report contract, which contains the IPFS address of the pirated evidence, the decryption key of the pirated evidence, the address of the reporter, the deposit paid by the reporter when reporting, etc.

b) Code Segment

• **Piracy Report**: The contract locks the deposit provided by the reporter in the pirated information variable; then, according to the provided URL or file address of the pirated work, the smart contract takes a snapshot of the pirated work, uploads it to IPFS, use CEK to encrypt pirated evidence, and then use the public key of the key "center" to encrypt CEK and store it in the "Piracy Info" variable. Finally, the contract set the "Work Lock Bool" variable to true. If the work itself is in the publicity period, the contract will force the copyright to extend the publicity period.

• **Withdraw Money**: The contract first determines whether the work is locked. If it is not locked and the function caller has the right to obtain the balance, then all the locked balance will be transferred to the author's account.

• **Political Review**: After the political review of the work is successful, the copyright center will call this smart contract. The contract first determines the identity of the center. If it is a legal organization, the "Political Bool" variable of the work will be set to true.

• **Transaction**: The contract first judges the copyright's "Political Bool" variable. If it has passed the political review, it judges the saleable variable in the copyright information of the work. If it can be sold, it initiates a transfer from the caller’s account to the copyright account, the price is stored in the "Copyright Info" variable. Then traverse the works cited in this work, and if the cited work requires corresponding benefits in the authority, initiate a transfer to it. Finally, the remaining amount is stored in the "Locked Income" variable. If all executions are successful, the authorization certificate is returned to the caller, which contains the key center address where the user can get CEK.

B. Node Roles

The nodes are divided into four roles:

• **User node**: a node composed of copyright authors and their computer equipment. Responsible for filling in copyright information and uploading copyright works. It needs a better user experience and a lower threshold for use.

• **Copyright Center Node**: A node composed of copyright reviewers and their computer equipment, responsible for the political review of works and the review of piracy reports.

• **Blockchain light/full node**: Responsible for storing and synchronizing account information, executing smart contracts, identity verification, and other functions. For nodes with only verification requirements, blockchain light nodes can be used; for nodes with writing requirements, blockchain full nodes are required.

• **Interplanetary File System node**: responsible for storing encrypted work files for review and dissemination. Since the physical nodes of the interplanetary file system do not trust each other, the content needs to be encrypted. Due to the difficulty in transmitting the secret key, the current IPFS system is mostly used to store user personal data. This system proposes a set of secret key transmission methods by introducing a secret key "center" and combining it with verifiable certificates.

The four roles can be deployed on any cheap computer, and one cheap computer can also run services for multiple roles. It is very flexible.

C. Physical Nodes and Software Architecture

The service of each role is a decentralized app, which consists of a front-end management interface, a back-end controller, a blockchain controller, and an IPFS controller. The front-end management interface is responsible for interacting with users, the back-end controller is responsible for authorization verification and business logic implementation, and the blockchain and IPFS controller are responsible for driving the local blockchain and IPFS nodes. Besides, the system can also be equipped with a central index node, which is composed of front-end, back-end, and database drivers, and is responsible for providing efficient material library indexing services. Although this node is a centralized server, it only provides material library indexing and acceleration functions. The rest works like the authorization verification, work storage, and transmission, copyright deposit, transaction records are all run and stored in a decentralized environment.

III. Core Functions

A. Decentralized Key and Content transmission

Obtain IPFS content: Because the nodes of Interplanetary Storage do not trust each other, the works cannot be stored in IPFS in plaintext; and the size of the works may be large, and the speed of all asymmetric encryption is slow, so this system adopts both symmetric Encryption and asymmetric encryption methods. We first use symmetric encryption to encrypt the work, upload it to IPFS, and then use the public key of the key "center" to encrypt the symmetric secret key and write it in the copyright CEK variable.

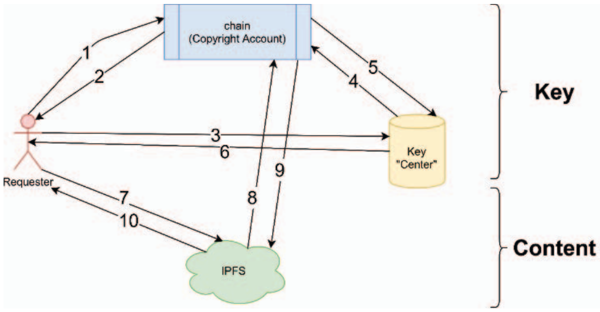

Figure 4. Process of Obtaining IPFS Files

Therefore, when users obtain copyrighted works, they need to obtain the file content from IPFS and then obtain the decryption key from the blockchain system. The overall process is divided into the following 11 steps:

1. The user initiates a transfer transaction to the copyright account.
2. The copyright account verifies transactions and issues a license(CA) to allow the user to obtain content.
3. User sends a request to the key "center" with the license.
4. The key "center" verifies the authenticity of the license in the blockchain.
5. The secret key "center" obtains the CEK encrypted with the secret key "center's" public key from the copyright account, and decrypts it, but does not store it.
6. The key "center" encrypts the CEK with the requester's public key and returns it to the requester; the requester uses its private key to decrypt the CEK.
7. The requester sends a request to IPFS with the license.
8. IPFS verifies the authenticity of the license on the blockchain.
9. Blockchain returns the authentication result.
10. If the license is valid, IPFS will provide the encrypted work to the requester.
11. The user uses the received CEK to decrypt the encrypted file to get the original file.

Note 1: There is more than one secret key "center". The copyright account can store multiple CEKs that encrypted each secret key "center's" public key. Any secret key center can transmit CEK, so it can effectively prevent a single point of excessive pressure or a single point of failure. The total amount of the "center" can be arbitrarily specified according to needs and the "center" server can just use civilian-grade cheap equipment to reduce costs.

Note 2: The Copyright Center also needs to obtain the original file from IPFS when reviewing. The copyright center has a super administrator certificate, so it can skip step 1 and step 2.

Note 3: The secret key "center" is a semi-centralized device and its security is guaranteed by cryptography. After the public and private keys are solidified in the device, they can run automatically. There is no human intervention and no secret key is stored. It only does secret key analysis and re-encryption.

B. Copyright Deposit

1) Genuine Certificate

The genuine certificate is to create a copyright account, encrypt the work with the symmetric secret-key CEK, upload it to IPFS, encrypt the CEK with the public keys of multiple key centers, store it in the CEK variable of the copyright account, and notify the copyright center to conduct a political review.

2) Piracy Deposit

That is, call the Piracy Report contract of the copyrighted work, provide it with the URL or file address of the pirated work, and initiate a piracy report review request to the copyright center.

C. Review

1) Political Review

When the copyright center processes the political review request, it first looks up the CEK variable of the copyright account on the chain and uses the private key of the secret key "center" to decrypt it (the private key of the secret key "center" is issued by the copyright center) to get the real CEK. Then request the work from IPFS, decrypt it with CEK, and review it. If the review is passed, the Political Review contract of the copyright account is called. After the political review is passed, if the "Index Agree" variable in the "Copyright Info" is true, the work will be displayed in the central material index library for other users to view and purchase.

2) Piracy Report Review

The Copyright Center uses the same method as a political review to obtain user works and evidence of piracy when processing a request for review of a piracy report. After the review, if the review is passed, the author's address of the copyrighted work will be compulsorily modified, and the reporter's deposit will be returned. If the review fails, the reporter's deposit will be transferred to the work's "Locked Income" variable.

D. Copyright Transaction

Users can search and browse materials in the material library, and when they encounter required materials, they can initiate a transaction request for legal materials. Users can purchase and download original materials through the 11-step process. After cited those works, you need to declare all referenced materials.

1) Chain Transaction

When calling the transfer contract, the contract will check the permission requirements of the cited work, and automatically allocate the required income to the account of the cited work.

2) Multi-User Trading

When the work is completed by multiple people, the user division of labor and the distribution of user benefits are completed by the multi-person account. In the work contract, the multi-person account and the single-person account are treated in a unified manner.

IV. Conclusion

This system uses the national secret algorithm. By introducing an automated copyright "center", it solves the problem of key transmission in decentralized scenarios. By looking at copyright protection from the perspective of a transaction, it solves the problems of copyright's uploading, review, transaction, reporting, and distribution in the decentralized scenario. Transactions can be done during the publicity period and the lock-up period. Point-to-point payments are available, which needs a low handling fee. Based on the decentralized concept, the system is high tolerance to single-point failure and is low equipment cost. The system can solve chain transactions and multi-person income distribution problems. There are many highlights of this system.

Acknowledgment

This work was supported by National Key R&D Program of China (2018YFB0803701-1) and Fundamental Research Funds for the Central Universities.

References

[1] Rongyan Sun, Changshu Cai, Zhou Zhou, Yanjie Zhao, Jinming Yang. Comparative Analysis and Research on National Secret SM2 Digital Signature Algorithm and ECDSA Algorithm [J]. Network Security Technology and Application,2013(02):60-62.

[2] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System [Online] available: https://bitcoin.org/bitcoin.pdf

[3] Ethereum White Paper. A next-generation smart contract and decentralized application platform [Online], available: https://github.com/ethereum/wiki/wiki/WhitePaper, November 12, 2015

[4] Juan Benet. IPFS - Content Addressed, Versioned, P2P File System available: https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf

[5] Yong Wang, Yuefei Wang. Current status and prospects of blockchain technology development [J]. Acta Automatica Sinica,2016,42(04):481-494.

[6] New kid on the blockchain[J] . New Scientist . 2015 (3009)

[7] Blockchain Monitoring Website [Online], available: https://blockchain.info/, January 8, 2016

[8] Cryptocurrency Monitoring Website [Online], available: http://coinmarketcap.com/, November 24, 2015

[9] CoinDesk Report [Online], available: http://www.bitcoin86.com/news/3527.html, February 21, 2016

[10] Fan Jie, Yi Le-Tian, Shu Ji-Wu. Research on the technologies of Byzantine system. Journal of Software, 2013, 24(6): 1346−1360

[11] Bitcoin Sourcecode [Online], available: https://github.com/bitcoin/bitcoin/, January 18, 2016

[12] Bitcoinmining Article [Online], available: https://www.bitcoinmining.com/bitcoin-mining-pools, December 8, 2015

[13] Factom White Paper [Online], available: http://bite01. com/bit/1421, December 29, 2015