Advances in Computer Science Research, volume 78

3rd International Workshop on Materials Engineering and Computer Sciences (IWMECS 2018)

Analysis of Consensus Mechanism Models in the Application of Industrial Projects Brought by Blockchain Technology

Yimin Qiu[1, a], Jia Fu[2, 3, b, *], and Weihui Lin[4, c]

[1] Shenzhen Nisen industrial co., LTD, Shenzhen 518115, China

[2] Southern University of science and technology, Shenzhen 518055, China

[3] Xi'an Shiyou University, Xi'an 710065, China

[4] Xi'an Jiaotong University, Xi'an, 710049, China

[a] 515655281@qq.com, [b] fujia@sustc.edu.cn, [c] linweihui@stu.xjtu.edu.cn

*Corresponding author: fujia@sustc.edu.cn

Keywords: Blockchain, decentralization, industrial chain, security architecture, application scenario.

Abstract: Based on ERC20 standard, industrial chain platform is developed, where numerical comparison of consensus mechanisms of POW and POS are analyzed and discussed. Besides, some basic concepts of block chain, such as its types, consensus mechanism and incentive mechanism were briefly introduced, combined with features of virtual users, the framework of industrial chain based on blockchain technology was developed. The technical realization of this framework was introduced, and the formulation of smart contract was added. Afterwards, specific applications of blockchain in dating scenario, transaction, settlement and physical constraints were illuminated. Challenges of blockchain's application in dating platform were discussed. The industrial chain aims to do more research and investigation on the design and implementation of blockchain technique, including security investigation for blockchain, related application of blockchain, the security architecture comparison of both blockchain security system and traditional centralized modes. The summaries for the advantages and disadvantages of consensus mechanism models in the application of industrial chain project brought by blockchain technology, and more actual application scenarios are derived.

1. Introduction

Since 2008, Satoshi Nakamoto has proposed the bitcoins, which has graduated as a new distributed, non-centralized and non-trust solution [1]. Blockchain has gradually gotten out of BitCoin as an independent innovation hot point [2-4]. It creating a new distributed data storage technology with an innovation change on system/program design. Min et al. [5] presents a Permissioned Blockchain Dynamic Consensus Mechanism (PBDCM) based multi-centers, each center has a peer blockchain that keeps itself transactions and global blockchain keeps the trusted transaction to link with multi peer blockchains to improve the performance of permissioned blockchain.

Blockchain contract can achieve a credible deal by all nodes stored in complete block chain. To improve the performance of block chain, bitcoins - NG [6] has extended the block capacity and transaction throughput by introducing the micro block, however, the problem of transaction latency and block chain branch have not been solved. Through the entire network nodes divided into different groups, SCP makes good use of work force to extend the throughput, etc. Andrew Miller [7] has used more reliable nodes to increase transaction throughput and to reduce network communication costs. But malicious nodes can use the more credible node to reduce the probability of rejection in the tamper block, which leads to the tamper with the data and makes the tamper effective. Christian Yoad Lewenberg [8] based on the directed acyclic graph to build the scalable block chain agreement to achieve a higher throughput. Decker [9] has proposed that the transaction support real-time trading

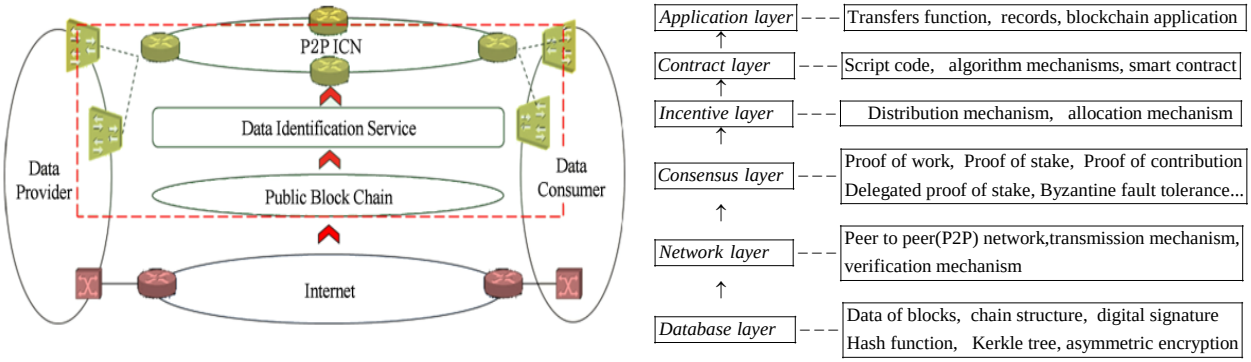
under the block chain, which aims to shorten trading delay by building trading channel between any two nodes without increasing the burden of the block chain network. Most research stays on the transaction speed of blockchain based on the measurement and simulation, without the quantitative research by the specific mathematical model. Based on the techniques mentioned above, we develop the industrial chain system, where functions are realized through smart contracts.

Simply speaking, the industrial chain system is a decentralized platform that runs smart contracts on the block chain. It is a piece of computer program running on a replicable, shared ledger, which processes, accepts, stores, and sends valuable information. Thus the whole smart contract on industrial chain system is an untampered program running on application scenario.

2. Framework of the industrial chain system

2.1 Description of industrial chain system

On industrial chain platform, users can bulid up on the application through our underlying system, which generate the contract similar to an automatic agent. The contract has its own address, and it will be activated when the user send a deal in the contract address, shown in Fig.1.



(a) Block chain based data security sharing network architecture [10]; (b)Basic technological structure of blockchain;

Fig. 1 Application scheme from data security sharing network architecture to industrial chain system

From Fig.1(a), block chain based data security sharing network architecture including decentralized data, unified naming technology authorized data, distributed storage and data distribution protocol, are given in reference [10], where an open data index naming structure (ODIN) based decentralized DNS (domain name sever) resolution module is designed and verified. In Fig.1(b) shows large data diagram of industrial chain system, which is actually a decentralized platform and an open-source underlying unchanged program by smart contract. The system aims to develop the application scenario, where any users can properly edit and develop their own application scenarios of online platform. For the application scheme from industrial chain system to platform, the built-in currency can be verified by the miners' team, stored, and then traded on the platform. The application can conclude a contract by using smart contract, where the artificial intelligence is used to manage this contract. In this way, platform users can conclude contracts with the platform to gain their own rights and applications, and blockchain technology can guarantee users' privacy and trust issues.

2.2 Block chain simulation

In theory, information radiates from one node to another in the multi-tree network are described:

$$t(n) = \frac{k_1 S}{B} + aS + \max\{t(n')\} \tag{1}$$

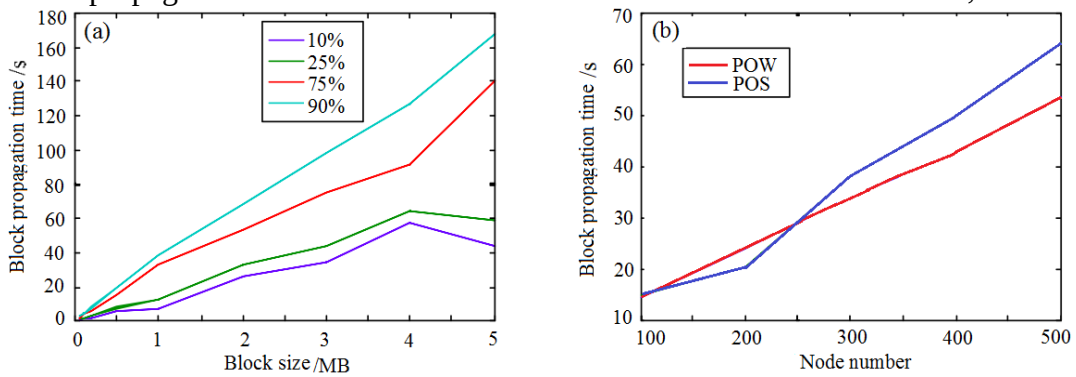
Where the number of nodes of the block chain is n, the bandwidth of each node network channel is B, the block size is S, k_i is the number of nodes that are sent to adjacent nodes at the same time, a is the proportionality coefficient, $t(n)$ represents the time required to propagate in some network the n nodes.

The block chain simulation program is written in ns3 based on the reference [11], besides, the simulation of the proof of stake (POS) mechanism is added for comparison. This program randomly generates a node topology network, which is used to simulate the mining of miner nodes and the diffusion process of the block in the network, and then the total time of the block propagated in the network is recorded. The network scale is fixed to 500 nodes. The block size is divided into 1MB, 2MB, 3MB, 4MB and 5MB. The network scale is increased from 50 nodes to 500 nodes successively. Among them, the transmission time in the 10%, 25%, 75% and 90% of total nodes are recorded.

3 Result and discussion

3.1 Effects of block size and consensus mechanism

Commonly, there are several mechanisms: POW (proof of work), POS (proof of stake) and POC (proof of contribution) etc. Through the competition of mining to find the new block, the validation of the random number during the spread is done to meet the prescribed requirements. Relationship between block propagation time and block size/consensus mechanism are simulated, shown in Fig.2.



(a) Block propagation time *vs* block size; (b) Block propagation time *vs* node number under different protocols

Fig. 2 Relationship between block propagation time and block size/different protocols

The Fig.2 (a) shows that between 0MB and 4 MB, with the increase of the block size, the more contained transaction number, the longer time of transmission. The restriction by network bandwidth cause the longer time of the node verification required after receiving blocks. There is an exception between 4MB and 5MB, which is due to the network topology structure randomly generated in the program, and the different network topology structure has a certain effect on the transmission time.

By Fig.2 (b), the mechanism of the POW (proof of work) and the POS (proof of stake) is the same, with slight value difference in block transmission time. The POS needs less time when the node number is 100-200, while within the region of 200-500 nodes, less time required by using POW. For different consensus mechanisms, the corresponding consensus method and the consensus time are different.

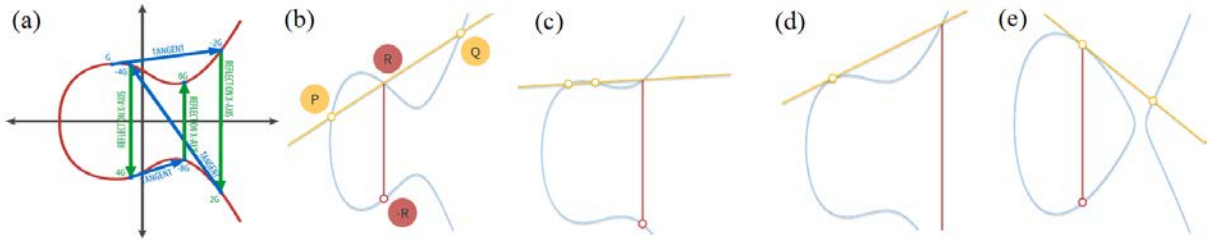
3.2 Discussion of Elliptic Curve (EC)

For the exponentiation: Given $(G, \times)$, $g \in G$ and $n \geq 0$, compute g^n. Elliptic curve scalar multiplication: Given P on an elliptic curve, and $k \geq 0$, compute: $[k]P = P + P + \cdots + P$ (k times). Elliptic curves are illustrated above for various values of a and b. If K has field characteristic, then the best [12] that can be done is to transform the curve into:

$$y^2 = x^3 + ax^2 + bx + c \tag{2}$$

Where, the x^2 term cannot be eliminated, $4a^3 + 27b^2 \neq 0$ is called Weierstrass normal form for elliptic curve. The generator point is always the same for all keys in bitcoin: $K = k*G$, where k is the private key, G is the generator point, K is the resulting public key, a point on curve.

Figure 3 shows the process for deriving G, $2G$, $4G$, as a geometric operation on the curve.



(a) The multiplication of a point G; (b) EC in finite fields; (c) $P \neq Q$; (d) $P = Q$ (e) $P \neq Q$, without point R

Fig.3 Elliptic curve cryptography and the group law of elliptic curves under various conditions.

From Fig.3, elliptic curves over finite fields and the discrete logarithm for the Weierstrass normal form is given. The group law of elliptic curves under various conditions is in Fig.3 (c)-(e). The addition rule is that: given three aligned, non-zero points P, Q and R, their sum is P+Q+R=0 [13]. If $P = -Q$ in Fig.3(c), it does not intersect any third point. When P=Q in Fig.3(d), the two points become closer then overlapped together, the line passing through them becomes tangent to the curve. From Fig.3(e), if $P \neq Q$ but there is no third point R, a case where the line passing through P and Q is tangent to the curve if line intersects just two points. The ECC security is used, a comparison of RSA is added. ECC private key operations (decryption and signature generation) are faster than RSA private-key operations [13].

4. Conclusions

The basic concept of industrial chain and the technological of blockchain were described. Block chain simulation on industrial chain is done to discussion the technique solution. Results are as follows:

(1) The industrial chain system and platform are explored, where the block chain and the smart contract are combined to explore more scenarios for application.

(2) With the increase of the block size, the more contained transaction number is, the longer time the transmission is.

(3) The POS needs less time when the node number is not large, while the larger the node number is, the less time the POW requires.

(4) The elliptic curve is discussed in the view of mathematic, and a comparison with RSA is given.

In conclusion, we believe that the design of the industrial chain will be applied in more and more fields, for example, marry chain, education chain, calculate power chain etc….

Acknowledgments

Authors acknowledge support by Shenzhen basic research project (No. JCYJ20160518112621719). Thanks to Qiufeng Wang for her proofreading and Linlin Guan for her participation.

References

[1] Sompolinsky Y, Zohar A. Secure high-rate transaction processing in bitcoin. Proceedings of the International Conference on Financial Cryptography and Data Security. Berlin, 2015: 507-527.

[2] Tsai W T, Blower R, Zhu Y, et al. A system view of financial blockchains. Proceedings of the Service-Oriented System Engineering (SOSE), San Francisco, USA, 2016: 450-457.

[3] Croman K., Decker C., Eyal I., et al. On scaling decentralized blockchains[C] Financial Cryptography and Data Security. Berlin Heidelberg: Springer, 2016.

[4] Göbel J, Krzesinski A. E., Keeler H. P., et al. Bitcoin blockchain dynamics: the selfish-mine strategy in the presence of propagation delay[J]. Performance Evaluation, 2016(104): 23-41.

[5] M. Xin-Ping, L. Qing-Zhong, K., Lan-Ju, Z. Shi-Dong, Z. Yong-Qing, X. Zong-Shui, Permissioned Blockchain Dynamic Consensus Mechanism Based Multi-Centers, 2018, 41(14):1-15.

[6] Watanabe H, Fujimura S, Atsushi, Kishigami J. Blockchain contract: A complete consensus using blockchain. Proceedings of the 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE). Shanghai,China 2015:577-578.

[7] Miller A, Litton J, Pachulski A, Gupta N, Levin D, Spring N, Bhattacharjee B. Discovering Bitcoin's public topology and influential nodes. Proceedings of the ACM Symposium on Applied Computing, Coimbra, Portugal, 2013: 121-128.

[8] Lewenberg Y, Sompolinsky Y, Zohar A. Inclusive block chain protocols. Financial Cryptography and Data Security. Berlin, Germany: Springer, 2015:528-547.

[9] Decker C, et al. A fast and scalable payment network with bitcoin duplex micropayment channels. Proceedings of the Symposium on Self-Stabilizing Systems. New York, USA, 2015. 9212, 3-18.

[10] W. Jiye,G. Lingchao, et al. Block Chain Based Data Security Sharing Network Architecture Research, Journal of Computer Research and Development, 2017,54(4):742-749.

[11] Gervais A., Karame G. O., St K., et al. On the security and performance of proof of work blockchains[C] ACM Sigsac Conference.ACM, 2016: 3-16.

[12] López, J. and Dahab, R. An Overview of Elliptic Curve Cryptography, Technical Report IC-00-10, State University of Campinas, 2000.

[13] McKean, H. and Moll, V. Elliptic Curves: Function Theory, Geometry, Arithmetic. Cambridge, England: Cambridge University Press, 1999.