Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Supplementary materials for

Wenbo ZHANG, Tao WANG, Chaoyang ZHANG, Jingyu FENG, 2023. Securing multi-chains consensus against diverse miners behaviors attacks in blockchain networks. *Front Inform Technol Electron Eng* (in press). https://doi.org/10.1631/FITEE.2200505

1 Related works

1.1 Cross-chain

Recently, several cross-chain technologies have been proposed. Wang et al. (2017) introduced a blockchain router to empower chains to connect and communicate across chains. Herlihy (2018) modeled the atomic cross-chain swap as a directed graph, in which vertexes are parties and arcs are proposed asset transfers. Borkowski et al. (2019) proposed the DeXTT cross-chain transfer protocol which can be used to record a token transfer in any number of blockchains simultaneously in a decentralized manner. He et al. (2020) proposed a joint operation mechanism for cross-chain trading in the combined distributed photovoltaic power generation market and the carbon market using blockchain technology.

Despite cross-chains broadening the application scenarios of blockchains, they also bring a new technical challenge. That is, malicious users are more likely to take advantage of the multi-chain context to make adverse actions to undermine the consensus process.

1.2 Consensus Schemes

The first consensus scheme was Proof-of-Work (PoW), which was initially used to defend against 51% of attacks through the solution of puzzles. However, PoW requires a great deal of computational power and energy to resolve the puzzle. It may serve a good purpose on the Bitcoin network, but cannot meet the needs of other chains that require rapid block creation. An improved version of PoW named GSCS has been proposed (Wang et al., 2020). GSCS has the potential to ensure a more secure and robust environment for decentralized blockchain systems.

The Proof-of-stake (PoS) (Frankenenfield, 2022) concept states that a person can mine or validate block transactions according to how many coins he or she holds instead of resolving a puzzle. Although PoS can save computational power effectively, it makes the rich get richer. Yang et al. (2019) proposed an improved consensus algorithm named Delegated Proof of Stake with Downgrade (DDPoS), which can detect and downgrade malicious nodes in a timely manner to ensure the security and good operation of the system. A behavior-based incentive mechanism named Proof-of-Behavior (PoB) was introduced by Wang et al. (2020), which can stimulate honest behavior and neutralize malicious attacks.

In recent years, more attention has been paid to consensus schemes with fair multi-miner participation. Instead of relying on computational power or coins, each user can compete fairly to become a miner in a blockchain network. For instance, Practical Byzantine Fault Tolerance (PBFT) (Castro and Liskov, 2002)

has been widely noted for allowing all users of the blockchain to participate in consensus, and for being able to withstand up to one-third of malicious attacks. But it can prevent malicious users from voting maliciously and false blocks from being created only on a single chain. Moreover, these malicious users cannot be accurately detected by PBFT. Tendermint (Buchman, 2016) is another classical BFT (Byzantine Fault Tolerance) consensus scheme that can work even if up to one-third of users in the network fail in arbitrary ways. Based on Tendermint, a consensus scheme that exploits randomness and game theory was proposed (Alzahrani and Bulusu, 2018), but the trust evaluation of the random miners is not considered in the block creation process.

1.3 Trust Management

Trust management has had an increasing influence on many application scenarios, including e-commerce (Morid and Shajari, 2012), online social communities (Li et al., 2016), and wireless sensor networks (Yang et al., 2019).

Trust management is introduced to prevent malicious users from joining the miner team. Representative trust management systems in blockchain networks are described below.

Sun et al. (2019) proposed a trustworthiness calculation method based on trust blockchain users. Malik et al. (2019) proposed TrustChain as a three-layered trust management framework that uses a consortium blockchain to track interactions among supply chain participants and dynamically assigns trust and reputation scores based on these interactions. Xiao et al. (2020) presented a blockchain-based trust mechanism in which the edge reputation system chooses the miner of the blockchain for the joint Proof-of-Stake consensus protocol to append a block recording the new service reputations. Feng et al. (2020) proposed a consensus scheme with fair multi-miner participation called PoN, in which the trust evaluation is designed to select trusted miners in a single-chain consensus scheme.

Currently, one of the most popular trust management designs is based on the beta function. It is regularly used to gain useful information (Sang et al., 2006). Beta trust management first counts the number of honest and dishonest behaviors a user has conducted, and then calculates the trust value with the beta function denoted by $Beta(\alpha, \beta)$ (Jøsang and Ismail, 2002):

$$Beta(\alpha,\beta)=\frac{\Gamma(\alpha,\beta)}{\Gamma(\alpha)\Gamma(\beta)}\delta^{\alpha-1}\left(1-\delta\right)^{\beta-1}. \tag{S1}$$

where δ is the probability of user's behaviors, $0<\delta<1$, $\alpha>0$, $\beta>0$.

A basic trust management system called Baseline can be adopted to evaluate trust value in blockchain networks. For a user U_i, the system calculates the number of true blocks created by U_i, with the role of a miner, denoted by tru_i, and the number of false blocks created by U_i, denoted by fal_i. When the blocks created by U_i are trusted, $\alpha=tru_i+1$, otherwise $\beta=fal_i+1$. Thus, the trust value of U_i is calculated with the beta function as:

$$t_i = Beta(tru_i+1, fal_i+1). \tag{S2}$$

In addition, consider the condition $\Gamma(x)=(x-1)!$ when x is an integer. The expectation value of the beta function is denoted as $E[Beta(\alpha,\beta)]=\alpha/(\alpha+\beta)$. For the initial trust value of U_i to be the threshold θ, the evaluation of t_i can be further described as:

$$t_i=\frac{tru_i+\theta}{tru_i+fal_i+\theta}. \tag{S3}$$

1.4 SVM

As a classical machine learning algorithm, the prediction result of SVM (Elaidi et al., 2018) depends only on the number of support vectors and has nothing to do with the correlation between data features (Gao et al., 2018), so it can avoid the disaster of dimension.

SVM takes the historical experiences (ψ^T) as the feature space and learns in the feature space to find an optimal hyperplane by analyzing the characteristics of data. Its ultimate goal is to maximize the interval. This process can be described as:

$$\psi^T x + \gamma = 0 \ . \tag{S4}$$

where γ is the decision constant of SVM.

According to the user data characteristics, SVM can map each user to the multidimensional space in the form of data points, which contain two types of users.

The first step is to label them respectively for SVM model training. The user type is represented by p_i, which can be represented as:

$$p_{ij} = \begin{cases} +1, & \mathrm{U}_i \text{ is one type of users,} \\ -1, & \mathrm{U}_i \text{ is another type of users.} \end{cases} \tag{S5}$$

Thus, the two sides of the hyperplane can be divided into two different types of users, which can be represented as:

$$\begin{cases} \psi^T x + \gamma \geq +1, & p_{ij} = +1, \\ \psi^T x + \gamma \leq -1, & p_{ij} = -1. \end{cases} \tag{S6}$$

To find an optimal hyperplane to separate these two types of users as far as possible, SVM needs to calculate the distance (d) between the data points and the hyperplane. In a multidimensional space, d can be calculated from:

$$d = \frac{\left|\psi^T x + \gamma\right|}{\left\|\psi\right\|}. \tag{S7}$$

By finding the data points closest to the hyperplane and taking them as the boundary of training results, SVM can separate different data points. At this point, d is at the minimum value (d_{min}). The data point closest to the hyperplane is the support vector of SVM. The plane where the support vector is located becomes the classification decision surface. $d_{\min 1}$ represents the minimum distance between trusted users and the hyperplane. $d_{\min 2}$ is the minimum distance between intensive DMB attackers and the hyperplane. Therefore, the gap between the two types of support vector (Δd) is equal to $d_{\min 1}+d_{\min 2}$, which can be further calculated as:

$$\Delta d = \frac{|\ \psi^T x + \gamma + 1 - (\psi^T x + \gamma - 1)\ |}{\left\|\psi\right\|} = \frac{2}{\left\|\psi\right\|}. \tag{S8}$$

When Δd is at the maximum value, the accuracy of training results will be highest. Specifically, Δd will attain the maximum value (Δd_{max}) under the following constraints:

$$\begin{cases} \Delta d_{\max} = \min_{\psi,\gamma} \dfrac{1}{2}\left\|\psi\right\|^2, \\ s.t.\ p_{ij}\left(\psi^T x + \gamma\right) \geq 1, \end{cases} \tag{S9}$$

where $p_{ij}\left(\psi^T x + \gamma\right) \geq 1$ is derived from Eq. (S6).

By introducing the Lagrange multiplier method, the objective function can be expressed as:

$$L(\psi, \gamma, \mu_r) = \frac{1}{2}\left\|\psi\right\|^2 + \sum_{r=1}^{s} \mu_r \left(1 - p_{ij}\left(\psi^T x_r + \gamma\right)\right), \tag{S10}$$

where μ is the Lagrangian multiplier and s is the number of data features. In the DBP scheme, s=7.

Since the Lagrangian has the duality property, it is often possible to solve its duality problem to obtain the final result.

Let $\frac{\partial L}{\partial \psi^T}=0, \frac{\partial L}{\partial \gamma}=0$, we can obtain:

$$\begin{aligned} &\psi=\sum_{r=1}^{s}\mu_r p_{ij}^r x_r, \\ &\sum_{r=1}^{s}\mu_r p_{ij}^r=0. \end{aligned} \tag{S11}$$

Substituting Eq. (S11) into Eq. (S10), we further obtain:

$$\begin{aligned} L(\psi,\gamma,\mu_r)&=\frac{1}{2}\|\psi\|_2^2+\sum_{r=1}^{s}\mu_r\left[1-p_{ij}^k\left(\psi^T x_r+\gamma\right)\right] \\ &=\frac{1}{2}\psi^T\psi-\sum_{r=1}^{s}\mu_r p_{ij}^r\psi^T x_r-\sum_{r=1}^{s}\mu_r p_{ij}^r\gamma+\sum_{r=1}^{s}\mu_r \\ &=\psi^T\left(\frac{1}{2}\psi-\sum_{r=1}^{s}\mu_r p_{ij}^r x_r\right)-\gamma\sum_{r=1}^{s}\mu_r p_{ij}^r+\sum_{r=1}^{s}\mu_r \\ &=\left(\sum_{q=1}^{s}\mu_q p_{ij}^q x_q\right)^T\left(\frac{1}{2}\sum_{r=1}^{s}\mu_r p_{ij}^r x_r-\sum_{r=1}^{s}\mu_r p_{ij}^r x_r\right)+\sum_{r=1}^{s}\mu_r \\ &=-\frac{1}{2}\sum_{r=1}^{s}\sum_{q=1}^{s}\mu_r\mu_q p_{ij}^r p_{ij}^q(x_r\cdot x_q)+\sum_{r=1}^{s}\mu_r, \end{aligned} \tag{S12}$$

where r and q are the data feature quantities of trusted users and intensive DMB attackers respectively. When p_{ij} and x are given, the Lagrangian multiplier μ can be obtained by Eq. (S12).

2 Experiment analysis

In the fifth experiment, we varied the round of blocks to analyze the network overload of PoDT, Tendermint (Buchman, 2016), and PoR (Alzahrani and Bulusu, 2018).

As shown in Fig. S1, Tendermint had the largest network overload. This is because all users of the blockchain network are selected as miners in Tendermint. Furthermore, we found that randomly selecting chain miners from the network miners can generate a lower network overload than randomly selecting miners from the entire blockchain network.

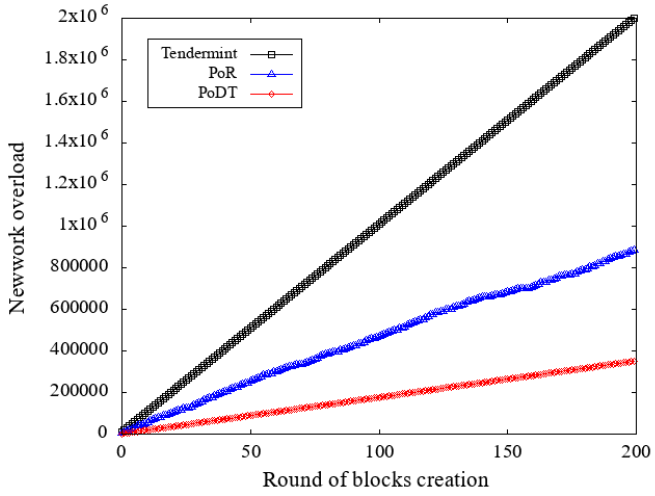

Fig. S1 Network overload comparison of PoDT, Tendermint and PoR

In the sixth experiment, to more intuitively evaluate the performance of PoDT, we verified the efficiency and storage volume consumption of PoDT without loss of generality. The size of a block is usually

set to 1 MB. As shown clearly in Fig. S2 and Fig. S3, the efficiency of PoDT was better than that of the other schemes with the increase of users from 1000 to 10000. Since only a few trusted miners can participate in the consensus in PoDT, the time consumption can be drastically reduced. Moreover, the blocks are backed up only on the trusted nodes, so PoDT had the lowest consumption in terms of storage volume.

In the last two experiments, we analyzed the block throughput and delay in the multi-chain consensus process. Some chain miners can participate in the consensus process of multiple chains, and the larger the number of chains involved, the greater the impact on block throughput and delay. These chain miners can be referred to as cross-chain miners.

In the seventh experiment, the block throughput was defined as the number of blocks created per unit time. During this experiment, there were 10 chain miners per chain, with cross-chain miners accounting for 80% of the miners. As shown in Fig. S4, we observed block throughput at 3, 5 and 8 chain thresholds (CT) for maximum participation of cross-chain miners. Each round of experiments took a fixed amount of time to create a block. As more chains were served simultaneously by cross-chain miners, the block output speed was reduced, and thus the block throughput was reduced. As the number of chains increased, the CT value decreases, leading to a reduced opportunity for cross miners to participate in multi-chain consensus. Therefore, they could focus on the block creation of the chain for which they were responsible, thereby increasing block throughput. Therefore, the setting of the CT value plays a key role in the block throughput. As to the level to which the CT value is set, this had to be further determined by the following delayed experiments.

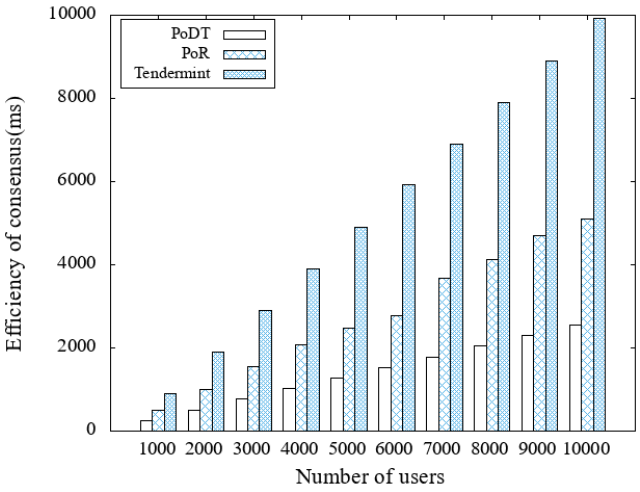

Fig. S2 Efficiency comparison of PoDT, Tendermint and PoR

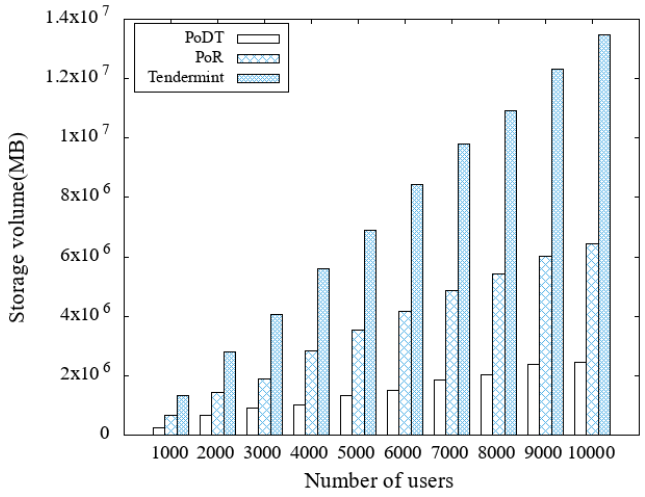

Fig. S3 Storage volume comparison of PoDT, Tendermint and PoR

The larger the number of chains in which cross-chain miners participate due to network latency, the greater the impact on the synchronization and latency of the created blocks in multi-chain consensus. In the final experiment, each round of experiment simulated 10 chains and the number of elections required to select 300 network miners. When the number of participating chains was larger than or equal to the CT value, the election was repeated. If the number of chains allocated to the cross-chain miner was less than the CT value, mining was conducted. After mining, the next round of elections was held until 300 network miners completed mining, and the elections were stopped. As the CT value increased, the probability of mining the assigned coincidence increased, fewer re-elections were needed and the delay was reduced. As shown in Fig. S5, the delay decreased with increasing CT value. In summary, when the CT value was set to 5, better block throughput was achieved with lower delay.

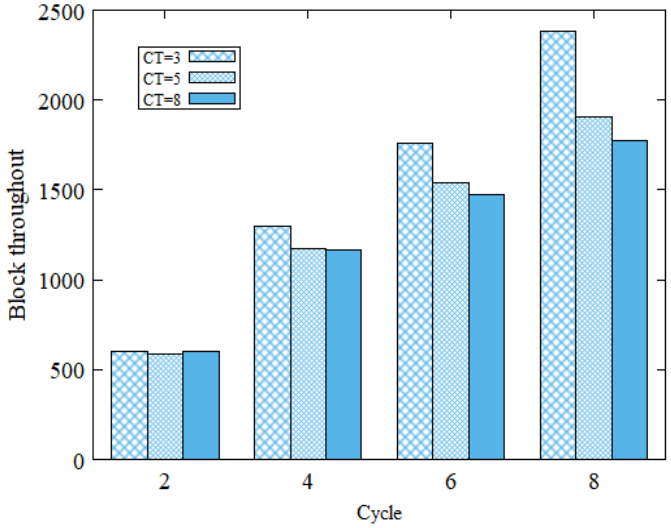

Fig. S4 Block throughput analysis in the multi-chain consensus process

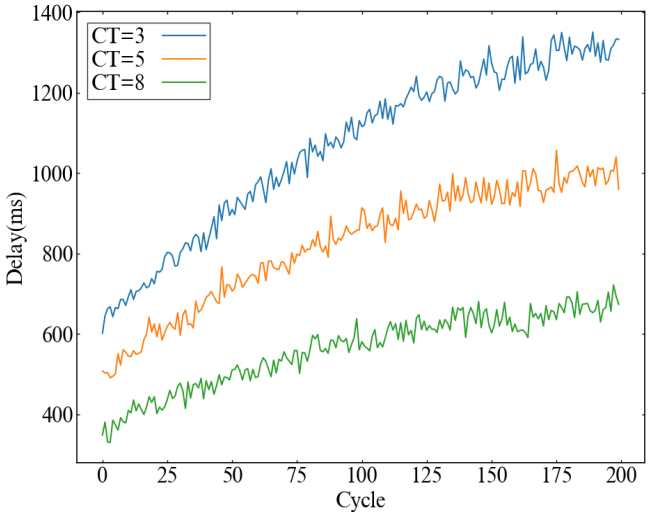

Fig. S5 Delay analysis in the multi-chain consensus process

3 Application analysis in the medical scenario

In this paper, we have described a diverse miner behavior (DMB) attack in a multi-chain parallel blockchain network, where a user may simultaneously process different business needs on multiple chains. The user will create false blocks on the chain in which it is interested, and work normally in other chains to hide his/her own attacks. Meanwhile, due to the drawback that traditional single-chain consensus mechanisms can maintain only the accuracy of block creation but cannot accurately detect DMB attacks, a multi-chain consensus mechanism named PoDT is proposed in our manuscript. The trust evaluation mechanism of PoDT can calculate the trust value of each user, which reflects the user's behavior during the consensus process. With this method, we can easily detect whether the user is a malicious attacker. Moreover, PoDT's trusted random selection algorithm is designed to randomly select honest miners, which can greatly reduce the consumption of network resources during the creation of new blocks and guarantee block accuracy.

After a thorough analysis, we found that the proposed PoDT scheme can be applied to scenarios requiring multi-chain consensus security, such as medical, power, finance, and manufacturing operations. For instance, it can help build a medical data-sharing alliance, so the medical “data island” can be overcome (Fig. S6). Data interconnection and sharing among medical institutions, social insurance institutions, research institutions, and regulators can effectively promote the progress in many fields such as medical research, medical finance, hospital management, clinical medicine, and big data medicine.

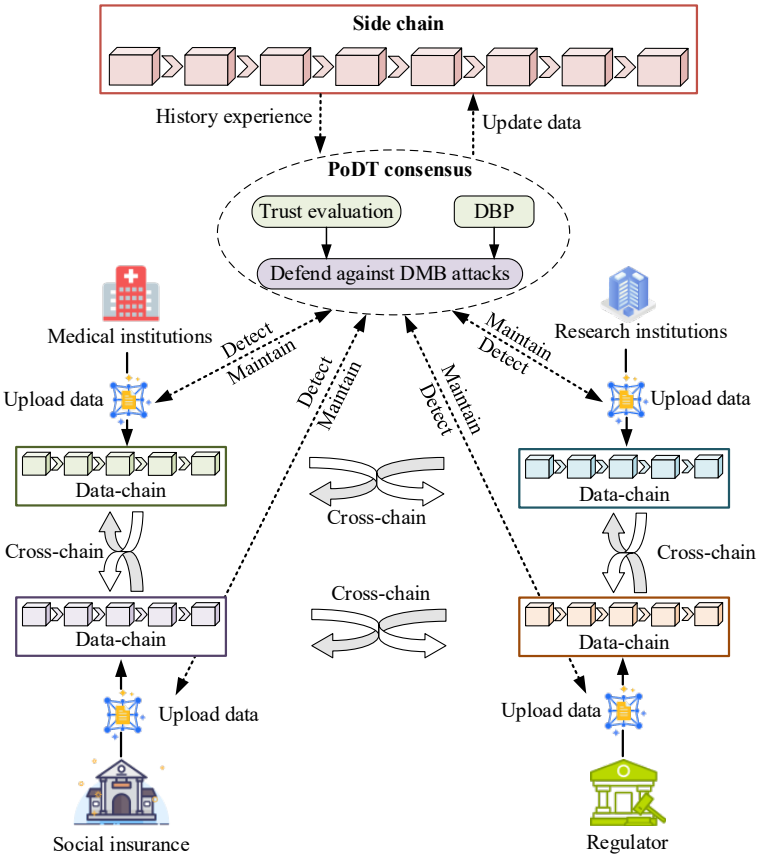

Fig. S6 Industrial application case of PoDT

In this case, each chain can use the same consensus mechanism to promote efficiency. However, this still carries a security risk. High-traffic applications are commonly seen in medical networks (Xia et al., 2013). Malicious code can lurk in high-traffic, so that some normal nodes may be compromised under the control of attackers. Therefore, DMB attacks could be launched by compromised nodes exhibiting diverse consensus behavior on different chains. Given the requirement of defending against DMB attacks, a trust mechanism can be introduced into our PoDT scheme. Implementing a universal reputation score can help to quickly and effectively detect malicious miners whose trust values are below the threshold and prevent them from destroying the consensus mechanism. This is also a function that cannot be achieved by single-chain consensus. Considering the trust values from the network level and quantifying the behavior of miners in consensus, the trust value of miners can be divided into a global trust value and a local trust value. The miner can be trusted only if both values are above the threshold, thereby avoiding widespread disruption of the blockchain.

In our PoDT scheme, a side chain is designed to store the trust values, which can make it tamper-resistant. According to the trust values of miners, some trusted miners are randomly selected to participate in the consensus, which can promote the efficiency of consensus and reduce the consumption of storage volume. Moreover, our PoDT scheme can guarantee security for blockchain networks with the low complexity of algorithms.

References

Alzahrani, N., Bulusu, N., 2018. Towards True Decentralization: A Blockchain Consensus Protocol Based on Game Theory and Randomness. Proc. 2018 International Conference on Decision and Game Theory for Security, p.465-485. https://doi.org/10.1007/978-3-030-01554-1_27

Borkowski, M., Sigwart, M., Frauenthaler, P., et al., 2019. Dextt: Deterministic Cross-Blockchain Token Transfers. *IEEE Access*,

7:111030-111042. https://doi.org/10.1109/ACCESS.2019.2934707

Buchman, E., 2016. Tendermint: byzantine fault tolerance in the age of blockchains. PhD thesis, The University of Guelph, Ontario, Canada.

Castro, M., Liskov, B., 2002. Practical byzantine fault tolerance and proactive recovery, *ACM Trans. Comput. Syst*., 20(4):398-461.https://doi.org/10.1145/571637.571640

Elaidi, H., Elhaddar, Y., Benabbou, Z., et al., 2018. An idea of a clustering algorithm using support vector machines based on binary decision tree. 2018 International Conference on Intelligent Systems and Computer Vision (ISCV), p.1-5. https://doi.org/10.1109/ISACV.2018.8354024

Feng, J.Y., Zhao, X.Y., Chen, K.X., et al., 2020. Towards random-honest miners selection and multi-blocks creation: Proof-of-negotiation consensus mechanism in blockchain networks. *Future Generation Computer Systems*, 105:248-258. https://doi.org/10.1016/j.future.2019.11.026

Frankenenfield, J., Accessed 2022. Proof-of-stake. https://www.investopedia.com/terms/p/proof-stake-pos.asp.

Gao, Y., Xiang, X., Xiong, N., et al., 2018. Human action monitoring for healthcare based on deep learning. *IEEE Access*, 6:52277-52285. https://doi.org/10.1109/ACCESS.2018.2869790

He, H., Luo, Z., Wang, Q., et al., 2020. Joint Operation Mechanism of Distributed Photovoltaic Power Generation Market and Carbon Market Based on Cross-Chain Trading Technology. *IEEE Acces*s, 8:66116-66130. https://doi.org/10.1109/ ACCESS.2020.2985577

Herlihy, M., 2018. Atomic Cross-Chain Swaps. Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, p.245-254. https://doi.org/10.48550/arXiv.1801.09515

Jøsang, A., Ismail, R., 2002. The beta reputation system. Proc. the 15th Bled Electronic Commence Conference, p.1-14.

Li, M., Xiang, Y., Zhang, B., et al., 2016. A trust evaluation scheme for complex links in a social network: a link strength perspective. *Applied Intelligence*, 44(4):969-987. https://doi.org/10.1007/s10489-015-0734-2

Malik, S., Dedeoglu, V., Kanhere, S.S., et al., 2019. TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains. Proc IEEE Conf on Blockchain, p.184-193. https://doi.org/10.1109/Blockchain.2019.00032

Morid, M.A., Shajari, M., 2012. An enhanced e-commerce trust model for community based centralized systems. *Electronic Commerce Research*, 12(4):409-427. https://doi.org/10.1007/s10660-012-9099-3

Sang, Y., Shen, H., Tan, Y., et al., 2006. Efficient protocols for privacy preserving matching against distributed datasets. International Conference on Information and Communications Security, p.210-227. https://doi.org/10.1007/11935308_15

Sun, Y., Zhao, Q., Zhang, P., 2019. Trust Degree Calculation Method Based on Trust Blockchain Node. Proc IEEE Conf on Service Operations and Logistics, and Informatics (SOLI), p.122-127. https://doi.org/10.1109/SOLI48380.2019.8955097

Wang, H., Cen, Y, 2017. Blockchain Router: A Cross-Chain Communication Protocol. Proceedings of the 6th International Conference on Informatics, Environment, Energy and Applications, p.94-97. https://doi.org/10.1145/3070617.3070634

Wang, J., Ding, Y., Xiong, N., et al., 2020, GSCS: General Secure Consensus Scheme for Decentralized Blockchain Systems. *IEEE Access*, 8:125826-125848. https://doi.org/10.1109/ACCESS.2020.3007938

Wang, L., Bai, Y., Jiang, Q., et al., 2020. Beh-Raft-Chain: A Behavior-based Fast Blockchain Protocol for Complex Networks. *IEEE Transactions on Network Science and Engineering*, 8(2):1154-1166. https://doi.org/10.1109/TNSE.2020.2984490

Xia. F., Hao, R., Li, J., et al., 2013. Adaptive GTS allocation in IEEE 802.15. 4 for real-time wireless sensor networks. *Journal of Systems Architecture*, 59(10):1231-1242. https://doi.org/10.1016/j.sysarc.2013.10.007

Xiao, L., Ding, Y., Jiang, D., et al., 2020. A Reinforcement Learning and Blockchain-Based Trust Mechanism for Edge Networks. *IEEE Transactions on Communications*, 68(9):5460-5470. https://doi.org/10.1109/TCOMM.2020.2995371

Yang, F., Zhou, W., Wu, Q., et al., 2019. Delegated Proof of Stake with Downgrade: A Secure and Efficient Blockchain Consensus Algorithm with Downgrade Mechanism. *IEEE Access*, 7:118541-118555. https://doi.org/10.1109/ACCESS.2019.2935149

Yang, G., Liang, T., He, X., et al., 2019. Global and Local Reliability-Based Routing Protocol for Wireless Sensor Networks. *IEEE Internet of Things Journal*, 6(2):3620-3632. https://doi.org/10.1109/JIOT.2018.2889379