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

Securing multi-chain consensus against diverse miner behavior attacks in blockchain networks[*#]

Wenbo ZHANG[†1], Tao WANG[1,2], Chaoyang ZHANG[1], Jingyu FENG[†‡1]

[1]*School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China*

[2]*Postal Savings Bank of China, Xi'an 710000, China*

[†]E-mail: zhangwenbo@xupt.edu.cn; fengjy@xupt.edu.cn

Received Oct. 25, 2022; Revision accepted June 16, 2023; Crosschecked Mar. 20, 2024

Abstract: As cross-chain technologies enable interactions among different blockchains (hereinafter "chains"), multi-chain consensus is becoming increasingly important in blockchain networks. However, more attention has been paid to single-chain consensus schemes. Multi-chain consensus schemes with trusted miner participation have not been considered, thus offering opportunities for malicious users to launch diverse miner behavior (DMB) attacks on different chains. DMB attackers can be friendly in the consensus process on some chains, called mask chains, to enhance their trust value, while on others, called kill chains, they engage in destructive behaviors on the network. In this paper, we propose a multi-chain consensus scheme named Proof-of-DiscTrust (PoDT) to defend against DMB attacks. The idea of distinctive trust (DiscTrust) is introduced to evaluate the trust value of each user across different chains. The trustworthiness of a user is split into local and global trust values. A dynamic behavior prediction scheme is designed to enforce DiscTrust to prevent an intensive DMB attacker from maintaining strong trust by alternately creating true or false blocks on the kill chain. Three trusted miner selection algorithms for multi-chain environments can be implemented to select network miners, chain miners, and chain miner leaders, separately. Simulation results show that PoDT is secure against DMB attacks and more effective than traditional consensus schemes in multi-chain environments.

Key words: Blockchain; Cross-chain; Trust mechanism; Multi-chain consensus
https://doi.org/10.1631/FITEE.2200505 **CLC number:** TP309

1 Introduction

Blockchain, originally devised for Bitcoin (Nakamoto, 2008), has evolved into a well-studied status in both industry and academia. It has had a revolutionary impact on all sectors of the industry (Sharma et al., 2019). In contrast to cloud computing (Xiong et al., 2012), blockchain is helpful in achieving decentralization. It also has numerous other benefits (Chen et al., 2021), such as persistence, pseudonymity, and auditability. Blockchain has been applied to many fields, including financial services (Peters et al., 2015), medicine (Azaria et al., 2016), Internet of Things (Hewa et al., 2020), intelligent transportation systems (Chaudhary et al., 2019), e-government (Hou, 2017), smart advertising networks (Liu et al., 2021), and smart cities (Kumar et al., 2021).

Cross-chain (Buterin, 2022) has gradually become the focus of research, aiming to build reliable interaction channels between different blockchains (hereinafter "chains"). Some cross-chain technologies have appeared (see supplementary materials, Section 1.1) which connect decentralized blockchain ecological islands and have become a bridge link for overall blockchain expansion (Herlihy, 2018; Borkowski et al., 2019;

[‡] Corresponding author

[*] Project supported by the Natural Science Basic Research Program of Shaanxi Province, China (No. 2023-JC-YB-561)

[#] Electronic supplementary materials: The online version of this article (https://doi.org/10.1631/FITEE.2200505) contains supplementary materials, which are available to authorized users

ORCID: Wenbo ZHANG, https://orcid.org/0000-0002-3304-3221; Jingyu FENG, https://orcid.org/0000-0002-5353-3295

He et al., 2020). While cross-chain facilitates interactions between different chains, it enables multi-chain consensus, which is increasingly critical in blockchain networks.

One of the cores of blockchain technology is the consensus scheme. In blockchain networks, blocks can be validated, shared, synchronized, and created across users via a peer-to-peer decentralized consensus scheme (Shi et al., 2008). The users responsible for creating blocks in the consensus scheme are called miners. Many researchers have tried to improve the consensus mechanism (see supplementary materials, Section 1.2). Consensus mechanisms with a focus on fair participation of multiple miners have also emerged (Castro and Liskov, 2002; Buchman, 2016; Alzahrani and Bulusu, 2018; Frankenfield, 2023). One of the most important properties of a blockchain platform is its security (Ding et al., 2021). At present, most trust management mechanisms focus mainly on the enhancement of the robustness of the whole network's security (Zhang et al., 2018). To detect malicious users, trust management can be introduced to estimate whether a user is honest based on his/her historical behavior. Thus, miners can be selected to participate in the consensus scheme according to their trust values.

However, most consensus schemes are based on a single-chain mode and universal trust evaluation. This may provide opportunities for malicious users in a multi-chain consensus scheme. When there are multiple chains in a blockchain network, some miners may exist on all chains so that they can simultaneously process different businesses on different chains. This can help them grasp all information or dispatch different tasks. Once these users are attacked or even hijacked, it is possible for malicious users to wreak havoc on one chain if the high trust value generated by their honest behavior on another chain is universal across the network. That is, malicious users may launch diverse miner behavior (DMB) attacks on different chains.

In this paper, we propose a multi-chain consensus scheme called Proof-of-DiscTrust (PoDT) along with a proof-of-concept blockchain design to defend against DMB attacks. The main contributions of this paper are as follows:

1. We conduct an in-depth investigation of DMB attacks. According to the strategy of DMB attacks, the chains in the network can be divided into kill chains and mask chains. The basic idea of DMB is as follows: DMB attackers may behave differently on different chains. They can be friendly in the consensus process of mask chains to enhance their trust value and maintain honest miners, while in kill chains they engage in behaviors that undermine the consensus process. Specifically, normal DMB attackers exploit the high trust values achieved from mask chains to engage in sabotage on kill chains. Further, intensive DMB attackers maintain high trust values by alternately creating true or false blocks on kill chains, which would make them hard to detect in the consensus scheme.

2. We introduce the idea of distinctive trust (DiscTrust) to evaluate the trust value of each user across different chains. The trustworthiness of a user is split into local and global trust values. The evaluation of the local trust value for a user is bound to each chain. A high local trust value for a user simply indicates that he/she is trusted on one chain rather than all chains. A user is recognized as honest only if both the local trust values and the global trust value associated with all chains are high. Normal DMB attackers can be detected due to their low local trust values on the kill chains.

3. We propose a dynamic behavior prediction (DBP) scheme based on DiscTrust. An additional side chain is used to store the experience of users on all chains. Because support vector machine (SVM) is highly accurate and fast in dichotomy prediction, it is well suited to DBP. By analyzing the experience of a user, a predictive model can be constructed by combining the Lagrangian multipliers into an objective function to predict a user's dynamic behavior on a kill chain. If the prediction result is +1, intensive DMB attackers can be detected.

4. We design three algorithms to select trusted miners for a multi-chain environment. The global trust value is used to design the algorithm for the selection of trusted network miners. Only after a user has been selected as a network miner, will he/she be eligible for selection as a chain miner who has the authority to create blocks in the consensus scheme. A chain miner who can be trusted on one chain may not be trusted on another. In this way, both local trust values and DBP are used to design algorithms for selecting trusted chain miners on a chain. To confirm block validation, the last algorithm is designed to periodically elect the leader of the chain miners.

2 Overview of diverse miner behavior attacks

When a trust management system is used in blockchain networks, false block threats can be easily suppressed if ordinary attackers always create false blocks against the consensus scheme (see supplementary materials, Section 1.3). This is because they will obtain a low trust value when they always create false blocks. To avoid the detection of trust management systems, attackers will change their strategies.

The advent of multiple chains may offer attackers new attack opportunities. DMB attacks are applicable under three key conditions: (1) each user in a blockchain network has the opportunity to act as a miner, (2) the traditional single-chain thinking mode makes the trust value universal in the whole blockchain network, and (3) no measures are adopted to evaluate the trust value of each user across different chains.

In short, an ordinary attacker would break the consensus scheme on all chains, whereas a DMB attacker may exhibit diverse consensus behaviors on different chains.

In general, DMB attackers divide the chains in the network into kill chains and mask chains to implement their attack strategy.

1. Kill chains: The kill chains are the chains whose consensus scheme is the destruction target of DMB attackers.

2. Mask chains: The mask chains are the chains where DMB attackers can be friendly in the consensus process to enhance their trust value. By disguising themselves as honest miners, they can undermine the consensus process of kill chains.

DMB attacks can be launched based on two aspects of threats: normal and intensive. Normal DMB attackers always behave viciously on kill chains, whereas intensive DMB attackers maintain high trust by alternately creating true or false blocks on kill chains.

DMB attackers are extremely sensitive to their trust value. They begin to launch DMB attacks under the constraint:

$$\begin{cases} \mathrm{gt}_i \le \theta + \xi_1 \xrightarrow{\text{launch}} \text{normal DMB attack}, \\ \mathrm{lt}_{ij} \le \theta + \xi_1 \xrightarrow{\text{launch}} \text{intensive DMB attack}. \end{cases} \tag{1}$$

The strategy of DMB attacks is shown in Fig. 1. Assume that U_i is one of the DMB attackers, gt_i the global trust value of U_i, and lt_{ij} the local trust value of U_i corresponding to the j^{th} chain (Chain_j). As each $\mathrm{gt}_i \in [0, 1]$ or $\mathrm{lt}_{ij} \in [0, 1]$, the threshold of the trust value (θ) is usually set to a moderate value, such as 0.5, which can be calculated when tru=fal (see supplementary materials, Eq. (S3)). When $\mathrm{gt}_i \le \theta + \xi_1$, U_i will launch normal DMB attacks to enhance his/her global trust value on mask chains. Here, ξ_1 is the trust value warning line. It is too late to increase the trust value when $\mathrm{gt}_i \le \theta$. This attack pattern will continue until $\mathrm{gt}_i \ge \theta + \xi_2$ (ξ_2 is the high trust line). During $\theta + \xi_1 \le \mathrm{gt}_i \le \theta + \xi_2$, U_i will launch normal DMB attacks to undermine the consensus process of kill chains since U_i can be disguised as an honest miner.

If lt_{ij} is introduced, U_i cannot engage in sabotage on the kill chains with intensive DMB attacks. U_i may get crafty and adopt normal DMB attacks to obtain an opportunity to be destructive on kill chains. Assuming that Chain_j is a kill chain, U_i will launch intensive DMB attacks to enhance his/her local trust value on Chain_j when $\mathrm{lt}_{ij} \le \theta + \xi_1$. This attack pattern will continue until $\mathrm{lt}_{ij} \ge \theta + \xi_2$. During $\theta + \xi_1 \le \mathrm{lt}_{ij} \le \theta + \xi_2$, U_i will launch intensive DMB attacks to undermine the consensus process of Chain_j.

3 Our proposed PoDT scheme

To select trusted miners in multi-chain environments, we propose a multi-chain consensus scheme named Proof-of-DiscTrust (PoDT).

3.1 Design idea

Some negotiation rules are necessary to achieve a fast and efficient consensus scheme in a distributed manner (Feng et al., 2020). To construct a better multi-chain consensus scheme, the following negotiation rules should be applied:

Rule 1 The global trust value is used to select and update network miners (Θ_{net}), while the local trust value is used to select and update chain miners (Θ_{chain}).

Rule 2 The number of members is $|\Theta_{\text{net}}| > n/2$, where n is the number of users in the network.

Rule 3 The number of members is $|\Theta_{\text{chain}}| > m/2$, where m is the maximum number of active users in a blockchain.

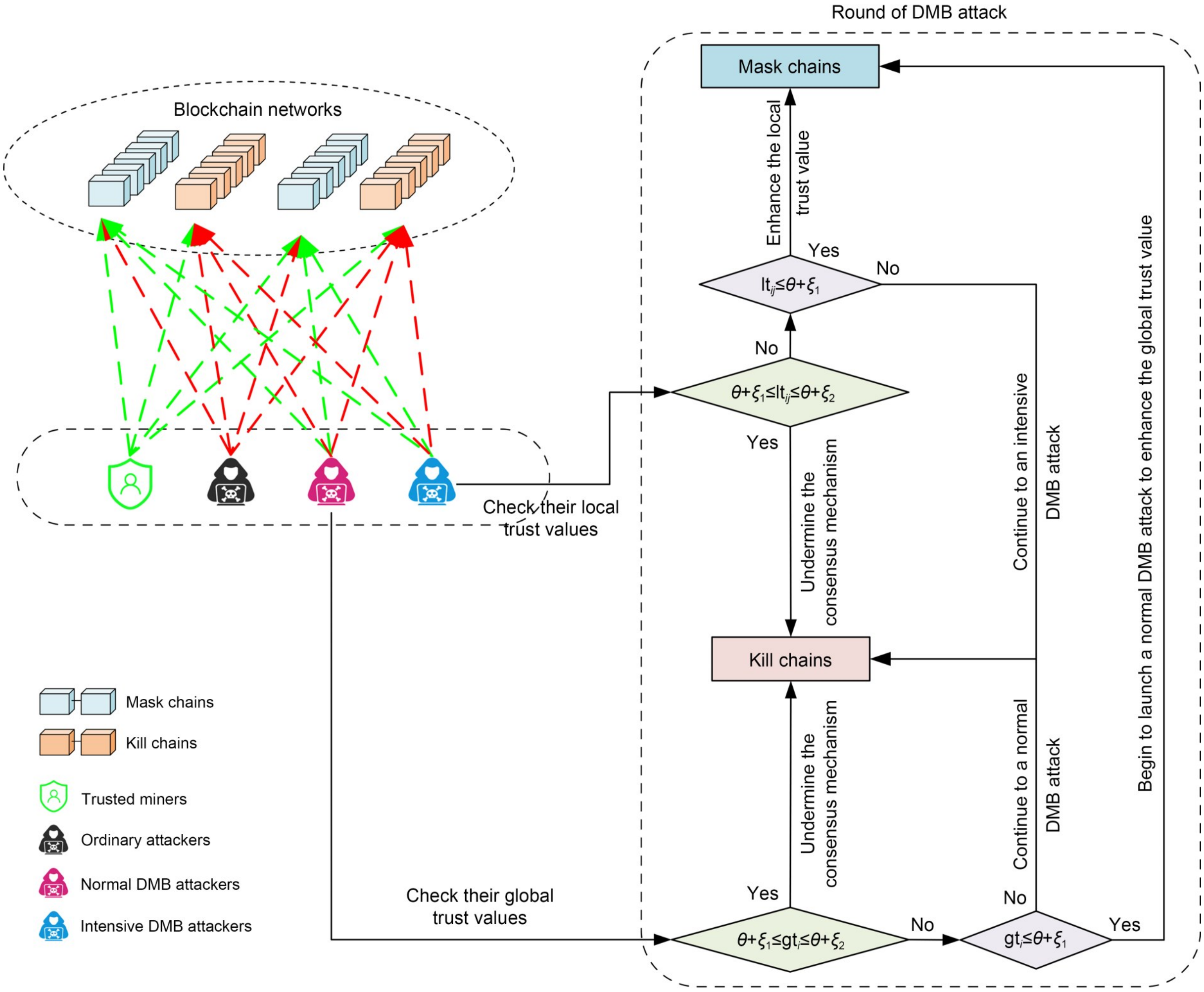
Round of DMB attack
Blockchain networks
Mask chains
Enhance the local trust value
Yes
No
$lt_{ij}\le\theta+\xi_1$
No
$\theta+\xi_1\le lt_{ij}\le\theta+\xi_2$
Yes
Undermine the consensus mechanism
Continue to an intensive DMB attack
Begin to launch a normal DMB attack to enhance the global trust value
Check their local trust values
Kill chains
Mask chains
Kill chains
Trusted miners
Ordinary attackers
Normal DMB attackers
Intensive DMB attackers
Undermine the consensus mechanism
Continue to a normal DMB attack
Yes
No
Check their global trust values
$\theta+\xi_1\le gt_i\le\theta+\xi_2$
No
$gt_i\le\theta+\xi_1$
Yes

Fig. 1 Strategy of diverse miner behavior (DMB) attacks

Rule 4 Only after a user has been selected as a network miner, will he/she be eligible for selection as a chain miner.

Rule 5 Only chain miners have the authority to create blocks in the consensus scheme.

Rule 6 Chain miners who can be trusted on one blockchain may not be trusted on another.

Rule 7 A round of block creation is usually made up of block generation, block validation, and block acceptance.

Rule 8 In a round of block creation, several chain miners are first randomly selected to be responsible for block generation, and then several are randomly selected to perform block validation.

Rule 9 On each blockchain, a chain miner leader shall be elected periodically to accept and broadcast confirmation of block validation.

With the negotiation rules, the architectural view of PoDT is shown in Fig. 2. To suppress DMB attacks, we design PoDT based on two-level defense.

In the first-level defense, DiscTrust is introduced to defend against normal DMB attacks. DiscTrust divides a user's trust values into global trust values and local trust values. Although the global trust value of normal DMB attackers is higher than the threshold, their local trust value in kill chains will be lower than the threshold. Therefore, DiscTrust can effectively detect normal DMB attackers. If the global trust value is smaller than the threshold, DiscTrust can also be used to detect ordinary attackers.

Nevertheless, the local and global trust values of intensive DMB attackers are both higher than the threshold, so they may not be detected. Supported by DiscTrust, the second-level defense can collect the dynamic

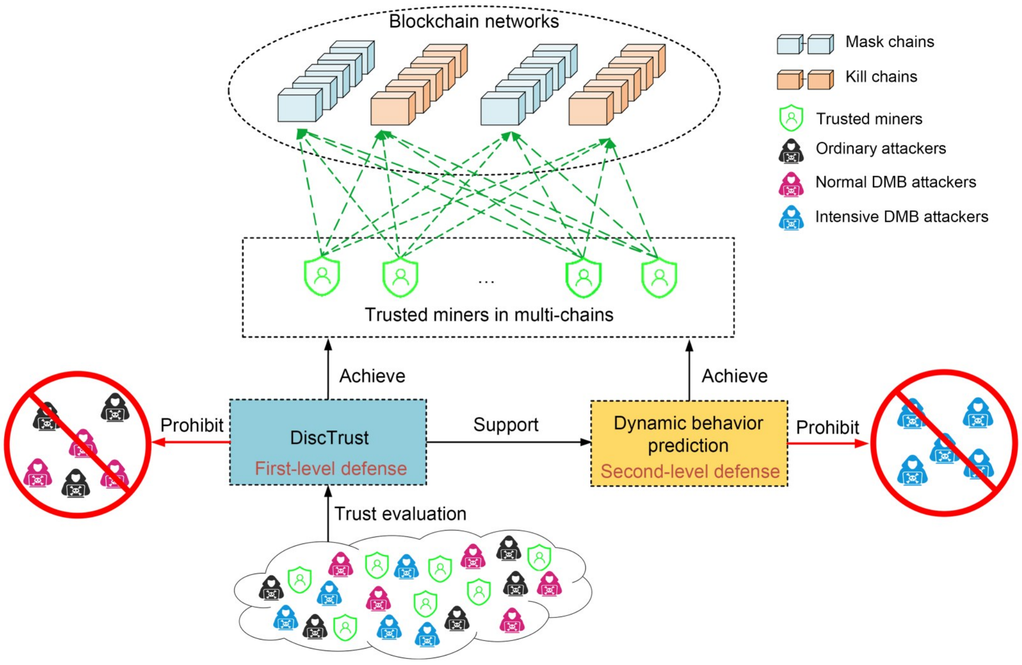

Fig. 2 Architectural view of Proof-of-DiscTrust (PoDT)

changes of the local and global trust values of users, and the proposed DBP scheme can be used to detect intensive DMB attackers and prevent kill chains from becoming their victims.

On this basis, trusted miner selection in a multi-chain environment can be achieved in a round of block creation.

3.2 Distinctive trust evaluation

Normal DMB attackers fake blocks on kill chains and create true blocks on mask chains to boost their trust value. In the DiscTrust scheme, our design idea is that the trust value of each user should be evaluated by his/her previous behavior on various chains. The DiscTrust scheme is built with three functional modules: local distinctive trust evaluation, global distinctive trust evaluation, and normal DMB attacker detection (Fig. 3).

1. Local distinctive trust evaluation

In the DiscTrust scheme, the result of trust evaluation for various chains is not a single value, but a set of local trust values. Taking the i^{th} user (U_i) as an example, the local trust value of U_i corresponding to the j^{th} blockchain (Chain$_j$) can be evaluated as

$$\mathrm{lt}_{ij}=\frac{\mathrm{tru}_{ij}+\theta}{\mathrm{tru}_{ij}+\mathrm{fal}_{ij}+1}, \tag{2}$$

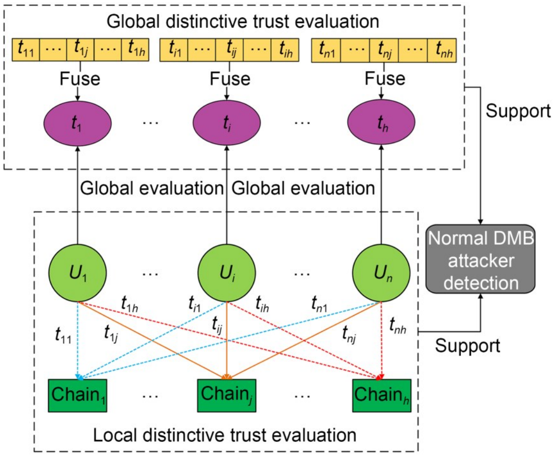
Global distinctive trust evaluation
t_{11} ··· t_{1j} ··· t_{1h}
t_{i1} ··· t_{ij} ··· t_{ih}
t_{n1} ··· t_{nj} ··· t_{nh}
Fuse
Fuse
Fuse
t_1 ··· t_i ··· t_h
Support
Global evaluation
Global evaluation
U_1 ··· U_i ··· U_n
Normal DMB attacker detection
t_{11}
t_{1j}
t_{1h}
t_{i1}
t_{ij}
t_{ih}
t_{n1}
t_{nj}
t_{nh}
Support
Chain$_1$ ··· Chain$_j$ ··· Chain$_h$
Local distinctive trust evaluation

Fig. 3 Functional modules in the DiscTrust scheme

where tru_{ij} and fal_{ij} denote the numbers of honest and false blocks created by U_i for Chain$_j$, respectively. When $\mathrm{tru}_{ij}=\mathrm{fal}_{ij}=0$, U_i is a newcomer and his/her local trust value is set to the threshold. Thus, the newcomer would have a chance to participate in the consensus scheme of Chain$_j$, and then his/her local trust value will be changed based on his/her future behavior.

Similarly, we can evaluate the local trust value of U_i for all chains in the network, and thus generate a trust vector for U_i, which can be expressed as

$$\mathrm{LT}_i=[\,\mathrm{lt}_{i1},\mathrm{lt}_{i2},\cdots,\mathrm{lt}_{ih}\,]. \tag{3}$$

In a blockchain network, the trust vectors of all users can be formed into a matrix $\mathrm{LT}_{n\times h}$, where n is the number of users and h is the number of chains in the network:

$$\mathrm{LT}_{n\times h}=\begin{bmatrix} \mathrm{lt}_{11} & \mathrm{lt}_{12} & \cdots & \mathrm{lt}_{1h} \\ \mathrm{lt}_{21} & \mathrm{lt}_{22} & \cdots & \mathrm{lt}_{2h} \\ \vdots & \vdots & & \vdots \\ \mathrm{lt}_{n1} & \mathrm{lt}_{n2} & \cdots & \mathrm{lt}_{nh} \end{bmatrix}. \tag{4}$$

2. Global distinctive trust evaluation

To analyze the holistic behavior of a user for all chains, the global trust value of the user corresponding to all chains should be considered. Again, using U_i as an example, the global trust value of U_i corresponding to all chains can be evaluated as

$$\mathrm{gt}_i=\frac{\mathrm{tru}_i+\theta}{\mathrm{tru}_i+\mathrm{fal}_i+1}, \tag{5}$$

where $\mathrm{tru}_i=\sum_{j=1}^{h}\mathrm{tru}_{ij}$ and $\mathrm{fal}_i=\sum_{j=1}^{h}\mathrm{fal}_{ij}$.

For all users, Ξ denotes the set of their global trust values, which are extremely valuable for trusted network miner selection.

3. Normal DMB attacker detection

To detect normal DMB attackers effectively, the trust state division of a user should be considered through the global trust value and the number of low local trust values (λ).

U_i and λ_i can be counted with Algorithm 1.

Algorithm 1 Count λ_i

```
Input: $\mathrm{LT}_i$
Output: $\lambda_i$
Initialize $\lambda_i=0$
for each $\mathrm{lt}_{ij}\in\mathrm{LT}_i$ $(1\le i\le h)$ do
    if $\mathrm{lt}_{ij}<\theta$ then
        $\lambda_i=\lambda_i+1$
    end if
end for
```

With (gt_i, λ_i), the trust state of U_i can be divided into four categories:

1. Trustworthy state ($\mathrm{gt}_i\ge\theta$ && λ_i==0)

This state shows that U_i always creates true blocks for all chains. His/her blocks can be accepted in the current chain.

2. Low-risk state ($\mathrm{gt}_i\ge\theta$ && $\lambda_i\ge1$)

This state shows that U_i creates false blocks for a small number of chains. U_i must be rejected to participate in the consensus scheme of Chain_j for $\mathrm{lt}_{ij}<\theta$.

3. Medium-risk state ($\mathrm{gt}_i<\theta$ && $\lambda_i\ge1$)

This state shows that U_i creates false blocks for most chains. U_i must be rejected to participate in the consensus scheme of Chain_j for $\mathrm{lt}_{ij}<\theta$. Meanwhile, his/her blocks should be rejected since his/her trust state might be converted to the high-risk state.

4. High-risk state ($\mathrm{gt}_i<\theta$ && λ_i==h)

This state shows that U_i always creates false blocks for all chains. His/Her blocks must be rejected in the current chain.

Based on the four categories of the trust state, Algorithm 2 is designed to separate the set of users (Φ) into four clusters to detect normal DMB attackers in the current chain.

Algorithm 2 Normal DMB attacker detection

```
Input: $\Phi$
Output: $\Phi_1$, $\Phi_2$, $\Phi_3$, $\Phi_4$
Initialize $\Phi_1=\Phi_2=\Phi_3=\Phi_4=\varnothing$
for each $U_i\in\Phi$ do
    Observe $\mathrm{gt}_i$ and $\lambda_i$
    if $\mathrm{gt}_i\ge\theta$ && $\lambda_i$==0 then
        $\Phi_1=\{U_i\}\cup\Phi_1$
    else if $\mathrm{gt}_i\ge\theta$ && $\lambda_i\ge1$ then
        $\Phi_2=\{U_i\}\cup\Phi_2$
    else if $\mathrm{gt}_i<\theta$ && $\lambda_i\ge1$ then
        $\Phi_3=\{U_i\}\cup\Phi_3$
    else if $\mathrm{gt}_i<\theta$ && $\lambda_i$==$h$ then
        $\Phi_4=\{U_i\}\cup\Phi_4$
    end if
end for
```

Both Φ_2 and Φ_3 are sets of normal DMB attackers. Φ_1 is the set of honest miners and Φ_4 the set of malicious attackers who always create false blocks on all chains.

3.3 Dynamic behavior prediction

Intensive DMB attackers maintain high trust by alternately creating true or false blocks on kill chains, which may allow them to be hided in Φ_1. By analyzing the experience of U_i, the DBP scheme can predict his/her dynamic behavior on a kill chain such as Chain$_j$, and thus detect whether U_i is an intensive DMB attacker.

With the function that the blockchain can securely maintain transactions and records (Gupta et al., 2019), an additional side chain is used to store the experience of users for all chains (Fig. 4). The experience stored in the side chain is shown in Table 1.

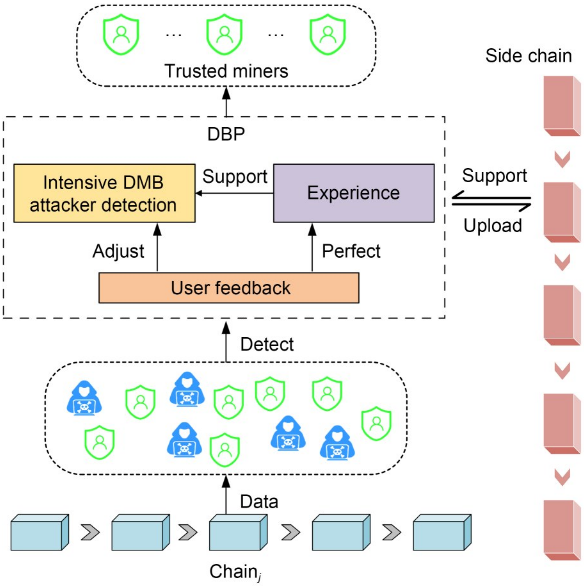

Fig. 4 Architectural overview of dynamic behavior prediction (DBP)

Table 1 Experience stored in the side chain

Parameter	Description
lt_{ij}	Local trust value of U_i corresponding to Chain$_j$
gt_i	Global trust value of U_i
t_i	Number of true blocks created by U_i
f_i	Number of false blocks created by U_i
L_j	Length of Chain$_j$
N_j	Number of active users on Chain$_j$
F_{ij}^k	Feedback to the k^{th} block created by U_i on Chain$_j$

After a round of new block creation, a lot of useful data are generated, including the local and global trust values of the miners who have created the block and the accuracy of block creation. These data can be collected and backed up to the side chain through cross-chain interaction technology.

The trusted miners are in charge of the side chain because they are trustworthy no matter on which chain they are. The data can be stored in the blocks of the side chain. For example, if a miner proposes a new block, the miner's identity (ID) and the chain's ID should be recorded in the block header, and the miner's trust value will be stored in the block body. The trust history data of the miner can be found quickly when they are needed urgently. Generally, the block generation rate and query efficiency are low when data are stored based on the upper block capacity limit. So, we consider storing data according to miners. Although this will make the blockchain longer, the storage capacity of each block is small, usually less than 1 MB (Zheng et al., 2018), which will not increase the overload on the server that deploys the side chain. Moreover, the longer the blockchain, the more difficult it is to tamper with. Blocks can be created faster and the query efficiency is higher. Whenever a new block is created, the trust value of each miner will be updated accordingly and transmitted to the side chain through the cross-chain protocol and packaged into a block. The miner's latest trust value can be quickly obtained just by searching the last block of the side chain.

The side chain can be regarded as the sharing link of experience generated by the users' activities on each blockchain. When it is necessary to judge whether U_i on Chain$_j$ is an intensive DMB attacker, DBP can access U_i's experience from the side chain through cross-chain interaction as predictive support.

In addition, once the newly created block is broadcast to all the users on Chain$_j$, those users provide feedback on the block's authenticity and upload it to the sidechain. F_{ij}^k is the feedback from other users on the k^{th} block created by U_i on Chain$_j$ and can be used to adjust the DBP scheme and improve its accuracy.

Data prediction is helpful in dealing with the abnormal condition (Cheng et al., 2019). In our DBP scheme, we need only a binary prediction result. SVM is highly accurate and fast in dichotomy prediction, so it could be well suited to predicting trusted users or intensive DMB attackers. The preliminaries of SVM are given in Section 1.4 of the supplementary materials.

In the DBP scheme, the experience (ψ^{T}) for SVM can be described as

$$\begin{cases}\psi^{\mathrm{T}}x+\gamma=0,\\ \psi^{\mathrm{T}}=\left(\mathrm{lt}_{ij},\mathrm{gt}_i,t_i,f_i,L_j,N_j,F_{ij}^k\right).\end{cases}\tag{6}$$

The user type can be represented as

$$p_{ij}=\begin{cases}+1, & U_i \text{ is an intensive DMB attacker},\\ -1, & U_i \text{ is a trusted user}.\end{cases}\tag{7}$$

Thus, the two sides of the hyperplane can be divided into two different types of users represented by

$$\begin{cases}\psi^{\mathrm{T}}x+\gamma\ge+1, & p_{ij}=+1,\\ \psi^{\mathrm{T}}x+\gamma\le-1, & p_{ij}=-1.\end{cases}\tag{8}$$

The distance (d) between the data points and the hyperplane can be calculated as

$$\begin{cases}d=\dfrac{\left|\psi^{\mathrm{T}}x+\gamma\right|}{\left\|\psi\right\|},\\ \left\|\psi\right\|=\sqrt{\mathrm{lt}_{ij}^2+\mathrm{gt}_i^2+t_i^2+f_i^2+L_j^2+N_j^2+\left(F_{ij}^k\right)^2}.\end{cases}\tag{9}$$

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

$$L(\psi,\gamma,\mu_r)=\frac{1}{2}\left\|\psi\right\|^2+\sum_{r=1}^{s}\mu_r\left(1-p_{ij}\left(\psi^{\mathrm{T}}x_r+\gamma\right)\right).\tag{10}$$

Let $\dfrac{\partial L}{\partial\psi^{\mathrm{T}}}$=0 and $\dfrac{\partial L}{\partial\gamma}$=0. We can obtain

$$\begin{cases}\psi=\displaystyle\sum_{r=1}^{s}\mu_r p_{ij}^r x_r,\\ \displaystyle\sum_{r=1}^{s}\mu_r p_{ij}^r=0.\end{cases}\tag{11}$$

Let $\psi^{\mathrm{T}}x_q+\gamma=1$ or $\psi^{\mathrm{T}}x_q+\gamma=-1$. Then according to Eq. (8), we can obtain $\psi^{\mathrm{T}}x_q+\gamma=p_{ij}^q$.

Further, γ can be expressed as

$$\gamma=p_{ij}^q-\psi^{\mathrm{T}}x_q=p_{ij}^q-\sum_{q=1}^{s}\mu_q p_{ij}^q x_q x_q.\tag{12}$$

ψ^{T} and γ can be used to make the optimal hyperplane selection. In the DBP scheme, s=7.

Substituting ψ^{T} and γ into Eq. (10), the prediction model can be built as follows:

$$\begin{aligned}f(x)&=\frac{1}{2}\left\|\psi\right\|^2+\sum_{r=1}^{s}\mu_r\left(1-p_{ij}\left(\psi^{\mathrm{T}}x_r+\gamma\right)\right)\\ &=\frac{1}{2}\left\|\psi\right\|^2+\sum_{r=1}^{s}\mu_r\left(1-p_{ij}\left(\psi^{\mathrm{T}}x_r+p_{ij}^q\right.\right.\\ &\quad\left.\left.-\sum_{q=1}^{s}\mu_q p_{ij}^q\left(x_r x_q\right)\right)\right)\\ &=\frac{1}{2}\left\|\psi\right\|^2+\sum_{r=1}^{s}\mu_r\left(1-p_{ij}\left(\sum_{r=1}^{s}\mu_r p_{ij}^r x_r x_r\right.\right.\\ &\quad\left.\left.+p_{ij}^q-\sum_{q=1}^{s}\mu_q p_{ij}^q x_r x_q\right)\right).\end{aligned}\tag{13}$$

With this model, the predicted value p_{ij} belonging to a user can be obtained by inputting the user data characteristics.

Let Φ_5 denote the set of intensive DMB attackers on Chain$_j$. Algorithm 3 can be performed to detect intensive DMB attackers.

Algorithm 3 Intensive DMB attacker detection

```
Input: $\Phi_1$, $\mathrm{lt}_{ij}$, $\mathrm{gt}_i$, $t_i$, $f_i$, $L_j$, $N_j$, $F_{ij}^k$
Output: $\Phi_5$
Acquire users' experience from the side chain
Extract $\psi^{\mathrm{T}}$ and $\gamma$ from the experience
Construct $f(x)=\frac{1}{2}\|\psi\|^2+\sum_{r=1}^{s}\mu_r(1-p_{ij}(\psi^{\mathrm{T}}x_r+\gamma))$
Export the prediction model
for each $U_i\in\Phi_1$ do
    Enter ($\mathrm{lt}_{ij}$, $\mathrm{gt}_i$, $t_i$, $f_i$, $L_j$, $N_j$, $F_{ij}^k$) into the prediction model
    Obtain $p_{ij}$
    if $p_{ij}$==+1 then
        $\Phi_5=\{U_i\}\cup\Phi_5$
    end if
end for
```

3.4 Trusted miner selection in a multi-chain environment

Current mainstream consensus protocols generally require more than 51% of users perform miner duties. At the beginning of the network, the first miner could be randomly generated. Once there is a history of behaviors, honest users should be selected as trusted miners. Fig. 5 shows the relationship of trusted miner selection.

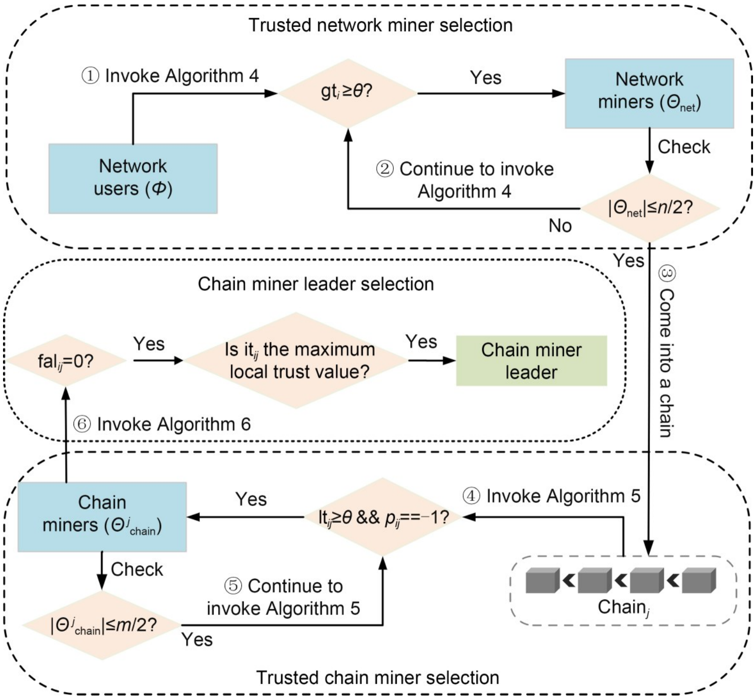
Trusted network miner selection
① Invoke Algorithm 4
gt$_i$≥θ?
Yes
Network miners (Θ_{net})
Network users (Φ)
Check
② Continue to invoke Algorithm 4
$|\Theta_{\text{net}}|\le n/2$?
No
Yes
③ Come into a chain
Chain miner leader selection
fal$_{ij}$=0?
Yes
Is it$_{ij}$ the maximum local trust value?
Yes
Chain miner leader
⑥ Invoke Algorithm 6
Chain miners (Θ^j_{chain})
Yes
lt$_{ij}$≥θ && p_{ij}==−1?
④ Invoke Algorithm 5
Check
⑤ Continue to invoke Algorithm 5
$|\Theta^j_{\text{chain}}|\le m/2$?
Yes
Chain$_j$
Trusted chain miner selection

Fig. 5 Relationship of trusted miner selection

Algorithm 4 can be triggered to select trusted network miners (Θ_{net}) from the entire network of users (Φ).

```
Algorithm 4  Trusted network miner selection
Input: $\Phi$, $\Xi$
Output: $\Theta_{\text{net}}$
for each $U_i \in \Phi$ do
    if $\text{gt}_i \ge \theta$ then
        $\Theta_{\text{net}}=\{U_i\}\cup\Theta_{\text{net}}$
    end if
end for
repeat
    if $|\Theta_{\text{net}}|\le n/2$ then
        Randomly select a user $U_p$ from $\Phi$
        $\Theta_{\text{net}}=\{U_p\}\cup\Theta_{\text{net}}$
    end if
until $|\Theta_{\text{net}}|>n/2$
```

Trusted network miner selection should be a dynamic updating process. Once $\text{gt}_i<\theta$, U_i will be removed from Θ_{net}. When $|\Theta_{\text{net}}|\le n/2$ due to the removal of unqualified miners, Algorithm 4 must be triggered again.

In our consensus scheme, only the chain miners (Θ_{chain}) selected from Θ_{net} have the authority to create blocks. Taking Chain$_j$ as an example again, Λ_j denotes the set of active users who often participate in Chain$_j$ activities. Since the number of active users is dynamic, the maximum number of active users over a period of time can be used to measure the required number of chain miners. That is, $|\Theta^j_{\text{chain}}|>m/2$, where m denotes the maximum number of active users in a blockchain.

In a round of block creation, Algorithm 5 can be performed to select trusted chain miners (Θ^j_{chain}) on Chain$_j$.

```
Algorithm 5  Trusted chain miner selection on Chain$_j$
Input: $\Lambda_j$, $\Theta_{\text{net}}$, $\text{LT}_{n\times h}$
Output: $\Theta^j_{\text{chain}}$
for each $U_i \in \Lambda_j$ do
    if $U_i \in \Theta_{\text{net}}$ then
        Perform Algorithm 3
        if $p_{ij}==-1$ && $\text{lt}_{ij}\ge\theta$ then
            $\Theta^j_{\text{chain}}=\{U_i\}\cup\Theta^j_{\text{chain}}$
        end if
    end if
end for
repeat
    if $|\Theta^j_{\text{chain}}|\le m/2$ then
        Randomly select a user $U_q$ from $\Lambda_j$
        $\Theta^j_{\text{chain}}=\{U_q\}\cup\Theta^j_{\text{chain}}$
    end if
until $|\Theta^j_{\text{chain}}|>m/2$
```

After a block is created, the chain miner leader shall be elected periodically to confirm the block validation and accept it. Algorithm 6 can be performed to elect and update the chain miner leader (L_j) on Chain$_j$.

When $\text{fal}_{ij}\geq 1$ or the lifetime of L_j has expired, Algorithm 6 must be triggered again to update the chain miner leader.

Algorithm 6 Chain miner leader selection

```
Input: $\Theta^j_{\text{chain}}$
Output: $L_j$
Initialize the set of chain miner leader $\Theta_L=\varnothing$
for each $U_i\in\Theta^j_{\text{chain}}$ do
    if $\text{fal}_{ij}==0$ then
        $\Theta_L=\{U_i\}\cup\Theta_L$
    end if
end for
for each $U_i\in\Theta_L$ do
    if $\text{lt}_{ij}$ is the maximum local trust value from $\Theta_L$ then
        $L_j=U_i$
    end if
end for
```

4 Security analysis

In addition to DMB attacks, our PoDT scheme can defend against denial-of-service, spoofing, eclipse, and replay attacks. The security analysis against these threats is as follows:

Challenge 1 Malicious users may launch DMB attacks on different chains to undermine the consensus process. DMB attackers can be friendly in the consensus process of mask chains to enhance their trust value and maintain honest miners, while in kill chains they engage in behaviors that undermine the consensus process.

Lemma 1 PoDT is resistant to DMB attacks.

Proof In our PoDT scheme, we introduce DiscTrust to evaluate the local and global trust values of each user across different chains. Normal DMB attackers can be detected due to their low local trust value on kill chains. We also propose a DBP scheme based on DiscTrust. Intensive DMB attackers can be detected when the prediction result is +1.

Challenge 2 After a block is created on a chain, the chain miner leader is responsible for confirming block validation and accepting it. When a chain miner leader processes block creation many times, he/she may be located by malicious users and paralyzed through denial-of-service attacks, thus making block creation in the consensus process impossible.

Lemma 2 PoDT is resistant to denial-of-service attacks.

Proof In our PoDT scheme, chain miners are not fixed in different chains, but dynamically elected and updated by Algorithm 6. We can set the maximum waiting time for block creation. If the response time of the chain miner exceeds the maximum waiting time, the smart contract will automatically call Algorithm 6 to elect a new chain miner leader.

Challenge 3 Malicious users infiltrate the miners and then submit false blocks through spoofing attacks to disrupt the consensus process.

Lemma 3 PoDT is resistant to spoofing attacks.

Proof In our PoDT scheme, trust management is adopted to suppress spoofing attacks. We can eliminate fake block creators from the ranks of miners using the trust value computation. A user is recognized as honest only if both the local and global trust values associated with all chains are high.

Challenge 4 After locating the chain miner leader, malicious users take advantage of the peer-to-peer characteristics of blockchain networks to control the surrounding neighbor nodes, making them isolated and unable to forward block validation and accept messages through routing, thus disrupting block creation.

Lemma 4 PoDT is resistant to eclipse attacks.

Proof In our PoDT scheme, the chain miner leader is dynamically elected and updated by Algorithm 6. We can ask each miner to send a reachable detection message to the chain miner leader before packing a new block. If a timely reachable response is returned, the new block is submitted to the chain miner leader for verification and acceptance. If an unreachable response is returned, the smart contract will automatically call Algorithm 6 to elect a new chain miner leader.

Challenge 5 When a new block is created, malicious users use the network delay to impersonate the chain miner and submit false blocks through replay attacks.

Lemma 5 PoDT is resistant to replay attacks.

Proof In our PoDT scheme, ID-based signatures can be used for message interactions between the chain miner leader and miners in block creation. Along with embedding the message timestamp, each chain miner loads a digital signature when submitting a new block. The private key is used to generate signatures and the public key is used to verify signatures.

5 Simulation analysis

5.1 Simulation setup

The performance of the proposed PoDT consensus scheme was analyzed through simulations using Python 3.7. The parameters used in the simulations are listed in Table 2.

Table 2 Description of parameters used in the simulations

Parameter	Description	Default value
N_u	Number of users	1000
N_c	Number of chains	10
θ	Threshold of the trust value	0.5
ξ_1	Trust warning line	0.1
ξ_2	High trust line	0.4
N_{cyc}	Number of cycles	200

We set up a blockchain network with 10 chains, in which four chains were randomly selected as kill chains and the others were mask chains. When network users were selected as miners to create blocks, they were divided into four types.

Trusted miners always create true blocks on all chains, while ordinary attackers always create false blocks on all chains. Normal DMB attackers create only false blocks on kill chains, but they behave well on mask chains. Intensive DMB attackers alternately create true or false blocks on kill chains.

5.2 Simulation results

We set up the peer-to-peer consensus process of the blockchain network and performed eight simulations to validate the effectiveness of PoDT. Simulations 5–8 are described in Section 2 of the supplementary materials.

The first three simulations were performed in a cycle-based fashion to further analyze DMB attacks and show the performance of PoDT's two-level defense scheme, which includes DiscTrust and DBP.

In the first simulation, we compared DMB attacks with ordinary attacks in terms of the global trust value. We chose an attacker from each of the three types of malicious users. As shown in Fig. 6, the global trust value of an ordinary attacker was far below the threshold θ. Thus, ordinary attackers could be easily detected by trust management. Along with 200 cycles, both the ordinary and intensive DMB attackers had a global trust value far above the threshold θ. As a result, common trust management systems would find it difficult to detect attackers.

To distinguish between normal and intensive DMB attackers, we randomly selected two kill chains and further observed their local trust values. As shown in Fig. 7, the local trust value of a normal DMB attacker was far below the threshold θ on kill chains, while the local trust value of an intensive DMB attacker was far above the threshold θ.

To perform simulations better, it was necessary to select a rational value of θ. As $\mathrm{gt}_i\in[0, 1]$ and $\mathrm{lt}_{ij}\in[0, 1]$, θ could be considered from the three types of optional states (low, medium, and high). Then, we could perform the first simulation under the three types of optional states of θ, in which 0.3, 0.5, and 0.8 denoted

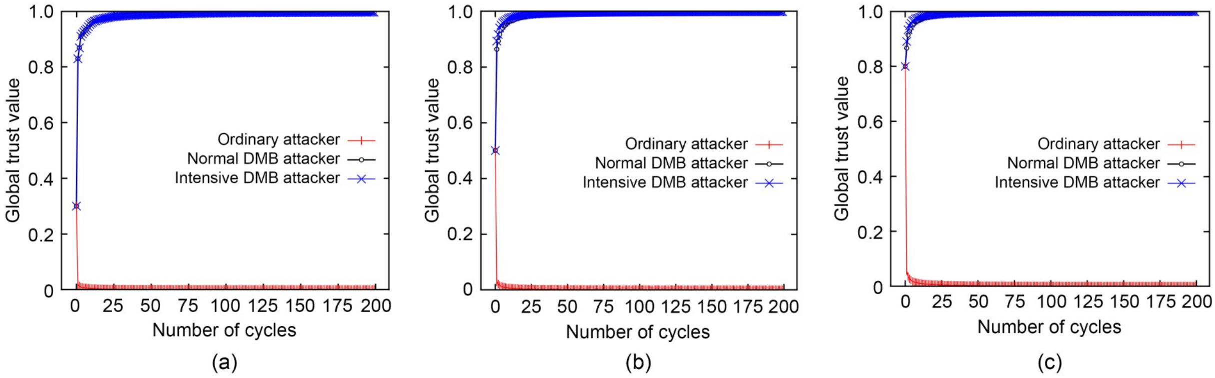

Fig. 6 Global trust values of different attackers: (a) θ=0.3; (b) θ=0.5; (c) θ=0.8

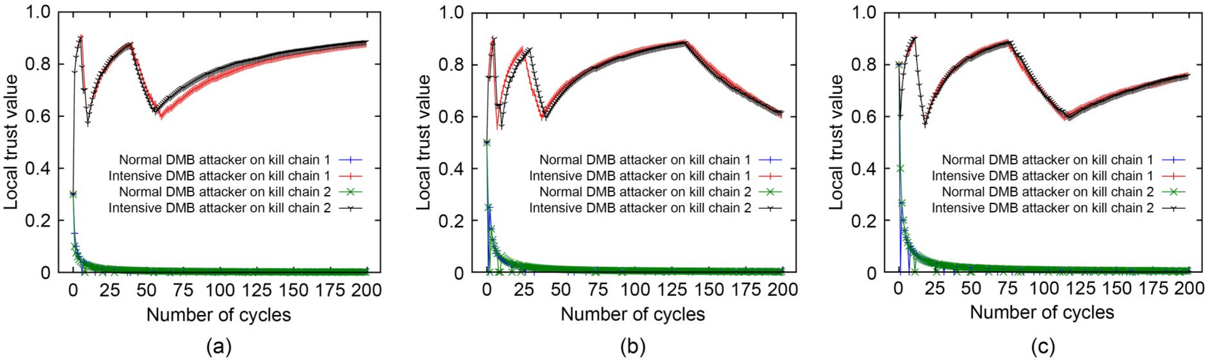

Fig. 7 Local trust values of different diverse miner behavior (DMB) attackers on kill chains: (a) θ=0.3; (b) θ=0.5; (c) θ=0.8

the low, medium, and high states of θ, respectively. If θ is overly low, such as 0.3, it is easy for an attacker to pretend to be a high truster. If θ is overly high, such as 0.8, some users' accidental errors may cause them to be misjudged as low trusters. As shown in Figs. 6 and 7, there was no significant difference between the results of the trust value simulation for those with θ= 0.5 and those with θ=0.8. Therefore, the rational value of θ was selected as 0.5 in the simulations.

Malicious users launch DMB attacks to increase their trust value, which may lead to a large number of malicious responses at each cycle. The DMB malicious responses may result in an unnecessary waste of network resources. So, reducing these malicious responses is the best approach for suppressing DMB attacks.

In the second simulation, we validated the performance of the DiscTrust scheme in reducing normal DMB malicious responses and the DBP scheme in reducing intensive DMB malicious responses.

Two trust evaluation schemes, Baseline and DiscTrust, were compared. As shown in Fig. 8, the number of normal DMB malicious responses of Baseline was much larger than that of DiscTrust. In the Baseline scheme, the trust value of each user was evaluated by his/her previous behaviors on all chains. In the DiscTrust scheme, the trust value of each user should be evaluated by considering his/her previous behaviors on different chains. Without any such trust evaluation measure in the Baseline scheme, the local trust value of normal DMB attackers slowly decreased and they can obtain more opportunities to launch DMB attacks, resulting in the most malicious responses. With the DiscTrust scheme, normal DMB attackers were prevented from joining the chain miners because of their lower trust value, thus suppressing malicious responses.

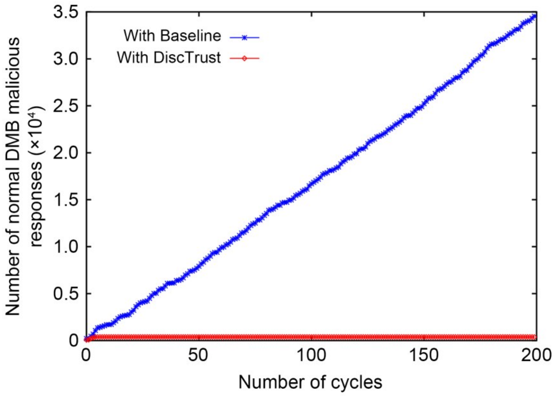

Fig. 8 Suppressing normal diverse miner behavior (DMB) malicious responses

We also compared the DiscTrust scheme with or without DBP. To further detect intensive DMB attackers, DBP is a dynamic behavior prediction scheme based on DiscTrust. As shown in Fig. 9, DBP could suppress intensive DMB malicious responses effectively, since it can predict intensive DMB attackers based on their experience.

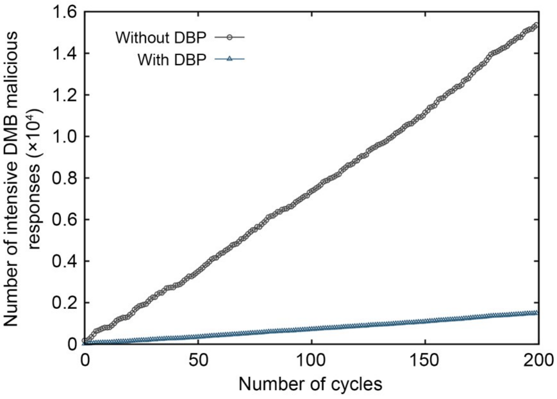

Fig. 9 Suppressing intensive diverse miner behavior (DMB) malicious responses

In the third simulation, we further evaluated the performance of the two-level defense scheme in suppressing the attack success ratio. Without loss of generality, the success rate of attacks was defined as the ratio of the number of false blocks successfully created by DMB attackers in each cycle to the number of newly created blocks.

As shown in Fig. 10, the normal DMB attack success ratio in DiscTrust was lower than that in Baseline. Under the protection of distinctive trust evaluation, normal DMB attackers could be effectively detected by analyzing their local trust values on kill chains, so their attacks could not succeed. As shown in Fig. 11, DBP could effectively reduce the success ratio of intensive DMB attacks.

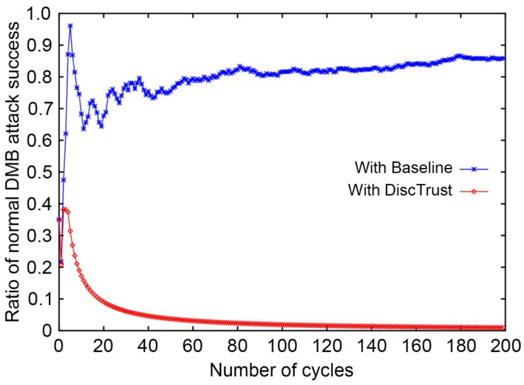

Fig. 10 Normal diverse miner behavior (DMB) attack success ratio

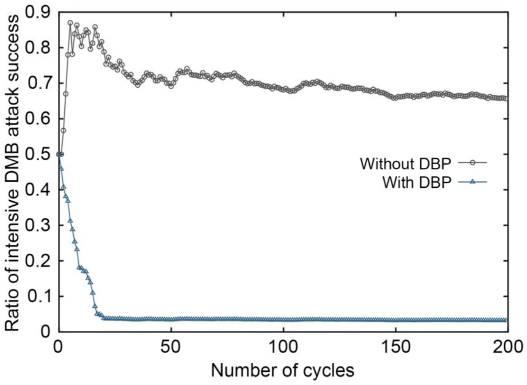

Fig. 11 Intensive diverse miner behavior (DMB) attack success ratio

How well does DBP detect DMB attackers with intensive attacks? As the number of users increased from 1000 to 10 000, the detection rate of DBP for intensive DMB attackers can generally reach 90% (Fig. 12). A better detection rate can be achieved even if the percentage of intensive DMB attackers was 50%. Even though the number of nodes was increasing, the dataset was larger. The DBP scheme can analyze more data and increase the detection rate.

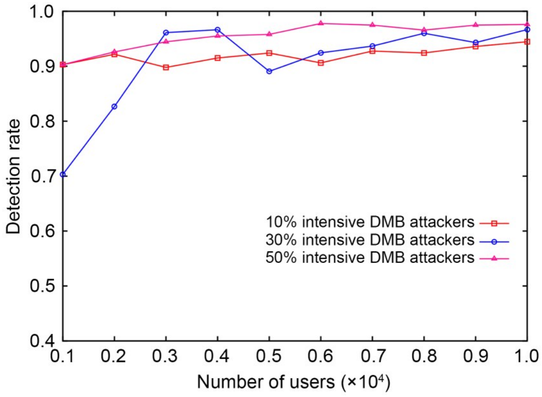

Fig. 12 Detection rate of dynamic behavior prediction (DBP)

In the fourth simulation, we compared PoDT with Tendermint (Buchman, 2016) and Proof of Reputation (PoR) (Alzahrani and Bulusu, 2018). These two common types of consensus schemes are based on fair multi-miner participation, where each user can fairly compete to become a miner in a blockchain network. In PoDT, trusted miners participate in the consensus process. In Tendermint, all nodes are selected as miners in the consensus process. In PoR, some nodes are randomly selected as miners in the consensus process.

In the simulation, attackers fell into three categories: ordinary attackers, normal DMB attackers, and intensive DMB attackers. The numbers of these three types of attackers were randomly assigned below a certain percentage. We varied the percentage of attackers to compare the accuracy.

As shown in Fig. 13, PoDT achieved high accuracy. On mask chains, it had the highest accuracy. Even when the accuracy of PoDT dropped slightly on the kill chain, it was still better than those of Tendermint and PoR. From the perspective of the entire blockchain network, PoDT was slightly better than the others since trust management was considered to select honest miners. Although the accuracy of PoDT dropped when the percentage of attackers exceeded 50%, such extreme cases do not occur in real blockchain networks.

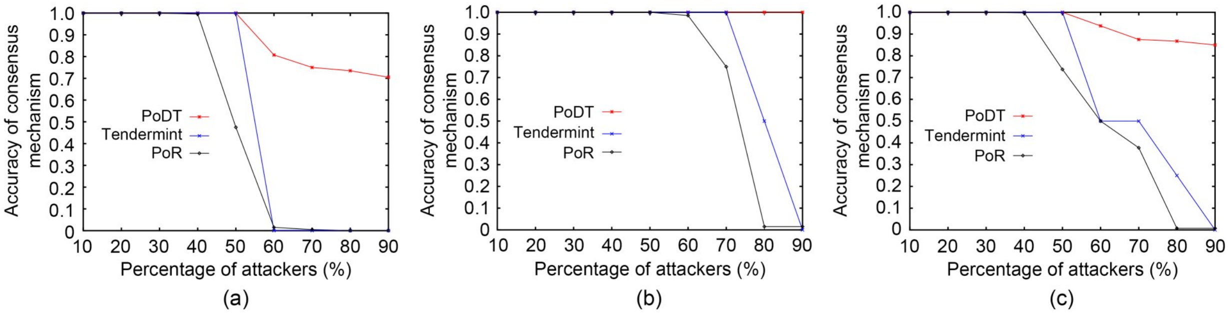

Fig. 13 Accuracy comparison of PoDT, Tendermint, and PoR: (a) kill chains; (b) mask chains; (c) whole blockchain network

6 Industrial applications

In this paper, we described the existence of DMB attack behaviors in multi-chain parallel blockchain networks. Traditional single-chain consensus mechanisms can maintain the accuracy of block creation but cannot accurately detect DMB attacks; therefore, we proposed a multi-chain consensus mechanism named PoDT.

After a thorough analysis, we found that the proposed PoDT scheme could be applied to scenarios involving multi-chain consensus security, such as medicine, electricity, finance, and manufacturing. For example, in a medical scenario, it could help build a medical data-sharing alliance to overcome the "data island" in healthcare (see supplementary materials, Section 3).

7 Conclusions and future work

In this paper, we proposed an advanced consensus scheme named PoDT for a multi-chain environment to defend against DMB attacks in blockchain networks. Two types of DMB attacks can be launched: normal and intensive. With the help of local trust values, DiscTrust was introduced to detect normal DMB attackers since they always behave viciously on kill chains. Even if intensive DMB attackers have the ability to maintain high trust on kill chains, the DBP scheme can strengthen DiscTrust to detect them. On this basis, three algorithms were designed to select trusted miners for multi-chain environments. Simulation results showed that our scheme is secure against DMB attacks in multi-chain environments. More importantly, simulation results showed that PoDT is more effective than Tendermint and PoR in terms of block creation.

Cross-chain technologies can connect multiple chains to form an Internet of Chains, which extensively expands the application of the blockchain. In future work, we will investigate the cloud-assisted Internet of Chains for threat intelligence sharing, where our PoDT scheme can ensure the security of multi-chain consensus.

Contributors

Wenbo ZHANG and Jingyu FENG designed the research. Tao WANG and Chaoyang ZHANG processed the data. Wenbo ZHANG and Tao WANG drafted the paper. Jingyu FENG helped organize the paper. Wenbo ZHANG and Jingyu FENG revised and finalized the paper.

Conflict of interest

All the authors declare that they have no conflict of interest.

Data availability

Due to the nature of this research, participants of this study did not agree for their data to be shared publicly, so supporting data are not available.

References

Alzahrani N, Bulusu N, 2018. Towards true decentralization: a blockchain consensus protocol based on game theory and randomness. Proc 9th Int Conf on Decision and Game Theory for Security, p.465-485. https://doi.org/10.1007/978-3-030-01554-1_27

Azaria A, Ekblaw A, Vieira T, et al., 2016. MedRec: using blockchain for medical data access and permission management. 2nd Int Conf on Open and Big Data, p.25-30. https://doi.org/10.1109/OBD.2016.11

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.

Buterin V, 2022. Chain Interoperability. Available from https://www.r3.com/reports/chain-interoperability [Accessed on Oct. 20, 2022].

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

Chaudhary R, Jindal A, Aujla GS, et al., 2019. BEST: blockchain-based secure energy trading in SDN-enabled intelligent transportation system. *Comput Secur*, 85:288-299. https://doi.org/10.1016/j.cose.2019.05.006

Chen CH, Chen X, Yu JS, et al., 2021. Impact of temporary fork on the evolution of mining pools in blockchain networks: an evolutionary game analysis. *IEEE Trans Netw Sci Eng*, 8(1):400-418. https://doi.org/10.1109/TNSE.2020.3038943

Cheng HJ, Xie Z, Shi YS, et al., 2019. Multi-step data prediction in wireless sensor networks based on one-dimensional CNN and bidirectional LSTM. *IEEE Access*, 7:117883-117896. https://doi.org/10.1109/ACCESS.2019.2937098

Ding XJ, Guo JX, Li DY, et al., 2021. An incentive mechanism for building a secure blockchain-based Internet of Things. *IEEE Trans Netw Sci Eng*, 8(1):477-487. https://doi.org/10.1109/TNSE.2020.3040446

Feng JY, Zhao XY, Chen KX, et al., 2020. Towards random-honest miners selection and multi-blocks creation: proof-of-negotiation consensus mechanism in blockchain networks. *Fut Gener Comput Syst*, 105:248-258. https://doi.org/10.1016/j.future.2019.11.026

Frankenfield J, 2023. What Does Proof-of-Stake (PoS) Mean in Crypto? Available from https://www.investopedia.com/terms/p/proof-stake-pos.asp [Accessed on June 1, 2023].

Gupta R, Tanwar S, Tyagi N, et al., 2019. HaBiTs: blockchain-based telesurgery framework for Healthcare 4.0. Int Conf on Computer, Information and Telecommunication Systems, p.1-5. https://doi.org/10.1109/CITS.2019.8862127

He HY, 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 Access*, 8:66116-66130. https://doi.org/10.1109/ACCESS.2020.2985577

Herlihy M, 2018. Atomic cross-chain swaps. Proc ACM Symp on Principles of Distributed Computing, p.245-254. https://doi.org/10.1145/3212734.3212736

Hewa TM, Kalla A, Nag A, et al., 2020. Blockchain for 5G and IoT: opportunities and challenges. IEEE 8th Int Conf on Communications and Networking, p.1-8. https://doi.org/10.1109/ComNet47917.2020.9306082

Hou H, 2017. The application of blockchain technology in e-government in China. 26th Int Conf on Computer Communication and Networks, p.1-4. https://doi.org/10.1109/ICCCN.2017.8038519

Kumar P, Kumar R, Srivastava G, et al., 2021. PPSF: a privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. *IEEE Trans Netw Sci Eng*, 8(3):2326-2341. https://doi.org/10.1109/TNSE.2021.3089435

Liu DX, Huang C, Ni JB, et al., 2021. Blockchain-based smart advertising network with privacy-preserving accountability. *IEEE Trans Netw Sci Eng*, 8(3):2118-2130. https://doi.org/10.1109/TNSE.2020.3027796

Nakamoto S, 2008. Bitcoin: a Peer-to-Peer Electronic Cash System. Available from https://bitcoin.org/bitcoin.pdf [Accessed on Oct. 20, 2022].

Peters GW, Panayi E, Chapelle A, 2015. Trends in cryptocurrencies and blockchain technologies: a monetary theory and regulation perspective. *J Finan Persp*, 3(3):92-113.

Sharma PK, Kumar N, Park JH, 2019. Blockchain-based distributed framework for automotive industry in a smart city. *IEEE Trans Ind Inform*, 15(7):4197-4205. https://doi.org/10.1109/TII.2018.2887101

Shi GH, Zhong H, Chen WG, 2008. Study on the models of cross-chain inventory collaboration in the cluster supply chain. IEEE Int Conf on Service Operations and Logistics, and Informatics, p.2114-2118. https://doi.org/10.1109/SOLI.2008.4682883

Xiong NX, Vasilakos AV, Wu J, et al., 2012. A self-tuning failure detection scheme for cloud computing service. IEEE 26th Int Parallel and Distributed Processing Symp, p.668-679. https://doi.org/10.1109/IPDPS.2012.126

Zhang W, Zhu SW, Tang J, et al., 2018. A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks. *J Supercomput*, 74(4):1779-1801. https://doi.org/10.1007/s11227-017-2150-3

Zheng ZB, Xie SA, Dai HN, et al., 2018. Blockchain challenges and opportunities: a survey. *Int J Web Grid Serv*, 14(4):352-375. https://doi.org/10.1504/IJWGS.2018.095647

List of supplementary materials