Anti-Collusion Multiparty Smart Contracts for Distributed Watchtowers in Payment Channel Networks

Miao Du, Peng Yang, *Member, IEEE*, Wen Tian, *Member, IEEE*, and Zhu Han, *Fellow, IEEE*

***Abstract*— Leveraging watchtowers to monitor payment channel networks (PCNs) is regarded to be a promising option to ensure off-chain transaction security and boost cryptocurrency scalability. However, existing solutions have two major limitations: First, since the watchtower's inaction or collusion with counterparties, the deposits in off-chain transactions will be threatened; Second, due to occasional false positives, the efficiency of the single watchtower in monitoring the payment channels for fraud is questionable. To solve this, we present anti-collusion multiparty smart contracts for distributed watchtowers in PCNs. Specifically, we first design the distributed watchtower mechanism to solve the false positive problem in regulating PCNs. In addition, we utilize smart contracts to constrain and force counterparties to relinquish collusion in the distributed watchtower mechanism, thus making collusion impossible for rational parties. We further offer a mathematical proof and contract implementation in Solidity. Finally, extensive experiments and contracts executed on Ethereum under various benchmarks with baseline comparison demonstrate the validity of our proposals. Specifically, our scheme can both improve the throughput and accuracy by up to 20-25% and 10-15%, respectively, and reduce the false positive rate by up to 10% compared with existing single watchtower mechanism.**

***Index Terms*— Watchtowers, payment channel networks, collusion attacks, smart contract, crypto-economy, ethereum.**

I. Introduction

With the massive expansion of users and transactions, the scalability of cryptocurrencies has become an imminent problem. According to [1], the average transaction fee for Bitcoin transactions is over $19. The low transaction throughput and high transaction fees have severely constrained the development of cryptocurrencies (*e.g.*, Bitcoin [2] and Ethereum [3]).

To address the dilemma of cryptocurrencies, payment channel networks (PCNs) provide a promising solution for micro and high-frequency transactions [4]. PCNs permit both parties to change the settlement scheme to achieve off-chain transaction. Specifically, the blockchain only records the opening and closing of the channel, and provides security for off-chain transactions, while both parties only write the transactions that create and close the payment channel to the blockchain; however, there is no limit to the number of off-chain transactions [5]. In order to avoid a payment channel where one party is offline and the other party is unable to close the payment channel and retrieve the funds, the payment channel allows participants to independently close the payment channel by sending the latest channel state proof (CSP) at any time [6]. However, the blockchain cannot determine whether the submitted state is the latest one, and a malicious participant may send a fraud CSP to close the payment channel, thereby reaping additional payoffs. This security risk requires channel participants to stay online regularly to monitor the state of transactions and synchronize with the blockchain [7]. According to [8], there are only 10,126 and 6,061 active users in Bitcoin and Ethereum who can continuously synchronize with the blockchain, respectively, representing less than 0.1% of all cryptocurrency users. Therefore, the majority of blockchain users face security concerns when implementing off-chain transactions in payment channels.

Fortunately, watchtowers have recently shown great potential to solve these issues. Large-scale blockchain communities such as Bitcoin and Ethereum have begun to implement watchtower mechanisms to supervise off-chain payment channels, thereby reducing the security risk of channel deposits. The prototype of watchtowers first appeared in the Lightning White Paper [9]. The core idea is to monitor counterparty fraud and issue default compensation transactions through a third-party agent. Once the watchtowers discover that the payment channel is settling with fraud CSPs, the security mechanism will be activated immediately to help users recover losses and punish malicious participants [10]. In recent years, researchers and development teams have been continuously proposing sophisticated technical solutions for the watchtower mechanism. For instance, McCorry et al. [11] proposed the Pisa protocol, Avarikioti et al. [12] proposed the distributed service protocol Disclose Cascade Watch Commit (DCWC) for

Manuscript received 14 February 2022; revised 14 June 2022; accepted 30 June 2022. Date of publication 17 October 2022; date of current version 22 November 2022. This work was supported in part by the Consulting Project of Chinese Academy of Engineering under Grant 2020-XY-5 and Grant 2018-XY-07, in part by the Fundamental Research Funds for the Central Universities and the Academy-Locality Cooperation Project of Chinese Academy of Engineering under Grant JS2021ZT05, in part by the Nanjing University of Information Science and Technology Talent Start-Up Funds under Grant 2022r068, and in part by NSF under Grant CNS-2107216 and Grant CNS-2128368. *(Corresponding author: Peng Yang.)*

Miao Du and Peng Yang are with the Key Laboratory of Computer Network and Information Integration, School of Computer Science and Engineering, Southeast University, Ministry of Education, Nanjing 211189, China (e-mail: dumiao0118@seu.edu.cn; pengyang@seu.edu.cn).

Wen Tian is with the School of Electronic and Information Engineering, Nanjing University of Information Science and Technology, Nanjing 211544, China (e-mail: csusttianwen@163.com).

Zhu Han is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul 446-701, South Korea (e-mail: hanzhu22@gmail.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JSAC.2022.3213355.

Digital Object Identifier 10.1109/JSAC.2022.3213355

watchtowers, as well as the watchtower incentive-compatible Cerberus channel [13]. In addition to academic research, the industry is also trying to implement watchtower mechanisms in real-world scenarios. For example, Lightning Labs first integrated watchtower technology into an expiring lightning network [14]. BitMEX upgraded its lightning network nodes to a version that includes watchtower functionality [15].

Indeed, these proposals design and implement the watchtower mechanism in PCNs. However, there still exist some daunting challenges that are unsolved. First, watchtowers may have an impact on the security of the payment channels. If the watchtower is a trusted third party, users can go offline at will without fear of malicious shutdown of the payment channel. In reality, neither watchtowers nor payment channel participants are necessarily trusted, as watchtowers may be passive or conspire with malicious nodes in the channel to inflict losses on honest users. The watchtower collusion issue has also been studied by some researchers. Zhang et al. [6] combined game theory and smart contract approaches to solve the watchtower collusion problem in PCNs. Nevertheless, we observe that the single watchtower mechanism suffers from the false positives problem. It is impossible to accurately determine whether this false positive is related to the collusion, thus rendering the efficiency and quality of supervision transactions.

Motivated by such facts, in this article, we propose *anti-collusion multiparty smart contracts for distributed watchtowers in PCNs*. Specifically, a hiring party can choose to engage multiple watchtowers, and then freely decide whether to go offline. The watchtowers can either earn payoffs from each detected fraud or just by monitoring PCNs. On the other hand, the hiring party sends the latest CSPs to the watchtowers after each transaction, while the counterparty intends to close the channel by sending fraud CSPs. In return, the watchtowers also need to offer proof to the hiring party that they have been monitoring the blockchain and storing CSPs. Once the counterparty's malicious behavior is monitored by the watchtowers, the counterparty will be punished, and the watchtower will receive revenue accordingly. Nonetheless, if one of the watchtowers fails to respond in time or incurs a false positive, it will also be punished and the payoffs will be deducted. We design smart contracts to constrain the behavior and benefits of each participant. Considering that watchtowers and participants are not always trustworthy, rational participants may achieve more payoffs by initiating collusion. As a result, we devise four distinct smart contracts to circumscribe the collusion problem and provide rigorous mathematical proofs of the corresponding solution. Specifically, *the Watchtower Contract* is an employment contract between channel participants and watchtowers, where the latter obtains payoffs by monitoring the payment channel. To break the equilibrium of employment contracts, *the Collusion Contract* is designed as a collusion between two watchtowers to obtain additional payoffs. Additionally, there can be collusion between counterparties and a malicious watchtower, as analyzed in *the Fraud Contract*. Finally, *the Anti-collusion Contract* is devised to effectively resist the above two collusion attacks, making rational channel participants give up collusion. Last but not least, we use Solidity to implement the proposed smart contract scheme. In conclusion, this article makes the following contributions:

1) We are the first to investigate smart contracts to deploy distributed watchtowers against collusion attacks in PCNs. This scheme can be effective against collusion in PCNs, and also reduce watchtower false positives and improve regulatory efficiency.
2) We design and leverage four smart contracts (*i.e.,* Watchtower Contract, Collusion Contract, Fraud Contract and Anti-Collusion Contract) to constrain and counter possible collusion attacks in various outsourced watchtower scenarios.
3) We analyze smart contracts using game tree models and prove that there exists a unique sequential equilibrium for each contract. In accordance with rigorous mathematical derivations, it is proved that rational parties will never execute collusion or betray the contracts.
4) We conduct smart contracts in Solidity and execute them on Ethereum. In addition, we setup the distributed watchtower platform on NS3 and simulate false positive experiments. Experimental results show that our scheme can effectively defend against collusion attacks with a small cost. In addition, distributed watchtowers can effectively reduce the false positive rate, while improving the efficiency and quality of regulatory transactions.

The remainder parts of this article are organized as follows. Section II illustrates the related work. We further present the preliminaries in Section III. The system model is demonstrated in Section IV. Then, we devise and analyze four smart contracts in Sections V-VIII, respectively. After that, we describe the implementation and experiment results in Section IX. Finally, Section X draws the conclusion.

II. Related Work

In this section, we present the existing literatures on PCNs, and watchtowers for collusion attacks.

A. Payment Channel Networks

Payment channel network has flourished in recent years along with the growing Bitcoin community [16]. Specifically, the Lightning Network [17] has been a prominent proposal for a Bitcoin payment channel, providing secure and efficient off-chain transactions. In addition, industry has designed and implemented Thunder [18] and Eclair [19], as well as Raiden [20] to provide technical support for off-chain transactions in Bitcoin and Ethereum, respectively. On the other hand, academics have focused more on onion routing security and optimal routing algorithms for PCNs [21], [22], [23], [24]. Zhang et al. [21] designed the cheapest routing scenario by assuming that each PCN routing node imposes a constant tariff. Malavolta et al. [25] presented SilentWhisper to solve the security constraint in onion routing. The scheme anchors a security landmark [26] and requires that all paths must pass through the landmark, thus improving security and privacy. SpeedyMurmurs [27] designed embedded paths [28] to address the issue of long paths in landmark schemes. Yu et al. [29] addressed the problem of inefficient and

costly payments using a distributed routing algorithm, but without taking into account the constraining effect of transaction costs. Engelmann et al. [30] designed a streamlined routing model such that the actual transaction costs were only correlated with the payment amount, but the costs of interlocutory nodes cannot be accountable. Wang et al. [24] proposed a dynamically balanced algorithm for path optimisation and detectable envelope overhead in onion routing networks. Sivaraman et al. [31] ingeniously packaged massive transactions for processing and designed a path switching transmission algorithm [32] to improve transaction efficiency and throughput. Schnorr et al. [33] developed a public-key signature-based authentication mechanism to detect identity information in PCN networks. Zhang et al. [34] improved the HTLC protocol so that both its robustness and security were strengthened.

B. Watchtowers for Collusion Attacks

The security and scalability of off-chain transactions has drawn widespread attention from the Bitcoin community [35], [36], [37], [38]. The proposal and implementation of the watchtower mechanism [39] has brought an effective solution to this problem. Dryja et al. presented Monitor [40], which uses isolated witness technology to achieve secure protection of off-chain transactions. Osuntokunn et al. [41] designed and deployed Watchtower by modifying the consensus rules of the bitcoin network to improve the efficiency of execution efficiency. Both schemes default to the watchtower as a fully trusted third party, ignoring the economic losses caused by the watchtower's inaction. Pisa [11] and Outpost [42] provide the hiring party with hash-based cryptographically verifiable CSPs that can be used to penalize the watchtower for inaction. Cerberus [13] ensures the security of watchtowers by introducing a deposit mechanism. Liu et al. [43] proposed the Fail-safe scheme, which introduced a review mechanism so that a single watchtower could intervene in off-chain status updates and on-chain channel closures, and periodically send the latest CSPs to the channel contract to ensure security. Table I is the performance comparison of each watchtower scheme. Note that the majority of current state-of-art focuses on the security design optimization and implementation of watchtower protocols (*e.g.*, Pisa, Fail-safe and Cerberus), but there is little research on collusion attacks in PCNs. The traditional approach is to defend against collusion attacks through complex cryptography, which is effective but expensive and difficult to implement. Game theory provides a good idea as an emerging crypto-economy method [44], [45]. Zhang et al. [6] proposed a single watchtower mechanism and combined game theory and smart contract approaches to solve the collusion problem in PCNs. Nevertheless, single watchtower mechanism suffers from false positives, affecting the efficiency and quality of regulatory transactions. To this end, we propose a distributed watchtower mechanism to address the collusion problem in off-chain transactions. Specifically, we develop four different smart contracts and use a game theoretic approach to analyse the equilibrium to find the optimal solution rather than sophisticated encryption algorithms. In addition, we deal with the problem of high false positive rate of a single watchtower and improve the throughput and scalability.

TABLE I
THE PERFORMANCE COMPARISON OF EACH WATCHTOWER SCHEME

Scheme	Dryja	Cerberus	Pisa	Fail-safe	Zhang	Ours
Scenarios	Bitcoin	Bitcoin	Ethereum	Ethereum	Ethereum	Ethereum
Security	Low	Medium	High	High	High	High
Cost	High	Medium	Low	Low	Low	Low
Anti-Collusion	No	No	No	No	Yes	Yes
False Positive Rate	/	/	/	/	High	Low

III. PRELIMINARIES

In this section, we give a brief introduction to the finite imperfect-information extensive-form game, strategy profile, and sequential equilibrium.

A. Finite Imperfect-Information Extensive-Form Game

The transactions in the payment channel are anonymous and the channel participants cannot obtain complete information. Motivated by this, we design finite imperfect-information extensive-form game, and further use the game tree to visualize the equilibrium point of the game.

Definition 1 (Finite Imperfect-Information Extensive-Form Game): A finite imperfect-information extensive-form game [60] is defined as $\mathcal{G} = \{\mathcal{N},\ \mathcal{H},\ \mathcal{A},\ \mathcal{Z},\ z,\ \chi,\ i,\ \eta_i,\ \rho,\ \mathcal{I}\}$, where:

- $\mathcal{N}$ is a set of players in the game.
- $\mathcal{H}$ is a set of non-terminal nodes.
- $\mathcal{A}$ is a set of players' finite actions.
- $\mathcal{Z}$ is a set of terminal nodes.
- z is a terminal node, each z completely determines a path in the game tree, and $z \in \mathcal{Z}$.
- χ: $\mathcal{H} \rightarrow 2^{\mathcal{A}}$ is the possible action of each non-terminal node.
- i: $\mathcal{H} \rightarrow \mathcal{N}$ represents the action taken by player i at this node.
- η_i is a set of payoff functions, where $\eta_i(z)$: $\mathcal{Z} \rightarrow \mathcal{R}$ is player i's payoff function at terminal node z.
- ρ: $\mathcal{H} \rightarrow \mathcal{N}$ is an action that each player $i \in \mathcal{N}$ is designated to choose at a non-terminal node.
- $\mathcal{I} = (\mathcal{I}_1,\ \mathcal{I}_2, \ldots, \mathcal{I}_n)$ is a set of information collected by players when they choose their actions.

Game trees are commonly used in extensive-form games [48], which explain the strategies and information that players can use while taking actions, as well as the sequence in which they execute actions and the games' outcomes and payoffs. Fig. 1 is an example game tree. The action set in this game is $\mathcal{A} = \{U,\ M,\ D,\ L,\ F\}$, the chosen node and the terminal node is $\mathcal{H} = \{v_0,\ u_0,\ u_1,\ u_2\}$, and $z = \{l_0,\ l_1,\ l_2,\ l_3,\ l_4,\ l_5\}$, respectively. In addition, χ maps the chosen node to the action set. Specifically, the node of P_1 and P_2 is $\{v_0\}$ and $\{u_0,\ u_1,\ u_2\}$, respectively, while the action set of node $\{v_0\}$ and $\{u_0,\ u_1,\ u_2\}$ is $\{U,\ M,\ D\}$ and $\{L,\ F\}$, respectively. The game then continues to the child node on the edge indicated with action once the player has made their choice. Each player's payoff function is located

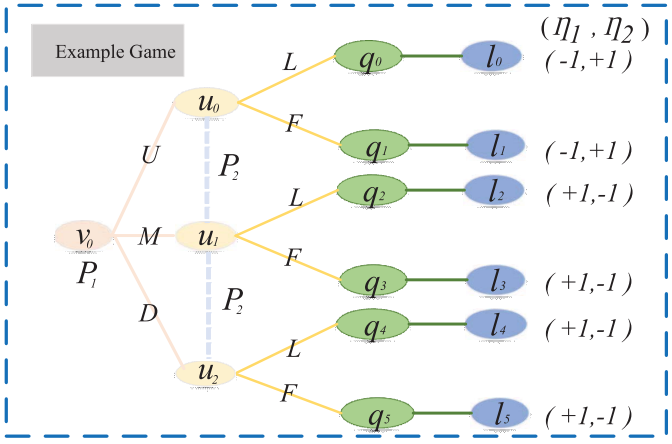

Fig. 1. Example game tree is a guidance for subsequent sequential games, in which action players P_1 and P_2 can choose the optimal strategy in the strategy set $\{U,\ M,\ D\}$ and $\{L,\ F\}$ to obtain the optimal payoff.

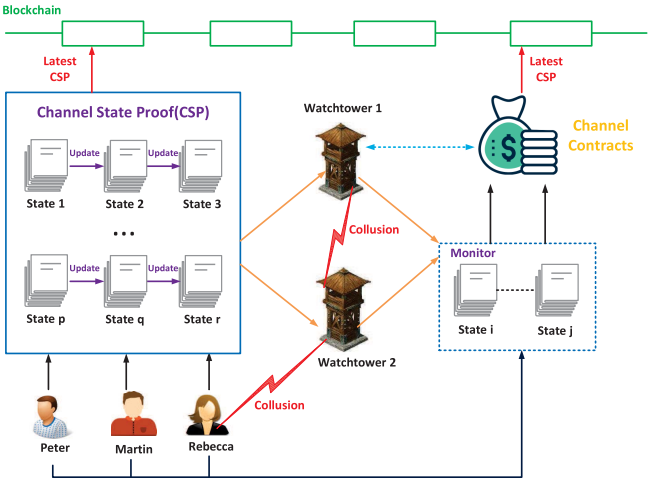

Fig. 2. The overview of our scheme. The watchtowers are responsible for monitoring PCNs in real time and regularly updating CSPs to match those sent by channel participants. Collusion risks can occur between two watchtowers, or between counterparty and malicious watchtowers. Our scheme adopts crypto-economy method and combines smart contracts to empower watchtowers to solve collusion attacks in PCNs.

to the right of the leaf node. Unless the information set has only one node, the information sets are represented as connected by dashed lines, that is, the participants cannot distinguish nodes in the same information set. For example, P_1 can rationally choose one of the strategies U, M or D to reach a certain child node according to the payoffs, which is unknown to P_2 since P_2 cannot know which specific strategy P_1 chooses.

B. Strategy and Sequential Equilibrium

We further give some necessary definitions about the strategy profiles and sequential equilibrium [46] in the following.

Definition 2 (Strategy & Strategy Profile): A strategy of a player i is a tuple of actions that specify the probability distribution of actions in each information set and are independent of each other under different information sets. In addition, a strategy profile of a game is a set of all players' strategies $s = (s_i)_{i \in \mathcal{N}}$.

Definition 3 (Sequential Equilibrium): If a strategy profile s is a sequential equilibrium of $\mathcal{G}$, there exist probability distributions η_i, which satisfy $(s,\ \eta) = \lim_{n \to \infty} (s_n,\ \eta_n)$ for some sequence $(s_1,\ \eta_1),\ (s_2,\ \eta_2), \ldots$, where s_n is fully mixed, and η_n is consistent with s_n.

TABLE II
LIST OF SYMBOLS IN THE PAPER

Symbols	Descriptions
$\mathcal{N}$	a set of players in the game
$\mathcal{H}$	a set of non-terminal nodes.
$\mathcal{A}$	a set of players' finite actions.
$\mathcal{Z}$	a set of terminal nodes.
z	a terminal node, and $z \in \mathcal{Z}$.
χ: $\mathcal{H} \to 2^{\mathcal{A}}$	the possible action of each non-terminal node.
i: $\mathcal{H} \to \mathcal{N}$	the action taken by player i at this node.
η_i	a set of payoff functions.
$\eta_i(z)$: $\mathcal{Z} \to \mathcal{R}$	player i's payoff function at terminal node z.
$\mathcal{I} = (\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_n)$	a set of information collected by players.
s	The deposit that counterparty and watchtowers pay.
c	The cost that watchtowers pay.
p	The bribe that W_1 paid to W_2 .
g	The deposit paid by the watchtowers.
r	The H_p agrees to compensate the watchtowers.
k	The cost of secondary proofreading.
e	The additional payoffs.
h	The deposit paid.
a	The bribe that the counterparty agreed to pay.

IV. System Model

In this section, we design the distributed watchtowers model, and introduce the contract parameters.

A. Distributed Watchtowers Model

As shown in Fig. 2, participants in off-chain transactions need to update their CSPs after each transaction is completed. Obviously, it is unrealistic for these participants to remain online for long periods of time. Therefore, participants can hire multiple watchtowers to assist off-chain transactions by signing smart contracts. However, collusion is still possible in this scenario. Specifically, the counterparty can enter into a contract with the watchtower to complete the fraud, thereby obtaining additional benefits. On the other hand, distributed watchtowers may also collude to defraud more commissions. To this end, we further devise various smart contracts to defend possible collusion attacks in various outsourced watchtower scenarios.

B. Contract Parameters

We assume that channel participants are rational players [6], and accordingly give the following contract parameters.

- s: The deposit that counterparty and watchtowers pay to the watchtower contract.
- c: The cost that watchtowers pay to monitor the payment channel.
- p: The bribe that $Watchtower_1(W_1)$ paid to $Watchtower_2(W_2)$ in the collusion contract.

- g: The deposit paid by the watchtowers in the collusion contract.
- r: The hiring party (H_p) agrees to compensate the watchtowers for monitoring the payment channel.
- k: The cost of secondary proofreading when the latest CSP feedback from the two watchtowers is inconsistent.
- e: The additional payoffs that counterparty can obtain by issuing a fraud CSP.
- h: The deposit paid by the counterparty and the watchtowers in the fraud contract.
- a: The bribe that the counterparty agreed to pay to the watchtowers in the fraud contract.
- z: The benefits from the watchtower that honestly monitors the payment channel, and $z = r - c + (s - k)/2$.

The above symbols have the following relationships:

1) $r \geq c$: the watchtowers otherwise cannot accept the hiring party's monitor request.
2) $e \geq a$: the counterparty is unwilling to pay more bribe in excess of the collusion.
3) $p < c$: W_2 agrees to collusion only if the bribe offered by W_1 is greater than the typical payoffs of W_2.

The detailed list of notations is provided in the Table II. Next, we will gradually design several smart contracts and analyze their equilibrium.

V. The Watchtower Contract

In this section, we We design the Watchtower contract and use game trees to analyze sequential equilibrium.

A. The Watchtower Contract

The watchtower contract is actually an outsourcing contract signed by the hiring party (H_p) and the two watchtowers W_1 and W_2, which allows the hiring party to entrust W_1 and W_2 to monitor the payment channel. However, the premise is that the watchtowers need to pay a deposit to the contract before monitoring the payment channel. Note that the deposit will be returned after verifying that the watchtower responds to the latest *CSP* in a timely manner and proves to be correct, while the watchtower that submits the fraud *CSP* will lose this deposit. If only one watchtower offers the correct *CSP*, the deposit of the watchtower that submitted the incorrect *CSP* will be paid to the trustworthy watchtower as a reward (after deducting the necessary fees). Although it appears that the two watchtowers colluding may achieve the maximum payoffs, both watchtowers may remain honest since they know the collusion is unstable, and the other party may betray and conspire to ensure their best payoffs. Therefore, they can try to obtain high payoffs by refusing the collusion. The contract's detailed steps are as follows:

1) The Watchtower contract is signed by H_p and W_1, and H_p and W_2, respectively.
2) H_p, W_1 and W_2 jointly follow the contract, and set three deadlines, $T_1 < T_2 < T_3$.
3) H_p agrees to pay funds r to the watchtower that submits the latest *CSP* correctly and timely.
4) W_1 and W_2 need to pay deposit s to the contract before the deadline T_1, otherwise the contract will be terminated, and the deposit can be temporarily managed by the contract.
5) W_1 and W_2 must submit the latest *CSPs* (y_1 and y_2) before the deadline T_2.
6) W_1 and W_2 have reported the latest *CSPs*, or after the deadline T_2:
   (a) If W_1 and W_2 cannot report the latest *CSP*, their deposits will be paid to H_p.
   (b) If W_1 and W_2 provide the same *CSP*, which means W_1 and W_2 have effectively monitored the payment channel, H_p needs to pay funds to W_1 and W_2, and the deposit can be returned to W_1 and W_2.
   (c) Otherwise, move to step (7).
7) Perform a second proofreading, and achieve the latest *CSP* as y_t:
   (a) If both W_1 and W_2 provide the correct *CSPs* y_1 and y_2, H_p must pay each watchtower and return their deposits, in addition to paying for the second proofreading fee.
   (b) If both W_1 and W_2 return the fraud *CSP*, their deposit will be paid to H_p, then H_p will pay the second proofreading fee.
   (c) If only one watchtower returns the fraud *CSP*, then the deposit of the watchtower will be paid to H_p. In addition, H_p cannot only pay for the second proofreading, but also pay $(s - k)/2$ additional rewards to the watchtower that provides the correct *CSP*, and return its deposit.
8) If H_p still fails to pay W_1 and W_2 after the deadline T_3, H_p will be required to pay W_1 and W_2 (provide *CSP* before the deadline T_2) according to the contract, and return their deposits.

The deadline ($T_1 < T_2 < T_3$) in the contract is used to enforce timeliness, which can prevent funds from being frozen if one party refuses to execute forward.

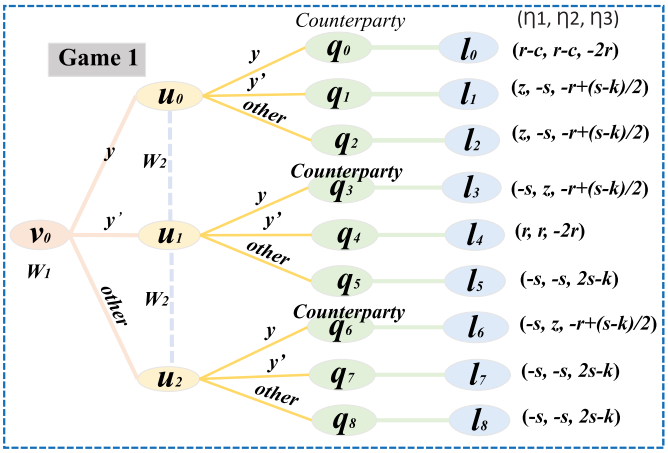

Fig. 3. *Game 1* induced by *the Watchtower Contract*.

B. Game Tree Analysis

Game 1 is induced by *the Watchtower Contract*. As shown in Fig. 3, the players are $N = \{Counterparty(C),\ W_1,\ W_2\}$,

and the action set is $A = \{y,\ y',\ other\}$, where y is the correct *CSP* returned by W_1 and W_2 before the deadline, and y' is the fraud *CSP* given by W if collusion occurs (obviously $y' \neq y$). Moveover, $other$ represents any other results that W may return. *Game 1* contains 5 information sets: $I_1 = \{v_0\}$, $I_2 = \{u_0,\ u_1,\ u_2\}$, $I_{3,1} = \{q_0,\ q_1,\ q_2\}$, $I_{3,2} = \{q_3,\ q_4,\ q_5\}$, $I_{3,3} = \{q_6,\ q_7,\ q_8\}$. In addition, η_1, η_2, η_3 is the payoff functions, and the payoffs of each party is listed next to the terminal node.

Next, we further analyze the strategies that all players will use in sequential equilibrium, as well as the conditions for achieving equilibrium. Formally, we have:

Theorem 1: If $e \geq a$ and $s > c + k$, Game 1 has a unique sequential equilibrium ($(s_1,\ s_2)$, $(\eta_1,\ \eta_2)$):

$$\begin{cases} s_1 = (1(y),\ 0(y'),\ 0(other)) \\ s_2 = (1(y),\ 0(y'),\ 0(other)) \\ \eta_1 = ([1(v_0)]) \\ \eta_2 = ([1(u_0),\ 0(u_1),\ 0(u_2)]). \end{cases}$$

According to the equilibrium, Game 1 will end at l_0.

Proof: We observe W_2's payoff at $u_0,\ u_1,\ u_2$, respectively. Note that the game will reach at nodes $\{q_0, q_1, q_2\}$, $\{q_3, q_4, q_5\}$, and $\{q_6, q_7, q_8\}$ when W_2 sends *CSP* $\{y, y', other\}$, respectively. Intuitively, the payoff of W_2 at q_0 is $(r-c)$, while the payoff at q_1 and q_2 is $(-s)$. Obviously, $(r-c)$ is positive, and $(r-c) > (-s)$. Analogously, W_2's payoff at node q_3 is z, which is better than r and $(-s)$ at nodes q_4 and q_5, while W_2's payoff at node q_6 is z, which is better than $(-s)$ at nodes q_7 and q_8, respectively. It can be judged that no matter what the strategy of W_1 is, W_2 will send *CSP* y to maximize its payoff. According to the above derivation, the actual reachable nodes of W_1 are q_0, q_3 and q_6, since W_2 is unable to send y' or $other$. Moreover, the payoff of W_1 at q_0 is $(r-c)$, which is better than $(-s)$ at q_3 and q_6, respectively. Therefore, W_1 will choose to send *CSP* y to maximize its payoff as well. ■

VI. The Collusion Contract

In this section, we present the Collusion contract and analyze the sequential equilibrium in this contract.

A. The Collusion Contract

The Collusion Contract aims to break *the Watchtower Contract*'s equilibrium. Furthermore, *the Collusion Contract* imposes additional rules that influence the all parties' payoffs, making collusion the most profitable option. In this contract, the watchtower that initiated the collusion will pay a bribe to the other watchtower to encourage the collusion. In addition, both watchtowers will pay a deposit when signing this contract. The deposits of the betrayal and conspiracy will be deducted. The detailed steps of the contract are as follows:

1) The Collusion contract is signed by W_1 and W_2. Assume that the collusion is initiated by W_1.
2) W_1 and W_2 agree to send fraud *CSPs* y' in *the Watchtower Contract*.
3) W_1 and W_2 need to pay deposits $p+g$ and g, respectively when signing the Collusion contract, and these two deposits are temporarily managed by *the Collusion Contract*.
4) W_1 and W_2 must pay the above deposits before the deadline $T_4 < T_2$. Otherwise, the contract will be forcibly terminated, and the deposits will be refunded.
5) When *the Watchtower Contract* ends, the following operations will be performed on the deposit balance held in *the Collusion Contract*:
   (a) If W_1 and W_2 both follow *the Collusion Contract*, the deposits g and $g+p$ will be returned to W_1 and W_2, respectively.
   (b) If W_2 betrays the contract, the deposit $2g+p$ will be returned to W_1, and W_2 will lose the deposit g.
   (c) If W_1 betrays the contract, the deposit $g+p$ will be returned to W_2, and W_1 will lose the deposit $g+p$.
   (d) If W_1 and W_2 both betray the contract, the deposits $g+p$ and g will be returned to W_1 and W_2, respectively.

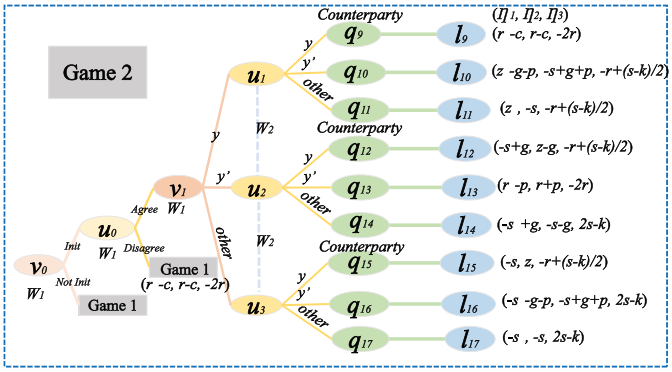

Fig. 4. *Game 2* induced by *the Collusion Contract* and *the Watchtower Contract*.

The Collusion Contract must be signed before the deadline T_2, since W_1 and W_2 need to send the latest *CSP* before the deadline T_2. The game induced by *the Collusion Contract* and *the Watchtower contract* is shown in Fig. 4. Actually, rational W_1 and W_2 will choose whether to sign *the Collusion Contract* according to their own payoffs. In this scenario, if only *the Watchtower Contract* is valid, the game will reach at *Game 1*.

B. Game Tree Analysis

Game 2 is induced by *the Watchtower Contract* and *the Collusion Contract*. The players are $N = \{C,\ W_1,\ W_2\}$, and the action set is $A = \{not\ init,\ init,\ disagree,\ agree,\ y,\ y',\ other\}$. As shown in Fig. 4, *Game 2* contains 7 information sets: $I_{1,1} = \{v_0\}$, $I_{1,2} = \{v_1\}$, $I_{2,1} = \{u_0\}$, $I_{2,2} = \{u_1,\ u_2,\ u_3\}$, $I_{3,1} = \{q_9,\ q_{10},\ q_{11}\}$, $I_{3,2} = \{q_{12},\ q_{13},\ q_{14}\}$, $I_{3,3} = \{q_{15},\ q_{16},\ q_{17}\}$. In addition, $\eta_1,\ \eta_2,\ \eta_3$ is the payoff functions, and the payoffs of each party is listed next to the terminal node.

In *the Collusion Contract*, W_1 pays a bribe to W_2 to initiate a collusion and satisfies $p < c$, where c is the cost that the watchtowers pay to monitor the *PCN*. If W_1 and W_2 both send fraud *CSP* y', the collusion is successful. Moreover, W_1 needs

to pay a bribe p, and its payoff is $(r-p)$. If W_1 is unable to initiate a collusion, its payoff is $(p-c)$. According to the collusion hypothesis, W_1 will initiate a collusion when $r-p > r-c$ $(p<c)$. Furthermore, W_1 and W_2 must pay a deposit g for this contract and demonstrate that $g > z+s-p$, where $z = r-c+(s-k)/2$. This criterion ensures that:

1) The payoffs who betrayed the collusion will be fewer than those who did not betray the collusion.
2) The payoffs who participated in the collusion will be higher than those who did not participate in the collusion.

Theorem 2: If $e \geq a$, $s > c+k$, $p < c$ and $g > z+s-p$, Game 2 has a unique sequential equilibrium ($(s_1,\ s_2)$, $(\eta_1,\ \eta_2)$):

$$\begin{cases} s_1 = ([1(init),\ 0(notinit)],\ [0(y),\ 1(y'),\ 0(other)]) \\ s_2 = ([1(agree),\ 0(disagree)],\ [0(y),\ 1(y'),\ 0(other)]) \\ \eta_1 = ([1(v_0),\ 1(v_1)]) \\ \eta_2 = ([1(u_0)],\ [0(u_1),\ 1(u_2),\ 0(u_3)]). \end{cases}$$

According to the equilibrium, Game 2 will end at l_{13}.

Proof: Similar to **Theorem 1**, we observe W_2's payoff at u_1, u_2, u_3, respectively. Note that the game will reach at nodes $\{q_9, q_{10}, q_{11}\}$, $\{q_{12}, q_{13}, q_{14}\}$, and $\{q_{15}, q_{16}, q_{17}\}$ when W_2 sends *CSP* $\{y, y', other\}$, respectively. Obviously, the payoff of W_2 at q_{10} is $(-s+g+p)$, which is higher than $(r-c)$ and $(-s-g)$ at nodes q_9 and q_{11}, respectively. Similarly, W_2's payoff at node q_{13} is $(r+p)$, which is higher than $(z-g)$ and $(-s-g)$ at nodes q_{12} and q_{14}, while W_2's payoff at node q_{16} is $(-s+g+p)$, which is higher than z and $(-s)$ at nodes q_{15} and q_{17}, respectively. In other words, W_1's strategy cannot affect W_2's choice, and W_2 will always choose to send fraud *CSP* y' under *Game 2*. Then, the actual reachable nodes of W_1 are q_{10}, q_{13} and q_{16}. Moreover, the payoff of W_1 at q_{13} is $(r-p)$, which is higher than $(z-g-p)$ and $(-s-g-p)$ at nodes q_{10} and q_{16}, respectively. Therefore, W_1 will likewise choose to send fraud *CSP* y' to achieve its maximum payoff. ■

VII. The Fraud Contract

In this section, we propose the Fraud Contract and analyze the sequential equilibrium using game tree model.

A. The Fraud Contract

The Fraud Contract is signed between the counterparty and a watchtower. The contract modifies the reward and punishment mechanism to encourage the watchtower to join the collusion and send a fraud *CSP* to terminate the transaction channel, thereby further defrauding the hiring party's transaction money as well as another watchtower's deposit in *the Watchtower Contract*. The rules in *the Fraud Contract* will inevitably affect the payoffs of all parties. Therefore, the counterparty and the watchtower will pay a deposit when signing this contract, and the deposits of the party who betrays the contract will be deducted. The detailed steps of *the Fraud Contract* are in the following:

1) *The Fraud Contract* is signed by C and W_1.

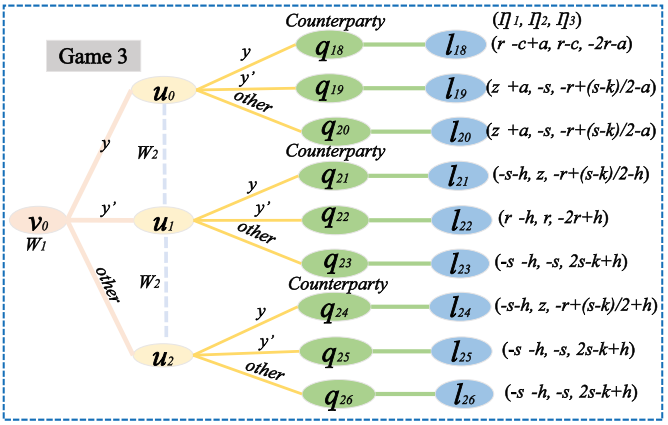

Fig. 5. *Game 3* induced by *the Fraud Contract* and *the Watchtower contract*.

2) W_1 agrees to send *CSP* y in *the Watchtower Contract*.
3) C and W_1 need to pay deposits $h+a$ and h, respectively when signing *the Fraud Contract*, and these two deposits are temporarily managed by *the Fraud Contract*.
4) C and W_1 must pay the above deposits before the deadline T_5, and $T_4 < T_5 < T_2$. Otherwise, the contract will be terminated and the deposits will be refunded.
5) When *the Watchtower Contract* ends, the following operations will be performed on the deposit balance held in *the Fraud Contract*:
   (a) If W_1 follows *the Fraud Contract*, and sends latest *CSP* y in *the Watchtower Contract*, the deposits h and $h+a$ will be returned to C and W_1, respectively.
   (b) If W_1 is unable to follow *the Fraud Contract*, the deposit $2h+a$ will be returned to C.

According to **Theorems 1 and 2**, W_1 and W_2 will normally monitor the *PCN* and send the latest *CSP* y when *the Collusion Contract* does not exist. However, if W_1 wants to obtain additional rewards from C in *the Fraud Contract*, W_1 can pretend to sign a collusion with W_2. Then, when W_2 sends fraud CSP y' in *the Watchtower Contract*, W_1 can betray *the Collusion Contract* and choose to send *CSP* y. As a result, W_1 will be punished and lose the deposit g in *the Collusion Contract*. In summary, W_1 can choose whether to collude with W_2 at this time. The following analyzes the game caused by the two situations.

B. Game Tree Analysis

We assume that W_1 can rationally choose whether to collude according to the payoffs situation. The specific analysis is as follows:

- **Case 1: W_1 chooses not to collude with W_2.**

Game 3 is induced by *the Fraud Contract* and *the Watchtowers Contract*. As shown in Fig. 5, the players are $N = \{C,\ W_1,\ W_2\}$, and the action set is $A = \{y,\ y',\ other\}$. *Game 3* contains 5 information sets: $I_1 = \{v_0\}$, $I_2 = \{u_0,\ u_1,\ u_2\}$, $I_{3,1} = \{q_{18},\ q_{19},\ q_{20}\}$, $I_{3,2} = \{q_{21},\ q_{22},\ q_{23}\}$, $I_{3,3} = \{q_{24},\ q_{25},\ q_{26}\}$. In addition, $\eta_1,\ \eta_2,\ \eta_3$ is the payoff

functions, and the payoffs of each party is listed next to the terminal node.

Theorem 3: If $e > (s-k)/2 > a$, Game 3 has a unique sequential equilibrium $((s_1,\ s_2),\ (\eta_1,\ \eta_2))$:

$$\begin{cases} s_1 = (1(y),\ 0(y'),\ 0(other)) \\ s_2 = (1(y),\ 0(y'),\ 0(other)) \\ \eta_1 = ([1(v_0)]) \\ \eta_2 = ([1(u_0),\ 0(u_1),\ 0(u_2)]). \end{cases}$$

According to the equilibrium, Game 3 will end at l_{18}.

Proof: We observe W_2's payoff at $u_0,\ u_1,\ u_2$, respectively. Note that the game will reach at nodes $\{q_{18}, q_{19}, q_{20}\}$, $\{q_{21}, q_{22}, q_{23}\}$, and $\{q_{24}, q_{25}, q_{26}\}$ when W_2 sends *CSP* $\{y, y', other\}$, respectively. Intuitively, the payoff of W_2 at q_{18} is $(r-c)$, while the payoff at q_{19} and q_{20} is $(-s)$. Obviously, $(r-c)$ is positive, and $(r-c) > (-s)$. Analogously, W_2's payoff at node q_{21} is z, which is better than r and $(-s)$ at nodes q_{22} and q_{23}, while W_2's payoff at node q_{24} is z, which is better than $(-s)$ at nodes q_{25} and q_{26}, respectively. It can be judged that no matter what the strategy of W_1 is, W_2 will send *CSP* y to maximize its payoff. According to the above derivation, the actual reachable nodes of W_1 are q_{18}, q_{21} and q_{24}, since W_2 is unable to send y' or $other$. Moreover, the payoff of W_1 at q_{18} is $(r-c+a)$, which is better than $(-s-h)$ and $(-s)$ at nodes q_{21} and q_{24}, respectively. Therefore, W_1 will choose to send *CSP* y to maximize its payoff as well. ■

- **Case 2: W_1 chooses to collude with W_2.**

Game 4 is induced by *the Fraud Contract*, *the Collusion Contract* and *the Watchtower Contract*. As shown in Fig. 6, the players are $N = \{C,\ W_1,\ W_2\}$, and the action set is $A = \{y,\ y',\ other\}$. *Game 4* contains 5 information sets: $I_1 = \{v_0\}$, $I_2 = \{u_0,\ u_1,\ u_2\}$, $I_{3,1} = \{q_{27},\ q_{28},\ q_{29}\}$, $I_{3,2} = \{q_{30},\ q_{31},\ q_{32}\}$, $I_{3,3} = \{q_{33},\ q_{34},\ q_{35}\}$. In addition, $\eta_1,\ \eta_2,\ \eta_3$ is the payoff functions, and the payoffs of each party is listed next to the terminal node.

Theorem 4: a) If $e \geq a$ and $h > r-z-a+g$, Game 4 has a unique sequential equilibrium $((s_1,\ s_2),\ (\eta_1,\ \eta_2))$:

$$\begin{cases} s_1 = (0(y),\ 1(y'),\ 0(other)) \\ s_2 = (0(y),\ 1(y'),\ 0(other)) \\ \eta_1 = ([1(v_0)]) \\ \eta_2 = ([1(u_0),\ 0(u_1),\ 0(u_2)]). \end{cases}$$

According to the equilibrium, W_1 will send CSP y and betray the Collusion Contract, and Game 4 will end at l_{28}.

b) If $e \geq a$ and $h < r-z-a+g$, Game 4 has a unique sequential equilibrium $((s_1,\ s_2),\ (\eta_1,\ \eta_2))$:

$$\begin{cases} s_1 = (1(y),\ 0(y'),\ 0(other)) \\ s_2 = (0(y),\ 1(y'),\ 0(other)) \\ \eta_1 = ([1(v_0)]) \\ \eta_2 = ([0(u_0),\ 1(u_1),\ 0(u_2)]). \end{cases}$$

According to the equilibrium, W_1 will send fraud CSP y' and betray the Fraud Contract, and Game 4 will end at l_{31}.

Proof: We observe W_2's payoff at u_0, u_1, u_2, respectively. Note that the game will reach at nodes $\{q_{27}, q_{28}, q_{29}\}$, $\{q_{30}, q_{31}, q_{32}\}$, and $\{q_{33}, q_{34}, q_{35}\}$ when W_2 sends *CSP* $\{y, y', other\}$, respectively. Intuitively, the payoff of W_2 at q_{28} is $(-s+g+p)$, which is higher than $r-c$ and $(-s)$ at nodes q_{29} and q_{30}. Analogously, W_2's payoff at node q_{31} is $(r+p)$, which is higher than $(z-g)$ and $(-s-g)$ at nodes q_{30} and q_{32}, while W_2's payoff at node q_{34} is $(-s+g+p)$, which is higher than z and $(-s)$ at nodes q_{33} and q_{35}, respectively. It can be judged that no matter what the strategy of W_1 is, W_2 will send *CSP* y to maximize its payoff. According to the above derivation, the actual reachable nodes of W_1 are q_{28}, q_{31} and q_{34}, since W_2 is unable to send y' or $other$. Moreover, the payoff of W_1 at nodes q_{28} and q_{31} is respectively $(z+a-p-g)$ and $(r-p-h)$, which is higher than $(-s-g-p-h)$ at node q_{34}. Therefore, W_1 will choose different strategies according to the real payoffs at nodes q_{28} and q_{31}. Specifically, W_1 will send *CSP* y and betray *the Collusion Contract* if $h > r-z-a+g$, otherwise W_1 will send fraud *CSP* y' and betray *the Fraud Contract*. ■

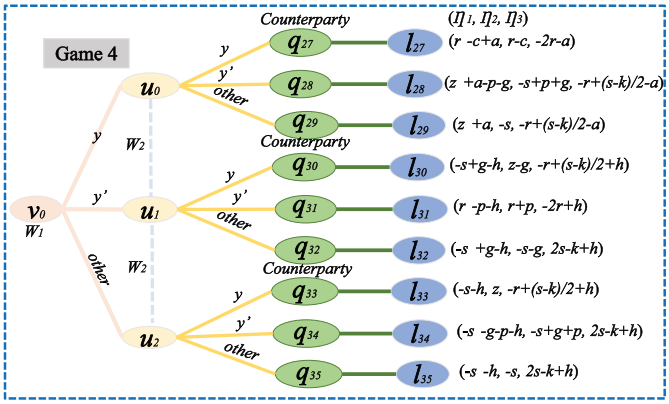

Fig. 6. *Game 4* induced by *the Fraud Contract*, *the Collusion Contract* and *the Watchtower contract*.

VIII. The Anti-Collusion Contract

In order to avoid effective collusion mentioned above, we further design *an Anti-collusion Contract* to break the equilibrium in *the Collusion Contract* and *the Fraud Contract* by providing additional rewards to honest watchtowers, making collusion an inappropriate choice.

A. The Anti-Collusion Contract

The Anti-collusion Contract allows the watchtower that reports to the hiring party to secretly betray the other party while pretending to follow the collusion. Without this exemption, the watchtower will not voluntarily report collusion: 1) If the watchtower reports and follows *the Collusion Contract*, it will lose its deposit in *the Watchtower Contract*. 2) If the watchtower reports to the hiring party and then betrays the collusion, it will lose its deposit in *the Collusion Contract*. In any scenario, it appears that reporting is less lucrative than not reporting. According to this, *the Anti-collusion Contract* guarantees that the watchtower that reports the collusion will not be penalized under *the Watchtower Contract*. The watchtower can then pretend to follow the

collusion, which can also avoid the punishment caused by betraying *the Collusion Contract*. On the other hand, if a collusion is discovered through secondary proofreading, *the Anti-collusion Contract* will reward the watchtower for reporting collusion. Accordingly, the report is not only risk-free but also profitable. In short, *the Anti-collusion Contract* breaks the collusion by incentivizing betrayal between the watchtowers, which can create distrust between the watchtowers and will ultimately prevent the collusion. In addition, the punishment mechanism of *the Anti-collusion Contract* can also effectively avoid the following false reports: 1) The watchtower reports a fraud collusion to the hiring party to obtain payoffs. 2) The watchtower deliberately sends a fraud CSP, triggering a second proofreading to obtain payoffs. The detailed steps of the contract are listed below:

1) *The Anti-collusion Contract* is signed by H_p and W. Assume that the collusion is initiated by W_1, and the collusion is reported by W_2. At this time, H_p and W need to have signed *the Watchtower Contract*.
2) H_p only signs *the Anti-collusion Contract* with the watchtower that first reports the collusion, and agrees to compensate the deposit lost in *the Watchtower Contract* where appropriate.
3) H_p needs to pay a deposit $r + 2s - k$, which is equal to W_2's maximum possible loss in *the Watchtower Contract*, while W_2 needs to pay a deposit k, which is equal to the cost of possible secondary proofreading. These deposits will be temporarily managed by *the Anti-collusion Contract*.
4) The contract should be signed before the deadline T_2, otherwise the contract is terminated and any deposits paid will be refunded.
5) W_2 must report the latest *CSP* $y*$ in this contract before the deadline T_2.
6) H_p needs to apply for a second proofreading and perform the following operations according to the judgment results:
   (a) If there is no fraud *CSP* in *the Watchtower Contract*, then refund the H_p's deposit $r + 2s - k$, and pay the W_2's deposit r to the H_p.
   (b) If W_1 sends the correct *CSP* y in *the Watchtower Contract*, while W_2 sends the fraud *CSP* y' and reports the *CSP* $y* = y$ in *the Watchtower Contract* and *the Anti-collusion Contract*, respectively. Then, H_p and W_2 will be paid $2s - k$ and $r + k$, respectively.
   (c) If both W_1 and W_2 sends the fraud *CSP* y' in *the Watchtower Contract*, while W_2 reports the *CSP* $y* = y$ in *the Anti-collusion Contract*. Then, W_1's deposit k will be returned, and the rewards $r+2s-k$ will be paid to W_2.
   (d) Otherwise, H_p and W_2 will be paid $r+2s-k$ and k, respectively.
7) If W_2 reports the latest *CSP* $y*$ in this contract, and the deadline T_3 is exceeded, all deposits will be refunded to W_2.

In addition, W_2 also needs to meet the following conditions:

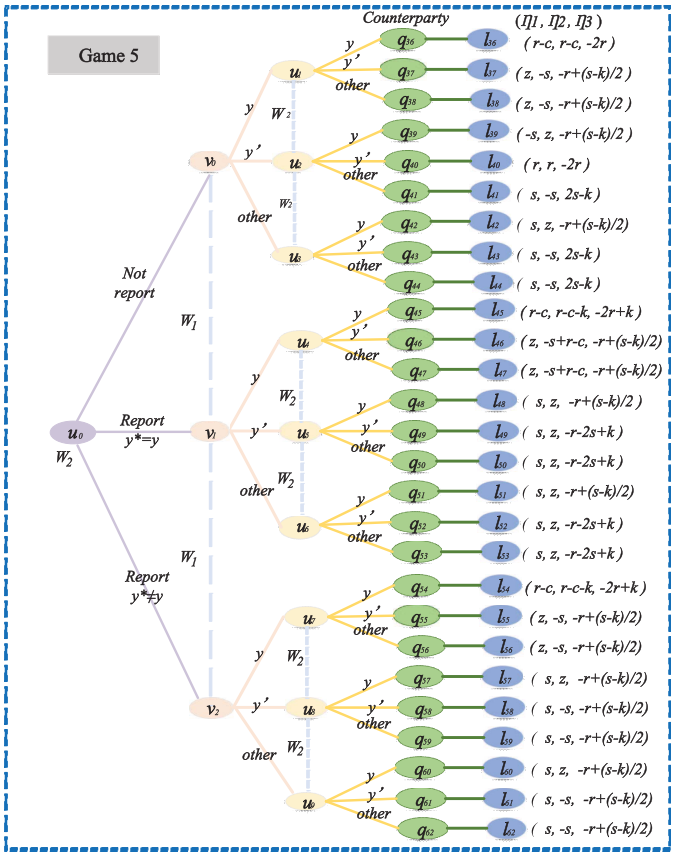

Fig. 7. *Game 5* induced by *the Watchtower Contract*, *the Fraud Contract* and *the Anti-collusion Contract*.

1) W_1 intends to initiate a collusion with W_2 and draw up *the Collusion Contract*.
2) W_2 reports the collusion to H_p before signing *the Collusion Contract*. W_2 can choose to submit evidence of the collusion, such as the address of *the Collusion Contract* and the fraud CSP y' sent at the time of collusion.
3) W_2 needs to sign *the Anti-collusion Contract* before signing *the Collusion Contract*

Before reporting, W_2 needs to wait for W_1 to initiate a collusion and sign *the Collusion Contract*. Otherwise, if the collusion is reported to the hiring party without collusion, W_2 will fall into a false report situation, since W_1 will provide the correct *CSP* y in *the Watchtower Contract*. Different from [6], in the distributed watchtowers scenario, rational W_2 is unlikely to obtain additional payoffs through false reports(*e.g.,* report some forged evidence), since W_2 cannot know whether it is possible that W_1 has also signed *the Anti-collusion Contract*. Consequently, distributed watchtowers can impose mutual restrictions, effectively preventing false reports. The subsequent experiments will also confirm our observations.

B. Game Tree Analysis

Fig. 7 is *Game 5* induced by *the Watchtower Contract*, *the Fraud Contract* and *the Anti-collusion Contract*. At this time,

the watchtowers do not initiate a collusion, or the collusion is rejected. In this game, the players are $N = \{C,\ W_1,\ W_2\}$, and the action set is $A = \{not\ report,\ report\ y* = y,\ report\ y* \neq y,\ y,\ y',\ other\}$. *Game 5* contains 14 information sets: $I_1 = \{v_0,\ v_1,\ v_2\}$, $I_{2,1} = \{u_0\}$, $I_{2,2} = \{u_1,\ u_2,\ u_3\}$, $I_{2,3} = \{u_4,\ u_5,\ u_6\}$, $I_{2,4} = \{u_7,\ u_8,\ u_9\}$, $I_{3,1} = \{q_{36},\ q_{37},\ q_{38}\}$, $I_{3,2} = \{q_{39},\ q_{40},\ q_{41}\}$, $I_{3,3} = \{q_{42},\ q_{43},\ q_{44}\}$, $I_{3,4} = \{q_{45},\ q_{46},\ q_{47}\}$, $I_{3,5} = \{q_{48},\ q_{49},\ q_{50}\}$, $I_{3,6} = \{q_{51},\ q_{52},\ q_{53}\}$, $I_{3,7} = \{q_{54},\ q_{55},\ q_{56}\}$, $I_{3,8} = \{q_{57},\ q_{58},\ q_{59}\}$, $I_{3,9} = \{q_{60},\ q_{61},\ q_{62}\}$. In addition, η_1, η_2, η_3 is the payoff functions, and the payoffs of each party is listed next to the terminal node.

Theorem 5: If $e \geq a$ and $s > c + k$, Game 5 has a unique sequential equilibrium $((s_1,\ s_2),\ (\eta_1,\ \eta_2))$:

$$\begin{cases} s_1 = ([1(y),\ 0(y'),\ 0(other)]) \\ s_2 = ([1(not\ report), 0(report, y* = y), 0(report, y* \neq y)], \\ \qquad [1(y),\ 0(y'),\ 0(other)], [1(y),\ 0(y'),\ 0(other)], \\ \qquad [1(y),\ 0(y'),\ 0(other)]), \\ \eta_1 = (1(v_0),\ 0(v_1),\ 0(v_2)), \\ \eta_2 = ([1(u_0)], [1(u_1), 0(u_2), 0(u_3)], [1(u_4), 0(u_5), 0(u_6)], \\ \qquad [1(u_7),\ 0(u_8),\ 0(u_9)]). \end{cases}$$

According to the equilibrium, Game 5 will end at l_{36}.

Proof: At the information set $I_{2,1}$, we first observe W_2's payoff at $\{(u_1,\ u_2,\ u_3), (u_4,\ u_5,\ u_6), (u_7,\ u_8,\ u_9)\}$, respectively. Note that the game will reach at nodes $\{[(q_{36},\ q_{37},\ q_{38}),\ (q_{39},\ q_{40},\ q_{41}),\ (q_{42},\ q_{43},\ q_{44})], [(q_{45},\ q_{46},\ q_{47}),\ (q_{48},\ q_{49},\ q_{50}),\ (q_{51},\ q_{52},\ q_{53})],\ [(q_{54},\ q_{55},\ q_{56}),\ (q_{57},\ q_{58},\ q_{59}),\ (q_{60},\ q_{61},\ q_{62})]\}$ when W_2 sends *CSP* $\{y,\ y',\ other\}$, respectively. Obviously, W_2's payoff at q_{36} is $(r - c)$, which is higher than $(-s)$ at nodes q_{37} and q_{38}. Similarly, W_2's payoff at node q_{39} is z, which is higher than r and $(-s)$ at nodes q_{40} and q_{41}, while W_2's payoff at node q_{42} is z, which is higher than $(-s)$ at nodes q_{43} and q_{44}, respectively. Therefore, no matter what the strategy of W_1 is, W_2 will send *CSP* y to maximize its payoff.

Deriving backwards, at $I_{2,2}$, W_2's payoff at q_{45} is $(r-c-k)$, which is higher than $(-s+r+c)$ at nodes q_{46} and q_{47}. Further, W_2's payoff at node q_{48} is z, which is equal to those at nodes q_{49} and q_{50}, the same situation also occurs at nodes q_{51}, q_{52}, and q_{53}. As a result, only when W_2 chooses to send *CSP* y, can its payoffs be maximized.

Deriving backwards, at $I_{2,3}$, W_2's payoff at q_{54} is $(r-c-k)$, which is higher than $(-s)$ at nodes q_{55} and q_{56}. Similarly, W_2's payoff at node q_{57} is z, which is higher than $(-s)$ at nodes q_{58} and q_{59}, while W_2's payoff at node q_{60} is z, which is higher than $(-s)$ at nodes q_{61} and q_{62}, respectively. In short, no matter what the strategy of W_1 is, W_2 will send *CSP* y to maximize its payoff.

Deriving backwards, at I_1, W_1's actual reachable nodes are $\{(q_{36},\ q_{39},\ q_{42}),\ (q_{45},\ q_{48},\ q_{51}),\ (q_{54},\ q_{57},\ q_{60})\}$. Moreover, W_1's payoff at q_{36} is $(r - c)$, which is higher than $(-s)$ at nodes q_{39} and q_{42}. The same payoff situations also appear at nodes $(q_{45},\ q_{48},\ q_{51})$ and $(q_{54},\ q_{57},\ q_{60})$. Thus, W_1 will send *CSP* y to maximize its payoff as well.

Deriving backwards, at $I_{2,1}$, W_2's actual reachable nodes are q_{36}, q_{45} and q_{54}. Apparently, W_2's payoff at q_{36} is $(r-c)$, which is higher than $(r-c-k)$ at nodes q_{45} and q_{54}. Therefore, *Game 5* will end at l_{36}. ■

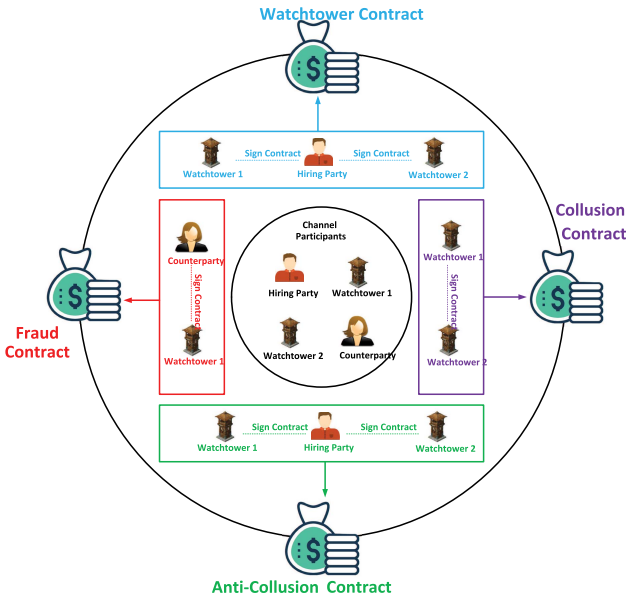

Fig. 8. Relationship among all the contracts. *Watchtower Contract* is an employment contract between channel participants and watchtowers. *Collusion Contract* is designed as a collusion between two watchtowers to obtain additional payoffs. There can be collusion between counterparties and a malicious watchtower, as analyzed in *Fraud Contract*. *Anti-collusion Contract* is devised to effectively resist the above two collusion attacks.

In summary, we analyze and derive the sequential equilibria of rational channel participants under *the Watchtower Contract*, *the Collusion Contract*, *the Fraud Contract*, and *the Anti-collusion Contract* scenarios, respectively. As shown in Fig. 8, *the Watchtower Contract* is a contract of employment between H_p and W_1, H_p and W_2, respectively, where W_1 and W_2 are paid for monitoring the payment channel. In order to undermine the former equilibrium, *the Collusion Contract* is designed as a conspiracy between W_1 and W_2 to obtain additional payoffs beyond *the Watchtower Contract*. Further, *the Fraud Contract* is a conspiracy between a counterparty and one of the malicious watchtowers, in which the counterparty intends to cooperate with the malicious watchtower for more additional revenue. Finally, we design *the Anti-collusion Contract* to effectively counter *the Fraud Contract*, which compels malicious watchtowers to betray previously signed contracts by exempting them from penalties.

C. The Full Game and Analysis

Next, we integrate all contracts for game analysis. Fig. 9 is *Game 6* induced by *the Watchtower Contract*, *the Collusion Contract*, *the Fraud Contract*, and *the Anti-collusion Contract*. We first assume that W_1 initiates the collusion, and chooses strategies first. If W_1 does not initiate a collusion, or initiates a collusion but W_2 refuses to join, then there is no *Collusion Contract* in the game, and the game will enter *Game 5*. However, if W_2 agrees to collude with W_1, in this game, W_2 will report the collusion to H_p and sign *the Anti-collusion Contract*. Besides, if W_1 and H_p sign

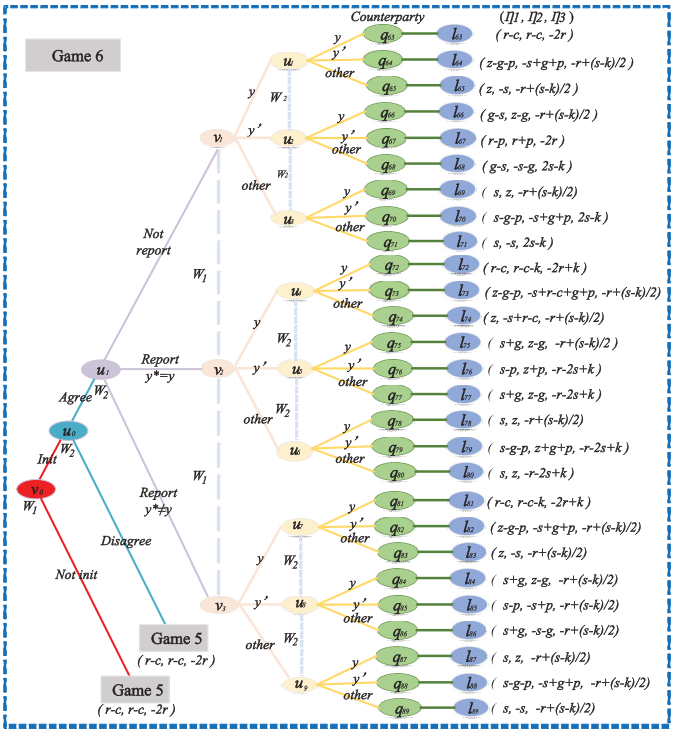

Fig. 9. *Game 6* induced by all the contracts.

the Anti-collusion Contract, W_2 will not sign *the Collusion Contract*, and the game will enter *Game 6*. In this game, the players are $N = \{C,\ W_1,\ W_2\}$, and the action set is $A = \{not\ report,\ report\ y* = y,\ report\ y* \neq y,\ not\ init,\ init,\ disagree,\ agree,\ y,\ y',\ other\}$. *Game 6* contains 7 information sets: $I_{1,1} = \{v_0\}$, $I_{1,2} = \{v_1,\ v_2,\ v_3\}$, $I_{2,1} = \{u_0\}$, $I_{2,2} = \{u_1\}$, $I_{2,3} = \{u_2,\ u_3,\ u_4\}$, $I_{2,4} = \{u_5,\ u_6,\ u_7\}$, $I_{2,5} = \{u_8,\ u_9,\ u_{10}\}$. In addition, η_1, η_2, η_3 is the payoff functions, and the payoffs of each party is listed next to the terminal node.

Theorem 6: If $e \geq a$, $s > c + k$, $p < c$ and $g > z + s - p$, Game 6 has a unique sequential equilibrium ($(s_1,\ s_2)$, $(\eta_1,\ \eta_2)$):

$$\begin{cases} s_1 = ([1(not\ init),\ 0(init)],\ [0(y),\ 1(y'),\ 0(other)]) \\ s_2 = ([0(disagree),\ 1(agree)], \\ \qquad [0(not\ report), 1(report, y*=y), 0(report, y*\neq y)], \\ \qquad [0(y),\ 1(y'),\ 0(other)],\ [0(y),\ 1(y'),\ 0(other)], \\ \qquad [0(\mathrm{y}),\ 1(\mathrm{y}'),\ 0(\mathrm{other})]), \\ \eta_1 = ([1(v_0)],\ [0(v_1),\ 1(v_2),\ 0(v_3)]), \\ \eta_2 = ([0(u_2),\ 1(u_3),\ 0(u_4)],\ [0(u_5),\ 1(u_6),\ 0(u_7)], \\ \qquad [0(u_8),\ 1(u_9),\ 0(u_{10})]). \end{cases}$$

According to the equilibrium, Game 6 will end at l_{76}.

Proof: Similar to **Theorem 5**, we first observe W_2's payoff. At the information set $I_{2,1}$, W_2's payoff at q_{64} is $(-s+g+p)$, which is higher than $(r-c)$ and $(-s)$ at nodes q_{63} and q_{65}. As a result, W_2 will send fraud *CSP* y' at $I_{2,1}$.

Deriving backwards, at $I_{2,2}$, W_2's payoff at node q_{73} is $(-s+r-c+g+p)$, which is higher than $(r-c-k)$ and $(-s+r-c)$ at nodes q_{72} and q_{74}, while W_2's payoff at nodes q_{76} and q_{79} is $(z+p)$ and $(z+g+p)$, which is higher than $(z-g)$ and z at nodes (q_{75}, q_{77}) and (q_{78}, q_{80}), respectively. Obviously, W_2 will send fraud *CSP* y' at $I_{2,2}$.

Deriving backwards, at $I_{2,3}$, W_2's payoff at node q_{82} is $(-s+g+p)$, which is higher than $(r-c-k)$ and $(-s)$ at nodes q_{81} and q_{83}, while W_2's payoff at nodes q_{85} and q_{88} is $(-s+p)$ and $(-s+g+p)$, which is higher than $(z-g)$ and $(-s-g)$, as well as z and $(-s)$ at nodes (q_{84}, q_{86}) and (q_{87}, q_{89}), respectively. Thus, W_2 will send fraud *CSP* y' at $I_{2,2}$. In summary, no matter what the strategy of W_1 is, W_2 will send fraud *CSP* y' to maximize its payoff.

Next, we observe W_1's payoff. At $I_{1,2}$, since W_2 is able to send fraud *CSP* y', and then W_1's reachable nodes at (v_0,v_1,v_2) are (q_{64}, q_{67}, q_{70}), (q_{73}, q_{76}, q_{79}), and (q_{82}, q_{85}, q_{88}), respectively. Apparently, W_1's payoff at q_{67} is $(r-p)$, which is higher than $(z-g-p)$ and $(-s-g-p)$ at nodes q_{64} and q_{70}. Similarly, W_1's payoff at node q_{76} is $(-s-p)$, which is higher than $(z-g-p)$ and $(-s)$ at nodes q_{73} and q_{79}, while W_1's payoff at node q_{85} is $(-s-p)$, which is higher than $(z-g-p)$ and $(-s-g-p)$ at nodes q_{82} and q_{88}, respectively. In short, W_1 will send fraud *CSP* y' to maximize its payoff as well.

Deriving backwards, at $I_{2,2}$, since W_1 is able to send fraud *CSP* y', then W_2's reachable nodes at v_0 are q_{67}, q_{76} and q_{85}. Moreover, W_2's payoff at q_{76} is $(z+p)$, which is higher than $(r+p)$ and $(-s+p)$ at nodes q_{67} and q_{85}. Therefore, W_2 will choose to report collusion and send *CSP* $y* = y$ in *the Anti-collusion Contract*.

Deriving backwards, at $I_{2,1}$, W_2's actual reachable nodes are q_{76} and *Game 6*. Apparently, W_2's payoff at q_{76} is $(z+p)$, which is higher than $(r-c)$ at nodes *Game 6*. Then, W_2 will choose to agree the collusion.

Deriving backwards, at $I_{1,1}$, W_1's actual reachable nodes are q_{76} and *Game 6* as well. It is obvious that W_1's payoff at q_{76} is $(-s+p)$, which is higher than $(r-c)$ at nodes *Game 6*. Then, W_1 will choose not to agree the collusion. Not only is it impossible for a rational counterparty to maliciously collude with the watchtower under *Game 6* to fraud other watchtowers's deposits and the the hiring party's balance, but also the rational watchtower cannot commence a collusion while routinely monitoring the *PCN* and truthfully sending *CSP* y. Consequently, *Game 6* will end at l_{76}. ■

According to Game 6, the unique sequential equilibrium requires that rational participants will not rashly initiate collusion in order to maximize their respective benefits, otherwise not only will they be unable to obtain normal benefits, but they will also pay more fines for this. Next, we will verify the validity of these contracts through massive experiments.

IX. Implementation and Evaluation

A. Experimental Setup

We conduct experiments on an Intel Core i7-6700 with a 3.4GHz CPU and an NVIDIA Tesla K80 GPU accelerator [49]. Specifically, we first leverage Solidity to create the *Watchtower Contract*, the *Collusion Contract*, the *Fraud*

TABLE III
THE COST OF EXECUTING SMART CONTRACTS ON ETHEREUM

Contract	Operation	Cost(Gas)	Cost($)
Watchtower Contract	Init	1675836	8.1806
	Create	227563	1.1108
	Collude	63488	0.3099
	Distributed	70964	0.3464
Collusion Contract	Init	1846963	9.0161
	Create	307926	1.5031
	Collude	80996	0.3953
	Distributed	110364	0.5387
Fraud Contract	Init	1783622	8.7069
	Create	264318	1.2903
	Collude	120049	0.5860
	Distributed	99831	0.4873
Anti-collusion Contract	Init	1865331	9.1058
	Create	337095	1.6455
	Collude	77083	0.3763
	Distributed	332408	1.6226

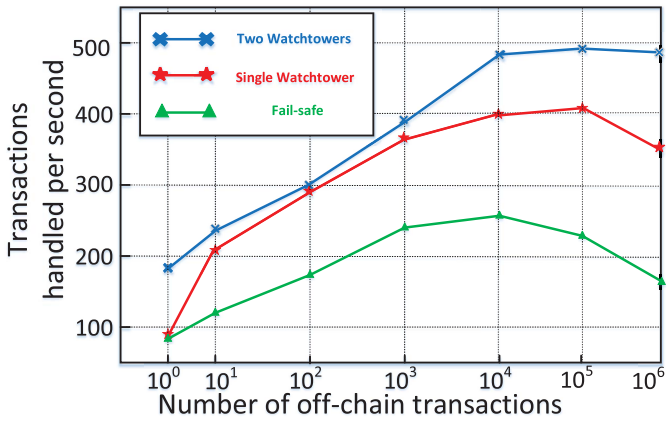

Fig. 10. Throughput of the watchtowers.

Contract, and the *Anti-collusion Contract*. Then, we deploy our proposal on Ethereum [3] to verify its effectiveness and scalability. In order to test the improvement of the distributed watchtowers in terms of false positive rate, furthermore, we build a simulation testbed on NS3 [50], and use Fail-safe [43] and Single Watchtower [6] as comparative benchmarks to test the throughput, accuracy and false positive rate of distributed watchtowers in processing transactions, respectively.

We first formulate the definition of accuracy and false positive rate as follows:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}, \quad (1)$$

$$False\ Positive\ Rate = \frac{FP}{FP+TN}, \quad (2)$$

where TP (True Positive) and FN (False Positive) respectively represent the number of fraud CSPs that can be correctly identified, while FP (False Positive) and TN (Ture Negative) respectively represent the number of normal CSPs that can be correctly identified.

B. Cost

We test the cost of implementing smart contracts on Ethereum, as shown in Table III. We can quantify the cost as the total amount of gas consumed to perform each function of the smart contracts. More intuitively, we can also quantify the cost in US dollars ($) by converting the current exchange rate. According to the latest investigation, the gas price was 2×10^{-9} ether (2 Gwei) and the exchange rate was 1 ether $=$ 2440.81 USD as of January 2022. We find that the total cost of Watchtower Contract, Collusion Contract, Fraud Contract and Anti-Collusion Contract is about 2.0 million gas ($10.26), 2.2 million gas ($10.99), 2.1 million gas ($10.58), and 2.6 million gas ($12.75), respectively.

The financial cost of running smart contracts is roughly related to the computational and storage complexity of the function. For example, the cost of the $Init$ operation is significantly higher than other operations. The fundamental reason is that the data storage cost on the blockchain is very expensive, and the data structure initialization cost needs to be paid in advance when the watchtower contract is initialized, but this part of the cost will be slightly reduced as the number of requests to close the state channel increases.

C. Throughput

We run the watchtower throughput on a system with an Intel Core i7 CPU and 64GB of RAM and compared the throughput of single watchtower [6] and Fail-safe [43] with that of distributed watchtowers. We first create 10^i off-chain transactions $(0 \leqslant i \leqslant 6)$ between the participants, each of which was requested to exchange CSPs once with at least one watchtower. Then, we calculate the time required to exchange CSPs, as well as the average time required to process each transaction to quantify throughput. As shown in Fig. 10, we can see that the throughput of the Fail-safe and single watchtower becomes stable when the number of requests is greater than 10^3 and 10^4, respectively, while the throughput of distributed watchtowers tends to be stable when the number of requests is greater than 10^5. In addition, when the number of requests reaches 10^6, we can clearly find that the throughput of Fail-safe and single watchtower shows a significant downward trend, while the distributed watchtower can still process requests as usual in the interval of 10^5 to 10^6, indicating that distributed watchtowers are more efficient at processing high volumes of transactions in batches.

D. Accuracy

We further build the simulation testbed on NS3 to test the accuracy and false positive rate of the watchtower processing transactions. Fig. 11 shows that the accuracy of the watchtowers decreases as the number of transactions processed in a batch accumulates. However, the accuracy of the distributed watchtowers is significantly superior to that of a single watchtower. Moreover, when the number of transactions is stable at a certain interval (10^4 off-chain transactions), as shown in Fig. 12, numerous experiments show that the accuracy of the

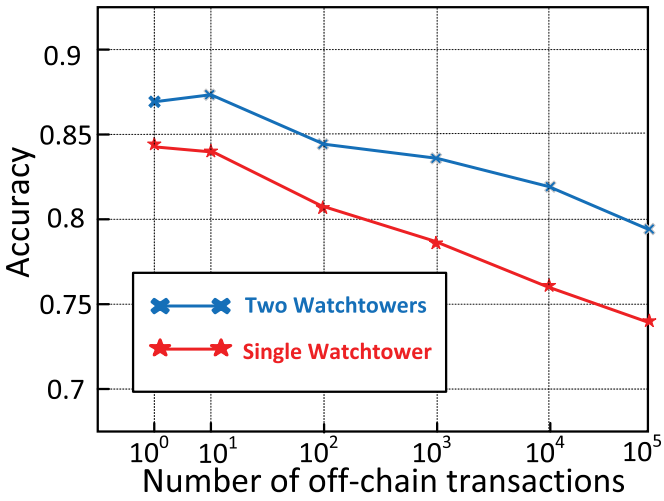

Fig. 11. Accuracy comparison with different number of off-chain transcations.

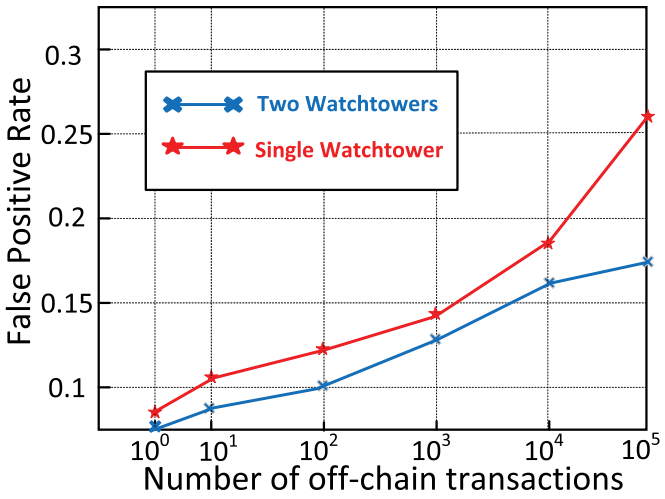

Fig. 13. False positive comparison with different number of off-chain transcations.

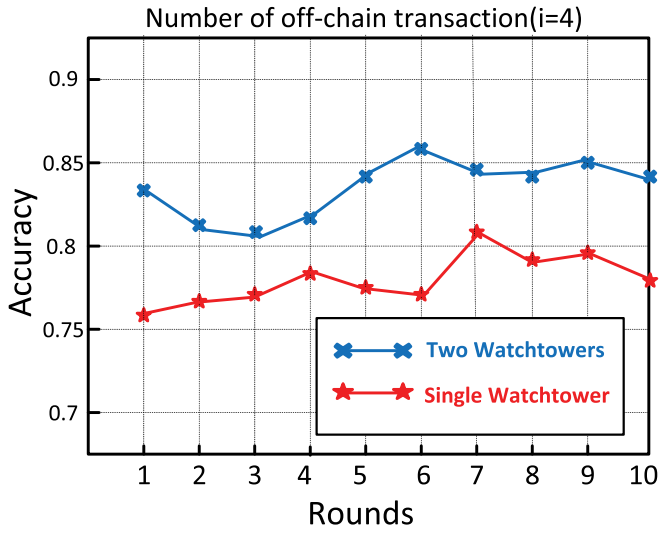

Fig. 12. Inspection on accuracy.

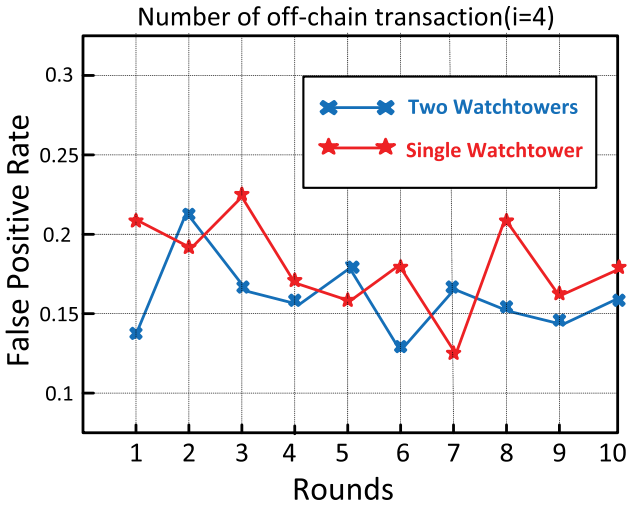

Fig. 14. Inspection on false positive.

distributed watchtowers is also higher than that of the single watchtower.

E. False Positive Rate

Similarly, we have also conducted experimental tests on the false positive rate of watchtowers. Fig. 13 shows that the false positive rate of the watchtowers increases as the number of transactions processed in a batch accumulates. Particularly, when the number of off-chain transactions reaches an order of magnitude of 10^5, the false positive rate of the single watchtower increases significantly, while the distributed watchtower still fluctuates within the normal range. In addition, from Figure 14, when the number of off-chain transactions is stable on the order of 10^4, the false positive rate of both the single watchtower and the distributed watchtowers fluctuate within the normal range (between 0.1 and 0.25). However, we can visually observe that the fluctuation of the single watchtower is significantly larger than that of the distributed watchtowers, thus we can infer that the distributed watchtowers are more stable and efficient in handling CSPs and off-chain transactions.

X. Conclusion

In this paper, we propose the anti-collusion multiparty smart contracts for distributed watchtowers in PCNs. We first propose the distributed watchtowers model to solve the false positive problem of off-chain transactions with the single watchtower. Then, to address the collusion attack in the off-chain transaction scenario, we design multiple smart contracts and analyze the contracts through the game tree model, and obtain a unique sequential equilibrium through mathematical derivation and proof. Finally, we perform extensive experiments on Ethereum and NS3 to verify the effectiveness and reliability of our scheme. The experimental results demonstrate that the proposed scheme can achieve low false positives and accuracy guarantees for distributed watchtowers, as well as effectively counter collusion attacks.

REFERENCES

[1] [Online]. Available: https://www.blockchain.com/charts/fees-usd-per-transaction

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Tech. Rep., 2008.

[3] (2015). *Ethereum Wiki: Geth*. [Online]. Available: https://github.com/ethereum/go-ethereum/wiki/geth

[4] N. Khan and R. State, "Lightning network: A comparative review of transaction fees and data analysis," in *Blockchain and Applications* (Advances in Intelligent Systems and Computing). Avila, Spain: Springer, Jun. 2019.

[5] A. Back et al. (Oct. 2014). *Enabling Blockchain Innovations With Pegged Sidechains [EB/OL*]. [Online]. Available: http://kevinriggen.com/files/sidechains.pdf

[6] Y. Zhang, D. Yang, G. Xue, and R. Yu, "Counter-collusion smart contracts for watchtowers in payment channel networks," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, Vancouver, BC, Canada, May 2021, pp. 1–10.

[7] S. Kim, Y. Kwon, and S. Cho, "A survey of scalability solutions on blockchain," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Jeju, South Korea, Oct. 2018, pp. 1204–1207.

[8] [Online]. Available: https://etherscan.io/charts

[9] *Fraud-Fighting Watchtowers to Arrive in Next Bitcoin Lightning Release*. [Online]. Available: https://www.coindesk.com/fraud-fighting-watchtowers are-coming-with-the-next-big-lightning-release

[10] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2014.

[11] P. McCorry, S. Bakshi, I. Bentov, S. Meiklejohn, and A. Miller, "PISA: Arbitration outsourcing for state channels," in *Proc. 1st ACM Conf. Adv. Financial Technol.*, Zurich, Switzerland, Oct. 2019, pp. 1–20.

[12] G. Avarikioti, O. S. T. Litos, and R. Wattenhofer, "CERBERUS channels: Incentivizing watchtowers for Bitcoin," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, Kota Kinabalu, Malaysia, Jul. 2020, pp. 346–366.

[13] *Cerberus Script*. [Online]. Available: https://github.com/OrfeasLitos/cerberus-script

[14] [Online]. Available: https://github.com/lightningnetwork/lnd/releases/tag/v0.7.0-beta-rc3

[15] K. Soska, J. Dong, A. Khodaverdian, A. Z. Jones, B. Routledge, and N. Christin, "Towards understanding cryptocurrency derivatives: A case study of BitMEX," in *Proc. Web Conf. (WWW)*, Ljubljana, Slovenia, Apr. 2021, pp. 45–57.

[16] *Bitcoin Wiki: Bitcoin Contract*. [Online]. Available: https://en.bitcoin.it/wiki/Contract

[17] *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. [Online]. Available: https://www.bitcoinlightning.com/wpcontent/uploads/2018/03/ lightning-network-paper.pdf

[18] *Thunder Network: Off-Chain Bitcoin Payments Using Smart Contracts*. [Online]. Available: https://github.com/blockchain/thunder

[19] *Eclair: A Scala Implementation of The Lightning Network*. [Online]. Available: https: //github.com/ACINQ/eclair

[20] *The Raiden Network*. [Online]. Available: https://raiden.network

[21] Y. Zhang, D. Yang, and G. Xue, "CheaPay: An optimal algorithm for fee minimization in blockchain-based payment channel networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Shanghai, China, May 2019, pp. 1–6.

[22] V. Sivaraman, S. B. Venkatakrishnan, M. Alizadeh, G. Fanti, and P. Viswanath, "Routing cryptocurrency with the spider network," in *Proc. 17th ACM Workshop Hot Topics Netw.*, Redmond, WA, USA, Nov. 2018, pp. 29–35.

[23] V. Bagaria, J. Neu, and D. Tse, "Boomerang: Redundancy improves latency and throughput in payment-channel networks," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, Kota Kinabalu, Malaysia, Mar. 2020, pp. 304–324.

[24] P. Wang, H. Xu, X. Jin, and T. Wang, "Flash: Efficient dynamic routing for offchain networks," in *Proc. 15th Int. Conf. Emerg. Netw. Exp. Technol.*, Orlando, FL, USA, Dec. 2019, pp. 1–13.

[25] G. Malavolta, P. Moreno-Sanchez, A. Kate, and M. Maffei, "SilentWhispers: Enforcing security and privacy in decentralized credit networks," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, San Diego, CA, USA, 2017, pp. 1–15.

[26] P. F. Tsuchiya, "The landmark hierarchy: A new hierarchy for routing in very large networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 18, no. 4, pp. 35–42, Aug. 1988.

[27] S. Roos, P. Moreno-Sanchez, A. Kate, and I. Goldberg, "Settling payments fast and private: Efficient decentralized routing for path-based transactions," 2017, *arXiv:1709.05748*.

[28] C. H. Papadimitriou and D. Ratajczak, "On a conjecture related to geometric routing," *Theor. Comput. Sci.*, vol. 344, no. 1, pp. 3–14, 2005.

[29] R. Yu, G. Xue, V. T. Kilari, D. Yang, and J. Tang, "CoinExpress: A fast payment routing mechanism in blockchain-based payment channel networks," in *Proc. IEEE Int. Conf. Comput. Commun. Netw.*, Hangzhou, China, Jul. 2018, pp. 1–9.

[30] F. Engelmann, H. Kopp, F. Kargl, F. Glaser, and C. Weinhardt, "Towards an economic analysis of routing in payment channel networks," in *Proc. 1st Workshop Scalable Resilient Infrastructures Distrib. Ledgers*, Las Vegas, NV, USA, Dec. 2017, pp. 1–7.

[31] V. Sivaraman et al., "High throughput cryptocurrency routing in payment channel networks," in *Proc. USENIX Symp. Networked Syst. Design Implement.*, Santa Clara, CA, USA, Feb. 2020, pp. 777–796.

[32] L. Eckey, S. Faust, K. Hostakova, and S. Roos, "Splitting payments locally while routing interdimensionally," IACR, Lyon, France, Tech. Rep. 555, 2020.

[33] C.-P. Schnorr, "Efficient signature generation by smart cards," *J. Cryptol.*, vol. 4, no. 3, pp. 161–174, Jan. 1991.

[34] Y. Zhang and D. Yang, "RobustPay: Robust payment routing with approximation guarantee in blockchain-based payment channel networks," *IEEE/ACM Trans. Netw.*, vol. 29, no. 4, pp. 1–11, Apr. 2021.

[35] *Bitcoin Lightning Fraud? Laolu is Building a Watchtower to Fight it*. [Online]. Available: https://www.coindesk.com/laolu-building-watchtower-fight-bitcoin-lightning-fraud

[36] *Bitcoin Wallet Electrum Now Supports Lightning, Watchtowers and Submarine Swaps*. [Online]. Available: https://www.coindesk.com/bitcoin-wallet-electrum-nowsupports-lightning- -and-submarine-swaps

[37] *Blockstreams Watchtowers Will Bring a New Justice System to the Lightning Network*. [Online]. Available: https://www.coindesk.com/blockstreamswatchtowers-will-bring-a-new-justice- system-to-the-lightning-network

[38] *Fraud-Fighting Watchtowers to Arrive in Next Bitcoin Lightning Release*. [Online]. Available: https://www.coindesk.com/fraud-fighting-watchtowers-are-coming-with-the-next-big-lightning-release

[39] P. Prihodko, S. Zhigulin, M. Sahno, A. Ostrovskiy, and O. Osuntokun, "Flare: An approach to routing in lightning network," Whitepaper, 2016.

[40] T. Dryja and S. B. Milano. (2016). *Unlinkable Outsourced Channel Monitoring*. [Online]. Available: https://diyhpl.us/wiki/transcripts/scalingbitcoin/milan/unlinkable-outsourced-channel-monitoring

[41] O. Osuntokunn, "Hardening lightning," in *Proc. BPASE*, 2018.

[42] M. Khabbazian, T. Nadahalli, and R. Wattenhofer, "Outpost: A responsive lightweight watchtower," in *Proc. 1st ACM Conf. Adv. Financial Technol.*, Zurich, Switzerland, Oct. 2019, pp. 31–40.

[43] B. Liu, P. Szalachowski, and S. Sun, "Fail-safe watchtowers and short-lived assertions for payment channels," in *Proc. 15th ACM Asia Conf. Comput. Commun. Secur.*, Taipei, Taiwan, Oct. 2020, pp. 506–518.

[44] J. Li, D. Niyato, C. S. Hong, K.-J. Park, L. Wang, and Z. Han, "Cyber insurance design for validator rotation in sharded blockchain networks: A hierarchical game-based approach," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 3, pp. 3092–3106, Sep. 2021.

[45] S. Xia, F. Lin, Z. Chen, C. Tang, Y. Ma, and X. Yu, "A Bayesian game based vehicle-to-vehicle electricity trading scheme for blockchain-enabled internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 6856–6868, Jul. 2020.

[46] L. Huang and Q. Zhu, "A dynamic game framework for rational and persistent robot deception with an application to deceptive pursuit-evasion," *IEEE Trans. Autom. Sci. Eng.*, vol. 16, pp. 1–15, 2021.

[47] I. H. Abdulqadder, S. Zhou, D. Zou, I. T. Aziz, and S. M. A. Akber, "Bloc-Sec: Blockchain-based lightweight security architecture for 5G/B5G enabled SDN/NFV cloud of IoT," in *Proc. IEEE 20th Int. Conf. Commun. Technol. (ICCT)*, Nanning, China, Oct. 2020, pp. 499–507.

[48] J. Li, T. Liu, D. Niyato, P. Wang, J. Li, and Z. Han, "Contract-theoretic pricing for security deposits in sharded blockchain with Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 10052–10070, Jun. 2021.

[49] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, and Z. Han, "Cloud/fog computing resource management and pricing for blockchain networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4585–4600, Nov. 2018.

[50] M. Du, K. Wang, Z. Xia, and Y. Zhang, "Differential privacy preserving of training model in wireless big data with edge computing," *IEEE Trans. Big Data*, vol. 6, no. 2, pp. 283–295, Jun. 2020.

Miao Du is currently pursuing the Ph.D. degree with the School of Computer Science and Engineering, Southeast University, Nanjing, China. His current research interests include wireless sensor networks, the Internet of Things, edge computing, network security, game theory, and blockchain.

Peng Yang (Member, IEEE) received the Ph.D. degree from Southeast University in 2006 by taking a successive postgraduate and doctoral program. He worked as a Research Scientist with CERN to participate in the alpha magnetic spectrometer (AMS) experiment (PI: Nobel laureate Samuel C.C. Ting) from 2007 to 2009. He is currently a Professor with the School of Computer Science and Engineering, Southeast University, where he is also the Deputy Director of the Future Network Research Center. His research interests include new-generation network architecture, edge computing, natural language processing, blockchain, and cyber content governance. He is a member of the National Technical Committee of Standardization Administration of China.

Wen Tian (Member, IEEE) received the B.S. degree in physics from the Changsha University of Science and Technology, Changsha, China, in 2014, the M.S. degree in control theory and control engineering from the Jiangsu University of Science and Technology, Zhenjiang, China, in 2017, and the Ph.D. degree in control science and engineering from the Nanjing University of Science and Technology, Nanjing, China. He is currently a Lecturer with the School of Electronic and Information Engineering, Nanjing University of Information Science and Technology. His research interests include covet communication, cyber-physical systems, the Internet of Things, game theory, and network security.

Zhu Han (Fellow, IEEE) received the B.S. degree in electronic engineering from Tsinghua University in 1997 and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, in 1999 and 2003, respectively.

From 2000 to 2002, he was a Research and Development Engineer at JDSU, Germantown, Maryland. From 2003 to 2006, he was a Research Associate at the University of Maryland. From 2006 to 2008, he was an Assistant Professor at Boise State University, ID, USA. He is currently a John and Rebecca Moores Professor with the Electrical and Computer Engineering Department and the Computer Science Department, University of Houston, TX, USA. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grid. He received a NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the *EURASIP Journal on Advances in Signal Processing* in 2015, IEEE Leonard G. Abraham Prize in the field of communications systems (Best Paper Award in IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS) in 2016, and several best paper awards in IEEE conferences. He was an IEEE Communications Society Distinguished Lecturer from 2015 to 2018. He has been an AAAS Fellow since 2019 and an ACM Distinguished Member since 2019. He has been a 1% highly cited researcher since 2017 according to Web of Science. He is also the Winner of the 2021 IEEE Kiyo Tomiyasu Award for outstanding early to mid-career contributions to technologies holding the promise of innovative applications with the following citation "for contributions to game theory and distributed management of autonomous communication networks."