Disincentivizing Double Spend Attacks Across Interoperable Blockchains

Kuheli Sai
School of Computing and Information
University of Pittsburgh
Pittsburgh, PA, USA
Email: kuheli.sai@pitt.edu

David Tipper
School of Computing and Information
University of Pittsburgh
Pittsburgh, PA, USA
Email: dtipper@pitt.edu

***Abstract*—Blockchain was originally developed to support decentralized cryptocurrency applications within a single network. However, the proliferation of blockchain technology has led to the need of supporting transactions across multiple networks requiring interoperability. Thus far, minimal analysis has been dedicated to the interoperability scenario and in particular the prevention of double spending attacks across interoperable blockchain networks. In this paper, we propose the use of neutral observers to monitor transactions that span multiple blockchains and design a protocol that obviates the double spending problem across interoperable blockchain networks. We show that the observers, can detect double spending, while remaining honest to the protocol as it is more profitable to them than colluding due to our proposed disincentivization scheme. Leveraging Ethereum's smart-contract functionality, we simulate our proposed disincentivization scheme and show its cost-effectiveness.**

***Keywords*-Blockchain, Interoperable-Blockchains, Cryptocurrency, Double Spending, Game Theory.**

I. Introduction

Blockchain [1] is a decentralized, distributed, public ledger whose main strength lies in creating an immutable ledger. Due to this transparency, blockchain technology has been used in a variety of application domains. For example, monitoring the flow of foods from farms to the customer [2]–[6]. As blockchain technology has expanded to other fields [7]–[11] and applications (e.g., smart-contracts), there is an emerging need to create interoperability across several different blockchain systems [12]–[15]. Note, this may include a mix of public/permissionless and private/permissioned blockchains [16]–[19]. Architectures for providing interoperability or supporting crosschain transactions focus on forming a trusted channel connecting two or more blockchains to enable transactions [20]–[23]. These trusted channels are prone to several types of attacks as it appears to be a centralized system [24], [25].

Built around blockchain technology, decentralized cryptocurrencies [26]–[28] were developed to obviate the need for trusting a centralized banking system. A known weakness of blockchain based decentralized cryptocurrency is the fast payment double spending attack [29] where a malicious user or group of colluding users seeks to spend a digital currency unit two or more times by exploiting the delays in verifying transactions. The double spending attack has been studied by a number of researchers [29]–[34] within the context of a single blockchain network/system. Furthermore, a variety of measures to mitigate the double spend attack have been proposed, such as having a trusted third party track transactions (e.g., notarized checkpoints). However, double spending continues to be a problem as illustrated by recent Ethereum Classic blockchain attack [35].

While interoperablility of blockchain systems has recently attracted attention [23], [49]–[59], to the best of our knowledge, our work is the first attempt to demonstrate the scenario where double spending is possible in an interoperable blockchain setting. Recent research suggests incorporating observer nodes to detect double spending in a single blockchain network [29]. However, this solution does not include the possibility of collusion between observers. Here, we propose to use a combination of observer nodes (within each participating blockchain), and policy to enforce monetary constraints to disincentivize crosschain double spends. Furthermore, we use game theory to show that it is in a rationale observer's best interest to remain honest to the system. Utilizing Ethereum's smart-contract functionality, we simulate our proposed disincentivization scheme, to investigate the cost-effectiveness of our proposal.

The remainder of the paper is organized as follows. Section II provides background on interoperable blockchain and the assumed attacker model. Section III details the proposed disincentivization mechanism. Section IV evaluated the proposed mechanism using game theory and provides the results of our Ethereum experimental implementation. Section V presents the related works. Section VI provides discussion on the proposal, and future work plans. Finally, Section VII presents our conclusions.

II. Interoperable Blockchains

A. Background on Blockchain

Blockchain is a decentralized, distributed, and an immutable ledger. Whenever any transaction happens within a blockchain network, a set of special nodes, called $miners$, listen to that transaction. They compete with each other to solve a computation-heavy puzzle fast enough by investing their computing resources to create a valid block of transactions.

978-1-7281-6741-1/19/$31.00 ©2019 IEEE
DOI 10.1109/TPS-ISA48467.2019.00014

The typical structure of a block (as shown in Figure 1) in a blockchain network includes a list of all transactions along with a nonce, merkle root hash, hash of previous block and a block header.

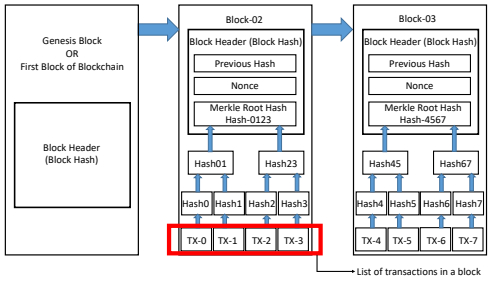

Figure 1: Typical structure of a block in a blockchain

With the increasing puzzle difficulty, it takes time for a miner to solve a puzzle. Whenever a miner node finds a solution to the puzzle, i.e. they are able to create a valid block of transactions, they broadcast that solution to all peer nodes. Verifying such a solution is straightforward. Acceptance of a block is determined if hash of that block has been included as previous block hash during formation of a new block. In this way, all nodes, eventually reach to a consensus (as demonstrated in Figure 2), known as $proof\text{-}of\text{-}work$ [26].

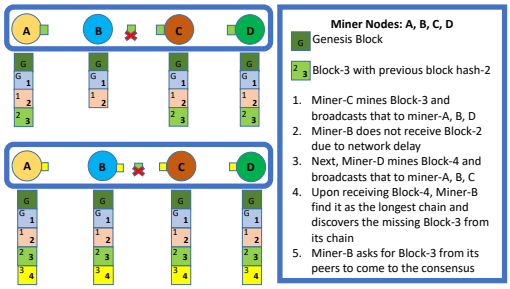

Figure 2: Proof-of-work consensus mechanism

Ethereum is a second generation blockchain [39]–[41]. It gives the user flexibility and platform to leverage the blockchain functionality for creating and deploying decentralized applications. It has two types of accounts: $externally\ owned\ account$ which is owned by the user, and $contract\ account$ which is owned by the contract. User creates smart-contract depending upon the application they want to build and deploys the smart-contract into the blockchain network. Leveraging Ethereum's smart-contract feature, any application can be build (Turing Completeness). We simulate our proposed disincentivization scheme (as demonstrated in Section IV (C)) utilizing this smart-contract functionality.

B. Trusted Interoperable Blockchains

Overview. With regards to design of an interoperable blockchains, the usage of a trustee (intermediate trusted node) for interoperation across two blockchains has been proposed [24], [36]–[38]. A trustee is part of both the participating blockchains which require interoperation between them. It is assumed that the trustee holds sufficient balance on both the participating blockchains and they transfer monetary information across the two networks. Thus far the research has focused on providing users interoperability across blockchains without consideration of the possibility that the user can double spend the transactions. Thus, we need enforcement in policy to penalize any dishonest behavior. In this regard, participating entities need to deposit money in the pre-signed smart-contract till the transaction gets confirmed in both the participating blockchains for interoperation.

Requirement 1: usage of trustee services. A set of trustees are selected which act as the forwarding agents across blockchain networks. They transfer interoperable transactions from one blockchain network to another. To operate as an interoperable agent, each trustee gets enrolled with a valid account in both participating blockchains.

Requirement 2: need for an interoperable channel. To transfer the interoperable transaction across other blockchain network, bidirectional channel is needed between participating interoperable blockchains.

Requirement 3: user's flexibility in choosing a trustee. To transfer an interoperable transaction from one blockchain network to another, each user needs the flexibility of choosing the trustee from a set of available trustees.

Requirement 4: policy to penalize dishonest behavior. We need a policy to penalize any dishonest behavior, and in this regard, participating entities need to deposit money in the pre-signed smart-contract till the interoperable transaction gets confirmed in both the participating blockchains.

Thus, any trusted interoperable blockchains should consists of the following components: (i) user enrolment service, (ii) trustee enrolment service, (iii) trustee selection service, (iv) interoperable channel, and (v) penalty service.

C. Attacker Model

Let us suppose, N_1 and N_2 are two blockchains which are part of the interoperable blockchain framework. We assume the presence of a malicious attacker $client_a$ in the first blockchain network N_1. He intends to inflict a double spend attack on the trusted interoperable blockchain system by spending the same money twice. We also assume that $client_a$ holds several other accounts in N_1. Let us assume, $user_1$ and $user_2$ are two accounts which appear as two different users but both are either possessed by or in collusion with $client_a$. Let us also assume, $user_3$ is another account belonging to another user, $client_h$ (honest user). In this situation, we have assumed that the account $user_3$ is not possessed by malicious user $client_a$, rather it is possessed by some honest user, $client_h$, which belongs to the second blockchain network N_2. $client_a$ sends money from $user_1$ to $user_3$ at time instance t_1 across the network

to get some service from $user_3$. However, after obtaining the service from the honest user $client_h$, the malicious user $client_a$ spends the same money at time instance t_2 (where, $t_2 = t_1 + \Delta$) within the blockchain network N_1 by transferring the money to another account $user_2$ which is owned by or in collusion with $client_a$. As the $client_a$ and $client_h$ belongs to two different blockchain networks (as pictorially differentiated with two different colors for two different blockchains in Figure 3), there is no way for honest user $client_h$ to detect whether double spend has been performed by the user $client_a$; thus, a successful double spend attack can be performed by the malicious user $client_a$. Pictorial demonstration of successful double spend attack on the interoperable blockchain framework is demonstrated in Figure 3. This figure as well include ledgers for two different blockchains which starts with G.

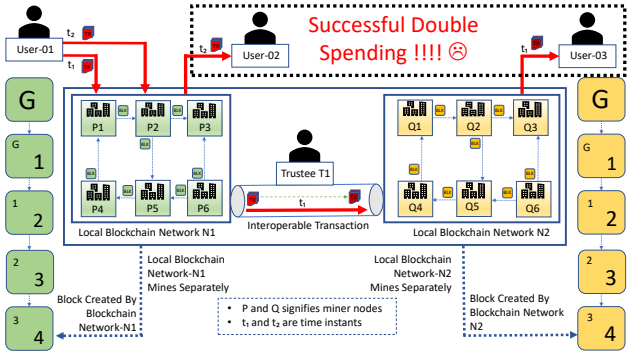

Figure 3: Double-spend attack on interoperable blockchains

III. Proposed Disincentivization Mechanism

With regards to disincentivizing double spending attempts across interoperable blockchain networks, we have incorporated the notion of observers. Every transaction sent to a trustee is endorsed by observers, i.e. the trustee accepts transactions which are only endorsed by the observers. We assume that the trustee remains honest to the system and does not double spend. The notion of an observer was proposed in [29] to solve the double spend attack in a single blockchain network. In [29] the observers were implanted by the user and thus were trusted entity for the user. However, in our proposed work, observer nodes are implanted by the trustee in both blockchain networks. Usage of single observer node for endorsement is not desirable as the observer node can collude with the user and provide wrong response to the trustee and help the user in successful double-spending. Hence, we propose the use of majority voter logic using an odd number of observer nodes (three is used here) in each of the participating networks. The response that the majority of observers submit is accepted by the trustee. With the help of the proposed disincentivization scheme, discussed next, we show via a game theoretic analysis, that instead of colluding, the three observer nodes prefer to remain honest.

A. Overview of proposed disincentivization mechanism.

Our approach incorporates three observers in each network. These observers are responsible for detecting double spending attempt while transferring monetary information between networks. Possible responses are:

1) All three observers can provide the wrong response.
2) All three observers can provide the correct response.
3) Two observers can provide the correct response, and one can provide the incorrect response.
4) Two observers can provide the incorrect response, and one can provide the correct response.

Overview of the signed smart-contract between the observer nodes and the trustee. Leveraging Ethereum's smart-contract functionality, contracts are signed between the observer nodes and a trustee. In the signed smart-contract, monetary variables and predefined rules are established and enforced. The trustee accepts the response that a majority of the observer nodes provide. In order to encourage honest behavior, money needs to be deposited in the smart-contract by all of the participating observers. This deposited money gets confiscated by the trustee from an observer node whose response differs from the response that the majority of the observer nodes provide. Monetary variables that are used for policy enforcement are listed in Table I.

Symbol	Objective
c	Cost of computation for correct result.
d_o	Deposit paid by the observer in the smart-contract signed with the trustee.
d_t	Payment given by the trustee to the observer for providing the correct computation (based upon the similar response provided by majority of the observers).
f_a	Money deposited in the collusion contract by advocate (collusion-initiator) and all other advisee (collusion-supporter). Here f signifies first secret contract, and a signifies the game initiated by the advocate.
b_a	Bribe given by the dishonest advocate to the colluder so that they take part in collusion.
μ	Reward given to all the honest observer nodes by the trustee for reporting collusion attempt.
f_h	Money deposited in the honest collusion contract (i.e., contract for report of collusion) by the observers (honest colluder and honest advisee).
b_h	Bribe given by the honest observer to the other colluder so that they take part in honest collusion.
r	Extra reward provided by trustee for honest computation based upon blockchain's data. However, this reward is given to the observer at the discretion of the trustee.

Table I: Description of monetary variables specified in the smart-contract

The functionality of the smart-contract operation for the proposed disincentivization mechanism is as follows:

- All three observer nodes and the trustee creates a signed digital smart-contract.
- To participate in detection of double-spend attempts, each of the observers deposits money d_o in the digitally signed smart-contract.

- Trustee accepts as true the majority of the observer responses.
- For computing the correct result (based on the majority of the submitted responses from the observer nodes), all the observer nodes whose response matches gets remuneration d_t from the trustee.
- An observer whose response do not match the final outcome looses the deposit d_o.
- If the interoperable transaction does not require fast payment, then the trustee can check the validity of the transaction (i.e., whether the transaction has been double spent or not) from the ledger of any randomly selected node. Then based upon the trustee's discretion each of the observer, which responses with honest computation, gets an extra reward r.

Overview of collusion between observer nodes. Due to the incorporation of majority voter logic, observers prefer to form a group for collusion (Figure 4). Note, observers and players are synonymous in our work. Out of three observers, if one responds honestly, still he may lose the deposit if other two observer nodes collude together to provide the incorrect response. The possible situations are as follows.

- $No\ Collusion$: The observers respond with their own computed value.
- $Attempted\ Collusion$: An observer tries to initiate collusion with one or more observers. However, the contacted observers decline to participate.
- $Collusion$: An observer initiates collusion with one or more observers, that agree to participate. The observer that initiates the collusion is termed the $advocate$ and any participating observers are termed as $advisees$.

To initiate collusion, observer involved in the collusion process deposits agreed-upon money to the collusion contract. For initiating the collusion with another observer, collusion-initiator (or advocate) provide incentives in terms of bribery. Upon successful completion of collusion, the participating colluder-observer receives the deposited money and agreed upon bribe; collusion initiator receives its deposited money present in the collusion contract.

Overview on the solution for the collusion prevention (i.e., report mechanism for the dishonest behavior). To achieve the manifested goals (i.e., all the observer respond honestly, and helps in double-spend detection), we need to report any dishonest behavior that any observer may incur. Out of collusion agreement in between three or less than three observers, two observers create a secret honest collusion contract with the trustee in this regard (as pictorially demonstrated in Case-04 of Figure 4). Note, this honest collusion is secret from the collusion initiator (i.e., collusion advocate). If any dishonest collusion happens, these two observers (as part of the secret honest collusion) sends the proof of collusion to the trustee. Thus, due to the report from two of the honest colluder nodes, payoff for attempting

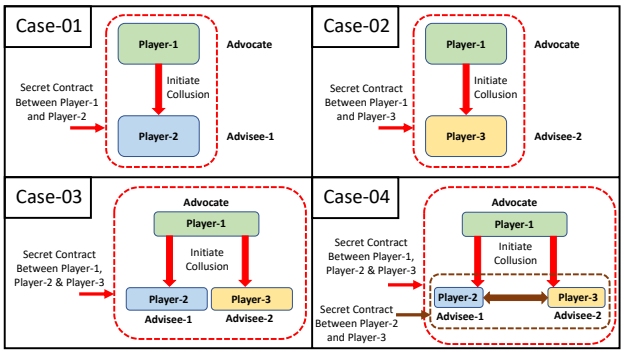

Figure 4: Pictorial demonstration of collusion between observers. Only case-4 contributes to the honest collusion and helps in achieving the desired honest response from all the observers.

collusion by the other observer turns out to be negative, and they gets banned from participating in the endorsement procedure anymore.

Even though, participating in collusion appears to be lucrative initially from the observer's point of view, still due to the chances of presence of a secret honest collusion contract in between other observer, there comes the fear of getting betrayed and losing its deposited money. Thus, remaining honest to the purpose serves as the best option for all three observer nodes.

Next section discusses in detail the evaluation on this proposed disincentivization mechanism utilizing concepts and approaches from game theory [42]. Alongside, Ethereum's smart-contract based experimental evaluation indicates the cost-effectiveness of our proposal on disincentivization.

IV. Evaluation

A. Game Theoretical Evaluation

This subsection presents game-theoretical approaches and analysis of the utilization for three observer nodes in a blockchain. However, this analysis is applicable to other networks as well (which are part of the interoperable blockchain).

Preliminaries on game theory. In each game table, for each column, consecutive three similar shades specify the possible decision path which is considered for finding the best possible utilization by a player (here, player and observer is synonymous). Utilization specified within a rectangular box for three consecutive similar shades specifies the best decision for a player among three paths.

For example, in Table II (c), for player-3, we are calculating best possible path from nodes V_{13}, V_{14} and V_{15} (shown in three consecutive similar shades) and among these three, path towards V_{13} leads to best possible utilization. For player-2, we are calculating best possible path from nodes V_{13}, V_{17} and V_{19} (shown in three consecutive similar shades) and among these three, path towards V_{17} leads to best possible utilization. For player-1, we are calculating best possible path from nodes V_{17}, V_{26} and V_{35} (shown in

three consecutive similar shades) and among these three, path towards V_{26} leads to best possible utilization.

In each game table, terminal node with red color signify the path that leads to the best possible utilization for all the three players, i.e. it leads to equilibria for all the three players. For each game table, utilization for each $Player_i$ is U_i, where $U_i = P_i - c_i$ for $i = 1, 2,$ and 3. P_i and c_i signifies the payoff and cost of computation for each of the $Player_i$. Cost of computation for the correct response to validate whether double spend has happened or not (irrespective of any specified rules as discussed in Section III) is demonstrated in Table II (a).

Brief demonstrations of games. Each steps contributing towards achieving the disincentivization rules are elaborated below in a form of game. Total 7 games with game tables (utilization matrix) and game tree are described concerning our disincentivization scheme. Payoff for Game-1 is demonstrated in Table II (b). However, original payoff for each $Player_i$ for all other games can be calculated back from the demonstrated utilization table corresponding to that game using $P_i = U_i + c_i$, for $i = 1, 2,$ and 3. Each game tree demonstrates all possible decision paths for all the observers. Paths that each of the observer node might take can be obtained by level order traversal of the game tree. As there are total 3 observer nodes and root of game tree starts with v_0, so leaf node starts from v_{13} and ends at v_{39}.

Game-1. Considering majority voter logic, i.e. the response that majority of the observers agreed upon, trustee sends money d_t to those observers; otherwise, observer's deposited money d_o gets confiscated by the trustee. Utilization matrix corresponding to this game is demonstrated in Table II (c). Figure 5 demonstrates that path leading towards terminal node V_{26} is more profitable for all the players. Thus, we conclude that taking part in collusion leads to better utilization for all the players present in game-1.

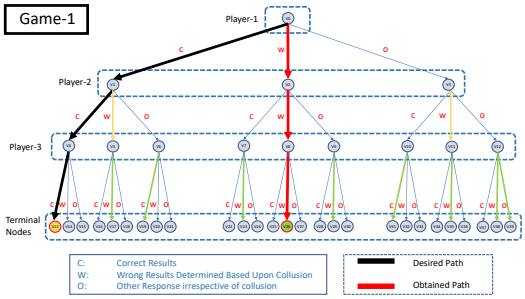

Figure 5: Game-1 demonstrating collusion as the best strategy for all the observers (shown in red path)

Game-2. We require to update the payoff in the payoff matrix (i.e., the reward mechanism needs to be changed) to change the previously demonstrated game dynamics. Added Reward: observer's deposited money d_o is given back to them if all the three observer provide the same response. Utilization matrix for each player of game-2 is demonstrated in Table II (d). As shown in Figure 6, path leading towards terminal node V_{26} is more profitable for all the players. Thus, we conclude that taking part in collusion leads to better utilization for all the players present in the game.

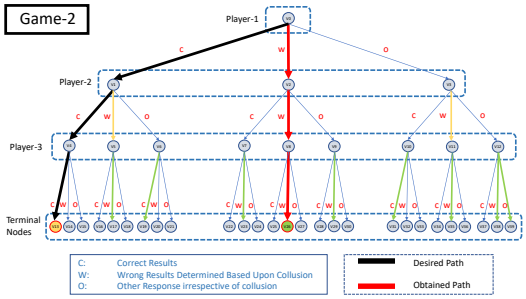

Figure 6: Game-2 demonstrating collusion as the best strategy for all the observers (shown in red path)

Game-3. We require to update the payoff in the payoff matrix to change the previously demonstrated game dynamics. Added Reward: extra reward r for all consecutive honest computation based on the discretion of trustee is provided to the observer. The utilization matrix for each of the players of game-3 is demonstrated in Table III (a). As demonstrated in Figure 7, path leading towards terminal node V_{13} is more profitable for all the players. Thus, we conclude that remaining honest to the protocol leads to better utilization for all the players present into the game.

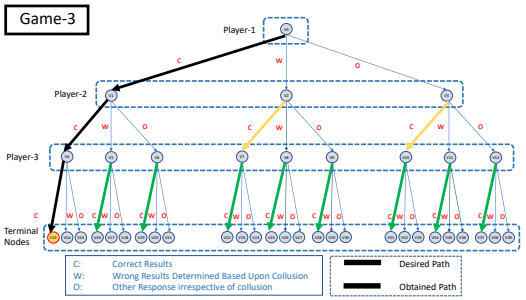

Figure 7: Game-3 demonstrating honesty as the best strategy for all the observers (shown in black path).

Game-4 (case-1 of collusion contract). Although game-3 demonstrates achievement of the desired result (i.e., honest behavior from all the observer nodes), it does not consider the possibility of collusion in between observers. Thus, if one of the observer initiate collusion (we term collusion initiator as an advocate), and another observer agrees to that collusion (we term collusion supporter as an advisee), then game-3 fails to provide the desired outcome. However, game-3 and game-4 is equivalent if the advocate does not initiate collusion, or if the advisee does not agree to collude with the advocate. In all other cases, game-4 deviates from the desired outcome which leads to game-3. Hence, we require to update the payoff (i.e., the reward) in the

Node	Player-1	Player-2	Player-3
V_{13}	c	c	c
V_{14}	c	c	0
V_{15}	c	c	0
V_{16}	c	0	c
V_{17}	c	0	0
V_{18}	c	0	0
V_{19}	c	0	c
V_{20}	c	0	0
V_{21}	c	0	0
V_{22}	0	c	c
V_{23}	0	c	0
V_{24}	0	c	0
V_{25}	0	0	c
V_{26}	0	0	0
V_{27}	0	0	0
V_{28}	0	0	c
V_{29}	0	0	0
V_{30}	0	0	0
V_{31}	0	c	c
V_{32}	0	c	0
V_{33}	0	c	0
V_{34}	0	0	c
V_{35}	0	0	0
V_{36}	0	0	0
V_{37}	0	0	c
V_{38}	0	0	0
V_{39}	0	0	0

(a) Initial cost of computation

Node	Player-1	Player-2	Player-3
V_{13}	d_t	d_t	d_t
V_{14}	d_t	d_t	$-d_o$
V_{15}	d_t	d_t	$-d_o$
V_{16}	d_t	$-d_o$	d_t
V_{17}	$-d_o$	d_t	d_t
V_{18}	$-d_o$	$-d_o$	$-d_o$
V_{19}	d_t	$-d_o$	d_t
V_{20}	$-d_o$	$-d_o$	$-d_o$
V_{21}	$-d_o$	$-d_o$	$-d_o$
V_{22}	$-d_o$	d_t	d_t
V_{23}	d_t	$-d_o$	d_t
V_{24}	$-d_o$	$-d_o$	$-d_o$
V_{25}	d_t	d_t	$-d_o$
V_{26}	d_t	d_t	d_t
V_{27}	d_t	d_t	$-d_o$
V_{28}	$-d_o$	$-d_o$	$-d_o$
V_{29}	d_t	d_t	d_t
V_{30}	$-d_o$	$-d_o$	$-d_o$
V_{31}	$-d_o$	d_t	d_t
V_{32}	$-d_o$	$-d_o$	$-d_o$
V_{33}	$-d_o$	$-d_o$	$-d_o$
V_{34}	$-d_o$	$-d_o$	$-d_o$
V_{35}	$-d_o$	d_t	d_t
V_{36}	$-d_o$	$-d_o$	$-d_o$
V_{37}	$-d_o$	$-d_o$	$-d_o$
V_{38}	$-d_o$	$-d_o$	$-d_o$
V_{39}	$-d_o$	$-d_o$	$-d_o$

(b) Game-1 payoff matrix

Node	Player-1	Player-2	Player-3
V_{13}	d_t - c	d_t - c	d_t - c
V_{14}	d_t - c	d_t - c	$-d_o$
V_{15}	d_t - c	d_t - c	$-d_o$
V_{16}	d_t - c	$-d_o$	d_t - c
V_{17}	$-d_o$ - c	d_t	d_t
V_{18}	$-d_o$ - c	$-d_o$	$-d_o$
V_{19}	d_t - c	$-d_o$	d_t - c
V_{20}	$-d_o$ - c	$-d_o$	$-d_o$
V_{21}	$-d_o$ - c	$-d_o$	$-d_o$
V_{22}	$-d_o$	d_t - c	d_t - c
V_{23}	d_t	$-d_o$ - c	d_t
V_{24}	$-d_o$	$-d_o$ - c	$-d_o$
V_{25}	d_t	d_t	$-d_o$ - c
V_{26}	d_t	d_t	d_t
V_{27}	d_t	d_t	$-d_o$
V_{28}	$-d_o$	$-d_o$	$-d_o$ - c
V_{29}	d_t	$-d_o$	d_t
V_{30}	$-d_o$	$-d_o$	$-d_o$
V_{31}	$-d_o$	d_t - c	d_t - c
V_{32}	$-d_o$	$-d_o$ - c	$-d_o$
V_{33}	$-d_o$	$-d_o$ - c	$-d_o$
V_{34}	$-d_o$	$-d_o$	$-d_o$ - c
V_{35}	$-d_o$	d_t	d_t
V_{36}	$-d_o$	$-d_o$	$-d_o$
V_{37}	$-d_o$	$-d_o$	$-d_o$ - c
V_{38}	$-d_o$	$-d_o$	$-d_o$
V_{39}	$-d_o$	$-d_o$	$-d_o$

(c) Game-1 utilization matrix

Node	Player-1	Player-2	Player-3
V_{13}	$d_t + d_o$ - c	$d_t + d_o$ - d	$d_t + d_o$ - d
V_{14}	d_t - c	d_t - c	$-d_o$
V_{15}	d_t - c	d_t - c	$-d_o$
V_{16}	d_t - c	$-d_o$	d_t - c
V_{17}	$-d_o$ - c	d_t	d_t
V_{18}	$-d_o$ - c	$-d_o$	$-d_o$
V_{19}	d_t - c	$-d_o$	d_t - c
V_{20}	$-d_o$ - c	$-d_o$	$-d_o$
V_{21}	$-d_o$ - c	$-d_o$	$-d_o$
V_{22}	$-d_o$	d_t - c	d_t - c
V_{23}	d_t	$-d_o$ - c	d_t
V_{24}	$-d_o$	$-d_o$ - c	$-d_o$
V_{25}	d_t	d_t	$-d_o$ - c
V_{26}	$d_t + d_o$	$d_t + d_o$	$d_t + d_o$
V_{27}	d_t	d_t	$-d_o$
V_{28}	$-d_o$	$-d_o$	$-d_o$ - c
V_{29}	d_t	$-d_o$	d_t
V_{30}	$-d_o$	$-d_o$	$-d_o$
V_{31}	$-d_o$	d_t - c	d_t - c
V_{32}	$-d_o$	$-d_o$ - c	$-d_o$
V_{33}	$-d_o$	$-d_o$ - c	$-d_o$
V_{34}	$-d_o$	$-d_o$	$-d_o$ - c
V_{35}	$-d_o$	d_t	d_t
V_{36}	$-d_o$	$-d_o$	$-d_o$
V_{37}	$-d_o$	$-d_o$	$-d_o$ - c
V_{38}	$-d_o$	$-d_o$	$-d_o$
V_{39}	$-d_o$	$-d_o$	$-d_o$

(d) Game-2 utilization matrix

Table II: (a) Cost of computation for finding the correct response by each of the observer. Desired path leads to end vertex V_{13} (shown in red color). (b) Demonstrated payoff matrix for Game-1. (c) Game-1 utilization matrix demonstrating collusion as the best strategy for all the observer (shown in red color terminal node V_{26}). (d) Game-2 utilization matrix demonstrating collusion as the best strategy for all the observer (shown in red color terminal node V_{26}).

Node	Player-1	Player-2	Player-3
V_{13}	$d_t + d_o + r - d$	$d_t + d_o + r - d$	$d_t + d_o + r - d$
V_{14}	$d_t + r - c$	$d_t + r - c$	$-d_o$
V_{15}	$d_t + r - c$	$d_t + r - c$	$-d_o$
V_{16}	$d_t + r - c$	$-d_o$	$d_t + r - d$
V_{17}	$-d_o + r - c$	d_t	d_t
V_{18}	$-d_o + r - c$	$-d_o$	$-d_o$
V_{19}	$d_t + r - c$	$-d_o$	$d_t + r - d$
V_{20}	$-d_o + r - c$	$-d_o$	$-d_o$
V_{21}	$-d_o + r - c$	$-d_o$	$-d_o$
V_{22}	$-d_o$	$d_t + r - d$	$d_t + r - d$
V_{23}	d_t	$-d_o + r - c$	d_t
V_{24}	$-d_o$	$-d_o + r - c$	$-d_o$
V_{25}	d_t	d_t	$-d_o + r - d$
V_{26}	$d_t + d_o$	$d_t + d_o$	$d_t + d_o$
V_{27}	d_t	d_t	$-d_o$
V_{28}	$-d_o$	$-d_o$	$-d_o + r - d$
V_{29}	d_t	$-d_o$	d_t
V_{30}	$-d_o$	$-d_o$	$-d_o$
V_{31}	$-d_o$	$d_t + r - d$	$d_t + r - d$
V_{32}	$-d_o$	$-d_o + r - c$	$-d_o$
V_{33}	$-d_o$	$-d_o + r - c$	$-d_o$
V_{34}	$-d_o$	$-d_o$	$-d_o + r - d$
V_{35}	d_t	d_t	d_t
V_{36}	$-d_o$	$-d_o$	$-d_o$
V_{37}	$-d_o$	$-d_o$	$-d_o + r - d$
V_{38}	$-d_o$	$-d_o$	$-d_o$
V_{39}	$-d_o$	$-d_o$	$-d_o$

(a) Game-3 utilization

Node	Player-1	Player-2	Player-3
V_{13}	$d_t + d_o + r - f_a - b_a - c$	$d_t + d_o + r - f_a - c$	$d_t + d_o + r - d$
V_{14}	$d_t + r - f_a - b_a - c$	$d_t + r - f_a - c$	$-d_o$
V_{15}	$d_t + r - f_a - b_a - c$	$d_t + r - f_a - c$	$-d_o$
V_{16}	$d_t + r - f_a - b_a - c$	$-d_o + 2f_a + b_a$	$d_t + r - d$
V_{17}	$-d_o + r - f_a - b_a - c$	$d_t + 2f_a + b_a$	d_t
V_{18}	$-d_o + r - f_a - b_a - c$	$-d_o + 2f_a + b_a$	$-d_o$
V_{19}	$d_t + r - f_a - b_a - c$	$-d_o - f_a$	$d_t + r - d$
V_{20}	$-d_o + r - f_a - b_a - c$	$-d_o - f_a$	$-d_o$
V_{21}	$-d_o + r - f_a - b_a - c$	$-d_o - f_a$	$-d_o$
V_{22}	$-d_o + 2f_a + b_a$	$d_t + r - f_a - c$	$d_t + r - d$
V_{23}	$d_t + 2f_a + b_a$	$-d_o + r - f_a - c$	d_t
V_{24}	$-d_o + 2f_a + b_a$	$-d_o + r - f_a - c$	$-d_o$
V_{25}	$d_t + f_a$	$d_t + f_a + b_a$	$-d_o + r - d$
V_{26}	$d_t + d_o + f_a$	$d_t + d_o + f_a + b_a$	$d_t + d_o$
V_{27}	$d_t + f_a$	$d_t + f_a + b_a$	$-d_o$
V_{28}	$-d_o + 2f_a + b_a$	$-d_o + f_a$	$-d_o + r - d$
V_{29}	$d_t + 2f_a + b_a$	$-d_o - f_a$	d_t
V_{30}	$-d_o + 2f_a + b_a$	$-d_o + f_a$	$-d_o$
V_{31}	$-d_o - f_a - b_a$	$d_t + r - f_a - c$	$d_t + r - d$
V_{32}	$-d_o - f_a - b_a$	$-d_o + r - f_a - c$	$-d_o$
V_{33}	$-d_o - f_a - b_a$	$-d_o + r - f_a - c$	$-d_o$
V_{34}	$-d_o - f_a - b_a$	$-d_o + 2f_a + b_a$	$-d_o + r - d$
V_{35}	$-d_o - f_a - b_a$	$d_t + 2f_a + b_a$	d_t
V_{36}	$-d_o - f_a - b_a$	$-d_o + 2f_a + b_a$	$-d_o$
V_{37}	$-d_o - f_a - b_a$	$-d_o - f_a$	$-d_o + r - d$
V_{38}	$-d_o - f_a - b_a$	$-d_o - f_a$	$-d_o$
V_{39}	$-d_o - f_a - b_a$	$-d_o - f_a$	$-d_o$

(b) Game-4 utilization

Node	Player-1	Player-2	Player-3
V_{13}	$d_t + d_o + r - f_a - b_a - c$	$d_t + d_o + r - c$	$d_t + d_o + r - f_a - c$
V_{14}	$d_t + r - f_a - b_a - c$	$d_t + r - d$	$-d_o + 2f_a + b_a$
V_{15}	$d_t + r - f_a - b_a - c$	$d_t + r - c$	$-d_o - f_a$
V_{16}	$d_t + r - f_a - b_a - c$	$-d_o$	$d_t + r - f_a - c$
V_{17}	$-d_o + r - f_a - b_a - c$	d_t	$d_t + 2f_a + b_a$
V_{18}	$-d_o + r - f_a - b_a - c$	$-d_o$	$-d_o - f_a$
V_{19}	$d_t + r - f_a - b_a - c$	$-d_o$	$d_t + r - f_a - c$
V_{20}	$-d_o + r - f_a - b_a - c$	$-d_o$	$-d_o + 2f_a + b_a$
V_{21}	$-d_o + r - f_a - b_a - c$	$-d_o$	$-d_o - f_a$
V_{22}	$-d_o + 2f_a + b_a$	$d_t + r - c$	$d_t + r - f_a - c$
V_{23}	$d_t + f_a - b_a$	$-d_o + r - c$	$d_t + f_a + b_a$
V_{24}	$-d_o + 2f_a + b_a$	$-d_o + r - c$	$-d_o - f_a$
V_{25}	$d_t + f_a$	$d_t + f_a + b_a$	$-d_o + r - f_a - c$
V_{26}	$d_t + d_o + f_a - b_a$	$d_t + d_o$	$d_t + d_o + f_a + b_a$
V_{27}	$d_t + 2f_a + b_a$	d_t	$-d_o - f_a$
V_{28}	$-d_o + 2f_a + b_a$	$-d_o$	$-d_o + r - f_a - c$
V_{29}	$d_t + f_a - b_a$	$-d_o$	$d_t + f_a + b_a$
V_{30}	$-d_o + 2f_a + b_a$	$-d_o$	$-d_o - f_a$
V_{31}	$-d_o - f_a - b_a$	$d_t + r - f_a - c$	$d_t + r - f_a - c$
V_{32}	$-d_o - f_a - b_a$	$-d_o + r - c$	$-d_o + 2f_a + b_a$
V_{33}	$-d_o - f_a - b_a$	$-d_o + r - c$	$-d_o - f_a$
V_{34}	$-d_o - f_a - b_a$	$-d_o$	$-d_o + r - f_a - c$
V_{35}	$-d_o - f_a - b_a$	d_t	$d_t + 2f_a + b_a$
V_{36}	$-d_o - f_a - b_a$	$-d_o$	$-d_o - f_a$
V_{37}	$-d_o - f_a - b_a$	$-d_o$	$-d_o + r - f_a - c$
V_{38}	$-d_o - f_a - b_a$	$-d_o$	$-d_o + 2f_a + b_a$
V_{39}	$-d_o - f_a - b_a$	$-d_o$	$-d_o - f_a$

(c) Game-5 utilization

Table III: (a) Game-3 utilization matrix demonstrating honesty as the best strategy for all the observer (shown in red color terminal node V_{13}). (b) Game-4 utilization matrix demonstrating collusion as the best strategy for majority of the observer (shown in red color terminal node V_{25}). (c) Game-5 utilization matrix demonstrating collusion as the best strategy for majority of the observer (shown in red color terminal node V_{23}).

payoff matrix to change the game dynamics of game-4. Added Reward: if advisee follows the agreed upon collusion, it is rewarded with bribe b_a, else its deposited money f_a gets confiscated. If advocate does not follow collusion and advisee follows, then its deposited money f_a is given to the advisee. This game is demonstrated in Table III (b). As shown in Figure 8, path leading towards terminal node V_{25} is more profitable for all the players. Thus, we conclude that collusion leads to better utilization for both colluders irrespective of the presence of third player into the game-4.

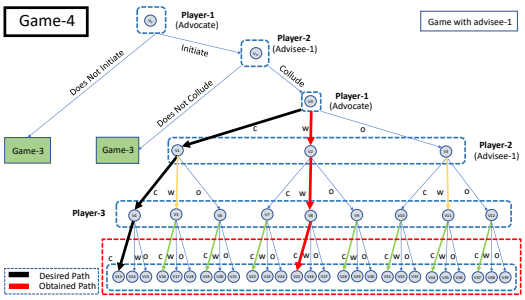

Figure 8: Game-4 shows path leading towards collusion is taken as it is more profitable for majority of the observer.

Game-5 (case-2 of collusion contract). Here, instead of choosing player-2 for collusion initiation, advocate initiate collusion with the player-3. Hence, game-4 and game-5 are essentially equivalent in terms of functionality, and their reward mechanism is similar. However, game-5 is equivalent to game-3, if the advocate does not initiate collusion, or if the advisee does not agree to collude with the advocate. In all other cases, game-5 deviates from the desired outcome that game-3 provides. The utilization matrix for each of

Node	Player-1	Player-2	Player-3
V_{13}	$d_t + d_o + r - f_a - 2b_a - c$	$d_t + d_o + r - f_a - c$	$d_t + d_o + r - f_a - c$
V_{14}	$d_t + r - f_a - 2b_a - c$	$d_t + r - f_a - c$	$\boxed{-d_o + 3f_a + 2b_a}$
V_{15}	$d_t + r - f_a - 2b_a - c$	$d_t + r - f_a - c$	$-d_o - f_a$
V_{16}	$d_t + r - f_a - 2b_a - c$	$-d_o + 3f_a + b_a$	$d_t + r - f_a - c$
V_{17}	$-d_o + r - f_a - 2b_a - c$	$\boxed{d_t + 1.5f_a + b_a}$	$\boxed{d_t + 1.5f_a + b_a}$
V_{18}	$-d_o + r - f_a - 2b_a - c$	$-d_o + 3f_a + b_a$	$-d_o - f_a$
V_{19}	$d_t + r - f_a - 2b_a - c$	$-d_o - f_a$	$d_t + r - f_a - c$
V_{20}	$-d_o + r - f_a - 2b_a - c$	$-d_o - f_a$	$\boxed{-d_o + 3f_a + 2b_a}$
V_{21}	$-d_o + r - f_a - 2b_a - c$	$-d_o - f_a$	$-d_o - f_a$
V_{22}	$-d_o + 3f_a + 2b_a$	$d_t + r - f_a - c$	$d_t + r - f_a - c$
V_{23}	$d_t + 1.5f_a + b_a$	$-d_o + r - f_a - c$	$\boxed{d_t + 1.5f_a + b_a}$
V_{24}	$-d_o + 3f_a + 2b_a$	$-d_o + r - f_a - c$	$-d_o - f_a$
V_{25}	$d_t + 1.5f_a + b_a$	$d_t + 1.5f_a + b_a$	$-d_o + r - f_a - c$
V_{26}	$\boxed{d_t + d_o + f_a - 2b_a}$	$\boxed{d_t + d_o + f_a - b_a}$	$\boxed{d_t + d_o + f_a + b_a}$
V_{27}	$d_t + 1.5f_a + b_a$	$d_t + 1.5f_a + b_a$	$-d_o - f_a$
V_{28}	$-d_o + 3f_a + 2b_a$	$-d_o - f_a$	$-d_o + r - f_a - c$
V_{29}	$d_t + 1.5f_a + b_a$	$-d_o - f_a$	$\boxed{d_t + 1.5f_a + b_a}$
V_{30}	$-d_o + 3f_a + 2b_a$	$-d_o - f_a$	$-d_o - f_a$
V_{31}	$-d_o - f_a - 2b_a$	$d_t + r - f_a - c$	$d_t + r - f_a - c$
V_{32}	$-d_o - f_a - 2b_a$	$-d_o + r - f_a - c$	$\boxed{-d_o + 3f_a + 2b_a}$
V_{33}	$-d_o - f_a - 2b_a$	$-d_o + r - f_a - c$	$-d_o - f_a$
V_{34}	$-d_o - f_a - 2b_a$	$-d_o + 3f_a + 2b_a$	$-d_o + r - f_a - c$
V_{35}	$-d_o - f_a - 2b_a$	$\boxed{d_t + 1.5f_a + b_a}$	$\boxed{d_t + 1.5f_a + b_a}$
V_{36}	$-d_o - f_a - 2b_a$	$-d_o + 3f_a + 2b_a$	$-d_o - f_a$
V_{37}	$-d_o - f_a - 2b_a$	$-d_o - f_a$	$-d_o + r - f_a - c$
V_{38}	$-d_o - f_a - 2b_a$	$-d_o - f_a$	$\boxed{-d_o + 3f_a + 2b_a}$
V_{39}	$-d_o - f_a - 2b_a$	$-d_o - f_a$	$-d_o - f_a$

(a) Game-6 utilization

Node	Player-1	Player-2	Player-3
V_{13}	$\boxed{d_t + d_o + r - f_a - 2b_a - c}$	$\boxed{d_t + d_o + r - f_a + f_h - b_h + \mu - c}$	$\boxed{d_t + d_o + r - f_a + f_h + b_h + \mu - c}$
V_{14}	$d_t + r - f_a - 2b_a - c$	$d_t + r - f_a + 2f_h + b_h + \mu - c$	$-d_o + 3f_a + 2b_a - f_h$
V_{15}	$d_t + r - f_a - 2b_a - c$	$d_t + r - f_a + 2f_h + b_h + \mu - c$	$-d_o - f_a - f_h$
V_{16}	$d_t + r - f_a - 2b_a - c$	$-d_o + 3f_a + b_a - f_h - b_h$	$\boxed{d_t + r - f_a + 2f_h + b_h + \mu - c}$
V_{17}	$-d_o + r - f_a - 2b_a - c$	$d_t + 1.5f_a + b_a - f_h - b_h$	$d_t + 1.5f_a + b_a - f_h$
V_{18}	$-d_o + r - f_a - 2b_a - c$	$-d_o + 3f_a + b_a - f_h - b_h$	$-d_o - f_a - f_h$
V_{19}	$d_t + r - f_a - 2b_a - c$	$-d_o - f_a - f_h - b_h$	$\boxed{d_t + r - f_a + 2f_h + b_h + \mu - c}$
V_{20}	$-d_o + r - f_a - 2b_a - c$	$-d_o - f_a - f_h - b_h$	$-d_o + 3f_a + 2b_a - f_h$
V_{21}	$-d_o + r - f_a - 2b_a - c$	$-d_o - f_a - f_h - b_h$	$-d_o - f_a - f_h$
V_{22}	$-d_o - 3f_a - 2b_a$	$\boxed{d_t + r - f_a + f_h - b_h + \mu - c}$	$\boxed{d_t + r - f_a + f_h + b_h + \mu - c}$
V_{23}	$d_t + 1.5f_a + b_a$	$-d_o + r - f_a + 2f_h + b_h + \mu - c$	$d_t + 1.5f_a + b_a - f_h$
V_{24}	$-d_o + 3f_a + 2b_a$	$-d_o + r - f_a + 2f_h + b_h + \mu - c$	$-d_o - f_a - f_h$
V_{25}	$d_t + 1.5f_a + b_a$	$d_t + 1.5f_a + b_a - f_h - b_h$	$\boxed{-d_o + r - f_a + 2f_h + b_h + \mu - c}$
V_{26}	$d_t + d_o + f_a - 2b_a$	$d_t + d_o + f_a + b_a - f_h - b_h$	$d_t + d_o + f_a + b_a - f_h$
V_{27}	$d_t + 1.5f_a + b_a$	$d_t + 1.5f_a + b_a - f_h - b_h$	$-d_o - f_a - f_h - b_h$
V_{28}	$-d_o + 3f_a + 2b_a$	$-d_o - f_a - f_h - b_h$	$\boxed{-d_o + r - f_a + 2f_h + b_h + \mu - c}$
V_{29}	$d_t + 1.5f_a + b_a$	$-d_o - f_a - f_h - b_h$	$d_t + 1.5f_a + b_a - f_h$
V_{30}	$-d_o + 3f_a + 2b_a$	$-d_o - f_a - f_h - b_h$	$-d_o - f_a - f_h$
V_{31}	$-d_o - f_a - 2b_a$	$\boxed{d_t + r - f_a + f_h - b_h + \mu - c}$	$\boxed{d_t + r - f_a + f_h + b_h + \mu - c}$
V_{32}	$-d_o - f_a - 2b_a$	$-d_o + r - f_a + 2f_h + b_h + \mu - c$	$-d_o + 3f_a + 2b_a - f_h$
V_{33}	$-d_o - f_a - 2b_a$	$-d_o + r - f_a + 2f_h + b_h + \mu - c$	$-d_o - f_a - f_h$
V_{34}	$-d_o - f_a - 2b_a$	$-d_o + 3f_a + 2b_a - f_h - b_h$	$\boxed{-d_o + r - f_a + 2f_h + b_h + \mu - c}$
V_{35}	$-d_o - f_a - 2b_a$	$d_t + 1.5f_a + b_a - f_h - b_h$	$d_t + 1.5f_a + b_a - f_h$
V_{36}	$-d_o - f_a - 2b_a$	$-d_o + 3f_a + 2b_a - f_h - b_h$	$-d_o - f_a - f_h$
V_{37}	$-d_o - f_a - 2b_a$	$-d_o - f_a - f_h - b_h$	$\boxed{-d_o + r - f_a + 2f_h + b_h + \mu - c}$
V_{38}	$-d_o - f_a - 2b_a$	$-d_o - f_a - f_h - b_h$	$-d_o + 3f_a + 2b_a - f_h$
V_{39}	$-d_o - f_a - 2b_a$	$-d_o - f_a - f_h - b_h$	$-d_o - f_a - f_h$

(b) Game-7 utilization

Table IV: (a) Game-6 utilization matrix demonstrating collusion as the best strategy for majority of the observer (shown in red color terminal node V_{26}). (b) Game-7 utilization matrix demonstrating honesty as the best strategy for all of the observer (shown in red color node V_{13}).

the player in game-5 is demonstrated in Table III (c). As shown in Figure 9, path leading towards terminal node V_{23} is more profitable for all the players. Thus, we conclude that collusion leads to better utilization for both the colluder irrespective of the presence of third player into the game.

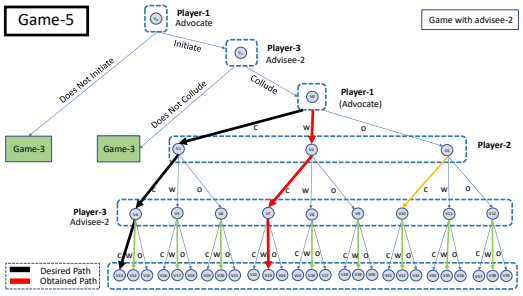

Figure 9: Game-5 shows path leading towards collusion is taken as it is more profitable for majority of the observer.

Game-6 (case-3 of collusion contract). Here, the advocate initiate collusion with both the advisee, compared to both game-4 or game-5. Thus, they are essentially similar in terms of functionality. Hence, the reward mechanism for game-6 is similar to that of game-4 and game-5. However, game-6 is equivalent to game-3, if the advocate does not initiate collusion, or if both the advisee does not agree to collude with the advocate. If advisee-1 does not agrees to collude, game-6 is equivalent to game-4, and if advisee-2 does not agrees to collude, then game-6 is equivalent to game-5. When both the advisee agrees to collude, then utilization matrix for each of the player (for game-6) is demonstrated in Table IV (a). As shown in Figure 10, path leading towards terminal node V_{26} is more profitable for all the players. Thus, we conclude that collusion leads to better utilization for all the players present into the game.

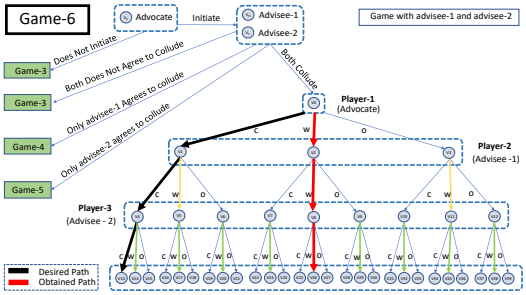

Figure 10: Game-6 demonstrate that collusion leads to better utilization for all the observers.

Game-7 (case-4 of collusion contract). Here, the reward mechanism for game-7 is similar to game-6. Thus, essentially both game-6 and game-7 are similar when both the advisee agrees to collude. Henceforth, we require to change the payoff in the payoff matrix, i.e., the reward mechanism needs to be updated to change the game dynamics.

Added Reward: extra reward μ from the trustee is given to both the honest colluder for demonstrating honest behavior. Due to this extra reward, both the advisee prefers to create a secret honest collusion contract in between them. The utilization matrix for each of the player in game-7 is demonstrated in Table IV (b). Figure 11 shows the flow of secret collusion contract in between observers. Figure 12 demonstrate path leading towards terminal node V_{13} (final desired path) is more profitable for all the players.

Thus, we conclude that remaining honest to the protocol leads to better utilization for all the players (i.e., observers) present in the game. Hence, double spending attempt across the interoperable blockchain network can successfully be disincentivized for all the rational observers.

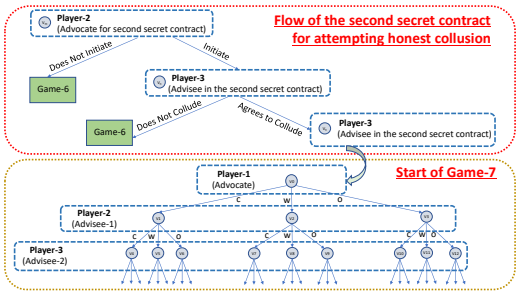

Figure 11: Pictorial demonstration of flow from game-6 to game-7 for starting secret contract for honest collusion in between observers

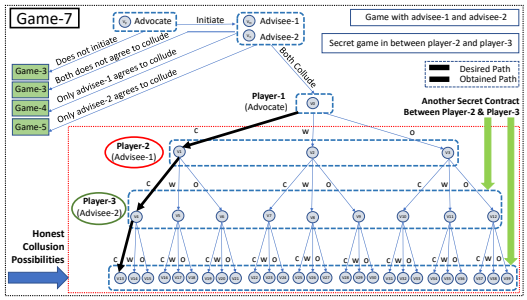

Figure 12: Game-7 demonstrating honesty as the best strategy for all the observers.

B. Monetary Policy Enforcement

With regards to detection of successful double spend attempt by the neutral observers, we demonstrate *disincentivization mechanisms* for which monetary policy needs to be enforced in the decentralized smart-contract. These enforced monetary constraints are obtained after rigorous game theoretic analysis of all the seven games, and updated reward mechanism for each of the games. These enforced constraints are listed in Table V.

Condition	Enforced monetary constraints
1.	$r > d_t + 2d_o + c$
2.	$d_t + d_o + r > c$
3.	$3f_a + 2b_a + c > d_t + d_o + r$
4.	$2f_a + b_a + c > r$
5.	$2f_h + b_h + \mu > 4f_a + 2b_a + c$
6.	$3f_h + b_h + \mu > 2d_o + d_t + 2f_a + b_a + c$
7.	$2f_h + r + \mu > 4f_a + 2b_a + c$

Table V: Rules for monetary policy enforcement.

C. Experimental Evaluation

Leveraging Ethereum's smart-contract functionality, we experimentally evaluated the effectiveness of our proposed disincentivization scheme (described in Section III (A) and in Section IV (A)) for the trusted interoperable blockchain. We evaluate the effectiveness in terms of required gas, gas costs, transaction fee, and monetary costs (in USD).

Setup. We perform all experiments on Ubuntu 18.04 LTS 64 bit operating systems, 16 GB RAM, and Intel Core i7, 2.81 GHz machine. Accounts are created using MetaMask [63]. To make all the accounts functional, we accumulate ETHER [64] from the Kovan TestNet network [65]. Utilizing the test network platform provided by Kovan TestNet [66], we perform experimental evaluation.

Smart-Contract Implementation. To simulate the proposed disincentivization scheme, we create four smart-contracts to simulate: (i) $framework$ (trusted interoperable blockchain), (ii) $agreement$, (iii) $collusion$, and (iv) $report$ mechanism. These smart-contracts are deployed using remix [61], [62] which is build for smart-contract deployment from the web browser in the Ethereum based decentralized blockchain platform. We simulate three observers, two users (including two accounts that belongs to the attacker and another which belongs to the honest user), and a trustee by creating total seven externally owned accounts.

Findings. We find (as shown in Figure 13) that each of the implemented and deployed smart-contract requires approximately 2 USD worth of gas [67] to operate effectively. Here, prices of gas are consistent (0.000000022 ETH) for all the deployed smart-contracts, and total costs changes due to the variation of required transaction fee. This conversion is performed with the exchange rate of 1 ETH = 165.82 USD.

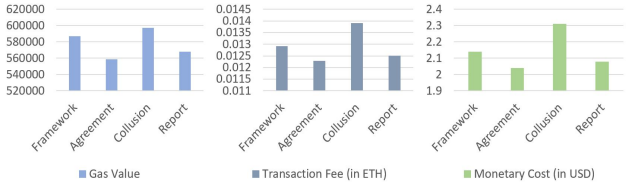

Figure 13: Experimental results summarizing smart-contract deployment costs in terms of required gas value, transaction fee (in ETH), and total monetary costs (in USD).

V. Related Work

Double spending has been a well known and difficult problem to solve in the cyber world for several decades [43]–[48]. In the blockchain ecosystem, all the work on double spending along with the measures to tackle the same [29]–[31] has been performed only on the Bitcoin-based single blockchain, and no attention have been given to the double spending problem across an interoperable blockchain [23], [49]–[60]. To the best of our knowledge, our work is the first attempt to demonstrate the scenario where double spending is possible in an interoperable blockchain and also proposes a solution to tackle the same.

We argue that direct incorporation of the existing solutions to tackle the double spend problem within a single blockchain network, i.e. incorporation of one or more observer nodes cannot be incorporated into the interoperable blockchain as it does not include the possibility of collusion in between observer nodes. We recommend incorporation of three neutral observers in each of the participating blockchains in the interoperable blockchain framework,

provided our proposed disincentivization mechanism is adopted that makes the system resilient against collusion and consequently resilient from the double-spend attack.

VI. Discussions and Future Work

The required assumptions, limitations, and discussions to our proposal on disincentivizing double-spend attempt using neutral observers are mentioned as follows:

- We propose disincentivization mechanism to safeguard the trustee from being a victim of double spend attack that the user might incur. Thus, we assume, trustee remain honest to the system.
- Observer nodes can be chosen by the trustee from the already existing blockchain network, or they can even be deployed by the trustee to each of the participating blockchains that require interoperation.
- Deployment of a node as the observer in a blockchain network is more expensive than using the already existing nodes as the observer. Thus, we recommend selecting observer from the already existing nodes from participating blockchains requiring interoperability.
- Due to the open, anonymous participation, anybody can join the public blockchain network. Thus, trustee may choose to appoint any node or miner as the observer.
- We assume, observer nodes are connected with the interoperable blockchain network in a peer-to-peer way.
- Deployment of more observer nodes are costly. Thus, we require to use as few observer nodes as possible. If we choose only one observer node, it can collude with the user. If we use two observer nodes, they can collude together. Thus, we require minimum three observers.
- Anyone from outside or inside the blockchain network can participate as the trustee, as long as they hold sufficient money on both the interoperating blockchains.
- We have demonstrated the attacker model and proposed disincentivization scheme considering only two blockchains requiring interoperability to preserve the simplicity in demonstration. However, our proposal is applicable for any number of blockchains.
- Scalability of our proposed approach can be improved by increasing the number of trustee. However, the measure to achieve the same is out of scope of this paper, and it is considered for future work.
- We consider the cross-blockchain transactions with the same architecture (e.g. Ethereum and Ethereum). However, it will be one interesting future direction to investigate the applicability of our proposal on cross-blockchains with different architectures.

Future Work. Additional future work includes: (i) analyzing the behavior of irrational observer, and its consequence on double spend detection, (ii) analyzing the behavior of dishonest trustee, and (iii) investigating the applicability of the proposed disincentivization mechanism on interoperable blockchain without requiring trusted intermediatory.

VII. Conclusion

We present disincentivization mechanism to prevent double spend attack across interoperable blockchains. With rigorous game theoretic analysis, we claim that rational observer remain true to the purpose of interoperation, provided the seven analyzed monetary conditions are satisfied during the determination of incentives amount. Additionally, utilizing Ethereum's smart-contract feature, we demonstrate cost-effectiveness of our proposal.

Acknowledgement

We thank Diptesh Majumdar, J. Stephanie Rose, and all the anonymous reviewers for their constructive feedback, and Prof. Balaji Palanisamy for discussing blockchains.

References

[1] Crosby, Michael, et al. "Blockchain technology: Beyond bitcoin." Applied Innovation 2.6-10 (2016): 71.

[2] IBM Blockchain. "IBM Food Trust. A new era for the world's food supply". URL: https://www.ibm.com/blockchain/solutions/food-trust. Accessed: 31st August, 2019.

[3] Walmart. "From farm to blockchain: Walmart tracks its lettuce". URL: https://www.nytimes.com/2018/09/24/business/walmart-blockchain-lettuce.html. Accessed: 31st August, 2019.

[4] Forbes. "What can blockchain really do for the food industry". URL: https://www.forbes.com/sites/jennysplitter/2018/09/30/what-can-blockchain-really-do-for-the-food-industry/#523429b488ef. Accessed: 31st August, 2019.

[5] Stephen O'Neal. "Blockchain for food, how the industry makes use of the technology". URL: https://cointelegraph.com/news/blockchain-for-the-food-how-industry-makes-use-of-the-technology. Accessed: 1st September, 2019.

[6] Chris Copenhaver and Ken Reiff. "How blockchain can change the food industry". URL: https://www.fooddive.com/news/how-blockchain-can-change-the-food-industry/551658/. Accessed: 1st September, 2019.

[7] Ameer Rosic. "17 Blockchain Applications That Are Transforming Society". URL: https://blockgeeks.com/guides/blockchain-applications/. Accessed: 1st September, 2019.

[8] Nolan Bauerle. "What Are the Applications and Use Cases of Blockchains?". URL: https://www.coindesk.com/information/applications-use-cases-blockchains. Accessed: 1st September, 2019.

[9] Sean Williams. "20 Real-World Uses for Blockchain Technology". URL: https://www.fool.com/investing/2018/04/11/20-real-world-uses-for-blockchain-technology.aspx. Accessed: 1st September, 2019.

[10] Mohsin Jameel. "Know about 10 Most Interesting Real-world Applications of Blockchain Technology Beyond Cryptocurrency by Mohsin Jameel". URL: https://cryptodigestnews.com/know-about-10-most-interesting-real-world-applications-of-blockchain-technology-beyond-b9112158d0c9. Accessed: 1st September, 2019.

[11] Research Briefs. "Banking Is Only The Beginning: 55 Big Industries Blockchain Could Transform". URL: https://www.cbinsights.com/research/industries-disrupted-blockchain/. Accessed: 1st September, 2019.

[12] Wood, Gavin. "Polkadot: Vision for a heterogeneous multi-chain framework." White Paper (2016).

[13] Aion. URL: https://aion.network/. Accessed: 12th February, 2019.

[14] Corda-Interoperability. URL: https://medium.com/corda/tagged/interoperability. Accessed: 12th February, 2019.

[15] Joshua. "The Supply Chain Industry doesn't need Private Blockchains, it needs Interoperability". URL: https://hackernoon.com/the-supply-chain-industry-doesnt-need-private-blockchains-it-needs-interoperability-v21yq3xg9. Accessed: 1st September, 2019.

[16] Tom Zilavy. "What Is A Hybrid Blockchain And Why You Need To Know About It?". URL: https://medium.com/altcoin-magazine/what-is-a-hybrid-blockchain-and-why-you-need-to-know-about-it-c7b887d2bae. Accessed: 1st September, 2019.

[17] Atul Khekade. "If you Thought Blockchain was Amazing, Wait till You Read about Hybrid Blockchain". URL: https://www.entrepreneur.com/article/307794. Accessed: 1st September, 2019.

[18] Yoav Vilner. "The (Relatively) Growing Ecosystem Of Hybrid Blockchain Game Developers". URL: https://www.forbes.com/sites/yoavvilner/2019/04/25/the-promise-and-hurdles-of-hybrid-blockchain-game-development/#696a83a571e7. Accessed: 1st September, 2019.

[19] Nitish Singh. "Hybrid Blockchain- The Best Of Both Worlds". URL: https://101blockchains.com/hybrid-blockchain/. Accessed: 1st September, 2019.

[20] Kan, Luo, et al. "A multiple blockchains architecture on inter-blockchain communication." 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE, 2018.

[21] Lerner, S. Demian. "Rootstock: Bitcoin powered smart contracts." (2015).

[22] Poa bridge. URL: https://github.com/poanetwork/poa-bridge. Accessed: 26th June, 2019

[23] Dilley, Johnny, et al. "Strong federations: An interoperable blockchain solution to centralized third-party risks." arXiv preprint arXiv:1612.05491 (2016).

[24] Moore, Tyler, and Nicolas Christin. "Beware the middleman: Empirical analysis of Bitcoin-exchange risk." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013.

[25] Mt.gox. URL: https://www.mtgox.com/. Accessed: 26th June, 2019

[26] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[27] Clem Chambers. "Decentralized Cryptocurrencies Are The Future". URL: https://www.forbes.com/sites/investor/2018/09/06/decentralized-cryptocurrencies-are-the-future/#2dec9fe735b1. Accessed: 1st September, 2019.

[28] Prableen Bajpai. "The 10 Most Important Cryptocurrencies Other Than Bitcoin". URL: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/. Accessed: 1st September, 2019.

[29] Karame, Ghassan O., Elli Androulaki, and Srdjan Capkun. "Double-spending fast payments in bitcoin." Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012.

[30] Bamert, Tobias, et al. "Have a snack, pay with Bitcoins." Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on. IEEE, 2013.

[31] Karame, Ghassan O., et al. "Misbehavior in bitcoin: A study of double-spending and accountability." ACM Transactions on Information and System Security (TISSEC) 18.1 (2015): 2.

[32] Rosenfeld, Meni. "Analysis of hashrate-based double spending." arXiv preprint arXiv:1402.2009 (2014).

[33] Karame, Ghassan, Elli Androulaki, and Srdjan Capkun. "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin." IACR Cryptology ePrint Archive 2012.248 (2012).

[34] John P. Podolanko et al. "Countering Double-Spend Attacks on Bitcoin Fast-Pay Transactions". URL: http://www.ieee-security.org/TC/SPW2017/ConPro/papers/podolanko-conpro17.pdf. Accessed: 1st September, 2019.

[35] Coinbase. URL: https://cointelegraph.com/news/coinbase-ethereum-classic-double-spending-involved-more-than-11-million-in-crypto. Accessed: 14th April, 2019.

[36] Atzei, Nicola, Massimo Bartoletti, and Tiziana Cimoli. "A survey of attacks on Ethereum smart contracts." IACR Cryptology ePrint Archive 2016 (2016): 1007.

[37] Baldwin, Clare, and H. Poon. "Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong." Reuters. URL: http://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10E0KP(2016). Accessed: 16th January 2017.

[38] Pagliery, J. "Another bitcoin exchange goes down." CNN Tech. Accessed: 26th June, 2019.

[39] Jason Wu. "Basics of Second Generation Blockchain and its Applications in Capital Market". URL: https://medium.com/datadriveninvestor/basics-of-second-generation-blockchain-and-its-applications-in-capital-market-244f75ce72ff. Accessed: 8th September, 2019.

[40] Buterin, Vitalik. "A next-generation smart contract and decentralized application platform." white paper (2014).

[41] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151 (2014): 1-32.

[42] Osborne, Martin J., and Ariel Rubinstein. A course in game theory. MIT press, 1994.

[43] Krsul, Ivan V., J. Craig Mudge, and Alan J. Demers. "Method of electronic payments that prevents double-spending." U.S. Patent No. 5,839,119. 17 Nov. 1998.

[44] Pointcheval, David, and Jacques Stern. "Security arguments for digital signatures and blind signatures." Journal of cryptology 13.3 (2000): 361-396.

[45] Everaere, Patricia, Isabelle Simplot-Ryl, and Issa Traor. "Double spending protection for e-cash based on risk management." International Conference on Information Security. Springer, Berlin, Heidelberg, 2010.

[46] Lee, Hyun Ju, Mun Suk Choi, and Chung Sei Rhee. "Traceability of double spending in secure electronic cash system." 2003 International Conference on Computer Networks and Mobile Computing, 2003. ICCNMC 2003.. IEEE, 2003.

[47] Hoepman, Jaap-Henk. "Distributed double spending prevention." International Workshop on Security Protocols. Springer, Berlin, Heidelberg, 2007.

[48] Osipkov, Ivan, et al. "Combating double-spending using cooperative P2P systems." 27th International Conference on Distributed Computing Systems (ICDCS'07). IEEE, 2007.

[49] Zamyatin, Alexei, et al. "XCLAIM: Trustless, Interoperable, Cryptocurrency-Backed Assets."

[50] Hardjono, Thomas, Alexander Lipton, and Alex Pentland. "Towards a design philosophy for interoperable blockchain systems." arXiv preprint arXiv:1805.05934 (2018).

[51] Back, Adam, et al. "Enabling blockchain innovations with pegged sidechains." URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains (2014): 72.

[52] Chen, Zhi-dong, et al. "Inter-blockchain communication." DEStech Transactions on Computer Science and Engineering cst (2017).

[53] Barima, Oliver. "Leveraging the blockchain technology to improve construction value delivery: the opportunities, benefits and challenges." Construction Projects (2017): 93-112.

[54] Hardjono, Thomas, Alexander Lipton, and Alex Pentland. "Towards a design philosophy for interoperable blockchain systems." arXiv preprint arXiv:1805.05934 (2018).

[55] Borkowski, M., et al. "Towards Atomic Cross-Chain Token Transfers: State of the Art and Open Questions within TAST. 2018." URL: http://dsg. tuwien. ac. at/staff/mborkowski/pub/tast/tastwhite-paper-1. pdf. White Paper, Technische Universitt Wien. Version 1.

[56] Frauenthaler, Philipp, et al. "Towards Efficient Cross-Blockchain Token Transfers."

[57] Borkowski, Michael, et al. "Cross-Blockchain Technologies: Review, State of the Art, and Outlook."

[58] Borkowski, Michael, et al. "DeXTT: Deterministic Cross-Blockchain Token Transfers." arXiv preprint arXiv:1905.06204 (2019).

[59] Koensa, T., and E. Polla. "Assessing Interoperability Solutions for Distributed Ledgers Extended version."

[60] Sai, Kuheli, and David Tipper. "Poster: Towards Attack Resilient Interoperable Hybrid Blockchain Framework." 2019 IEEE International Symposium on Security and Privacy (S&P).

[61] Remix browser. URL: https://remix.ethereum.org/. Accessed: 1st September, 2019.

[62] Remix browser wiki page. URL: https://theethereum.wiki/w/index.php/Remix. Accessed: 1st September, 2019.

[63] Meta mask: URL: https://metamask.io/. Accessed: 1st September, 2019.

[64] Ether. URL: https://www.coindesk.com/information/what-is-ether-ethereum-cryptocurrency. Accessed: 3rd September, 2019.

[65] Faucet kovan network. URL: https://faucet.kovan.network/. Accessed: 1st September, 2019.

[66] Kovan TestNet Network. URL: https://kovan-testnet.github.io/website/. Accessed: 3rd September, 2019.

[67] What is Ethereum Gas? URL: https://blockgeeks.com/guides/ethereum-gas/. Accessed: 1st September, 2019.