# Poster: Towards Attack Resilient Interoperable Hybrid Blockchain Framework

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

***Abstract*—With the inception of Blockchain [1], the cyber world has seen a widespread change. It is believed that Blockchain will bridge the Trust Gap into the digital world. Blockchain's decentralized, distributed ledger creates timestamp on the transaction and maintains a consistent state among all its replicated copy by coming to an agreement via Proof-of-Work. However, allocation of more than 50% of the computing power to a single or a set of attacking nodes is enough to create an inconsistent state. Hence the presence of a single blockchain network is prone to the *centralization of hashing power* [2] due to colluding nodes which might throw out a legitimate transaction and consequently influence the inclusion of a transaction into the ledger maintained by the blockchain network. We are addressing these issues by designing a global blockchain network in which computational power of sets of nodes are divided among two blockchain networks where different components of a single application are deployed onto different networks, mines and stores data separately, and stores the interoperable transaction in both networks. However, there is no secure interoperable feature among different blockchain networks. This leads us to the first major challenge- designing a new protocol for secure interoperability across different blockchain systems. In order to circumvent the problem of centralization of hashing power, our design enforces the following condition- even if colluding nodes of a single blockchain network throws out a legitimate interoperable transaction, user always have the *Proof-of-Presence* of that transaction as long as it is present in other networks. Alongside, in the context of crypto-banking applications, we have demonstrated that the designed secure interoperable protocol obviates *Double Spending* [3] problem across two networks as maintaining honesty to the protocol is more profitable than colluding and spending the same money twice.**

***Keywords*-Blockchain, Interoperable Blockchain, Game Theory, Double Spend Problem, Cryptocurrency, 50% Attack, Centralization**

## I. Motivation & Problem Description

Even though blockchain is tamper-proof in nature, still whether a transaction gets added or discarded is solely dependent on the discretion of the miner nodes which are in charge of block creation. So, allocation of more than 50% of the hashing power to a single or set of attacking nodes enough to destroy the tamper-resistant ability of the overhyped capability of blockchain. In the context of crypto-banking applications, we have approached the stated scenario with a possible solution in which same transaction is deployed onto two blockchains and as long as the transaction is present in either of the networks, user holds the benefit of *proof-of-presence* of the transaction. Underlying assumption is that both networks does not hold majority of the malicious miners. However, this solution approach leads us to find our first major problem- *no interoperation across blockchains*. We have addressed the stated problem by designing an interoperable hybrid blockchain framework which is discussed in the next section.

## II. Interoperable Hybrid Blockchain

**Our design choices.** We have solved the stated problem of *no-interoperation across two networks* by incorporating handful number of *trustee* (trusted nodes) which are in charge of interoperation across two networks. We have made several design decisions which were implemented as services using ethereum's smart-contract [4] feature. Our framework components are- (i) user enrolment service, (ii) trustee enrolment service, (iii) trustee selection service, (iv) insurance money service, (v) interoperable channel, (vi) data integrity checker service and (vii) penalty detector service. Underlying assumption- trustee holds sufficient balance on both networks and they transfer monetary information across two networks. However, this designed framework leads to the first significant challenge- *double spend across two networks*.

**Attacker Model.** Foremost challenge due to the formation of trusted interoperable channel for transferring the monetary information is the notion of double spending same money across networks.

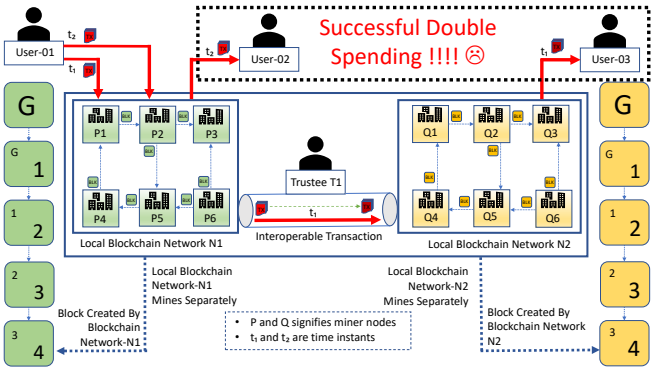


Figure 1: First challenge- double spend across two networks

For example. $N_1$ and $N_2$ are two blockchains connected by an interoperable trusted channel $Ch_{secure}$. Each trustee has two accounts $T_{N_1}$ and $T_{N_2}$ on both the blockchains. Malicious user $A$ holds two accounts (*User-01* and *User-02*) on the same blockchain network $N_1$ (eventhough these account appears as two different users, but they are controlled by the same single entity). Account *User-03* belongs to honest user $H$ on the network $N_2$. Figure-1 demonstrates the situation where *User-01* sends a transaction $TX_1$ to the trustee $T_1$ and afterwards, send the same transaction $TX_1$ to its another account (*User-02*). After processing the money for the second blockchain network, trustee has no way to check for double spending and get its money back. Thus, successful double spending is possible in the designed framework (as shown in figure-1). We have solved the problem of double spend across networks by incorporating three *observers* in each of the networks. These observers are responsible for double spend detection before sending a transaction to the trustee.

## III. Encouraging Rationality

With regards to double spend detection across two networks, we have analyzed the need for incorporating three observers in each

of the participating networks. Pre-signed smart-contract with the trustee makes observers eligible to participate in the framework and consequently, make them eligible for obtaining reward upon successful double spend detection. However, observers can collude and provide wrong response to the trustee. Different cases of collusion in between observers are demonstrated in figure-2.

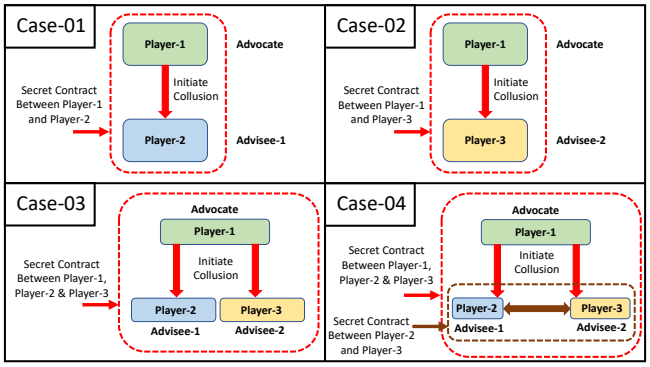


Figure 2: Second challenge- collusion in between observers

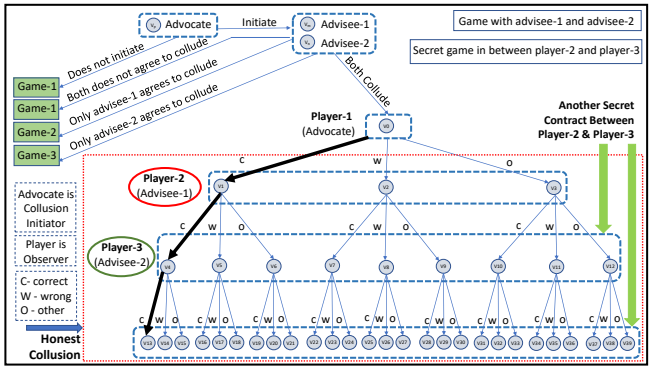


Figure 3: Path following honest computations by all observers reaches equilibrium with enforced policy as stated in Table II

**Monetary policy enforcement.** Monetary variables that need to be enforced in the smart-contract are listed in Table I. With regards to successful double spend detection by the observers, monetary policies need to be enforced in the decentralized smart contract. These enforced constraints are listed in Table II which are obtained from rigorous game theoretic analysis. We have come across these monetary constraints by changing the rewards mechanism to achieve honest behavior from all the participating observers. We have analyzed total 7 games that includes 14 game tables. In figure-3, game-1 leads to honest behavior by all the particpating observers, however it does not consider collusion in between observers. All other games mentioned in the figure-3 leads to collusion as the best strategy. Among all the analyzed games, figure-3 demonstrates the final game played in between all the three observers that leads to the equilibrium i.e. reward mechanism (Table II) obtained from this game encourages all the observers to be honest.

## IV. Discussions and Future Work

We have demonstrated our interoperable hybrid blockchain framework which uses trusted agent for providing the necessary interoperation. Alongside, we have demonstrated attacker model for successful double spend attack across our designed framework. Consequently, we have solved the problem of double spend by incorporating the notion of observer nodes in each of the network and demonstrated a game theoretic analysis which henceforth proves that the *rational* observer remains true to the purpose of interoperation provided a few reasonable assumptions and monetary enforcement are followed. In future, we would like to analyze the behavior of irrational observer and its consequence on interoperation and consequently on the solution to the double spend problem.

| Symbol | Description |
|---|---|
| $c$ | Cost of computation for correct result |
| $d_o$ | Deposit paid by the observer in the contract signed with the trustee |
| $d_t$ | Reward given by the trustee to the observer for providing the correct computation based upon majority rules. |
| $f_a$ | Money deposited in the collusion contract by advocate and all other advisees who agrees to play in terms of collusion. Here $f$ signifies first secret contract and $a$ signifies which is initiated by the advocate. |
| $b_a$ | Bribe given by the dishonest advocate to the colluder so that they take part in collusion. |
| $\mu$ | Reward provided by trustee for honest collusion report. |
| $f_h$ | Money deposited in the honest collusion contract. |
| $b_h$ | Bribe given by the honest player to the other colluder so that they take part in collusion. |
| $r$ | Extra reward provided by trustee for honest computation based upon blockchains data. However, this reward is given to the observer at the discretion of the trustee. |

Table I: Monetary variables for policy enforcement

| Condition | Enforced monetary constraints for encouraging rationality |
|---|---|
| 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 II: Monetary policy enforcement in smart-contract

## References


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

[2] Beikverdi, Alireza, and JooSeok Song. "Trend of centralization in Bitcoin's distributed network." 2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD). IEEE, 2015.

[3] 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.

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

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