Formalizing Cost Fairness for Two-Party Exchange Protocols using Game Theory and Applications to Blockchain (Extended Version)

Matthias Lohr[*], Kenneth Skiba[†], Marco Konersmann[*], Jan Jürjens[*‡], Steffen Staab[§¶]
[*]Institute for Software Technology, University of Koblenz-Landau, Koblenz, Germany
[†]Artificial Intelligence Group, Fernuniversität in Hagen, Hagen, Germany
[‡]Fraunhofer ISST, Dortmund, Germany
[§]Institute for Parallel and Distributed Systems (IPVS), University of Stuttgart, Stuttgart, Germany
[¶]University of Southampton, Southampton, United Kingdom

Abstract—**Existing fair exchange protocols usually neglect consideration of cost when assessing their fairness. However, in an environment with non-negligible transaction cost, e.g., public blockchains, high or unexpected transaction cost might be an obstacle for wide-spread adoption of fair exchange protocols in business applications. For example, as of 2021-12-17, the initialization of the FairSwap protocol on the Ethereum blockchain requires the selling party to pay a fee of approx. 349.20 USD per exchange. We address this issue by defining cost fairness, which can be used to assess two-party exchange protocols including implied transaction cost. We show that in an environment with non-negligible transaction cost where one party has to initialize the exchange protocol and the other party can leave the exchange at any time cost fairness cannot be achieved.**

I. Introduction

In commerce, two or more parties want to exchange goods. According to Asokan [1], an exchange becomes a *fair exchange* iff it is guaranteed that either all involved parties get exactly the good they requested, or no good has been transferred at the end of the exchange [1], [2]. It has been shown that a trusted third party is required to achieve fairness for a two-party exchange [3], [4]. In non-digital exchanges (e.g., buying/selling a house), notaries or banks take on the role of a trusted third party. In electronic commerce, several approaches have been developed that ensure a fair exchange between two parties either utilizing dedicated organizations as trusted third parties or utilizing blockchains (or more general, distributed ledgers) as distributed trusted third party [5], [6], [7], [8], [9].

When a trusted third party is involved in an exchange, it can raise non-negligible transaction cost (e.g., notary fees or fees for a bank guarantee). Such transaction cost must be considered separately from possible payments as part of the exchange, as they are intended to pay the trusted third party for their services rather then being part of the goods (including money) to be exchanged between the participants[1].

When an exchange protocol is used in which a public blockchain (e.g., Ethereum [10]) acts as a trusted third party, all interactions with the trusted third party are performed using *blockchain transactions*, which require the acting party to pay transaction cost in form of *blockchain transaction fees*[2]. For example, the initialization of the FairSwap protocol (deployment of a single-use smart contract for the exchange), which provides functionality to fairly sell data for money on the Ethereum blockchain, requires the selling party to pay for blockchain transaction fees of approx. 1,050,000 Gas[3], which, as of 2021-12-17, is worth approx. 349.20 USD[4]. There exist alternative approaches, such as optimistic protocol design [12] or the usage of state channels [13] that can generally be used to reduce blockchain transaction fees. Nevertheless, even then transaction cost is greater than zero and often non-negligible.

For private blockchains, the existence of transaction cost depends on the selected concepts and implementations decided to be applied. E.g., the Hyperledger Fabric [14] blockchain framework does per default not include any means or features of financial values or currencies. However, also operation of a private blockchain costs money (e.g., for buying the required servers), which can be apportioned to each blockchain transaction sent to the private blockchain instance, or asking for a fixed monthly fee but not charging per blockchain transaction.

So far, all blockchain-based fair exchange protocols known to us only consider the whereabouts of the goods to be exchanged for fairness assessment, while they ignore transaction cost accrued by using the blockchain as trusted third party.

The research reported here was partly supported by the Deutsche Forschungsgemeinschaft under grant KE 1413/11-1.

[1] In this work, we use the terms *transaction* and *transaction cost* generally for interactions with the trusted third party and resulting cost.

[2] Every time we need to refer to concrete type of transaction or transaction cost, e.g., in context of blockchains, we prefix it with the according concretization, such as *blockchain transaction* and *blockchain transaction fee*

[3] As stated by Dziembowski et al. [6]. During our tests with minor bug fixes we observed cost of approx. 1,500,000 Gas. Our version of the smart contract with bug fixes is available online at https://gitlab.com/MatthiasLohr/bdtsim.

[4] As of 2021-12-17, Ethereum block 13,823,842 was created with a base Gas price of approx. 60 GWei/Gas and an exchange rate of approx. 3880 USD/Eth (1 Eth = 10^9 GWei), which results in blockchain transaction fees of approx. 349.20 USD for deployment the smart contract, assuming zero tip [11].

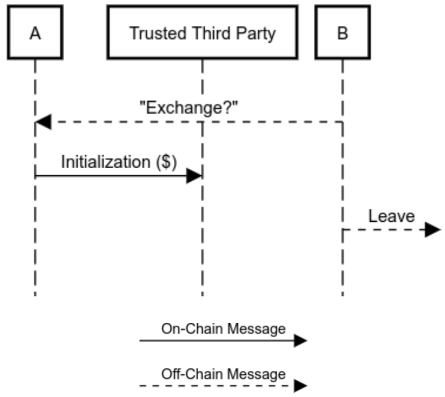

Fig. 1: Diagram of exemplary action sequence for a grieving attack, conducted by B. *Initialization* is an action where A pays fees to the Trusted Third Party in the belief that B will continue the targeted exchange.

This opens the possibility for a *grieving attack* [7] as it is shown in Figure 1, where an unfaithful party B causes a faithful party A to initiate an exchange with a transaction that accrues transaction cost and then leaves without finishing the exchange. Doing so, an attacker can harm the attacked party (e.g., business opponent) with only low or even zero cost for the attacker while the attacked party has to bear possibly non-negligible transaction cost for the initialization. Due to blockchain anonymity[5], the faithful party cannot reliably distinguish between a repeated request from the same unfaithful party or a new party. Even given an exchange that is proven to be fair following the definition by Asokan [1, p. 9f], a faithful party may either accept incoming requests and risk bearing the costs of a grieving attack, or not accept incoming requests at all and thus not complete their planned exchange of goods.

This raises the question of what an exchange protocol has to achieve in order to be fair *and* resilient against grieving attacks. We will introduce a formal definition of *cost fairness* to address the following research questions:

RQ 1 How can two-party exchange protocols be modeled so that transaction cost is taken into account?
RQ 2 How can the fairness of two-party exchange protocols be assessed regarding transaction cost?
RQ 3 How to achieve cost fairness for public blockchain-based two party exchange protocols (e.g., FairSwap)?
RQ 4 How to achieve cost fairness for private blockchain-based two party exchange protocols?

In order to introduce the topic and provide the foundations our work bases on, we describe related work in Section II. Our first contribution, a model for two-party fair exchange protocols, answering RQ 1, is presented in Section III. To answer RQ 2, as our second contribution, we provide a definition for *partial cost fairness* and *full cost fairness* in Section IV. Our third contribution consists of two theorems, presented in Section V, addressing the achievability of partial cost fairness and full cost fairness, especially in the context of blockchains. We discuss our contributions and use these theorems to answer RQ 3 and RQ 4 in Section VI. We summarize our work and conclude in Section VII.

This paper is the extended version of the short paper published by Lohr et al. [16].

II. Related Work

Cost fairness has been informally defined by Lohr et al. [17]. Our work provides a formal underpinning for cost fairness that allows for modeling exchange protocols and for assessing them regarding cost fairness. To this end, we use game theory as a formal framework and apply our model to blockchain-based exchange protocols.

A. Fair Exchange

The term *fair exchange* describes the challenge of two or more parties that want to exchange their own goods with the guarantee that, despite absence of mutual trust, no party can gain advantage over the other parties [2]. In this context, several definitions of fairness have been presented as well as different approaches for designing fair exchange protocols, which claim to ensure a fair exchange (fairness as defined by Asokan [1]) as long as at least one party follows the fair exchange protocol [18], [19], [20], [21], [22], [23], [1]. It has been shown that it is impossible to achieve fair exchange without involving a trusted third party [3], [4]. None of the approaches referenced above considers possible transaction cost of involving a trusted third party in an exchange.

B. Game Theory

In general, game theory deals with making strategic decisions when two or more parties interact with each other. In game theory, the parties are referred to as players, which can choose between and follow different strategies to conduct and finish the interaction in the best way for the individual party by maximizing their payoffs [24].

Game theory already has been applied to the field of fair exchange [25], [26], [2]: A fair exchange can be interpreted as multi-party game, where the fair exchange protocol can be represented by a game tree and the parties (players) involved in the exchange can choose between different strategies (e.g., “behave faithfully” or “cheat”). Buttyán and Hubaux introduced game theory as an approach for a formal framework, which can be used to assess and compare different types of fairness [26]. While their model can be used to assess fairness of exchange protocols, it lacks the ability to assess other aspects of an exchange protocol such as the cost of involving a trusted third party.

For our work, we adopt and modify the general idea of Buttyán and Hubaux of modeling an exchange protocol using game theory to consider the values of the items to be exchanged as well as the transaction cost, which may arise during an exchange, furthermore additional expenses or revenues such as security deposits, paying or receiving a compensation.

[5] It has been shown by, e.g., Biryukov and Tikhomirov that there exist several but unreliable methods for identity deanonymization on blockchains such as Bitcoin [15]. We assume that deanonymization might not be sufficiently reliable to prevent grieving attacks.

C. Blockchain

A blockchain is an append-only data structure reflecting a state (e.g., bank account balances, variable values), where each state update is collected into a so-called block, which gets appended to the existing data structure. All modifications to the data can be verified against a set of rules for allowed modifications and no single entity can prevent or enforce something related to the data without the support of the majority of blockchain participants [27]. Further research and development has extended the concept to support Turing-complete programs for formalizing modification rules, usually referred to as *smart contracts*, e.g., in context of the Ethereum blockchain [10]. Ethereum smart contracts are computer programs, whose source code is added as bytecode to the blockchain data. This way, everybody who downloads the Ethereum data can execute the program and verify the results submitted to the network by other participants[6].

Several approaches implement a trusted third party for fair exchange using Ethereum smart contracts [6], [9], [7]. This is usually done by providing a proof of successful transfer or a proof of misbehavior to the smart contract implementing the trusted third party, who will either forward or pay back the payment if the proof can be verified. Typically, blockchain-based fair exchange protocols are designed to conduct an exchange of data for money, usually in form of a blockchain-specific financial equivalent, which is often referred to as crypto-currency. Alternatively, also non-fungible tokens could be exchanged, such as digital ownership representations of physical objects (e.g., house, car).

III. Modeling Exchange Protocols using Game Theory

In this section, we present our model of an exchange protocol using game theory, building upon the work of Buttyán and Hubaux [26].

A. Extensive Game

We will build on the notion of an *extensive game*, which can be formalized using as follows:

A *game tree* [24], [28] (see Figure 2 for an example) is a tree that depicts all possible ways to play a game.

Definition III.1 (Game Tree [24])**.** *A* game tree $T = (V, E, \mathcal{P}, o, \vec{p})$ *is a directed tree with a set of vertices* V *with root* $v_0 \in V$*, a set of edges* $E \subseteq V \times V$ *called moves, a set of* n *players* $\mathcal{P}$*, a labeling function* $o : V \to \mathcal{P}$*, which labels each non-terminal vertex* $v \in V$ *with a player* $P \in \mathcal{P}$ *to* own v *and a labeling function* $\vec{p}(v) = (p_{P_1}, ..., p_{P_n})$*, which labels each terminal vertex* $v \in V$ *with an* n*-tuple of numbers called* payoff*, which defines the individual payoff for each player* P_i*.*

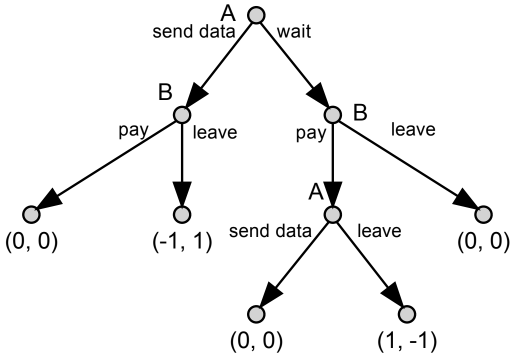

Fig. 2: Example of a game tree with players A and B exchanging data for money with different orders of payment and data transfer.

Each vertex v represents a possible state of the game to which T belongs. Being in a state that is represented by $v \in V$, player $P = o(v)$, $P \in \mathcal{P}$ is responsible to choose the next move, represented by $e = (v, v')$, $e \in E, v' \in V$, leading to a new state v'.

The behavior of players resulting in the selection of the next move in an extensive game is described by a *strategy*. For simplicity reasons, we only provide a basic definition of a strategy, which covers the aspects required for our work. For a detailed and more formal definition of strategy we refer to Morris [24].

Definition III.2 (Strategy)**.** *A* strategy S *for player* P *is represented by a partial function called* choice function $c_P : V \to V$*, which for each* $v \in V : o(v) = P$ *returns a child* v' *of* v *with* $(v, v') \in E$ *being the next move chosen by* P *following strategy* S*.*

The set of all available strategies to a player is called *strategy set*:

Definition III.3 (Strategy Set [24])**.** *For player* P *a* strategy set $\Sigma = \{S_1, ..., S_m\}$ *is the set of all possible strategies of* P*.*

Using the previously defined terms, we can now define an extensive game:

Definition III.4 (Extensive Game [24])**.** *An* extensive game *is defined as* $\Gamma = (T, \mathcal{P}, \{\Sigma_{P_1}, ..., \Sigma_{P_n}\})$ *with game tree* T*, set of players* $\mathcal{P} = \{P_1, ..., P_n\}$ *and their strategy sets* $\Sigma_{P_1}, ..., \Sigma_{P_n}$*.*

B. Moves of an Extensive Game

Using the terms defined in Section III-A, we introduce our model of an exchange protocol based on game theory. For simplicity reasons, we only consider two-party exchange protocols and postpone the expansion to n-party exchange protocols to future work. Similar to Buttyán and Hubaux [26], we do not consider the trusted third party to be in the set of players, since we assume that it always behaves deterministically according to the protocol and will never act on its own, only at the instigation of a player.

[6] Despite theoretically possible, not every node connected to the Ethereum network does this kind of verification. It is up to the node's administrator to decide if he is willing to invest the computational power and therefore has to pay for the required energy to support the blockchain by enabling the verification mechanisms. Alternatively, a node will accept all blocks of the longest chain of blocks.

We assume a two-party exchange with parties $\mathcal{P} = \{A, B\}$ who are interested to exchange their items ι_A and ι_B. We assume that A and B agreed on using the exchange protocol $\mathcal{X}$ (we will provide the formal definition of an exchange protocol in Definition III.7), but neither A nor B can technically be coerced to follow $\mathcal{X}$ during the exchange. In order to conduct the exchange, A and B can choose their strategies S_A and S_B from their strategy sets Σ_A and Σ_B. We denote the set of conducted moves of A with E_A and the set of conducted moves of B with E_B.

Each move can impact the state of the exchange, e.g., a payment can be conducted or the item (or parts of it, if the item is divisible, e.g., in context of gradual release [18]) can be handed over between the parties. We reflect these state changes by a tuple of attributes, which represent the move's effects on the ongoing exchange:

Definition III.5 (Move Attributes). *Let $e \in E$ be an edge in a game tree T of an extensive game Γ. Let $\mathcal{P} = \{A, B\}$ be the set of players in Γ. Let, w.l.o.g., A be the player conducting e. We define a tuple $a(e) = (\overrightarrow{\rho_e}, cost_e, deposit_e, \overrightarrow{comp_e})$ to be the* move attributes *of e, where $\overrightarrow{\rho_e} = (\rho_e^A, \rho_e^B)$ is a vector of shares of the item transferred to A and B during e with $0 \le \rho_e^P \le 1$, $P \in \mathcal{P}$, $cost_e \ge 0$ is the transaction cost that has to be paid by A to the trusted third party for conducting e, $deposit_e \in \mathbb{R}$ are the funds deposited or retracted by A conducting e and $\overrightarrow{comp_e} = (comp_e^A, comp_e^B)$ with $comp_e^P$, $P \in \mathcal{P}$ is a vector of the compensations paid out to player P in this move e.*

The *item share* ρ_e^A refers to the portion of the item ι_B, which is released to A in move e. Indivisible items such as a valuable painting can only be transferred in one piece, in which case $\rho_e^A \in \{0, 1\}$. Divisible items such as money or data can also be transferred in steps, in which case $0 \le \rho_e^A \le 1$. Note that A may do a move e that releases an item share ρ_e^B to B. The same move e may also trigger that another item share ρ_e^A is released to A himself.

The *transaction cost*, denoted with $cost_e$, describes the fees the party conducting move e has to pay to the trusted third party for conducting move e.

In order to enable the trusted third party to punish an unfaithfully behaving party and to compensate a faithfully behaving party, an exchange protocol can require to make a *deposit*, which is managed by the trusted third party. The total amount of deposit is tracked per party. A party can change its total deposit in a move e by amount $deposit_e$ ($deposit_e > 0$ for depositing, $deposit_e < 0$ for retracting and $deposit_e = 0$ for not changing the total amount of the party conducting move e).

If B behaves unfaithfully, an exchange protocol can be designed to compensate A. $comp_e^A$ denotes the compensation paid to A by the trusted third party in move e.

Usually, a trusted third party does not use its own money to pay out compensations. Instead, the compensation paid out (e.g., to a faithful party) is taken from deposits made before (e.g., from the unfaithful party). Additionally, for our work we assume the environment, in which the exchange protocol is running, to be a financially closed system. Therefore, the amount of total compensation paid out can never exceed the total amount of deposits not retracted at the end of the exchange, considering the conducted moves of all players $P_i \in \mathcal{P}$, where $\mathcal{P} = \{A, B\}$:

$$\sum_{P_i \in \mathcal{P}} \Bigg(\sum_{e \in E_{P_i}} \big(deposit_e - \sum_{P_j \in \mathcal{P}} comp_e^{P_j} \big) \Bigg) \ge 0 \qquad (1)$$

Note that a move e conducted by A can cause compensations payouts to A as well as to B.

In an exchange of a good for a monetary payment both, the good and the monetary payment, are modeled as items ι_{good} and ι_{money} of the exchange protocol. Both goods and money can temporarily be owned by the trusted third party acting as escrow, but only if the good or the money becomes available for the requesting party this is reflected by an item share $\rho > 0$. E.g., in an exchange using a blockchain-based trusted third party, sending money to the trusted third party does not make it available to one of the parties (therefore $\rho = 0$) while sending unencrypted data to the trusted third party will make it available to everyone (because of the public readability of a blockchain), including the requesting party, therefore $\rho > 0$.

Example III.1 (Move Attributes). *We assume an extensive game with two players A and B. We assume that A is the party conducting the move e. We give three different examples:*

- *$a(e) = ((0, 1), 50, 0, (0, 0))$ – The move of A makes the item fully available to B, charged by the trusted third party with transaction cost $cost_e = 50$.*
- *$a(e) = ((0.5, 0), 0, 100, (0, 0))$ – The move of A reveals half of B's item to A. A deposits an amount of 100 to the trusted third party that could be used as payment for B in later moves.*
- *$a(e) = ((0, 0), 0, -100, (150, 0))$ – A withdraws 100 from the funds A deposited with the trusted third party. This is only possible if more than 100 have been deposited by A before and were not used for paying or compensating B. Additionally, A retrieves 150 as payment or compensation from the funds deposited by B.*

Even if A and B have agreed on using an exchange protocol $\mathcal{X}$ for their exchange, they usually cannot technically be coerced to conduct a specific move $e \in E$ of $\mathcal{X}$. Therefore, an exchange protocol $\mathcal{X}$ needs to differentiate between *possible* and *allowed* moves. In our model, a game tree $T = (V, E, \mathcal{P}, o, \overrightarrow{p})$ contains all *possible* moves $e \in E$ for players $P \in \mathcal{P}$. We label moves *allowed* by an exchange protocol $\mathcal{X}$ to be faithful and all other moves to be unfaithful using the following function:

Definition III.6 (Faithfulness). *Let $e = (v, v') \in E$ be an edge in a game tree T, $v \in V$ be the parent and $v' \in V$ one of its child nodes. We define a total function $faithful?$: $E \to \{faithful, unfaithful\}$ that returns for each move e if e*

is considered to be faithful or unfaithful behavior of player $A = o(v)$.

Using the definitions presented before, we can now formally define an *exchange protocol* to be a tuple of an extensive game Γ, a function $a(e)$ that returns move attributes for each move of the game tree of Γ and a function $\mathit{faithful?}(e)$ that labels moves to be faithful or unfaithful behavior according to the exchange protocol:

Definition III.7 (Exchange Protocol)**.** *We define an* exchange protocol $\mathcal{X} = (\Gamma, a, \mathit{faithful?})$ *as an extensive game* Γ *together with a function* $a(e)$ *for retrieving move attributes and a function for determining the faithfulness of a move* $\mathit{faithful?}(e)$, $e \in E$ *of the game tree of* Γ.

An exchange protocol $\mathcal{X}$ is called *fair exchange protocol* iff it achieves fairness according to Asokan, who request that in order to achieve fairness, either both parties have to get what they wanted or nobody got anything valuable at the end of the exchange [1].

For an exchange protocol $\mathcal{X} = (\Gamma, a, \mathit{faithful?})$, using $\mathit{faithful?}(e)$, $e \in E$ we can classify all available strategies in Γ regarding their faithfulness:

Definition III.8 (Faithful and Unfaithful Strategies and Strategy Sets)**.** *Let* $\mathcal{X} = (\Gamma, a, \mathit{faithful?})$ *be an exchange protocol. We define a strategy* S_A^* *to be a* faithful strategy *of A, if for all possible moves* $e = (v, v')$ *defined by its choice function* $v' = c_A(v)$ *it holds that* $\mathit{faithful?}(e) = \mathit{faithful}$. *We define a strategy* $S_A^\diamond$ *to be an* unfaithful strategy *of A, if it is not a faithful strategy of A. We define the* faithful strategy set Σ_A^* *of A as the set of all faithful strategies of A. We define the* unfaithful strategy set $\Sigma_A^\diamond$ *of A with* $\Sigma_A^\diamond = \Sigma_A \setminus \Sigma_A^*$ *as the set of all unfaithful strategies of A.*

As introduced in Definition III.1, the quality of a chosen strategy is expressed using its *payoff*. In an exchange between A and B, the payoff for A is everything A received (such as the received shares of ι_B and received compensations) minus everything A had to give away (such as shares of ι_A, the cost for conducting the exchange, and compensations paid to B). In order to consider the values of the shares of ι_A and ι_B for the payoff, we need to introduce a value function that returns the values of the shares of ι_A and ι_B in the same unit as the cost or compensation. However, A and B may have different valuations of the same item ι and shares of it, therefore A and B each have their own *value function*:

Definition III.9 (Value Function, Valuation)**.** *Given a party A and a share* ρ *of an item* ι, *the* value function $v_A(\iota, \rho)$ *returns the* valuation *of A regarding the possession of a share of* ρ *of* ι, $0 \leq \rho \leq 1$.

In a game, the payoff for a player A depends on the strategies chosen by all players of the game:

Definition III.10 (Payoff Function)**.** *Let* $\mathcal{X} = (\Gamma, a, \mathit{faithful?})$ *be an exchange protocol with players A and B and let* S_A *and* S_B *be their selected strategies. Let* $c_A(v)$ *be the choice function defined by* S_A *and* $c_B(v)$ *be the choice function defined by* S_B. *Let* E_A *and* E_B *be the conducted moves of A and B and* v_t *be the terminal node after the moves have been conducted. Let* $a(e) = (\overrightarrow{\rho_e}, cost_e, deposit_e, \overrightarrow{comp_e})$ *be the move attributes of an edge e. We define the payoff function* $\vec{p}(S_A, S_B)$ *such that it labels a terminal vertex* v_t *in* $\mathcal{X}$ *with the payoffs* p_A, p_B *for A and B as follows:*

$$
\begin{aligned}
&(p_A, p_B) = \vec{p}(S_A, S_B) = \vec{p}(v_t) = \\
&\Bigg(v_A(\iota_B, \sum_{e \in E_A \cup E_B} \rho_e^A) - v_A(\iota_A, \sum_{e \in E_A \cup E_B} \rho_e^B) \\
&\quad + \sum_{e \in E_A} (comp_e^A - deposit_e - cost_e) + \sum_{e \in E_B} comp_e^A \ , \\
&v_B(\iota_A, \sum_{e \in E_A \cup E_B} \rho_e^B) - v_B(\iota_B, \sum_{e \in E_A \cup E_B} \rho_e^A) \\
&\quad + \sum_{e \in E_B} (comp_e^B - deposit_e - cost_e) + \sum_{e \in E_A} comp_e^B \Bigg)
\end{aligned}
$$

Given two strategies S_A and S_B, the payoff function $\vec{p}(S_A, S_B) = (p_A, p_B)$ returns the payoff p_A for A for participating in the exchange as well as the payoff p_B for B. The payoff for each player (w.l.o.g. using A as example for now) is calculated by summing up the difference of the value $v_A(\iota_B, \rho_e^B)$ of the item shares received minus the value $v_A(\iota_A, \rho_e^A)$ of the item shares given away (see Definition III.9), plus compensations $\sum_{e \in E_A} comp_e^A$ received as a result of moves conducted by A, minus deposits $\sum_{e \in E_A} deposit_e$ made or retracted by A minus the cost $\sum_{e \in E_A} cost_e$ A has to pay for, plus compensations $\sum_{e \in E_B} comp_e^A$ received by A as a result of moves conducted by B.

The payoff can be interpreted as financial benefit (or loss) a player experiences participating in an exchange.

If the technical environment cannot force the parties to conduct a next move, a party may leave an exchange at any time. In this case, it is also not possible to forcefully withdraw money from the leaving party and send it to the faithful party as compensation. For example, in a blockchain environment, no party can be forced to create new transactions, and withdrawing money from its wallet inevitably requires collaboration. Since leaving the protocol is not indicated by an explicit action of a party, it has to be assumed by the exchange protocol after a previously defined timeout. We model the possibility of such an unfaithful leave of an exchange protocol $\mathcal{X}$ with an edge e_{leave} in its game tree T:

Definition III.11 (Unfaithful Leave)**.** *Let* $e_{leave} \in E$ *represent an unfaithful leave, then*

- $a(e_{leave}) = (\vec{0}, 0, 0, \vec{0})$
- $faithful?(e_{leave}) = unfaithful$

Definition III.12 (Unfaithful Leave At Any Time)**.** *An exchange protocol* $\mathcal{X}$ *allows A to* unfaithfully leave at any time*, if for each strategy* $S_A \in \Sigma_A$ *with* $E_A = (e_1, ..., e_n)$ *all strategies* S_A^i *with* $E_A^i = (e_1, ..., e_i, e_{leave}), 1 \leq i \leq n$ *it holds:* $S_A^i \in \Sigma_A^\diamond$ *and also* $E_A^0 = (e_{leave}) \in \Sigma_A^\diamond$.

Example III.2 (Environment without Unfaithful Leave)**.** *Assuming a situation in which a shoplifter B can decide to buy or to steal, but if he steals he will definitely be caught by the police. When getting caught, he can decide to confess or not to confess, but he cannot leave the police station until he decides either to confess or not to confess. This results in a faithful strategy S_B^f with $E_B = (e_{pay})$ and unfaithful strategies S_B^{u1} with $E_B = (e_{steal}, e_{confess})$ and S_B^{u2} with $E_B = (e_{steal}, e_{notconfess})$. A strategy S_B^{u3} with $E_B = (e_{steal}, e_{leave})$, in which B leaves the protocol after stealing without the decision of confession is not allowed by the environment and therefore $S_B^{u3} \notin \Sigma_B$.*

Depending on the environment in which an exchange protocol is used, suffering transaction cost might be inevitable. If transaction cost is non-negligible, we call the exchange protocol to be in an *environment with non-negligible transaction cost*:

Definition III.13 (Environment with non-negligible transaction cost)**.** *Given an exchange protocol $\mathcal{X}$ represented by game tree $T = (V, E, \mathcal{P}, o, \overrightarrow{p})$. We define $\mathcal{X}$ to be in an* environment with non-negligible transaction cost *if for all $e \in E \setminus e_{leave}$ with $a(e) = (\overrightarrow{\rho_e}, cost_e, deposit_e, \overrightarrow{comp_e})$: $cost_e > 0$.*

IV. Cost Fairness

Cost fairness has already been informally defined by Lohr et al. [17]. Using the model for exchange protocols described in Section III, we present a formal definition of two notions of cost fairness. *Partial cost fairness* provides a guarantee of cost fairness to one of the two parties involved in the exchange while *full cost fairness* provides the guarantee to both parties.

If an exchange protocol $\mathcal{X}$ achieves partial cost fairness in favor of A, it will provide the guarantee that regardless whether an actual exchange of items took place the possible benefit (or loss) induced by the exchanged items minus potential cost plus potential compensations received will not lead to a loss for A in total.

Definition IV.1 (Partial Cost Fairness)**.** *A two-party exchange protocol $\mathcal{X}$ with players A and B achieves* Partial Cost Fairness *in favor of A iff for any strategy $S_B \in \Sigma_B$ for B there exists at least one strategy $S_A \in \Sigma_A^*$ for A such that for $\overrightarrow{p}(S_A, S_B) = (p_A, p_B)$ it holds $p_A \geq 0$.*

Applying the definition of partial cost fairness in favor of both parties, A and B, an exchange protocol achieves full cost fairness:

Definition IV.2 (Full Cost Fairness)**.** *A two party exchange protocol $\mathcal{X}$ with players A and B achieves* Full Cost Fairness *iff*

- *$\mathcal{X}$ achieves Partial Cost Fairness in favor of A and*
- *$\mathcal{X}$ achieves Partial Cost Fairness in favor of B.*

Using Definition IV.1 and Definition IV.2, two-party exchange protocols modeled as described in Section III can be assessed regarding cost fairness as it has been asked for in RQ 2.

V. Achievability of Cost Fairness

If w.l.o.g., B cannot leave the exchange protocol without the approval of the trusted third party due to environmental constraints, an exchange protocol could be designed in such a way that B can only leave the exchange protocol if B compensated A for the transaction cost in case that A was behaving faithfully while B was behaving unfaithfully. This way, an exchange protocol can be designed to always guarantee cost fairness.

Theorem V.1. *Given a two-party exchange protocol $\mathcal{X}$ with parties A and B in an environment with non-negligible transaction cost. If A initializes the exchange protocol and B can unfaithfully leave at any time, it is not possible to achieve partial cost fairness in favor or A.*

Proof by Contradiction. We assume that A initializes $\mathcal{X}$ and B can unfaithfully leave at any time. We assume that partial cost fairness in favor of A can be achieved, therefore, according to Definition IV.1, for any strategy S_B chosen by B, there must exist a strategy S_A for A with $\overrightarrow{p}(S_A, S_B) = (p_A, p_B)$ where the payoff of A $p_A \geq 0$. Since B can leave $\mathcal{X}$ unfaithfully at any time, B can choose a strategy S'_B such that $E_B = (e_{leave})$. According to Definition IV.1 and Definition III.10, there has to be a strategy S'_A for A such that

$$p_A = v_A(\iota_B, \sum_{e \in E_A \cup E_B} \rho_e^B) - v_A(\iota_A, \sum_{e \in E_A \cup E_B} \rho_e^A) + \sum_{e \in E_A} (comp_e^A - deposit_e - cost_e) + \sum_{e \in E_B} comp_e^A \geq 0$$

Since the only move of B is e_{leave}, B did not share anything to A, therefore $v_A(\iota_B, \sum_{e \in E_A \cup E_B} \rho_e^B) = 0$. Since $\mathcal{X}$ is a fair exchange protocol, also A did not share anything to B, so $v_A(\iota_A, \sum_{e \in E_A \cup E_B} \rho_e^A) = 0$. Furthermore, S'_B does not contain any moves causing compensation payouts to A, therefore $\sum_{e \in E_B} comp_e^A = 0$. It remains to show that

$$\sum_{e \in E_A} (comp_e^A - deposit_e - cost_e) \geq 0 \qquad (2)$$

Since $\mathcal{X}$ is assumed to be in an environment with non-negligible transaction cost and A initialized $\mathcal{X}$ with a move $e \neq e_{leave}$, we know that $\sum_{e \in E_A} cost_e > 0$. Since the only move in S'_B is e_{leave} with $a(e) = (\overrightarrow{0}, 0, 0, \overrightarrow{0})$, therefore, in Equation 1, $\sum_{e \in E_B} \big(deposit_e - \sum_{P \in \mathcal{P}} comp_e^P\big) = 0$. Therefore, according to Equation 1, it has to hold that $\sum_{e \in E_A} \big(deposit_e - \sum_{P \in \mathcal{P}} comp_e^P\big) \geq 0$. Hence Equation 2 can never be satisfied. Therefore, for a strategy S'_B with $E_B = (e_{leave})$ there does not exist such a strategy S'_A such that for $\overrightarrow{p}(S_A, S_B) = (p_A, p_B)$ it holds that $p_A \geq 0$, which is a contradiction to the assumption that partial cost fairness can be achieved. □

Theorem V.2. *Given a two-party fair exchange protocol $\mathcal{X}$ with parties A and B using an environment with non-negligible transaction cost. If A and B can unfaithfully leave the protocol at any time and moves of A and B are always* *executed sequentially, it is impossible to achieve full cost fairness.*

Proof. Since moves of A and B are always executed sequentially, either A or B has to initialize $\mathcal{X}$. If, w.l.o.g., A initializes the protocol and B can leave unfaithfully, according to Theorem V.1 partial cost fairness in favor of A cannot be achieved. Hence, full cost fairness cannot be achieved. □

VI. Discussion

The main difference of our game-theoretic model of exchange protocols compared with existing models is the consideration of transaction cost and values within the payoff calculation. We argue why consideration of transaction cost and cost fairness is important for the usability and acceptance of exchange protocols, using blockchain-based exchange protocols as an example. We also highlight differences regarding transaction cost and cost fairness between public and private blockchains.

A. Game-Theoretic Model of Exchange Protocols

In order to answer RQ 1, we developed a model for two-party exchange protocols considering transaction cost. In contrast to the formal model presented by Buttyán and Hubaux [26], in our model of two-party exchange protocols presented in Section III, we do not consider the actual item but the individual valuations of the items of the parties involved in the exchange for the following reasons: Game theory generally assumes rational players, which try to maximize their own payoff. If $p_A + p_B < 0$, at least one player will not have any benefit from the exchange, so they rather would not participate in the exchange at all [29]. Looking at individual values $v_A(\iota, \rho^A)$ and $v_B(\iota, \rho^B)$ for an item ι or a share of it, it is possible that both parties may benefit from an exchange at the same time, if the received item has a higher value for the receiving party than the item that has been passed instead (see [30]: "You must price your information goods according to consumer value, not according to your production cost."). Furthermore, our model also covers additional financial aspects of an exchange, such as cost (decreasing the benefit) or compensations paid to a party (increasing the benefit).

B. Cost Fairness

Due to the necessity of the existence of a trusted third party in order to achieve fairness in an exchange [3], [4], potential transaction cost charged by a trusted third party cannot be avoided when fairness according to Asokan [1] is required. For this reason, in Section IV, we defined cost fairness, which takes into account transaction cost, but also potential differences in the value of the items to be exchanged and possible compensation payments. With our definitions of partial cost fairness (Definition IV.1) and full cost fairness (Definition IV.2) we provide a concept that is applicable for two party-exchange protocols. With the definitions of cost fairness, we provide a possibility to assess fairness of two-party exchange protocols regarding transaction cost, as asked for in RQ 2.

Intentionally, we did not define cost fairness as an extension of fairness, since the concept cannot only be applied for fair exchange protocols but also general exchange protocols (e-commerce as well as in analog world). As there are protocols, which do not (yet) aim for cost fairness while achieving fairness, it might also be desirable to have a protocol that achieves cost fairness but does not need to achieve fairness. We suggest that an exchange protocol should try to achieve both, fairness according to [23] and (full) cost fairness.

As long as all parties can be forced to follow the exchange protocol they agreed on and cannot leave it unfaithfully before completing one of the strategies allowed by the protocol, cost fairness can be established by enforcing a compensation payment to the faithful party at the end of the protocol if one party behaves unfaithfully. If a party can unfaithfully leave the exchange, such a compensation payment directly originating from the unfaithful party cannot be enforced. To reduce the amount of unilateral cost in such a case, a compensation mechanism can be used, where all parties deposit some money at the beginning of the exchange protocol, which then can be used by the trusted third party to take the amount required to compensate the faithful party from the deposit of the unfaithful party. However, also the depositing step might raise cost for the faithful party and therefore has to be included in the cost fairness analysis.

C. Application of Cost Fairness to Blockchain-based Fair Exchange Protocols

As the motivation of this work is based on blockchain-based fair exchange protocols, we also want to apply cost fairness to blockchain-based fair exchange protocols. Since there are fundamental differences between public and private blockchains regarding transaction cost, the assessment of cost fairness has to be done differently for public and private blockchains.

1) Cost Fairness in Public Blockchain-based Fair Exchange Protocols: In context of public blockchains, transaction cost is accrued in form of fees, which have to be paid per blockchain transaction to incentivize so-called miners in operating and supporting the blockchain infrastructure [10]. Therefore, for blockchain-based exchange protocols executed on a public blockchain, having transaction cost is inevitable. Furthermore, due to the pseudo-anonymity [15] and the distributed nature of a blockchain, parties involved in the exchange can leave the exchange protocol at any time (by stopping to interact, usually assumed after a timeout defined before the protocol starts). Therefore, since both parties of a two-party exchange can leave unfaithfully at any time, according to Theorem V.1 it is not possible to achieve partial cost fairness in favor of the party that has to initialize the exchange protocol. At least it is possible to achieve partial cost fairness in favor of the second party, if the initializing party is requested to deposit funds during the initialization move. This compensation can be used by the trusted third party to compensate the other party in case the initializing party behaves unfaithfully. One example for a blockchain-based two-party fair exchange protocol implementing a compensation mechanism is SmartJudge [8].

For an exemplary assessment of a public blockchain-based two-party fair exchange protocol, we take a detailed look at FairSwap, which is designed for the Ethereum blockchain. The seller initializes the exchange protocol by deploying the smart contract to the blockchain, which is charged with transaction fees of approx. 1,050,000 Gas[7]. Since the Ethereum blockchain cannot protect against unfaithful leave, the buyer can leave the protocol right after the seller deployed the contract. Therefore, partial cost fairness in favor of the seller is not achieved, since the payoff is $(p_{seller}, p_{buyer}) = (-1050000Gas, 0)$.

As shown in Theorem V.1, it is not possible to fix FairSwap to achieve full cost fairness. However, it is possible to reduce cost of the initialization step by creating a *container protocol*, which contains requests a deposit in its initialization move and monitors the behavior of the parties of the contained exchange protocol (e.g., FairSwap) and pays out compensations to the honest party if one party starts to cheat. Alternatively, state channels [13] can be used to execute the protocol off-chain and therefore reduces the amount of blockchain transactions and therefore transaction cost to be paid.

In order to allow for public blockchain-based exchange protocols to achieve cost fairness, a change of the blockchain environment is required in which initializing deposits, such as for initializing a container protocol or opening a state channel, is not charged with transaction cost.

Concluded, answering RQ 3, it is not possible to achieve full cost fairness on public blockchains with transaction cost, since (at the current state of art) cost is inevitable and one party has to initialize the protocol, and therefore, according to Theorem V.1, partial cost fairness can never be achieved simultaneously in favor of A and B.

2) Cost Fairness in Private Blockchain-based Fair Exchange Protocols: In contrast to a public blockchain, a private blockchain only allows access for well-identified participants. Therefore, the risk of, e.g., a grieving attack is considerably lower since a party behaving unfaithfully can be punished by getting ignored on future attempts or the access to the private blockchain can be revoked. Furthermore, a private blockchain does not necessarily come with any means of transaction cost (e.g., Hyperledger Fabric [14]), therefore concepts of cost or money are not an inherent part of a private blockchain. In this case, means of financial (or comparable) compensations for provided services or items exchanged is in the responsibility of the implementation of the respective smart contract, implementing the exchange. If means of transaction cost is introduced by such a smart contract, cost fairness can also be assessed like it is done for public blockchains.

However, since the actual operation of the private blockchain network is not necessarily covered by their smart contract applications, also these cost can be taken into account for cost fairness assessment (e.g., cost for servers, internet connection, etc.). If however (as it is, e.g., with Quorum Blockchain[8]) the private blockchain comes with a financial concept similar to the one of public blockchains, the blockchain network itself could be extended to provide a compensation service of last resort, which takes care about compensation payouts if neither the actual exchange protocol nor superior container protocols are able to provide cost fairness.

Therefore, we have to incorporate operational cost instead of considering transaction cost for the assessment of cost fairness in order to answer RQ 4. Since the choice of the blockchain concept and its implementation is up to the operator(s) of the private blockchain network, they are also free to implement any kind of compensation mechanism, which could be used as compensation of last resort, if inner protocols do not achieve cost fairness.

VII. Conclusion

In this work, we have introduced our approach on how to model an exchange protocol using notions from game theory (answering RQ 1). This model can be used as a base for further works for formal analyses of different aspects of two-party exchange protocols. We used this model to define partial cost fairness and full cost fairness as a desirable property of exchange protocols (answering RQ 2). As major finding, we have shown that cost fairness cannot be achieved on current state-of-the-art blockchains such as Ethereum (answering RQ 3). In private blockchains, which can be designed by the operators, cost fairness can be enabled by allowing for free depositing transactions or even enforced by adding a compensation mechanism as part of the blockchain network (answering RQ 4).

In future work, we want to use our model to compare existing blockchain-based two-party exchange protocols regarding different aspects, such as fairness, cost, cost fairness and game-theoretical strategy equilibria [24]. Furthermore, we plan to apply state channels to reduce total transaction cost of blockchain-based fair exchange protocols and to allow for a reliable prediction of maximum cost to be covered for the honest party if full cost fairness cannot be achieved, which can be used as a metric for the risk to be taken when joining an exchange. Related to this, we want to introduce another definition of cost fairness, which considers if the transaction cost of an exchange protocol are guaranteed to stay within the prediction. We will name this definition *cost fairness with* ϵ, which states if the maximum cost that have to be covered by the honest party if the other party behaves unfaithfully are smaller than ϵ. The value of ϵ can then also be used to compare worst-case transaction cost between two exchange protocols.

One drawback of our model is that it is limited to two-party exchanges. In order to allow a more general usage, we want to extend our model to allow for n-party exchanges.

[7] approx. worth about 349.20 USD as of 2021-12-17, see Section I

[8] Quorum Blockchain — https://github.com/ConsenSys/quorum, accessed 2021-12-17

References

[1] N. Asokan, "Fairness in electronic commerce," Ph.D. dissertation, IBM, 1998.

[2] H. Pagnia, H. Vogt, and F. C. Gärtner, "Fair exchange," *Comput. J.*, vol. 46, no. 1, pp. 55–75, 2003. [Online]. Available: https://doi.org/10.1093/comjnl/46.1.55

[3] S. Even and Y. Yacobi, "Relations among public key signature systems," Computer Science Department, Technion, Tech. Rep., 1980.

[4] H. Pagnia and F. C. Gärtner, "On the impossibility of fair exchange without a trusted third party," Technical Report TUD-BS-1999-02, Darmstadt University of Technology, Darmstadt, Germany, Tech. Rep., 1999.

[5] S. Delgado-Segura, C. Pérez-Solà, G. Navarro-Arribas, and J. Herrera-Joancomartí, "A fair protocol for data trading based on bitcoin transactions," *IACR Cryptol. ePrint Arch.*, p. 1018, 2017. [Online]. Available: http://eprint.iacr.org/2017/1018

[6] S. Dziembowski, L. Eckey, and S. Faust, "Fairswap: How to fairly exchange digital goods," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*, D. Lie, M. Mannan, M. Backes, and X. Wang, Eds. ACM, 2018, pp. 967–984. [Online]. Available: https://doi.org/10.1145/3243734.3243857

[7] L. Eckey, S. Faust, and B. Schlosser, "Optiswap: Fast optimistic fair exchange," in *ASIA CCS '20: The 15th ACM Asia Conference on Computer and Communications Security, Taipei, Taiwan, October 5-9, 2020*, H. Sun, S. Shieh, G. Gu, and G. Ateniese, Eds. ACM, 2020, pp. 543–557. [Online]. Available: https://doi.org/10.1145/3320269.3384749

[8] E. Wagner, A. Völker, F. Fuhrmann, R. Matzutt, and K. Wehrle, "Dispute resolution for smart contract-based two-party protocols," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2019, pp. 422–430.

[9] M. Hall-Andersen, "Fastswap: Concretely efficient contingent payments for complex predicates." *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 1296, 2019.

[10] G. Wood *et al.*, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," *Ethereum Project Yellow Paper*, 2014.

[11] V. Buterin, E. Conner, R. Dudley, M. Slipper, I. Norden, and A. Bakhta, "Fee market change for eth 1.0 chain," https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md, accessed: 2021-12-17.

[12] A. Küpçü and A. Lysyanskaya, "Usable optimistic fair exchange," in *Topics in Cryptology - CT-RSA 2010, The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings*, ser. Lecture Notes in Computer Science, J. Pieprzyk, Ed., vol. 5985. Springer, 2010, pp. 252–267. [Online]. Available: https://doi.org/10.1007/978-3-642-11925-5_18

[13] S. Dziembowski, S. Faust, and K. Hostáková, "General state channel networks," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*, D. Lie, M. Mannan, M. Backes, and X. Wang, Eds. ACM, 2018, pp. 949–966. [Online]. Available: https://doi.org/10.1145/3243734.3243856

[14] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. D. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolic, S. W. Cocco, and J. Yellick, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference, EuroSys 2018, Porto, Portugal, April 23-26, 2018*, R. Oliveira, P. Felber, and Y. C. Hu, Eds. ACM, 2018, pp. 30:1–30:15. [Online]. Available: https://doi.org/10.1145/3190508.3190538

[15] A. Biryukov and S. Tikhomirov, "Deanonymization and linkability of cryptocurrency transactions based on network analysis," in *IEEE European Symposium on Security and Privacy, EuroS&P 2019, Stockholm, Sweden, June 17-19, 2019*. IEEE, 2019, pp. 172–184. [Online]. Available: https://doi.org/10.1109/EuroSP.2019.00022

[16] M. Lohr, K. Skiba, M. Konersmann, J. Jürjens, and S. Staab, "Formalizing cost fairness for two-party exchange protocols using game theory and applications to blockchain," in *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2022*. IEEE, 2022.

[17] M. Lohr, B. Schlosser, J. Jürjens, and S. Staab, "Cost fairness for blockchain-based two-party exchange protocols," in *2020 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2020, pp. 428–435.

[18] R. Cleve, "Controlled gradual disclosure schemes for random bits and their applications," in *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, ser. Lecture Notes in Computer Science, G. Brassard, Ed., vol. 435. Springer, 1989, pp. 573–588. [Online]. Available: https://doi.org/10.1007/0-387-34805-0_50

[19] J. D. Tygar, "Atomicity in electronic commerce," in *Proceedings of the Fifteenth Annual ACM Symposium on Principles of Distributed Computing, Philadelphia, Pennsylvania, USA, May 23-26, 1996*, J. E. Burns and Y. Moses, Eds. ACM, 1996, pp. 8–26. [Online]. Available: https://doi.org/10.1145/248052.248054

[20] H. Pagnia and R. Jansen, "Towards multiple-payment schemes for digital money," in *Financial Cryptography, First International Conference, FC '97, Anguilla, British West Indies, February 24-28, 1997, Proceedings*, ser. Lecture Notes in Computer Science, R. Hirschfeld, Ed., vol. 1318. Springer, 1997, pp. 203–216. [Online]. Available: https://doi.org/10.1007/3-540-63594-7_79

[21] F. Bao, R. H. Deng, and W. Mao, "Efficient and practical fair exchange protocols with off-line TTP," in *Security and Privacy - 1998 IEEE Symposium on Security and Privacy, Oakland, CA, USA, May 3-6, 1998, Proceedings*. IEEE Computer Society, 1998, pp. 77–85. [Online]. Available: https://doi.org/10.1109/SECPRI.1998.674825

[22] M. K. Franklin and M. K. Reiter, "Fair exchange with a semi-trusted third party (extended abstract)," in *CCS '97, Proceedings of the 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, April 1-4, 1997*, R. Graveman, P. A. Janson, C. Neuman, and L. Gong, Eds. ACM, 1997, pp. 1–5. [Online]. Available: https://doi.org/10.1145/266420.266424

[23] N. Asokan, M. Schunter, and M. Waidner, "Optimistic protocols for fair exchange," in *CCS '97, Proceedings of the 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, April 1-4, 1997*, R. Graveman, P. A. Janson, C. Neuman, and L. Gong, Eds. ACM, 1997, pp. 7–17. [Online]. Available: https://doi.org/10.1145/266420.266426

[24] P. Morris, *Introduction to game theory*. Springer Science & Business Media, 2012.

[25] L. Buttyán and J. Hubaux, "Rational exchange - A formal model based on game theory," in *Electronic Commerce, Second International Workshop, WELCOM 2001 Heidelberg, Germany, November 16-17, 2001, Proceedings*, ser. Lecture Notes in Computer Science, L. Fiege, G. Mühl, and U. G. Wilhelm, Eds., vol. 2232. Springer, 2001, pp. 114–126. [Online]. Available: https://doi.org/10.1007/3-540-45598-1_12

[26] L. Buttyan and J.-P. Hubaux, "Toward a formal model of fair exchange, a game theoretic approach," Tech. Rep., 2000.

[27] S. Nakamoto *et al.*, "Bitcoin: A Peer-to-peer Electronic Cash System," 2008.

[28] R. B. Myerson, *Game theory - Analysis of Conflict*. Harvard University Press, 1997. [Online]. Available: http://www.hup.harvard.edu/catalog/MYEGAM.html

[29] X. T. Tao, Y. G. Gu, and G. Q. Li, "A formal game-theoretic model for rational exchange protocol," in *Advanced Materials Research*, vol. 204. Trans Tech Publ., 2011, pp. 2033–2040.

[30] C. Shapiro and H. R. Varian, *Information rules - a strategic guide to the network economy*. Harvard Business School Press, 1999. [Online]. Available: https://www.worldcat.org/oclc/39210116