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

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

2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) | 978-1-6654-9538-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICBC54727.2022.9805522

***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

When a trusted third party (TTP, e.g., notary service) is involved in a *fair exchange* [1], [2], it can raise non-negligible transaction cost. Such transaction cost must be considered separately from possible payments as part of the exchange for fairness assessment, as they are intended to pay the TTP for their services rather then being part of the goods (including money) to be exchanged between the participants.

When an exchange protocol is used in which a public blockchain (e.g., Ethereum [3]) acts as a TTP, all interactions with the TTP are performed using *blockchain transactions*, which require the acting party to pay transaction cost in form of *blockchain transaction fees*. There exist alternative approaches, such as optimistic protocol design [4] or the usage of state channels [5] that can generally be used to reduce blockchain transaction fees. Nevertheless, even then transaction cost is greater than zero and often non-negligible.

So far, all fair exchange protocols using a public blockchain as TTP 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 TTP. This opens the possibility for a *grieving attack* [6] 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, 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], 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: RQ1: How can two-party exchange protocols be modeled so that transaction cost is taken into account? RQ2: How can the fairness of two-party exchange protocols be assessed regarding transaction cost? RQ3: How to achieve cost fairness for public blockchain-based two party exchange protocols (e.g., FairSwap)? Due to space limitations we published an extended version including the proofs and further details in [7].

II. Fair Exchange

The term *fair exchange* describes the challenge of two or more distrusting parties that want to exchange their own goods with the guarantee that no party can gain advantage over

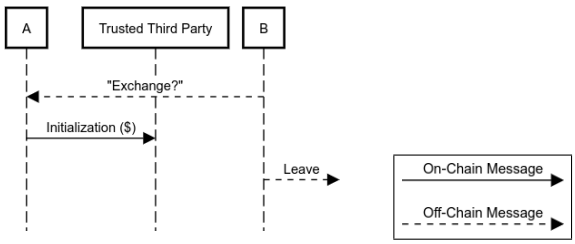

Fig. 1: Grieving attack, conducted by B. *Initialization* is an action where A pays fees to the TTP in the belief that B will continue the targeted exchange.

Kenneth Skiba was supported by the Deutsche Forschungsgemeinschaft under grant KE 1413/11-1 and Jan Jürjens by the EC (Horizon 2020) within the projects "Digital Reality in Zero Defect Manufacturing (Qu4lity)" and "Trusted Secure Data Sharing Space (TRUSTS)".

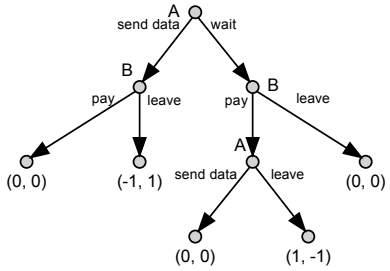

Fig. 2: Game tree with players A and B exchanging data for money with different orders of payment and data transfer.

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 [1] as long as at least one party follows the fair exchange protocol [8], [9], [10], [11], [12], [13], [1]. It has been shown that it is impossible to achieve fair exchange without involving a TTP [14], [15]. None of the approaches referenced above considers possible transaction cost of involving a TTP in an exchange.

Cost fairness has already been informally defined by Lohr et al. [16]. 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.

III. Modeling an Exchange using Game Theory

Game theory deals with making strategic decisions when two or more parties interact with each other with the goal of maximizing their individual payoff [17]. In this section, we present our model of an exchange protocol using game theory, building upon the work of Buttyán and Hubaux [18].

We build on the formal notion of an *extensive game*: A *game tree* [17], [19] (see Figure 2 for an example) is a tree that depicts all possible ways to play a game.

Definition III.1 (Game Tree [17])**.** *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.*

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 $P = o(v)$, $P \in \mathcal{P}$ chooses the next move, represented by $e = (v, v')$, $e \in E, v' \in V$, leading to v'. The behavior of players resulting in the selection of the next move in an extensive game is described by a *strategy*. We only provide a basic definition of a strategy, for a detailed and more formal definition of strategy we refer to Morris [17].

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.*

Definition III.3 (Strategy Set [17])**.** *For player P a* strategy set *$\Sigma = \{S_1, ..., S_m\}$ is the set of all possible strategies of P.*

Now we can define an extensive game:

Definition III.4 (Extensive Game [17])**.** *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 $\Sigma_{P_1}, ..., \Sigma_{P_n}$.*

We only consider two-party exchange protocols. Similar to Buttyán and Hubaux [18], we do not consider the TTP 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.

We assume a two-party exchange with parties $\mathcal{P} = \{A, B\}$ who are interested to exchange their items ι_A and ι_B and that A and B agreed on using the exchange protocol $\mathcal{X}$ (see 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 $S_A \in \Sigma_A$ and $S_B \in \Sigma_B$. 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) 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. Let $a(e) = (\overrightarrow{\rho_e}, cost_e, deposit_e, \overrightarrow{comp_e})$ 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 $0 \leq \rho_e^P \leq 1$, $P \in \mathcal{P}$, $cost_e \geq 0$ is the transaction cost that has to be paid by A to the TTP 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 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 parts, in which case $0 \leq \rho_e^A \leq 1$. 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 TTP for conducting move e. To enable the TTP 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 TTP. 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 compen-

sate A. $comp_e^A$ denotes the compensation paid to A by the TTP in move e. Usually, a TTP does not use its own money to pay out compensations. Instead, the compensation paid out is taken from deposits made before. 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 $\mathcal{P} = \{A, B\}$: $\sum_{P_i \in \mathcal{P}} \left(\sum_{e \in E_{P_i}} \left(deposit_e - \sum_{P_j \in \mathcal{P}} comp_e^{P_j} \right) \right) \geq 0$

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}. Both goods and money can temporarily be owned by the TTP 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 TTP, sending money to the TTP does not make it available to one of the parties (therefore $\rho = 0$) while sending unencrypted data to the TTP will make it available to everyone, therefore $\rho > 0$.

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 $T = (V, E, \mathcal{P}, o, \vec{p})$ 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. Let $faithful? : E \to \{faithful, unfaithful\}$ be a total function that returns for each move e if e is considered to be faithful or unfaithful behavior of player $A = o(v)$.*

We can now formally define an *exchange protocol*:

Definition III.7 (Exchange Protocol)**.** *We define an* exchange protocol $\mathcal{X} = (\Gamma, a, faithful?)$ *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 $faithful?(e)$, $e \in E$ of the game tree of Γ.*

An exchange protocol $\mathcal{X}$ is called *fair exchange protocol* iff it achieves fairness according to Asokan [1]. For an exchange protocol $\mathcal{X} = (\Gamma, a, faithful?)$, using $faithful?(e)$, $e \in E$ we can classify all available strategies in Γ regarding their faithfulness:

Definition III.8 (Faithful and Unfaithful Strategies and Strategy Sets)**.** *Let $\mathcal{X} = (\Gamma, a, faithful?)$ 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 $faithful?(e) = faithful$. 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 minus everything A had to give away. In order to consider the values of the shares of ι_A and ι_B for the payoff, we 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. 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 $\mathcal{X} = (\Gamma, a, faithful?)$ 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:*

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

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, 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. Then it is also not possible to forcefully withdraw money from the leaving party and send it to the faithful party as compensation. 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 At Any Time)**.** *Let $e_{leave} \in E$ represent an unfaithful leave, then $a(e_{leave}) = (\vec{0}, 0, 0, \vec{0})$ and $faithful?(e_{leave}) = unfaithful$.*

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.1 (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 the exchange protocol is used, 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.12 (Environment with non-negligible transaction cost)**.** *Given an exchange protocol $\mathcal{X}$ represented by game tree $T = (V, E, \mathcal{P}, o, \vec{p})$. We define $\mathcal{X}$ to be in an* environment with non-negligible transaction cost *if for all $e \in E \setminus e_{leave}$ with $a(e) = (\vec{\rho_e}, cost_e, deposit_e, \overrightarrow{comp_e})$: $cost_e > 0$.*

IV. Cost Fairness

Cost fairness has already been informally defined by Lohr et al. [16]. 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 $\vec{p}(S_A, S_B) = (p_A, p_B)$ it holds $p_A \geq 0$.*

Applying Definition IV.1 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 wrt. cost fairness as it has been asked for in RQ2.

V. Achievability of Cost Fairness

If w.l.o.g., B cannot leave the exchange protocol without the approval of the TTP 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.*

Theorem V.2. *Given a two-party fair exchange protocol $\mathcal{X}$ with parties A, 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.*

VI. Discussion

For answering RQ1, we developed a formal model for two-party exchange protocols, which considers financial aspects of an exchange, such as cost (decreasing the benefit) or compensations paid to a party (increasing the benefit). Due to space limitations, for an more extensive discussion we refer to the extended version of this work [7].

Due to the necessity of the existence of a TTP in order to achieve fairness in an exchange [14], [15], potential transaction cost charged by a TTP 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 the definitions of cost fairness, we provide a method to assess fairness of two-party exchange protocols wrt. transaction cost to answer RQ2.

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.

VII. Conclusion

In this work, we have introduced our approach on how to model an exchange protocol using notions from game theory (RQ1), which can be used as a base for further works for formal analyses 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 (RQ2). As major finding, we have shown that cost fairness cannot be achieved on current state-of-the-art blockchains such as Ethereum (RQ3).

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

[4] 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

[5] 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

[6] 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

[7] 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 (extended version)," 2022. [Online]. Available: https://doi.org/10.48550/arXiv.2203.05925

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

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

[15] 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.

[16] 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.

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

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

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