Pricing Anonymity

Daniel G. Arce[1] and Rainer Böhme[2,3]

[1] University of Texas at Dallas, darce@utdallas.edu
[2] University of Innsbruck, Austria, rainer.boehme@uibk.ac.at
[3] Westfälische Wilhelms-Universität Münster, Germany

Abstract. In electronic anonymity markets a taker seeks a specified number of market makers in order to anonymize a transaction or activity. This process requires both coalition formation, in order to create an anonymity set among the taker and makers, and the derivation of the fee that the taker pays each maker. The process has a novel property in that the taker pays for anonymity but anonymity is created for both the taker and the makers. Using the Shapley value for nontransferable utility cooperative games, we characterize the formation of the anonymity set and the fee for any arbitrary number of makers selected by the taker.

Keywords: Anonymity, Markets, Privacy, Game theory

1 Introduction and Literature Review

Several advances in information technology have brought about that electronic transactions reveal identifying information of transaction partners. Specifically, packet-switched networks transmit addresses in every data packet to ensure delivery, digital signatures include identifying public keys for verification, and public ledger-based cryptocurrencies use references to – unique and therefore potentially identifying – past transactions for verification.

Sometimes identifiability is dysfunctional, and demand for anonymity arises out of private or public interest. However, establishing anonymity in systems that depend on identifying information requires effort. Technical solutions, known as *mixes*, bundle and shuffle the electronic records of similar activities (messages, transactions) from many participants so as to hide the relation between subjects and objects. Practical examples include the Tor network for Internet communication [11], mixes offering transaction anonymization in Bitcoin[4] [25], or the existence of dark pools next to conventional financial markets [40].

Surprisingly little research studies the price of anonymity. Acquisti et al. [2] describe the economics of participating in (message) mixing services. They observe that anonymity is co-created by multiple agents sharing activities with the same observable features: one cannot be anonymous alone. More specifically,

[4] The popular belief that Bitcoin payments are anonymous is wrong. This cryptocurrency uses pseudonymous accounts and a public transaction ledger. Agents who want to hide the relation between their accounts, some of which may fully identify them, need anonymizing technology [6].

the authors consider decentralized anonymity infrastructures and suggest non-cooperative game theory to identify viable participation equilibria, but they do not offer a solution to their game. Acquisti and Varian [4] consider optional anonymization with simple technology ("delete cookie"), available without cost to some customers in their model, as a constraint to individual pricing. By contrast, Friedman and Resnick [14] study the effect of optional anonymity on the social level. Their repeated game with random matching predicts negative welfare effects. This is because bad reputation does not stick when agents can choose to be anonymous, resounding with the models of credit information sharing, which also contribute to the formal economic treatment of identity [30, 29].

Other works, broadly related to anonymity and prices, focus on the payment system needed to compensate the operators of anonymizing infrastructure without revealing identifying information on the payment channel [13, 5, 17]; or empirically approximate users' willingness to pay for anonymous Internet access by measuring the tradeoff between the anonymity provided by a mixing service and the experienced performance [19].

The present work is inspired by our measurement study of JoinMarket[5] [23], a platform in the Bitcoin ecosystem that matches agents who seek to merge their payments in a single transaction in order to improve anonymity. Such transactions are called CoinJoins in jargon [21] and, to offer some anonymity, they must entail payments of the same amount at the same time.[6] JoinMarket is organized as platform where supply-side agents, called *makers*, offer funds to participate in CoinJoin transactions for an advertised mixing fee.[7] Demand-side agents, called *takers*, initiate an anonymizing transactions by choosing several of these offers. As a result, a typical transaction from this market is funded by exactly one taker and two or more makers. The matching and settlement is supported with software provided by the JoinMarket developers and run in a decentralized manner on many Internet nodes. Möser and Böhme [24] speculate why demand and supply might exist in this market, but acknowledge that "puzzles" remain. They do not formally characterize the relation between key parameters, such as the level of anonymity provided and its price (i. e., the fees paid to form the CoinJoin).

Here, to the best of our knowledge, we provide the first formal solution to price anonymity in systems which require the coordination of multiple participants. While we adopt the terminology of transaction anonymization used in CoinJoins, our results generalize to all anonymization schemes with similar properties. As one cannot be anonymous alone, anonymity requires an agreement among individuals to behave in an indistinguisable way; e.g. via common message length or transaction amount. This results in the formation of an *anonymity set*, being the collection of individuals that nonmembers cannot distinguish between. The degree of anonymity is generally associated with the size of the

[5] See http://joinmarket.io. Last visited on May 8th, 2017.

[6] See Meiklejohn and Orlandi [22] on the hardness of untangling CoinJoin transactions.

[7] The fee is composed of fixed and variable parts to account for contributions to the Bitcoin network's miner fees. Our model abstracts from this complexity by assuming a normalized nominal transaction value.

anonymity set [32]. An anonymity set therefore requires coalition formation, and the traditional game-theoretic approach to coalition formation is cooperative game theory. Consequently, at its most basic level, a CoinJoin transaction requires the formation of an anonymity set/coalition organized around a common transaction amount. In addition, the formation of the anonymity set/coalitions is enforceable because a Bitcon CoinJoin agreement occurs only if all members of the anonymity set sign the transaction [21]. This is again consistent with cooperative game theory.

In a cooperative game representation of a CoinJoin, a characteristic function is specified for all potential coalitions in the transaction. For each coaltion, the characteristice function is a vector of payoffs for each member of that coalition, where payoffs are defined in terms of the size of the anonymity set specified by the taker, each player's valuation of their identity, the fee paid by a taker to get enough makers to join the anonymity set, the fee received by makers for joining the anonymity set, etc. What matters is that this approach captures the key property of anonymity markets, which is that some participants pay for anonymity but all participants benefit from anonymity being created. This is also novel from the perspective of cooperative game theory in that one player (the taker) is *paying* other players (the makers) to form a coalition from which *all* members benefit. Consequently, the characteristic function is defined for the anonymity set (the grand coalition) and all potential subcoalitions of the anonymity set, where the anonymity fee is an unknown to be determined endogenously as a function of the solution concept used to solve the game.

In this paper we use the Shapley value to solve the cooperative game. The Shapley value an economically-motivated solution that gives each player their expected marginal contribution to the anonymity set and all possible subcoalitions of the anonymity set. In particular, we derive expressions for the Shapley value of the market participant demanding anonymity (the taker) and any number of suppliers (the market makers) participating in a CoinJoin. This in turn allows for a characterization of the price of anonymity. The class of anonymization schemes to which our theory applies can be further expanded by adapting the characteristic function to the anonymization scheme and attacker model.

Our work is distinct from a line of formal research on privacy quantification with respect to *attribute* disclosure. For example, differential privacy offers a framework to measure and account the privacy loss when querying private databases interactively [12]. Game theory, also in its cooperative form [18, 9], has been applied in this subfield in order to establish the price of attribute values as a function of their precision, or to incentivize disclosure [15, 8]. Acquisti et al. [3] survey the economics of privacy more broadly.

This paper is organized as follows. Section 2 specifies anonymity markets as a cooperative game. Section 3 presents the Shapley value as the solution concept for the game. Section 4 solves the game for the case of three players. Section 5 generalizes to N players, and Section 6 concludes.

2 Anonymity Markets as Cooperative Games

In this section we introduce the building blocks for specifying an anonymity market as a cooperative game. We consider anonymity markets with two types of participants: *takers* and (market) *makers* [24]. Makers offer their identities or pseudoidentities (such as Bitcoin addresses) for use in a transaction or activity that the taker seeks to engage in anonymously. Recall from the introduction that existing markets match exactly one taker with two or more makers to form a transaction. All makers are assumed to be honest in that they do not seek to ascertain the taker's identity for their own purposes. Hence, the returns of interest to a maker in an anonymity transaction are the fee that the maker receives from the taker and the anonymity that the maker receives as well in the transaction. This is the peculiarity of anonymity markets: the taker pays for anonymity but the transaction itself anonymizes the identities of the taker and makers alike. In this sense anonymity is akin to a public good that only the taker pays for.[8]

Following Pfitzmann and Köhntopp [32, p. 2], anonymity can be defined as: "the state of being not identifiable within a set of subjects, the anonymity set."[9] The purpose of an anonymity market is to create an anonymity set, S, which is a coalition consisting of a taker and makers. As anonymity is meant to preserve identities, the term D will denote the taker's value of its identity. All makers will be assumed to value their identity identically, with d denoting a maker's valuation of its identity. The fee that a taker pays to each maker in an anonymity set is denoted as f (to be determined endogenously). A cooperative game approach to anonymity is appropriate because the focus is on the distribution of benefits among the taker and makers when they form an anonymity set.

In a CoinJoin, the probability that a player remains anonymous (retains their identity) against a global passive adversary (GPA) in an anonymity set/coalition of size $|S|$ is $(|S|-1)/|S|$, as all $|S|$ members of the anonymity set are indistinguishable to the GPA owing to the common transaction amount and use of different input and output addresses in the transaction. In other words, the probability that the GPA randomly guesses the identity of a member of anonymity set S is $1/|S|$. Hence, participating in an anonymity market involves some risk of of loss of identity to each maker, and the fee we derive that is paid by the taker to each maker must compensate makers for this risk.[10]

[8] Public goods have the property that they are *nonexclusive* and *nonrival* [34]. Nonexclusive means that once created, the associated benefits of the good cannot be withheld from others. Technically, the nonexcludability property of anonymity applies only to the makers and taker engaged in the transaction. Nonrivalry means that use of the good does not prohibit its use by others.

[9] This definition is compatible with common alternatives. For example, the size of the anonymity set corresponds to the parameter k in the k-anonymity model [39]. Entropy-based anonymity metrics generalize to sets with non-uniform priors [10, 35].

[10] In addition to the first-order risk of losing one's identity, makers may also face the risk of legal authorities investigating Bitcoin purchases as part of a criminal investigation. This potentiality lies beyond the scope of the present paper.

In addition, it is assumed that anonymity is only created within coalitions involving a taker. Intuitively, potential makers do not costlessly create anonymity amongst themselves because they have no underlying transaction or message that requires anonymization, and forming an anonymity set always carries some risk. Instead, makers rely on a taker (who does have a transaction or message needing anonymization) to compensate them for creating anonymity for both the taker and themselves. This implies that the payoffs for makers in coalitions that do not involve a taker are normalized to zero. Normalizing in this way facilitates an emphasis on taker identity, maker identity and the public nature of anonymity in determining the fee for anonymity, which is the focus of the paper.

The specifics of the transaction to be anonymized (e. g., amount, message length, or time) precludes takers from matching with other takers. As Narayanan et al. [27] observe, a one-taker transaction avoids the necessity for multiple takers to agree on transaction specifics, which is inefficient and costly. Hence, there is no requirement for coincidence of transaction specifics among takers. Only makers customize the transaction to the specific needs of a taker so as to make their activities indistinguishable in the anonymity set. The incentive for makers to form a coalition with the taker is that they are compensated for facilitating anonymity by meeting the taker's transaction needs. This compensation takes the form of a fee, f, paid by the taker *and* the anonymity received by the maker when participating in the CoinJoin.

The taker's alternative is known as a *mix*, and is addressed within the model as the taker's outside option. Specifically, instead of an anonymity market, such as JoinMarket, a taker could go to an outside option (e. g., a mix) and pay a fee, F, for anonymity. Anonymity markets are almost instantaneous transactions for the taker whereas the outside option may involve a significant delay and risk. Mixing services in the Bitcoin ecosystem reportedly stole their clients' funds, a threat that can be mitigated with CoinJoin transactions arranged on anonymity markets [25]. Consequently, the reservation value of anonymity for the taker of going to the outside option for anonymity is δD where $\delta \in (0, 1)$ is a function of both the probability that the funds are transmitted as intended while anonymity is preserved by this outside option, and the taker's time preference (discount factor). As both probabilities and discount factors lie within the (0,1) interval, $\delta \in (0, 1)$ by definition. By comparison, in a CoinJoin with an anonymity set of size $|S|$ the taker retains its anonymity with probability $(|S| - 1)/|S|$, leading to an expected value of anonymity of $(|S| - 1)/|S| \times D$. Lastly, the mixing fee, F, is posted, whereas the CoionJoin fee, f, is to be determined via the equilibrium process associated with the CoinJoin.

Finally, anonymity is a public good but it need not be valued identically among the anonymity market participants; hence, the value D for the taker's identity and d for each maker's identity. Moreover, interpersonal comparisons of anonymity are not possible. For example, the taker's value of its identity need not be expressed in terms of the same measure of value as the maker's. Another rationale for nontransferable utility is that it is likely that takers and makers have differing time preferences [24]. Even if the valuation of anonymity was comparable between players, practical anonymity markets are restricted in arranging transfer payments. For example with Bitcoin and JoinMarket, transfer payments are either not enforceable (because alternative payments cannot be part of the same atomic transaction), or compromise the anonymity of the transaction (because the GPA may infer identity information from observing the transfer payments). In this model the transfer payment is the fee for anonymity, which is the same for every maker. Enforceable sidepayments beyond this constant fee would potentially compromise anonymity.

This implies that what is attainable by an anonymity set associated with a coalition of taker and makers cannot be assigned a single real number, as is the case in cooperative games with transferable utility, known as *TU games* [33]. More-to-the point, the assumption of transferable utility would imply that identity can be expressed in the same units of measurement for every member of the anonymity set and that it is possible to distribute the value that each member places on their identity across the membership of the anonymity set in a meaningful way. We do not believe that identity has such properties. Following Shapley [37, 38],"Interpersonal comparability of utility is generally regarded as an unsound basis on which to erect theories of multipersonal behavior." For this reason, much of noncooperative game theory steers clear of the transferable utility assumption. For similar reasons we use cooperative games with nontransferable utility, known as *NTU games*. NTU games are a more generalized version of cooperative games, as transferable utility is a restrictive assumption. Indeed, any TU game can be expressed as an NTU game. We therefore turn to the formal definition of an NTU game and the Shapley value solution to NTU games.

3 NTU Games and the Shapley Value

In a NTU game, for any non-empty coalition, S, the associated *NTU characteristic function*, $V(S)$, denotes the set of feasible utility vectors attainable by that coalition. Specifically, $V(S) \subseteq \mathbb{R}^{|S|}$, where $|S|$ is the cardinality of S. For each vector $\boldsymbol{x} \in V(S)$ the entry x_i specifies the maximum payoff to player i should player i be a member of that coalition.[11] Characteristic function $V(S)$ is the vector of utilities that is feasible for the members of S when they cooperate with each other. As described, an anonymity market is a cooperative game with sidepayments but without transferable utility [31].

An NTU game is defined by a pair (N, V), where N is the set of all players, and $V(S)$ is the characteristic function specifying the payoff to each member $i \in S$ for all coalitions $S \subseteq N$. Given the game (N, V) our approach uses the Shapley value [36] to derive the anonymity fee, f. The Shapley value allocates the total net benefits of an anonymity transaction according to each player's marginal contribution to every subcoalition of the anonymity set that the player can potentially be a member of.

[11] Technically, any $y_i \leq x_i$ is a potential payoff for player i as well. This property is known as "comprehensiveness" [28].

The Shapley value was originally defined for TU cooperative games. Later, Shapley [37, 38] established that one can create a TU game associated with an NTU game by creating a *fictitious transfer game* (a λ-transfer game), which converts the NTU game into a TU game that can be solved via Shapley's original method. The steps associated with this procedure can be summarized as follows. First, begin with a nonnegative set of weights for each of the players, $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_{|N|})$. Given these weights, find the maximum sum of the $\boldsymbol{\lambda}$-weighted utility for each vector $\boldsymbol{x} \in V(S)$. Second, these maximal sums essentially define a TU game (the fictitious transfer game) for which a Shapley value can be derived. Solve for the Shapley value. Denote as $\varphi_i(\omega, \boldsymbol{\lambda})$ the allocation received by player i in the Shapley value, where $\omega(S)$ is the characteristic function for the fictitious transfer game. Third, verify that the vector $[\varphi_i(\omega, \boldsymbol{\lambda})/\lambda_i]_{i \in N}$ is feasible for the grand coalition in the NTU game; i. e., $[\varphi_i(\omega, \boldsymbol{\lambda})/\lambda_i]_{i \in N} \in V(N)$. If feasible, then $\varphi_i(\omega, \boldsymbol{\lambda})/\lambda_i$ is the Shapley value allocation for player i in the NTU game.

Given this synopsis we now specify the formal procedure. First, create a fictitious transfer game by specifying a vector $\boldsymbol{\lambda} \in (\mathbb{R}^+)^{|N|}$. For each coalition, S, the function $\omega(S)$ is called the *worth function* (the characteristic function of the fictitious transfer game), where

$$\omega(S) = \max_{\boldsymbol{x} \in V(S)} \sum_{i \in S} \lambda_i x_i. \tag{1}$$

The λ_i/λ_j ratios can be considered as exchange rates between the nontransferable utilities of the players. As a simple example, if a taker measures its identity in terms of US$ and makers in terms of euros, €, then an exchange rate, $\lambda_{€}/\lambda_{\$}$, is needed to relate D to d, and $\lambda_{\$}/\lambda_{€}$ is needed to relate d to D.[12]

Second, the worth functions, $\omega(S)$, can be regarded as characteristic functions for a TU game derived from the NTU game. The *Shapley value for the associated TU game* is

$$\varphi_i(\omega, \boldsymbol{\lambda}) = \sum_{\substack{i \in S, \\ S \subseteq N}} \frac{(|S|-1)!(|N|-|S|)!}{|N|!} \cdot (\omega(S) - \omega(S \setminus \{i\}))\,. \tag{2}$$

For any coalition, S, that i is a member of, the term $\omega(S) - \omega(S \setminus \{i\})$ in Equation (2) measures i's *marginal contribution* to coalition S. That is, the difference $\omega(S) - \omega(S \setminus \{i\})$ is what the coalition can achieve with i as a member less what it achieves without i. The Shapley value is therefore the expected value of a player's marginal contribution over all potential $|N|!$ orderings of the players in the game. The coefficient on the marginal contribution of i in Equation (2) is the probability that a particular coalition with i as a member occurs, assuming

[12] Myerson [26, p. 16] offers an alternative interpretation: "With nontransferable utility, we have no grounds for interpersonal comparison of utility, so we may feel free to rescale either player's utility separately by a positive scaling factor or utility weight λ_i. Now, in the rescaled version of the game, pretend that the weighted-utility payoffs are transferable."

that all $|N|!$ orderings are equally likely. In this way, the Shapley value allocates each player their marginal contribution averaged over all possible orderings (permutations) of the players. For any TU game the Shapley value exists and has the following properties, among other characteristics [36]: (i) uniqueness, (ii) symmetry: any two players that are treated identically by characteristic function $\omega(\cdot)$ have equal Shapley value allocations, and (iii) (Pareto) efficiency, the gains of the grand coalition must be fully distributed:

$$\sum_{i \in N} \varphi_i = \omega(N). \tag{3}$$

These properties make the Shapley value the predominant solution concept for cooperative games. As a reminder, the Shapley value is also individually rational.

Third, $[\varphi_i(\omega, \boldsymbol{\lambda})/\lambda_i]_{i \in N}$ is the *Shapley value (λ-transfer value) for the NTU game* if it is feasible for the grand coalition in the NTU game. This is the case when $[\varphi_i(\omega, \boldsymbol{\lambda})/\lambda_i]_{i \in N} \in V(N)$. If it is not feasible, then the procedure must be redone for another vector $\boldsymbol{\lambda'} \neq \boldsymbol{\lambda}$ until a solution is found. Shapley [37, 38] establishes that such a solution exists.[13] Most importantly, in establishing feasibility we endogenously derive the fee, f, paid by the taker to each maker in the anonymity set. An example is given in the following section.

4 A Three-Player Anonymity Market

In a 3-player anonymity market the taker specifies that it desires two makers in the associated anonymity set. Let player t be the taker and players 1 and 2 be the makers. For single-player coalitions the NTU characteristic functions, which specify the vector of maximum utilities achievable by each member of a coalition when that coalition is formed, are

$$V(\{t\}) = \{x_t \mid x_t \leq \delta D - F\}, \tag{4}$$

this reflects the outside option for the taker (the mix); and

$$V(\{i\}) = \{x_i \mid x_i \leq 0 : i = 1, 2\} \text{ for makers 1 and 2.} \tag{5}$$

Makers require a taker for an anonymity market to form. Without a taker, a maker's utility is normalized to zero.

For 2-player coalitions, in a coalition of $\{t, 1\}$ or $\{t, 2\}$ each player remains anonymous with probability $1/2$. It is the existence of these intermediate coalitions that separates this analysis from 3-player bargaining. Consequently,

$$V(\{t, 1\}) = \{(x_t, x_1) \mid x_t \leq 1/2 D - f, x_1 \leq 1/2 d + f\}\,; \tag{6}$$

$$V(\{t, 2\}) = \{(x_t, x_2) \mid x_t \leq 1/2 D - f, x_2 \leq 1/2 d + f\}\,. \tag{7}$$

[13] As the proof is based on a fixed point theorem it does not guarantee uniqueness. We are unaware of any example in the literature where multiple weights are derived that lead to alternative NTU Shapley values. If multiple fixed points exist, selecting among them is a well-defined problem. A natural criterion would be to maximize the taker's payoff.

Notice how (i) anonymity is akin to a public good that is (probabilistically) produced when an anonymity set/coalition is formed, and (ii) only the taker is paying for anonymity. Consequently, no anonymity is produced in a $\{1,2\}$ maker-only coalition because neither maker pays the other to create anonymity. To wit, makers are direct suppliers of anonymity to the taker. As a byproduct makers supply anonymity to each other. Makers do not contract directly for anonymity amongst themselves:

$$V(\{1,2\}) = \{(x_1, x_2) \mid x_1 \leq 0, x_2 \leq 0\}\,. \tag{8}$$

Finally, the probability of retaining one's identity is increased to $2/3$ in the grand coalition, $N = \{t, 1, 2\}$:

$$V(N) = \{(x_t, x_1, x_2) \mid \; x_t \leq 2/3D - 2f, x_1 \leq 2/3d + f, x_2 \leq 2/3d + f\,\}. \tag{9}$$

Note that in all of these specifications, the anonymity fee in the NTU game is not taken as given, but is an unknown to be solved for.

Following the procedure outlined above, the solution is derived by following these three steps. First, set $\boldsymbol{\lambda} = (\lambda_t, \lambda_1, \lambda_2) = (1,1,1)$.[14] Second, create the worth functions that are consistent with this $\boldsymbol{\lambda}$ and solve for the Shapley value of the TU game. Third, demonstrate feasibility of the NTU solution for this $\boldsymbol{\lambda}$.

The associated worth functions, which can be regarded as characteristic functions for the TU game derived from the NTU game, are constructed via Equation (1). Therefore the worth functions are

$$\omega(\{t\}) = \delta D - F; \tag{10}$$

$$\omega(\{1\}) = \omega(\{2\}) = 0; \tag{11}$$

$$\omega(\{t,1\}) = 1/2D + 1/2d; \tag{12}$$

$$\omega(\{t,2\}) = 1/2D + 1/2d; \tag{13}$$

$$\omega(\{1,2\}) = 0; \tag{14}$$

$$\omega(N) = 2/3D + 4/3d. \tag{15}$$

Once the worth functions have been derived, the result is a TU game. The Shapley value is calculated according to the formula in Equation (2). The Shapley values for this TU game are (derivation in Appendix A),

$$\varphi_t(\omega, \boldsymbol{\lambda}) = \frac{14}{36}D + \frac{22}{36}d + \frac{1}{3}(\delta D - F); \text{ and} \tag{16}$$

$$\varphi_1(\omega, \boldsymbol{\lambda}) = \varphi_2(\omega, \boldsymbol{\lambda}) = \frac{5}{36}D + \frac{13}{36}d - \frac{1}{6}(\delta D - F). \tag{17}$$

To establish the NTU Shapley values, feasibility requires:

$$(\varphi_t(\omega, \boldsymbol{\lambda})/\lambda_t, \varphi_1(\omega, \boldsymbol{\lambda})/\lambda_1, \varphi_2(\omega, \boldsymbol{\lambda})/\lambda_2) \in V(N). \tag{18}$$

Recall that $(\lambda_t, \lambda_1, \lambda_2) = (1,1,1)$; hence, feasibility for the taker requires that $\varphi_t(\omega, \boldsymbol{\lambda}) \leq 2/3D - 2f$; i. e.,

$$\frac{14}{36}D + \frac{22}{36}d + \frac{1}{3}(\delta D - F) \leq \frac{2}{3}D - 2f. \tag{19}$$

Solving for f yields the following result.

[14] This is consistent with finding a solution under the condition $\lambda_t = \lambda_1 = \lambda_2$ (where all λ's are finite), which yields an equivalent result.

Result 1 *The fee associated with Shapley value of a 3-player (one taker, two makers) anonymity set is*

$$f = \frac{5}{36}D - \frac{11}{36}d - \frac{1}{6}(\delta D - F). \tag{20}$$

Proof. What remains is to show that the solution is feasible for the makers. Given the definition of $V(N)$, feasibility also requires that $\varphi_1(\omega, \boldsymbol{\lambda}) \leq 2/3d + f$ and $\varphi_2(\omega, \boldsymbol{\lambda}) \leq 2/3d + f$. Substituting in the value for f in Equation (20), $2/3d + f = \frac{5}{36}D + \frac{13}{36}d - \frac{1}{6}(\delta D - F)$, which according to Equation (17) is the solution for both $\varphi_1(\omega, \boldsymbol{\lambda})$ and $\varphi_2(\omega, \boldsymbol{\lambda})$.

This result establishes that the Shapley value can be used to characterize the fees for anonymity as a function of the taker's subjective identity valuation (D), the makers' subjective identity valuation (d) and the outside alternative (δ and F). Several novel observations emerge from this result. First, it cannot be the case that anonymity/identity is symmetrically valued across takers and makers ($D = d$) because then $f < 0$.[15] This would require makers to pay the taker. As such an arrangement is never observed, it must be the case that $D \gg d$. Second, the maker fee, f, is increasing in the outside fee, F, but only by a factor of one-sixth. Third, one can re-write the fee in (20) as

$$f = \frac{5 - 6\delta}{36}D - \frac{11}{36}d + \frac{1}{6}F, \tag{21}$$

in which case it is clear that non-fee based characteristics of the outside option, captured by δ, contribute significantly to determining the fee in a one taker, two maker market. Recall that δ is a function of both the taker's time preferences and the size of the anonymity set generated by the outside option (mix). In particular, Möser and Böhme [24] posit that takers' time preference cause takers to pay a premium for immediate anonymity services. Such a low discount factor implies a low value of δ, perhaps approaching zero.

5 The Price of Anonymity

Now we derive the anonymity fee for an arbitrary number of makers, m. As the makers are assumed to be identical, what matters in expressing the NTU characteristic function for a coalition is the number of makers involved. Let:

- m be the total number of makers that the taker seeks in the anonymity set;
- $n = 1, 2, \ldots, m$ be the number of makers in a coalition;
- $\{t, n\}$ is a coalition with the taker, t, and n makers;
- $\{t\}$ is a coalition where the taker instead uses the outside option (mix);
- $\{n\}$ is a coalition with n makers and no taker.

[15] The term $\delta D - F$ must be nonnegative; otherwise, the outside alternative is not viable for the taker.

Then the NTU characteristic functions for the game are

$$V(\{t\}) = \{x_t \mid x_t \le \delta D - F\}\,; \tag{22}$$

$$V(\{n\}) = \{(x_i) \mid x_i \le 0 \ \forall i : 1 \le i \le n\}\,; \tag{23}$$

$$V(\{t,n\}) = \Big\{\big(x_t, (x_i)\big) \mid x_t \le \frac{n}{n+1}D - nf; x_i \le \frac{n}{n+1}d + f \quad \forall i : 1 \le i \le n\Big\}. \tag{24}$$

The worth functions for a coaltition, S, in the λ-transfer game are derived by setting $\lambda_i = 1$ for all $i \in S$ and applying Equation (1):

$$\omega(\{t\}) = \delta D - F; \tag{25}$$

$$\omega(\{n\}) = 0 \ \forall n : 1 \le n \le m; \tag{26}$$

$$\omega(\{t,n\}) = \frac{n}{n+1}D + \frac{n^2}{n+1}d. \tag{27}$$

Theorem 2. *The Shapley values for an anonymity set with one taker, t, and m makers are*

$$\frac{\varphi_t(\omega, \boldsymbol{\lambda})}{\lambda_t} = \frac{\delta D - F}{m+1} + \frac{D}{m+1}\sum_{n=1}^{m}\frac{n}{n+1} + \frac{d}{m+1}\sum_{n=1}^{m}\frac{n^2}{n+1} \ \text{; and} \tag{28}$$

$$\frac{\varphi_i(\omega, \boldsymbol{\lambda})}{\lambda_i} = \frac{D}{m\cdot(m+1)}\sum_{n=1}^{m}\frac{1}{n+1} + \frac{d}{m\cdot(m+1)}\sum_{n=1}^{m}\frac{n^2+n-1}{n+1} - \frac{\delta D - F}{m\cdot(m+1)}, \tag{29}$$

for all makers $i \in \{1, \dots, m\}$.

See Appendix B for the proof. An alternative representation using harmonic numbers instead of finite sums is given in Appendix C.

The associated anonymity fee is derived from the requirement that φ_t/λ_t must be feasible for $V(\{t,m\})$; i.e., $\varphi_t/\lambda_t \le \frac{m}{m+1}D - mf$. From Equation (28) and given $\lambda_t = 1$, this becomes

$$\frac{\varphi_t}{\lambda_t} = \frac{\delta D - F}{m+1} + \frac{D}{m+1}\sum_{n=1}^{m}\frac{n}{n+1} + \frac{d}{m+1}\sum_{n=1}^{m}\frac{n^2}{n+1} \le \frac{m}{m+1}D - mf. \tag{30}$$

Setting the two sides of the inequality equal to each other and solving for f yields the following characterization.

Corollary 1. *The fee associated with the Shapley value for an anonymity set with $m \ge 1$ makers is*

$$f = \frac{D}{m+1} - \frac{D}{m\cdot(m+1)}\sum_{n=1}^{m}\frac{n}{n+1} - \frac{d}{m\cdot(m+1)}\sum_{n=1}^{m}\frac{n^2}{n+1} - \frac{\delta D - F}{m\cdot(m+1)}. \tag{31}$$

Once again, the anonymity fee, f, is increasing in the outside fee, F. Yet the increase in f due to F is decreasing in the number of makers, m. Specifically, f is increasing in F by a factor of $1/(m(m+1))$. The anonymity fee is also increasing in the taker identity, D, and decreasing in the makers' identity, d. In particular, the pricing of anonymity has remained a puzzle because the production of anonymity generates a positive externality in that all agents who supply anonymity also receive it as a good [24]. We provide the first characterization of the relation between f and d.

Regarding computational aspects, observe that the calculation of the Shapley value and its associated fee requires linear time in m at fixed precision, and polynomial time at arbitrary precision. Hence, our solution offers an efficient algorithm to determine the price of anonymity.

6 Conclusion

We have specified a cooperative game that captures the features of anonymity markets known as CoinJoins. More generally, our model captures the fact that in anonymity markets it is often the case that one demand-side participant ("taker") pays for anonymity, but all participants of a trade, including $m > 1$ "makers" on the supply side, receive anonymity if the trade happens. This is novel from a game-theoretic perspective as well because one member of a coalition is paying a fee to all other members to form the coalition even though *all* members utlimately benefit from the resulting coalition. Using the Shapley value as solution concept, we have derived the price of anonymity endogenously as a function of the taker's and makers' valuation of their identities, as well as the price and quality of an outside option for the taker. Of particular note is that we are able to characterize the way in which the associated positive externality received by makers (anonymity) affects the fee paid by the taker. The model is general enough to inform the design of all anonymity schemes that create anonymity by coordinating observable activities in order to make them look alike. These include anonymous communication systems and their applications in electronic voting and privacy-enhancing middleware, cryptocurrency transaction systems, and possibly the organization of dark pools in finance.

The model establishes a broad canvas for follow-up work. An immediate example is that alternative cooperative solution concepts exist for NTU games; most notably, the core, and the NTU values introduced by Harsanyi [16] and Maschler-Owen [20]. The Shapley value is utilitarian in that it maximizes the weighted sum of the individual payoffs in *each* coalition. This is only the case for the grand coalition in the Harsanyi value. Instead, the Harsanyi value is equitable in that weighted net utility gains are equal for each individual in a coalition. By investigating these alternative solutions one may gather whether CoinJoins may be able to compete on different coalitional ethics. Our results can also be experimentally tested via behavioral techniques in which subjects (a taker and makers) are endowed with values for their respective identities. One could then see how fees vary with alternative magnitues of indentity values and also the amount of anonymity provided. In addition, the question of whether the fee varies with the external fee for anonymity mixes can be investigated both experimentally and via comparisons of the prices in CoinJoins and mixes.

In its present form, the game is one-shot. It does not capture the reported practice of repeated anonymization [25], which could increase anonymity as the cardinality of the joint anonymity set grows. Hence, a direction for future work is to consider alternative payoff functions than the global passive adversary (GPA) used here, who guesses exactly once with uniform probability. For example, a straightforward extension is to model varying risk appetite of takers by adjusting the NTU characteristic function. The problem gets substantially more complicated if non-identical and potentially adversarial makers are considered. Möser and Böhme [24] speculate that attackers could try to actively participate in CoinJoin transactions, possibly with multiple identities, in order to extract information about the composition of the anonymity set and eventually de-anonymize the taker. Such attackers could offer their enticing services at subsidized fees, below the Shapley value, in order to increase their odds of being selected. This scenario clearly requires an analysis based on characteristic functions that are derived from an underlying noncooperative game. The same applies to situations where takers choose m out of a large number of competing makers. Let us emphasize again that, although we give solutions for arbitrary m, the present theory does not lend itself to interpretations where m is endogenous.

Other directions of potential interest are to consider (opportunity) costs of engaging in anonymous transactions; to endogenize the quality of the outside option, δ, by modeling the behavior of the mix operator under incentive regimes as suggested by Bonneau et al. [7]; to consider transactions with coins of different quality as proposed by Abramova et al. [1]; to relax the strict dichotomy between taker and makers and replace it with heterogenous agents in some preference space. Finally, the mechanism design required to elicit the fair price of anonymity derived here is up to future work. JoinMarket, the platform that inspired this line of research, seems to employ ad-hoc mechanisms, as witnessed by many changes in the course of its history. And there seems to be room for improvement on the mechanism as well as need for a more principled approach towards constructing anonymity markets.

Acknowledgement We thank the anonymous reviewers for helpful comments. The second author is funded by the German Bundesministerium für Bildung und Forschung (BMBF) under grant agreement 16KIS0382.

References

[1] Abramova, S., Schöttle, P., Böhme, R.: Mixing coins of different quality: A game-theoretic approach. In: Brenner, M., et al. (eds.) Proceedings of the 4th Workshop on Bitcoin and Blockchain Research. Lecture Notes in Computer Science, vol. 10323, pp. 280–297. Springer, Berlin, Heidelberg (2017)

[2] Acquisti, A., Dingledine, R., Syverson, P.: On the economics of anonymity. In: Wright, R.N. (ed.) Financial Cryptography and Data Security. Lecture Notes in Computer Science, vol. 2742, pp. 84–102. Springer, Berlin, Heidelberg (2003)

[3] Acquisti, A., Taylor, C., Wagman, L.: The economics of privacy. Journal of Economic Literature 54(2), 442–492 (2016)

[4] Acquisti, A., Varian, H.R.: Conditioning prices on purchase history. Marketing Science 24(3), 367–381 (2005)

[5] Androulaki, E., Raykova, M., Srivatsan, S., Stavrou, A., Bellovin, S.M.: PAR: Payment for anonymous routing. In: Borisov, N., Goldberg, I. (eds.) Privacy Enhancing Technologies. Lecture Notes in Computer Science, vol. 5134, pp. 219–236. Springer, Berlin, Heidelberg (2008)

[6] Böhme, R., Christin, N., Edelman, B., Moore, T.: Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives 29(2), 213–238 (2015)

[7] Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J.A., Felten, E.W.: Mixcoin: Anonymity for Bitcoin with accountable mixes. In: Christin, N., Safavi-Naini, R. (eds.) Financial Cryptography and Data Security. Lecture Notes in Computer Science, vol. 8437, pp. 486–504. Springer, Berlin, Heidelberg (2014)

[8] Chessa, M., Grossklags, J., Loiseau, P.: A game-theoretic study on non-monetary incentives in data analytics projects with privacy implications. In: Cédric Fournet, Michael W. Hicks, L.V. (ed.) Proceedings of the Computer Security Foundations Symposium (CSF). pp. 90–104. IEEE Computer Society (2015)

[9] Chessa, M., Loiseau, P.: A cooperative game-theoretic approach to quantify the value of personal data in networks. In: Proceedings of the 12th Workshop on the Economics of Networks, Systems and Computation. No. 9, ACM, Cambridge, MA (2017)

[10] Díaz, C., Seys, S., Claessens, J., Preneel, B.: Towards measuring anonymity. In: Syverson, P., Dingledine, R. (eds.) Workshop on Privacy Enhancing Technologies. Lecture Notes in Computer Science, vol. 2482. Springer, Berlin, Heidelberg (2003)

[11] Dingledine, R., Mathewson, N., Syverson, P.: Tor: The second-generation onion router. In: 13th USENIX Security Symposium. USENIX Association (2004)

[12] Dwork, C.: Differential privacy: A survey of results. In: Theory and Applications of Models of Computation, pp. 1–19. Springer (2008)

[13] Franz, E., Jerichow, A., Wicke, G.: A payment scheme for mixes providing anonymity. In: Lamersdorf, W., Merz, M. (eds.) Trends in Distributed Systems for Electronic Commerce. Lecture Notes in Computer Science, vol. 1402, pp. 94–108. Springer, Berlin, Heidelberg (1998)

[14] Friedman, E., Resnick, P.: The social cost of cheap pseudonyms. Journal of Economics and Management Strategy 10(2), 173–199 (2001)

[15] Gkatzelis, V., Aperjis, C., Huberman, B.A.: Pricing private data. Electronic Markets 25(2), 109–123 (2015)

[16] Harsanyi, J.C.: A simplified bargaining model for the n-person cooperative game. International Economic Review 4(2), 194–220 (1963)

[17] Jansen, R., Johnson, A., Syverson, P.: LIRA: Lightweight incentivized routing for anonymity. In: Proceedings of the Network and Distributed System Security Symposium (NDSS). The Internet Society (2013)

[18] Kleinberg, J., Papadimitriou, C.H., Raghavan, P.: On the value of private information. In: Proceedings of the 8th Conference on Theoretical Aspects of Rationality and Knowledge (TARK). pp. 249–257. ACM, New York (2001)
[19] Köpsell, S.: Low latency anonymous communication – How long are users willing to wait? In: Müller, G. (ed.) Emerging Trends in Information and Communication Security (Proc. of ETRICS). Lecture Notes in Computer Science, vol. 3995, pp. 221–237. Springer, Berlin, Heidelberg (2006)
[20] Maschler, M., Owen, G.: The consistent Shapley value for games without sidepayments. In: Selten, R. (ed.) Rational Interaction. pp. 5–12. Springer, New York (1992)
[21] Maxwell, G.: CoinJoin: Bitcoin privacy for the real world (2013), https://bitcointalk.org/index.php?topic=279249.0
[22] Meiklejohn, S., Orlandi, C.: Privacy-enhancing overlays in Bitcoin. In: Brenner, M., Christin, N., Johnson, B., Rohloff, K. (eds.) Financial Cryptography and Data Security, 2nd Workshop on BITCOIN Research. Lecture Notes in Computer Science, vol. 8976, pp. 127–141. Springer, Berlin, Heidelberg (2015)
[23] Möser, M., Böhme, R.: Join me on a market for anonymity. In: Workshop on the Economics of Information Security (WEIS). Berkeley, CA (2016)
[24] Möser, M., Böhme, R.: The price of anonymity: Empirical evidence from a market for Bitcoin anonymization. Journal of Cybersecurity (August 2017)
[25] Möser, M., Böhme, R., Breuker, D.: An inquiry into money laundering tools in the Bitcoin ecosystem. In: Proceedings of the APWG E-Crime Researchers Summit. pp. 1–14. IEEE, San Francisco (2013)
[26] Myerson, R.B.: Fictitious-transfer solutions in cooperative game theory. In: Selten, R. (ed.) Rational Interaction. Essays in the Honor of John C. Harsanyi. pp. 13–33. Springer, Berlin, Heidelberg (1992)
[27] Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S.: Bitcoin and Crypocurrency Technologies. A Comprehensive Introduction. Princeton University Press, Princeton, NJ (2016)
[28] Owen, G.: Game Theory. W. B. Saunders, Philadelphia (1968)
[29] Padilla, A.J., Pagano, M.: Sharing default information as a borrower discipline device. European Economic Review 44(10), 1951–1980 (2000)
[30] Pagano, M., Jappelli, T.: Information sharing in credit markets. Journal of Finance 48(5), 1693–1718 (1993)
[31] Peleg, B., Sudhölter, P.: Introduction to the Theory of Cooperative Games. Kluwer Academic, Boston, 2nd edn. (2007)
[32] Pfitzmann, A., Köhntopp, M.: Anonymity, unobservability, and pseudonymity – a proposal for terminology. In: Federrath, H. (ed.) Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science, vol. 2009, pp. 1–9. Springer, Berlin, Heidelberg (2001)
[33] Saad, W., Han, Z., Debbah, M., Hjørungnes, A., Başar, T.: Coalitional game theory for communication networks: A tutorial (2009), https://arxiv.org/abs/0905.4057
[34] Sandler, T.: Collective Action. University of Michigan Press, Ann Arbor (1992)

[35] Serjantov, A., Danezis, G.: Towards an information theoretic metric for anonymity. In: Syverson, P., Dingledine, R. (eds.) Workshop on Privacy Enhancing Technologies. Lecture Notes in Computer Science, vol. 2482. Springer, Berlin, Heidelberg (2003)
[36] Shapley, L.S.: A value for n-person games. In: Kuhn, H.W., Tucker, A.W. (eds.) Contributions to the Theory of Games. vol. II, pp. 307–317. Princeton University Press, Princeton, NJ (1953)
[37] Shapley, L.S.: Utility comparisons and the theory of games. In: La Décision: Aggrégation et Dynamique des Orders de Préférences. pp. 251–263. Éditions du Centre Nationale de la Recherche Scientifique, Paris (1969)
[38] Shapley, L.S.: Utility comparisons and the theory of games. In: Roth, A.E. (ed.) The Shapley Value. Essays in Honor of Lloyd S. Shapley. pp. 307–319. Cambridge University Press (1988)
[39] Sweeney, L.: k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10(5), 571–588 (2002)
[40] Zhu, H.: Do dark pools harm price discovery? Review of Financial Studies 27(3), 747–780 (2014)

APPENDIX

A Shapley Value Derivation for the 3-Player Example

Following the formula given in Equation (2), the Shapley value for the taker, t, with the makers as players 1 and 2, is

$$\begin{aligned}\varphi_t(\omega, \boldsymbol{\lambda}) =& \frac{1}{3}\big(\omega(N) - \omega(\{1,2\})\big) + && \text{(grand coalition)}\\ & \frac{1}{6}\big(\omega(\{t,1\}) - \omega(\{1\})\big) + && \text{(taker \& maker 1)}\\ & \frac{1}{6}\big(\omega(\{t,2\}) - \omega(\{2\})\big) + && \text{(taker \& maker 2)}\\ & \frac{1}{3}\big(\omega(\{t\}) - \omega(\emptyset)\big). && \text{(taker alone)}\end{aligned} \tag{32}$$

Substituting in the worth function values, Eqs. (10)–(15),
(by convention, $\omega(\emptyset) = 0$):

$$\varphi_t(\omega, \boldsymbol{\lambda}) = \frac{1}{3}\left(\frac{2}{3}D + \frac{4}{3}d\right) + \frac{1}{6}\left(\frac{1}{2}D + \frac{1}{2}d\right) + \frac{1}{6}\left(\frac{1}{2}D + \frac{1}{2}d\right) + \frac{1}{3}\left(\delta D - F\right). \tag{33}$$

Aggregating terms,

$$\varphi_t(\omega, \boldsymbol{\lambda}) = \left(\frac{2}{9} + \frac{1}{12} + \frac{1}{12}\right) D + \left(\frac{4}{9} + \frac{1}{12} + \frac{1}{12}\right) d + \frac{1}{3}\left(\delta D - F\right) \tag{34}$$

and simplifying:

$$= \frac{14}{36} D + \frac{22}{36} d + \frac{1}{3} (\delta D - F) . \tag{35}$$

Using Equation (2) to calculate the Shapley value for player 1, who is a maker:

$$\begin{aligned} \varphi_1(\omega, \boldsymbol{\lambda}) = & \frac{1}{3} \big(\omega(N) - \omega(\{t, 2\})\big) + && \text{(grand coalition)} \\ & \frac{1}{6} \big(\omega(\{t, 1\}) - \omega(\{t\})\big) + && \text{(taker \& maker 1)} \\ & \frac{1}{6} \big(\omega(\{1, 2\}) - \omega(\{2\})\big) + && \text{(both makers)} \\ & \frac{1}{3} \big(\omega(\{1\}) - \omega(\emptyset)\big). && \text{(maker 1 alone)} \end{aligned} \tag{36}$$

Substituting in the worth function values:

$$\varphi_1(\omega, \boldsymbol{\lambda}) = \frac{1}{3} \left(\frac{2}{3} D + \frac{4}{3} d - \frac{1}{2} D - \frac{1}{2} d \right) + \frac{1}{6} \left(\frac{1}{2} D + \frac{1}{2} d - (\delta D - F) \right) . \tag{37}$$

Aggregating terms and simplifying:

$$\varphi_1(\omega, \boldsymbol{\lambda}) = \left(\frac{2}{9} - \frac{1}{6} + \frac{1}{12} \right) D + \left(\frac{4}{9} - \frac{1}{6} + \frac{1}{12} \right) d - \frac{1}{6} (\delta D - F) \tag{38}$$

$$= \frac{5}{36} D + \frac{13}{36} d - \frac{1}{6} (\delta D - F) . \tag{39}$$

By the symmetry property of the Shapley value, $\varphi_2(\omega, \boldsymbol{\lambda}) = \varphi_1(\omega, \boldsymbol{\lambda})$. □

B Proof of Theorem 2

The proof consists of three parts.

B.1 Shapley value for the taker

Proof. From Equation (2), the coefficient on $\omega(\{t\}) - \omega(\emptyset) = \delta D - F$ in the Shapley value is $1/N = 1/(m+1)$. This is the first term in Equation (28).

Given m makers, there are $\binom{m}{n} = \frac{m!}{n!\,(m-n)!}$ combinations of coalitions that can be expressed as $S = \{t, n\}$. Note also that $N = m + 1$. From Equation (2), the coefficient on each coalition $\{t, n\}$ in the Shapley value is

$$\frac{(|S| - 1)!\,(N - |S|)!}{N!} = \frac{\big((n+1) - 1\big)!\,\big((m+1) - (n+1)\big)!}{(m+1)!} = \frac{n!\,(m-n)!}{(m+1)\,m!} . \tag{40}$$

For each coalition, $\{t, n\}$, the marginal contribution for the taker in the formula for φ_t is $\big(\omega(\{t, n\}) - \omega(\{n\})\big) = \omega(\{t, n\})$. In aggregate, the partial sum in the Shapley value for a specific n is the product of the following three terms: (i) the number of $\{t, n\}$ coalitions, (ii) the Shapley coefficient that is common to each $\{t, n\}$ coalition, (40), and (iii) $\big(\omega(\{t, n\}) - \omega(\{n\})\big) = \omega(\{t, n\})$, from Equation (27):

$$\frac{m!}{n!\,(m-n)!} \times \frac{n!\,(m-n)!}{(m+1)\,m!} \times \omega(\{t, n\} = \frac{1}{m+1}\left(\frac{n}{n+1}D + \frac{n^2}{n+1}d\right). \tag{41}$$

Summing this over all possible $n = 1, \ldots, m$ yields the final two terms in Equation (28). This completes the derivation of the Shapley value for the taker, φ_t/λ_t, given that $\lambda_t = 1$.

B.2 Shapley value for the makers

In deriving the Shapley value for maker i, φ_i, note that for any coalition, $\hat{S}$, where $t \notin \hat{S}, \omega(\hat{S}) = 0$. This simplifies the remaining steps for calculating the Shapley value for i to only those worth functions whose coalitions include a taker, t, as a member; i. e., $\omega(\{t, n\})$.

Proof. For any maker, i, there is one and only one $\{t, i\}$ coalition. The coefficient on this coalition in the Shapley value is

$$\frac{(2-1)!\,\big((m+1)-2\big)!}{(m+1)!} = \frac{(m-1)!}{(m+1)!} = \frac{1}{m \cdot (m+1)}. \tag{42}$$

As $\omega(\{t, i\}) = {}^1\!/\!_2 D + {}^1\!/\!_2 d$ and $\omega(\{t, i\} \setminus \{i\}) = \delta D - F$, the part of the calculation of φ_i that corresponds to the marginal contribution of i to $\{t, i\}$ is:

$$\frac{1}{m \cdot (m+1)}\Big(\omega(\{t, i\}) - \omega(\{t, i\} \setminus \{i\})\Big) = \frac{1}{m \cdot (m+1)}\left(\frac{1}{2}D + \frac{1}{2}d - (\delta D - F)\right). \tag{43}$$

From Equation (2) the calculation of the Shapley value is now:

$$\begin{aligned} \varphi_i = {} & \frac{1}{m \cdot (m+1)}\left(\frac{1}{2}D + \frac{1}{2}d - (\delta D - F)\right) + \\ & + \sum_{\substack{i \in \left\{\{t,n\} \mid n \geq 2\right\}, \\ \{t,n\} \subseteq N}} \frac{(|S|-1)!\,(N-|S|)!}{N!} \times \Big(\omega(\{t, n\}) - \omega(\{t, n\} \setminus \{i\})\Big). \end{aligned} \tag{44}$$

The remainder of the coalitions where $i \in \{t, n\}$ require $n \geq 2$. For a given n, the number of coalitions for which maker i is a member, $i \in \{t, n\}$, is

$$\binom{m-1}{n-1} = \frac{(m-1)!}{(n-1)!\,\big((m-1)-(n-1)\big)!} = \frac{(m-1)!}{(n-1)!\,(m-n)!}. \tag{45}$$

Given n, the coefficient in the Shapley value for the marginal contribution, $\omega(\{t,n\}) - \omega(\{t,n\} \setminus \{i\})$, of maker i is

$$\frac{\big((n+1)-1\big)!\,\big((m+1)-(n+1)\big)!}{(m+1)!} = \frac{n!\,(m-n)!}{(m+1)!}. \tag{46}$$

To calculate $\omega(\{t,n\}) - \omega(\{t,n\} \setminus \{i\})$, use Equation (27) and observe that

$$\omega(\{t,n\} \setminus \{i\}) = \omega(\{t,n-1\} = \frac{n-1}{n}D + \frac{(n-1)^2}{n}d. \tag{47}$$

Consequently, i's marginal contribution to the coalition $\{t,n\}$ is

$$\omega(\{t,n\}) - \omega(\{t,n\} \setminus \{i\}) = \frac{1}{n\cdot(n+1)}D + \frac{n^2+n-1}{n\cdot(n+1)}d. \tag{48}$$

Hence, when $n \geq 2$, for a given value of n the partial sum within the Shapley value corresponding to $\{t,n\}$ such that $i \in \{t,n\}$ is the product:

$$\underbrace{\frac{(m-1)!}{(n-1)!\,(m-n)!}}_{\text{Equation (45)}} \times \underbrace{\frac{n!\,(m-n)!}{(m+1)!}}_{\text{Equation (46)}} \times \underbrace{\left(\frac{1}{n\cdot(n+1)}D + \frac{n^2+n-1}{n\cdot(n+1)}d\right)}_{\text{Equation (48)}}$$

$$= \frac{1}{m\cdot(m+1)} \times \left(\frac{1}{n+1}D + \frac{n^2+n-1}{n+1}d\right). \tag{49}$$

Summing this over all possible $n = 2, \ldots, m$ yields:

$$\frac{D}{m\cdot(m+1)}\sum_{n=2}^{m}\frac{1}{n+1} + \frac{d}{m\cdot(m+1)}\sum_{n=2}^{m}\frac{n^2+n-1}{n+1}. \tag{50}$$

To derive φ_i, combine this with the Shapley value term for $\{t,i\}$, Equation (43):

$$\begin{aligned}\varphi_i = {} & \frac{1}{m\cdot(m+1)}\left(\frac{1}{2}D + \frac{1}{2}d - (\delta D - F)\right) + \\ & \frac{D}{m\cdot(m+1)}\sum_{n=2}^{m}\frac{1}{n+1} + \frac{d}{m\cdot(m+1)}\sum_{n=2}^{m}\frac{n^2+n-1}{n+1}.\end{aligned} \tag{51}$$

Aggregating terms:

$$\varphi_i = \frac{D}{m\cdot(m+1)}\sum_{n=1}^{m}\frac{1}{n+1} + \frac{d}{m\cdot(m+1)}\sum_{n=1}^{m}\frac{n^2+n-1}{n+1} - \frac{\delta D - F}{m\cdot(m+1)}. \tag{52}$$

This completes the derivation of the Shapley value for a maker, φ_i/λ_i, given $\lambda_i = 1$.

B.3 Feasibility check

The final step requires verification that φ_i/λ_i is feasible for $V(N)$. This is facilitated using the expressions of φ_t/λ_t and φ_i/λ_i in terms of harmonic numbers, as given in Equations (56) and (57) in Appendix C.

Proof. Recall that the fee, f, given in Equation (31) was derived from the feasibility condition for φ_t/λ_t when $\lambda_t = 1$: $\varphi_t \leq \frac{m}{m+1}D - mf$, yielding $f = \frac{1}{m+1}D - \frac{1}{m}\varphi_t$. The feasibility condition for φ_i/λ_i when $\lambda_i = 1$ is

$$\varphi_i \leq \frac{m}{m+1}d + f = \frac{m}{m+1}d + \frac{1}{m+1}D - \frac{1}{m}\varphi_t. \tag{53}$$

Setting the two sides equal and substituting in the value for φ_t, Equation (56):

$$\begin{aligned}\varphi_i = {} & \frac{m \cdot d}{m+1} + \frac{D}{m+1} - \\ & \frac{1}{m}\left(\frac{\delta D - F + D\,(m - H_{m+1} + 1)}{m+1}\right) + \\ & \frac{1}{m}\left(\frac{d\left(H_{m+1} + \left(\frac{m}{2} - 1\right)(m+1)\right)}{m+1}\right),\end{aligned} \tag{54}$$

which reduces to

$$\varphi_i = \frac{D(H_{m+1} - 1) + d\left(\frac{m^2+m}{2} - H_{m+1} + 1\right) - \delta D + F}{m \cdot (m+1)}. \tag{55}$$

This is exactly the right side of Equation (57). Hence the condition holds under the theorem.

C Alternative Form of Theorem 2 Using Harmonic Numbers

Let H_m denote the m-th harmonic number, i. e., $H_m = \sum_{n=1}^{m} \frac{1}{n}$. Using this shorthand, Equation (28) of Theorem 2 can be rewritten as,

$$\frac{\varphi_t(\omega, \boldsymbol{\lambda})}{\lambda_t} = \frac{\delta D - F + D \cdot (m - H_{m+1} + 1) + d \cdot \left(H_{m+1} + \left(\frac{m}{2} - 1\right)(m+1)\right)}{m+1}; \tag{56}$$

and Equation (29) becomes:

$$\frac{\varphi_i(\omega, \boldsymbol{\lambda})}{\lambda_i} = \frac{D \cdot (H_{m+1} - 1) + d \cdot \left(\frac{m^2+m}{2} - H_{m+1} + 1\right) - \delta D + F}{m \cdot (m+1)}. \tag{57}$$