Trust Is Risk: Games, Network Health and Risk Invariance Algorithms

Orfeas Stefanos Thyfronitis Litos[1] and Dionysis Zindros[2]

[1] University of Edinburgh
[2] National and Kapodistrian University of Athens
o.thyfronitis@ed.ac.uk, dionyziz@di.uoa.gr

Abstract. Trust Is Risk [1] proposes a decentralized reputation system. In an effort to deepen our understanding of the dynamics of networks created by this construction and to provide useful tools that facilitate the completion of purchases, we expand our research in three directions. We firstly describe some games, leveraging approaches from Game Theory. Secondly we introduce measures that gauge the health of such networks using the concepts of connectedness and centrality. We will finally describe several algorithms that redistibute a player's direct trust in a way that a desired indirect trust towards a specific player is achieved.

1 Common Setup

We propose three different kinds of games, all of them finite (but possibly generalizable to the infinite setting). The first consists of one sole strategy where the players do not initially know whether they will be buyers, sellers or nothing at all, this being decided in the last moment. The second game consists of three strategies: buyers, sellers and middlemen. The last game consists of two strategies: creators and consumers. Before delving into the details of each game, we first describe their common elements.

The general approach taken is as follows: After a game is described in detail, each player is assigned a specific strategy and a relevant utility function. All players are considered to follow their respective strategy without deviating from it, except for one player that is allowed to follow any desired strategy; her utility function however remains unchanged. If that player is proven to have an incentive to deviate from her appointed strategy, we can deduce that the given strategies and utility functions do not constitute a Nash equilibrium. If on the other hand we can repeat the aforementioned process (keeping all players except for one honest) for all given strategies and no player has an incetive to deviate, then we will come to the conclusion that the given strategies and utility functions do constitute a Nash equilibrium. This approach is common in game theoretic analyses, given that allowing for all players to be rational and then searching for a Nash equilibrium constitutes a practically intractable problem [daskalakis citation]. Another common approach employed is that of considering only a generic product that all buyers want and all sellers have, and not a variety of different products.

A description of the structure that is common for all three games follows. The game graph has a random initial configuration where every player has a random direct trust towards every other player, as well as a random capital. These values may be uniformly distributed in an interval or may follow another distribution such as the exponential, or may have a high probability of being zero. The exact distribution however is not determined at this point, as it is not yet needed. Further constraints may be applied to each game separately. This distribution will be common knowledge to the players. Transaction fees are not considered.

The players play simultaneously in each round and can do any of the known actions. If two actions conflict (e.g. A reduces $DTr_{A \to B}$ and B steals from $DTr_{A \to B}$ as well), then one of the two actions is chosen with equal probability (50%). To better model a player's actions and the aforementioned conflict resolution, we demand that each change explicitly mentions the source and the destination of the funds for each of her actions. Player A decides on the values of all the following variables. This constitutes a concrete round for A.

$$\forall B, C \in \mathcal{V}, move\left(A, \left(A, B\right), \left(A, C\right)\right) = ?$$
$$\forall B, C \in \mathcal{V}, B \neq A, move\left(A, \left(B, A\right), \left(A, C\right)\right) = ?$$

The first argument is the player who decides, the second argument is from which direct trust to take the funds and the third is to which direct trust to deposit the funds.

To clarify a detail, for any $B \in \mathcal{V}$ (including A), A is not allowed to set $move\left(A, \left(A, B\right), \left(A, B\right)\right)$ to any value different than 0. This choice is made to facilitate the analysis and because in the real-world setting this kind of behaviour has a totally different result, effectively dragging B into an arms race for the higher fee. In the real world case, the exact same reasoning goes for $move\left(A, \left(B, A\right), \left(B, A\right)\right)$. In our case however, the latter move is already not permitted.

Of course there are some constraints for player's A move:

- It makes no sense to deposit to and withdraw from a specific direct trust in the same round. Furthermore, such a possibility would allow for "chain reactions" in the conflict resolution phase that would add unnecessary complications. This constraint applies only to outgoing direct trusts, because incoming direct trusts cannot be increased.

$$\forall B, C, D \in \mathcal{V}, move\left(A, \left(A, B\right), \left(A, C\right)\right) \times move\left(A, \left(A, D\right), \left(A, B\right)\right) = 0$$
$$\wedge$$
$$\forall B, C, D \in \mathcal{V}, move\left(A, \left(A, B\right), \left(A, C\right)\right) \times move\left(A, \left(D, A\right), \left(A, B\right)\right) = 0$$

- One cannot use more funds than are available from a single direct trust.

$$\forall B \in \mathcal{V}, \sum_{C \in \mathcal{V}} move\left(A, \left(A, B\right), \left(A, C\right)\right) \leq DTr_{A \to B}$$
$$\forall B \in \mathcal{V}, \sum_{C \in \mathcal{V}} move\left(A, \left(B, A\right), \left(A, C\right)\right) \leq DTr_{B \to A}$$

If two players try to change the same direct trust, then set the relevant moves of one of the two players (chosen uniformly at random) to 0.

```
resolveConflict(A, B) :
  sum1 = \sum_{C \in V} move(A, (A, B), (A, C))
  sum2 = \sum_{C \in V} move(B, (A, B), (B, C))
  if (sum1*sum2 != 0)
    choice <-$ {A, B}
    if (choice == A)
      \forall C \in V, move(A, (A, B), (A, C)) = 0
    else # if (choice == B)
      \forall C \in V, move(B, (A, B), (B, C)) = 0

resolveAllConflicts() :
  \forall A, B \in V
    resolveConflict(A, B)
    resolveConflict(B, A)
```

`resolveAllConflicts()` is executed after all players choose their moves for a round.
We now move on to describe the individual games.

1.1 Random Roles

All players follow the same strategy, according to which each player is permitted to freely add or steal direct trust from other players. After

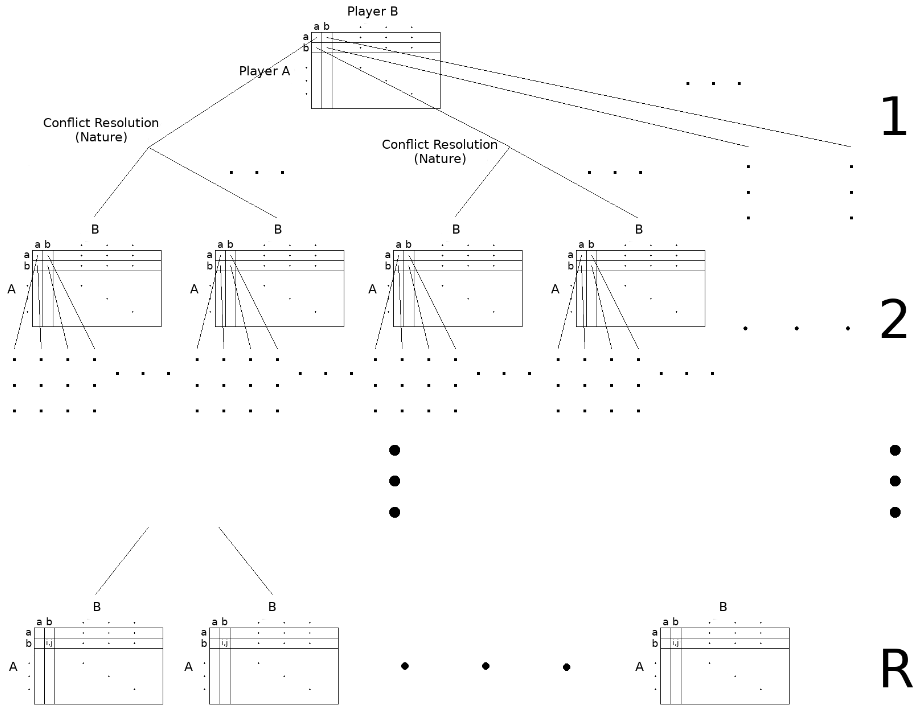

Fig. 1. The general form of the game (inspiration due here, p. 3.)

R rounds (blocks in bitcoin terms) exactly two players are selected at random (these choices follow the uniform distribution). One is dubbed seller and the other buyer. The seller offers a good that costs C, which she values at $C - l$ and the buyer values at $C + l$. The values R, C and l, as well as the uniform distribution with which the buyer and seller are chosen, are common knowledge from the beginning of the game. The exchange completes if and only if $DTr_{Buyer \rightarrow Seller} \geq C$. In this game, Fig 1 would be augmented by one level at the bottom, where Nature chooses the two transacting players.There are three variants of the game, each with a different utility for the players (the first two versions have two subvariants each).

1.1.1 Hoarders

If player A is not chosen to be either buyer or seller, then her utility is equal to $Cap_{A,R}$. Intuitively players do not attach any value to having (incoming or outgoing) direct trust at the end of the game. If the buyer and the seller do not manage to complete the exchange, the buyer's utility is $Cap_{Buyer,R}$. If on the other hand they manage to exchange the good, then the buyer's utility is $Cap_{Buyer,R} + l$. Intuitively these utilities signify that the buyer uses her preexisting Capital to buy. As for the seller there exist two subvariants for her utility:

1. If the exchange is eventually not completed, the seller's utility is $Cap_{Seller,R} - l$. If the exchange takes place, the seller's utility is $Cap_{Seller,R}$. Intuitively, the seller is first obliged to buy the good from the environment at the cost of C.
2. If the exchange is eventually not completed, the seller's utility is $Cap_{Seller,R} + C - l$. If the exchange takes place, the seller's utility is $Cap_{Seller,R} + C$. Intuitively, the seller is handed the good for free by the environment.

1.1.2 Sharers

If player A is not chosen to be either buyer or seller, then her utility is equal to

$$\sum_{\substack{B \in \mathcal{V} \\ B \neq A}} (DTr_{A \rightarrow B,R} + DTr_{B \rightarrow A,R}) + Cap_{A,R} \ .$$

Intuitively, players attach equal value to all the funds they can directly spend, regardless of whether others can spend them as well. If the buyer and the seller do not manage to complete the exchange, the buyer's utility is

$$\sum_{\substack{B \in \mathcal{V} \\ B \neq Buyer}} (DTr_{Buyer \rightarrow B,R} + DTr_{B \rightarrow Buyer,R}) + Cap_{Buyer,R} \ .$$

If on the other hand they manage to exchange the good, then the buyer's utility is

$$\sum_{\substack{B \in \mathcal{V} \\ B \neq Buyer}} (DTr_{Buyer \rightarrow B,R} + DTr_{B \rightarrow Buyer,R}) + Cap_{Buyer,R} + l \ .$$

Intuitively these utilities signify that the buyer uses her preexisting accessible funds to buy. As for the seller there exist two subvariants for her utility:

1. If the exchange is not completed, the seller's utility is

$$\sum_{\substack{B \in \mathcal{V} \\ B \neq Seller}} (DTr_{Seller \rightarrow B,R} + DTr_{B \rightarrow Seller,R}) + Cap_{Seller,R} - l \ .$$

If the exchange takes place, the seller's utility is

$$\sum_{\substack{B\in\mathcal{V}\\B\neq Seller}}(DTr_{Seller\to B,R}+DTr_{B\to Seller,R})+Cap_{Seller,R}\ .$$

Intuitively, the seller is first obliged to buy the good from the environment at the cost of C.

2. If the exchange is not completed, the seller's utility is

$$\sum_{\substack{B\in\mathcal{V}\\B\neq Seller}}(DTr_{Seller\to B,R}+DTr_{B\to Seller,R})+Cap_{Seller,R}+C-l\ .$$

If the exchange takes place, the seller's utility is

$$\sum_{\substack{B\in\mathcal{V}\\B\neq Seller}}(DTr_{Seller\to B,R}+DTr_{B\to Seller,R})+Cap_{Seller,R}+C\ .$$

Intuitively, the seller is handed the good for free by the environment.

1.1.3 Materialists

If player A is not chosen to be either buyer or seller, then her utility is 0. If the buyer and the seller do not manage to complete the exchange, their utility is 0 as well. If on the other hand they manage to exchange the good, then the utility is l for both of them. Intuitively these utilities signify that in this game there is gain only for those who exchange goods and the gain is exactly the difference between the objective value and the subjective value that the relevant parties perceive.

1.2 Buyers, Sellers, Middlemen

Buyers only desire to buy as many products as possible and do not have incoming trust. Sellers only desire to sell as many products as possible in the highest possible price and do not have outgoing trust. Middlemen desire to accumulate capital and are allowed to have both incoming and outgoing trust. Their utility stems only from in-game factors. A more thorough description follows.

1.2.1 Buyers

Buyers initially are provided only with outgoing direct trust towards sellers and middlemen, no Capital or incoming direct trust. They cannot reallocate their outgoing direct trust, only complete purchases of the product from sellers that are trustworthy enough.

Buyers always want to buy the cheapest products provided. To pay for a product, they use the linear program defined in thesis.pdf to aquire the funds needed and directly entrust the necessary part of these funds to the seller. The rest of the funds are kept as Capital. Sellers are supposed to complete their part of the exchange within a constant amount of rounds, r. If the product has arrived after r rounds, during the turn following the arrival of the product the remaining funds are reallocated to the players from whom they were taken in proportional fashion. The way they are reallocated ensures that

$$\forall B \in \mathcal{S}_1, \frac{DTr_{Buyer \to B,i}}{\sum\limits_{C \in \mathcal{S}_1} DTr_{Buyer \to C,i}} = \frac{DTr_{Buyer \to B,i+r}}{\sum\limits_{C \in \mathcal{S}_1} DTr_{Buyer \to C,i+r}} \ ,$$

where $\mathcal{S}_1$ is the set of players from whom the buyer reduced her direct trust to initiate the purchase (this set may also contain the seller).

If the product does not arrive after r rounds, the direct trust to the seller is withdrawn (if it is still available) and all the funds involved (both the price and the surplus funds removed because of the linear program) are reallocated as direct trusts towards the rest of the players in a proportional fashion. The way they are reallocated ensures that

$$\forall B \in \mathcal{S}_2, \frac{DTr_{Buyer \to B,i}}{\sum\limits_{C \in \mathcal{S}_2} DTr_{Buyer \to C,i}} = \frac{DTr_{Buyer \to B,i+r}}{\sum\limits_{C \in \mathcal{S}_2} DTr_{Buyer \to C,i+r}} \ ,$$

where $\mathcal{S}_2 = (\mathcal{V} \setminus \mathcal{S}_1) \setminus \{Buyer, Seller\}$.

The buyers' utilities are straightforward: They are equal to the amount of products they managed to buy throughout the game. This explains why buyers always prefer cheaper products: This way they are able to save funds so that they are hopefully able to buy more products.

1.2.2 Sellers

Sellers initially are provided only with incoming direct trust from buyers and middlemen, no Capital or outgoing direct trust. They also possess a limited supply of products; the quantity of the products each seller initially has is decided randomly by the environment, much like the direct trusts. These products are useless to the sellers, they only want to sell them. The amount of products each seller has is common knowledge.

During each round, each seller decides how many products and for what price (common for all products) she will make available for purchase during the next round. Obviously a seller cannot offer more products than she owns. Furthermore, if a buyer initiated a transaction during the previous round, the buyer must ship the product (reducing the amount of owned products by one). The seller may choose to convert any amount of incoming direct trust that she obtained through selling products into Capital. The seller is not allowed to convert into Capital any incoming direct trust that did not stem from a successful exchange.

A seller's utility is the total amount of incoming direct trust and Capital at the end of the game that stems solely from successfully completed purchases.

1.2.3 Middlemen

Middlemen initially have incoming direct trust from buyers and other middlemen, outgoing direct trust to sellers and other middlemen and some Capital. They do not own or desire any products, they simply want to maximize the amount of Capital they own at the end of the game.

Middlemen have a very permissive strategy: They are allowed any combination of moves that do not violate the basic constraints described in the first section.

The utility of a middleman is simply the Capital the middleman possesses at the end of the game.

1.3 Creators and Consumers

The last type of game described here consists of two categories of players: Creators and consumers. Creators generate shareable products as long as they have sufficient incoming direct trust. Consumers do not have to pay to obtain the products; as a matter of fact, any product can be accessed as long as some baseline. Consumers collectively fund the creators. We may think of creators as artists, researchers, programmers, journalists or other occupations that generate content which can then be easily distributed and shared.

2 Degree of Connectedness

We would like to have a measure of how well connected is the graph. Viewed as a whole, a network with a lot of disconnected cliques should score lower than a loosely connected network. From the perspective of a single player, this measure can be expressed as the expected mean indirect trust, defined incrementally as follows:

$$Tr(A) = \sum_{B \in \mathcal{V} \setminus \{A\}} Tr_{A \to B} \text{ (Total indirect trust for player } A\text{)}$$

$$ETr\left(A\right) = \frac{Tr(A)}{|\mathcal{V} \setminus \{A\}|} = \frac{Tr(A)}{|\mathcal{V}| - 1} \text{ (Expected indirect trust for player } A\text{)}$$

$$EMTr = \frac{1}{|\mathcal{V}|} \sum_{A \in \mathcal{V}} ETr\left(A\right) \text{ (Expected mean indirect trust)}$$

3 Centrality

Another important measure is the network centrality. We propose here some different measures to that end.

3.1 Degree Centrality

One possible approach is the degree centrality [Freeman citation], that can be broken down as in-degree and out-degree centrality. We first define the node in-degree centrality.

$$C_{in}^{d}\left(A\right) = \sum_{B \in \mathcal{V} \setminus \{A\}} DTr_{B \to A}{}^{3} \text{ (Node in-degree centrality)}$$

Let $A^* = \underset{A \in \mathcal{V}}{\operatorname{argmax}}\, C_{in}^{d}\left(A\right)$. The network in-degree centrality is defined as:

$$C_{in}^{d} = \sum_{A \in \mathcal{V}} \left(C_{in}^{d}\left(A^*\right) - C_{in}^{d}\left(A\right) \right) \text{ (Network in-degree centrality)}$$

Similarly, for the out-degree centrality we have:

$$C_{out}^{d}\left(A\right) = \sum_{B \in \mathcal{V} \setminus \{A\}} DTr_{A \to B}{}^{3} \text{ (Node out-degree centrality)}$$

[3] Maybe indirect trust is more intuitive here than direct trust.

Let $A^* = \underset{A \in \mathcal{V}}{\operatorname{argmax}} C^d_{out}(A)$. The network out-degree centrality is defined as:

$$C^d_{out} = \sum_{A \in \mathcal{V}} \left(C^d_{out}(A^*) - C^d_{out}(A) \right) \text{ (Network out-degree centrality)}$$

A problem of these centrality measures is that their unit is the currency used (i.e. Bitcoin) and thus may not always have an intuitive meaning. We would thus like to have a measure of *centalization* that has no units and can take values in the interval $[0,1]$, with 0 corresponding to a network of no centralization (all nodes are equal, e.g. cycle) and 1 to a network with the maximum centralization possible (there is one central vital node for all, e.g. star). A centralization measure that achieves this target is proposed in [Freeman citation]. Here we use the following modified form. For a graph $\mathcal{G}$, the in- and out-centralization are defined as:

$$Cn^d_{in} = \frac{C^d_{in}}{\max C^d_{in}} \text{ (in-degree centralization)}$$
$$Cn^d_{out} = \frac{C^d_{out}}{\max C^d_{out}} \text{ (out-degree centralization)} ,$$

where $\max C^d_{in}$ is defined as the maximum in-degree centrality for any graph with the same number of nodes for which the maximum direct[4] trust is equal to the maximum direct[4] trust of $\mathcal{G}$; $\max C^d_{out}$ is defined equivalently.

3.2 maxFlow Centrality

An alternative measure of centrality for a player $A \in \mathcal{V}$ of a network $\mathcal{G}$ can be defined as the impact that the removal of A would have on the indirect trust between the rest of the players. More specifically, let $\mathcal{G}' = \mathcal{G} \setminus \{A\}$. Then it is:

$$C^{mF}(A) = \sum_{B,C \in \mathcal{V}'} \left(Tr_{\mathcal{G},B \to C} - Tr_{\mathcal{G}',B \to C} \right) \text{ (Node maxFlow centrality)} .$$

We can now follow the same steps as previously for the relevant network definitions. Let A^* be the player with the maximum maxFlow centrality:

$$A^* = \underset{A \in \mathcal{V}}{\operatorname{argmax}} C^{mF}(A) .$$

[4] Maybe indirect trust is more intuitive here than direct trust.

Then the network maxFlow centrality is defined as follows:

$$C^{mF} = \sum_{A \in \mathcal{V}} \left(C^{mF}(A^*) - C^{mF}(A) \right)$$

and the centralization:

$$Cn^{mF} = \frac{C^{mF}}{\max C^{mF}} \text{ (Network maxFlow centralization) },$$

where $\max C^{mF}$ is the maximum centrality for any graph with the same number of nodes for which the maximum direct[5] trust is equal to the maximum direct[5] trust of $\mathcal{G}$.

---

[5] Maybe indirect trust is more intuitive here than direct trust.

Here we can see several possible network health measures. A combination of them will probably do the job.

1. $n := |\mathcal{V}|$ — How many players
2. $e := |\mathcal{E}| - |\{A : DTr_{A \to A} > 0\}|$[6] — How many direct trust lines
3. $\frac{e}{n}$ — Mean direct trust lines per player
4. $DTr := \sum\limits_{\substack{A,B \in \mathcal{V} \\ A \neq B}} DTr_{A \to B}$[6] — How much direct trust in total
5. $\mu := \frac{DTr}{n}$ — Mean direct trust per player
6. $Cap := \sum\limits_{A \in \mathcal{V}} DTr_{A \to A}$ — Total capital
7. $\frac{Cap}{n}$ — Mean capital per player
8. $\frac{DTr - Cap}{n}$ — Mean direct trust minus capital per player
9. $\frac{1}{n} \sum\limits_{A \in \mathcal{V}} \left(\sum\limits_{\substack{B \in V \\ B \neq A}} DTr_{A \to B} - \mu \right)^2$[6] — Outgoing direct trust variance
10. $\frac{1}{n} \sum\limits_{B \in \mathcal{V}} \left(\sum\limits_{\substack{A \in V \\ A \neq B}} DTr_{A \to B} - \mu \right)^2$[6] — Incoming direct trust variance
11. $\frac{Cap}{DTr}$ — Total capital to total direct trust ratio

References

1. Thyfronitis Litos O. S., Zindros D.: Trust Is Risk: A Decentralized Financial Trust Platform. IACR Cryptology ePrint Archive (2017)

[6] Maybe it makes sense to include looped direct trusts (Capital) as well.