Ride the Lightning: The Game Theory of Payment Channels

Zeta Avarikioti(✉), Lioba Heimbach, Yuyi Wang, and Roger Wattenhofer

ETH Zürich, Zürich, Switzerland
{zetavar,hlioba,yuwang,wattenhofer}@ethz.ch

Abstract. Payment channels were introduced to solve various eminent cryptocurrency scalability issues. Multiple payment channels build a network on top of a blockchain, the so-called layer 2. In this work, we analyze payment networks through the lens of network creation games. We identify betweenness and closeness centrality as central concepts regarding payment networks. We study the topologies that emerge when players act selfishly and determine the parameter space in which they constitute a Nash equilibrium. Moreover, we determine the social optima depending on the correlation of betweenness and closeness centrality. When possible, we bound the price of anarchy. We also briefly discuss the price of stability.

Keywords: Blockchain · Payment channels · Layer 2 · Creation game · Network design · Nash equilibrium · Price of anarchy · Price of stability

1 Introduction

1.1 Motivation

Bitcoin [31] and other cryptocurrencies [25,34,35] are electrifying the world. Thanks to a distributed data structure known as the blockchain, cryptocurrencies can execute financial transactions without a trusted central authority. However, every computer participating in a blockchain must exchange, store and verify each and every transaction, and as such the transaction throughput of blockchains is embarrassingly low. The Bitcoin blockchain for instance does not process more than seven transactions per second.

With seven transactions per second, Bitcoin cannot rival established payment systems such as Visa, WeChatPay, or PayPal. Consequently, various research groups have proposed a blockchain paradigm shift – *payment channels* [17,32,33]. All payment channels follow the same basic principle: Instead of sending every transaction to the blockchain, transactions are only exchanged between the involved parties. If Alice and Bob expect to exchange multiple payments, they can establish a payment channel. The channel is set up with a blockchain funding transaction. Once the channel is available, Alice and Bob exchange all

J. Bonneau and N. Heninger (Eds.): FC 2020, LNCS 12059, pp. 264–283, 2020.
https://doi.org/10.1007/978-3-030-51280-4_15

payments directly, by sending each other digitally signed payment messages. If Bob tries to cheat Alice, Alice can show the signed payment messages as a proof to the blockchain, using the original funding transaction as security.

Instead of establishing a payment channel to every other person and company in the world, thanks to a technique called Hash Time Locked Contracts (HTLCs) [1,17,32], payments can also be sent atomically through a path of payment channels. More precisely, each payment channel is now an edge in a *payment network*, and payments will be routed along a path of payment channels in the payment network. Such a payment network is called the layer 2 of the blockchain, the blockchain itself being the layer 1.

The payment channels/networks have many significant advantages over vanilla blockchains: With payment channels, the transaction throughput becomes unlimited, as each transaction is only seen by the nodes on the path between sender and receiver of a payment. This is like sending a packet in the internet instead of sending every packet to a central server. Solving the throughput problem will also drastically decrease transaction fees. In addition, payments will be instantaneous, as one does not have to wait multiple minutes before the blockchain verifies a transaction. Payment networks also allow for more privacy as transactions are only seen by the parties involved. On the negative side, to set up a channel, the channel owner(s) must lock some capital. However, whenever a payment channel routes a transaction on behalf of other parties, the channel owner(s) can collect a transaction fee.

Payment networks are currently a hot topic in blockchain research. In practice, the first payment networks have been deployed, and are being actively used. Prominent examples are Bitcoin's Lightning network [16,32] with more than 30,000 active channels, or Ethereum's Raiden network [3].

As Bitcoin's Lightning network is growing quickly, we need to understand these newly forming payment networks. Which channels will be created, and what will the network topology eventually look like? Network creation games [21] are a perfect tool to understand these questions, since they capture the degradation of the network's efficiency when participants act selfishly.

In a network creation game, the incentive of a player is to minimize her cost by choosing to whom she connects. In our model, players weigh the benefits they receive from using payment channels against the channels' creation cost, and selfishly initiate connections to minimize their cost. There are two types of benefits for each player: (i) the forwarding fees she receives for the transactions she routed through her channels, (ii) the reduced cost for routing her transactions through the payment network in comparison to publishing the transactions on the blockchain (blockchain fee). On the other hand, establishing a channel costs the blockchain fee. Thus, a player has to balance all these factors to decide which channels to establish to minimize her cost. Our goal is to gain a meaningful insight on the network structures that will emerge and evaluate their efficiency, in comparison to centralized structures designed by a central authority that previous work has shown to be almost optimal.

1.2 Our Contributions

In this work, we provide a game-theoretic approach to analyze the creation of blockchain payment networks. Specifically, we adopt betweenness centrality, a natural measure for fees a player is expected to receive by forwarding others' transactions on a path of payment channels. On the other hand, we employ closeness centrality as an intuitive proxy for the transaction fees encountered when executing transactions through other players in the network. We reflect the cost of payment channel creation by associating a price with link creation. Therefore, we also generalize previous work on network creation games as our model combines both betweenness and closeness centralities.

Under this model, we study the topologies that emerge when players act selfishly. A specific network structure is considered a Nash equilibrium when no player can decrease her cost by unilaterally changing her connections. We examine various such structures and determine the parameter space in which they constitute a Nash equilibrium. Moreover, we determine the social optima depending on the correlation of betweenness and closeness centrality. When possible, we bound the price of anarchy, the ratio of the social costs of the worst Nash equilibrium and the social optimum [26], to obtain insight into the effects of lack of coordination in payment networks when players act selfishly. Furthermore, we briefly discuss the price of stability, the ratio of the social costs of the best Nash equilibrium and the social optimum [6], specifically concerning the parameter values that most accurately represent blockchain payment networks.

The omitted proofs can be found in the full version [11].

1.3 Related Work

Various payment channel protocols have been proposed in literature [8,9,17,24,27,28,32,33], all presenting different solutions on how to create payment channels. However, our work is independent of the channel construction specifications and thus applies to all such solutions.

Payment networks have been studied from an algorithmic (not game theoretic) viewpoint by Avarikioti et al. [7,10]. In [7], they examined the optimal graph structure and fee assignment to maximize the profit of a central authority that creates the payment network and bears the relevant costs and benefits. Furthermore, in [10], they investigated the online and offline computation of a capital-efficient payment network for a central authority. In contrast, our work studies the decentralized payment network design, where the network is created by multiple participants and not a single authority. This model reflects more accurately the currently operating payment networks, which are indeed created by thousands of users rather than a single company, following the decentralized philosophy of cryptocurrencies like Bitcoin.

Network creation games were originally introduced by Fabrikant et al. [21]. In their game, referred to as sum network creation game, a player unilaterally creates links to minimize the sum of distances to other players in the network (closeness centrality). Later, Albers et al. [4] improved the upper bound for the

price of anarchy and also examined a weighted network creation game. While these works solely focus on a player's closeness centrality, our model is more complex and additionally includes another metric, the players' betweenness centrality that represents the importance of a player in the network.

In parallel, network creation games were expanded to various settings. The idea of bilateral link creation was introduced by Corbo and Parkes [15]. Demaine et al. [18] devise the max game, where players try to minimize their maximum distance to any other player in the game. Intrinsic properties of peer-to-peer networks are taken into account in the network creation variation conceived by Moscibroda et al. [29,30]. Nodes strive to minimize their stretch, the ratio between the distance of two nodes in a graph, and their direct distance. The idea of bounded budget network creation games was proposed by Ehsani et al. [19]. In bounded budget network creation games, players have a fixed budget to establish links. Moreover, Àlvarez et al. [5] introduced the celebrity game, where players try to keep influential nodes within a fixed distance. However, the objectives in all these games give little insight to the control a player has over a network. This control is desired by players in blockchain payment networks to maximize the fees received for routing transactions, in essence their betweenness centrality.

A bounded budget betweenness centrality game was introduced by Bei et al. [12]. Given a budget to create links, players attempt to maximize their betweenness centrality. Due to their complexity, betweenness network creation games yield limited theoretical results, in comparison to those of the sum network creation game, for instance. In contrast to our work, a players closeness centrality is not taken into account in [12]. Thus, this model is insufficient for our purpose since it does not consider how strategically connected is a player that wants to route many transactions through the payment network.

Buechel and Buskens [14] compare betweenness and closeness centralities; however, not in a network creation game setting, as their notion of stability does not lead to Nash equilibria. We, on the other hand, study the combination of betweenness and closeness incentives in a network creation game setting.

2 Preliminaries and Model

In this section, we first introduce the essential background and assumptions for our payment network creation game, and then we introduce the necessary notation and the game-theoretic model.

2.1 Payment Networks

Payment channels operate on top of the blockchain (Layer 2) and allow instant off-chain transactions. Generally, a channel is set up by two parties that deposit capital in a joint account on the blockchain. The channel can then be used to make arbitrarily many transactions without committing each transaction to the blockchain. When opening a channel, the parties pay a blockchain fee and place

capital in the channel. The blockchain fee is the transaction fee to the miner, paid to have the transaction included in a block and thereby published on the blockchain. The deposited capital funds future channel transactions and is not available for other transactions on the blockchain during the channel's lifetime.

In our model, we assume a player single-handedly initiates a channel to a subset of other players. Incoming channels are always accepted and once installed, the channels can be used to send money in both directions (from sender to receiver, and vice versa). While any player can typically choose the amount to lock in a channel, we assume that the locked capital placed in all channels is high enough to be modeled as unlimited. In particular, we assume that all players are major (large companies, financial institutions etc.) that have thus access to large amounts of temporary capital. It is natural to assume only major players to participate in the network creation game. Typically, a market is created when there is demand for a service. Thus eventually, the payment network will be dominated by service providers that will individually connect with clients and act as intermediaries for all transactions. In this work, we only consider the flow of transactions through these service providers. Therefore, the cost of opening a channel in our model solely reflects the permanent cost, i.e. the blockchain fee, and is set to 1 (wlog). Furthermore, since we assume major players only, the transactions between the players can be considered uniform.

In addition to enabling parties connected by a channel to exchange funds off-chain, payment channels can also be used to route off-chain transactions between a sender and receiver pair not directly connected by a channel. Transactions between the sender and receiver can be routed securely through a path of channels. Since we assume that all channels are funded with unlimited capital, the channel funds cannot deplete, and so any path in the payment network between sender and receiver is viable.

Together, the payment channels form a payment network. In the network, players receive a payment when transactions are routed through their channels. This payment is a transaction fee, which is typically proportional to the value of the routed transaction, to compensate the intermediate node for the loss of her channel's capital capacity. However, we consider a fixed fee for all nodes, independent of the routed value, since we assume unlimited channel capital.

2.2 Formal Model

A payment network can be formally expressed by an unweighted undirected graph consisting of V nodes, representing the set of players, and E edges, representing the set of payment channel between the players.

A payment network game consists of n players $V = \{0, 1, \ldots, n-1\}$, denoted by $[n]$. The strategy of player u expresses the channels she chooses to open and is denoted by s_u, and the set $S_u = 2^{[n]-\{u\}}$ defines u's strategy space. We denote by $G[s]$ the underlying undirected graph of $G_0[s] = \left([n], \bigcup_{u\in[n]}\{u\} \times s_u\right)$, where $s = (s_0, \ldots, s_{n-1}) \in S_0 \times \cdots \times S_{n-1}$ is a strategy combination. Note that while

a channel can possibly be created by both endpoints, this will never be the case in a Nash equilibrium.

Betweenness Centrality. The fees received by a player for providing gateway services to other players' transactions are modeled by her betweenness centrality. Betweenness centrality was first introduced as a measure of a player's importance in a social network by Freeman et al. [22]. According to [22], the betweenness centrality of a player u in a graph $G(V, E)$ is $\sum_{\substack{s,r \in V \\ s \neq r \neq u, m(s,r) > 0}} \frac{m_u(s,r)}{m(s,r)}$, where $m_u(s,r)$ is the number of shortest paths between sender s and receiver r that route through player u and $m(s,r)$ is the total number of shortest paths between s and r. Additionally, $s \neq r \neq u$ indicates that $s \neq r$, $s \neq u$ and $r \neq u$. Intuitively, the betweenness centrality of player u is a measure of the expected number of sender and receiver pairs that would choose to route their transactions through her in a payment network. Providing an insight into the transaction fees a player is expected to receive, the betweenness centrality lends itself to reflect the motivation of a player in a payment network to maximize the payments secured through providing transaction gateway services.

However, in our model, the betweenness of player u is measured as follows:

$$\text{betweenness}_u(s) = (n-1)(n-2) - \sum_{\substack{s,r \in [n]: \\ s \neq r \neq u, m(s,r) > 0}} \frac{m_u(s,r)}{m(s,r)}.$$

We subtract u's betweenness centrality, as defined by Freeman et al. [22], from her maximum possible betweenness centrality to ensure that the social cost is always positive - avoiding cases where price of anarchy is undefined.

Closeness Centrality. Furthermore, we model the fees encountered by a player when having her transactions routed through the network with her closeness centrality. Closeness centrality measures the sum of distances of player u to all other players and is given by

$$\text{closeness}_u(s) = \sum_{r \in [n]-u} \left(d_{G[s]}(u,r) - 1 \right),$$

for a player u, where $d_{G[s]}(u,r)$ is the distance between u and r in the graph $G[s]$. With the transaction fees fixed per edge in our model, the distance to a player r estimates the costs encountered by player u when sending a transaction to player r. Therefore, the sum of distances to all other players is a natural proxy for the fees u faces for making transactions when assuming uniform transactions.

Thus, the combination of betweenness and closeness centralities accurately encapsulates the incentives inherent to players in a blockchain payment network.

Cost. The cost of player u under the strategy combination s is $\text{cost}_u(s) = |s_u| + b \cdot \text{betweenness}_u(s) + c \cdot \text{closeness}_u(s)$, where $b \geq 0$ is the betweenness weight and $c > 0$ the closeness weight. Letting $c > 0$ ensures that the graph is always connected, as a player's cost is infinite in a disconnected graph. Additionally, the model assumes the same price for all nodes and embeds this into coefficients b and c. While this does not exactly encapsulate reality, it is a reasonable assumption. Different paths offer similar services to payers. In such a setting, Bertrand competition [13] suggests that competition will drive the prices from different players to be within a close region of each other.

Social Optimum. The objective of player u is to minimize her cost, $\min_{s_u} \text{cost}_u(s)$. The social cost is the sum off all players' costs, $\text{cost}(s) = \sum_{u \in [n]} \text{cost}_u(s)$. Thus, the social optimum is $\min_s \text{cost}(s)$.

3 Payment Network Creation Game

To gain an insight into the efficiency of emerging topologies when players act selfishly, we will first analyze the social optimum for our model. After studying if and when prominent graphs are Nash equilibria, we conclude by bounding the price of anarchy and the price of stability.

3.1 Social Optimum

By the definition of the cost function, the social cost is

$$\text{cost}(s) = \sum_{u \in [n]} \text{cost}_u(s) = |E(G)| + b \sum_{u \in [n]} \text{betweenness}_u(s) + c \sum_{u \in [n]} \text{closeness}_u(s),$$

for any graph where no channel is paid by both endpoints. This condition is met for all Nash equilibria. To lower bound the social cost, we will first simplify the social cost expression. Lemma 1 is proven in [23] and relates the average betweenness and distance in a connected graph.

Lemma 1 (Theorem 1 [23]). *The average betweenness $\overline{B}(G)$ in a connected graph G can be expressed as: $\overline{B}(G) = (n-1)(\bar{l}(G)-1)$, where $\bar{l}(G)$ is the average distance in G.*

We take advantage of Lemma 1 to simplify the social cost expression. With this we show in Lemma 2 how the social cost can be expressed directly in terms of the number of edges and the sum of the players' closeness centrality costs, facilitating further analysis.

Lemma 2. *The social cost in G is given by $\text{cost}(s) = |E(G)| + b \cdot n \cdot (n-1)(n-2) + (c-b) \cdot \sum_{u \in [n]} \text{closeness}_u(s)$.*

Proof. According to Lemma 1 the social cost can be expressed as follows for all $b \geq 0$ and $c > 0$.

$$\begin{aligned}
\text{cost}(s) &= |E(G)| + b \sum_{u \in [n]} \text{betweenness}(u) + c \sum_{u \in [n]} \text{closeness}(u) \\
&= |E(G)| + b \sum_{u \in [n]} \left((n-1)(n-2) - \sum_{\substack{s,r \in [n]: \\ s \neq r \neq u, \\ m(s,r) > 0}} \frac{m_u(s,r)}{m(s,r)} \right) \\
&\quad + c \sum_{u \in [n]} \sum_{r \in [n]-u} \left(d_{G[s]}(u,r) - 1 \right) \\
&= |E(G)| + b \cdot n \cdot (n-1)(n-2) - b \cdot n \cdot \overline{B}(G) + c \cdot n \cdot (n-1)(\overline{l}(G) - 1) \\
&= |E(G)| + b \cdot n \cdot (n-1)(n-2) + (c-b) \cdot n \cdot (n-1)(\overline{l}(G) - 1) \\
&= |E(G)| + b \cdot n \cdot (n-1)(n-2) + (c-b) \cdot \sum_{u \in [n]} \sum_{r \in [n]-u} \left(d_{G[s]}(u,r) - 1 \right) \quad \square
\end{aligned}$$

The distance of a vertex v of a connected graph G is $d(v) := \sum_{u \in [n]-v} d_G(v,u)$. The distance of a connected graph G is $d(G) := \sum_{v \in [n]} d(v)/2$. If G is not connected, then $d(v) = \infty$ for any v, and $d(G) = \infty$.

Lemma 3 (Theorem 2.3 [20]). *If G is a connected graph with n vertices and k edges then $n \cdot (n-1) \leq d(G) + k \leq \frac{1}{6} \cdot \left(n^3 - 5 \cdot n - 6 \right)$.*

Lemma 3 provides bounds for the distance of a graph G,

$$d(G) = \frac{1}{2} \sum_{u \in [n]} \sum_{r \in [n]-u} d_G(u,r)$$

which is useful for finding the social optimum for our game.

In [20] Lemma 3 is proven and stated that the path graph achieves the upper bound; maximizes the distance term. This can be used to find the social optimum. Dependent on the weights b and c, the social optimum for our payment network creation game is given in Theorem 1, and illustrated in Fig. 1.

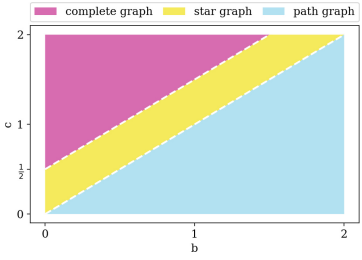


Fig. 1. Parameter map for social optimum.

Theorem 1. *The social optimum is a complete graph for $c > \frac{1}{2} + b$, a star graph for $b \leq c \leq \frac{1}{2} + b$ and a path graph for $c < b$.*

Proof. Using Lemma 2 we can lower bound the social cost for $c \geq b$ as follows:

$$\begin{aligned}\text{cost}(s) &= |E(G)| + b \cdot n \cdot (n-1)(n-2) + \underbrace{(c-b)}_{\geq 0} \sum_{u \in [n]} \sum_{r \in [n]-u} \left(d_{G[s]}(u,r) - 1\right) \\ &\geq |E(G)| + b \cdot n \cdot (n-1)(n-2) + (c-b)(n \cdot (n-1) - 2|E(G)|) \\ &= (1 - 2 \cdot (c-b)) \cdot |E(G)| + b \cdot n \cdot (n-1)(n-2) + (c-b)(n \cdot (n-1))\end{aligned}$$

since every pair of nodes that is not connected by an edge is at least distance 2 apart [21]. This lower bound is achieved by any graph with diameter at most 2. It follows that for $c > \frac{1}{2} + b$ the social optimum is a complete graph, maximizing $|E|$, and for $b \leq c \leq \frac{1}{2} + b$ the social optimum is a star, minimizing $|E|$.

To find the social optimum for $c < b$, we rewrite the social cost as

$$\begin{aligned}\text{cost}(s) &= |E(G)| + b \cdot n \cdot (n-1)(n-2) - (b-c) \cdot \sum_{u \in [n]} \sum_{r \in [n]-u} \left(d_{G[s]}(u,r) - 1\right) \\ &= |E(G)| - 2 \cdot (b-c) \cdot d(G) + b \cdot n \cdot (n-1)(n-2) + (b-c) \cdot n \cdot (n-1)\end{aligned}$$

For a connected graph the social cost is then minimized for a tree, as $|E(H)| - a \cdot d(H) > |E(G)| - a \cdot d(G)$ if G is a subgraph of H and $a > 0$. For any tree, the number of edges is $n - 1$. Using Lemma 3, we get that

$$\begin{aligned}\text{cost}(s) &= |E(G)| + b \cdot n \cdot (n-1)(n-2) - (b-c) \sum_{u \in [n]} \sum_{r \in [n]-u} \left(d_{G[s]}(u,r) - 1\right) \\ &\geq \left(1 + \left(\frac{2}{3}b + \frac{1}{3}c\right) n \cdot (n-2)\right)(n-1)\end{aligned}$$

is a lower bound for the social cost which is achieved by a path graph. □

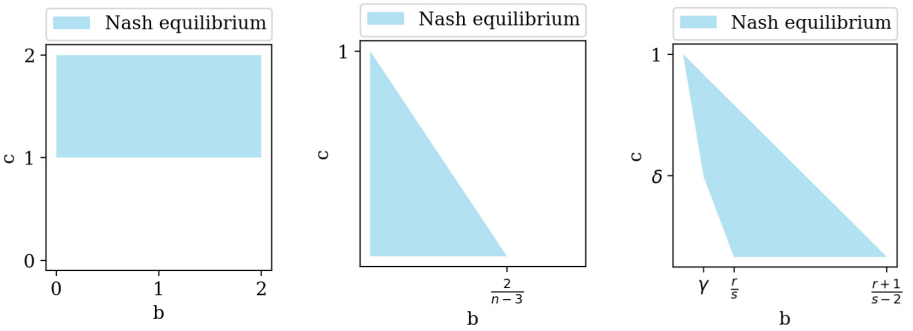
In areas most accurately describing payment networks, we expect the weights b and c to be smaller than the cost of channel creation and close to each other. For these cases, we observe the star graph is the social optimum.

3.2 Nash Equilibria

To find a Nash equilibrium, one could follow a naive approach: start with a fixed graph structure and then continuously compute a player's best response in the game. However, Theorem 2 shows that it is NP-hard to calculate a player's best response.

Theorem 2. *Given a strategy $s \in S_0 \times \cdots \times S_{n-1}$ and $u \in [n]$, it is NP-hard to computed the best response of u.*

Therefore, with this in mind, we analyze prominent graph topologies theoretically, to see if and when they are Nash equilibria in our game. The results are illustrated in Fig. 2. However, complementary to the theoretical analysis we also run a simulation to get insights into emerging graph topologies for a small number of players.



(a) complete graph (b) star graph ($n \geq 4$) (c) biclique

Fig. 2. Parameter map for prominent graphs. In Fig. 2c, r and s are the subset sizes ($3 \leq r \leq s$). With $\alpha = \frac{s \cdot (s-1)}{r \cdot (s-2)}$ and $\beta = \frac{1}{s-r+1}\left(\frac{s \cdot (s-1)}{r} - \frac{(r-2)(r-1)}{s+1}\right)$, (γ, δ) is the intersection between $1 = \frac{s}{r}b + \frac{s+r-3}{s-1}c$ and $1 = \min\{\alpha, \beta\} \cdot b + c$.

Complete Graph. For large values of c the complete graph is the only Nash equilibrium as stated in Theorem 3. Additionally, the complete graph is also a Nash equilibrium for $c = 1$, but it is not necessarily the only one. However, for small values of c, which are the values we expect to encounter in a payment network creation game, the complete graph is not a Nash equilibrium, as stated in Theorem 4.

Theorem 3. *For $c > 1$, the only Nash equilibrium is the complete graph.*

Proof. The addition of an edge by a player never increases her betweenness cost. Thus, by the definition of the cost function any Nash equilibrium cannot be missing any edges whose addition would reduce a players closeness by more than 1, the cost of building an edge. As $c > 1$, no edge can be missing in the graph and the only Nash equilibrium is the complete graph. □

Theorem 4. *For $c < 1$ and $n \geq 3$, the complete graph is never a Nash equilibrium.*

Proof. In a complete graph the removal of an edge by a player does not change her betweenness cost and her closeness cost is increased by c. Thus, the cost of a player would decrease when removing one edge. Therefore, the complete graph is not a Nash equilibrium for $c < 1$. □

Figure 2a visualizes the combination of these results, i.e., when the complete graph is a Nash equilibrium in our game. We observe that for some weight combinations the complete graph is both the social optimum and a Nash equilibrium. However, most payment networks are not expected to fall into this area of the parameter space.

Path Graph. While the path graph is the social optimum for a significant area of the parameter space, we show it can only be a Nash equilibrium for small sets of players. For $n = 3$, the path graph is a Nash equilibrium for all $c \leq 1$, as it is the only possible connected graph that is not the complete graph.

Proposition 1. *For $n = 4$, the path graph is a Nash equilibrium if and only if $1 \leq b + 2 \cdot c$.*

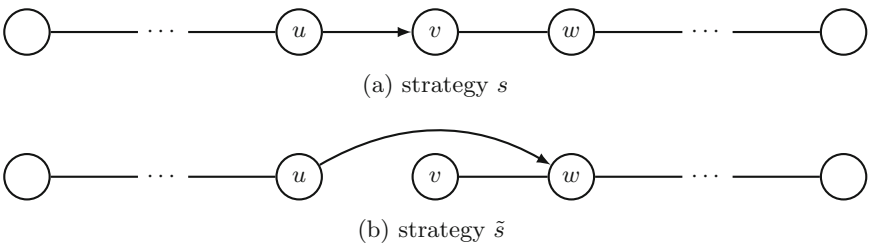
Proposition 2. *For $n = 5$, the path graph is a Nash equilibrium if and only if $1 \leq 2 \cdot b + 4 \cdot c$.*

Propositions 1 and 2 identify when the path graph is a Nash equilibrium for networks with four and five players respectively. These bounds partly overlap with areas in which the path graph is the social optimum. While this partial correspondence between the Nash equilibrium and social optimum appears promising for the coordination of our game, Theorem 5 suggests to the contrary.

Theorem 5. *For $n \geq 6$, the path graph is never a Nash equilibrium.*

Proof. To show that the path graph is never a Nash equilibrium for $n \geq 6$, we will show that at least one player in a path graph consisting of more than six players can always reduce her cost by changing strategy.

In a path graph with at least six players, at least one player u has an outgoing edge to a player v at least two steps from the end of the path on the opposite side of player u. This is illustrated in Fig. 3a and we consider this to be strategy s. In this case it is always more beneficial for player u to connect to player w instead of player v. Let's refer to this strategy as strategy $\tilde{s}$ (Fig. 3b).



(a) strategy s

(b) strategy $\tilde{s}$

Fig. 3. Strategy deviation of player 1.

The change in cost for this strategy is given as

$$\Delta \text{cost}_u(s \text{ to } \tilde{s}) = -c \cdot (m - 2),$$

where m is the number of edges player v is away from the endpoint on the opposite side u. Thus, the change in cost is negative and the path graph cannot be a Nash equilibrium for $n \geq 6$. □

Hence, the path graph is not expected to be a Nash equilibrium for payment networks that typically consist of many nodes.

Circle Graph. The results we find for the circle graph are similar to those for the path graph. For small values of n, the circle graph can be a Nash equilibrium depending on the weights b and c. The circle graph and the complete graph are the same for $n = 3$. Thus, for $n = 3$ the circle graph is a Nash equilibrium if and only if $c \geq 1$.

Proposition 3. *For $n = 4$, the circle graph is a Nash equilibrium if and only if $c \leq 1 \leq b + 2 \cdot c$.*

Proposition 4. *For $n = 5$, the circle graph is a Nash equilibrium if and only if $b + c \leq 1 \leq 2 \cdot b + 4 \cdot c$.*

Propositions 3 and 4 show that for small n, the circle graph can be a Nash equilibrium depending on the weights b and c. However, for large n the circle graph is never a Nash equilibrium, as stated in Theorem 6.

Theorem 6. *There exists a $N > 0$, such that for all $n \geq N$ the circle graph is never a Nash equilibrium.*

We note that simulations suggest that for $n \geq 6$ the circle graph is never a Nash equilibrium. Parameter sweeps indicating that $N = 6$ can be found in the full version [11].

Star Graph. The star graph is the social optimum for a significant part of our parameter space. In a star graph the player in the center has minimal closeness and betweenness costs; all other players have maximal betweenness cost. While this does not directly appear to be a stable network, Theorem 7 suggests that the star graph is a Nash equilibrium for smaller values of b and c. These results are depicted in Fig. 2b.

Theorem 7. *For $n \geq 4$, the star graph is always a Nash equilibrium if and only if $0 \leq 1 - \frac{n-3}{2}b - c$.*

Proof. To show that the star is always a Nash equilibrium for $n \geq 4$ and $0 \leq 1 - \frac{n-3}{2}b - c$, we will consider a star graph consisting of n players $V = \{0, 1, \ldots, n-1\}$. Without loss of generality we assume that player 0 is the center of the star.

No player in the star graph has an incentive to remove an edge, as this would lead to infinite cost. Thus, player 0 has no incentive to change strategy, as she is connected to everyone.

Next we consider star graphs where all links are initiated by player 0 and star graphs where at least one link is initiated by another player separately.

If all links are initiated by player 0, players 1, 2, ..., $n-1$ are all in an equivalent position and it is therefore sufficient to solely consider player 1. Player 1 would only add links, if this leads to a decrease in her cost. Initiating an edge to player 0 would only increase her cost. Additionally, for the remaining $n-2$ players, it only matters to how many player 1 connects. The change in cost when adding m, where $1 \leq m \leq n-2$, edges is given by $\Delta\text{cost}_1(\text{add } m \text{ links}) = m -$

$\frac{m \cdot (m-1)}{2} b - m \cdot c$. Thus, player 1 will change strategy if $\Delta\text{cost}_1(\text{add } m \text{ links}) < 0$. The change in cost is minimized for $m = n - 2$.

In star graphs where at least one player other than 0 initiates a link, players that have no outgoing links are in the same position as those analyzed previously. Thus, it suffices to consider player i, where $i \neq 0$, that has one outgoing link. In addition to only initiating new links, player i can remove the link to player 0 and initiates l, where $1 \leq l \leq n-2$, new links. The change in cost is then given as $\Delta\text{cost}_i(\text{add } l \text{ links}) = (l-1) - \frac{l \cdot (l-1)}{2} b - (l-1) \cdot c$. However, this leads to more restrictive bounds and there is no need for players other than player 0 to have outgoing links.

Thus, the star is a Nash equilibrium if and only if $0 \leq 1 - \frac{n-3}{2} b - c$. □

We note that the areas where the star is both a Nash equilibrium and the social optimum overlap partially.

Complete Bipartite Graph. The star graph is a complete bipartite graph where one group has size one. In this section, we analyze more general complete bipartite graphs or bicliques $K_{r,s}$, where r is the size of the smaller subset and s is the size of the larger subset. In a complete bipartite graph, every node from one subset is connected to all nodes from the other subset.

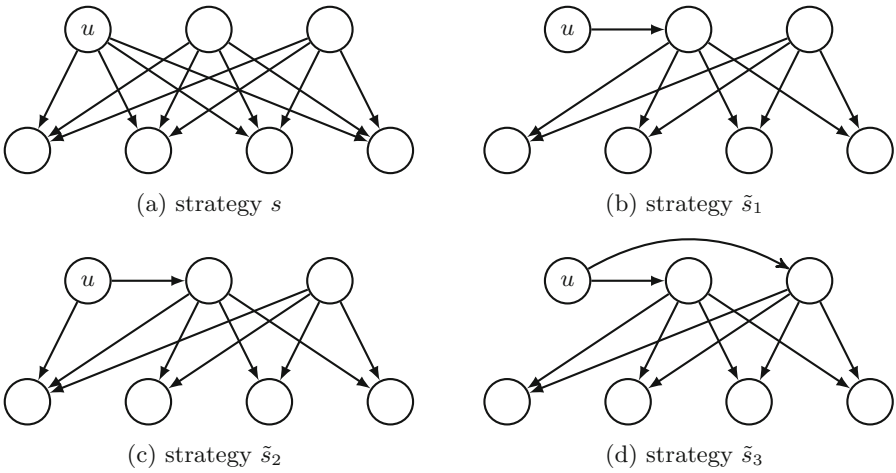
Theorem 8. *The complete bipartite graph $K_{r,s}$ with $3 \leq r \leq s$ is stable if and only if $\frac{s-2}{r+1} b + c \leq 1 \leq \min\left\{\frac{s}{r} b + \frac{s+r-3}{s-1} c, \min\{\alpha, \beta\} \cdot b + c\right\}$, where $\alpha = \frac{s \cdot (s-1)}{r \cdot (s-2)}$ and $\beta = \frac{1}{s-r+1}\left(\frac{s \cdot (s-1)}{r} - \frac{(r-2)(r-1)}{s+1}\right)$.*

Proof. Additional links can only be created within a subset in a complete bipartite graph. Similarly to adding links in a star graph, the change in cost when adding m links is given by $\Delta\text{cost}_u(\text{add } m \text{ links}) = m - \frac{m \cdot (m-1)}{l+1} b - m \cdot c$, where $l \in \{r, s\}$ is the size of the subset not including the player.

A player changes strategy when $\Delta\text{cost}_u(\text{add } m \text{ links}) < 0$. The change in cost is minimized when m is maximized and $l = r$. m can therefore be $s-1$ at most. Thus, the upper bound for $K_{r,s}$ being a Nash equilibrium is $1 \geq \frac{s-2}{r+1} b + c$.

Players in the subset of size r, benefit more from a link to the other subset, as their betweenness cost is smaller. Thus, players from the larger subset with outgoing links would change strategy sooner. In the case where the subsets are of equal size, the link direction does not matter. Hence, to find a lower bound for b and c we only consider complete bipartite graphs, in which all links are established from the smaller subset, as seen in Fig. 4a. Without loss of generality we will only consider player u in the following analysis. It is not reasonable for player u to remove all her links without adding any new links, as her cost would become infinite. Depending on the other parameters, it might be more optimal to remove all her previous links and only connect to one player in her subset (Fig. 4b), connect to one player in her subset and one player from the other

subset (Fig. 4c), or to remove all her previous links and instead connect to all other players in her subset (Fig. 4d). When player u changes to strategy $\tilde{s}_1$, seen in Fig. 4b the change in cost is as follows:



(a) strategy s (b) strategy $\tilde{s}_1$

(c) strategy $\tilde{s}_2$ (d) strategy $\tilde{s}_3$

Fig. 4. Strategy deviations of player u.

$$\Delta\text{cost}_u(s \text{ to } \tilde{s}_1) = -(s-1) + \frac{s\cdot(s-1)}{r}b + (s+r-3)\cdot c$$

as player u initiates $s-1$ less links than before - losing all her previous betweenness. Additionally, she is one edge further away from all other players except for the one she connects to directly. Thus, the above strategy is less preferable than the complete bipartite graph for player u, if

$$1 \leq \frac{s}{r}b + \frac{s+r-3}{s-1}c.$$

Player u's change to strategy $\tilde{s}_2$ (Fig. 4c) leads to $s-2$ less links initiated by her. The player is further away from $s-1$ players from the other subset and closer to one in her own. All transaction-routing potential is lost. Therefore, the change in cost is given by

$$\Delta\text{cost}_u(s \text{ to } \tilde{s}_2) = 2 - s + \left(\frac{s\cdot(s-1)}{r}\right)b + (s-2)\cdot c.$$

Hence, for this strategy to be less preferable than the complete bipartite graph,

$$1 \leq \left(\frac{s\cdot(s-1)}{r\cdot(s-2)}\right)b + c = \alpha\cdot b + c.$$

When severing all previous links and connecting to all players in her subset instead, strategy $\tilde{s}_3$ (Fig. 4d), player u builds $s-r+1$ less links than before.

Furthermore, she is closer to players previously in her own subset and further away from the rest. While player u can now transmit transactions of players previously in her own subset, she is no longer a preferable intermediary for players previously in the other subset. Therefore, the change in cost is given by

$$\Delta\text{cost}_u(s \text{ to } \tilde{s}_3) = r - s + 1 + \left(\frac{s \cdot (s-1)}{r} - \frac{(r-1)(r-2)}{s+1}\right) b + (s - r + 1) \cdot c.$$

Hence, for this strategy to be less preferable than the complete bipartite graph for player u,

$$1 \leq \frac{1}{(s-r+1)} \left(\frac{s \cdot (s-1)}{r} - \frac{(r-1)(r-2)}{s+1}\right) b + c = \beta \cdot b + c.$$

To summarize, the complete bipartite graph $K_{r,s}$ is a Nash equilibrium for

$$\frac{s-2}{r+1} b + c \leq 1 \leq \min\left\{\frac{s}{r} b + \frac{s+r-3}{s-1} c, \min\{\alpha, \beta\} \cdot b + c\right\}.$$

□

The parameter map for the complete bipartite graph is drawn in Fig. 2c. There (γ, δ) is the intersection between $1 = \frac{s}{r} b + \frac{s+r-3}{s-1} c$ and $1 = \min\{\alpha, \beta\} \cdot b + c$.

Simulation. To better understand the behaviour of a player in our payment network creation game, we implement a simulation of the game [2]. Our simulation enumerates all Nash equilibria for a given number of players n, as well as the weights for the betweenness and closeness costs. However, this is only feasible for small n. Parameter sweeps for the weights b and c can also be performed to see when a given topology is a Nash equilibrium. Some parameter sweeps for topologies previously analyzed can be found in [11]. Finally, starting from an initial graph the progression of the game can be simulated.

3.3 Price of Anarchy

The ratio between the social optimum and the worst Nash equilibrium is the price of anarchy (PoA), formally,

$$\text{PoA} = \frac{\max_{s \in N} \text{cost}(s)}{\min_{s \in S} \text{cost}(s)},$$

here S is the set of all strategies and N is the set of strategies that are Nash equilibria.

The price of anarchy provides an insight to the effects of lack of coordination, i.e. measures the performance degradation of the system when players act selfishly in comparison to central coordination. When the price of anarchy is low, selfish actors do not heavily degrade network efficiency. In contrast, a high price of anarchy indicates that network formation by a central authority would significantly increase efficiency.

For $c > 1$, we can determine the price of anarchy exactly, as we established both the social optimum and the (unique) Nash equilibria for $c > 1$.

Corollary 1. *For $c > 1$ and $c > \frac{1}{2} + b$, the price of anarchy is $PoA = 1$.*

Corollary 2. *For $c > 1$ and $b \leq c \leq \frac{1}{2} + b$, the price of anarchy is*

$$PoA = \frac{\left(\frac{1}{2} + (n-2) \cdot b\right) \cdot n}{1 + (c + b \cdot (n-1))(n-2)}.$$

Corollary 3. *For $1 < c < b$, the price of anarchy is*

$$PoA = \frac{\left(\frac{1}{2} + (n-2) \cdot b\right) \cdot n}{1 + \left(\frac{2}{3}b + \frac{1}{3}c\right) \cdot n \cdot (n-2)}.$$

Combining the results of Corollary 1, 2 and 3 allows us to upper bound the price of anarchy to a constant for $c > 1$, as stated in in Corollary 4. This upper bound is asymptotically tight, as the price of anarchy is always greater or equal to one (hence at least constant) by definition.

Corollary 4. *For $c > 1$, the price of anarchy is $PoA = \mathcal{O}(1)$.*

Proof. For $c > 1$ and $c > \frac{1}{2} + b$, the price of anarchy is one and therefore it is also $\mathcal{O}(1)$.

We have that for $c > 1$ and $b \leq c \leq \frac{1}{2} + b$,

$$\text{PoA} = \frac{\left(\frac{1}{2} + (n-2) \cdot b\right) \cdot n}{1 + (c + b \cdot (n-1))(n-2)} = \mathcal{O}\left(\frac{b \cdot n^2}{b \cdot n^2}\right) = \mathcal{O}(1),$$

and for $1 < c < b$,

$$\text{PoA} = \frac{\left(\frac{1}{2} + (n-2) \cdot b\right) \cdot n}{1 + \left(\frac{2}{3}b + \frac{1}{3}c\right) \cdot n \cdot (n-2)} = \mathcal{O}\left(\frac{b \cdot n^2}{b \cdot n^2}\right) = \mathcal{O}(1).$$

Thus, for $c > 1$ we have $\text{PoA} = \mathcal{O}(1)$. □

For small b and c we can also upper bound the price of anarchy as follows:

Theorem 9. *For $c + b < \frac{1}{n^2}$, the price of anarchy is $PoA = \mathcal{O}(1)$.*

Proof. For $c + b < \frac{1}{n^2}$, all Nash equilibria are trees. Unless the distance to a player is infinite, no player in the network will have an incentive to build an edge.

As both the maximum possible change in $\text{betweenness}_u(s)$ and $\text{closeness}_u(s)$ for a node u in a connected graph is less than n^2 and all Nash equilibria are connected, $\Delta\text{cost}_u(s) > -n^2 \cdot c - n^2 \cdot b + 1$. We require $\Delta\text{cost}_u(s) \geq 0$ such that u does not benefit from initiating an additional channel. Thus, for $c + b \leq \frac{1}{n^2}$ all Nash equilibria are spanning trees.

For $c + b \leq \frac{1}{n^2}$ the social optimum is also a spanning tree, as it is either the star or path graph. It easily follows that for $c + b \leq \frac{1}{n^2}$ and all spanning trees $\text{cost}(s) = \Theta(n)$ and therefore the price of anarchy is $\mathcal{O}(1)$.

Finally, for $c+b \geq \frac{1}{n^2}$ and $c < 1$, we show an $\mathcal{O}(n)$ upper bound for the price of anarchy.

Theorem 10. *For $c + b \geq \frac{1}{n^2}$ and $c < 1$, the price of anarchy is PoA $= \mathcal{O}(n)$.*

Proof. The price of anarchy is

$$\text{PoA} = \mathcal{O}\left(\frac{|E(G)| + n^3 \cdot b + (c-b) \cdot \sum_{u\in[n]} \sum_{r\in[n]-u} (d_G(u,r) - 1)}{n^3 \cdot b + n}\right).$$

We can say that $d_G(u,r) < \Theta\left(\frac{2}{\sqrt{c+b}}\right)$, as player u would connect to player r otherwise. Player u would become closer to half the nodes on the path otherwise and reduce her betweenness cost through the routing potential gained by the link addition. Therefore we have,

$$\text{PoA} = \mathcal{O}\left(\frac{|E(G)| + n^3 \cdot b + n^2 \frac{c-b}{\sqrt{b+c}}}{b \cdot n^3 + n}\right).$$

It follows that

$$\mathcal{O}\left(\frac{n^3 \cdot b}{n^3 \cdot b + n}\right) = \mathcal{O}(1), \quad \text{and} \quad \mathcal{O}\left(\frac{n^2 \frac{c-b}{\sqrt{b+c}}}{n^3 \cdot b + n}\right) = \mathcal{O}\left(\frac{c-b}{n^2 \cdot b + 1}\right) = \mathcal{O}(1),$$

as $c + b \geq \frac{1}{n^2}$ and $c < 1$. Thus, it only remains to consider $\mathcal{O}\left(\frac{|E(G)|}{b \cdot n^3 + n}\right)$.

As $|E(G)| = \mathcal{O}(n^2)$ for any Nash equilibrium, we have PoA $= \mathcal{O}(n)$. □

3.4 Price of Stability

The price of stability (PoS), a close notion to price of anarchy, is defined as the ratio between the social optimum and the best Nash equilibrium,

$$\text{PoS} = \frac{\min_{s\in N} \text{cost}(s)}{\min_{s\in S} \text{cost}(s)},$$

where S is the set of all strategies and N is the set of strategies that are Nash equilibria. The price of stability expresses the loss in network performance in stable systems in comparison to those designed by a central performance. Corollary 5 gives insight into the price of stability in regions of the parameter space previously discussed in the context of the price of anarchy.

Corollary 5. *For $c > 1$ and $b + c < \frac{1}{n^2}$, the price of stability PoS $= \mathcal{O}(1)$.*

Proof. As the price of stability is smaller than or equal to the price of anarchy, we can follow from Corollary 4, that the price of stability is $\mathcal{O}(1)$ for $c > 1$. Additionally, Theorem 9 indicates that PoS $= \mathcal{O}(1)$ for $b + c < \frac{1}{n^2}$. □

However, we expect blockchain payment networks to fall into the remaining area, where $c + b \geq \frac{1}{n^2}$ and $c < 1$. In particular, considering the underlying uniform transaction scenario and the fixed blockchain fee equal to one (wlog), a competitive transaction fee would be $\frac{1}{n}$. Thus, an appropriate allocation for the weights is $b = \frac{1}{2n}$ and $c = \frac{1}{n}$, as the betweenness term counts each sender and receiver pair twice. For these weights the star is the social optimum (Theorem 1), as well as a Nash equilibrium (Theorem 7). Hence, the price of stability for payment networks is one; indicating that an optimal payment network is stable in a game with selfish players. Thus, payment networks can be stable and efficient.

4 Conclusion

We introduced a game-theoretic model to encapsulate the creation of payment networks. To this end, we generalized previous work, as our model is more complex and demands a combination of betweenness and closeness centralities that have thus far only been studied independently in network creation games.

First, we identified the social optimum for the entire parameter space of our game. Depending on the weights placed on the betweenness and closeness centralities either the complete graph, the star graph or the path graph is the social optimum. In the area of the parameter space that most accurately reflects payment networks, we found the star graph to be the social optimum.

Next, we examined the space of possible Nash equilibria. After establishing that finding the best response of a player is NP-hard, we analyzed prominent graphs and determined if and when they constitute a Nash equilibrium. We showed that the complete graph is the only Nash equilibrium if players place a large weight on their closeness centrality; reflecting payment channels in which players execute many transactions or value privacy highly. On the other hand, both the path and circle graph are Nash equilibria only for small number of players and thus are not expected to emerge as stable structures in payment networks. On the contrary, the star graph emerges as a Nash equilibrium for the areas of our parameter space most accurately representing payment networks. In addition, we observed that depending on the size of the subsets, the complete bipartite graph is also a Nash equilibrium in similar regions of the parameter space as the star graph.

Last, combining our results, we bounded the price of anarchy for a large part of the parameter space. In particular, we proved that when the closeness centrality weight is high, meaning that the players execute transactions frequently or demand privacy, the price of anarchy is constant; indicating little loss in network performance for selfish players. On the other hand, for small weight on the closeness centrality, we showed an $\mathcal{O}(n)$ upper bound on the price of anarchy. Nevertheless, the price of stability in payment networks is equal to one, since the star is both the social optimum and a Nash equilibrium for suitable parameters; demonstrating that blockchain payment networks can indeed be both stable and efficient, when forming more centralized network structures.

References

1. Hash time locked contracts. https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts. Accessed 25 June 2019
2. Micropayment channels network creation game simulation. https://gitlab.ethz.ch/hlioba/micropayment-channels-network-creation-game-simulation. Accessed 19 June 2019
3. Raiden network (2017). http://raiden.network/
4. Albers, S., Eilts, S., Even-Dar, E., Mansour, Y., Roditty, L.: On Nash equilibria for a network creation game. ACM Trans. Econ. Comput. **2**(1), 2:1–2:27 (2014)
5. Àlvarez, C., Blesa, M.J., Duch, A., Messegué, A., Serna, M.: Celebrity games. Theor. Comput. Sci. **648**, 56–71 (2016)
6. Anshelevich, E., Dasgupta, A., Kleinberg, J., Tardos, E., Wexler, T., Roughgarden, T.: The price of stability for network design with fair cost allocation. SIAM J. Comput. **38**(4), 1602–1623 (2008)
7. Avarikioti, G., Janssen, G., Wang, Y., Wattenhofer, R.: Payment network design with fees. In: Garcia-Alfaro, J., Herrera-Joancomartí, J., Livraga, G., Rios, R. (eds.) DPM/CBT -2018. LNCS, vol. 11025, pp. 76–84. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-00305-0_6
8. Avarikioti, G., Kogias, E.K., Wattenhofer, R.: Brick: asynchronous state channels. arXiv preprint: arXiv:1905.11360 (2019)
9. Avarikioti, G., Litos, O.S.T., Wattenhofer, R.: Cerberus channels: incentivizing watchtowers for bitcoin. In: Bonneau, J. (ed.) Financial Cryptography and Data Security, FC 2020. LNCS, vol. 12059, pp. 346–366. Springer, Cham (2020)
10. Avarikioti, G., Wang, Y., Wattenhofer, R.: Algorithmic channel design. In: 29th International Symposium on Algorithms and Computation (ISAAC), pp. 16:1–16:12 (2018)
11. Avarikioti, Z., Heimbach, L., Wang, Y., Wattenhofer, R.: Ride the lightning: the game theory of payment channels (2019)
12. Bei, X., Chen, W., Teng, S.H., Zhang, J., Zhu, J.: Bounded budget betweenness centrality game for strategic network formations. Theor. Comput. Sci. **412**(52), 7147–7168 (2011)
13. Bertrand, J.: Book review of theorie mathematique de la richesse social and of recherches sur les principes mathematiques de la theorie des richesses. Journal des Savants (1883)
14. Buechel, B., Buskens, V.: The dynamics of closeness and betweenness. J. Math. Sociol. **37**(3), 159–191 (2013)
15. Corbo, J., Parkes, D.C.: The price of selfish behavior in bilateral network formation. In: Proceedings of the Twenty-Fourth Annual ACM Symposium on Principles of Distributed Computing, PODC, pp. 99–107 (2005)
16. Decker, C., Russell, R., Osuntokun, O.: Eltoo: a simple layer 2 protocol for bitcoin. https://blockstream.com/eltoo.pdf
17. Decker, C., Wattenhofer, R.: A fast and scalable payment network with bitcoin duplex micropayment channels. In: Pelc, A., Schwarzmann, A.A. (eds.) SSS 2015. LNCS, vol. 9212, pp. 3–18. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-21741-3_1
18. Demaine, E.D., Hajiaghayi, M.T., Mahini, H., Zadimoghaddam, M.: The price of anarchy in network creation games, vol. 8, pp. 13:1–13:13 (2012)
19. Ehsani, S., et al.: A bounded budget network creation game. ACM Trans. Algorithms (TALG) **11**(4), 34 (2015)

20. Entringer, R.C., Jackson, D.E., Snyder, D.: Distance in graphs. Czechoslovak Math. J. **26**(2), 283–296 (1976)
21. Fabrikant, A., Luthra, A., Maneva, E.N., Papadimitriou, C.H., Shenker, S.: On a network creation game. In: Proceedings of the Twenty-Second ACM Symposium on Principles of Distributed Computing, PODC, pp. 347–351 (2003)
22. Freeman, L.C.: Centrality in social networks conceptual clarification. Soc. Netw. **1**(3), 215–239 (1978)
23. Gago Álvarez, S.: The betweenness centrality of a graph (2007). https://pdfs.semanticscholar.org/5673/a1a7229855a3b5a4bbfb69cf3571bcf73379.pdf
24. Green, M., Miers, I.: Bolt: anonymous payment channels for decentralized currencies. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 473–489. ACM (2017)
25. Hopwood, D., Bowe, S., Hornby, T., Wilcox, N.: Zcash protocol specification. Technical report, 2016–1.10. Zerocoin Electric Coin Company, Technical Report (2016)
26. Koutsoupias, E., Papadimitriou, C.: Worst-case equilibria. In: Meinel, C., Tison, S. (eds.) STACS 1999. LNCS, vol. 1563, pp. 404–413. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-49116-3_38
27. Lind, J., Naor, O., Eyal, I., Kelbert, F., Sirer, E.G., Pietzuch, P.R.: Teechain: a secure payment network with asynchronous blockchain access. In: Proceedings of the 27th ACM Symposium on Operating Systems Principles, SOSP, pp. 63–79 (2019)
28. Miller, A., Bentov, I., Bakshi, S., Kumaresan, R., McCorry, P.: Sprites and state channels: payment networks that go faster than lightning. In: Goldberg, I., Moore, T. (eds.) FC 2019. LNCS, vol. 11598, pp. 508–526. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-32101-7_30
29. Moscibroda, T., Schmid, S., Wattenhofer, R.: On the topologies formed by selfish peers. In: Proceedings of the Twenty-Fifth Annual ACM Symposium on Principles of Distributed Computing, PODC, pp. 133–142 (2006)
30. Moscibroda, T., Schmid, S., Wattenhofer, R.: Topological implications of selfish neighbor selection in unstructured peer-to-peer networks. Algorithmica **61**(2), 419–446 (2011)
31. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008)
32. Poon, J., Dryja, T.: The bitcoin lightning network: scalable off-chain instant payments (2015)
33. Spilman, J.: Anti dos for TX replacement. https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2013-April/002433.html. Accessed 17 Apr 2019
34. Van Saberhagen, N.: Cryptonote v 2.0 (2013)
35. Wood, G., et al.: Ethereum: a secure decentralised generalised transaction ledger (2014)