Payment Networks as Creation Games

Georgia Avarikioti, Rolf Scheuner, and Roger Wattenhofer

ETH Zurich, Switzerland
{zetavar,schrolf,wattenhofer}@ethz.ch

Abstract. Payment networks were introduced to address the limitation on the transaction throughput of popular blockchains. To open a payment channel one has to publish a transaction on-chain and pay the appropriate transaction fee. A transaction can be routed in the network, as long as there is a path of channels with the necessary capital. The intermediate nodes on this path can ask for a fee to forward the transaction. Hence, opening channels, although costly, can benefit a party, both by reducing the cost of the party for sending a transaction and by collecting the fees from forwarding transactions of other parties.
This trade-off spawns a network creation game between the channel parties. In this work, we introduce the first game theoretic model for analyzing the network creation game on blockchain payment channels. Further, we examine various network structures (path, star, complete bipartite graph and clique) and determine for each one of them the constraints (fee value) under which they constitute a Nash equilibrium, given a fixed fee policy. Last, we show that the star is a Nash equilibrium when each channel party can freely decide the channel fee. On the other hand, we prove the complete bipartite graph can never be a Nash equilibrium, given a free fee policy.

Keywords: blockchain· payment channels· layer 2· creation game· network design· Nash equilibrium· payment hubs

1 Introduction

Distributed ledgers that employ the Nakamoto [13] or similar consensus mechanisms suffer from major scalability problems [8]. In essence, the security of the consensus is based on the ability of each node to verify and store a replica of the entire blockchain history. Prominent solutions to this problem are payment channels [10, 14, 17]. Payment channels are constructions that allow participants of the blockchain to execute the transactions off-chain while maintaining the security guarantees of the blockchain. The parties that enter a payment channel open a joint account with a specific capital and update the distribution of this capital every time they exchange a transaction. This way the parties can execute an unlimited number of transactions as long as they all agree on the current distribution of capital. In case of a dispute, the blockchain acts as a judge, ensuring that the latest agreed capital distribution is enforced.

Multiple payment channels create a payment network, where a transaction can be executed even though there is no direct channel between payer and payee. Currently, this is achieved with the Bitcoin Lightning Network [14] using Hash Timelock Contracts (HTLCs) [1,10]. When a sender wants to route a transaction through the network, a path of channels is discovered that has enough capital on each edge to route the transactions to the receiver [12, 15, 16]. The intermediate nodes that move their capital act as service providers for the sender, and ask for a fee for their service. Therefore, operating a payment channel can offer revenue to the owner of the channel apart from reducing the cost of executing transactions on-chain. On the other hand, creating a payment channel is costly, since the opening and closing of the channel must occur on-chain, which requires to pay the regular blockchain transaction fee to the miner.

In this work, we study this trade-off. We investigate possible strategies for a participant. Assuming a constant blockchain fee for each transaction, when does it make sense to open a channel? If a path from sender to receiver already exists, does it make sense to create a cheaper path (or even a direct channel) to claim the fees for forwarding transactions? Our goal is to understand under which constraints specific network structures are Nash equilibiria. In other words, when can the participants of the network increase their profit (or decrease their costs) by changing the network structure? Further, we ask which network structures are stable under a free fee policy where each node on the network that operates a channel can set its own fee on the channel. To the best of our knowledge, our work is the first to analyze payment channels in a formal game theoretic model.

Our Contributions. First, we introduce a formal game-theoretic model which we later use to study the potential strategies for network creation for the nodes of the payment network. The model encapsulates a network creation game on payment channels: each node of the network can create multiple channels to other nodes to collect fees from the transactions that are routed through their channel. However, each channel creation costs the blockchain fee, and also each node competes with the other nodes in the network, since the sender of each transactions will choose the cheapest path to route the transaction to the receiver.

We assume there is a fixed fee a sender has to pay to each intermediate node to route the transaction to the receiver. Further, we assume nodes have unlimited temporary capital, and that each pair of nodes are sender and receiver to an equal amount of transactions. Under these assumptions, we explore various network structures, namely the path, the star, the complete bipartite graph and the clique. We find that each network structure constitutes a Nash equilibrium for a specific fee value. In particular, we show that the path is a weak Nash equilibrium only if the network fee is zero. Then, we show an upper bound for value of the fee on the star graph. The bound depends on the number of transactions, number of nodes and the value of the blockchain fee. This means that creating a hub is a Nash equilibrium as long as the fee is very low (compared to the blockchain fee). We observe that if the fee is above the upper bound, a two-

stars structure emerges as a Nash equilibrium. We generalize this observation by examining complete bipartite graphs. We provide upper and lower bounds for such graphs which additionally depend on the number of centers (smaller side of the complete bipartite graph). This specific network structure defines an entire class of Nash equilibria. Finally, we consider the complete graph (clique), which is naturally a Nash equilibria when the network fee is very high.

From the plethora of network structures that constitute Nash equilibria when the fee policy is fixed, only the star is stable under a free fee policy. Specifically, we show that the star is a pure Nash equilibrium, and the nodes will set the fee almost equal to the upper bound of the fixed fee policy. Further, we prove that the complete bipartite graph can never be a Nash equilibrium when nodes chose the fee of their channels freely as part of their strategy.

2 Model

In this section, we introduce the game theoretic model. To this end, we first define the necessary notation and assumptions.

Capital & fees. We assume all participants (nodes of the network) have unlimited temporary capital and thus the capital locked in all channels is also considered unlimited. This means that the channels can never be depleted. Moreover, this leads to stable fees that do not depend on the value of the routed transaction, because the participants are only interested in the number of transactions routed through their channel since the capital movement does not cost (they have unlimited capacity).

The cost of every transaction and hence the cost of opening and closing a channel on the blockchain costs the blockchain fee. We assume a fixed blockchain fee, $F_B \in \mathbb{R}^+$, i.e., the fee is constant and stable over time. Further, we assume the fee is unilaterally paid by the node opening or closing the channel. We also assume a fee f_0 for forwarding a transaction through a channel (that is not owned by the sender of the transaction) is the same for all nodes and stable in time.

Information & time. We assume full information, i.e., every node of the system knows the complete payment scenario, and the channels created by other nodes. Although the decision of closing and opening a channel can occur at any time by any participant of the network, we assume a simultaneous game, i.e., the participants open the channels in the beginning before executing any transactions. This is reasonable because we assume a full information game, thus every node knows its optimal strategy apriori.

Notation. The set of nodes participating in the network is denoted by $\boldsymbol{N}$, and the set of transactions to be executed (payment scenario) by $\boldsymbol{P}$. We assume $N > 3$ and we use the terms transaction and payment interchangeably throughout the paper. We define as $\boldsymbol{R}(x, p)$ the (set of) cheapest route(s) of a transaction $p \in \boldsymbol{P}$

in network state x. The network state x is dependent on the strategy of the nodes, i.e. which channels the nodes have opened in the network. We note that if there is no route with cost lower than the blockchain fee, the set will return empty and the transaction will be executed on the blockchain. Thus, the cost for a transaction p for the sender of the transaction on a network state x is the number of edges of the shortest path (for constant fee f_0 the cheapest is the shortest path) times the fee f_0,

$$f(x,p) = \begin{cases} (|\boldsymbol{R}(x,p)| - 1) \cdot f_0, \ if \ \boldsymbol{R}(x,p) \neq \emptyset \\ F_B, \ else \end{cases}$$

On the other hand, the revenue of a node $u \in \boldsymbol{N}$ from a transaction $p \in \boldsymbol{P}$ when executed on the network in state x is f_0 if node u is part of the cheapest route $\boldsymbol{R}(x,p)$; otherwise the revenue is zero.

Moreover, the *strategy set* of a node $u \in \boldsymbol{N}$ is the set of all strategies available to node u. It is denoted as $\boldsymbol{S}_u$. The strategy of node u is denoted as $\mu_u \in \boldsymbol{S}_u$. The strategy set in our setting represents the channels a node decides to open at the beginning of the game. A *strategy combination* is a set containing a strategy for every node. The set of all possible strategy combinations is defined as $\boldsymbol{S}^N := \prod_{u \in \boldsymbol{N}} \boldsymbol{S}_u$, while a strategy combination is denoted by $\boldsymbol{\mu} \in \boldsymbol{S}^N$. For simplicity, we will abuse the notation μ and μ_u to also denote the cardinality of the set, i.e., how many channels are open in the network and how many channels node u opens in the network, respectively. Last, we define the number of on-chain payments made by a node u as b_u and the total number of on-chain payments as $b = \sum_{\forall u \in \boldsymbol{N}} b_u$.

Next, we define the necessary functions for the analysis, namely the cost function, the social cost and the social optimum.

Cost Function. The cost function contains the cost for channel creation, on-chain payments, payments routed through the network and the revenue from forwarding payments. For a node u it is defined as

$$c(\boldsymbol{\mu}, \mu_u) = \mu_u \cdot F_B + b_u \cdot F_B + \sum_{p \in \boldsymbol{P}: s(p) = u} f(x,p) - \sum_{p \in \boldsymbol{P}: u \in \boldsymbol{R}(x,p)} f_0$$

where $s(p)$ denotes the sender of transaction p. In our setting, sender and receiver of a transaction p are the only relevant pieces of information of each payment, since all fees are independent of the value of a transaction.

Social Cost. The social cost (or negative welfare) is the sum of the costs of all nodes

$$-W = \sum_{n \in \boldsymbol{N}} c(\boldsymbol{\mu}, \mu_u) = (\mu + b) \cdot F_B$$

Social Optimum. The social optimum is the minimum social cost, which depends on the number of open channels and the number of payments executed on-chain.

This term is minimized when all transactions are executed off-chain and the network forms a tree (connected with minimum number of channels). Hence, the social optimum is $min(-W) = (N-1) \cdot F_B$

3 Channel Creation Game

First, we show some observations that hold generally under any set of transactions and graph structure. Then, we analyze specific structures and determine under which parameters they constitute a Nash equilibrium.

3.1 Basic Properties

Lemma 1. *In a pure Nash equilibrium, no channels are opened twice.*

Proof. (Towards contradiction.) Suppose there is a pure Nash equilibrium in which two nodes have opened a channel with each other twice. In this case, each node can reduce his cost by not opening the second channel and thus the strategy cannot be a Nash equilibrium. □

Lemma 2. *In a pure, strict Nash equilibrium*[1]*, none of the transactions are executed on-chain.*

Proof. (Towards contradiction.) Suppose there is a pure, strict Nash equilibrium in which a node (sender) executes a transaction on-chain. If there is a channel to the receiver of the transaction, the sender can reduce his cost by simply using the channel. The same holds if there is a path of channels with total fees less than the blockchain fee. Therefore, either there is no cheap path from sender to receiver or no path at all. In this case, if the sender has at least two transactions to send to the receiver, he would open a channel and reduce the cost. Thus, the sender has a single transaction to send to the receiver. However, the cost of opening a channel and the cost of executing the transaction on-chain is exactly the same (blockchain fee). If we assume there are no transactions routed through the channel from sender to receiver, the payoff (cost) of the sender in both strategies is the same. Hence, executing the transaction on-chain cannot be a strict Nash equilibrium. Thus, there are transactions routed through the channel from sender to receiver. Then, the payoff of the sender increases and hence the dominant strategy is to open the channel. This contradicts the assumption that executing the transaction on-chain is a Nash equilibrium. □

Next, we analyse the channel creation game for a homogeneous payment scenario, where every node makes exactly $k \geq 1$ payments to every other node. The number of transactions is therefore $P = k \cdot N \cdot (N-1)$. For this payment scenario, we analyze multiple strategy combinations, i.e., different graph structures such

[1] If a strategy is always strictly better than all others for all profiles of other players' strategies, then it is strictly dominant. If the strategy is strictly dominant for all players, then it is a strict Nash equilibrium.

as the path, the star, a complete bipartite graph and the clique, to discover under which parameters these graph structures constitute a Nash equilibrium. We note that all graph structures that are trees (e.g. path, start, complete bipartite graph) are social optima.

3.2 Path

The first graph structure we investigate is the path: each node connects to the node with the next higher ID. The node with the highest ID does not create a channel, but he is connected to the network through the node with the second highest ID.

Social Cost. The social cost is $-W = (N-1) \cdot F_B$.

Nash Equilibrium. A specific strategy is a Nash equilibrium if none of the players can increase their payoff by deviating from it. This means that the path is a NE only if all possible deviations lead to higher cost (or equivalent if it is a weak NE) for the deviating node. We observe that for $f_0 = 0$, deviating from the path structure cannot decrease the cost, thus the path is a weak NE (similarly to every other tree structure). However, for any fee $f_0 > 0$, the first node can increase the revenue from the fees, and thus decrease his cost, by connecting to a middle node on the path and allowing transactions to be routed through his channel. Thus, for any non-zero fee, the path is not a NE.

3.3 Star

The second graph structure we investigate is the star: one node creates channels to everyone else, while the other nodes do not create any channels. The strategy to create channels to $a \in [0, N-1]$ outer nodes is denoted as (a).

Cost Functions. The cost of the center node is $c(\boldsymbol{\mu}, (N-1)) = (N-1) \cdot F_B - (N-1) \cdot (N-2) \cdot k \cdot f_0$.
The cost of the outer nodes is $c(\boldsymbol{\mu}, (0)) = (N-2) \cdot k \cdot f_0$.
The social cost is $-W = (N-1) \cdot F_B$.

Nash Equilibrium. A node can only deviate from the strategy as follows: An outer node creates channels to $a \in [1, N-2]$ other outer nodes. This holds because in the homogeneous payment scenario, a pure Nash equilibrium demands a connected graph, else Lemma 2 is violated. This means the center node will not disconnect the graph. Moreover, from Lemma 1 no outer node will create a channel to the center node.

If an outer node creates channels to $a \in [1, N-2]$ other outer nodes, his cost function is $c(\boldsymbol{\mu}, (a)) = a \cdot F_B + (N-2-a) \cdot k \cdot f_0 - a \cdot (a-1) \cdot k \cdot \frac{1}{2} \cdot f_0$.

If there is an $a \in [1, N-2]$ for which the cost function of an outer node is decreased, then the star is not a NE. Since the second derivative with respect to a is strictly negative, we only have to check the corner cases below:

- For $a = 1$: $c(\boldsymbol{\mu}, (0)) < c(\boldsymbol{\mu}, (1)) \Leftrightarrow f_0 < \frac{F_B}{k}$.
- For $a = N-2$: $c(\boldsymbol{\mu}, (0)) < c(\boldsymbol{\mu}, (N-2)) \Leftrightarrow f_0 < \frac{F_B}{k} \cdot \frac{2}{N-1}$.

Thus, for $N > 3$, the star is a NE when

$$f_0 < \frac{F_B}{k} \cdot \frac{2}{N-1}$$

3.4 Star with two centers

We observe that for a very low constant fee any star can be a Nash equilibrium. Further, we notice that if the fee is high enough the dominant strategy for the outer nodes is to create more channels, eventually becoming the center of a second star. We examine this exact case, where there are two center nodes, each creating channels to all outer nodes, but not to each other. The outer nodes do not create any channels. We denote the strategy to create $a \in [0, 2]$ channels to center nodes and $b \in [0, N-2]$ channels to outer nodes as (a, b).

Cost Functions. The cost of the center nodes is $c(\boldsymbol{\mu}, (0, N-2)) = (N-2) \cdot F_B + k \cdot f_0 - (N-2) \cdot (N-3) \cdot k \cdot \frac{1}{2} f_0$.
The cost of the outer nodes is $c(\boldsymbol{\mu}, (0, 0)) = (N-3) \cdot k \cdot f_0 - 2 \cdot k \cdot \frac{1}{(N-2)} f_0$.
The social cost is $-W = 2 \cdot (N-2) \cdot F_B$.

Nash Equilibrium. The nodes can deviate as follows:

(A) A center node creates channels to $b \in [1, N-3]$ outer nodes.
(B) A center node creates channels to $b \in [0, N-2]$ outer nodes and creates a channel to the other center node.
(C) An outer node creates channels to $b \in [1, N-3]$ other outer nodes.

We analyze each case to determine the parameter space for which these deviations do not decrease the cost of a node, and thus the two center structure is a NE.

(Deviation A) If a center node created channels to only $b \in [1, N-3]$ outer nodes, his cost function would become

$$c(\boldsymbol{\mu}, (0, b)) = b \cdot F_B + k \cdot f_0 + (N-2-b) \cdot k \cdot 2 f_0 - b \cdot (b-1) \cdot k \cdot \frac{1}{2} f_0$$

This cost function must be higher than $c(\boldsymbol{\mu}, (0, N-2))$ for all b. Since the second derivative w.r.t. b is strictly negative, we only have to check the corner cases:

- For $b = 1$: $c(\boldsymbol{\mu}, (0, N-2)) < c(\boldsymbol{\mu}, (0, 1)) \Leftrightarrow f_0 > \frac{F_B}{k} \cdot \frac{2}{N+2}$.
- For $b = N-3$: $c(\boldsymbol{\mu}, (0, N-2)) < c(\boldsymbol{\mu}, (0, N-3)) \Leftrightarrow f_0 > \frac{F_B}{k} \cdot \frac{1}{N-1}$

(Deviation B) If an center node creates a channel to the other center node and channels to $b \in [0, N-2]$ outer nodes, his cost function is

$$c(\boldsymbol{\mu}, (1, b) = (b+1) \cdot F_B + (N-2-b) \cdot k \cdot f_0 - b \cdot (b-1) \cdot k \cdot \frac{1}{2} f_0$$

This cost function must be higher than $c(\boldsymbol{\mu}, (0, N-2))$ for all b. Similarly, we only have to check the corner cases:

- For $b = 0$: $c(\boldsymbol{\mu}, (0, N-2)) < c(\boldsymbol{\mu}, (1, 0)) \Leftrightarrow f_0 < \frac{F_B}{k} \cdot \frac{2}{N}$.
- For $b = N-2$: $c(\boldsymbol{\mu}, (0, N-2)) < c(\boldsymbol{\mu}, (1, N-2)) \Leftrightarrow f_0 > \frac{F_B}{k}$.

(Deviation C) If an outer node creates channels to $b \in [1, N-2]$ other outer nodes, his cost function is

$$c(\boldsymbol{\mu}, (0, b)) = b \cdot F_B + (N-3-b) \cdot k \cdot f_0 - 2 \cdot k \cdot \frac{1}{(N-2)} f_0 - b \cdot (b-1) \cdot k \cdot \frac{1}{3} f_0$$

This cost function must be higher than $c_o(\boldsymbol{\mu}, (0, 0))$ for all b. Similarly, we only have to check the corner cases:

- For $b = 1$: $c(\boldsymbol{\mu}, (0, 0)) < c(\boldsymbol{\mu}, (0, 1)) \Leftrightarrow f_0 < \frac{F_B}{k}$.
- For $b = N-3$: $c(\boldsymbol{\mu}, (0, 0)) < c(\boldsymbol{\mu}, (0, N-3)) \Leftrightarrow f_0 < \frac{F_B}{k} \cdot \frac{3}{N-1}$.

Combining all the bounds from the deviating strategies, for $N > 3$, we derive the parameter space for which the two center structure is a NE. Specifically, the conditions reduce to

$$\frac{F_B}{k} \cdot \frac{2}{N} < f_0 < \frac{F_B}{k} \cdot \frac{3}{N-1}$$

3.5 Complete bipartite graph

Previously, we showed that stars with one or two center nodes can be a Nash equilibrium, if there is a constant fee that fulfills certain conditions. Furthermore, if f_0 is high, outer nodes decrease their cost by creating channels to other outer nodes. Intuitively, this leads to a NE that is a bipartite graph structure. We study exactly this case: $c \in [2, N/2]$ nodes build a center by creating channels to everyone else but each other. For simplicity we denote the number of outer nodes by $d := N - c$. The network structure now is a complete bipartite graph with c nodes in the smaller partition and d nodes in the larger partition. We denote the strategy to create channels to $a \in [0, c]$ center nodes and to $b \in [0, d]$ outer nodes as (a, b).

Cost Functions. The cost of the center nodes is $c(\boldsymbol{\mu}, (0, d)) = d \cdot F_B + (c-1) \cdot k \cdot f_0 - d \cdot (d-1) \cdot k \cdot \frac{1}{c} f_0$.
The cost of the outer nodes is $c(\boldsymbol{\mu}, (0, 0)) = (d-1) \cdot k \cdot f_0 - c \cdot (c-1) \cdot k \cdot \frac{1}{d} f_0$.
The social cost is $-W = c \cdot (N-c) \cdot F_B$.

Nash Equilibrium. The nodes can deviate as follows:

(A) A center node creates channels to only $b \in [1, d-1]$ outer nodes.
(B) A center node creates channels to $a \in [1, c-1]$ center nodes and to $b = 0$ outer nodes.
(C) A center node creates channels to $a \in [1, c-1]$ center nodes and to $b \in [1, d]$ outer nodes.
(D) An outer node creates channels to $b \in [1, d-1]$ other outer nodes.

Next, we discover the parameter space for which the strategies above lead to the increase of the cost function of a node.

(Deviation A) If a center node created channels to only $b \in [1, d-1]$ outer nodes, his cost function would become

$$c(\boldsymbol{\mu}, (0, b)) = b \cdot F_B + (c-1) \cdot k \cdot f_0 + (d-b) \cdot k \cdot 2f_0 - b \cdot (b-1) \cdot k \cdot \frac{1}{c} f_0$$

This cost function must be higher than $c(\boldsymbol{\mu}, (0, d))$ for all b. Since the second derivative w.r.t. b is strictly negative, we only check the corner cases:

- For $b = 1$: $c(\boldsymbol{\mu}, (0, d)) < c(\boldsymbol{\mu}, (0, 1)) \Leftrightarrow \frac{F_B}{k} \cdot \frac{c}{N+c} < f_0$.
- For $b = d-1$: $c(\boldsymbol{\mu}, (0, d)) < c(\boldsymbol{\mu}, (0, d-1)) \Leftrightarrow \frac{F_B}{k} \cdot \frac{c}{2N-2} < f_0$.

(Deviation B) If a center node creates channels to $a \in [1, c-1]$ other center nodes and to $b \in [1, d]$ outer nodes, his cost function is

$$c(\mu, (a, b)) = (a+b) \cdot F_B + (d-b) \cdot k \cdot f_0 + (c-1-a) \cdot k \cdot f_0$$

$$-b \cdot (b-1) \cdot k \cdot \frac{1}{c} f_0 - a \cdot (a-1) \cdot k \cdot \frac{1}{d+1} f_0$$

This cost function must be higher than $c(\boldsymbol{\mu}, (0, d))$. Since the second derivatives w.r.t. a and b are strictly negative, we only have to check the corner cases:

- For $a = 1, b = 1$:

$$c(\boldsymbol{\mu}, (0, d)) < c(\boldsymbol{\mu}, (1, 1)) \Leftrightarrow \frac{F_B}{k} \cdot \frac{cN - c^2 - 2c}{N^2 - cN + N - 3c} < f_0$$

- For $a = 1, b = d$: $c(\boldsymbol{\mu}, (0, d)) < c(\boldsymbol{\mu}, (1, d)) \Leftrightarrow f_0 < \frac{F_B}{k}$
- For $a = c-1, b = 1$:

$$c(\boldsymbol{\mu}, (0, d)) < c(\boldsymbol{\mu}, (c-1, 1)) \Leftrightarrow \frac{F_B}{k} \cdot \frac{cN^2 - 3c^2N + cN + 2c^3 - 2c^2}{N^3 - 2cN^2 + cN - N + c^2 - c} < f_0$$

- For $a = c-1, b = d$: $c(\boldsymbol{\mu}, (0, d)) < c(\boldsymbol{\mu}, (c-1, d)) \Leftrightarrow f_0 < \frac{F_B}{k} \cdot \frac{N-c+1}{N-1}$

(Deviation C) If a center node creates channels to $a \in [1, c-1]$ other center nodes and to $b = 0$ outer nodes, his cost function is

$$c(\boldsymbol{\mu}, (a, 0)) = a \cdot F_B + d \cdot k \cdot f_0 + (c - 1 - a) \cdot k \cdot 2f_0 - (a) \cdot (a - 1) \cdot k \cdot \frac{1}{d+1} f_0$$

This cost function must be higher than $c(\boldsymbol{\mu}, (0, d))$ for all a. Since the second derivative w.r.t. a is strictly negative, we only have to check the corner cases:

- For $a = 1$:

$$c(\boldsymbol{\mu}, (0, d)) < c(\boldsymbol{\mu}, (1, 0)) \Leftrightarrow \frac{F_B}{k} \cdot \frac{cN - c^2 - c}{N^2 - cN - N + c^2 - 2c} < f_0$$

- For $a = c - 1$:

$$c(\boldsymbol{\mu}, (0, d)) < c(\boldsymbol{\mu}, (c-1, 0)) \Leftrightarrow \frac{F_B}{k} \cdot \frac{cN^2 - 3c^2N + 2cN + 2c^3 - 3c^2 + c}{N^3 - 2cN^2 + 2cN - N} < f_0$$

(Deviation D) If an outer node creates channels to $b \in [1, d-1]$ other outer nodes, his cost function is

$$c(\boldsymbol{\mu}, (0, b)) = b \cdot F_B + (d - 1 - b) \cdot k \cdot f_0 - c \cdot (c-1) \cdot k \cdot \frac{1}{d} f_0 - b \cdot (n-1) \cdot k \cdot \frac{1}{c+1} f_0$$

This cost function must be higher than $c_o(\boldsymbol{\mu}, (0, 0))$ for all b. Since the second derivative w.r.t. b is strictly negative, we only have to check the corner cases:

- For $b = 1$: $c(\boldsymbol{\mu}, (0, 0)) < c(\boldsymbol{\mu}, (0, 1)) \Leftrightarrow f_0 < \frac{F_B}{k}$
- For $b = d - 1$: $c(\boldsymbol{\mu}, (0, 0)) < c(\boldsymbol{\mu}, (0, d-1)) \Leftrightarrow f_0 < \frac{F_B}{k} \cdot \frac{c+1}{N-1}$

From the analysis on the possible deviations from the strategy, we derive multiple upper and lower bounds for the value of f_0. For $N > 3$ and $2 \leq c \leq {}^{N}/_{2}$ these conditions reduce to the following:

$$f_0 > \frac{F_B}{k} \cdot \frac{cN - c^2 - 2c}{N^2 - cN + N - 3c}$$

$$f_0 > \frac{F_B}{k} \cdot \frac{cN - c^2 - c}{N^2 - cN - N + c^2 - 2c}$$

$$f_0 < \frac{F_B}{k} \cdot \frac{c+1}{N-1}$$

We have defined not only one Nash equilibrium in this analysis, but a whole class of Nash equilibria. Table 1 shows the numerical values for the bounds of a complete bipartite graph as Nash equilibrium. Figure 1 shows a plot of the bounds for $N = 10^3$. The Nash equilibria lay in the thin area between the lowest red and the highest blue line.

N	c	lower bound $[\frac{F_B}{k}]$	upper bound $[\frac{F_B}{k}]$	active lb	active ub
10^3	2	$.2000000 \cdot 10^{-2}$	$.30030 \cdot 10^{-2}$	5	3
	3	$.2999991 \cdot 10^{-2}$	$.40040 \cdot 10^{-2}$	5	3
	5	$.4999925 \cdot 10^{-2}$	$.60060 \cdot 10^{-2}$	5	3
	10	$.9999192 \cdot 10^{-2}$	$.11011 \cdot 10^{-1}$	5	3
	100	$.9970024 \cdot 10^{-1}$	.10110	3	3
	499	.4975016	.50050	3	3
	500	.4984984	.50150	3	3
10^4	2	$.20000 \cdot 10^{-3}$	$.30003 \cdot 10^{-3}$	5	3
	3	$.29997 \cdot 10^{-3}$	$.40004 \cdot 10^{-3}$	5	3
	5	$.49995 \cdot 10^{-3}$	$.60006 \cdot 10^{-3}$	5	3
	10	$.99990 \cdot 10^{-3}$	$.11001 \cdot 10^{-2}$	5	3
	100	$.99981 \cdot 10^{-2}$	$.10101 \cdot 10^{-1}$	5	3
	1000	$.99971 \cdot 10^{-1}$	.10011	3	3
	4999	.49976	.50005	3	3
	5000	.49985	.50015	3	3
10^5	2	$.200000 \cdot 10^{-4}$	$.300003 \cdot 10^{-4}$	5	3
	3	$.299997 \cdot 10^{-4}$	$.400004 \cdot 10^{-4}$	5	3
	5	$.499995 \cdot 10^{-4}$	$.600006 \cdot 10^{-4}$	5	3
	10	$.999990 \cdot 10^{-4}$	$.110001 \cdot 10^{-3}$	5	3
	100	$.999990 \cdot 10^{-3}$	$.101001 \cdot 10^{-2}$	5	3
	1000	$.999971 \cdot 10^{-2}$	$.100101 \cdot 10^{-1}$	3	3
	10000	$.999971 \cdot 10^{-1}$	.100011	3	3
	49999	.499976	.500005	3	3
	50000	.499985	.500015	3	3

Table 1. Numerical results for the lower and bounds for a complete bipartite graph as a Nash equilibrium.

3.6 Clique

The last graph structure we investigate is the clique, i.e., the complete graph. In this case, the i-th node opens $N - i$ channels. The strategy of creating channels to a nodes without self-loops is denoted as (a).

Cost Functions. The cost of the i-th node is $c(\boldsymbol{\mu}, (N - i)) = (N - i) \cdot F_B$. The social cost is $-W = \frac{N \cdot (N-1)}{2} \cdot F_B$.

Nash Equilibrium. The nodes can deviate as follows:

(A) The first node creates channels to only $a \in [1, N - 2]$ other nodes.
(B) Node i (but not the first or last one) creates channels to only $a \in [0, N-i-1]$ nodes from the set of nodes he would originally connect to (node $i + 1$ to node N).

Now, we analyze these deviation strategies to explore the parameter space for which the strategies above lead to the increase of the cost function of a node.

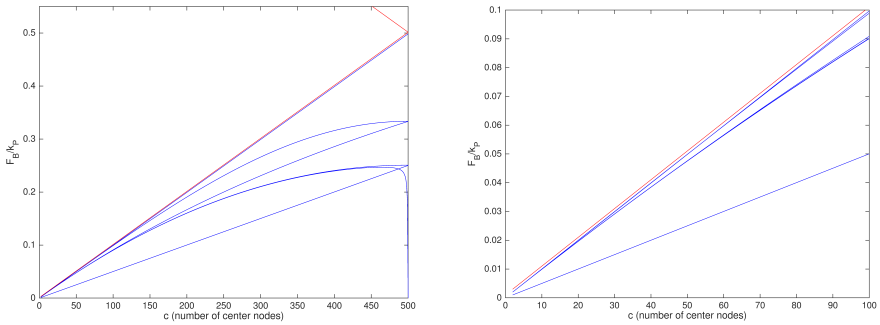

Fig. 1. Plots of the bounds for $N = 10^3$ with the upper bounds in red and the lower bounds in blue.

(Deviation A) If the first node creates channels to $a \in [1, N-2]$ other nodes his cost function is $c(\boldsymbol{\mu}, (a)) = a \cdot F_B + (N-1-a) \cdot k \cdot f_0$. This cost function must be higher than $c(\boldsymbol{\mu}, (N-1))$ for all a. Thus, $c(\boldsymbol{\mu}, (N-1)) < c(\boldsymbol{\mu}, (a)) \Leftrightarrow f_0 > \frac{F_B}{k}$.

(Deviation B) If node i (not the first or last one) creates channels to $a \in [0, N-i-1]$ nodes from the set of nodes he would originally connect to (node $i+1$ to node N), his cost functions is $c(\boldsymbol{\mu}, (a)) = a \cdot F_B + (N-i-a) \cdot k \cdot f_0$. This cost function must be higher than $c(\boldsymbol{\mu}, (N-i))$ for all a. Thus, $c(\boldsymbol{\mu}, (N-i)) < c(\boldsymbol{\mu}, (a)) \Leftrightarrow f_0 > \frac{F_B}{k}$.

To summarize, the clique is a Nash equilibrium for $f_0 > \frac{F_B}{k}$.

3.7 The fee game

In this subsection we investigate how the nodes set the fees, if the network structure is fixed to one of the previously found Nash equilibria. Especially, we try to find a Nash equilibrium, which also holds for the conditions discussed in the previous subsections. Therefore, we slightly change the model as follows: x is a Nash equilibrium from the previous subsections. The nodes can only set a constant fee on each of their channels. Further, the nodes cannot create new channels. We still consider simultaneous game play, i.e., the nodes must (simultaneously) choose their strategy before any transaction is executed in the network. The payment scenario is still the same (homogeneous).

Complete Bipartite Graph. We start with a complete bipartite graph with $c \in [2, N/2]$ nodes in the smaller partition creating the channels. The goal of this analysis is to gain a better intuition of the fee evolution and therefore determine the number of hubs that will be eventually established.

We make following statement about the Nash equilibrium of the described game.

Lemma 3. *For $k > 2$, a strategy combination is a (weak) Nash equilibrium if and only if there are at least two node-distinct paths which are free (zero fees) for all indirect transactions.*

Proof. ($\rightarrow$) Suppose there is a Nash equilibrium in which there is a set of k indirect transactions (according to the payment scenario, each pair of sender and receiver executes k transactions) that can be routed only through a single path with positive fees. Then, another node will open a channel to connect the two nodes and increase his payoff, since on expectation half the k transactions will go through the new channel. Contradiction.

Suppose now, there is only a single path with zero fees to route the transaction. Then, the nodes acting as intermediaries will increase the fee almost matching the price of the blockchain fee. In such a case, we have the same effect as described above. Contradiction.

Therefore, there cannot be a single path connecting any two nodes in the network. Suppose now there are multiple node-distinct paths that connect sender and receiver, but with positive fees. Then, each node of these paths will decrease the fee in an attempt to win out the competition by being the cheapest path. Contradiction. Therefore, any strategy that is a Nash equilibrium must contain at least two node-distinct paths for each pair of sender and receiver.

($\leftarrow$) If there exist a path with zero fees for every transaction, no node stands to gain from opening a new channel. Furthermore, increasing the fee in any path will not lead to the decrease of the cost function (higher revenue) since the path containing the non-zero fee will be ignored and no transactions will be routed through such a path. Thus, no node can gain from choosing a different strategy, i.e., the strategy combination is a Nash equilibrium. □

Theorem 1. *The complete bipartite graph is not a Nash Equilibrium when the nodes are free to chose the fees on their channels.*

Proof. Follows immediately from Lemma 3 and the lower bound established in subsection 3.5. □

Star. Next, we consider the fee evolution when the network structure is a star. The reason we proceed with this specific network structure is the previous observations; when nodes can freely chose the fees they impose on their channels, having multiple paths leads to zero-fee paths. Intuitively, the star does not suffer from this problem.

Particularly, we notice that the center node is the only node that can charge fees, since all transactions are routed through the center node. However, in subsection 3.3, we showed that there is an upper bound on the value of the fee the center node can ask for; otherwise other nodes will deviate from the strategy combination and form a second hub.

Corollary 1. *The star is a pure Nash equilibrium when* $f_0 = \frac{F_B}{k} \cdot \frac{2}{N-1} - \epsilon$.

4 Related Work

Payment channels were originally introduced by Spilman [17]. The core idea was to use unidirectional channels with a predefined sender and receiver. Later, various constructions for bidirectional payment channels were proposed [6, 9, 10, 14, 17]. They all use a common account for the parties and off-chain exchange of signed transactions proving the state of the channel. The creation of multiple such channels on a common blockchain network leads to the formation of channel networks, such as the Lightning network [14] on Bitcoin [13], and the Raiden network [2] on Ethereum [18]. In this work, we study different strategies for the nodes in such payment networks, independent of which payment channel construction method is used. Thus, this work applies to all payment channel solutions.

Avarikioti et al. [5, 7] formulated a similar problem to the one studied in this paper. Their goal was to find an optimal strategy for a central coordinator, a so-called payment service provider. In contrast to [5, 7], our work studies a situation with *multiple* players. In other words, our work is rooted in the area of game theory, whereas [5, 7] was using optimization methods. Despite these differences, we found that the near-optimal solution of [5, 7] (the star as network structure) is also a Nash equilibrium in an uncoordinated situation. So we get a similar result despite two completely different approaches. This is a strong indication that the Lightning network (and similar others) will eventually develop into a more centralized network structure.

Network creation games, originally introduced in by Fabrikant et al. [11], are used to model distributed networks with rational players. Each player wants to maximize/minimize a profit/cost function which represents the cost of creating and using the network. Fabrikant et al. [11] modeled the Internet using Network Creation Games. They introduced a cost function containing the network creation cost and the sum of the distances to the other nodes. For their model, they proved upper and lower bounds for the Price of Anarchy(PoA). They also conjectured that the Nash equilibria in this game are trees, however this was disproved by Albers et al. [3]. Alon et al. [4] aimed for stronger bounds on PoA of the Network Creation Game (sum and local-diameter version). Both these works, however, use simple cost functions, where the creation cost and the usage cost of an node are independent. In contrast, in this work the cost function of a node on the payment network contains both the revenue from the fees of the channel when the node is an intermediate node in a multihop transaction as well as the fees paid by the node when he is sending a multihop transaction. Hence, the cost function depends on the state of the network which itself contains the individual fee policies of the nodes. Overall, the channel creation game is probably more complex than previous work in this domain.

5 Conclusion

We introduced the first game-theoretic model that encapsulates the payment channel creation game on blockchain networks. First, we explored various net-

work structures and determined the parameter space for which they constitute a Nash equilibrium. For the analysis, we initially assumed a fixed fee policy where each node benefits the same for each transaction routed through any of his channels. Then, we briefly considered a free fee policy, where the fee of each channel is part of the strategy of the node.

Particularly, for the fixed fee policy, we observed that the path is a Nash equilibrium only when the fee is zero. Otherwise, for a small positive fee we noticed the formation of a star. Furthermore, we showed that beyond an upper bound the star ceased to be a Nash equilibrium and multiple star structures emerged. This observation lead to the investigation of the complete bipartite graph which defined a class of Nash equilibria dependent on the correlation between the sizes of the two independent sets of nodes. Finally, the complete graph was proven to be a Nash equilibrium when the fee is relatively high, as expected.

More importantly, we showed that even in a free fee policy, the star with uniform fees almost equal to the upper bound discussed above is a pure Nash equilibrium. On the contrary, the complete bipartite graph was proven unstable under this fee policy; we proved that a complete bipartite graph can never be a Nash equilibrium. We note, that these observations indicate the stability of a star structure, even though its centralized nature is opposed to the philosophy of decentralized and distributed payment networks.

References

1. Bitcoin Wiki: Hashed Time-Lock Contracts. https://en.bitcoin.it/wiki/Hashed_Timelock_Contracts, accessed: 2018-05-16
2. Raiden network (2017)
3. Albers, S., Eilts, S., Even-Dar, E., Mansour, Y., Roditty, L.: On nash equilibria for a network creation game. ACM Transactions on Economics and Computation **2**(1), 2 (2014)
4. Alon, N., D. Demaine, E., Hajiaghayi, M., Leighton, T.: Basic network creation games. SIAM Journal on Discrete Mathematics **27**, 106–113 (01 2010). https://doi.org/10.1145/1810479.1810502
5. Avarikioti, G., Janssen, G., Wang, Y., Wattenhofer, R.: Payment network design with fees. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology, pp. 76–84. Springer (2018)
6. Avarikioti, G., Kogias, E.K., Wattenhofer, R.: Brick: Asynchronous state channels (2019)
7. Avarikioti, G., Wang, Y., Wattenhofer, R.: Algorithmic Channel Design. In: 29th International Symposium on Algorithms and Computation (ISAAC), Jiaoxi, Yilan County, Taiwan (December 2018)
8. Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E.G., et al.: On scaling decentralized blockchains. In: International Conference on Financial Cryptography and Data Security. pp. 106–125. Springer (2016)
9. Decker, C., Russell, R., Osuntokun, O.: eltoo: A simple layer2 protocol for bitcoin (2018)

10. Decker, C., Wattenhofer, R.: A fast and scalable payment network with bitcoin duplex micropayment channels. In: Pelc, A., Schwarzmann, A.A. (eds.) Stabilization, Safety, and Security of Distributed Systems. pp. 3–18. Springer International Publishing, Cham (2015)
11. Fabrikant, A., Luthra, A., Maneva, E., Papadimitriou, C.H., Shenker, S.: On a network creation game. In: Proceedings of the twenty-second annual symposium on Principles of distributed computing. pp. 347–351. ACM (2003)
12. Moreno-Sanchez, P., Kate, A., Maffei, M.: Silentwhispers: Enforcing security and privacy in decentralized credit networks (2017)
13. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)
14. Poon, J., Dryja, T.: The bitcoin lightning network: Scalable off-chain instant payments (2015)
15. Prihodko, P., Zhigulin, S., Sahno, M., Ostrovskiy, A., Osuntokun, O.: Flare : An approach to routing in lightning network white paper (2016)
16. Roos, S., Moreno-Sanchez, P., Kate, A., Goldberg, I.: Settling payments fast and private: Efficient decentralized routing for path-based transactions. arXiv preprint arXiv:1709.05748 (2017)
17. Spilman, J.: Anti dos for tx replacement. https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2013-April/002433.html, accessed: 2019-04-17
18. Wood, G., et al.: Ethereum: A secure decentralised generalised transaction ledger (2014)