Brief Announcement: Musketeer – Incentive-Compatible Rebalancing for Payment Channel Networks

Zeta Avarikioti
TU Vienna
Austria

Stefan Schmid
TU Berlin & Weizenbaum Institute
Germany

Samarth Tiwari
CWI
Netherlands

ABSTRACT

We revisit the severely limited throughput problem of cryptocurrencies and propose a novel rebalancing approach for Payment Channel Networks (PCNs). PCNs are a popular solution for increasing the blockchain throughput, however, their benefit depends on the overall users' liquidity. Rebalancing mechanisms are the state-of-the-art approach to maintaining high liquidity PCNs. However, existing opt-in rebalancing mechanisms exclude users that may assist in rebalancing for small service fees, leading to suboptimal solutions and under-utilization of the PCNs' bounded liquidity.

We introduce the first rebalancing approach for PCNs that includes *all users*, following a *"all for one and one for all"* design philosophy that yields optimal throughput. The proposed approach introduces a double-auction rebalancing problem, which we term Musketeer, where users can participate as buyers (paying fees to rebalance) or sellers (charging fees to route transactions). The desired properties are tailored to the unique characteristics of PCNs, including the novel game-theoretic property of *cyclic budget balance* that is a stronger variation of strong budget balance.

Basic results derived from auction theory, including an impossibility and multiple mechanisms that either achieve all desiderata under a relaxed model or sacrifice one of the properties, are presented. We also propose a novel mechanism that leverages time delays as an additional cost to users. This mechanism is provably truthful, cyclic budget balanced, individually rational and economic efficient but only with respect to liquidity.

CCS CONCEPTS

• **Theory of computation → Algorithmic game theory and mechanism design**; • **Security and privacy → Human and societal aspects of security and privacy**; • **Computer systems organization → Distributed architectures**.

KEYWORDS

Blockchains, Payment Channels, Rebalancing, Game Theory

ACM Reference Format:
Zeta Avarikioti, Stefan Schmid, and Samarth Tiwari. 2024. Brief Announcement: Musketeer – Incentive-Compatible Rebalancing for Payment Channel Networks. In *ACM Symposium on Principles of Distributed Computing (PODC '24), June 17–21, 2024, Nantes, France.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3662158.3662809

PODC '24, June 17–21, 2024, Nantes, France

ACM ISBN 979-8-4007-0668-4/24/06
https://doi.org/10.1145/3662158.3662809

1 INTRODUCTION AND CONTRIBUTION

Bitcoin and other cryptocurrencies are significantly transforming the financial landscape. However, a well-known issue of the celebrated Nakamoto consensus introduced with Bitcoin, is that it inherently prohibits high transaction throughput which in turn hinders the widespread adoption of blockchain technologies [6]. Furthermore, blockchains are evidently environments for-profit, therefore user-incentive design is critical. Although several works have studied blockchain-related topics under the lens of game theory, e.g., [3–5, 7, 10], there is still much to be explored, particularly concerning scaling protocols. *In this work, we model and investigate incentive-compatible mechanisms that can enhance the limited transaction throughput of blockchains like Bitcoin.*

Specifically, we focus on one of the most prominent and well-studied scalability solutions for blockchains, called *payment channels* [12]. With payment channels, users can transact off-chain at far lower costs and faster speeds. The core idea is that any two users can lock their coins in a "joint account" on-chain, namely the payment channel. Thereby, the channel parties may perform arbitrarily many off-chain transactions with each other by signing messages with the new distribution of coins in their joint account.

Multiple payment channels operating on the same underlying blockchain, comprise a *payment channel network (PCN)*. PCNs allow users who have at least one channel open to route transactions through the network to other users with whom they do not share a direct payment channel. To successfully route a transaction, a path of channels with sufficient liquidity for all senders must exist. For example, if Alice wants to send 3 coins to Carol through Bob, Alice must have 3 coins available in her channel with Bob, and Bob must have 3 coins available in his channel with Carol. The intermediaries (e.g., Bob) that offer to use their channel liquidity to route another user's transaction typically ask for a routing service fee. If a channel in the selected path is depleted (i.e., has low liquidity) in the desired direction, all the transfers in the path will be reverted and the transaction will fail. *The liquidity of individual payment channels is, therefore, a crucial factor in the effectiveness of PCNs as a scaling solution.* It determines the ability to route transactions and impacts the overall efficacy of PCNs in enhancing the transaction throughput.

Rebalancing mechanisms are an attractive solution to improve liquidity within PCNs [1, 2, 9]. These mechanisms aim to identify cycles of depleted edges (channels) and route transactions across them in a way that ensures each node in the network has an equal amount of coins at the end of the process. By leveraging cycles within the PCN, parties with depleted channels can rebalance their channels by utilizing two of their channels – one as a source to send coins and another as a destination to receive coins.

However, the deployed local rebalancing algorithms [1] may be practically insufficient for two main reasons. Firstly, they only involve parties interested in rebalancing, thereby excluding channels that may route transactions for low or no routing fees; after all, intermediaries are indifferent to whether the routed payment concerns a payment (path) or rebalancing (cycle). Secondly, local searching algorithms may miss optimization opportunities leading to poor outcomes.

To address the latter limitation, Revive [9] proposed globally coordinated channel rebalancing, thus, achieving optimal outcomes. Hide & Seek [2] recently improved on Revive by enabling global rebalancing in a decentralized and privacy-preserving manner. However, in both algorithms, the rebalancing subgraph only includes the parties that wish to rebalance while the vast majority of channels of the PCN that may route transactions for low or no fees are neglected. *Thus, even with globally coordinated rebalancing, the limited rebalancing subgraph still impacts the optimality of the overall solution, and subsequently the PCN's scaling capability, i.e., how many transactions can succeed off-chain given a bounded overall liquidity.*

Our Contribution

We propose a novel approach to rebalancing that *involves all PCN users* in order to maximize the liquidity utilization and subsequently the transaction throughput. Our approach allows all users to submit their liquidity and bid for every one of their channels. The liquidity in this setting captures the number of coins they are willing to use for routing/rebalancing while the bid encapsulates how much they are willing to pay per coin for rebalancing the specific channel. So positive bids express the desire of buyers to rebalance, whereas negative (and zero) bids the desire of sellers to sell their routing service. Now, modeling this problem reveals a major challenge: *how can we design an incentive-compatible rebalancing mechanism for both buyers and sellers?*

We examine, for the first time, user incentives in the context of rebalancing mechanisms for PCNs. Our goal is twofold: First, to formally model the problem, capturing the unique characteristics present in PCNs; second, to discover satisfactory solutions, exploring different trade-offs. To achieve our objectives, we extend Hide & Seek [2] to accommodate both buyers and sellers of rebalancing liquidity. This approach leads to a double-auction problem with several challenges stemming either from traditional auction theory or from the individual needs of PCNs. In modeling our problem, we pinpoint *channel depletion* as a distinct feature, setting it apart from other network mechanism designs like routing games [8]. Channel depletion signifies that transactions can *permanently* lower an edge's capacity (here, liquidity) until counteracted by an opposite flow. Unlike railway networks where trains need tracks only temporarily, flows in our model can *compensate* for each other. Thus, existing results do not directly apply.

To determine the desiderata of our mechanism, we revisit conventional requirements from auction theory: (1) *economic efficiency*, i.e., maximizing the social welfare which captures that channels are prioritized for rebalancing based on their bids, (2) *truthfulness*, meaning users submit their true value, and (3) *individual rationality*, i.e., non-negative utility for rebalancing participants. However, our problem encounters an idiosyncrasy rooted in the payment channel primitive itself, affecting the budget-balanceness of the mechanism, i.e., the mechanism does not incur a deficit (nor a surplus). Specifically, coins cannot be burned in a payment channel because intuitively channel updates must always benefit one party; if there exists a coin distribution where both parties in the channel can benefit from changing, then there is no way to enforce it. For instance, we cannot enforce a distribution of 3 coins to Alice and Bob each and 2 coins burned, because the parties will cooperatively update their channel to hold 4 coins each. This implies that the mechanism cannot have either a surplus or a deficit, rendering (weakly) budget-balanced mechanisms infeasible. What's more, rebalancing itself occurs via individual cycles in the PCN. As a result, our setting demands a stronger notion of budget balance, which we term (4) *cyclic budget balance*, i.e., each cycle must be strongly budget balanced independently.

Unfortunately, the above four desired properties cannot be simultaneously achieved by any mechanism. We prove this by applying the classic Myerson-Satterthwaite impossibility result for double auctions [11]. We further emphasize the significance of the cyclic budget balance property in shaping potential solutions: The output of a rebalancing mechanism consists of a set of rebalancing circulations, which are global solutions where user preferences in one segment of the graph can impact the rebalancing cycles in distant segments of the graph. While in VCG-type mechanisms users are compensated for the global effects of their channels, the constraint of cyclic budget balance prevents this approach.

To provide satisfactory solutions, we apply standard techniques such as the renowned VCG mechanism and first-price auctions to the problem at hand. In particular, we showcase a mechanism that satisfies all the desired properties but is only applicable when all users are aware of the potential maximum and minimum fees they might pay or earn for their participation. Subsequently, we present a VCG-type mechanism that also satisfies all the desiderata exclusively for buyers, under the assumption that sellers are not treated as strategic agents. We then provide a mechanism that also considers sellers but, similarly to first-price auctions, sacrifices truthfulness. Finally, we propose a novel mechanism that introduces *time delays* as a natural characteristic of this problem, with the aim of incentivizing users to actively and truthfully participate in the rebalancing process while optimizing the outcome. The inclusion of time delays allows us to navigate around the impossibility and maintain our objective of maximizing rebalanced liquidity, in exchange for losing economic efficiency in terms of time delays and liquidity combined.

2 OVERVIEW OF MUSKETEER

In Musketeer, each PCN channel may participate in the rebalancing process either as a depleted or as an indifferent edge. Depleted edges are channels owned by players that wish to rebalance their channels (i.e., act as *buyers*), while indifferent edges are owned by players that sell their routing services (i.e., act as *sellers*). We model this problem as a double auction: each player submits their (non-negative or non-positive) bid for each channel they are part of, which indicates the maximum or minimum amount they are willing to pay or receive per unit coin for rebalancing or routing through that channel, respectively.

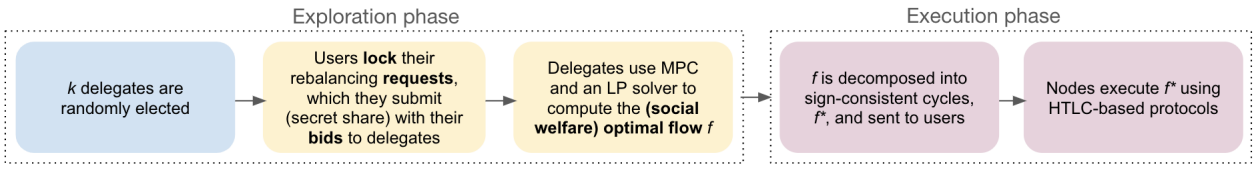

Figure 1: The backbone of Musketeer.

Additionally, for each channel, the users submit their liquidity, i.e., the number of coins available to the rebalancing mechanism. These coins may be available because buyers want to rebalance their channels or because sellers may want to earn fees for their service. With this knowledge, we extract the rebalancing subgraph: a directed graph with capacities capturing each channel's liquidity.

The resulting combinatorial problem can be modeled as a max-flow problem, aiming to maximize the total number of coins (flow) weighted by the buyer's bids. In other words, we calculate the flow that maximizes social welfare, respecting the channel capacities. We then decompose the flow in simple independent cycles that may be executed atomically [2]. Our main problem is pricing each cycle separately, awarding fees to sellers paid by the buyers.

Musketeer's participants are required to pre-lock the coins intended for rebalancing prior to the mechanism revealing the individual cycles. This design decision is primarily to prevent buyers from choosing whether to proceed with rebalancing after the output of the mechanism is known, as this could potentially incentivize dishonest strategies. From a different perspective, if buyers have the option to abort the mechanism in hindsight, the effectiveness of the mechanism may be severely hindered as a cycle can only be executed only if all players choose to participate and lock their coins. Figure 1 illustrates Musketeer's protocol flow.

3 TOWARDS TRUTHFUL REBALANCING

In this section, we explore how to provide incentive-compatible rebalancing in various settings using auction theory, yielding a flurry of results. We first prove that *satisfying all the desired properties of the Musketeer is impossible* by applying the classic Myerson-Satterthwaite impossibility result for double auctions.

Theorem 3.1. *No mechanism can simultaneously satisfy all the desired properties of Musketeer, namely economic efficiency, individual rationality, truthfulness, and cyclic budget balance.*

To circumvent the impossibility, we present a variety of mechanisms, all of which relax the notion of economic efficiency by restricting the set of possible bids we consider when maximizing social welfare. In particular, we first consider the limited setting where buyers and sellers choose to participate in the mechanism *knowing upfront the maximum and minimum fees* they would potentially pay or gain, respectively. The presented algorithm is fairly simple but restricts the choices for participants.

Theorem 3.2. *Athos satisfies economic efficiency, individual rationality, and cyclic budget balance. It also provides sellers with a fee of $\hat{q}$ per unit flow along their edges.*

To expand our results to the broader context where players are allowed to submit bids, we relax our model to a *single auction, solely considering the buyer's incentives*. Specifically, we assume players are willing to forward flow through their indifferent edges hoping to earn some fees in the process, but without a guarantee on the fees. Under this assumption, we present a *VCG-type mechanism*, satisfying incentive compatibility for buyers.

Theorem 3.3. *Porthos assuming $\mathbf{b} \geq 0$, satisfies economic efficiency, individual rationality, and cyclic budget balance. Users' bids for depleted edges are truthful.*

Next, we present a double-auction mechanism that takes into account the bids of both buyers and sellers, albeit sacrificing truthfulness, similarly to a *first price auction*.

Theorem 3.4. *Aramis satisfies economic efficiency, individual rationality, and cyclic budget balance, but not truthfulness.*

Finally, we leverage *time delays* to navigate around the impossibility result and design a novel double auction that satisfies all the desiderata in exchange for some costs that users incur in the form of time delays. The basic concept is that *cycles with lower social welfare will be released later in time*. Consequently, users who attempt to save on fees by underbidding will experience an undesirable delay in rebalancing. This concept is akin to that of opportunity cost, where users face potential losses from the inability to use their locked funds.

Theorem 3.5. *d'Artagnan (parameterized by delay d) satisfies economic efficiency, truthfulness, cyclic budget balance, and individual rationality.*

4 CONCLUSION

Our work demonstrates that the unique characteristics of PCNs, particularly the cyclic budget balance property, pose significant challenges in designing a mechanism that simultaneously satisfies all the desiderata. In particular, given our impossibility result, we developed a variety of mechanisms that balance the various desiderata. For more details on our results and proofs, we refer to our arXiv technical report (with the same title).

ACKNOWLEDGMENTS

We would like to express our gratitude to Constantinos Varsos and Makis Arsenis for providing their invaluable feedback and insights. The work was partially supported by ERC Starting Grant QIP–805241, the WWTF through the project 10.47379/ICT22045, and the Austrian Science Fund (FWF) through the SFB SpyCode project F8512-N, the project CoRaF (grant agreement ESP 68-N) and ADVISE (grant agreement I 4800-N).

REFERENCES

[1] [n. d.]. Rebalance Plugin. https://github.com/lightningd/plugins/tree/master/rebalance.

[2] Zeta Avarikioti, Krzysztof Pietrzak, Iosif Salem, Stefan Schmid, Samarth Tiwari, and Michelle Yeo. 2022. Hide and Seek: Privacy-Preserving Rebalancing on Payment Channel Networks. In *Proc. Financial Cryptography and Data Security (FC)*.

[3] Christian Badertscher, Juan Garay, Ueli Maurer, Daniel Tschudi, and Vassilis Zikas. 2018. But why does it work? A rational protocol design treatment of bitcoin. In *Eurocrypt*. https://doi.org/10.1007/978-3-319-78375-8_2

[4] Burak Can, Jens Leth Hougaard, and Mohsen Pourpouneh. 2022. On reward sharing in blockchain mining pools. *Games and Economic Behavior* 136 (2022), 274–298. https://doi.org/10.1016/j.geb.2022.10.002

[5] Xi Chen, Christos Papadimitriou, and Tim Roughgarden. 2019. An axiomatic approach to block rewards. In *AFT*. https://doi.org/10.1145/3318041.3355470

[6] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, Dawn Song, and Roger Wattenhofer. 2016. On scaling decentralized blockchains. In *International Conference on Financial Cryptography and Data Security*. Springer, 106–125.

[7] Ittay Eyal and Emin Gün Sirer. 2014. Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security*. Springer, 436–454.

[8] Joan Feigenbaum, Christos H Papadimitriou, Rahul Sami, and Scott Shenker. 2005. A BGP-based mechanism for lowest-cost routing. *Distributed Computing* 18, 1 (2005), 61–72.

[9] Rami Khalil and Arthur Gervais. 2017. Revive: Rebalancing off-blockchain payment networks. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 439–453.

[10] Aggelos Kiayias, Elias Koutsoupias, Maria Kyropoulou, and Yiannis Tselekounis. 2016. Blockchain mining games. In *EC*. https://doi.org/10.1145/2940716.2940773

[11] Roger B Myerson and Mark A Satterthwaite. 1983. Efficient mechanisms for bilateral trading. *Journal of Economic Theory* 29, 2 (1983), 265–281. https://doi.org/10.1016/0022-0531(83)90048-0

[12] Joseph Poon and Thaddeus Dryja. 2015. The Bitcoin lightning network: Scalable off-chain instant payments.