Payment Channel Networks with Resource-constrained Devices

Gabriel A. F. Rebello[1,2,3], Luís Henrique M. K. Costa[1] (advisor),
Maria Potop-Butucaru[2] (advisor), Marcelo Dias de Amorim[2] (advisor),
Otto Carlos M. B. Duarte[1] (advisor, *in memoriam*)

[1]Universidade Federal do Rio de Janeiro - GTA/COPPE/UFRJ

[2]Sorbonne Université, CNRS, LIP6, F-75005 Paris, France

[3]Instituto de Pesquisas Eldorado, Brazil

Abstract. *Payment-channel networks (PCN) represent the leading solution to scale blockchain-based payments to the performance levels of centralized payment systems. However, current PCNs require nodes to stay permanently online and have enough resources to execute payment security mechanisms. Such assumptions are difficult to guarantee in battery-powered devices with intermittent connectivity patterns, such as mobile phones, smart objects, and sensors. In this thesis, we address the case of PCNs with resource-constrained devices on several fronts. First, we formalize a hybrid PCN model that considers light nodes and propose a mechanism to protect payment channels with resource-constrained devices. Our experiments show that the proposed mechanism is efficient for devices with high and medium availability in mobile broadband connections. Next, we propose PCNsim, a simulator that replicates the main functionalities of a PCN in the OMNeT++ framework. PCNsim allows researchers to experiment with payments under custom networking conditions representing resource-constrained devices' connections. PCNsim's demonstrations show that it correctly reproduces the behavior of a PCN over unreliable communication channels. Finally, we address the problem of routing payments from resource-constrained devices. We present a payment scheme that anticipates payment confirmations for time-sensitive applications and two routing algorithms that route payments considering application-specific constraints. The results show that our routing algorithms are efficient both for single-path and multi-path payments and reach their top performance when the problem's constraints are tight.*

1. Introduction

Payment-channel networks (PCNs) represent the leading solution to solve the problem of low throughput and high confirmation delays in blockchains. In PCNs, two users wishing to transact continuously can transfer some of their coins to a joint address in the blockchain. This process creates a *payment channel* between them in which the locked coins can be transferred immediately. It suffices to reallocate the channel funds through off-chain private transactions. The collection of payment channels between users forms a peer-to-peer *payment channel network* in which payments can be routed like packets. Figure 1 depicts an example of a PCN. In the example, Alice has a payment channel of 12 coins with Bob, of which 10 are on her side. This means she can send up to 10 coins to

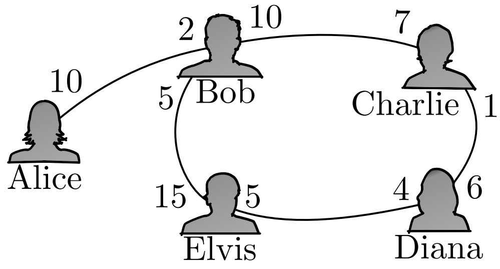

Figure 1. A payment-channel network (PCN) composed of bidirectional payment channels with limited capacity. Users can route payments through intermediaries to reach their destinations.

Bob in one or more transactions without validating the transactions in the blockchain. She can also send coins to Charlie through a multi-hop payment. In this case, she sends the coins in her channel with Bob, and Bob relays them to Charlie. The routing process happens in a few seconds, even if Alice and Charlie do not share a direct payment channel. To ensure Bob cannot steal Alice's coins while forwarding them, a hash-based fund-locking mechanism puts Bob's coins in custody until he proves he forwarded the payment.

PCNs reduce transaction latency from minutes to, at most, a few seconds and yield near-zero transaction costs, which significantly improves the efficiency of blockchains [Hafid et al. 2020, Sguanci et al. 2021, Gangwal et al. 2022, Yang et al. 2020, Zhou et al. 2020, Sanka and Cheung 2021]. The ability to execute fast and secure payments without consensus validation narrows the gap between cryptocurrencies and real-life payments, enhancing the use of blockchain systems. For instance, PCNs have played a crucial role in the recent adoption of Bitcoin as an official currency in El Salvador [CloudTweaks 2021].

2. Problem Statement and Objectives

Despite efficiently scaling blockchains, current PCN implementations present a significant limitation: they rely on powerful nodes to work. Specifically, they require that nodes stay online at all times and have enough resources to execute the security mechanisms involved in a payment. For example, Bitcoin's Lightning Network and Ethereum's Raiden Network assume that nodes maintain an updated view of the network topology, that they can verify channels in the blockchain whenever needed and that all nodes adopt onion routing as the only payment forwarding mechanism to guarantee privacy [Erdin et al. 2021]. This implies that nodes must have high availability to keep the topology up-to-date, enough bandwidth and storage capacity to download and maintain blocks, and strong computational power to encrypt onion packets. Furthermore, PCNs often assume connections between nodes are reliable so that payments are never dropped.

Such assumptions may be reasonable for servers but are difficult to guarantee in battery-powered devices with intermittent connectivity patterns, such as mobile phones, smart objects, and IoT sensors. These devices typically have limited resources and communicate through lossy wireless connections that do not provide the required reliability to send payments. Furthermore, it is unrealistic to assume light nodes[1] will maintain updated topologies or execute security mechanisms that spend most of their energy reserve.

[1] This thesis considers the terms "resource-constrained devices" and "light nodes" as synonyms.

Surprisingly, very few works consider PCNs in which users send or route payments from light nodes through wireless connections [Kurt et al. 2022, Mercan et al. 2020, Hannon and Jin 2019, Robert et al. 2020]. *This thesis aims to fill this gap in the literature by analyzing what challenges arise when we include resource-constrained devices into a PCN.* Specifically, we identify four main challenges to overcome:

- **Challenge #1 (Architecture):** There is no reference network model that considers the limitations of light nodes. Apart from payment channels, this model should consider direct communication between nodes used to request blocks or efficiently update the network graph on demand.
- **Challenge #2 (Channel Security):** Attack prevention through constant blockchain monitoring is infeasible for resource-constrained devices that disconnect frequently. There is no efficient way to secure payments from such devices while they are offline.
- **Challenge #3 (Simulation):** Resource-constrained devices often operate under unreliable networking conditions that can lead to interruptions or delays in the payment process. No open-source simulator can replicate simulate such conditions to understand how unfavorable scenarios affect payments.
- **Challenge #4 (Payment Routing):** Resource-constrained devices cannot be assumed to have the same computing power as common nodes. Therefore, finding paths and finalizing payments in these nodes can be too slow for some applications. We need a payment scheme that considers such limitations and speeds up payments from light nodes.

3. Contributions and Results

Our work started with the goal of analyzing the problem of blockchain scalability. We compared several state-of-the-art consensus protocols to understand their main advantages and drawbacks, providing a direction on which protocol we should adopt for each use case. This initial work yielded four publications, listed as 1 through 4 in Section 4. The discoveries from this analysis concluded that consensus, regardless of type, is the main bottleneck for transaction processing in blockchains. Hence, we moved to consensus-free approaches such as payment channel networks. The first contribution of this thesis is a survey about such approaches, which are formally called *off-chain* or *layer-two* protocols:

Contribution 1: A survey on blockchain scalability. We provide a survey on the recent efforts to improve the scalability of blockchains, focusing on layer-two protocols such as payment channel networks and rollups. These technologies process computations off-chain and only leverage consensus when needed. A large portion of the work addresses the open challenges of payment channel networks, such as payment routing, channel rebalancing, network design strategies, security and privacy, payment scheduling, congestion control, simulators, and support for light nodes.

The survey has been published at IEEE Communication Surveys and Tutorials, a top-tier journal with current impact factor of 34.4 (publication 5). As we prepared the survey, we noticed that PCNs have major challenges regarding the security of resource-constrained devices. The main problem is that the security of channel funds is only guaranteed if both channel parties are online, which cannot be assumed for light nodes. Thus, we proposed the following contribution that aims to solve Challenges #1 and #2:

Contribution 2: A mechanism to secure channels with light nodes. We formalize the model of hybrid PCNs, i.e., PCNs with capable nodes and wireless resource-constrained devices, and address the coin theft problem, a vulnerability that affects nodes with intermittent connectivity. We propose a countermeasure based on minimum time windows that lock funds whenever a user disconnects. The duration of the window is proportional to the mean time to recovery (MTTR) of devices, which gives them enough time to reconnect and contest attacks.

Using a proposed network model as reference, this work adapted the default dispute periods of existing PCNs to accommodate light devices. We evaluated our proposal with real channels from Bitcoin's Lightning Network [Poon and Dryja 2016] and estimated the MTTR of devices using data from 3G/4G mobile broadband connections [Baltrunas et al. 2014, Elmokashfi et al. 2017]. Our results showed that increasing the dispute period is an efficient security measure for devices with downtimes of a few hours to a day. However, for devices that disconnect for long periods, the simplest solution is to fall back to blockchain transactions, otherwise the money can be stuck in the channel for as long as the device is offline. The work resulted in three publications, listed as 6, 7, and 8.

Experimenting with mobile connections showed that its often difficult to predict the behavior of payment channels when they operate under unstable networking conditions. Besides, we missed an automated tool that would accurately simulate payment channel networks with several network topologies and communication protocols. This need generated our third contribution, which aims to solve Challenge #3:

Contribution 3: PCNsim. PCNsim is an open-source payment channel network simulator that reproduces the state machine of the Lightning Network on top of the OMNeT++ framework. The simulator allows users to model channel parameters such as channel capacity and routing fees and to test routing protocols on real data obtained from payment datasets. Because OMNeT++ offers a wide range of communication protocols through the INET library, PCNSim also supports testing PCNs with different networking protocols in lower layers. PCNsim is available to the scientific community at *https://github.com/gfrebello/pcnsim.*

We published the details of PCNsim and some simulations of payment routing protocols in IEEE INFOCOM 2022 (publication 9). Our results showed that PCNSim can accurately simulate the behavior of payment channels under lossy connections and unreliable transport protocols.

Finally, our simulations with PCNsim helped us realize that routing payments efficiently is a major challenge of dealing with resource-constrained devices in PCNs.

Particularly, routing payments from light nodes can be too slow for applications requiring minimum payment latency to work, such as stock markets, cross-chain trades, and electronic toll collection. We contribute to Challenge #4 with:

Contribution 4: A payment scheme for payments from light nodes. We propose a special payment scheme that reduces confirmation latency when issuing payments from resource-constrained devices. The payment scheme securely offloads payments to gateway nodes which compute routes and forward payments as a service. This saves energy, speeds up payments, and allows light nodes to remain offline most of the time at the expense of a small service fee.

Contribution 5: GenPulse and MultiPulse. We develop two optimal payment routing algorithms that consider application-specific needs when computing paths. The Generalized Pulse (GenPulse) algorithm finds a constrained shortest path in the graph, i.e., a path that minimizes a routing metric while respecting side constraints. Multipath Pulse (MultiPulse) extends GenPulse to issue optimal multipath payments via successive flow allocation. GenPulse and MultiPulse can be used in PCNs, for instance, to minimize the routing costs of a payment that is subject to a maximum payment latency or network resource consumption.

The above contributions provide an efficient scheme for light nodes to issue payments in PCNs. Our results showed that GenPulse and MultiPulse outperform several state-of-the-art payment routing algorithms in restricted applications. We are currently writing a paper that includes these final contributions.

The results of all contributions can be found in the thesis: `https://www.gta.ufrj.br/ftp/gta/TechReports/Rebello23.pdf`. Several other works that were done in collaboration with colleagues are omitted due to space restrictions. For a full list of products of this thesis, please refer to Section 4.

4. List of Products

4.1. Open-source Software

- ”PCNSim, an open-source PCN simulator on top of OMNeT++”. Available at: *https://github.com/gfrebello/pcnsim*
- ”A framework for estimating secure lock time windows for payment channels”. Available at: *https://github.com/gfrebello/pcn-time-window*

4.2. Publications

1. **Rebello, G. A. F.**, Camilo, G. F., Guimarães, L. C. B., Souza, L. A. C., Duarte, O. C. M. B., “On the Security and Performance of Proof-based Consensus Protocols”, in 4th Conference on Cloud and Internet of Things (CIoT 2020), Niterói, Brazil, October 2020.
2. **Rebello, G. A. F.**, Camilo, G. F., Guimarães, L. C. B., Souza, L. A. C., Duarte, O. C. M. B., “Segurança e Desempenho de Protocolos de Consenso Baseados em Prova para Corrente de Blocos”, in XX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2020), Petrópolis, Brazil, October 2020.

3. **Rebello, G. A. F.**, Camilo, G. F., Guimarães, L. C. B., de Souza, L. A. C., Thomaz, G. A., Duarte, O. C. M. B. – "A Security and Performance Analysis of Proof-based Consensus Protocols", in Annals of Telecommunications, no. 7, pp. 517-537, 2021.
4. **Rebello, G. A. F.**, Camilo, G. F., Guimarães, L. C. B., Souza, L. A. C., Duarte, O. C. M. B. - "Security and Performance Analysis of Quorum-based Blockchain Consensus Protocols", in 6th Cyber Security in Networking Conference (CSNet'22) - Rio de Janeiro, Brazil, October 2022.
5. **Rebello, G. A. F.**, Camilo, G. F., Souza, L. A. C., Potop-Butucaru, M., Amorim, M. D., Campista, M. E. M., Costa, L. H. M. K. - "A Survey on Blockchain Scalability: From Hardware to Layer-two Protocols", IEEE Communications Surveys and Tutorials, ISSN: 1553-877X, DOI: 10.1109/COMST.2024.3376252, March 2024.
6. **Rebello, G. A. F.**, Potop-Butucaru, M., Amorim, M. D., Duarte, O. C. M. B. – "Protegendo Redes de Canais de Pagamento Sem Fio com Janelas de Tempo de Bloqueio Mínimas", XXI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2021), Belém, Brazil, October 2021. *Honorable mention.*
7. **Rebello, G. A. F.**, Potop-Butucaru, M., Amorim, M. D., Duarte, O. C. M. B. - "Securing Wireless Payment-Channel Networks With Minimum Lock Time Windows", IEEE International Conference on Communications (ICC 2022), Seoul, South Korea, May 2022.
8. **Rebello, G. A. F.**, Potop-Butucaru, M., de Amorim, M. D., Duarte, O. C. M. B. "Sécurisation des réseaux de canaux de paiement sans fil avec des fenêtres de temps de verrouillage réduites". In CORES 2022–7ème Rencontres Francophones sur la Conception de Protocoles, l'Évaluation de Performance et l'Expérimentation des Réseaux de Communication.
9. **Rebello, G. A. F.**, Camilo, G. F., Potop-Butucaru, M., Campista, M. E. M., Amorim, M. D., Costa, L. H. M. K. - "PCNsim: A Flexible and Modular Simulator for Payment Channel Networks", IEEE International Conference on Computer Communications Workshops (INFOCOM WKSHPS), Virtual Conference, May 2022.
10. Camilo, G. F., **Rebello, G. A. F.**, de Souza, L. A. C., Campista, M. E. M., and Costa, L. H. M. K. - "ProfitPilot: Enabling Rebalancing in Payment Channel Networks through Profitable Cycle Creation", in IEEE Transactions on Network and Service Management, ISSN: 1932-4537, DOI: https://doi.org/10.1109/TNSM.2024.3361250, January 2024.
11. Camilo, G. F., **Rebello, G. A. F.**, de Souza, L. A. C., Campista, M. E. M., Costa, L. H. M. K. – "Posicionamento Lucrativo de Nós e Criação de Rotas de Baixo Custo na Rede Relâmpago", in XLI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2023), Brasília, DF, Brazil, May 2023. *Honorable mention.*
12. de Souza, L. A. C., **Rebello, G. A. F.**, Camilo, G. F., Campista, M. E. M., Costa, L. H. M. K. – "GITI-CB: Gestão de Identidade com Troca de Informações entre Correntes de Blocos", in VI Workshop Blockchain: Teoria, Tecnologia e Aplicações (Wblockchain 2023), Brasília, DF, Brazil, May 2023.
13. Camilo, G. F., **Rebello, G. A. F.**, de Souza, L. A. C., Thomaz, G. A., Potop-

Butucaru, M., Amorim, M. D., Campista, M. E. M., Costa, L. M. K. – "Redes de Canais de Pagamento: Provendo Escalabilidade para Pagamentos em Criptomoedas", in Minicursos do XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2022), Fortaleza, Brazil, May 2022.

14. Camilo, G. F., **Rebello, G. A. F.**, de Souza, L. A. C., Potop-Butucaru, M., Amorim, M. D., Campista, M. E. M., Costa, L. H. M. K. – "Análise da Evolução Topológica da Rede Lightning de Canais de Pagamento", in XXII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2022), Santa Maria, Brazil, September 2022.
15. Camilo, G. F., **Rebello, G. A. F.**, de Souza, L. A. C., Campista, M. E. M., Costa, L. H. M. K. – "Posicionamento Lucrativo de Nós e Criação de Rotas de Baixo Custo na Rede Relâmpago", in XLI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2023), Brasília, DF, Brazil, May 2023. *Honorable mention.*
16. de Souza, L. A. C., **Rebello, G. A. F.**, Camilo, G. F., Campista, M. E. M., Costa, L. H. M. K. – "GITI-CB: Gestão de Identidade com Troca de Informações entre Correntes de Blocos", in VI Workshop Blockchain: Teoria, Tecnologia e Aplicações (Wblockchain 2023), Brasília, DF, Brazil, May 2023.
17. Camilo, G. F., **Rebello, G. A. F.**, de Souza, L. A. C., Thomaz, G. A., Potop-Butucaru, M., Amorim, M. D., Campista, M. E. M., Costa, L. M. K. – "Redes de Canais de Pagamento: Provendo Escalabilidade para Pagamentos em Criptomoedas", in Minicursos do XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2022), Fortaleza, Brazil, May 2022.
18. Camilo, G. F., **Rebello, G. A. F.**, de Souza, L. A. C., Potop-Butucaru, M., Amorim, M. D., Campista, M. E. M., Costa, L. H. M. K. – "Análise da Evolução Topológica da Rede Lightning de Canais de Pagamento", in XXII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2022), Santa Maria, Brazil, September 2022.
19. Camilo, G. F., **Rebello, G. A. F.**, Souza, L. A. C., Duarte, O. C. M. B., "A Secure Personal-Data Trading System Based on Blockchain, Trust, and Reputation", in 3rd IEEE International Conference on Blockchain (Blockchain-2020), Rhodes Island, Greece, November 2020.
20. Camilo, G. F., **Rebello, G. A. F.**, Souza, L. A. C., Duarte, O. C. M. B. – "AutAvailChain: Disponibilização Segura, Controlada e Automática de Dados IoT usando Corrente de Blocos", in III Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain SBRC 2020), Rio de Janeiro, Brazil, December 2020. *Honorable mention.*
21. Souza, L. A. C., **Rebello, G. A. F.**, Camilo, G. F., Guimarães, L. C. B., Duarte, O. C. M. B., "DFedForest: Decentralized Federated Forest", in 3rd IEEE International Conference on Blockchain (Blockchain-2020), Rhodes Island, Greece, November 2020.
22. Camilo, G. F., **Rebello, G. A. F.**, Souza, L. A. C., Duarte, O. C. M. B., "Um Sistema Seguro de Comercialização de Dados Pessoais Sensíveis baseado em Reputação, Confiança e Corrente de Blocos", in XX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2020), Petrópolis, Brazil, October 2020.

References

Baltrunas, D., Elmokashfi, A., and Kvalbein, A. (2014). Measuring the reliability of mobile broadband networks. In *14th ACM IMC*, pages 45–58.

CloudTweaks (2021). How Bitcoin Brought The Lightning Network To El Salvador. `https://cloudtweaks.com/2021/07/how-bitcoin-brought-lightning-network-el-salvador/`. Last access: Mar. 6th 2023.

Elmokashfi, A., Zhou, D., and Baltrünas, D. (2017). Adding the next nine: An investigation of mobile broadband networks availability. In *23rd ACM MobiCom*, pages 88–100.

Erdin, E., Mercan, S., and Akkaya, K. (2021). An Evaluation of Cryptocurrency Payment Channel Networks and Their Privacy Implications. arXiv:2102.02659 [cs].

Gangwal, A., Gangavalli, H. R., and Thirupathi, A. (2022). A Survey of Layer-Two Blockchain Protocols. arXiv:2204.08032 [cs].

Hafid, A., Hafid, A. S., and Samih, M. (2020). Scaling Blockchains: A Comprehensive Survey. *IEEE Access*, 8:125244–125262. Conference Name: IEEE Access.

Hannon, C. and Jin, D. (2019). Bitcoin payment-channels for resource limited IoT devices. In *IEEE COINS*, pages 50–57.

Kurt, A., Akkaya, K., Yilmaz, S., Mercan, S., Shlomovits, O., and Erdin, E. (2022). LNGate^2: Secure Bidirectional IoT Micro-payments using Bitcoin's Lightning Network and Threshold Cryptography. arXiv:2206.02248 [cs].

Mercan, S., Erdin, E., and Akkaya, K. (2020). Improving Transaction Success Rate via Smart Gateway Selection in Cryptocurrency Payment Channel Networks. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–3.

Poon, J. and Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments.

Robert, J., Kubler, S., and Ghatpande, S. (2020). Enhanced lightning network (off-chain)-based micropayment in iot ecosystems. *Future Generation Computer Systems*, 112:283–296.

Sanka, A. I. and Cheung, R. C. C. (2021). A systematic review of blockchain scalability: Issues, solutions, analysis and future research. *Journal of Network and Computer Applications*, 195:103232.

Sguanci, C., Spatafora, R., and Vergani, A. M. (2021). Layer 2 Blockchain Scaling: a Survey. arXiv:2107.10881 [cs].

Yang, D., Long, C., Xu, H., and Peng, S. (2020). A Review on Scalability of Blockchain. In *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology*, pages 1–6.

Zhou, Q., Huang, H., Zheng, Z., and Bian, J. (2020). Solutions to Scalability of Blockchain: A Survey. *IEEE Access*, 8:16440–16455.