Poster: Sleepy Channels: Bi-directional Payment Channels without Watchtowers

Lukas Aumayr[§]
TU Wien
lukas.aumayr@tuwien.ac.at

Sri AravindaKrishnan Thyagarajan[§]
NTT Research
t.srikrishnan@gmail.com

Giulio Malavolta
Max Planck Institute for Security and Privacy
giulio.malavolta@hotmail.it

Pedro Moreno-Sanchez
IMDEA Software Institute
pedro.moreno@imdea.org

Matteo Maffei
Christian Doppler Laboratory Blockchain
Technologies for the Internet of Things, TU Wien
matteo.maffei@tuwien.ac.at

Abstract

Payment channels (PC) are a promising solution to the scalability issue of cryptocurrencies, allowing users to perform the bulk of the transactions off-chain without needing to post everything on the blockchain. Many PC proposals however, suffer from a severe limitation: Both parties need to constantly monitor the blockchain to ensure that the other party did not post an outdated transaction. If this event happens, the honest party needs to react promptly and engage in a punishment procedure. This means that prolonged absence periods (e.g., a power outage) may be exploited by malicious users. As a mitigation, the community has introduced watchtowers, a third-party monitoring the blockchain on behalf of off-line users. Unfortunately, watchtowers are either trusted, which is critical from a security perspective, or they have to lock a certain amount of coins, called collateral, for each monitored PC in order to be held accountable, which is financially infeasible for a large network.

We present Sleepy Channels, the first bi-directional PC protocol without watchtowers (or any other third party) that supports an unbounded number of payments and does not require parties to be persistently online. The key idea is to confine the period in which PC updates can be validated on-chain to a short, pre-determined time window, which is when the PC parties have to be online. This behavior is incentivized by letting the parties lock a collateral in the PC, which can be adjusted depending on their mutual trust and which they get back much sooner if they are online during this time window. Our protocol is compatible with any blockchain that is capable of verifying digital signatures (e.g., Bitcoin), as shown by our proof of concept. Moreover, our experimental results show that Sleepy Channels impose a communication and computation overhead similar to state-of-the-art PC protocols while removing watchtower's collateral and fees for the monitoring service.

Full reference: Lukas Aumayr, Sri AravindaKrishnan Thyagarajan, Giulio Malavolta, Pedro Moreno-Sanchez, and Matteo Maffei. 2022. Sleepy Channels: Bi-directional Payment Channels without Watchtowers. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS'22), November 7–11, 2022, Los Angeles, CA, USA*. ACM, New York, NY, USA, 14 pages. https://dl.acm.org/doi/10.1145/3548606.3559370

URL/DOI: https://dl.acm.org/doi/10.1145/3548606.3559370

Acknowledgment

This work has been partially supported by Madrid regional government as part of the program S2018/TCS-4339 (BLOQUES-CM) co-funded by EIE Funds of the European Union, by grant IJC2020-043391-I/MCIN/AEI/10.13039/501100011033 and European Union NextGenerationEU/PRTR, by SCUM Project (RTI2018-102043-B-I00) MCIN/AEI/10.13039/501100011033/ERDF A way of making Europe, and by the project HACRYPT. This work was also partially supported by the European Research Council (ERC) under the European Union's Horizon 2020 research (grant agreement 771527-BROWSEC), by the Austrian Science Fund (FWF) through the projects PROFET (grant agreement P31621) and the project Security and Privacy by Design for Smart Contracts (F 8510-N), by the Austrian Research Promotion Agency (FFG) through the COMET K1 SBA and COMET K1 ABC, by the Vienna Business Agency through the project Vienna Cybersecurity and Privacy Research Center (VISP), by the Austrian Federal Ministry for Digital and Economic Affairs, the National Foundation for Research, Technology and Development and the Christian Doppler Research Association through the Christian Doppler Laboratory Blockchain Technologies for the Internet of Things (CDL-BOT) and by CoBloX Labs. This work was further partially supported by the German Federal Ministry of Education and Research BMBF (grant 16K15K042, project 6GEM). The work was also funded through the support of THE DAVID AND LUCILLE PACKARD FOUNDATION - Award #202071730, SRI INTERNATIONAL - Award #53978 / Prime: DEFENSE ADVANCED RESEARCH PROJECTS AGENCY - Award #HR00110C0086, NATIONAL SCIENCE FOUNDATION - Award #2212746.

[§] These two authors contributed equally to the referenced work.

Sleepy Channels: Bitcoin-Compatible Bi-directional Payment Channels without Watchtowers

Accepted at ACM CCS '22

Lukas Aumayr*[1], Sri AravindaKrishnan Thyagarajan*[2], Giulio Malavolta[3], Pedro Moreno-Sanchez[4], Matteo Maffei[1]

[1]TU Wien, [2]Carnegie Mellon University, [3]Max Planck Institute for Security and Privacy, [4]IMDEA Software Institute

1. Scalability & Payment Channels

Scalability:

- Blockchain + global consensus: everyone records and checks every transaction

Problem: Permissionless blockchains have limited throughput

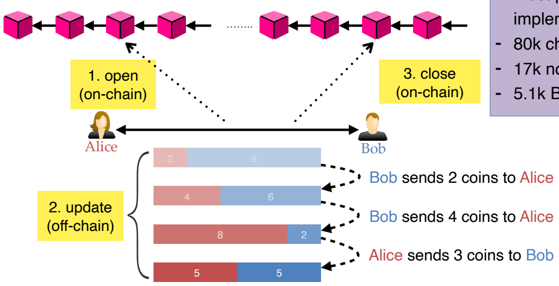
Transaction rates
Bitcoin: ~10 tx/sec
vs.
Visa: ~10K tx/sec

Payment Channels:

Exchange transactions off-chain, Blockchain for disputes.

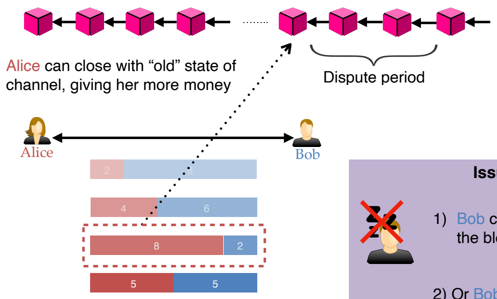
Lightning Network [1]

- most popular implementation
- 80k channels
- 17k nodes
- 5.1k BTC locked


1. open
(on-chain)
3. close
(on-chain)
Alice
Bob
2. update
(off-chain)
2
8
4
6
8
2
5
5
Bob sends 2 coins to Alice
Bob sends 4 coins to Alice
Alice sends 3 coins to Bob

2. How are disputes handled?

Problem: Need to prevent that old state is posted


Alice can close with "old" state of channel, giving her more money
Dispute period
Alice
Bob
2
4
6
8
2
5
5

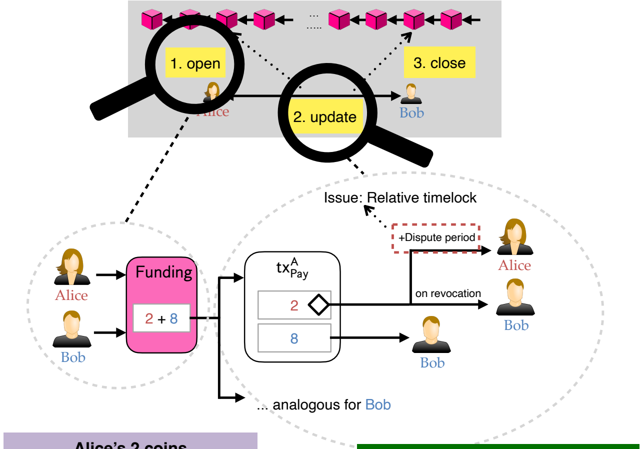
Problem comes from how channels work
See 3.

Issues

1) Bob constantly monitors the blockchain

2) Or Bob employs a watchtower (e.g., [2]), but:
   - Either he trusts the watchtower
   - Or the watchtower needs to provide collateral per channel

3. Lightning-style Channels



Alice's 2 coins

- If state old, Bob can get coins before dispute period ends (in practice: 1 day)
- Otherwise, Alice gets coins after dispute period

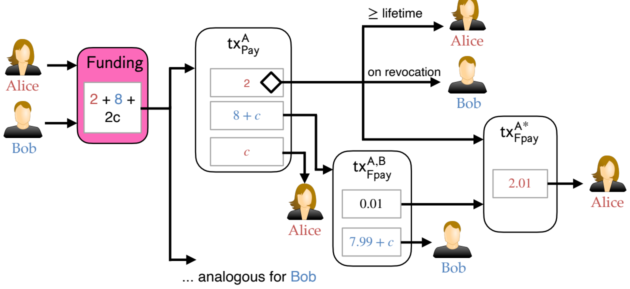
Bob's 8 coins

- Bob gets coins right away
- For tx^{B}_{Pay} this logic is reversed

Challenges:

1. Allow Bob to go offline without watchtower
2. Ensure balance (properly handle disputes)
3. Money doesn't stay locked for a long time

4. Sleepy Channels



Alice's 2 coins

- If state old, Bob can get coins after lifetime expires
- Otherwise Alice gets it after lifetime
- Or if Bob initiates fast unlock

Bob's 8 + c coins

- Bob's can get coins right away
- The 0.01 coins trigger fast unlock
- Collateral c incentivizes fast unlock

Alice's collateral c

- Alice's collateral is unlocked
- For tx^{B}_{Pay} this logic is reversed

Overcoming challenges:

1. "Dispute period" as long as channel lifetime
2. Dispute period as absolute timelock
3. Fast unlock mechanism, incentivized by collateral

✓ Now Bob can safely go offline!

5. Evaluation

Watchtower collateral:

- Untrusted watchtowers ⇒ collateral per channel
- Collateral increases linearly in number of channels
- **If 30% of channels used one watchtower provider, it would need almost 20% of all BTC currently in the Lightning Network**

Risk of going offline:

- In Lightning users need to check daily
- In Sleepy Channels, only once before lifetime expires
- **Over a 1 month period, Lightning users are ~30x more at risk of stolen funds**

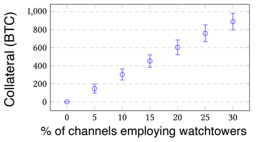


Fig. 1: Watchtower collateral by % usage of channels in current Lightning Network.

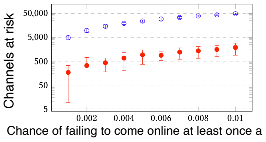


Fig. 2: Channels at risk of losing funds by chance of failing to go online daily, red for Sleepy Channels and blue for Lightning

6. Discussion

- **First bi-directional channel** construction without watchtowers & unbounded payments
- **Proof-Of-Concept implementation**: Compatible with Bitcoin
- Formally modelled and **proved in the UC framework**
- Replacing absolute timelocks with verifiable timed signatures [3] makes the construction **compatible with Monero**
- **Comparison** with other payment channel schemes
- **Other challenges** in Payment Channels:
  - Faster payments [4]
  - Channels for more than payments [5]
  - Virtual channels [6,7]
  - Multi-channel updates [8]

Scan me!

References:

[1] J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," *2016*
[2] A. Mirzaei, A. Sakzad, J. Yu and R. Steinfeld, "FPPW: A Fair and Privacy Preserving Watchtower For Bitcoin," in FC, *2021*.
[3] SAK. Thyagarajan, A. Bhat, G. Malavolta, N. Döttling, A. Kate and D. Schröder, "Verifiable Timed Signatures Made Practical," in ACM CCS, *2020*.
[4] L. Aumayr, P. Moreno-Sanchez, A. Kate and M. Maffei, "Blitz: Secure Multi-Hop Payments Without Two-Phase Commits," in USENIX Security, *2021*.
[5] L. Aumayr et al., "Generalized Channels from Limited Blockchain Scripts and Adaptor Signatures," in Asiacrypt, *2021*.
[6] L. Aumayr et al., "Bitcoin-Compatible Virtual Channels," in IEEE Security and Privacy, *2021*.
[7] L. Aumayr, P. Moreno-Sanchez, A. Kate and M. Maffei, "Donner: UTXO-Based Virtual Channels Across Multiple Hops," eprint.iacr.org/2021/855, *2021*.
[8] L. Aumayr, Kasra Abbaszadeh, and Matteo Maffei, "Thora: Atomic And Privacy-Preserving Multi-Channel Updates," in ACM CCS, *2022*.