Poster: Thora: Atomic and Privacy-Preserving Multi-Channel Updates

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

Kasra Abbaszadeh[§]
University of Maryland
kasraz@umd.edu

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

Abstract

Most blockchain-based cryptocurrencies suffer from a heavily limited transaction throughput, which is a barrier to their growing adoption. Payment channel networks (PCNs) are one of the promising solutions to this problem. PCNs reduce the on-chain load of transactions and increase the throughput by processing many payments off-chain. In fact, any two users connected via a path of payment channels (i.e., joint addresses between the two channel end-points) can perform payments, and the underlying blockchain is used only when there is a dispute between users. Unfortunately, payments in PCNs can only be conducted securely along a path, which prevents the design of many interesting applications. Moreover, the most widely used implementation, the Lightning Network in Bitcoin, suffers from a collateral lock time linear in the path length, it is affected by security issues, and it relies on specific scripting features called Hash Timelock Contracts that hinders the applicability of the underlying protocol in other blockchains.

In this work, we present Thora, the first Bitcoin-compatible off-chain protocol that enables the atomic update of arbitrary channels (i.e., not necessarily forming a path). This enables the design of a number of new off-chain applications, such as payments across different PCNs sharing the same blockchain, secure and trustless crowdfunding, and channel rebalancing. Our construction requires no specific scripting functionalities other than digital signatures and timelocks, thereby being applicable to a wider range of blockchains. We formally define security and privacy in the Universal Composability framework and show that our cryptographic protocol is a realization thereof. In our performance evaluation, we show that our construction requires only constant collateral, independently from the number of channels, and has only a moderate off-chain communication as well as computation overhead.

Full reference: Lukas Aumayr, Kasra Abbaszadeh, and Matteo Maffei. 2022. Thora: Atomic and Privacy-Preserving Multi-Channel Updates. 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/10.1145/3548606.3560556

URL/DOI: https://dl.acm.org/doi/10.1145/3548606.3560556

ACKNOWLEDGMENT

The work was partially supported by CoBloX Labs, 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 W1255-N23 and the project Security and Privacy by Design for Smart Contracts (F 8510-N), by the Austrian Research Promotion Agency (FFG) through the Bridge-1 project PR4DLT (grant agreement 13808694), 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).

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

Thora: Atomic And Privacy-Preserving Multi-Channel Updates

Accepted at ACM CCS '22

Lukas Aumayr*[1], Kasra Abbaszadeh*[2], Matteo Maffei[1]

[1]TU Wien, [2]University of Maryland

1. Scalability & Payment Channels

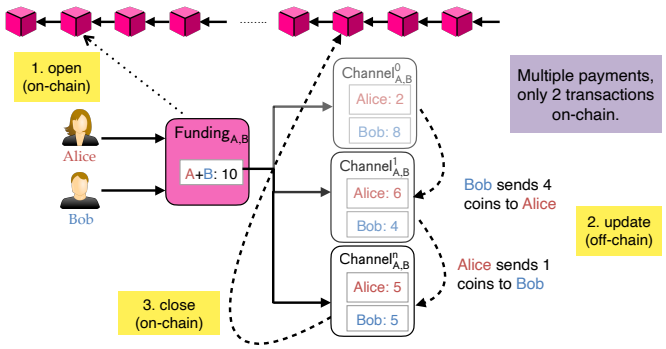
Scalability:

Problem: Permissionless blockchains have limited throughput

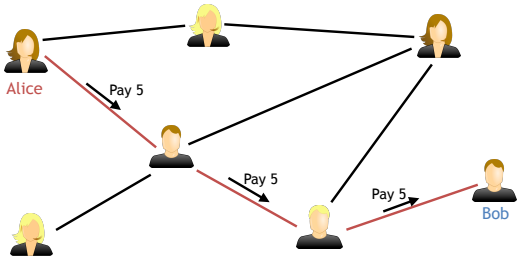
Transaction rates
Bitcoin: ~10 tx/sec
vs.
Visa: ~10K tx/sec

Payment Channels:

Exchange transactions off-chain, Blockchain for disputes.



2. Payment Channel Networks



Lightning Network [1]
- most popular implementation
- 80k channels
- 17k nodes

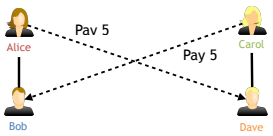
Problem: Infeasible to open a payment channel to everyone

Solution: Link payment channels to network, pay if connected by path

However: Current schemes (e.g., Lightning Network) only allow path based payments

Question:
Can we update channels for any topology?

Challenge:
Achieve atomicity & privacy!



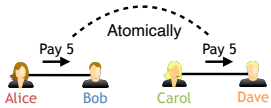
3. Thora

Desired properties:

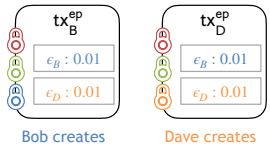
Atomicity: Either all channels are updated or none

Value privacy: No-one learns about the value of updates

Setting

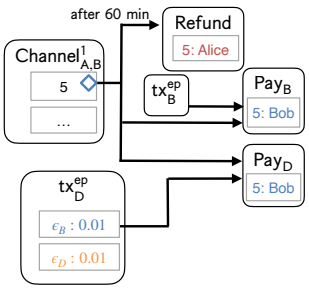


Step 1 - "Pre-Setup"

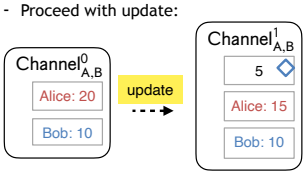


- "Receivers" (Bob, Dave) create "enable payment" transaction tx^{ep} each.
- Requires signature of senders and themselves
- Send tx^{ep} to all other parties.

Step 2 - "Setup"



- Alice and Bob prepare update above
- Payment if a tx^{ep} is posted
- Refund after 60min
- Proceed with update:



- Send "confirm" to all other parties
- Carol and Dave do the same steps

Step 3 - "Confirmation"

- Alice signs $\sigma_A(tx_B^{ep})$ and $\sigma_A(tx_D^{ep})$
- Carol signs $\sigma_C(tx_B^{ep})$ and $\sigma_C(tx_D^{ep})$
- They send $\sigma_A(tx_B^{ep})$ and $\sigma_C(tx_D^{ep})$ to Bob
- And $\sigma_A(tx_D^{ep})$ and $\sigma_C(tx_D^{ep})$ to Dave
- (Bob, Dave) reply with "ok" after receiving all signatures
- After "ok" from all channels, move to next step

Why atomicity holds:

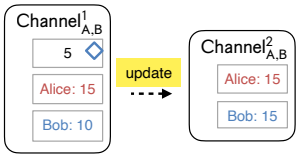
Step 2: Refunded after 60min, no payment if no tx^{ep} posted, tx^{ep} requires signature ("ok") of all channels

Step 3: Alice and Carol only give their signature after all channels completed step 2

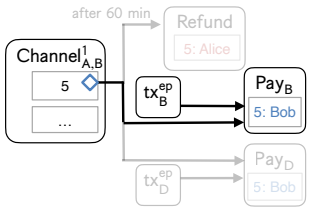
Step 4: Channels start updating only after all channels can post tx^{ep} (forcing all payments)

Step 4 - "Finalization"

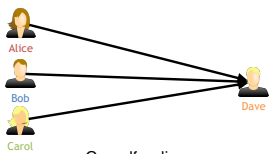
Honest:
- Users update their channel honestly, e.g., Alice and Bob:



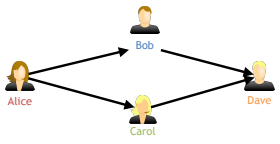
Forced update:
- If anyone, e.g., Alice, refuses to update, Bob simply posts tx_B^{ep}



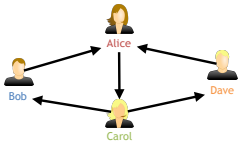
4. Application examples



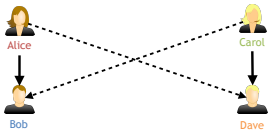
Crowdfunding



Atomic Multi-Path Payments



Rebalancing



Transaction Aggregation Problem [2]

5. Discussion

- **First secure** multi-channel update scheme
- Atomicity and value privacy, constant timelock
- **Proof-Of-Concept implementation**: Compatible with Bitcoin and the Lightning Network
- Formally modelled and **proved in the UC framework**
- Enables new interesting applications
- **Comparison** with other payment channel schemes
- **Other challenges** in Payment Channels:
  - Faster payments [3]
  - Channels for more than payments [4]
  - Virtual channels [5,6]
  - Allow users to go offline [7]

Scan me!

References:

[1] J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," *2016*

[2] S. Tiwari et al., "Wiser: Increasing Throughput in Payment Channel Networks with Transaction Aggregation," in AFT, *2022*.

[3] L. Aumayr, P. Moreno-Sanchez, A. Kate and M. Maffei, "Blitz: Secure Multi-Hop Payments Without Two-Phase Commits," in USENIX Security, *2021*.

[4] L. Aumayr et al., "Generalized Channels from Limited Blockchain Scripts and Adaptor Signatures," in Asiacrypt, *2021*.

[5] L. Aumayr et al., "Bitcoin-Compatible Virtual Channels," in IEEE Security and Privacy, *2021*.

[6] L. Aumayr, P. Moreno-Sanchez, A. Kate and M. Maffei, "Donner: UTXO-Based Virtual Channels Across Multiple Hops," eprint.iacr.org/2021/855, *2021*.

[7] L. Aumayr et al., "Sleepy Channels: Bitcoin-Compatible Bi-directional Payment Channels without Watchtowers," in ACM CCS, *2022*.