

Payment Channels with Proofs

Chad E. Brown, Cezary Kaliszyk, Josef Urban

Czech Technical University in Prague, University of Melbourne, University of Innsbruck

October 2025

Outline

- 1 Introduction
- 2 Payment Channels
- 3 Payment Channels With Proofs
- 4 Conclusion

Introduction

- Bitcoin is for sending money.
- Proofgold is for paying for (formal mathematical) proofs.
- Problem: Bitcoin is slow (10 minutes)
- and Proofgold is slower (1 hour)
- Solution: Lightning network...with proofs?
- Built using payment channels...with proofs

High Level Example

- Alice wants a proof of the Four Color Theorem by the end of 2025.
- Bob thinks he can supply one by that time.
- Alice bets Bob there will *not* be a proof by the end of 2025.
- Either Bob supplies a proof in time and gets paid by winning the bet,
- or doesn't and Alice gets paid by winning the bet.
- Offchain unless one side doesn't cooperate.

Payment Channels

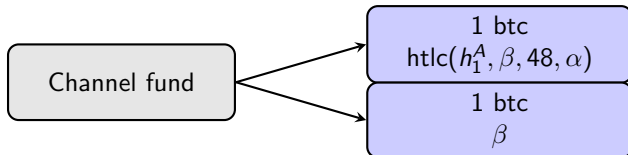
- Payment channels are between two parties: Alice and Bob.
- Alice has a balance and Bob has a balance.
- Example: Alice and Bob both put 1 bitcoin into a 2-of-2 multisig.
- Both have a starting balance of 1 bitcoin.
- Alice can send Bob 0.5 bitcoins. New balances:
 - Alice: 0.5
 - Bob: 1.5
- At any point either participant can close the channel to obtain their balance on chain.
- If either party tries to cheat, the other party can take all the funds.

HTLC: Hash Time Lock Contract

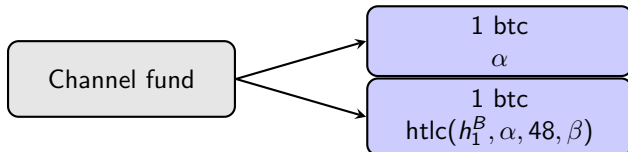
- Technically payment channels use HTLCs.
- Let $\text{htlc}(h, \alpha, N, \beta)$ denote the HTLC script spendable in two ways:
 - giving a secret s hashing to h and signing by α , or
 - waiting N blocks and signing by β .

Commitment Transactions

Alice:



Bob:



PTLC: Proposition Time Lock Contract

- PTLC scripts are like HTLC scripts but
- instead of knowing a secret a proposition would need to be proven.
- Proposition P , e.g.,
 - There are infinitely many primes. (Already done)
 - The 4 Color Theorem (Hard, but doable)
 - Fermat's Last Theorem (Unrealistic for now)
- Let $\text{ptlc}(P, \alpha, T, \beta)$ denote the PTLC script spendable in two ways:
 - Waiting until P has been proven (on chain) and signing by α , or
 - waiting until block T has passed and signing by β .

HTLC and PTLC Composed

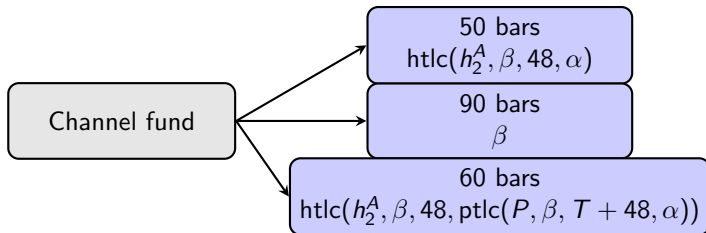
- For payment channels with proofs, the two scripts must be composed:

$$\text{htlc}(h, \delta, N, \text{ptlc}(P, \alpha, T, \beta))$$

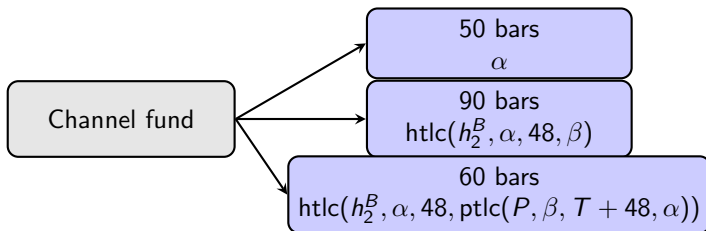
- This is a script spendable in three ways:
 - Giving a secret s hashing to h and signing by δ , or
 - waiting until P has been proven (on chain) and signing by α , or
 - waiting until block T has passed and signing by β .
- In practice the δ will always be either α or β .

Commitment Transactions with Bet

Alice:



Bob:



Challenges for Future Work (Extension to a Network)

- Formal analysis of economics and incentives
- Are there ways to significantly game proof revelation timing?
- When is a middleman incentivized to withhold a proof?
- Routing...
- Liquidity...

Conclusion

- Extension of payment channels with an optional third output.
- Third output allows participants to “bet” on whether a proof will be given by a deadline.
- Effectively allows participants to pay for proofs only using the (slow) Proofgold chain when things go wrong
- Necessary component for lightning network with proofs

Conclusion

- Extension of payment channels with an optional third output.
- Third output allows participants to “bet” on whether a proof will be given by a deadline.
- Effectively allows participants to pay for proofs only using the (slow) Proofgold chain when things go wrong
- Necessary component for lightning network with proofs

Thanks! Questions?

The results were supported by the Ministry of Education, Youth and Sports within the dedicated program ERC CZ under the project POSTMAN no. LL1902, Czech Science Foundation grant no. 25-17929X, Amazon Research Awards, and the ERC PoC grant *FormalWeb3* no. 101156734.