STREAMING LIGHTNING PAYMENTS WITH ROLLING HOLD INVOICES

Andy Schroder

2024-10-26

TABConf 6

How to sell variable products and services when the amount and time period in which the customer needs them are unknown?

EXAMPLES WHERE WE CAN SEE THIS PROBLEM

- Electrical energy sales at an electric car charging station or RV campsite
- Automotive gasoline or diesel sales at a fuel station
- Natural gas or electrical energy delivered to a home
- Fiber optic, cellular, or WiFi internet services
- Wireguard tunneling services
- Audio and video streaming
- Parking space usage

CONSTRAINTS

- Seller wants no risk (always wants some prepayment or deposit).
- Seller only wants their POS to be used to receive payments, never send.
- Buyer wants to minimize risk.
- Buyer wants to maintain privacy.
- Buyer wants minimal intervention.

POTENTIAL APPROACHES

- Manual large initial deposit payments with a partial refund when the product or service consumption is complete
- Automated high frequency micropayments until the product or service consumption is complete with no partial refund

PROBLEMS WITH PARTIAL REFUND PAYMENTS

- Requires manual intervention to coordinate the refund invoice after the product/service is done being delivered (there is no payment protocol for mobile wallets designed yet to coordinate this in advance).
  - Can we get an optionally required refund invoice added to BOLT12 invoice_requests?
- LNURL can be used to manually coordinate the refund invoice, but it requires a webserver and SSL, which complicate the software stack and introduce centralization of the SSL certificate authorities and DNS root nameservers.
- BOLT12 withdrawals aren't supported by any mobile wallets yet, and we are unsure if the onion messaging used by BOLT12 to return the refund invoice will scale since it is unmonetized like TOR.

PROBLEMS WITH PARTIAL REFUND PAYMENTS

- Need a way for the merchant to ensure (authenticate) that they are receiving a refund invoice from the original customer and not another party.
  - A passive or active eavesdroppers of the invoice request can try to send a refund invoice to the merchant quicker than actual customer.
  - This is particularly an issue for public, automated point of sale devices.
- Refund receiver privacy can be lost, making onion routing of the original payment useless.
  - BOLT11 invoices with blinded paths are a very new thing (~1 month), only supported by the latest release of LND, with no broader ecosystem support.
  - BOLT12 invoices with blinded paths don't have broad ecosystem either.
- Requires the merchant POS system to have the ability to send funds.

PROBLEMS WITH HIGH FREQUENCY MICRO PAYMENTS

- Buyer loses some small credit when they are done consuming products or services.
- High frequency small payments are hard to do reliably over unreliable and jittery cellular internet connections.
- Small payments often have higher fee percentages due to the base fee usually being at least 1 sat.
- Products or services with a high delivery rate and/or value require not-so-micro payments due to routing latency in the lightning network.
- We don't want to promote very high frequency and excessively small payments because they can't be settled on chain if below the dust limit and they also consume more local storage data and bandwidth.
- Some applications require dedicated hardware for sending the streaming payments, all require dedicated software.

WHAT IS A HOLD INVOICE?

- A HOLD invoice is a normal invoice, but the receiver's lightning node does not automatically release the preimage immediately when an HTLC is accepted.
- The preimage may not be automatically released because a party does not know it yet, or because they don't want to release it yet.
- The preimage can be released before the HTLC expires and settle the HTLC, or the HTLC can be canceled before expiration if the receiver no longer wants to accept the funds. If neither of these happen, the payment can always go on chain after the time lock.

USE HOLD INVOICES FOR SELLING AN UNKNOWN AMOUNT OF A PRODUCT OR SERVICE

1. Seller requests an initial deposit.
2. Buyer pays the deposit.
3. Seller receives the HTLC.
4. Seller does not release the preimage, but does begin to deliver products or services.
5. Buyer consumes some products or services.
6. If buyer reaches the credit limit, seller stops delivering products or services and releases the preimage and settles the HTLC.
7. If buyer does not reach the credit limit and is done consuming products or services, they request a final invoice.
8. Seller provides final invoice.
9. Buyer pays final invoice, seller receives the HTLC and automatically releases the preimage and settles the HTLC.
10. Seller cancels the initial deposit.

ELECTRIC CAR CHARGING EXAMPLE

The buyer makes a large initial payment and then makes a medium sized final payment to receive their held deposit back.

State	Description	Deposits Held	Consumed	Settled After Holding	Immediately Settled	Canceled	Total Deposits Held	Total Consumed	Total Settled After Holding	Total Immediately Settled	Total Settled	Total Canceled	Unsettled Consumption Needs to be paid to release held	Credit
1	buyer makes initial payment	100					100	0	0	0	0	0		100
2	charging		75				100	75	0	0	0	0	75	25
3	buyer makes final payment				75		100	75	0	75	75	0		100
4	held invoices canceled					100	0	75	0	75	75	100		0

FLEXIBILITY OF USING HOLD INVOICES

- Broad wallet compatibility, even works with submarine swaps and custodial services such as Strike and CashApp since it exists as part of the BOLTs.
- The buyer does not need to be authenticated.
  - Only the original sender can receive the funds back from the canceled HOLD invoice.
  - No one else is incentivized to pay the final invoice but the person that will receive the HOLD invoice canceled.
- Buyer's privacy is maintained.
- In LND, HOLD invoices can be controlled with just an invoice macaroon.

CHALLENGES WITH HOLD INVOICES

- Hard for the sender to tell if the payment failed to route or the invoice was canceled.
- Limited time of the HTLC limits the time the payment can be held and products or services can be consumed in.
- Held funds are locked up in all HTLC in the payment route while products or services are being consumed.
  - The longer the route, the more funds are locked up.
  - Some people don't like HOLD invoices and believe broad use will cause fees to be driven up because liquidity along the entire payment route is tied up.

PROBLEMS WITH THIS WORKFLOW

- Buyer temporarily needs extra funds to receive their initial deposit back.
- Buyer needs to trust the seller even more with their extra funds to receive their initial deposit back.
- It is confusing to users why they need to pay twice.
- Seller stops delivering products or services if initial deposit estimate was too low.

AN IMPROVEMENT: ROLLING HOLD INVOICES

- We can extend the previous workflow by making multiple payments to HOLD invoices, without waiting for the previous HOLD invoices to settle.
- Seller can keep multiple HOLD invoices unsettled.
- As buyer consumes products or services, seller can settle invoices and issue new invoices to extend the amount of products or services that can be delivered.
- If HTLC time limits are close to being reached, new HOLD invoices can be issued and the previous HOLD invoices canceled once the new HOLD invoice is paid.
- When the buyer is done consuming products or services, the seller can provide a final invoice. Once the final invoice is paid, all unsettled HOLD invoices can be canceled.
- Buyer can make smaller manual initial deposits and trust the seller less. As the buyer's confidence in the seller improves (say they actually received some product), they can make more payments.
- The final payment will always be less than the smallest unsettled invoice.

ELECTRIC CAR CHARGING EXAMPLE: ROLLING HOLD INVOICES

The buyer makes a large initial payment (possibly they already have some trust in the seller and are willing to take some higher risk), adding one additional payment because they undershot their initial deposit amount, and then makes a small final payment with low risk to receive held deposits back.

State	Description	Deposits Held	Consumed	Settled After Holding	Immediately Settled	Canceled	Total Deposits Held	Total Consumed	Total Settled After Holding	Total Immediately Settled	Total Settled	Total Canceled	Unsettled Consumption Needs to be paid to release held	Credit
1	buyer makes initial payment	100					100	0	0	0	0	0		100
2	charging		90				100	90	0	0	0	0	90	10
3	add a little more funds	20					120	90	0	0	0	0		30
4	charging continued		10				120	100	0	0	0	0		20
5	first invoice settled			100			20	100	100	0	100	0		20
6	charging completes		10				20	110	100	0	100	0	10	10
7	buyer makes final payment				10		20	110	100	10	110	0		20
8	held invoices canceled					20	0	110	100	10	110	20		0

ELECTRIC CAR CHARGING EXAMPLE: ROLLING HOLD INVOICES

The buyer makes a small initial risk, makes some additional payments after confidence is built in the seller and some product is consumed, and then some medium final risk to receive held deposits back.

State	Description	Deposits Held	Consumed	Settled After Holding	Immediately Settled	Canceled	Total Deposits Held	Total Consumed	Total Settled After Holding	Total Immediately Settled	Total Settled	Total Canceled	Unsettled Consumption Needs to be paid to release held	Credit
1	buyer makes initial payment	10					10	0	0	0	0	0		10
2	charger worked		4				10	4	0	0	0	0	4	6
3	buyer adds more funds	100					110	4	0	0	0	0		106
4	charging continued		6				110	10	0	0	0	0		100
5	first invoice settled			10			100	10	10	0	10	0		100
6	charging continued		90				100	100	10	0	10	0	90	10
7	buyer adds more funds	100					200	100	10	0	10	0		110
8	charging continued		10				200	110	10	0	10	0		100
9	second invoice settled			100			100	110	110	0	110	0		100
10	charging continued		30				100	140	110	0	110	0	30	70
11	buyer adds more funds	100					200	140	110	0	110	0		170
12	charging complete		40				200	180	110	0	110	0	70	130
13	cancel unneeded hold invoice					100	100	180	110	0	110	100	70	30
14	buyer makes final payment				70		100	180	110	70	180	100		100
15	held invoice canceled					100	0	180	110	70	180	200		0

SUMMARY

With rolling HOLD invoices, we can privately stream payments at a variety of payment sizes and frequencies, both manually and automatically. If the seller is honest, the buyer only pays for the exact amount of product or service that was consumed. The seller's POS does not need to have the ability to send any payments. The buyer can have an unreliable internet connection.

In the physical world, we can't eliminate risk completely, but we can make trade-offs and achieve a practical user experience. Rolling HOLD invoices allows the buyer to put some trust into the seller but still give the opportunity for the seller be honest. As the payment size is reduced, the trust required can be reduced, and the minimum payment size (and trust) limit is dependent on if one wants to dedicate hardware to automate payments, the stability of internet connection, the value of the product or service, and the speed at which the product or service is delivered at.

Questions?

http://AndySchroder.com/

info@AndySchroder.com