

# Sequential Commit

## Table of contents

[Table of contents](#)

[Motivation](#)

[Idea](#)

[Principles](#)

[Application of principles in different final states](#)

[Completed](#)

[Revoked](#)

[Cancelled](#)

[Retracted](#)

[Resolved/Decided](#)

[Resolved/Decided](#)

[Mathematical models](#)

[Reference implementation](#)

[P&L table](#)

[Cash flows](#)

[Basic model: all funds encumbered till the end](#)

[Capital-time optimized model: funds partially released after every commit](#)

[Examples](#)

[How to read the tables below](#)

[No seller deposit, buyer cancellation penalty and royalties](#)

[Completed/Retracted](#)

[Revoked/Cancelled](#)

[Resolved/Decided](#)

[Non-zero seller deposit and buyer cancellation penalty. Royalties still zero](#)

[Completed/Retracted](#)

[Revoked](#)

[Cancelled](#)

[Resolved/Decided](#)

[All offer parameters are greater than zero](#)

[Completed/Retracted](#)

[Revoked](#)

[Cancelled](#)

[Resolved/Decided](#)

[Known drawbacks](#)

[Seller and last buyer collaboration](#)

[Seller buyback and Revoke](#)

# Motivation

## **Trust-minimized exchange on the secondary market**

In Boson Protocol v1 & v2.0 vouchers are only backed by funds relating to the commit step of an exchange (price + seller deposit).

In this current architecture Boson Protocol fully protects buyers on the primary market but only partially protects buyers on the secondary market.

*This could result in buyers ending up with a loss when buying on the secondary market, if the seller fails to deliver on their promise.*

An example:

Alice commits to an offer with a price of 100 USDC and a seller deposit of 10 USDC, Alice then sells the voucher to Bob for 200 USDC. Bob redeems the voucher but doesn't receive the item and raises a dispute.

In this case of the seller failing to fulfil their promise, Bob can only receive a refund of 110 USDC (price + seller deposit) instead of the 200 USDC he used to purchase the voucher - losing a total of 90 USDC.

# Idea

## **How might we protect buyers on the secondary market?**

Sequential commit is a proposed solution in which funds involved in the secondary sale of a voucher are locked up in escrow until the redemption of the voucher has been settled.

This protects buyers on the secondary market and allows them to receive back a full refund of the secondary market price they paid in case the seller doesn't deliver.

Alice commits to an offer with a price of 100 USDC and a seller deposit of 10 USDC.

Alice sells the voucher to Bob for 200 USDC.

Bob redeems the voucher but doesn't receive the item and raises a dispute.

Bob escalates the dispute and receives back the secondary market price he paid (200 USDC) and the seller deposit (10 USDC).

# Principles

This section describes the principles that must be followed in every scenario (unless specified otherwise), regardless of factors such as:

- number of resellers,
- initial offer properties (price, seller deposit, buyer cancellation penalty,
- exchange final state (completed, revoked, cancelled, retracted, resolved, decided, refused).

Based on these principles, behaviour in each scenario can be determined and mathematically described.

**Principle №1: All buyers get back the money they put in, in the event of a Seller default.**

If Seller fails to deliver on their promise all Buyers should be reversed/repaid in full.

Seller default is considered when:

- Seller revokes.
- Buyer is given 100% in Dispute Resolution (MR or EDR)

**Principle №2: Final Buyer ( $B_N$ ) is the only buyer that receives any compensation from Seller Deposit.**

$B_N$  is the only Buyer that incurs a direct loss (i.e. doesn't get the item, endures poor quality), whereas intermediary Buyers might suffer lost profit only. In case of Seller default,  $B_N$  gets full seller deposit and in case of Dispute Resolution Seller gets a part of the deposit, as determined by DR. Effectively Seller Deposit is split between Seller and  $B_N$  in a same way, regardless of number of intermediary Buyers.

View Seller deposit as a voucher / bearer guarantee.

**Principle №3: Final Buyer ( $B_N$ ) should be able to have up to 100% of their payment returned via DR.**

Buyer assurance should not depend on the provenance of a voucher. Regardless of a prior chain of resales, if Buyer  $B_N$  purchases an item for Price  $P$ , they should be able to be refunded for the full or part payment amount via DR.

**Principle №4: Seller should not receive more than the initial Payment price  $P_0$ .**

Even if the last price  $P_N$  is greater than the original price  $P_0$ , Seller should always receive at most  $P_0$  (i.e. payout in happy path - exchange is Completed). If there was a chance to get more than  $P_0$  (for example in DR), Seller might be tempted to provoke a dispute to get better payout.

**Principle №5: If two different scenarios represent the same end state, payouts to all involved parties should be the same in both scenarios**

Equivalent end states are:

- Completed == Retracted (after MR or EDR) == Buyer gets 0% in DR
- Revoked == Buyer gets 100% in DR

When payouts for one final state is determined, other equivalent final states must have the same payout.

**Principle №6: Intermediary Buyer  $B_i$  should receive at least  $\min(P_i, P_{i+1})$  and at most  $\max(P_i, P_{i+1})$  regardless of final state**

$P_i$  is the price  $B_i$  paid and  $P_{i+1}$  is the price they sold the voucher for to the next buyer. The maximum the  $B_i$  can get is if the exchange completes in a happy path and  $P_{i+1}$  is greater than  $P_i$ . The minimum they can get is if the exchange completes in a happy path and  $P_{i+1}$  is lower than  $P_i$ . Any other scenario must result in total payout between  $P_i$  and  $P_{i+1}$ .

**Principle №7: Final state determines effective price of voucher in every exchange**

Effective price  $P'$  is the price that the last buyer  $B_N$  actually pays. Last price on the secondary market is  $P_N$ , which can be considered as an effective price only in a happy path ( $P_N$ ). In case of Revocation or Cancellation  $P' = 0$  and in case of DR  $P' = (1 - \text{buyerPercent}) * P_N$ . Ratio

$P'/P_N$  is then applied to all intermediary prices  $P'_i = P'/P_N * P_i$ . This affects Buyers' profits by the same ratio.

**Principle №8: Royalties are calculated based on effective prices**

Effective prices are determined by principle №7 and royalties are a percentage of effective price.

**Principle №9: Fees are taken for every successful order**

Whenever royalties are paid out, protocol fees are taken. Conceptually fees can be considered as additional royalty. Sum of fees and royalties must not exceed item price.

**Principle №10: Minimize complexity**

We should seek to minimise cognitively complex (for humans) or computationally complex (for blockchains) calculations.

**Principle №11: Optimise capital-duration efficiency**

We should seek to minimise the product of the capital and duration of lock-up, whilst ensuring that all commitments can be met. Following principle №6,  $\min(P_i, P_{i+1})$  can always be released to buyer  $B_i$  once item is sold to buyer  $B_{i+1}$  for price of  $P_{i+1}$

**Principle №12: Subsequent trades must all be done in the same exchange token as the original order**

Allowing any exchange token would complicate the bookkeeping. It would also affect protocol fees which would either be paid out in different tokens (undesired) or it would require more complex fx exchange every time when sequential commit would happen in another token.

## Application of principles in different final states

### Completed

This is the happy path.

- Seller gets:
  - Original price  $P_0$
  - Seller deposit back
  - Royalties from every sale
- Intermediary buyers get a difference between the price they paid and the price they sold for, reduced by royalties. Net profit can be negative.
- Buyer  $B_N$  gets item and nothing from the protocol

### Revoked

- Seller:
  - Loses Seller Deposit
  - Doesn't get price  $P_0$

- Gets no royalties
- Intermediary buyers get back the price they paid. Net profit is 0.
- Buyer  $B_N$  gets
  - Back price they paid on secondary market
  - Seller deposit in full

## Cancelled

- Seller:
  - Gets back Seller Deposit
  - Doesn't get price  $P_0$
  - Gets buyer cancelation penalty
  - Gets no royalties
- Intermediary buyers get back the price they paid. Net profit is 0.
- Buyer  $B_N$  gets
  - Back price they paid on secondary market less buyer cancelation penalty

## Retracted

After the dispute was raised (and potentially escalated), Buyer can retract from it, signalling that everything is ok. This end state is equivalent to Completed

- Seller gets:
  - Original price  $P_0$
  - Seller deposit back
  - Royalties from every sale
- Intermediary buyers get a difference between the price they paid and the price they sold for, reduced by royalties. Net profit can be negative.
- Buyer  $B_N$  gets item and nothing from the protocol

## Resolved/Decided

After the dispute was raised (and potentially escalated), Buyer and Seller can mutually resolve it (final state Resolved) or Dispute Resolver can decide on split. Effectively what is decided in the process is how much of last price  $P_N$  is given back to Buyer N

- Seller gets:
  - Part of original price  $P_0$
  - Part of Seller deposit back
  - Royalties from every sale, adjusted following principles №7 and №8
- Intermediary buyers get part of a difference between the price they paid and the price they sold for, reduced by royalties. Effectively their net profit is multiplied by the percent given to the original seller in DR. Net profit can be negative.
- Buyer  $B_N$ 
  - Potentially gets (Unsatisfactory) item
  - Gets Part of price  $P_N$
  - Gets Part of seller deposit

There are two extreme cases:

- Buyer gets 100%. This is equivalent to “Revoked”.
- Buyer gets 0%. This is equivalent to “Completed”.

## Resolved/Decided

If the dispute was raised and potentially escalated, DR can explicitly refuse to resolve it or simply let it expire. In that case everyone gets back everything they paid in.

- Seller gets:
  - Seller deposit back
- Intermediary buyers get back the price they paid. Net profit is 0.
- Buyer  $B_N$  gets back  $P_N$

## Mathematical models

This section presents two model:

1. Basic model, where all funds are encumbered until the end
2. Capital-time optimized model where part of funds is released after every sequential commit.

Following the principles **№10** and **№11** there is a tradeoff between these two models. Basic model is less complex (principle №10), while optimized model is more efficient when it comes to capital-time (principle №10).

We mathematically describe two things

- **Net Profit & Loss.** These formulas directly describe the difference between inputs and outputs in the protocol for every involved entity. They are model invariant. Total net profit should always be 0.
- **Cash flows.** These formulas describe the change of escrow and entities' balances after every action (i.e. commit or finalization). These differ across the models. Sum of all cash flows should always be 0.

The following symbols will be used:

- Seller:  $S$
- Buyers:  $B_0, B_1, \dots, B_N$
- Price paid by buyer  $B_i$ :  $p_i$
- Seller deposit:  $d$
- Buyer cancellation penalty:  $c$
- Buyer split percent:  $s$
- Royalties and fees at the time of exchange:  $r_i$

Note the in special cases (e.g.  $d = 0$  or  $c = 0$  or  $s = 0$  or  $s = 1$  or  $r = 0$ ) formulas can be further simplified.

## Reference implementation

All formulae from the tables below are implemented in: [📄 Sequential commit](#) .

Implementation is for sequential commits with three intermediary buyers. You can play around with input parameters to see how it affects cash flows and net profit under both models.

## P&L table

This table represents net financial profit for different exchange final states. They are the same for optimised and non-optimised model

	Final state	Seller	Buyers $B_i \in [B_0, B_{N-1}]$	Buyer $B_N$
	Completed	$p_0 + \sum_{i=1}^N r_i p_i$	$(1 - r_i)p_{i+1} - p_i$	$- p_N$
	Revoked	$- d$	0	$d$
	Cancelled	$c$	0	$- c$
disputed	Retracted	$p_0 + \sum_{i=1}^N r p_i$	$(1 - r_i)p_{i+1} - p_i$	$- p_N$
	Resolved	$(1 - s)(d + p_0 + \sum_{i=1}^N r_i p_i)$	$s p_i + (1 - s)(1 - r_i)p_{i+1} - p_i$ $= (1 - s)((1 - r_i)p_{i+1} - p_i)$	$s(p_N + d) - p_N$
	Decided	$- d$		
	Refused	0	0	0

## Cash flows

Next tables shows cash flows into and out of the protocol at different steps:

- First commit (exchange start)
- Sequential commits
- Exchange finalisation

Note that buyer's cash flows into protocol are true cash flows (i.e. token balance gets updated), while cash flows out of the protocol only release funds (make them available for withdrawal), but funds are not sent anywhere. Buyer or seller must withdraw them by themselves.

In addition to cash flows, tables also show escrow balance after every step.

Notation:

- $CF(A, i)$  - Cash flows for actor  $A$  at step  $i$ . (e.g.  $CF(B_5, 5)$  is cash flow of seller 5 at 5th commit)
- $E(i)$  - Total funds locked in escrow at step  $i$

Note that at every step  $E(i) = E(i - 1) + \sum_{A \in [S, B_0, \dots, B_i]} CF(A, i)$ ; with  $E(-1) = 0$  (before

exchange starts, no encumbered funds are associated with it)

## Basic model: all funds encumbered till the end

This model is less complex to understand, since involved parties just wait till the end and get a full payout, depending on the final state of exchange. However this is not capital-time optimal since after each trade it's certain that the reseller will get some money out, regardless of final state and that capital unnecessarily stays locked in escrow.

First commit:

$$\begin{aligned} CF(S, 0) &= -d \\ CF(B_0, 0) &= -p_0 \\ E(0) &= p_0 + d \end{aligned}$$

Sequential commit  $i$ :

$$\begin{aligned} CF(B_i) &= -p_i \\ E(i) &= E(i - 1) + p_i = d + \sum_{j=0}^i p_j \end{aligned}$$

Cash flows after finalization:

		Final state	Seller	Buyers $B_i \in [B_0, B_{N-1}]$	Buyer $B_N$
		Completed	$d + p_0 + \sum_{i=1}^N r_i p_i$	$(1 - r_{i+1})p_{i+1}$	0
		Revoked	0	$p_i$	$p_N + d$
		Cancelled	$d + c$	$p_i$	$p_N - c$
disputed	escalated	Retracted	$d + p_0 + \sum_{i=1}^N r_i p_i$	$(1 - r_{i+1})p_{i+1}$	0
		Resolved	$(1 - s)(d + p_0 + \sum_{i=1}^N r_{i+1} p_i)$	$sp_i + (1 - s)(1 - r_{i+1})p_{i+1}$	$s(p_N + d)$
		Decided			
		Refused	$d$	$p_i$	$p_N$

Total cash flow after finalization should match the amount in escrow  $E(N) = d + \sum_{i=0}^N p_i$



## Capital-time optimized model: funds partially released after every commit

This model provides a solution to the capital-time inefficiency of the basic model. After every commit it's possible to determine the minimal payout to the reseller (principle №6) which is released immediately (i.e. during commit). The difference between minimal and maximum payout is then release during the finalization and the amount released depends on the final state and relationship between the price Buyer paid for and the price they sold it for.

First commit:

$$\begin{aligned} CF(S, 0) &= -d \\ CF(B_0, 0) &= -p_0 \\ E(0) &= p_0 + d \end{aligned}$$

Sequential commit  $i > 0$ :

$$\begin{aligned} CF(B_i) &= -p_i \\ CF(B_{i-1}) &= \min(p_{i-1}, (1 - r_i)p_i) \end{aligned}$$

$$\begin{aligned} E(i) &= E(i - 1) + p_i - \min(p_{i-1}, (1 - r_i)p_i) = d + \sum_{j=0}^i (p_j - \min(p_{j-1}, (1 - r_j)p_j)) \\ \text{with } E(-1) &= p_{-1} = 0 \end{aligned}$$

In special case, where  $\forall i: (1 - r_i)p_i \geq p_{i-1} \Rightarrow E(i) = d + p_i$

Cash flows after finalization:

		Final state	Seller	Buyers $B_i \in [B_0, B_{N-1}]$	Buyer $B_N$
d i s p u t e d	e s c a l a t e d	Completed	$d + p_0 + \sum_{i=1}^N r_i p_i$	$\max((1 - r_{i+1})p_{i+1} - p_i, 0)$	0
		Revoked	0	$\max(p_i - (1 - r_{i+1})p_{i+1}, 0)$	$p_N + d$
		Cancelled	$d + c$	$\max(p_i - (1 - r_{i+1})p_{i+1}, 0)$	$p_N - c$
		Retracted	$d + p_0 + \sum_{i=1}^N r_i p_i$	$\max((1 - r_{i+1})p_{i+1} - p_i, 0)$	0
		Resolved	$(1 - s)(d + p_0 + \sum_{i=1}^N r_i p_i)$	$sp_i + (1 - s)p_{i+1} - \min(p_i(1 - r_{i+1})p_{i+1})$ $= \max((1 - s)((1 - r_{i+1})p_{i+1} - p_i), s(p_i - (1 - r_{i+1})p_{i+1}))$	$s(p_N + d)$
		Decided			
		Refused	$d$	$\max(p_i - (1 - r_{i+1})p_{i+1}, 0)$	$p_N$


Total cash flow after finalization should match the amount in escrow

$$E(N) = d + \sum_{i=0}^N (p_i - \min(p_{i-1}, (1 - r_{i+1})p_i))$$

## Examples

This section provides examples for certain scenarios and only for optimized model. No examples are provided for final state “Refused” since everyone just gets everything back regardless of input parameters.

For an arbitrary input parameters or to see behaviour in a basic model, please use

 Sequential commit .

Variables that will be varied in examples:

Price dynamic:

- Strictly increasing
- Constant
- Strictly decreasing
- Mixed (increase, constant, decrease)

Final state:

- Completed/Retracted
- Revoked
- Cancelled
- Resolved/Decided

Offer parameters

- Seller deposit and buyer cancellation penalty (zero vs non zero)
- Royalties (with or without)

Original price  $p_0 = 100$  in all examples.

How to read the tables below

Tables contain the information about:

- Prices paid by each buyer
- Cash flows for all commits and finalization
- Escrow balance after every commit or finalization
- Net profits for each entity

Other information (royalties, split amount) is provided in sections where it is relevant.

Here is the example for Completed exchange with 10% royalties.

			prices $p_i$			
			100	150	160	400
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	160		100	-150		
Commit 2	176			144	-160	
Commit 3	416				160	-400
Finalization: Completed	0.00	181.00	35.00	0.00	200.00	0.00
Net profit	0.00	171.00	35.00	-6.00	200.00	-400.00

Amount in escrow after each step. E.g. after commit 1, escrow holds 160 units.

Cash flows during the commit. During commit 1, buyer 1 paid in 150 units, while 100 units were released to Buyer 0

Cash flows during the finalization. For example seller gets the sum of original price, royalties and seller deposit.

Net profit of each entity. This is sum of all cash flows each entity. For example, Seller's net profit is 10 less than they got at finalization, since they paid in 10 for seller deposit.

Prices paid by each buyer. Price directly above the buyer is the amount buyer paid, so price on to the right is the amount it was resold for. Difference between these prices is expected Buyers profit (less royalties).

## No seller deposit, buyer cancellation penalty and royalties

The simplest setup where seller deposit, buyer cancellation penalty and royalties are all 0.

### Completed/Retracted

#### Strictly increasing prices

			prices $p_i$			
			100	150	160	400
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	100	0	-100			
Commit 1	150		100	-150		
Commit 2	160			150	-160	
Commit 3	400				160	-400
Finalization: Completed	0.00	100.00	50.00	10.00	240.00	0.00
Net profit	0.00	100.00	50.00	10.00	240.00	-400.00

#### Constant prices

			prices $p_i$			

			100	100	100	100
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	100	0	-100			
Commit 1	100		100	-100		
Commit 2	100			100	-100	
Commit 3	100				100	-100
Finalization: Completed	0.00	100.00	0.00	0.00	0.00	0.00
Net profit	0.00	100.00	0.00	0.00	0.00	-100.00

### Strictly decreasing prices

			prices $p_i$			
			100	90	85	50
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	100	0	-100			
Commit 1	100		90	-90		
Commit 2	100			85	-85	
Commit 3	100				50	-50
Finalization: Completed	0.00	100.00	0.00	0.00	0.00	0.00
Net profit	0.00	100.00	-10.00	-5.00	-35.00	-50.00

Note: if prices decrease and exchange is completed, resellers don't get anything during the finalization, since all funds were released already during the commit.

### Mixed price behaviour

			prices $p_i$			
			100	130	130	120
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	100	0	-100			
Commit 1	130		100	-130		
Commit 2	130			130	-130	
Commit 3	130				120	-120
Finalization: Completed	0.00	100.00	30.00	0.00	0.00	0.00
Net profit	0.00	100.00	30.00	0.00	-10.00	-120.00

Note: if prices sometimes increase and sometimes decrease, some reseller's get money out during finalization and others don't.

## Revoked/Cancelled

Examples for revoked and cancelled are in this section presented together, since payouts are the same if there is no seller deposit and buyer cancelation penalty.

### Strictly increasing prices

			prices $p_i$			
			100	150	160	400
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	100	0	-100			
Commit 1	150		100	-150		
Commit 2	160			150	-160	
Commit 3	400				160	-400
Finalization:						
Revoked	0.00	0.00	0.00	0.00	0.00	400.00
Net profit	0.00	0.00	0.00	0.00	0.00	0.00

### Constant prices

			prices $p_i$			
			100	100	100	100
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	100	0	-100			
Commit 1	100		100	-100		
Commit 2	100			100	-100	
Commit 3	100				100	-100
Finalization:						
Revoked	0.00	0.00	0.00	0.00	0.00	100.00
Net profit	0.00	0.00	0.00	0.00	0.00	0.00

### Strictly decreasing prices

			prices $p_i$			
			100	90	85	50
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	100	0	-100			
Commit 1	100		90	-90		
Commit 2	100			85	-85	
Commit 3	100				50	-50
Finalization:						
Revoked	0.00	0.00	10.00	5.00	35.00	50.00
Net profit	0.00	0.00	0.00	0.00	0.00	0.00

Note: if prices decrease and exchange is revoked or cancelled, resellers actually get additional funds released at the end which offset their loss.

### Mixed price behaviour

			prices p <sub>i</sub>			
			100	130	130	120
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	100	0	-100			
Commit 1	130		100	-130		
Commit 2	130			130	-130	
Commit 3	130				120	-120
Finalization: Revoked	0.00	0.00	0.00	0.00	10.00	120.00
Net profit	0.00	0.00	0.00	0.00	0.00	0.00

### Resolved/Decided

Split: 50%:50%

### Strictly increasing prices

			prices p <sub>i</sub>			
			100	150	160	400
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	100	0	-100			
Commit 1	150		100	-150		
Commit 2	160			150	-160	
Commit 3	400				160	-400
Finalization: Resolved	0.00	50.00	25.00	5.00	120.00	200.00
Net profit	0.00	50.00	25.00	5.00	120.00	-200.00

Note: if exchange goes into dispute resolution, final split affects resellers' profits. If DR assigns X% to Seller, also resellers get only X% of their profit.

### Constant prices

			prices p <sub>i</sub>			
			100	100	100	100
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	100	0	-100			
Commit 1	100		100	-100		
Commit 2	100			100	-100	
Commit 3	100				100	-100

Finalization: Resolved	0.00	50.00	0.00	0.00	0.00	50.00
Net profit	0.00	50.00	0.00	0.00	0.00	-50.00

### Strictly decreasing prices

			prices $p_i$			
			100	90	85	50
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	100	0	-100			
Commit 1	100		90	-90		
Commit 2	100			85	-85	
Commit 3	100				50	-50
Finalization: Resolved	0.00	50.00	5.00	2.50	17.50	25.00
Net profit	0.00	50.00	-5.00	-2.50	-17.50	-25.00

### Mixed price behaviour

			prices $p_i$			
			100	130	130	120
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	100	0	-100			
Commit 1	130		100	-130		
Commit 2	130			130	-130	
Commit 3	130				120	-120
Finalization: Resolved	0.00	50.00	15.00	0.00	5.00	60.00
Net profit	0.00	50.00	15.00	0.00	-5.00	-60.00

Non-zero seller deposit and buyer cancellation penalty.

Royalties still zero

Seller deposit  $d = 10$  and buyer cancellation penalty  $c = 30$

Completed/Retracted

### Strictly increasing prices

			prices $p_i$			
			100	150	160	400
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			

Commit 1	160		100	-150		
Commit 2	170			150	-160	
Commit 3	410				160	-400
Finalization: Completed	0.00	110.00	50.00	10.00	240.00	0.00
Net profit	0.00	100.00	50.00	10.00	240.00	-400.00

### Constant prices

			prices p <sub>i</sub>			
			100	100	100	100
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	110		100	-100		
Commit 2	110			100	-100	
Commit 3	110				100	-100
Finalization: Completed	0.00	110.00	0.00	0.00	0.00	0.00
Net profit	0.00	100.00	0.00	0.00	0.00	-100.00

### Strictly decreasing prices

			prices p <sub>i</sub>			
			100	90	85	50
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	110		90	-90		
Commit 2	110			85	-85	
Commit 3	110				50	-50
Finalization: Completed	0.00	110.00	0.00	0.00	0.00	0.00
Net profit	0.00	100.00	-10.00	-5.00	-35.00	-50.00

### Mixed price behaviour

			prices p <sub>i</sub>			
			100	130	130	120
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	140		100	-130		
Commit 2	140			130	-130	
Commit 3	140				120	-120



Finalization: Completed	0.00	110.00	30.00	0.00	0.00	0.00
Net profit	0.00	100.00	30.00	0.00	-10.00	-120.00

## Revoked

### Strictly increasing prices

			prices $p_i$			
			100	150	160	400
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	160		100	-150		
Commit 2	170			150	-160	
Commit 3	410				160	-400
Finalization: Revoked	0.00	0.00	0.00	0.00	0.00	410.00
Net profit	0.00	-10.00	0.00	0.00	0.00	10.00

Note: non zero seller deposit does not affect resellers' cash flows or net profit.

### Constant prices

			prices $p_i$			
			100	100	100	100
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	110		100	-100		
Commit 2	110			100	-100	
Commit 3	110				100	-100
Finalization: Revoked	0.00	0.00	0.00	0.00	0.00	110.00
Net profit	0.00	-10.00	0.00	0.00	0.00	10.00

### Strictly decreasing prices

			prices $p_i$			
			100	90	85	50
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	110		90	-90		
Commit 2	110			85	-85	
Commit 3	110				50	-50
Finalization:	0.00	0.00	10.00	5.00	35.00	60.00

Revoked						
Net profit	0.00	-10.00	0.00	0.00	0.00	10.00

### Mixed price behaviour

			prices $p_i$			
			100	130	130	120
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	140		100	-130		
Commit 2	140			130	-130	
Commit 3	140				120	-120
Finalization: Revoked	0.00	0.00	0.00	0.00	10.00	130.00
Net profit	0.00	-10.00	0.00	0.00	0.00	10.00

### Cancelled

#### Strictly increasing prices

			prices $p_i$			
			100	150	160	400
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	160		100	-150		
Commit 2	170			150	-160	
Commit 3	410				160	-400
Finalization: Cancelled	0.00	40.00	0.00	0.00	0.00	370.00
Net profit	0.00	30.00	0.00	0.00	0.00	-30.00

Note: non zero buyer cancellation penalty does not affect resellers' cash flows or net profit.

#### Constant prices

			prices $p_i$			
			100	100	100	100
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	110		100	-100		
Commit 2	110			100	-100	
Commit 3	110				100	-100
Finalization: Cancelled	0.00	40.00	0.00	0.00	0.00	70.00

Net profit	0.00	30.00	0.00	0.00	0.00	-30.00
------------	------	-------	------	------	------	--------

### Strictly decreasing prices

			prices p <sub>i</sub>			
			100	90	85	50
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	110		90	-90		
Commit 2	110			85	-85	
Commit 3	110				50	-50
Finalization: Cancelled	0.00	40.00	10.00	5.00	35.00	20.00
Net profit	0.00	30.00	0.00	0.00	0.00	-30.00

### Mixed price behaviour

			prices p <sub>i</sub>			
			100	130	130	120
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	140		100	-130		
Commit 2	140			130	-130	
Commit 3	140				120	-120
Finalization: Cancelled	0.00	40.00	0.00	0.00	10.00	90.00
Net profit	0.00	30.00	0.00	0.00	0.00	-30.00

### Resolved/Decided

Split: 50%:50%

### Strictly increasing prices

			prices p <sub>i</sub>			
			100	150	160	400
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	160		100	-150		
Commit 2	170			150	-160	
Commit 3	410				160	-400
Finalization: Resolved	0.00	55.00	25.00	5.00	120.00	205.00
Net profit	0.00	45.00	25.00	5.00	120.00	-195.00

### Constant prices

			prices p <sub>i</sub>			
			100	100	100	100
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	110		100	-100		
Commit 2	110			100	-100	
Commit 3	110				100	-100
Finalization: Resolved	0.00	55.00	0.00	0.00	0.00	55.00
Net profit	0.00	45.00	0.00	0.00	0.00	-45.00

### Strictly decreasing prices

			prices p <sub>i</sub>			
			100	90	85	50
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	110		90	-90		
Commit 2	110			85	-85	
Commit 3	110				50	-50
Finalization: Resolved	0.00	55.00	5.00	2.50	17.50	30.00
Net profit	0.00	45.00	-5.00	-2.50	-17.50	-20.00

### Mixed price behaviour

			prices p <sub>i</sub>			
			100	130	130	120
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	140		100	-130		
Commit 2	140			130	-130	
Commit 3	140				120	-120
Finalization: Resolved	0.00	55.00	15.00	0.00	5.00	65.00
Net profit	0.00	45.00	15.00	0.00	-5.00	-55.00

## All offer parameters are greater than zero

Seller deposit  $d = 10$ , buyer cancellation penalty  $c = 30$  and constant royalties  $r = 10\%$

### Completed/Retracted

#### Strictly increasing prices

			prices $p_i$			
			100	150	160	400
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	160		100	-150		
Commit 2	176			144	-160	
Commit 3	416				160	-400
Finalization: Completed	0.00	181.00	35.00	0.00	200.00	0.00
Net profit	0.00	171.00	35.00	-6.00	200.00	-400.00

Note: even if prices are strictly increasing, reseller can incur loss if difference between prices is less than royalties paid (look at sale between Buyer 1 and Buyer 2).

#### Constant prices

			prices $p_i$			
			100	100	100	100
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	120		90	-100		
Commit 2	130			90	-100	
Commit 3	140				90	-100
Finalization: Completed	0.00	140.00	0.00	0.00	0.00	0.00
Net profit	0.00	130.00	-10.00	-10.00	-10.00	-100.00

#### Strictly decreasing prices

			prices $p_i$			
			100	90	85	50
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	119		81	-90		
Commit 2	127.5			76.5	-85	
Commit 3	132.5				45	-50
Finalization:	0.00	132.50	0.00	0.00	0.00	0.00

Completed						
Net profit	0.00	122.50	-19.00	-13.50	-40.00	-50.00

### Mixed price behaviour

			prices p <sub>i</sub>			
			100	130	130	120
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	140		100	-130		
Commit 2	153			117	-130	
Commit 3	165				108	-120
Finalization: Completed	0.00	148.00	17.00	0.00	0.00	0.00
Net profit	0.00	138.00	17.00	-13.00	-22.00	-120.00

### Revoked

#### Strictly increasing prices

			prices p <sub>i</sub>			
			100	150	160	400
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	160		100	-150		
Commit 2	176			144	-160	
Commit 3	416				160	-400
Finalization: Revoked	0.00	0.00	0.00	6.00	0.00	410.00
Net profit	0.00	-10.00	0.00	0.00	0.00	10.00

Note: Buyer 1 gets some funds during finalization to cover virtual loss because of royalties.

#### Constant prices

			prices p <sub>i</sub>			
			100	100	100	100
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	120		90	-100		
Commit 2	130			90	-100	
Commit 3	140				90	-100
Finalization: Revoked	0.00	0.00	10.00	10.00	10.00	110.00

Net profit	0.00	-10.00	0.00	0.00	0.00	10.00
------------	------	--------	------	------	------	-------

### Strictly decreasing prices

			prices p <sub>i</sub>			
			100	90	85	50
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	119		81	-90		
Commit 2	127.5			76.5	-85	
Commit 3	132.5				45	-50
Finalization: Revoked	0.00	0.00	19.00	13.50	40.00	60.00
Net profit	0.00	-10.00	0.00	0.00	0.00	10.00

### Mixed price behaviour

			prices p <sub>i</sub>			
			100	130	130	120
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	140		100	-130		
Commit 2	153			117	-130	
Commit 3	165				108	-120
Finalization: Revoked	0.00	0.00	0.00	13.00	22.00	130.00
Net profit	0.00	-10.00	0.00	0.00	0.00	10.00

### Cancelled

#### Strictly increasing prices

			prices p <sub>i</sub>			
			100	150	160	400
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	160		100	-150		
Commit 2	176			144	-160	
Commit 3	416				160	-400
Finalization: Cancelled	0.00	40.00	0.00	6.00	0.00	370.00
Net profit	0.00	30.00	0.00	0.00	0.00	-30.00

### Constant prices

			prices p <sub>i</sub>			
			100	100	100	100
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	120		90	-100		
Commit 2	130			90	-100	
Commit 3	140				90	-100
Finalization: Cancelled	0.00	40.00	10.00	10.00	10.00	70.00
Net profit	0.00	30.00	0.00	0.00	0.00	-30.00

### Strictly decreasing prices

			prices p <sub>i</sub>			
			100	90	85	50
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	119		81	-90		
Commit 2	127.5			76.5	-85	
Commit 3	132.5				45	-50
Finalization: Cancelled	0.00	40.00	19.00	13.50	40.00	20.00
Net profit	0.00	30.00	0.00	0.00	0.00	-30.00

### Mixed price behaviour

			prices p <sub>i</sub>			
			100	130	130	120
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	140		100	-130		
Commit 2	153			117	-130	
Commit 3	165				108	-120
Finalization: Cancelled	0.00	40.00	0.00	13.00	22.00	90.00
Net profit	0.00	30.00	0.00	0.00	0.00	-30.00

### Resolved/Decided

Split: 50%:50%

### Strictly increasing prices



			prices $p_i$			
			100	150	160	400
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	160		100	-150		
Commit 2	176			144	-160	
Commit 3	416				160	-400
Finalization: Resolved	0.00	90.50	17.50	3.00	100.00	205.00
Net profit	0.00	80.50	17.50	-3.00	100.00	-195.00

### Constant prices

			prices $p_i$			
			100	100	100	100
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	120		90	-100		
Commit 2	130			90	-100	
Commit 3	140				90	-100
Finalization: Resolved	0.00	70.00	5.00	5.00	5.00	55.00
Net profit	0.00	60.00	-5.00	-5.00	-5.00	-45.00

### Strictly decreasing prices

			prices $p_i$			
			100	90	85	50
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3
Commit 0	110	-10	-100			
Commit 1	119		81	-90		
Commit 2	127.5			76.5	-85	
Commit 3	132.5				45	-50
Finalization: Resolved	0.00	66.25	9.50	6.75	20.00	30.00
Net profit	0.00	56.25	-9.50	-6.75	-20.00	-20.00

### Mixed price behaviour

			prices $p_i$			
			100	130	130	120
	Escrow	Seller	Buyer 0	Buyer 1	Buyer 2	Buyer 3

Commit 0	110	-10	-100			
Commit 1	140		100	-130		
Commit 2	153			117	-130	
Commit 3	165				108	-120
Finalization: Resolved	0.00	74.00	8.50	6.50	11.00	65.00
Net profit	0.00	64.00	8.50	-6.50	-11.00	-55.00

## Known drawbacks

### Seller and last buyer collaboration

This is not the exploit of the protocol itself, but is listed here to be aware that it can happen and that protocol cannot prevent it.

If the last price on the secondary market is higher than the original item price, the original seller and voucher owner can collaborate to both gain financially. They can agree on the price between original price and last price and they cancel/revoke the voucher. They then settle their transaction outside of the protocol. Resellers gain zero, the last buyer is better off since they paid less and the original seller got more for the item. The only thing that original seller gave up was royalties, but the agreed price can be high enough to compensate for it.

### Seller buyback and Revoke

If the seller wants to revoke a voucher, and the voucher is available on a secondary market, this gives the seller an opportunity to purchase it and potentially not lose the seller deposit. If the exchange is finalized in any unhappy path, intermediate buyers get back what they paid, but they don't realize any profits. The remainder in escrow (seller deposit + last price on secondary market) is then split between the seller and the last buyer, which is the seller in this case. So it doesn't matter which action the seller takes (revoke, cancel, mutual resolution), they always get the total pot back. Different actions only technically affect how split is done in the protocol, but at the end total pot comes to the seller.

*Viability:*

This is viable as soon as costs of doing this are lower than loss in case of revocation.

- Revocation loss: seller deposit + give up royalties
- Buyback: give up royalties + capital costs

Since both cases are unhappy paths, no protocol or marketplace fees are charged, so they don't affect it. Capital costs in buyback are costs associated with having enough capital to even purchase voucher back. If the seller has enough funds to buy it back, then these costs are zero (neglecting tx fee). If they don't they need to borrow it, so the costs are interest paid (can be very efficient with a flash loan).

So as soon as the seller's deposit is greater than buyback capital costs, the seller is incentivized to do buyback instead of revocation.

*Is this problematic?*

Although it may look like an attack at first, this is actually a completely valid scenario. First note that it can happen only if the voucher is listed on the secondary market. If it's not, the seller's only option is to revoke (or simply not deliver and a dispute is raised) and they lose their seller deposit. On the other hand, if the current voucher owner lists the item on the secondary market, they always expose themselves to the risk that at some point the voucher will be revoked and they will not realise any profit from secondary sale. In this case the seller just optimises the business by buying the voucher back instead of revoking it.