The Real World Transport Protocol

Evan Conrad

April 2022

1 Introduction

The Real World Transport Protocol (RWTP) defines a way for two parties, who may not trust each other, to securely exchange physical goods via a decentralized ledger, such as a blockchain. Let the first party be *Seller*, and the second party be *Buyer*.

To create a sell order, the *Seller* generates a new public-private key-pair (*Item*) to represent the item they are seller. Then, the *Seller* transfers some amount of a *Currency*[1] into an escrow ($Stake_{seller}$), to be used as collateral. A potential *Buyer* submits a request to purchase by transferring the payment into an escrow (referred to as the *Payment*) and additionally transfers funds into another escrow ($Stake_{buyer}$). The *Buyer* also includes the public key $Buyer_{pu}$ of their own public-private keypair. If the *Seller* accepts the purchase request, then no other potential *Buyer* can make a request and neither the *Seller* or *Buyer* can, at this point, withdraw from the escrows.

To deliver the item, the *Seller* generates a public-key pair to represent the *Item*. They encrypt the *Item* private key with the public key of the buyer to create a ShippingKey.

$$ShippingKey = Encrypt_{Buyer_{pu}}(Item_{pk}) \tag{1}$$

Because the *ShippingKey* is encrypted, it can be added to the package publicly such as on a QR-code or an NFC-capable device. When the *Buyer* receives the package, they decrypt the *ShippingKey* with their own private keypair, to get the Item's private key ($Item_{pk}$). Finally, they sign a message with the $Item_{pk}$ and publish it to the immutable ledger. At this point, the *Payment* moves to the *Seller*, the $Stake_{buyer}$ is returned to the buyer, and the $Stake_{seller}$ is returned to the seller. However, if after some time period[2], the $Item_{pk}$ have not signed a message, the *Currency* in both party's escrow is permanently destroyed.

[1] For example, Ether, DAI, USDC, SOL

[2] Or, perhaps use-defined rules

2 Game Theory

Let S_{yes} be the outcome where the *Seller* delivers the item and S_{no} be the outcome where the *Seller* does not to deliver the item. Let B_{yes} be the outcome where the *Buyer* signs that they received the item. Let B_{no} be the outcome where the buyer signs that they did not receive the item. Let I be the market value of the item at the point of exchange. Let P be the payment for the item. Because an exchange has occurred, we assume that the value of the item and the payment are equal.[3]

We can then define a pay-off matrix that shows the results of different outcomes

	S_{yes}	S_{no}
B_{yes}	$(0, 0)$	$(-Stake_{buyer}, -Stake_{seller} + P)$
B_{no}	$(-Stake_{buyer} + I, -Stake_{seller}))$	$(-Stake_{buyer}, -Stake_{seller})$

(2)

B_{yes} and S_{yes} is the saddle point for the *Buyer* if the following applies.

$$Stake_{buyer} > I \tag{3}$$

B_{yes} and S_{yes} is the saddle point for the *Seller* if the following applies.

$$Stake_{seller} > P \tag{4}$$

In a finite game, RWTP works if both parties over-collateralized. However, most real-world trade is not a finite game. Therefore both buyers and sellers may be able to reduce the stake required depending on their level of trust after repeated purchases.

If the *Buyer* and *Seller* have perfect trust in each other, then the stake for both sides can be 0. If the *Buyer* and *Seller* have no trust for each other, then the stake for both sides must be equal to I and P.

3 Motivation

RWTP lets you program the real world.

It allows for previously impracticable use cases of decentralized ledgers, programmatic supply chains, automated companies, decentralized futures over real-world goods, decentralized competitors to Amazon and other e-commerce sites, and potentially more.

[3] This may not necessarily be the case! For example, the price of the item may go up after purchase, but before delivery.