

University of Amsterdam

Master Thesis

Software Engineering

---

# **Facilitating Peer-to-Peer Decentralized Transport Contracts**

---

Student Name:

Dylan Bartels

Student Number:

10607072

Supervisor:

Jaap van Ginkel

Host Organization:

CargoLedger

July 1, 2018

## **Abstract**

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

# Contents

---

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Initial Study . . . . .	3
1.2	Problem Statement . . . . .	3
1.3	Related Work . . . . .	4
<b>2</b>	<b>Background</b>	<b>7</b>
2.1	Bitcoin . . . . .	7
2.2	Ricardian Contracts . . . . .	8
2.3	Decentralized Marketplace . . . . .	8
<b>3</b>	<b>Test Setup</b>	<b>9</b>
<b>4</b>	<b>Result</b>	<b>12</b>
4.1	Transparency . . . . .	12
4.2	Advantages & Disadvantages . . . . .	13
4.3	Claim . . . . .	13
<b>5</b>	<b>Evaluation</b>	<b>14</b>
5.1	Research Questions & Answers . . . . .	14
5.2	Evidence . . . . .	14
<b>6</b>	<b>Conclusion</b>	<b>15</b>
<b>7</b>	<b>Discussion</b>	<b>16</b>
<b>A</b>	<b>List of Symbols</b>	<b>17</b>
<b>B</b>	<b>Ricardian Contract</b>	<b>18</b>
<b>C</b>	<b>Bitcoin Mempool Anomaly</b>	<b>19</b>
<b>D</b>	<b>Transaction Script Byte-map</b>	<b>20</b>

# 1 Introduction

---

The gig economy is in full effect, individual actors get paid for the execution of short term contracts and centralized companies intermediate in the supply and demand of this labour. With the intermediation of these parties the companies profit of margins and deny individuals full ownership of the value of the produced labour. Recent advancements in peer-to-peer technologies and decentralized possibilities interest the academic domain if there are alternative options to shift towards decentralized solutions in the logistics domain.

## 1.1 Initial Study

Recent successful technical innovations have been due to a shift from centralization to peer-to-peer services, examples of these are Uber, Airbnb and Kickstarter. In the domain of supply chain logistics this innovation has been lacking. O. Gallay et al. [2] have proposed a peer-to-peer framework supporting interoperability between different actors in the logistics chains. This research lacks insight related to trust, network and technical implementation but establishes interest in the domain regarding implementation.

According to N. Hackius et al. [4] surveys in the logistics domain show that there is a clear demand on what blockchain technology can realistically do for the domain.

With the recent progression in the domain of trustless value transference, research towards the applicability of this in the supply chain offers relevancy. In [6] M. Klems et al. have formulated possible implementation of trustless intermediation in blockchain based decentralized service marketplaces. The research topic arises if this or other intermediation solutions can also be applied to peer-to-peer logistics marketplaces and to which degree will there be a custodian in the process due to it including transferring a physical asset.

## 1.2 Problem Statement

The problem which will be explored in this study is how to trust actors to transport a physical good without trusting centralized intermediation and reputation systems are not a necessity. Currently the transport domain operates around centralized reputation systems, whereby the companies with aggregated reputation and trust offer the service and carry responsibility for conflict resolution.

However reputation loss might not be the only incentive available to achieve transport. In chapter 4 an alternative incentive construction will be demonstrated which aims to achieve decentralization, reduction on trusting reputation systems and every actor being able to fulfill every role in transport. The setup uses trustless escrow to lock the transport actor into not behaving hostile due to possible punishment. Deviation of rational behaviour would result in loss of value to counteract the inavailability of current applied reputation loss punishment.

### 1.2.1 Research Questions

We examine the proposed mechanism from the perspective of the following research question:

- How can you provide a mechanism to facilitate peer-to-peer decentralized trustless transport contracts?

To contribute to a clear view of what the mechanism provides we state the following subquestions:

- Can trustless intermediation exists without a custodian for dispute prevention and resolution?
- How decentralized is the mechanism?
- To what degree do oracles play a role in the verification of the information?
- What level of anonymity is possible?
- Which attack vectors are possible to undermine this mechanism?

### **1.2.2 Solution Outline**

Our solution uses a digital representation of the transport contract which includes the begin address, end address and the end address public key. This contracts will be called the asset and ownership on this contract will be tied to the owner of the physical asset which is intended to be transported with the process. When the transport actor is custodian of transporting the asset an equivalent value or more will be put in escrow which can be unlocked by the endpoint actor. The setup incentivezes for the transport actor to move the asset to the endpoint else losing the escrow equivalent value.

We chose to implement the escrow on the Bitcoin network due to it being well tested and offering a baseline environment in the decentralized domain.

### **1.2.3 Research Method**

The study will apply the action research methodology research method. Action research can be defined as an approach in which the action researcher and a client collaborate in the diagnosis of the problem and in the development of a solution based on the diagnosis. With this method a prototype of the marketplace and transport intermediation solution will be build in collaboration with Cargoledger. The methodology has the downside that biases might occur towards the chosen solution due to also being responsible for the development.

## **1.3 Related Work**

### **1.3.1 Building Trust in Decentralized Peer-to-Peer Electronic Communities [11]**

**Summary:** Many players in electronic markets have to cope with much higher amount of uncertainty as to quality and reliability of the products they buy and the information they obtain from other peers in the respective online business communities. One way to address this uncertainty problem is to use information such as feedbacks about past experiences to help making recommendation and judgment on product quality and information reliability. This paper presents PeerTrust, a simple yet effective reputation-based

trust mechanism for quantifying and comparing the trustworthiness of peers in a decentralized peer-to-peer electronic marketplace. There are three main contributions in this paper. First, we argue that the trust models based solely on feedbacks from other peers in the community is inaccurate and ineffective. We introduce three basic trust parameters in computing trust within an electronic community. In addition to feedbacks in terms of amount of satisfaction, we incorporate the feedback context such as the total number of transactions and the credibility of the feedback sources into the PeerTrust model for evaluating the trustworthiness of peers. Second, we develop a basic trust metric that combines the three critical parameters to compare and quantify the trustworthiness of peers. Third, we present a concrete method to validate the proposed trust model and report the set of initial experiments, showing the feasibility, costs, and benefits of our approach.

**Differ from my approach:** Xiong & Liu, 2003 focus on the wide domain of trust in decentralized peer-to-peer communities. With my specific case regarding a marketplace with transport of goods trust between the peers is an important aspect but is more contained in a specific domain than Xiong & Liu.

**Obtained result:** Xiong & Liu, 2003 present PeerTrust a trust mechanism for building trust in peer-to-peer electronic communities. They identified three important trust parameters, these are: amount of satisfaction, number of interactions and balance factor of trust. They put the results into experiments which demonstrated the effectiveness, costs, and benefits of the approach.

**Remaining open questions:** Looking at ways to make the approach more robust against malicious behaviors, such as collusions among peers. Combining trust management with intrusion detection to address concerns of sudden and malicious attacks. How to uniquely identify peers over time and associate their histories with them

### 1.3.2 The challenge of decentralized marketplaces [10]

**Summary:** Online trust systems are playing an important role in to-days world and face various challenges in building them. Billions of dollars of products and services are traded through electronic commerce, files are shared among large peer-to-peer networks and smart contracts can potentially replace paper contracts with digital contracts. These systems rely on trust mechanisms in peer-to-peer networks like reputation systems or a trustless public ledger. In most cases, reputation systems are build to determine the trustworthiness of users and to provide incentives for users to make a fair contribution to the peer-to-peer network. The main challenges are how to set up a good trust system, how to deal with security issues and how to deal with strategic users trying to cheat on the system. The Sybil attack, the most important attack on reputation systems is discussed. At last match making in two sided markets and the strategy proofness of these markets are discussed.

**Differ from my approach:** Very similar by giving a rundown of all the research done towards trust enforcements in p2p file sharing, decentralized markets and sybil attacks.

**Obtained result:** B van Ijzendoorn gives a summary of academical research on decentralization, Sybil attacks, trust and peer-to-peer in relation to marketplaces.

**Remaining open questions:** Not applied.

### 1.3.3 A Peer-To-Peer Platform for Decentralized Logistics [2]

**Summary:** We introduce a novel platform for decentralized logistics, the aim of which is to magnify and accelerate the impact offered by the integration of the most recent advances in Information and Communication Technologies (ICTs) to multi-modal freight operations. The essence of our peer-to-peer (P2P) framework distributes the management of the logistics operations to the multiple actors according to their available computational resources. As a result, this new approach prevents the dominant players from capturing the market, ensures equal opportunities for different size actors, and avoids vendor lock-in. The latest ICTs such as Industrial Data Space (IDS), Blockchain, and Internet-of-Things (IoT) are used as basic building blocks which, together, enable the creation of a trusted and integrated platform to manage logistics operations in a fully decentralized way. While IDS technology allows for secured data exchange between the different parties in the logistics chain, Blockchain technology handles transaction history and agreements between parties in a decentralized way. IoT enables the gathering of real-time data over the logistics network, which can be securely exchanged between the different parties and used for managing the decision-making related to the control of the freight transportation activities. The practicability and the potential of the proposed platform is demonstrated with two use cases, involving various actors in the logistics chains.

**Differ from my approach:** It is an academic research which originated from the logistics domain and aimed at solving the contradiction between interoperability and data sovereignty.

**Obtained result:** High level decentralized logistics system architecture with data flows. Two initial use cases.

**Remaining open questions:** Development of business models in parallel.

## 2 Background

---

### 2.1 Bitcoin

Introduced by the anonymous Satoshi Nakamoto in 2008, Bitcoin (BTC) is a decentralized peer-to-peer currency system. Bitcoin allows digital payments without going through a financial institution and solves the double spend problem by hashing timestamped transactions into an continues chain of hash-based Proof-of-Work (PoW) [7]. Payment are possible by creating transactions, signing them and sending them to Bitcoin addresses. The user has a public/private keypair whereby addresses are a mapping function of the public key and the private key can sign transactions. Creating of transactions is only possible if they have been send to one of the user owned addresses and are then called unspent transactions (UTXO).

The broadcasted transactions are send to the mempool and included in blocks once the network has formed consensus on the correct order of transactions. To generate a block the miners have to find a nonce value, peers than include it in a block which allows anybody to verify the PoW. Miners get rewarded upon generating a block thus incentivizing to support the network with computational power. The generated computational power of the network, also expressed in hash rate or hash power, protects the integrity of the PoW chain. For a user the definition of owning a bitcoin is the right to sign a UTXO with your keypair.

The PoW mechanism solves the double spend problem by guaranteeing that the transaction is not spend twice when it is included in a block. For a malicious actor to double spend a BTC without detection they would have to recompute all previous blocks, so as long as the honest peers in the network exceed the malicious the integrity of the work is guaranteed [7].

The average block time of the bitcoin network is 10 minutes, to guarantee that the double spend would not occur on average the receiver of the transaction would have to wait 10 minutes minus the time of last found block. Fast transactions (i.e. in the order of seconds) are not reliable because low cost attacks can be mounted effectively to spoof a transaction [5].

#### 2.1.1 Trustless

Markus Klems et al. define trustless and trustless intermediation as follows:

*A system property which guarantees rules of interaction that are known to and agree upon by all participants of the system, and which cannot be unilaterally changed. These guarantees are enforced through, what we call trustless intermediation, a set of mechanisms for decentralizing the enforcement of rules in a system, thereby removing the need for and existence of trusted intermediaries. [6]*

Bitcoin can be defined as a trustless system because once an UTXO is signed and broadcasted to the mempool with a high enough transaction fee it is guaranteed that it will be put inside a block. No intermediation takes place for this mechanism to occur. The mechanism cannot be changed easily, only if a hard forking is proposed including a code change. However this chain split would not count as bitcoin unless it is backed by the majority of hash rate thus being classified as longest chain [7].



Extrapolating the definition to the logistics domain means that trustless logistics can be defined as an logistic contract which has predefined unchangeable rules and no need for trusted intermediaries.

### 2.1.2 Script

Bitcoin uses a stack-based scripting system for transactions which is intentionally not Turing-complete. One possible output script is the multisignature script which allows any of  $N$  out of  $M$  signatures to spend the UTXO available in the generated multisignature address. To create a multisignature address  $M$  amount of public keys need and the required amount of signatures  $N$  to allow to send from the address need to be given. Multisignature addresses will be denoted as  $MSig_{PubK_x, PubK_y, \dots}^{n/m}$  from now on. Bitcoin provides the OP\_CHECKMULTISIG operators for multisig verification which make it possible to verify a generated transaction script for the content before it is broadcasted.

## 2.2 Ricardian Contracts

A Ricardian contract is designed to register a legally binding digital document to a specific object [3]. The contract puts all information in a format which is parsable by software and humans. It represents a legal agreement between individuals and a protocol for integrating the agreement securely within a infrastructure.

The Ricardian contract can be used to form an agreement by forming the liability when trading with another party. It can represent a unit of goods or service and uses signed agreement between the parties which cannot be falsified once signed.

Just as smart contracts [?] they can achieve taking out of the middle man in contract construction, execution and enforcement. A Ricardian contract is acceptable withing the existing legislation frameworks.

## 2.3 Decentralized Marketplace

Markus Klems et al. define centralized marketplaces[6] as providing mechanisms to facilitate efficient spot trades between numbers of sellers and buyers by providing match-making and payment transaction processes that are accompanied by trust-building mechanisms, most importantly, reputation and dispute resolution systems. Some examples of centralized marketplaces for logistics are Postmates for deliveries, Uber for the transport of people and Uship for shipping of goods. These peer-to-peer marketplaces facilitate the intermediation process of transport contracts.

Decentralized marketplaces facilitate the same spot trades without a central provider and intermediaries. The upside of such a mechanism is the lowering of the entry barrier [1], no intermediation fees [12], increasing sensorship resistance [8], and improving privacy [9].

### 3 Test Setup

As a new idea, this study introduces the concept of trustless transport which replaces the need of centralized intermediation of supply and demand. We propose a mechanism which punishes hostile actors automatically resulting in no conflict resolution required from central entities. The meaning of used abbreviations in this chapter can be found in the list of symbols appendix A.

In our scenario seen at figure 3.1, we assume that the service consumer  $A$  wants to send an physical asset to the endpoint actor  $B$ . The third and last actor is the service provider  $C$  who will execute the transport contract. Let  $A$ ,  $B$  and  $C$  all have an ECDSA key pair and Bitcoin address.

$$\text{GenerateAddress}(\text{PubK}_n): \text{Adr}_n$$

The scenario starts of with  $A$  creating a Ricardian contract representing a request for transport, this contract minimally contains  $B$  public key,  $B$  location,  $A$  location, physical asset equivalent cost and the transport reward.

$$Rc \supseteq \{\text{PubK}_b, \text{Loc}_b, \text{Loc}_a, \text{EqC}, \text{Tr}\}$$

This contract is accepted by  $C$  which then signs an unspent transaction from  $\text{Adr}_c$ , denoted by  $tx_1$ , containing the physical asset equivalent cost or more to the 2/2 multisignature address of the service provider and endpoint actor

$$\text{SignTransaction}(\text{PrivK}_c): \{\text{EqC}, \text{Adr}_C, \text{MSig}_{bc}\} \mapsto tx_1$$

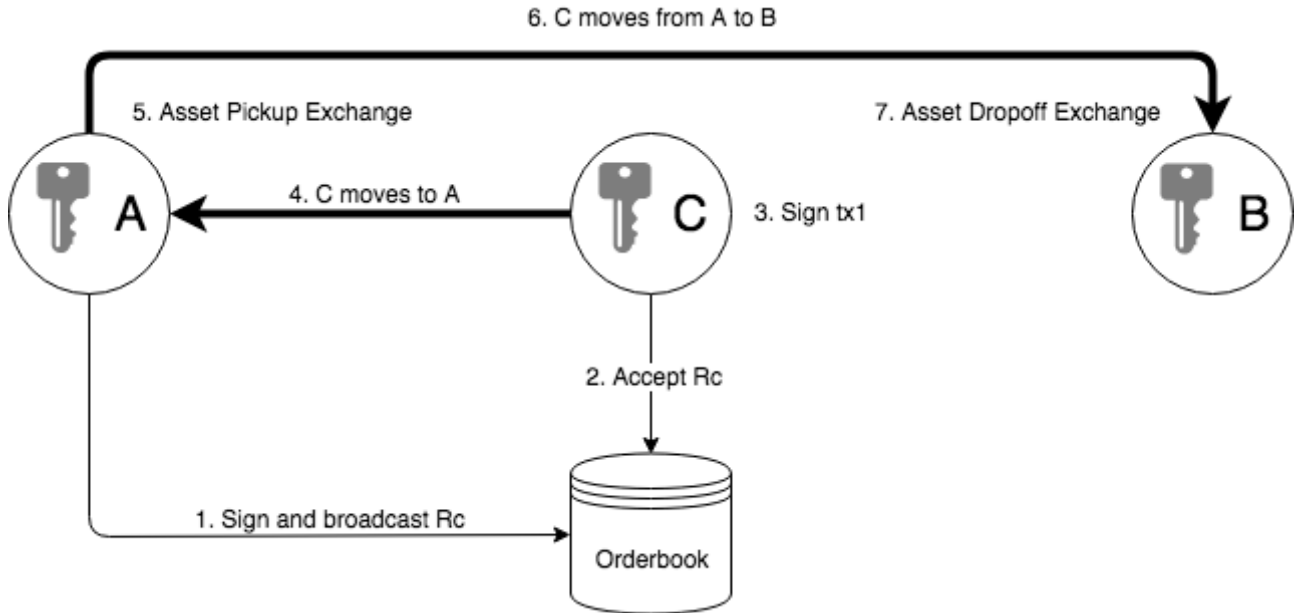


Figure 3.1: Overview test scenario

Upon accepting  $C$  moves to the physical location of  $A$  bringing transaction script  $tx_1$ . As illustrated with figure 3.2, upon  $C$  arriving at  $A$  the asset pickup exchange can take place.

1.  $C$  initiates the exchange by giving  $A$  the transaction script  $tx_1$
2.  $A$  signs a unspent transaction from  $Adr_a$  to the multisignature address containing the reward for transporting the physical asset.

$$SignTransaction(PrivK_a): \{Tr, Adr_a, MSig_{bc}\} \mapsto tx_2$$

3.  $A$  broadcasts the transport incentive into escrow  $\{tx_1, tx_2\}$
4.  $A$  signs and broadcasts the ownership change of the  $Rc$  from  $A \rightarrow C$
5. Wait block confirmation containing  $\{tx_1, tx_2\}$
6. Exchange the physical asset from  $A \rightarrow C$

Before  $\{tx_1, tx_2\}$  get broadcasted  $A \vee C$  can individually verify if the signed transactions actually contain what they should.

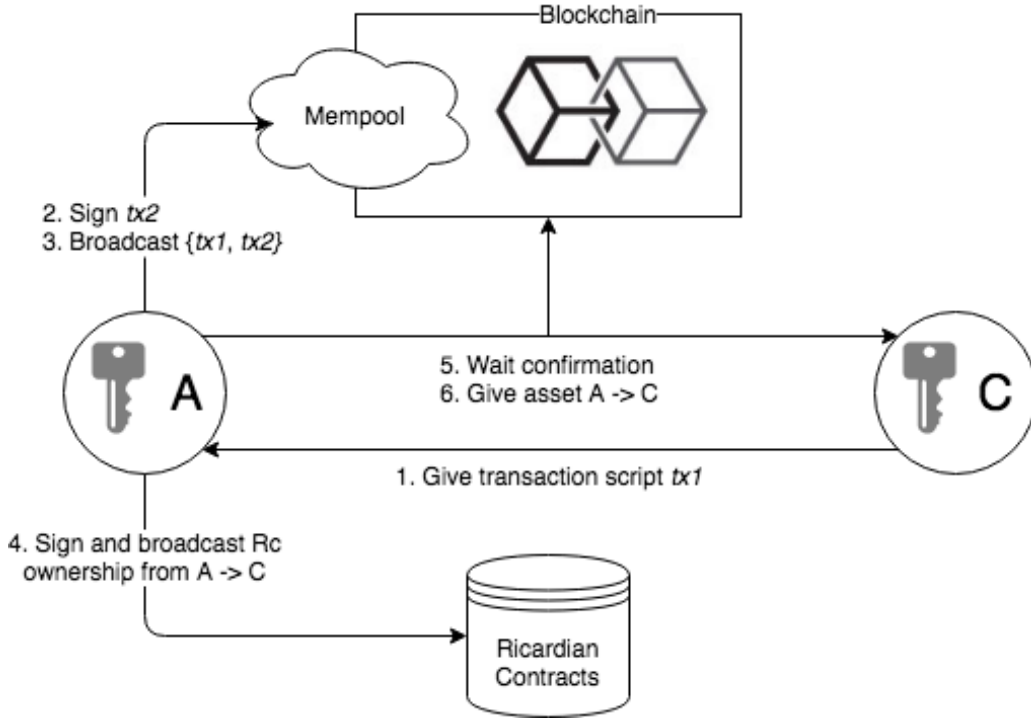


Figure 3.2: Asset Pickup Exchange

When  $C$  receives the physical asset he is the custodian and will move to the endpoint  $Loc_b$  to claim the reward locked in the escrow. As illustrated with figure 3.3, upon  $C$  arriving at  $Loc_b$  the physical asset dropoff exchange takes place which consists of the following steps:

1.  $B$  signs  $tx_3$  containing the equivalent value and transporting reward from  $MSig_{bc}$  to  $Adr_c$

$$SignTransaction(PrivK_b): \{\{tx_1, tx_2\}, MSig_{bc}, Adr_c\} \mapsto tx_3$$

2.  $B$  gives the transaction script  $tx_3$  to  $C$

3.  $C$  signs and broadcasts the ownership change of the  $Rc$  from  $C \rightarrow B$
4. Exchange physical asset from  $C \rightarrow B$

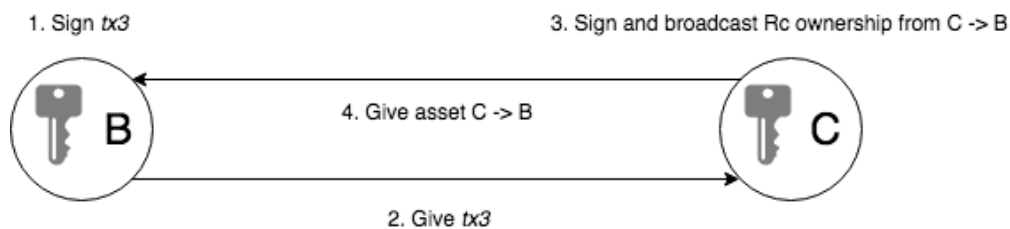


Figure 3.3: Asset Dropoff Exchange

At the end of the second exchange actor  $C$  now owns  $tx_3$  which has been signed by  $B$ . He can now sign and broadcast the transaction with his own keypair whenever he wants to redeem the funds.

## 4 Result

---

In this chapter we describe OpenLogistics, the created decentralized marketplace prototype for facilitating trustless transport contracts. OpenLogistics uses the bitcoin mainnet for the multisignature trustless intermediation mechanism, the distributed data storage bigchaindb to store legally binding liability Ricardian contracts and the software client aggregates the contracts and facilitates the interaction.

To analyze the obtained result of OpenLogistics will be divided into three parts representing the three roles which can interact with the mechanism. Every role owns a Bitcoin and BigchainDB keypair once interacting with the software client. The roles which interact with the mechanism are the following:

1. Service consumer
2. Endpoint actor
3. Service provider

The **service consumer** uses OpenLogistics because he wants to transport a physical good. He can create and sign a Ricardian contract which will then be stored on BigchainDB. This represents a request for transport, the ownership of the physical good and includes the information regarding the transport, an example of the data model can be found in appendix B.

The **service provider** can access the OpenLogistics marketplace orderbook and accept the contract in his local client. Upon accepting he creates a  $tx_1$  and travels to the location of the service consumer. Upon the **service provider** arriving at the **service consumer** the **service consumer** accesses the client and selects his own Ricardian Contract and the pickup exchange takes place illustrated in figure 3.2. The **service provider** now moves to the **endpoint actor** and the **endpoint actor** accesses the client and the dropoff exchange takes place illustrated in figure 3.3. Eventually the **service provider** ends up with  $tx_3$  and can claim the reward in his own client for his provided labor.

### 4.1 Transparency

An example of a mainnet testrun can be seen locally, if copy of blockchain is present, or through commonly used block explorers [add as footnote] with the following addresses:

1. Service consumer: 17F4ZhEJp83qqEG1S6z8YcPbWW7AdqbkZ3
2. Endpoint actor: 19exDB5Fb2gQAv7k2dH93WbLga1ZUNz9mh
3. Service provider: 1EY38FGwuSg3uRzetBwYqYh9jibX55fHsL
4. Multisig (Endpoint actor + Service provider): 3MiFyavsRpMZBzfxFk94WdeZUnbQP1hdDy

The **service provider** actually has no transaction being broadcasted from his address, this is due only using his keypair to sign the transactions. The function **service provider** actually fulfills is being the oracle for conflict resolution upon dropoff exchange by signing or not.

The asset transferring taking place can also be seen by exploring bigchaindb addresses.

The aggregation of the movement of assets between addresses can be used for a reputation system.

## 4.2 Advantages & Disadvantages

The advantage of the facilitated mechanism of OpenLogistics is that if all actors agree upon the set rules *anybody* can participate. We chose to implement the payment and escrow mechanism on the Bitcoin network, which is in the blockchain domain perceived as simpler and less vulnerable in terms of incentive structure than other networks. The downside is that the average blocktime is 10 minutes, which is not a viable period to wait when the pickup exchange is taking place. Other blockchain alternatives can be chosen depending as long as they support multisignature.

We chose to implement the OpenLogistics client with Javascript libraries which can be developed towards mobile.

Disadvantages is that you have to spend three transaction fees to make the mechanism work.

## 4.3 Claim

We claim that OpenLogistics facilitates peer-to-peer decentralized transport contracts while aiming to create trustless intermediation. Through the evaluation of the research questions in Chapter 5 we will provide evidence of our claim.

## 5 Evaluation

---

### 5.1 Research Questions & Answers

In Chapter 1 we stated our research questions and so far we answered them considering the motivating prototype. Generally, we answered the research questions as follows:

**How can you provide a mechanism to facilitate peer-to-peer decentralized trustless transport contracts?** From our research we conclude that to facilitate this mechanism a Bitcoin multisignature escrow incentive structure can incentivize the transportation without relying on trusted intermediaries.

**Can trustless intermediation exist on this marketplace without a custodian for dispute prevention and resolution?** Trustless intermediation cannot take place with the transport of physical goods. During the process of transport a person will *always* be custodian of the physical good.

**How decentralized is the mechanism?** We claim that the mechanism is as decentralized as the two networks it is built upon.

**To what degree do oracles play a role in the verification of the information?** The verification of information by an oracle takes place twice during the mechanism. The first time by the service provider when he verifies that the physical asset is similar to the stated Ricardian Contract when it is being picked up. The second time by the endpoint actor when he verifies that the physical asset being delivered is correct.

**What level of anonymity is possible?** We claim that the starting point and endpoint of the transport identity will always be known. However the transport actor can maintain privacy in this mechanism, the only aspect of privacy he will have to turn in is the sight of his physical appearance to the service consumer and endpoint actor.

**Which attack vectors are possible to undermine this mechanism?** The mechanism uses the PoW solution twice to counteract the double spending possibilities of the escrow and the Ricardian contract proof of ownership. We claim that if the actors behave rational the incentive structure holds.

### 5.2 Evidence

To outline the proof of our incentive structure we will analyze the possible actions the actors can take during the various stages of the mechanism. Starting at the pickup exchange once the service provider has provided  $tx_1$  the service consumer can verify the content of the  $tx_1$ , an example of a transaction script byte-map can be found in Appendix D.

$$\{EqC, PubK_c\} \in tx_1 \wedge PrivK_c \notin tx_1$$

## 6 Conclusion

---

Attack vectors: Eating the difference in equivalence cost if the reputation cost of the starting actor is beneficial to the actor eating the costs blockchain is the right to sign a UTXO, the right is valued due to being censorship resistant. The capacity to make it censorship resistant cost a lot of energy. From an economic perspective centralization is very efficient due to not needing to form consensus which cost a lot of energy. Traditional reputation systems in place form all the “aanspraakelijkheid” the smart logistics contract resembles. They do this quite well, if bad events occur when tnt post is custodian of your asset than resolution is often very dynamic. This would be hard to capture in similair smart contract construction as OpenLogistics[1]. Conflict resolution is currently a loss for all parties when a package is lost, these kind of conflict could beter be immediated by current traditional logistics caretakers. It’s only economically viable to spend such an amount of energy to defeat the possible censorship that it becomes viable. Zero confirmation: Zero confirmations are currently not safe to be used in production setups, the attacker could easily write a script broadcasting the same UTXO moments later. This double spend attack will remain harmfull in the current testsetup. Solutions are available, bitcoincash[cite safe accept 0-conf] accepting zero-conf safely, microsoft currently accepts this payment since declining to accept bitcoin for the mentioned reason. Since bitcoincash is a fork of bitcoin the testsetup could easily be alternated to work on this network. Another possiblity to counteract the double spend attack would be to use the bitcoin lightning network which is a second layer solution which enables instant transactions. Given that blockchain mainchain does not scale and remain decentralized this alternative would provide more promise. RBF (replace-by-fee): no rbf: 51 attack or Finney attack(<https://bitcoin.stackexchange.com/questions/4942/what-is-a-finney-attack>) A network like ethereum has a average block time of 15 seconds and with a is quite safe after 8 confirmations.

The bitcoin protocol does not provide any guarantee at all about zero-conf transactions. It provides probabilistic guarantees for n-conf transactions, but only when n is 1 or more. Specifically, as Satoshi proved, the probability of an n-conf transaction being reversed and double-spent decays very quickly with n, so that for  $n = 6$  it can be considered impossible.

Attempts to get zero-conf payments to work, e.g. by inspecting the mempools of volunteer relay nodes, are attempts to solve the double-spending problem without the blockchain, the miners, and proof-of-work. People tried to do that for 25 years with no success.

You can get a solution for the 0-conf double-spend problem that “works” only in the hacker’s sense of the word, not in the engineer’s sense. That level of security is OK for bittorrent or Tor – but not for a payment system.

The only change that would actually improve bitcoin’s dismal usability (and make it competitive with other altcoins) is a reduction of the block interval from 10 minutes to under a minute. Then it would still be too slow to compete with credit and debit cards for walk-in stores and restaurants, but may be good enough for e-commerce.

By the way, the payment channels that are supposed to be the building block of the Lightning Network use zero-conf transactions that are kept on file for months before being sent to the miners. Thus payment channels too are secure only in the hackers’ sense of the term – that is, not really secure.



## 7 Discussion

---

blockchain is nothing other than the right to sign a UTXO, need to depend on oracles to verify the data which it represents.

## A List of Symbols

---

---

$A$	Actor $A$
$\{PubK_a, PrivK_a\}$	EDSCA keypair containing private and public key owned by actor $A$
$Adr_a$	Bitcoin address owned by $A$
$MSig_{ab}^{n/m}$	Multisignature address with $n$ signatures signed out of $m$ signatures needed, can be signed by private key of $A \vee B$
$Loc_a$	Physical location of $A$
$tx_1$	Transaction script number 1
$A \rightarrow B$	Exchange physical asset from $A$ to $B$
$Rc$	Ricardian Contract
$EqC$	Equivalent cost of the physical asset
$Tr$	Reward for transporting the physical asset
$GenerateAddress(PubK_n): Adr_n$	Generating a bitcoin address with script language mapping function
$SignTransaction(PrivK_y): \{x, y, z\} \mapsto tx_i$	Signing a unspent transaction $x$ , from bitcoin address $y$ to bitcoin address $z$ and resulting in transaction script $tx_i$

## B Ricardian Contract

---

```
1 {
2   "type": "OpenLogisticsBeta",
3   "created_on": "2018-06-19T10:10:13.627Z",
4   "value_category": "50",
5   "pickup": {
6     "name": "John Doe",
7     "address": "Kinkerstraat 236",
8     "postal": "7634YX",
9     "city": "Amsterdam",
10    "country": "Netherlands",
11    "date_day": "2018-06-21",
12    "date_time": "10:09:23",
13    "public_key": "03e1b9f8f7114ffb05ee6a006479230fa2d7635e32f8655728cbc29
    a77ccdbbfe0"
14  },
15  "dropoff": {
16    "name": "Harry de Vries",
17    "address": "Amstelstraat 12",
18    "postal": "9283JS",
19    "city": "Amsterdam",
20    "country": "Netherlands",
21    "date_day": "2018-06-22",
22    "date_time": "11:09:23",
23    "public_key": "02d7cef6f0c3109cef11c2bb3304dcb0d453551233ad5873abe9e29
    2a0f9eff226"
24  }
25 }
```

## C Bitcoin Mempool Anomaly

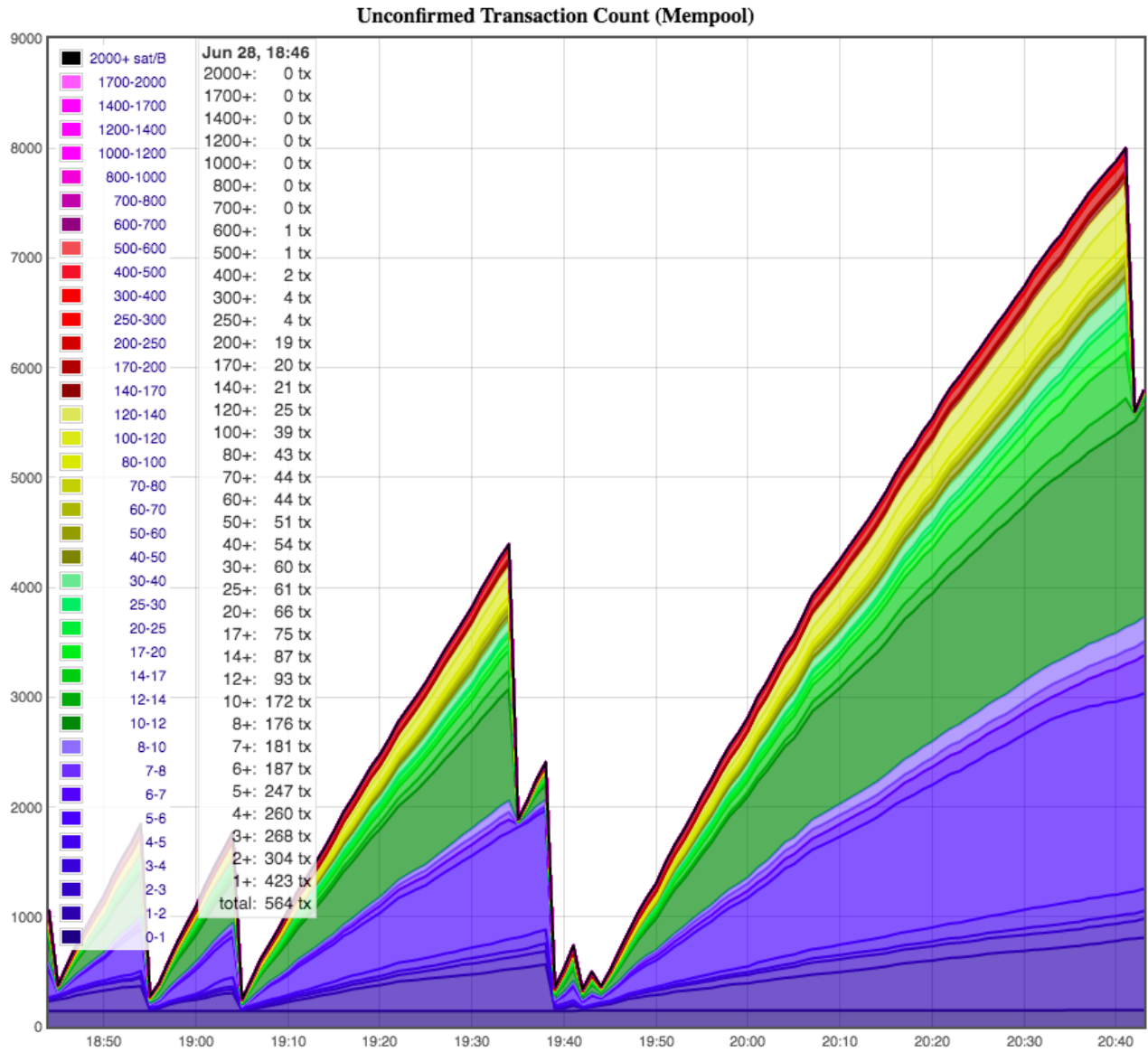
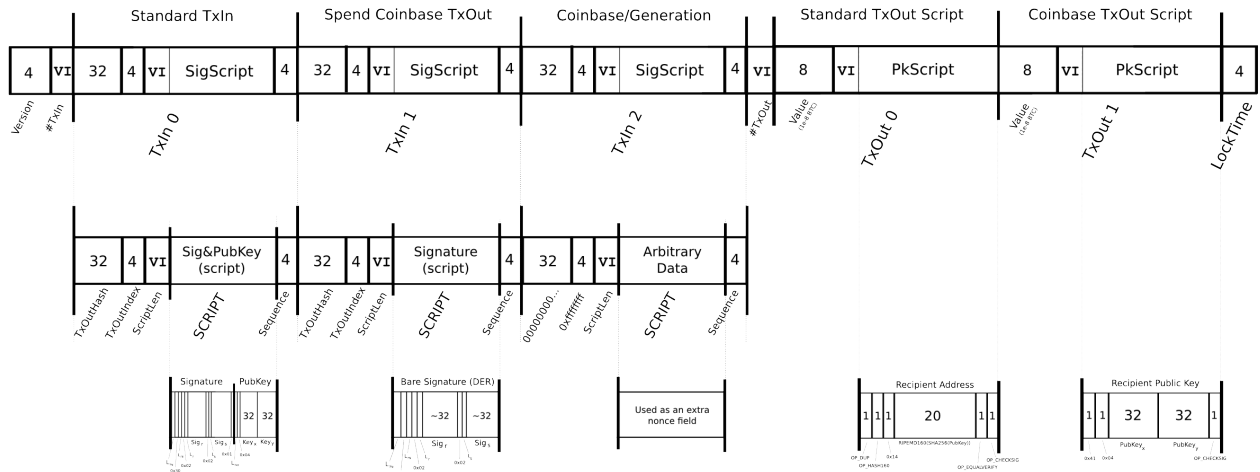


Figure C.1: Block confirmation far exceeding average of 10-minutes

# D Transaction Script Byte-map

## Transaction



Scripts and DER encoding both use big-endian values, all other serializations use little-endian

etotheipi@gmail.com / 1Gffm7LKXcNFPrty6yF4JBoe5rVka4sn1

Figure D.1: Bitcoin transaction byte-map

## References

---

- [1] Liran Einav, Chiara Farronato, and Jonathan Levin. Peer-to-peer markets. *Annual Review of Economics*, 8:615–635, 2016.
- [2] Olivier Gallay, Kari Korpela, Niemi Tapio, and Jukka K. Nurminen. A peer-to-peer platform for decentralized logistics. In *Digitalization in Supply Chain Management and Logistics*, oct 2017. <http://tubdok.tub.tuhh.de/handle/11420/1476>; Proceedings of the Hamburg International Conference of Logistics (HICL).
- [3] Ian Grigg. The ricardian contract. In *Electronic Contracting, 2004. Proceedings. First IEEE International Workshop on*, pages 25–31. IEEE, 2004.
- [4] Niels Hackius and Moritz Petersen. Blockchain in logistics and supply chain: trick or treat? In *Proceedings of the Hamburg International Conference of Logistics (HICL)*, pages 3–18. epubli, 2017.
- [5] Ghassan Karame, Elli Androulaki, and Srdjan Capkun. Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin. *IACR Cryptology ePrint Archive*, 2012(248), 2012.
- [6] Markus Klems, Jacob Eberhardt, Stefan Tai, Steffen Härtlein, Simon Buchholz, and Ahmed Tidjani. *Trustless Intermediation in Blockchain-Based Decentralized Service Marketplaces*, pages 731–739. Springer International Publishing, Cham, 2017.
- [7] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
- [8] J. Winter M.J.G. Olsthoorn. Decentral market: self-regulating electronic market. *DelftUniversity of Technology*, 2016.
- [9] Kyle Soska, Albert Kwon, Nicolas Christin, and Srinivas Devadas. Beaver: A decentralized anonymous marketplace with secure reputation. *IACR Cryptology ePrint Archive*, 2016:464, 2016.
- [10] Bas van IJzendoorn. The challenge of decentralized marketplaces. *CoRR*, abs/1703.05713, 2017.
- [11] Li Xiong and Ling Liu. Building trust in decentralized peer-to-peer electronic communities. In *In The 5th International Conference on Electronic Commerce Research. (ICECR, 2002*.
- [12] Dionysis S. Zindros. Trust in decentralized anonymous marketplaces, 2015.