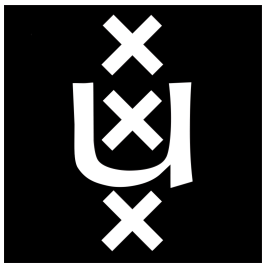

University of Amsterdam

Master Thesis

Software Engineering

A Realistic Approach to Trustless Asset Transport

Student Name:	Dylan Bartels
Student Number:	10607072
Supervisor:	Jaap van Ginkel
Host Organization:	CargoLedger

June 24, 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

1 Introduction

The gig economy is in full effect, individual actors get payed 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 posibilities interrest 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. [**?**] 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. [**?**] 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 [**?**] 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 a physical process.

1.2 Problem Statement

The problem which will be explored in this study is the possiblity of creating a trustless transport system where reputation is not a neccesity. 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 fullfill 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 inavalibility of current applied reputation loss punishment.

1.2.1 Research Questions

Main research question:

- What are the specific problems and characteristics of a trustless decentralized peer-to-peer marketplace for transportation contracts?

Subquestions:

For the following subquestions marketplace is defined as a trustless decentralized peer-to-peer marketplace for transportation of goods.

- Can trustless intermediation exists on this marketplace without a custodian for dispute prevention and resolution?
- What level of anonymity is possible on this marketplace?

1.2.2 Solution Outline

None specific cryptocurrency for escrow marketplace orderbook orders consist out of transport coordinates and asset being transported. Ownership of this translate to ownership in the physical domain. todo: figure

1.2.3 Why Blockchain?

Paper why blockchain cencorship resistance immutability ownership transparency downside upside

1.2.4 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

2 Background

2.1 Blockchain

Different definitions depending on the interpreter. Can be a ethics framework, speculative asset or a distributinon of rights to spend an unspend transaction (UTXO). There are no wrong answers. Blockchain is the right to sign a UTXO (unspent transaction) with your keypair.

2.1.1 Decentralized

Centralization is very efficient compared to decentralization. The forming of consensus requers high amount of value by putting energy in computation with the proof of work algorithm, going back to the byzantine fault tolerance trusting other parties to comform to the input of information will be more costly. The function decentralization fulfills is raising the cost of attacking the consensus which is being formed every input stream of information captured in blocks. The sensorship resistance of decentralization is the function it excels at.

Following this premises in the domain of logistics centralizated entities fulfill trustworthy responsibllities which cannot compete with decentralized services. This is unless this service wants to benefit the cencorship resistance which could be made possible. Censoring is not often applied in logistics, some examples along many are:

1. Transportation of written religious information in corresponding religion underpressed areas
2. Transportation of illicit goods
3. Entry level of competition

The other option which logistics could benefit in the model of trade-offs is: The costs of the controlling the goods to be transported and transporting being more constly than actually transporting the goods without intermediation of checking on the parameters of censorship.

2.1.2 Trustless

The definiton of trustless can be achieved if no entity is custodian of any process. In the domain of logistics a custodian will always be responsible for the actual transport of the physical good. This means that

2.1.3 Multisigniture

2.2 Smart Contracts

Smart contracts are digital representations of a contracts which will be activated once certain input activates parameters. The contracts promise to: enforce contracts automatically Take out the middle man in contract construction, execution and enforcement A normal contract smart contracts are very difficult to implement well. They all trust on some oracle input which has to be correct for contracts to behave. but how can you garantee the input is correct? Conesnsus on the correctness of data which is stored depends on the correctness of input. If the oracles who register the data are in full control of input they are lone ruler of correctness disregarding the consensus.

2.3 Marketplace

In the domain of logistical contracts for being the custodian for transport settled identities work on reputation based systems to create trust for transport. If decentralized trustless aggregation of contracts could take place in a orderbook everybody should be able to fulfill the same side of this marketplace, supply and demand. The marketplace is a orderbook filled with digital representations of transport contracts. The contracts are demand of transport from place A to B, the supply is facilitators of this transport. Once the order is met and work has to be facilitated the supply picks up the asset and brings it to designated place of dropoff. The three actors: pickup, drop-off and transport are represented by a keypair which gives the right of ownership throughtout the process of the asset. This ownership is the right to the transport contract and asset being transported, the data it contains is the pickup and dropoff point.

3 Test Setup

As a new idea, this study introduces the concept of trustless transport which replaces the need of central intermediation of supply and demand. We propose a mechanism which punishes hostile actors automatically resulting in no conflict resolution required from central entities.

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, and that the asset payment between them already took place. Let the service provider C, A and B all have an ECDSA key pair $\{PK, SK\}$.

The scenario starts of with A creating a request for transport minimally containing PKb, $Loc\ b$ and $Loc\ A$. This order in the orderbook is accepted by C which then signs $\{PKc, SKc\}$ a UTXO $tx1$ containing the equivalent cost of the asset or more to 2/2 multisig address of $\{PKb, PKc\}$.

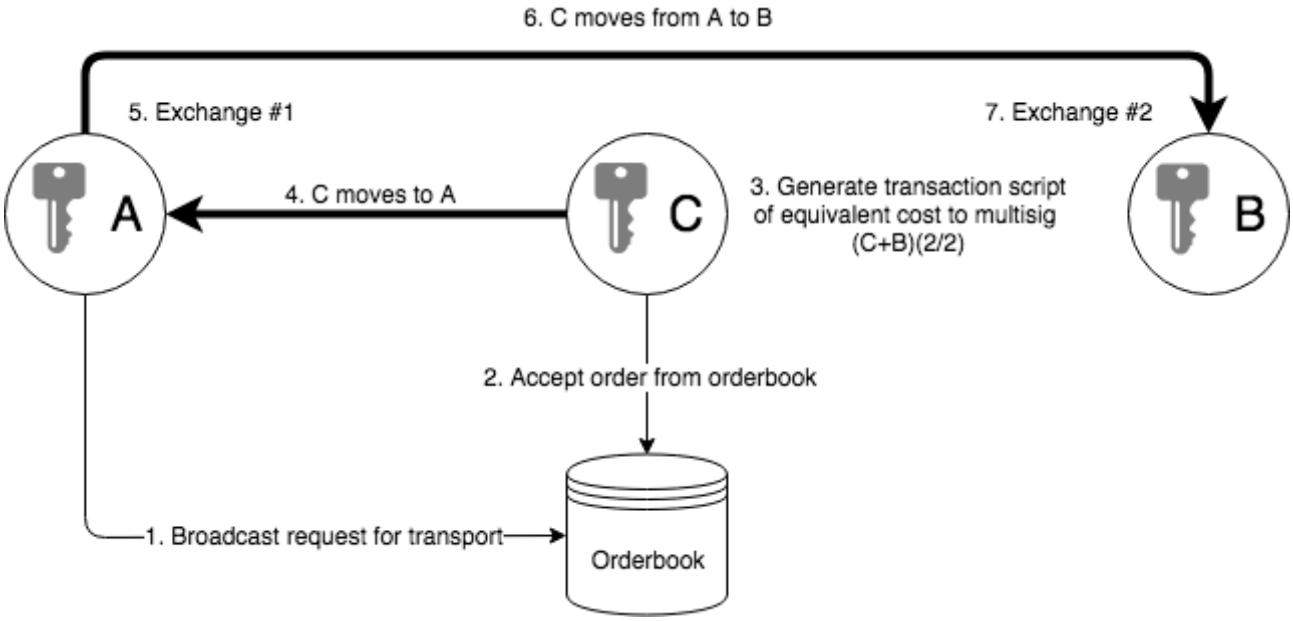

Figure 3.1: Overview test scenario

Actor C moves to the physical location of actor A bringing the signed transaction script. As illustrated with figure 3.2, upon C arriving at A the first exchange can take place.

C innitiates the exchange by giving A the transaction script of $tx1$. Upon receiving the transaction script A generates and signs $\{PKa, SKa\}$ UTXO $tx2$ containing the tansport cost of the asset to 2/2 multisig address of $\{PKb, PKc\}$. The service consumer actor A now broadcasts $tx1$, $tx2$ and digital asset ownership from A to B. Before $tx1$ and $tx2$ get broadcasted A and C can individually verify if the signed transactions actually contain what they should. After waiting the appropiate confirmations the physical asset gets exchanged from A to B.

When C recieves the asset he is the custodian and will move the asset to the endpoint $Loc\ B$. Upon C arriving at $Loc\ B$ the second exchange takes place which consist out of the following steps:

1. B signs $\{PKb, SKb\}$ two UTXO's $\{tx1, tx2\}$ containing the (equivalent cost + tansport cost) of 2/2 multisig address of $\{PKb, PKc\}$ to address of C $\{PKc\}$ and give this to C

2. Exchange asset C to B

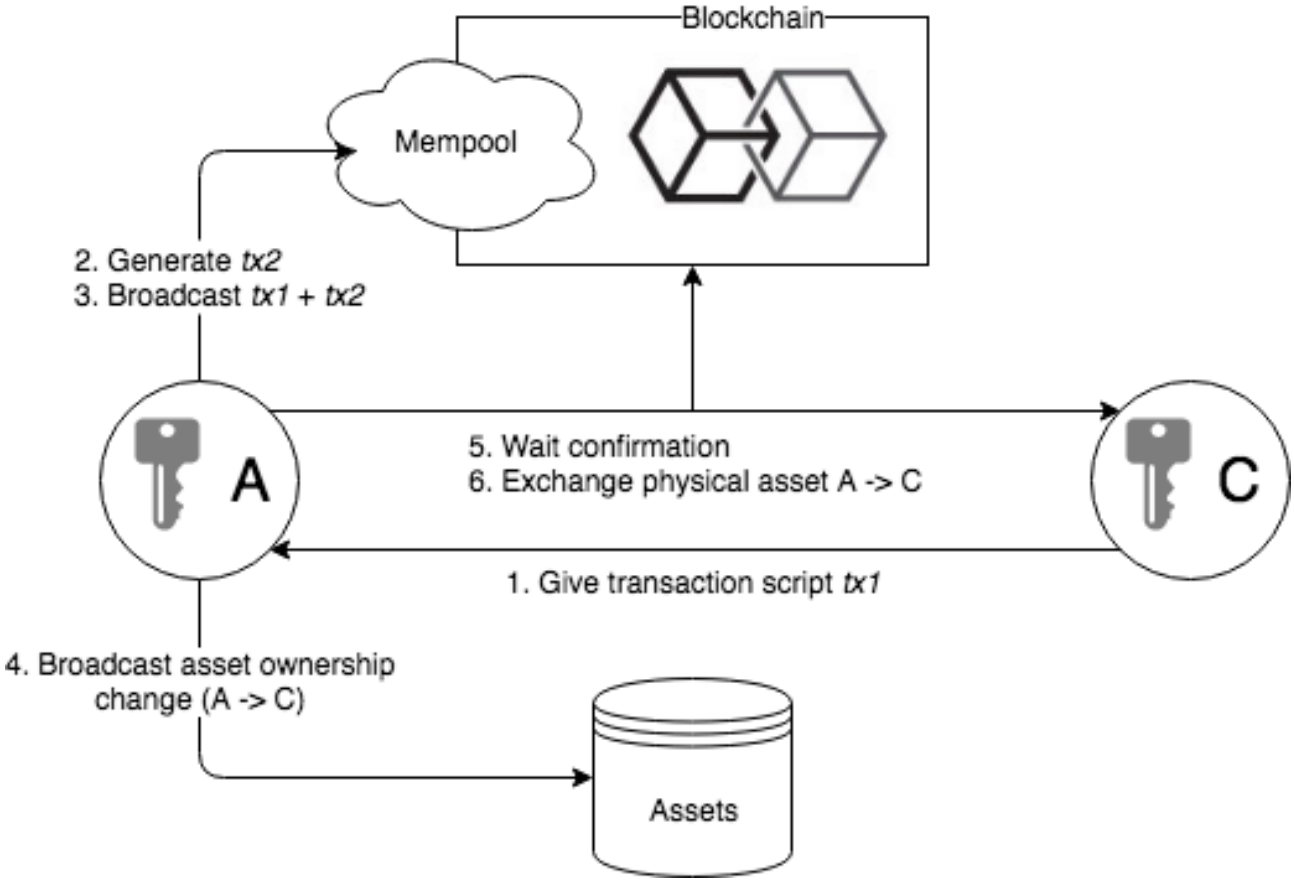

Figure 3.2: Exchange between A and C

At the end of the second exchange actor C now owns the transaction script containing the (equivalent cost + tansport cost) of 2/2 multisig address of $\{PKb,\ PKc\}$ to address of C $\{PKc\}$ and can sign 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 transport contracts. OpenLogistics uses the bitcoin mainet for the multisignature mechanism and bigchaindb to create orders and aggregate them in a orderbook.

To analyze the results the whole testsetup will be devided into different phases, at every phase the possible actor actions will be evaluated. The phases to be analyzed are the following:

1. Setup
2. Pickup
3. Dropoff
4. Redeeming

What is really being exchanged is the right to the transaction id by being possible to acces it with the private key. What the transaction id represent in the orderbook is proof that asset ownership is possible to acces. The exchange of owner innitiates the escrow balance which is equavalent to the asset value.

4.1 Transparancy

A 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. Actor A: 17F4ZhEJp83qqEG1S6z8YcPbWW7AdqbkZ3
2. Actor B: 19exDB5Fb2gQAv7k2dH93WbLga1ZUNz9mh
3. Actor C: 1EY38FGwuSg3uRzetBwYqYh9jjbX55fHsL
4. Multisig (B+C): 3MiFyavsRpMZBzfxFk94WdeZUnbQP1hdDy

Actor B actually has no UTXO on his address, this is due only using his keypair to sign the transactions. The function Actor B 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.

5 Conclusion

Attack vectors: Eating the difference in equivalance cost if the reputation cost of the starting actor is benefitial 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.

6 Discussion

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

References

[1] 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).

[2] 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.

[3] 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.