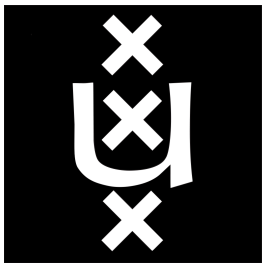

University of Amsterdam

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 20, 2018

Contents

1 Abstract

2 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.

2.1 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. [1] 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. [2] 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 [3] 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.

2.2 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.

2.2.1 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?

2.2.2 Solution Outline

None specific cryptocurrency

2.2.3 Why Blockchain?

Paper why blockchain cencorship resistance immutability ownership transparency downside upside

2.2.4 Research Method

2.3 Related Work

3 Background

3.1 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.

3.1.1 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: Transportation of written religious information in corresponding religion underpressed areas Transportation of illicit goods 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.

3.1.2 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

3.1.3 Multisigniture

3.2 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.

3.3 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.

4 Test Setup

Nomenclature A = Begin actor B = End actor C = Transport actor D = Value equvalent of transport E = Transport cost F = Multisig wallet

Assumptions: A, B, C got public/private keys

Scenario A:

1. A broadcasts request transport (A -¿ B)

2. C accepts transport

    (a) All 3 public keys are known, possible to create 3/3 F

3. C picks up physical good at A

    (a) moment of exchange:

        i. C puts value equivalent in F

        ii. A puts E in F

        iii. A gives physical good to C

        iv. A signs 1/3 F signature of outgoing (D + E) to C (total signature aggregation: 1/3)

4. C delivers physical good at B

    (a) moment of exchange:

        i. C gives physical good to B

        ii. B signs 1/3 F signature of outgoing (D + E) to C (total signature aggregation: 2/3)

5. C can redeem (D + E) whenever he want (total signature aggregation: 3/3)

Bottlenecks:

1. Relies on 0-confirmation at 3.a, if C broadcast another transaction before mined there is a chance of the other transaction being mined. Not all cryptocurrencies got this double spending behaviour. Some are reliable.

2. B losing private key after 3.a, funds will be locked.

Scenario B: A broadcasts request transport (A -¿ B) To counteract spamming A pays insertion fee C accepts transport All 3 public keys are known, possible to create 3/3 F C puts value equivalent in F C delivers physical good at B moment of exchange: C gives physical good to B B signs 1/3 F signature of outgoing (D + E) to C (total signature aggregation: 2/3) C can redeem (D + E) whenever he want (total signature aggregation: 3/3) Bottlenecks: Where does the insertion fee go

4.1 Architecture

4.2 Actor Balance

5 Result

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.

6 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.

7 Discussion

blockchain is nothing other than the right to sign a UTXO

8 Notes

Transport is the moving of goods, a digital marketplace to offer intermediation in the demand good transport and the supply of goods transport. Decentralization would have to garantue that everybody can use the same function on the marketplace, this means that any actor would have to be incentivezed to act according to the rightful outcome of the transport. The transport actor would have to be balanced to counteract hostile actions.

Todo: Actions which are possible from different multisig setups for the actors (A,B,C).

Trustless is not possible in a physical domain, Charly would always be a custodian of the value of the transport. It is possible to construct decentralized escrow of the value equivalent Charly has to be custodian for. This escrow can be in place once the exchange of value of transport takes place between Charly and Alice and released once the transport has arrived at Bob.

Blockchain decentralized p2p logistics only has purpose when no attack vector towards a central entity is possible. This is due primairy value blockchain has is being censorship resistance. In logistics the only market value p2p decentralized logistics has is cencorship resistant transport of goods, centralized solutions are always more efficient[economics centralization vs decentralization].

The technological stack which would make this possible would have to be able to offer

censorship resistant datastorage. A few examples of technologies which currently communicate being able to offer mentioned resistance are: IPFS, BigchainDB, Ethereum Swarm, Sia. IPFS Offers no incentive to run client node and store the partial datacluster Large files / media BigchainDB:

Transactions, Certificates, Contracts and Receipts Ethereum Swarm BigchainDB+Electrum+Multisignat would teoratically provide the possible incentive and security of keys combining local and BigchainDB to store public and private key. The signing of the signiture of 2/3 MS when Charly is transporting between Alice and Bob could occur offline and when Charly wants to claim ownership publish on BTC mainchain.

private key would be saved locally public key would be saved with BigchainDB

Todo: How to gather all public keys to generate multisigniture

For the technological purpose of blockchain/decentralization to exists anonymity has to exsist because else attack vectors could exsist. If all the transport coordinates of (Alice and Bob)*n would be available decentralized, centralization would probably be more efficient.

The stack gives all data open for public, but it is also fully transparant what data is given to the public. Full democratic ownership between all interested exsists, no central logistics actor has ownership. There is a split of data, multisig vs coordinates/public key.

Downside of all actors having to have generated keypair before lising is possible on marketplace.

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.