University of Amsterdam

Master Thesis

Course Code

Decentralized p2p trustless logistics

Student Name:
Dylan Bartels

Student ID:
10607072

June 14, 2018

Contents

1 Abstract

2 Introduction

The gig economy is in full effect, individuals get payed for the execution of short term contracts and big companys 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 possiblities to shift towards decentralized solutions in the logistics domain[**?**][**?**][**?**].

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. Recent research [**?**] 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.

With the recent progression in the domain of trustless value transference, research towards the applicability of this in the supply chain offers relevancy. In [**?**] research has 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.

Main research question:

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

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?

3 Background

3.1 Decentralized

3.2 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

3.3 Marketplace

3.4 Multisigniture

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

6 Conclusion

7 Discussion

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.