The challenge of decentralized marketplaces

Bas van IJzendoorn, 4024850

ABSTRACT

Categories and Subject Descriptors

1 [**A**]: B

; 2 [**C**]: D

Keywords

1. INTRODUCTION AND PROBLEM DESCRIPTION

Commodities are traded on decentralized markets (Miao, J., 2005).

http://www.uniba.it/ricerca/dipartimenti/dse/seminari/seminari-2011/Schiraldi-al2011.pdf Rapson, D. (2011) Proof that transaction costs are less in decentralized markets and that

2. CREATING ON-LINE AND OFFLINE TRUST SYSTEMS IS HARD

In order to understand the problems with computerized markets and in particular the decentralized markets a touch of economic theory in offline markets is researched to understand the underlying economic mechanisms. Especially generating trust among actors is hard both on-line and offline. In traditional economic theory of a perfect market their is no discussion for trust and the concept is kept outside the domain of economics. In the traditional market anonymous buyers and sellers come together to exchange standardized goods. It is assumed that buyers and sellers try to maximise their welfare. Because of the transparent nature of the perfect market their are no opportunities to be dishonest and so there is a natural trust among buyers and sellers. In more recent research the concept of trust has become a part of economic theory and is evaluated in a number of economic theories. It is general consensus among economic theorists that social relations are of vital importance to create trust between actors. For computers it is thus hard to generate a trust relationship because computers are inherently not social and need to provide other means to generate a trust relationship. This trust relationship can be a computer to computer relationship, a computer to human relationship or a human to human relationship where the only interaction is between computers. When their is trust among actors trade can be done and according to transaction theory trust even lowers the transaction costs. Business can be done quicker when there are broader social relations among actors that generate trust. At the same time the social relations minimize the risk of opportunistic behaviour in the market. Actors are less likely to cheat each other when they are part of a larger social group. In computer markets with no social relationship the incentive for actors to cheat on each other becomes higher. The insight that trust can lower the costs of exchange and minimizes risk has pushed the concept of trust in the economic debate.

The lack of social relations with other actors in the economies creates problems in communication and trust. Communication issues can be solved by providing well enough information about products, vendors, buyers etc. to actors in the markets. However, questions arise as to how much of the information should be made available to actors and to what extent should information be anonymous. Sharing of information gives opportunities for actors to use this information and exploit the sharing trader. For instance, a buyer in grain trading markets might be reluctant in sharing how much grain it wants to buy because this gives valuable information about the trading position of the buyer. When other actors know the trading position of the buyer they can play economic games like only selling grain for a higher price to this buyer. What kind of information and how information should be presented to users depend on the structure and information demand in each market. These information streams should thought of carefully in the design of the decentralized market to avoid exploitation of the information.

Trust issues in a digitalized world are not easy to solve. For computers it is even harder to generate trust and determine the trust of agents in comparison to real life social interactions. To understand this better let's take a look at the irrationality on which offline actors make decisions on who to trust. There is consensus among economic theorists that actors have a bounded rationality when making economic decisions. This is contrast with rational choice theory which states that actors always make rational decisions. Economic actors simply do not have the overview of all the possibilities to make a rational decision about what

economic decision would be the best. Instead the offline human economic actors base themselves on all sorts of trust mechanisms. Williamson (1993) distinguishes six types of these trust contexts that are important for economic activity: societal trust, political trust, regulatory trust, professional trust, network trust and trust in the corporates themselves. These contexts are largely outside of the digital world and thus it is very hard for an on-line programmable agent to take these contexts into consideration and make a trust decision on behalf of an offline user. There is no purely logical reason for an offline actor to make a trust decision. As computers are purely rational actors it is very hard to calculate whether another party is trustworthy or not (Furlong, D., 1996).

However, there are a large number of positive examples where computer systems are trusted for economic activity. In this paper we will first look into further detail of failed and successful cases and proposals of on-line trust systems. We will look into the details of what problems causes the failures and what we can learn from successful systems. After that we will look into what additional requirements are needed in a decentralized market apart from a good trust system.

3. ONLINE TRUST SYSTEMS

In a lot of computer systems there are alternative trust mechanisms in place like reputation systems for agents, anonymization systems to guarantee anonymity and thereby trust and brand usage to get a trust label. In business to consumer electronic commerce there are multiple examples of successful trust systems. There has been research done as to when users accept to do an electronic purchase and when users have an intent to go to an electronic shop instead of a real physical one. It turns out that not only the information quality, service quality and system quality have its effect on the perceived usefulness of the system, but also the perceived trust of an e-commerce website plays a vital role in the perceived usefulness of the system and the altitude of the system. The importance of perceived trust by a user on e-commerce websites has been shown in multiple studies (BRON). It is shown that in e-commerce have a lower level of trust and that successful e-commerce websites ensure a low level of consumer risk perception and a high level of consumer trust perception (Corbit et al, 2003). EVENTUEEL EXTRA BRONNEN TOEVOEGEN. Examples of successful e-commerce systems are Amazone.com, bol.com, alibaba.com, Uber and AirBnB. Some of these examples build on a successful brand. In other examples where you buy from another user other trust systems are in place like reputation system. In AirBnB houses are rented out to users. Both the house owners and the users have a reputation. When trading in second-hand goods on for instance bol.com, a reputation of the seller is also kept up. Interesting to note is that in AirBnB the pictures of the rented apartments appear to be the success factor of the website to create trust (BRON).

We will now describe into detail different kind of trust systems that are in researched in academics. Some are proposals of designs that are never implemented and some are real implemented examples that either are very successful or fail. The reason behind this discussion is to find best practices of online trust systems for the decentralized market case. What works and what doesn't? What can we learn from past successes and failures of systems?

3.1 Trust in P2P file sharing

In P2P file sharing research there are a number of systems proposed with mechanisms to prevent free riding. This is mainly done with reputation systems that either use payment systems to maintain reputations or another form of maintaining a reputation. The reputation systems in generally work well but are not always resilient against the Sybil attack. The Sybil attack is discussed after the systems discussion.

3.1.1 Research proposals

According to Moreton, T. (year) the major problem in P2P systems is the mutual distrust between peers. There are many pseudonyms or Sybil nodes that take up resources without providing resources to the network. These Sybils are run by agents which have a bad trust relationship with the other agents of the network. The behaviour of these agents is in P2P filesharing also denoted as freeriding. The problem was first described by Wilcox O'Hearn after his experiences with the deployment of the Mojo Nation file sharing system. O'Hearn also describes the mistrust among nodes as the biggest problem in Mojo Nation syste. The motivation between nodes to cooperate was not there. Nodes did not upload data to the network which made data availability a problem. There were even attacks on the network by which users altered their clients to gain more advantage for himself. Users altered their clients to gain more trust in the system.

Vishnumurthy, V. (year) introduces a design of a P2P file sharing system where a currency is introduced in where a single value called KARMA. The currency KARMA represents the amount of resources a peer has contributed and consumed in the network. This represents a users trustworthiness with regard to upload/download ratio within the system. The idea behind is that a user who has uploaded more is more likely to upload in the future and is therefore more trustworthy. This means other users can upload to this user and the user with high KARMA gets a higher download speed. The proposal of Vishnumurty is quite complex. There are groups of k nodes called bank-sets that keep track of the KARMA of each user. Mechanisms are in place to make the KARMA system work. Distributed hash tables (DHT's) map nodes towards a bank set. When a node goes down, a new node becomes part of the bank set. It is impossible for nodes to adjust their KARMA level at will and KARMA can compensate bank nodes for participating in transactions with KARMA. Thus nodes who help in maintaining the system by banking get a small KARMA reward. This idea is also used in block-chain (BRON). There are also security mechanisms for replay attacks, malicious providers, malicious consumers, attacks against DHT routing, corrupt bank sets and denial of service attacks. However, KARMA does not protect against Sybil attacks. Protection against Sybil attacks will be discussed in a later section.

Tsuen-Wan et al (2003) proposed three solutions to the freeriding problem and to enforce sharing. Two of them are not suitable according to the authors. The third one introduces

a method that involves the auditing of peer nodes. Each node maintains a usage file where it defines the amount of capacity it advertises and it also maintains the advertised capacities of all neighbours. A simple rule is added that says that a node can only download new data if its own advertised capacity is larger than the sum of the advertised capacity of all its neighbors. An auditing procedure is introduced that let nodes check on each other whether to tell whether they are trustworthy or not. The economics of the auditing model seems very unlikely to be successful. The required capacity needs to be very high to be able to download data. What's interesting about the paper is that the concept of an auditing procedure by other peers is introduced. By this way the network maintains its own reputation.

The design of Vishnumurthy, V. (year) is an example of a P2P system design that is a combination of a reputation system and a payment protocol. A paper that tries to capture the essence of this combination is the stamp trading model by Moreton et al (year). Moreton describes that payment protocols operate using a currency. Moreton introduces stamps that can be traded between nodes and can later redeemed at a node for service. In this payment protocol the stamps have a variable value and are traded based on this value. It is assumed there is a centralized exchange rate mechanism which can observe all interactions between node and thus provide perfect valuations to the stamps' value. This assumption has practical issues. In the first place it is hard to observe all interactions between nodes and secondly the centralized exchange rate node has to be trusted fully. If this central nodes gets compromised by an adversary, all interactions can be observed and the whole network is compromised. In the paper multiple price valuation methods are proposed with different properties. The schemes have to be both token-compatible and trust-compatible. A scheme is token-compatible if the total value of the stamps in the network is bounded. A scheme is trust-compatible if failure by a node to redeem a stamp never increases the total value of its stamps. In four of the proposed methods for pricing the system can be flooded with requests by nodes with a higher bandwidth to artificially obtain a higher trust. In the last method called Bounded Redemption Rate (BRR) the value of the stamp is chosen in such a way that flooding the network with stamps causes a node's total stamp value to approach zero value. In this way the BRR method becomes trust-compatible. It is also proven that BRR is also token-compatible. BRR can resist Sybil attacks because when a nodes becomes flooded with requests of pseudonyms, the total stamp value of a node approaches zero. However, stamp trading still has the following open problems: double spending, cryptographically signing stamps, audit trails of stamps, the token exchange problem which is now fixed with the central node assumption and limited knowledge on both the stamp-trading economies and attacks. Thus although stamp trading is resistant against some form of Sybil attacks it has many open problems which makes is impractical to implement in the real world.

PPay is a system introduced by Yang, B. et al that uses payment systems to fix the free-riding problem in P2P systems. The solution Ppay is introduced in this paper and improves performance of micropayments while maintaining security. Unlike traditional transferable cash, coins in Ppay do not grow in size as they are transferred. A user purchases digital coins from a broker B. The user U is now the owner of the coin. U can assign the coin to another user V and V can do reassignment request to U. When V wants to reassign the coin to user X it has to go through the user of the coin U. Therefore U must always be online in order to reassign coins. To solve the problem of a potential crash of U there is a downtime protocol introduced that allows the holder of the coin to have the coin reassigned by the broker. In this case broker B will charge both U and V a percentage of the reassigned amount for this service. This charging gives incentives for nodes to remain online. The reassigning of the coin is computationally expensive. Ppay does not prevent coin fraud at the outset, but instead makes fraud unprofitable. Ppay ensures that any fraud can be detected and traced back to the misbehaving peer by means of an âĂIJaudit trailâĂİ of the coin. The system can be attacked by replicating an assigned coin and spending it twice, wrongful denial and double spending. The broker will create the right punishments and will do risk management for the system. There 4 four issues and extensions described to solve certain problems. 1) Printing raw coins is expensive for the broker. This responsibility can be divided to users with limit certifications. 2) Layered coins: The coin transfer history is saved in layers at each coin. The reassignment adds a new layer to the coin. 3) Coin renewal: The audit trail is purged once in a while to limit the amount of state each peer should maintain. 4) Soft Credit Windows: Quick payments that go back and forth can be washed out. Payword hash chains are also a fast method. A quantitative analysis is performed that compares Ppay to RM. Ppay can significantly outperform existing schemes in terms of broker load, while maintaining a reasonable peer load.

Ham, M. and Agha, G. solves the free riding problem in a similar way as with micropayments with servers. The payment (credit) is made volatile and the approach does not rely on servers. It is assumed that a stricter system does not degrade its popularity because a system with free riders will eventually starve. Four types of cheating are targeted: Exaggerated credit by an individual peer, Conspiracy: a peer may evade detection using collaborators, Blame Transfer: a cheater might blame an innocent peer to hide malicious peer misbehavior, Omitting Interested Peers: Omitting peers from malicious lists send to other peers. A credit system is introduced where credit is the uploaded bytes (contribution) minus the downloaded bytes (consumption). Two values LL and LLe are introduced as limits to the system as to when a peer should serve another peer. These limits solve the start-up deadlock and the starvation.

Feldman, M. et al (2004) made a mathematical model that studies the free-riding problem. The mathematical model has not been tested in the real world so nothing can be said about its validity. However, some useful observations can be extracted from the model. For instance, the behaviour of white-washers: users who leave the system and rejoin with new identities to avoid reputation penalties are added to the model. In the paper is not a new incentive scheme proposed. This is an example of a Sybil attack where pseudonyms leave the system and later rejoin to renew download speed. Sybil attacks are discussed later.

3.1.2 Real implemented examples

All of the reputation systems described so far have not been implemented. BitTorrent has a mechanism in place for free-riding inspired on Tit-for-Tat . A peer in BitTorrent prefers to upload more data to another peer it has downloaded from. In Kazaa a more complicated mechanism is in place where some peers are elected super nodes and peers receive peer-points for uploads. Super nodes get more responses of peers who spend their peer-points to gain a higher download speed (Tamilmani, K., 2003). Tamilmani, Karthik (25 October 2003). "Studying and enhancing the BitTorrent protocol". Stony Brook University. Archived from the original (DOC) on 19 November 2004. Retrieved 6 May 2006.

At Delft University of Technology, Tribler is a P2P file sharing system used for research. Two trust schemes have been tested in Tribler: Bartercast and Multichain. In BarterCast, a peer collects upload and download speeds of other peers by requesting this information from peers. The information received is then forwarded to ten other peers. By this way upload/download ratio information is shared among all peers and a map of peers with their ratios can be created. A bloom filter algorithm is in place that deletes duplicate information. Each peer can calculate the reputation values of other peers with the max-flow algorithm. In BarterCast there is no global reputation value calculated by an authority. Every peer maintains its own list of reputations of other peers. It is assumed that no cheating is done upon the sharing of information. Truth-telling of nodes is assumed and the trustworthiness of nodes is assumed to be high (BarterCast bronnen). It is easy to attack BarterCast by simply stating a high upload amount to other users. Sybils can verify this high upload amount to help fool honest nodes.

MultiChain is an improvement on BarterCast. A payment system is introduced that replaces BarterCast completely. The payment protocol and datastructure is inspired by the BlockChain payment technology. In MultiChain and in BlockChain a chain of blocks with transactions is maintained to prevent the double-spending of coins. The difference between BlockChain and MultiChain is that MultiChain blocks are distributed among the two peers of the interaction instead of one single BlockChain. The benefit of this is that the ChainSize is kept small in MultiChain. In BlockChain the size is ever increasing and becomes inoperatable after some time. But MultiChain also introduces some of its own problems. When a node fails MultiChain cannot check anymore for double spending. The coin could be traded by the failing node and the failing node is the only node that knows where the coin goes next. Also transactions cannot be performed fastly after each other. A transaction has to be processed completely in a block before a new transaction can be made. This gives scalability problems (Norberhuis, S., 2015).

Tribler also uses decentralized credit mining to gain trust in other P2P file sharing networks. The system aims to earn trustworthiness of peers in other swarms. In the paper by Capota et al (2015) this is described as earning credit in other swarms on behalf of the user. The system is part of the Tribler P2P client and is implemented for every peer and therefore completely decentralized. The system selects swarms on its upload potential and start to upload data to these swarms. In this way the peer gains trust in that swarm. Information is frequently updated to maximise upload to swarms and there are also spam detection and duplicate content detection to further enhance the upload process. The system is also tested to show that trust is gained in other swarms with the system. The underlying mechanism to gain trust in the paper is simple. The peers simply behave cooperatively by uploading data to proof that they are not free riders and thus to proof their trustworthiness.

3.1.3 Sybil attack to reputation systems

In order to solve the problems of Sybil attacks several research has been done. For instance, PageRank is a trust mechanism that determines the trustworthiness of websites. The trustworthiness is based on multiple factors, but the most important factors are the number of links directing towards that website and the trustworthiness of a website that is referring. It is based on the principle that if more trustworthy people link toward a website, this website should be trustworthy. With Sybil attacks PageRank can be easily exploited. Pseudonyms can refer to each other to become trustworthy and these trustworthy pseudonyms can then increase the trust of certain websites by linking towards them. This is called the "two-loop attack".

In order to be protected against the Sybil attack alternative algorithms other than PageRank are proposed by researchers. Hopcroft and Sheldon introduced the Global Hitting Time Mechanism (GHT) score. This algorithm differs from PageRank in that the links outgoing from the website of which the GHT score is determined are removed from the PageRank calculations. This protects against the two-loop attack where websites link towards Sybils and the Sybils link back toward the website. However GHT is still vulnerable to the restart-capture attack. The restart-capture attack make use of a vulnerability in the GHT algorithm when the calculation restarts at a different node. Thus Brandon proposes a new algorithm called Personalized Hitting Time to solve this problem and improve the GHT algorithm. PHT works almost the same as GHT but calculates the score with a minor adjusted random walk. With an experiment is shown that PHT gives resistance against a specific kind of attack when agents show strategic behavior. Strategic behavior means that more sybils can be created by an agent. Also the informativeness of PHT remains high when more Sybils are added. But this property also remains high with Personalized PageRank. The definition of strategic behavior among agent is that a strategic agent creates misreports for other agents. Thus the agent will slander other agents with misreports. In PageRank this is equal to cutting outlinks to other pages or in other words to not create links to other pages. The strategic behavior is changed and redefined for every type of trust algorithm. In the PHT version no Sybils are added. The title of the paper: "Personalized Hitting Time for Informative Trust Mechanisms Despite Sybils" suggests that PHT provides an improvement on the trust mechanisms with Sybils. However, in the paper the strategic behavior of agents do not add any Sybils. Thus the impact of Sybils is not tested on PHT.

The lack of good algorithms to calculate trust scores with Sybils gave inspiration to Otte, P. to research sybil-resistant trust mechanisms. The informativeness is the percentage of agents that have a non zero score. Otte, P. introduces

Temporal Page Rank, another random walk variant that makes use of a random jump in the random walk. An experiment shows that a higher uploaded amount (trustworthiness) leads to a higher downloaded amount and thus that a fair trust mechanism is in place. Temporal Page Rank does not offer resistance to Historical attacks. Another algorithm that is introduced by Otte, P. is the NetFlow algorithm that makes use of the Max-Flow algorithm to calculate a trust score. To solve the informativeness problem scaling is used to higher the trust values of nodes with a low trust score. With the scaling Sybils will be allowed to get a higher trust score. This creates a trade-off between weakly profitable Sybil attacks and informativeness. Seuken and Parkes showed that it is impossible to be completely Sybil proof.

Clustering algorithm / community detection in graphs. Notion of sybil community support. Hier zijn al papers voor. Deze kan ik later toevoegen. http://micans.org/mcl/

The difference between a global trust score and a personalized trust score is as follows. In a personalized trust score the trustworthiness of an agent is calculated from the perspective of another agent. With a global trust score a trust score is calculated for every agent.

3.2 Trust in anonymous systems

At first the academic research that has been proposed to create a mechanism to let users pay for TOR anonymization software is discussed. TOR is a software where contributors work together to provide an anonymity layer for the user. Here again rises the free-riding problem where users have little incentives to contribute to the network. A system where users can pay for usage of the system and contributing nodes get a reward for contributing might be a solution to this problem. The internal economy of nodes contributing to the TOR network is the same trust structure as with P2P file sharing systems. A node is trusted when it contributes to the TOR network. Secondly, anonymity in itself can also give more trust to the system. When users are anonymous it gives the user the trust that no sensitive information is gained from using the system. There are a few implemented examples in the real world where this is the case.

3.2.1 Research Proposals

Androulaki, E. (2008) proposes a design that addresses problems such as the double spending problem with a hybrid payment scheme by combining features from the micropayment system and the e-cash scheme. The proposed scheme does not attempt to achieve absolute financial security but the authors are willing to accept small amounts of cheating. There are two types of coins in the proposal: S-coins and A-coins. S-coins are coins signed by relay nodes and are used to pay successor nodes in a circuit. A-coins are signed by th e bank and bought by users to use the anonymization network. S-coins can also be used to pay for using the anonymous network. This gives economic incentives for tor relays to forward traffic.

In another research by Tsuen-Wan et al (year) a solution is presented in which a âĂIJgold starâĂİ is given to relays that provide good services for others. A gold star relayâĂŹs traffic is given higher priority by other relays. The bandwith is audited by the existing directory authorities to give users gold stars. After experimentation it is shown that nodes who are âĂIJcooperativeâĂİ and thus share bandwidth and forward all goldstar traffic according to the rules have a faster download time and lower ping time. No practical implementation is given where it is tested whether users are indeed willing to contribute in exchange for a better service.

Another such a system is the TEARS system proposed by Rob Jansen et al (2010) and the BRAIDS system by Jansen, R. et al (2010). In the TEARS system are Bandwith contributions rewarded with Shallots. Users can exchange Shallots for PriorityPasses to gain traffic priority. Shallots can be traded with other users. Open problems are with making incentives to participate, market economics policies, community effects and with deployment. Also the problem to determine if a relay was honest or not is not solved. BRAIDS introduces a ticket system which users can obtain from a bank and can be embedded into Tor cells to request services. The tickets are distributed by agent nodes that monitor other nodes. The agent nodes distribute tickets from the bank in proportion to the provided bandwidth. Each relay verifies itâĂŹs tickets to prevent double spending. A discrete event based simulator is used to show that their is an increased performance in traffic. With both TEARS and BRAIDS no implementation to test the system is given.

A more complex solution to the free riding problem in TOR networks is the LIRA system proposed by Jansen, R. (2010). LIRA produces incentives with a novel cryptographic lottery design together with a new circuit scheduling algorithm that prioritizes traffic from those winning the lottery. Relays acquire electronic coins from the bank by providing service to the network. These coins can be exchanged for guaranteed winning tickets in the lottery and therefore provide in prioritized traffic in the TOR network. Other clients can also guess winning tickets with tune-able probability. Relays cannot distinguish from a guessed winner and a payed winner and thus maintain anonymity for paying clients. Mathematical arguments are given that LIRA provides economic incentives to buy tor usage, however no experiments are given in which LIRA is in use and there is a good working economy.

3.2.2 Implemented examples

Christin, N. (2012) and Soska, K. (2015) have done measurements to the activity of the successful anonymous online marketplace the Silk Road. The Silk Road marketplace is an independent marketplace where buyers and seller conduct in electronic commerce transactions. Using TOR technology the Silk Road also provides anonymity for its users. Items are payed with bitcoins. Most items being sold on the Silk Road are illegal narcotics such as Weed, Drugs, Cannabis, Cocaine and Pills where most of the items come from the U.S.A. (43,86%), U.K. (10.14%) and the Netherlands (6,51%). The items are delivered worldwide. Interestingly the transaction volume stays about the same while the bitcoin price changed. The number of sellers doubled almost in 6 months time from february to august 2012. Most of the new sellers leave the site fairly quickly. Only about 4% of the sellers have been on the site for the entire duration of the measurements in 2012. Because of the illegal items that are being sold on the Silk Road some of the the Silk Road

got eventually taken down by law enforcement. After some time a new version shown up where the same kind of items where being sold. Nog even wat verder uitwerken.

3.3 Trust in smart contracts

With smart contracts people may be able to execute trades through Trustless public ledgers (TPLs). TPLs allow a restructering of power relations between parties and intermediaries. TPLs enable parties to store digital assets online without the need of banking intermediary who charges a fee. In addition to that they also allow parties to transfer digital assets directly to each other on their own terms. The conditions of the terms can be programmed in a "smart contract": "an automated program that transfers digital assets with BlockChain technology upon certain triggering conditions". Smart contracts do not require an institution as an intermediary exchange. Smart contracts also solve the longstanding problem of e-commerce courts to refuse to protect consumer contract terms. With smart contracts consumers can express their own wishes for the contractual terms and negotiate with other parties on their own. The way this is implemented is via automated consumer purchasing agents that can be used throughout the whole web. A standard online infrastructure on which consumers and providers can negotiate on their terms is provdided (Fairfield, 2014). Users put their trust in the TPLs and the programmable smart contracts.

In an early paper where a contract between two peers is named is the paper by Ghosal et al (2005). The idea of an exchange between two peers based on a single value is questioned. Instead there is an exchange with relation to an amount of service S provided by a peer. The service S a peer can offer is actually a vector that contains different service specifications. For instance, in file sharing S can contain the amount of data that is shared and the available bandwidth for each file. The peers exchange money for a service level that can be specified differently for each type of service and each peer.

A practical implementation of smart contracts is the Ethereum system (White paper Ethereum). In the Ethereum system money is traded with smart contracts using its own currency: "Ether". The underlying transactions of the smart contracts are done with BlockChain Technology by Satoshi Nakamoto's (2009). BlockChain does not only provide an infrastructure for digital payments, but also provides a distributed consensus for the rightness of the payments and prevents double spending attacks. Ethereum is a fully fledged Turing-complete programming language that can create a wide range of financial applications like smart contracts, digital currencies for exchange and also programmable decentralized autonomous organizations (DAOs) (Ethereum paper). Egbertsen researched the possibility to replace paper contracts by Ethereum contracts. Paper contracts are an agreement between parties to do or not do something. For instance, a grain seller agrees on delivering an amount of grains to the Paranagua harbor in Brazil at a certain date and time. With Ethereum it is possible to handle the contract details online in the BlockChain. Egbertsen recognizes four fields of examples where Ethereum smart contracts could replace paper contracts. The first and probably the most widely used is a purchase agreement. The example of the Paranagua grain paper contract is an example of such a purchase agreement. In a lot of cases in the current world money is put in Escrow at a third party. When both sides have fulfilled their parts, the purchase agreement is met Examples uitleggen. Juridische limitaties uitleggen. PROBLEMS WITH ETHEREUM, LAW PROBLEMS

3.4 Decentralized markets

3.4.1 Research proposals

Soska, K. et al (2014) introduces a formal model for a decentralized anonymous marketplace (DAM), and the design of Beaver, a Sybil resistant DAM. The transactions and reviews of items in the marketplace are public, the relationship between the transaction and reviews are kept private and the customers in Beaver always remain anonymous. There are four basic transactions in Beaver 1) Registration: a vendor adds an item to the list of available items. 2) Payment: Funds are moved from a customer to a vendor. 3) Review: leave a review for an item. 4) Add transaction: add transcation to ledger. The ledger is a log of all the transactions which is maintained with bitcoin technology. The vendors first register themselves to the network, a customer can browse the different vendors and purchase an item from a vendor by doing an anonymous payment transaction. A customer can also give a review by tighting a review to a payment transaction he made earlier. In the security thread model are two assumptions made: 1) 75% of the nodes in the network need to be honest. 2) The customers and vendors are rational and do not behave maliciously if the cost of doing so is significant. Maybe say something about assumptions. For each transaction is a detailed algorithm described to perform the action. Fees are paid for each transaction and obtained by the node that adds the transaction to the ledger with bitcoin technology. Some limitations and points for future work are discussed like: vendor privacy(vendors might want to conceal their transaction volume) and values of fees.

3.4.2 Implemented examples

Beaver is a Sybil resilient and customer anonymous system design for a decentralized market. These high requirements of the system are difficult to achieve. A real implementation of a system with such high requirements is so far unavailable. At Delft Univeristy of Technology a first start has been made of decentralized market.

The first system is Tsukiji, a first implementation by The,M. and Reinbergen, H. (2013). It is a simple implementation where decentralized nodes act as traders. The traders can place bid and ask offers and respond to an offer such that a trade can be established. The discovery of peers is also implemented but there is no real money traded and there also isn't a working user interface.

An improvement on the design of Tsukiji is the Decentral market design by Olsthoorn, M.J.G. and Winter, J. (2016). Instead of peer discovery bid and ask prices together with quantities are distributed across the network with ticks when a peer bids or asks a certain quantity. Secondly, there is a simple matching engine implemented that matches bid and ask quantity amounts with the highest and lowest prices. Then when a match is made real money is traded. MultiChain coins of Tribler peers are traded against BitCoins in

a single transaction where both wallets of both traders are updated. The design is successfully implemented in Tribler, constructed with Dispersy and tested.

4. REQUIREMENT ANALYSIS

To take the decentralized market software to the next level thought should be given to the design of the system. Of course, the normal security aspects of a software system are important and the system should be easy to use. A not so trivial aspect of the system is how the matching engine mechanism should work. Matching engines bring buyers and sellers together and vary over markets. To some extent, the mechanisms can be exploited via strategies. The strategy-proofness of matching algorithms is researched in economic theory around "two sided markets".

4.1 Strategy-proofness in two-sided markets

A "two sided market" is a market where two parties are linked together. For instance, a creditcard links consumers and merchants to each other or newspapers link subscribers to advertisers. The software platforms that bring together these groups of users are considered a very important innovation and can be found in many industries (Eisenman, T. et al, 2006). The research in this paper is a first direction towards a two-sided market that does not require a central component. A first research towards a distributed two-sided market is done in this survey.

Agents that operate in a two-sided market can develop strategies to exploit weaknesses in the market. In this section possible exploitative strategies of agents in the original platform based two-sided markets are researched. When making the two-sided markets the possibility of new strategies that allow to exploit the market might be introduced. This should be researched carefully in theory and perhaps be discovered by experimentation in a implemented distributed two sided market.

In 1962 Gale and Shapley introduced the first matching model that researches strategies in two sided markets (Abdulkadioglu, 2010). Gale and Shapley (1962) introduce a preference list of an agent. This is a ranked list where the agent gives a prefered order of all the agent it wants to be matched with. For instance, a grain buyer provides an ordered ranked list of all the grain sellers it wants to buy from. With the deferred acceptance algorithm a "stable" match can be found. A "stable" match is a matching of all the buyers and sellers such that they can never do a better matching when re-matching each other later. The deferred acceptance algorithm is a greedy algorithm because it makes the local optimal choice at each stage. The algorithm works as follows. Each buyer proposes to match itself to its preferred seller. A seller who receives multiple proposals from buyers chooses greedily the favourite buyer and rejects all other buyers. In the next stages each rejected buyer now proposes to their next choice and again sellers choose their most preferred option or reject otherwise. Gale and Shapley prove that this algorithm always lead to a stable matching. Thus a matching is made where no party could be better of in another stable matching (Gale and Shapley, 1962).

There are multiple ways in which matching can occur in two sided markets. In One-to-One matching there is one buyer matched to one seller. The deferred acceptance algorithm gives a stable matching for each One-to-One problem. Also, the buyer weakly prefers the stable matching from the algorithm over other stable matchings.

Strategy-proof means that truth-telling upon preference revelation in the deferred acceptance algorithm is a dominant strategy equilibrium. According to Roth (1982) there exists no matching algorithm that is both stable and strategy-proof for one-to-one matching problems. This means that there always incentives to not tell the truth among revelation of preferences. However, in the One-To-One case the proposing side (buyers) have truth-telling as a dominant strategy. Thus a stable matching is compatible with truth-telling for one side of the market. Another interesting thing is that according to Gale Sotomayor (1985) any stable matching in the One-to-One case is a Nash equilibrium in undominated strategies. An undominated strategy in game theory is a strategy where the outcome could be better or worse than another strategy depending on what other players do. This means that in the market case the side that receives matching proposals might be better off with another strategy than truthtelling depending on what the proposing side (buyers) do.

Colleges have capacity manipulation and truthtelling manipulation. Dit even verder uitwerken. student optimal matching is used as a policy to prevent to "Game the System".

The game theoretic analysis show that there are incentives to manipulate the stable matching process. This gives the possibility for traders in the decentralized markets to play games with revelation and capacity strategies to influence the matching. A trader could develop a strategy that influences who trades with who. Because of the impossibility to create a matching algorithm that is both strategy-proof and provides stable matching, the designer of the matching algorithm should think carefully about the requirements and the design for the matching algorithm.

TTC

Many-to-Many matching

5. DRAFT MATCHING ENGINE

Is fixed in matching engine. According to Bichler, M. dynamic pricing mechanisms can be implemented such that market prices match the market conditions and therefore creating an optimal outcome for both buyer and seller. In physical markets, the high transaction costs of auctions have made it impossible to implement these price mechanisms. With information technology it might be possible to implement auctions and change the way how the markets are operated. Ebay has already proven itself to be successful in online auctions. An example of an auction is where buyers send their bid prices to suppliers. The suppliers can then accept the bid prices as a contract. Electronic exchanges can focus on the buyer side or the seller side. The actor that has the least market power usually takes the initiative. There are also auction techniques on which over multiple attributes of the contract are negotiated to allow complex products (Bichler, 2001). In other markets there is also a need for dynamic pricing models. There is research done

in multiple markets to find suitable price discovery mechanisms that suits each market. For instance, in the cloud computing market Anandasivam, A. and Prem, M. (2009) introduce a dynamic pricing model for price determination in the cloud computing market In cloud computing systems, sometimes the demand is high and sometimes the demand is low. The price is changed when the demand level changes. This price change is calculated in a mathematical model. Another example of the need for a dynamic pricing mechanism is in modern electric power grids. ELECTRONIC POWER GRID UITWERKEN.

Methods: Auction from Bichler, Auction from Lee,

Various possibilities on matching engine and price discovery mechanism

6. DRAFT PROBLEM DESCRIPTION

Decentralized markets are hard to create. Buyers and sellers need to be matched to each other according to their preferences. A price should be negotiated and a trade deal should be made. The requirements vary among markets. Brunner, E. et al divides the economic requirements into four categories of parameters: basic, composed, complex and comments. Basic and composed parameters are simple values like price, volume and quantity. Composed parameters are more complex economic measurements that needs to be computed from more values like Return of Investment (ROI) and Price-earnings ratio. The last parameters are comments like quality or expert reviews. Policies on how these parameters should be created, altered and read needs to be specified for each market. Other research introduces the concept of contracts between peers called P2P contracts or smart contracts. These contracts allow to transfer user specified amounts against user specified conditions. For instance, ABN AMRO bank uses smart contracts in a case in which it only transfers money after a quality check has been done successfully (BRON). These conditions allow great flexibility in the economic parameters. Namely, all transactions conditions and requirements can be programmed as a smart contract. This allows to maintain money on the Internet without the need of an intermediate party (Fairfield, J., 2014). Brunner, E. *et al* also specifies time sensitive and historic information that should be made public to the user. Also privacy information of the public and private market and personal data of the user are considered parameters by Brunner, E. *et al*.

7. DRAFT STRATEGY PROOFNESS

Impact on market according to Bichler with broker services. However, time has proven that the market still requires the broker. Example van Olsthorn et al, just buy out the bid prices.

As markets can obtain a variety of characteristics it is important to notice that for each market a different market mechanism is required. To reason easier about markets the following concepts are described in the paper by Hatfield and Kominers for market mechanism design. 1) Stability: There is no blocking pair for a match. A blocking pair is a match with a higher utility function than the original match. e.a. the blocking pair match is a better match than the original match. Thus a stable match is the best match available. If a match is stable this implies a future match offer will never be better (Niederle, Yariv, 2008, Gale and Shapley, 1962). Gale and Shapley (1962) showed that any market has a stable matching and provided an algorithm that identifies one in the deferred acceptance algorithm. 2) Strategy-Proofness: When a matching mechanism is implemented there might be strategies that disrupt the market. For instance, a person might BETER OPZOEKEN in two sided matching literature (Niederle, Yariv, 2008). Roth and Sotomayer have an example of a market where agents have an incentive to misstate its preferences even tough the optimal match is chosen by the implemented mechanism. 3) Substitutability: The definition of substitutability is as follows. Lets assume two group of agents G and H that are matched. An agent $a \in G$ chooses $b \in H$ as its optimal match. If b is also chosen as the optimal match from $H' \cup w$ where subset $H' \subset H$ than the preferences of a are substitutable. When b is chosen from a set, it is also chosen from a smaller set. (Echenique, F, Oviedo, J., 2006). SO a CAN ALSO CHOOSE ANOTHER WORKER. http://people.hss.caltech.edu/ fede/published/echen-oviedo-TE.pdf STRONG SUBSTITUTABILITY OOK NOG ERBIJ DOEN. 4) The Law of Aggregate demand: (Condition) If the choice set of contracts for an agent increases, the agent chooses a bit more contracts.

8. BIBLIOGRAPHY

http://link.springer.com/article/10.1007/s12599-009-0071-2/fulltext.h
Current cloud computing solutions lack pricing mechanisms, but there are movements to bring this into the business world (Weinhardt, C.)

https://pdfs.semanticscholar.org/85e2/69c8b6a9d791424e16747a6d390
Auction as a dynamic price mechanism in e-commerce (Lee, J.)

https://books.google.nl/books?hl=nllr=id=-lhLmmSM–4Coi=fndpg=
Book on matching (Bichler, M.)
file:///C:/Users/Lenovo/Pictures/wilson-market-architecture.pdf
Economisch paper over markets (Wilson, R.) http://www.emeraldinsig
Importance of trust in economic commerce (Pauline Ratnasingham) http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.5
Commodity trading using an auction (Preist, C.). http://people.bu.edu
Search model centralized and decentralized trade (Miao, J.). (Matching engine)

http://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3/?utm
scholarlycommons.law.wlu.eduSmartcontracts(*Fairfield*)

http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4536461
Requirements and architecture decentralized information system (Brunner)

http://www.sciencedirect.com/science/article/pii/S002205318471074X
Equilibrium mechanisms in decentralized market (Peters, M.)

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.359.3617re
Contract design and stability in markets (Harvard, Hatfield, 2011).

TRUST in electronic commerce (Ratnashingham, 1999). https://www

https://pdfs.semanticscholar.org/d490/3a683c7b60a27a0c19c28d0a7774eb9dd373.pdf
http://www.emeraldinsight.com/doi/pdfplus/10.1108/10662249810231050
Trust in electronic commerce.

Importance of trust in electronic commerce: http://www.emeraldinsight.com/doi/pdfplus/10.1108/10662249810231050
Importance of perceived trust, security and privacy in online
trading systems. https://www.researchgate.net/profile/Juan$_{G}arcia95/publication/220207958_{T}he_{i}mportance_{o}f_{p}erceived_{t}rust_{s}ecurity_{a}$
$shoppinghttp : //download.springer.com/static/pdf/565/art$

http://dspace.unive.it/bitstream/handle/10579/7203/830275-
1190055.pdf?sequence=2

9. REFERENCES