

OneMarket: A Peer-to-Peer Internet Marketplace

TheDagger

thedagger@mail.com

www.cloakcoin.com

Abstract: An entirely peer to peer form of internet e-commerce that will permit buyers and sellers to trade with one another without a governing central point of control. The existing Cloakcoin blockchain, a descendant of the Bitcoin protocol, provides a key part in distributing the “public marketplace listings ledger” across an existing p2p network. OneMarket is designed to be a decentralized, trustless, self-organizing, and self-regulating system to facilitate trade.

1. Introduction

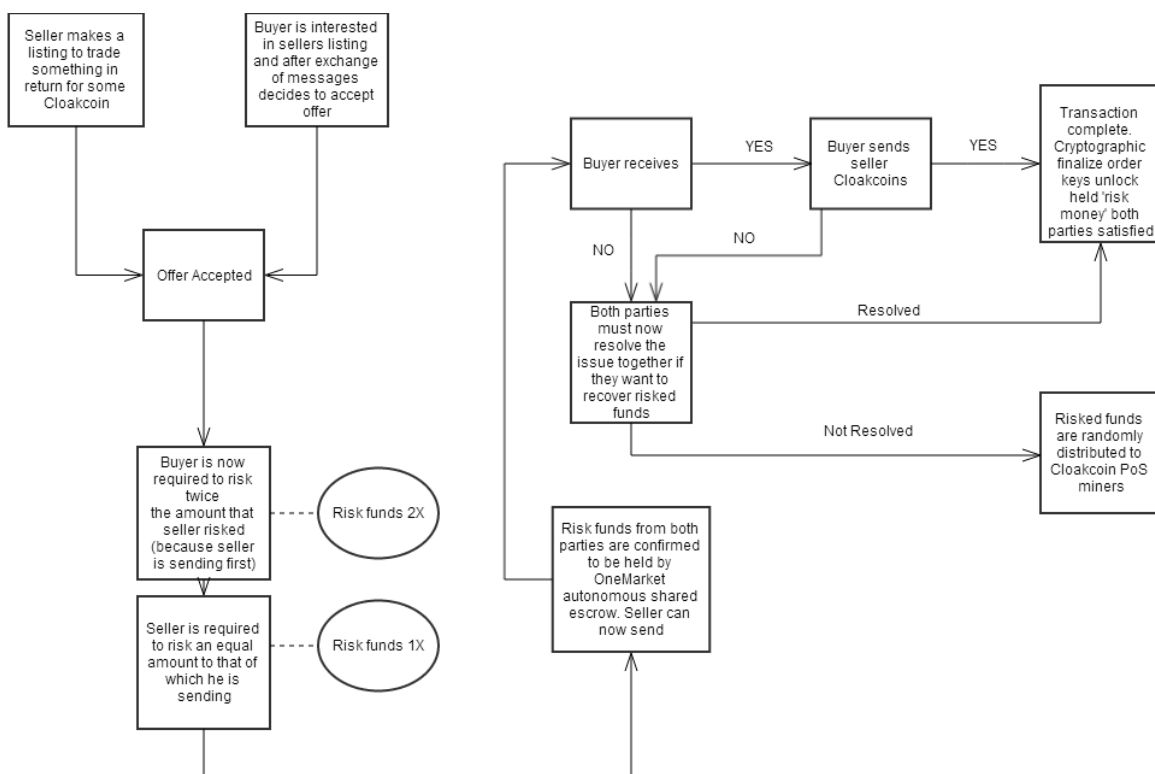
With cryptocurrency revolutionizing electronic payment systems since the launch of Bitcoin, it is now time to do the same with e-commerce. Whilst the current internet commerce systems work well enough, most of the time, they have an ultimate point of failure by making the buyer and seller transact via the hands of a trusted third party (such as eBay). The cost of placing such trust in “third party mediators” comes at a price, usually by the way of transaction fees, advertisements, loss of privacy, and dictated consensus of items permitted for sale. Existing third party mediators that preside over consumer to consumer transactions at present are driven by profit making aspirations, keeping books clean, and upholding partnerships with third party payment processing partners, such as PayPal. It is no surprise that traditional e-commerce systems therefore generate elevated costs for the end users (i.e., buyers and sellers) because of running costs and capitalistic tendencies. What we propose is a trading platform with the advantages of existing solutions, but one that is autonomous by design using cryptocurrency as decentralized units of transaction. OneMarket is a buy/sell platform that is not limited by geographical boundaries.

2. Trustless Escrow

One of the major hurdles of a p2p network will be trust in the parties involved. Other proposed solutions have tried to combat this by proposing a rating system tied to cryptocurrency addresses or to involve an escrow service. However, rating systems are flawed in that they can be manipulated by third parties and escrow services are potentially biased in their final rulings and likewise can also have their ratings manipulated [1].

The solution is to implement a trustless based escrow system that was inspired by Noble Prize winning mathematician John Nash's game theory concept of 'Mutually Assured Destruction'[2]. This can be achieved by having the buyer and seller put *twice* the amount of the item or service for sale ('risk money'), into a shared escrow, locked by cryptographic finalize-order keys and cancel keys contracted to a time they agree upon. Only when both finalize-order or cancel keys (one from seller and one from buyer) is the escrow unlocked and funds appropriated to the correct parties. If both cancel keys are used, the money and 'risk money' goes back to the buyer and seller as if nothing happened. If finalize-order keys are used then the buyers funds will go to the seller and the buyer will get back their 'risk funds', and the seller gets back their 'risk' funds. If the buyer and seller can not come to an agreement by the time the escrow contract states then the funds will be dispersed permanently and randomly into the 'miner' pool. This further incentivises users to leave their wallets open to gain in these profits and prevents deflation of the economy by destroying the money.

Of course if users want to, they can purchase items on the marketplace outside of the built in escrow system and use a third party escrow service, but they do so at their own risk.



3. Self Regulating & Spam Prevention (OneJury)

Another major hurdle is the problem of immoral postings. Such as and not limited to, dangerous weapons, child porn, assassinations, human trafficking, and other morally wrong activities. One might think to introduce a user-flagging system much like Craigslist. The problem with this is that a powerful enough individual or group of individuals could control the market by selectively flagging listings to get a competitive edge, not to mention flagging is highly subjective to the person flagging. Another problem is someone just posting over and over again to flood the network (a.k.a., Spamming).

To combat both these problems, we created a review-penalty-reward system called OneJury. How it works is when you place a listing, you are required to pay a *transaction fee* and a *self-regulating fee*. The transaction fee is used to prevent spamming since it will cost a (market based) fee to post a listing, making it not cost effective to spam the network constantly. This transaction fee is paid out to miners giving yet again another incentive to leave the wallet open. The listing is not eligible to go live until this transaction fee has cleared the blockchain. The self-regulating fee is split amongst and used to pay the reviewers of the listing that answered *in favor of the masses*. To better explain, the review requests are sent out to the network randomly to anyone it can find that is online. These reviews would appear in the 'reviews' area of the marketplace if one was sent to you. The first person to review is eligible for their portion of the self-regulating fee.

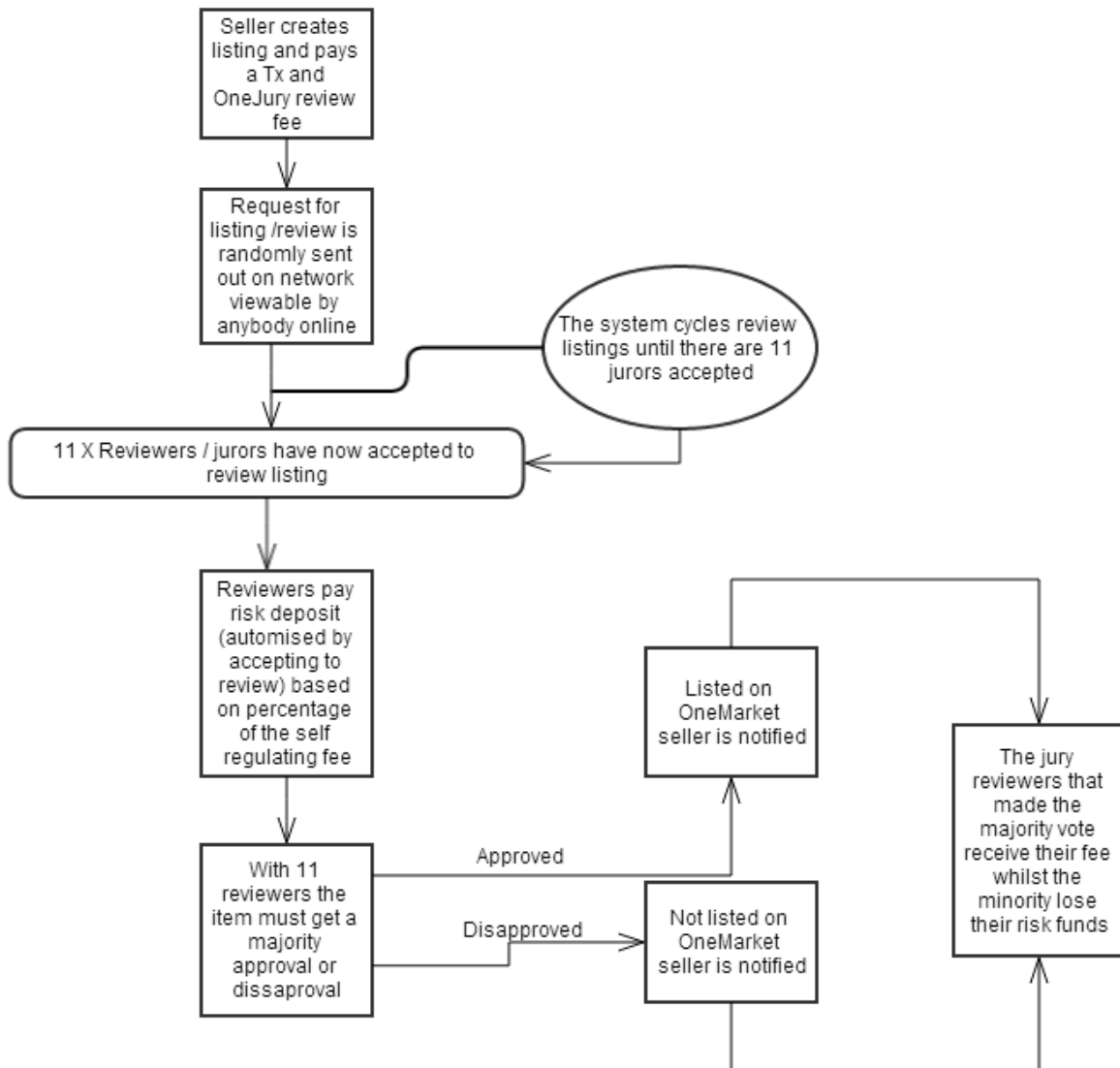
This brings up the issue of people just clicking reviews without actually reading them or making an automated bot to just click 'yes', or 'no' randomly. To solve this we implement the review-penalty-reward system. In order to review you have to put up a *percentage of the reward* you would get for answering the review of the listing as 'risk mitigation'. If you answer the review in the same way as the majority of the other 11 selected reviewers then you get your 'risk' funds back plus the reward. If you fail to answer the review according to the masses then you LOSE your reward. This gives a huge incentive to actually *think* about what you are reviewing and how others will think and what they will choose otherwise you will lose your 'risk' money. Since most listings will probably be valid listings after a certain point, it is possible you could make a bot to always click 'yes' and therefore counter the system again. To combat this the penalty fee needs to be substantially higher than these odds and adjust as a *percentage of the reward*.

The percentage is determined based on the amount of 'yes' votes given in the network on average. So if 90% of the market is giving good listings, then this means the *percentage of reward risk* amount is 9X the bid + 1X the bid. So for example, if it cost 1 cloak to review a listing and there is a 90% chance the answer will be yes to it, you need to risk at least '10' cloak so there is no financial incentive to make an automated tool since you will lose more than you would gain.

In the possible situation that 99% of posts become valid this will be the maximum *percentage of the reward risk fee*. In this way the risk that needs to be put up-front is not too expensive to allow the average person access.

This also gives less incentive to review ‘grey-area’ posts that are in between right and wrong in which case the masses may sway to one side or the other, leaving only positive posts getting reviewed and accepted, or very bad posts being reviewed if one believes the masses will agree its bad. It’s up to the reviewer to decide what risk they are willing to take.

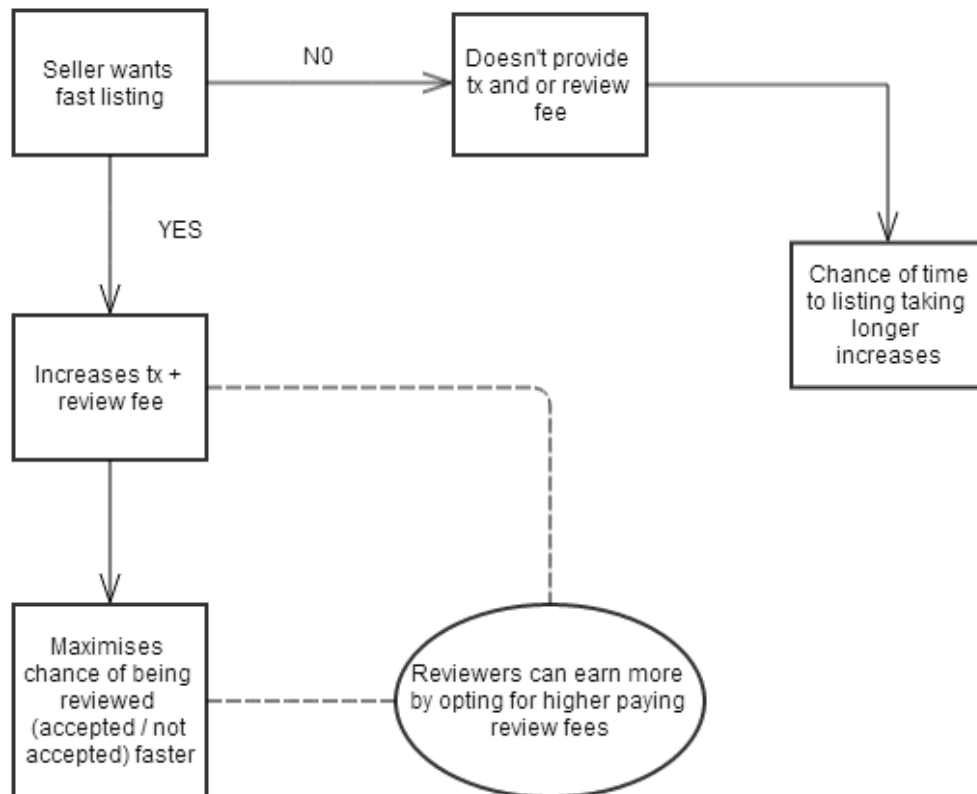
By doing this a safe and secure self-regulating network is possible.



4. Marketplace Scalability Issues Regarding Spam & Self-Regulating

One of the major issues to preventing spam is that the price stays high enough to deter them. Same for reviewers, the price needs to be rewarding enough for them to want to spend their time reviewing. To combat this when you place a listing you are required to supply a transaction fee

and self-regulating fee. The higher these fees the faster (and more likely) you will get your listing up on the market, since reviewers will want the more profitable review to take on. Listings put into the que to be reviewed can only stay in the que for 7 days, they will be deleted and assumed not accepted if not enough reviews are submitted. Transaction and user-regulation fees, used to place a listing, are *never* refunded as to prevent spamming the network. This will allow the system to scale as the price of cloak changes.



5. Optional Rating System

While this system does not *require* a rating system due to the trustless escrow, a rating system can help the sellers and buyers better decide if they want to enter into a trustless escrow. They can be privy to such information as an address that has done escrow before, only to have the money be *burned* by not working together.

To combat this; the rating should be split into '5' factors each for buyer & seller actions related to the cloak address in question to contemplate their escrow decision with.

1.) Cloak Address Marketplace Age

Cloak Address Marketplace Age is how long the address has been active on the market. An address that has been involved in the market longer is less likely to be a throw away address since it becomes harder and harder to fake those.

2.) Number Failed Transactions (Escrow went bad)

Indicates cooperation ability and probably the most important metric of them all.

3.) Failed Transaction Amount

The value in cloak involved for failed transactions.

4.) Number Successful Transactions (Escrow worked out)

Indicates cooperation ability and probably the second most important metric.

5.) Successful Transactions Amount

The value in cloak involved for all successful transactions.

One general lump sum rating is not reliably possible, but using these 5 factors the buyers and sellers can make decisions on whether to do business or not.

6. Technical Details

- Will use the existing P2P network for transferring data related to marketplace ledgers [3].
- No Images Allowed (Users should use online image hosting urls to refer to images)
- 1000 Character Limit On Descriptions For Entries. (UTF-8 Encoded)
 - To prevent bloating the network.
- Listings valid for 7 days (listings will automatically drop from the ledgers after 7 days)
- Listing Info Stored in database using existing Bitcoin Database Library on clients that opt-in.
- Will employ Trustless Escrow system.

P2P Marketplace Ledger Contents

These were set as a bare minimum essentials to keep the market running efficiently.

- Title (Limited to 30 characters)
- Cloak Address (Address of seller)
- Description Of Service
- Country

- Allows results to be more fine-tuned via filters.
- Can also allow downloading of ledgers only from 'countries' to save time syncing the network.
- Region
 - Allows results to be more fine-tuned via filters.
 - Can also allow downloading of ledgers only from 'regions' to save time syncing the network.
- City
 - Allows results to be more fine-tuned via filters.
 - Can also allow downloading of ledgers only from the city to save time syncing the network.
- Category
 - eBay categories [4]
 - We will copy all the categories here as the valid categories that can be selected.
 - For everything not listed, we will have an 'other' category.
 - Used for searching efficiently through the marketplace.
- Startdate
 - Keeps track of the start date of the listing. Listings older than 7 days are removed to help clean up the network. A re-list option can be used to automatically re-create your listing after the 7 days expires. This does require the wallet to always be on. Which also increases the stability of the cloak coin network as a side effect to help prevent forking.
- Contact Email
 - Needed for reminder emails and/or future parsing
- Price
 - Used for sorting marketplace listings.
- Rate
 - Hour
 - Week
 - Month
 - Year
 - One-Time
- Unique SHA512 Hash
 - Hash representing the ledger contents. Necessary to uniquely identify a market listing and prevent blatant/obvious duplicates.

7. Conclusion

OneMarket introduces a system of allowing person to person buy/sell without relying on any third party intermediaries during both listing and purchasing stages. The project takes advantage of existing and proven p2p decentralized cryptocurrency technology and ties into the Cloakcoin blockchain to provide a distributed marketplace ledger. Bloating is one of the main concerns raised when working directly within a blockchain: To solve this information will be stored in the same way that bitcoin ledgers do, via a database. The same database platform will be

used to keep track of records minimizing lag times. Once updates are propagated through the network they are stored in a local database copy and deleted after 7 days unless renewed.

There can be no breakdown of a centralized server disrupting service and because Cloak Cryptocurrency is the currency of OneMarket there are no third party and trust based payment options.

Every computer with a Cloak wallet can opt in or opt out at any time as a node/storage device that serves as a distributed database for the OneMarket network.

In connection with the users public cloak address, there will be indicators derived from their trustless escrow transactions displaying past buy / sell successes and failures.

The system employs OneJury to have listings reviewed by 11 randomly selected reviewers to self-regulate its content based on the majority consensus of the 11 reviewers. The reviewers are incentivized to review honestly and correctly or they lose the risk money they put up front, and if they answer correctly then they get a portion of the reward offered during the listing creation phase by the user. To answer correctly a reviewer simply has to give the same answer as the majority of the other reviewers. The higher the self-regulating fee, the more likely the reviewer will spend the time to make sure its a good listing. A reviewer will hesitate to accept a listing that is even potentially morally in question for fear of losing their 'risk' deposit and guessing wrong what the other reviewers would think. This provides a safe place to do business that the *collective morality of the masses* (or reviewers which represent this) decide what is allowed or not, thus self-regulating.

References

- [1] Federico Dini and Giancarlo Spagnolo “Manipulating soft performance indicators in public procurement” 2006
- [2] John Forbes Nash “Nash equilibrium”
http://en.wikipedia.org/wiki/Nash_equilibrium
- [3] Protocol specification https://en.bitcoin.it/wiki/Protocol_specification
- [4] Ebay catagories <http://www.ebay.com/sch/allcategories/all-categories>