OpenBazaar

Connor Sheehan

Danny Mandel

Shandelle Murray

A free, open, peer to peer marketplace for online trading of goods and services

Goals

- Eliminate need for third party corporations involved in online trade (Amazon, eBay)

- Eliminate extra fees and restrictions

- Reduce overhead costs of trade

- Allow global communication and trade

Sellers

- Install program on computer

- Create store

- Generate contract(s) to list items/services in store

- Send and receive messages from potential buyers

Buyers

- Install program on computer

- Search for items/services or browse through stores

- Send and receive messages from sellers

- Potentially select goods and services to purchase

Notaries

- Notaries are moderators in the event of a dispute

- Buyer selects a contract, creates "multi-signature" bitcoin pubkey with the notary

- Buyer sends funds to "escrow" address

- Seller confirms order processing, sends signed copy of transaction

- Releases funds from the multi-signature address

- Buyer either:
  - Accepts and releases funds
  - Disputes: notary can then release of not release funds

Process

- A contract describing the item and specifying the terms of sale is generated by the seller and posted to their store

- A buyer interested in purchasing the item can choose to do so

- A third party notary may be selected in order to mediate the trade

- The seller ships the item or provides the service

- The buyer receives the item/service

- If both parties agree that the contract is satisfied, the Bitcoin funds are able to transfer from one party to another

- If there is a problem with the trade and the parties are in disagreement, they must provide proof of a discrepancy and the notary then decides how to proceed

- If the notary decides that the seller has satisfied their part of the trade, the funds get transferred according to the terms of the contract

- Otherwise, the notary may rule in favor of the buyer and the funds may not get transferred

Implementation Details

- Kademlia-style Peer-to-Peer Network to allow the possibility of connecting millions of people

- BitCoin as a medium of exchange

- Ricardian Contracts define trade terms

Ricardian Contract

- To ensure fairness and to avoid unauthorized changes to the contract

- Protects both buyers and sellers

- States terms of contract and may include a third party notary

- From the original OpenBazaar website:

  A Ricardian Contract can be defined as a single document that is a) a contract offered by an issuer to holders, b) for a valuable right held by holders, and managed by the issuer, c) easily readable by people (like a contract on paper), d) readable by programs (parsable like a database), e) digitally signed, f) carries the keys and server information, and g) allied with a unique and secure identifier.

  - Ian Grigg

  Makes use of a chain of digitally signed and checksum hashed contracts to create an unalterable record of agreement

- Digital signatures from involved parties provide proof of agreement

- Hashes provide proof of authenticity because the tiniest change in the contract will show in the hash

Demonstration