TEzcrow —- A decentralized peer 2 peer Escrow Solution for Digital Assets

Whitepaper v1.0

Cryptovet, Keerthiz, Blueprint, Clurbsauce

Abstract. Trust has been associated with the trading of goods and services since the first grain was traded for a fine rock. Trust is still a part of every economic transaction that takes place today. Computers and online transactions have had a staggering impact on how we interact and trade with each other, however certain flaws still persist. Among these flaws are economic crimes and rising transaction costs. The fact is that computers are better at numbers than people are , and most of us have come to trust a computers “code” over that ever so trusted hand shake. Fraud and high transaction fees going to the middle person was initially in Bitcoins whitepaper and remains a driving force amongst decentralization purists. Exchanges for art and other non-fungibles have taken the place of these middle men and become the next entry point for the flaws that have existed since the beginning of time. Trust.

1. Introduction

Electronic transfer of non-fungible tokens relies almost exclusively on a few platforms that process and serve as trusted 3rd parties. These 3rd parties we believe have potential for flaws to be interjected into a persons trading digital goods with another. Namely the fees charged and required even if not agreed upon by both parties. Secondly online fraud : the uncertainty of the counterparty’s identities and the uncertainty of the products quality or authenticity.

In this version we will solve the first flaw by creating a smart contract that is strictly peer 2 peer and allows for agreement between parties involved on price and fees. The second flaw of online fraud and its many parts will be addresses in subsequent versions of Tezcrow.

We feel that these flaws must be addressed to onboard users of any digital goods and of higher end financial applications on digital blockchains.

2. Smart Contracts

Most modern cryptocurrencies rely on smart contracts, a self-executing contract based on a programming language. Nick Szabo proposed this first concept of a smart contract by comparing it to the purchase of an item from a vending machine.

Smart contracts allow digital and physical assets to move according to an arbitrary pre-specified set of rules. Smart contracts have a blockchain as an underlying layer, whereby all involved transactions are time-stamped and respectively added to the chain. Due to the design of a blockchain, there is no central authority that validates or screens these transactions. In contrast, it is a network of decentralized nodes that validate transactions. This technology is a form of Distributed Ledger Technology.

Due to the self executing mechanism of smart contracts, the trade will automatically settle whenever these predetermined conditions are met. Once executed , the contracts state cannot

be altered. The contract can however be seen and verified anytime by anyone on the blockchain by what is called a block explorer.

Benefits of using a smart contract

This technology enables contracts to operate more cost and resource efficient. The mechanism and terms to transfer digital assets are fully transparent. All transactions and data associated are accessible for the involved parties. Finally, the simplicity of peer 2 peer trading in a smart contract allows for a unique opportunity to decrease language and cost ambiguity. Ambiguity occurs when there is a lack of clarity or a sense of uncertainty about why a cost is being applied, or why one has to buy this token or pay this fee.

TeZcrow

Tezcrow intends to create a decentralized and secure ecosystem that eliminates the need for trust during a transaction of digital assets by providing tools to solve the trust flaws inherent in economic transactions and provide rapid settlement in a time efficient manner and a convenient interface. Tezcrow does this by removing intermediaries, lowering overhead costs, and increasing the users flexibility. Users are provided with a secure , standardized smart contract to ensure accessibility and security of the protocol.

The utilized blockchain layer of Tezcrow is Tezos, an open-source, community governed blockchain network. Tezos uses a Proof-of-Stake (ie Liquid Proof of Stake) mechanism as consensus method. This method utilizes baking and features optional delegation, allowing any stake holder to participate in consensus without giving up custody of their tokens. Tezos is formally verified and is nearing its 10th upgrade Jakarta. In its most recent upgrade Ithaca it upgraded to an interoperable consensus ability. We believe this makes Tezos an ideal blockchain to build a truly decentralized peer2 peer trading platform that can be adopted by the 7billion inhabitants of planet earth, and to do so in the most efficient and green way possible. It is a lofty goal however we know that the transfer with the least co2 emissions possible will ultimately be what has to survive.

Decentralized Escrow

The Tezcrow escrow service eliminates the perceived risk and inherent flaws during a digital property transfer through leveraging smart contracts.

In an escrow exchange , the Seller first offers the exchange of a digital asset in trade for another held by Buyer. The offer goes into escrow awaiting acceptance from the Buyer. The Buyer then either accepts or declines the offer. Upon acceptance the smart contract makes the trade from one connected wallet to another and fulfills the agreed upon trade of digital assets.

If conditions are not agreed upon the parties could enter into an arbitration in which parties would negotiate the trade based on predetermined time ranges and asset values by either party.

The current implementation of Tezcrow covers the use case for exchange of one digital asset to another after a proposition is made and agreed upon by both parties.

Creation of an escrow proposition

Acceptance of a proposition

Cancellation of a proposition

The actors in the workflow define a system architecture that resembles that of a Decentralized Application pattern where the tezcrow web service simplifies the interactions between the final users and the smart contracts on the blockchain, via an application program interface which may store relevant data in an offline database. Among other activities this API would be in

charge of 1)Authenticating final users through registering tezos wallet address of users 2) validating and preparing the data to be included in the blockchain transactions, which are sent to the final users in order to be signed with the users wallets thus invoking the corresponding smart contract.
The Authentication of final users and digital asset authenticity has proven a challenge that will take longer than we currently have for this hack. However we felt that some explanation of its usefulness was necessary and relevant to this project as decentralization and trust is the overall goal.

Topics possibly explored in future versions of Tezcrow

1)The blockchain is perceived as a potentially revolutionary solution of transferring property digitally efficiently, safely, and trustless. The benefits of smart contracts serve to be the catalyst for a new era of e-commerce. Tezcrow platform will likely need to go through KYC process to comply with FATF guidelines. The buyer and seller connects the Tezos compatible (eventually all chain compatible) wallets to the tezcrow escrow service through a tezcrow api and the data written to create a smart escrow contract.
2)Transferring physical property and challenges presented.
3)Decentralized Identity management
4)Identity provided by a Certification Authority
5)Identity provided by the blockchain
6)Decentralized Oracle Networks
7)Economy and Token features

It should be noted that for now we have chosen not to incorporate a token into Tezcrow. We believe that Tezos has all the functionality and useablity necessary to allow exchange of digital goods from one party to another and see a new token as an area for the inherit flaws to come into the trade.