Astero : a peer-to-peer international money transfer protocol

Teng Peng
draft April 24, 2021

Abstract

Westernunion and its competitors have been highly inefficient in transferring money across borders. These legacy organizations, built before the internet age, do not provide service with low fees, short waiting time and high amount limits. This paper outlines a peer-to-peer international money transfer platform called Astero that supports individuals and business transfer and exchange money worldwide with instant delivery, unlimited amounts and low fees. To achieve these goals, we introduces 1.an orderbook-based fiat currency exchange. 2.a stackexchange-like community for dispute resolution and counter-party risk reduction. Astero can outperform Westernunion by 100x with sub-minute settlement time, 100x higher amount limits, 10x lower fees.

1 Introduction

The foreign exchange is the largest financial market in the world – 40x to 100x larger than crypto exchange, with a daily volume of $6.6 trillion. SWIFT handles about $5 trillion per day. However, the legacy money transfer service are slow and expensive based on the standard of the internet-age. US bank requires customers to initiate transfer in-person. Westernunion limits the amounts transferred to $5000 from the U.S. to China. Paypal boasts their international payment fees are "as low as 4.4% plus fixed fees".

These legacy service fall short with the expectations in 2 situations:

1. **E-commerce**: Many small cross-border e-commerce owners get paid via Amazon Pay, Paypal and Shopify Pay and they are charged insane fees to transfer the money to their own local bank account. The common alternative is underground banks who often disappear overnight with even higher fees.
2. **Workers, travellers & students**: They have to follow the low amount limits imposed by Westernunion and send small amounts of money many times. The common alternative is to exchange money with their colleagues, classmates and other acquaintance and this is inefficient and risky.

This paper presents a peer to peer international money transfer platform called Astero, which is more efficient, cheaper, and faster than legacy organizations; safer than underground banks and other alternatives:

Solutions	Time	Costs	Risks
Legacy	1-5 business days	1%-5%+	**Very low**
Underground bank	Various	1%-5%+	Very high
Acquaintance	Various	Various	High
Astero	**Sub-minute**	**0.1%-**	**Very low**

Table 1: Comparisons of international money transfer solutions

The main process of Astero is to convert international money transfer to local money transfer by matching two transfer with opposite directions, and resolve disputations on-chain if there are any.

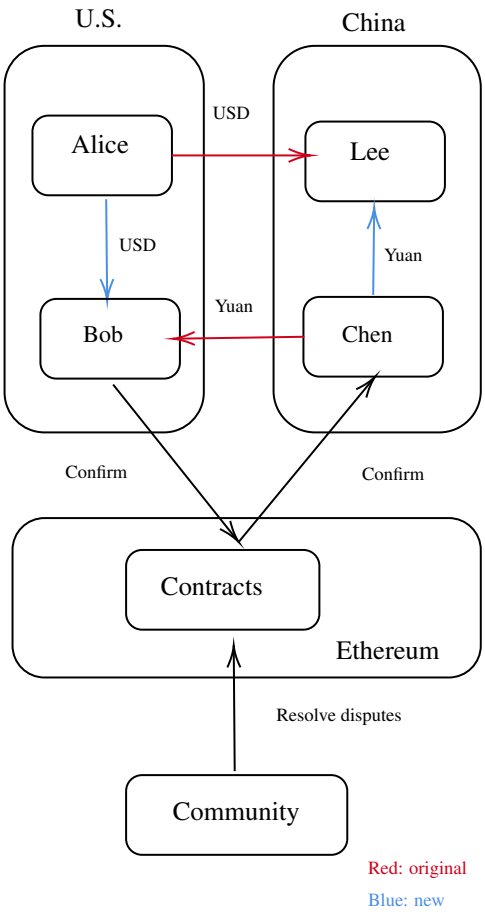
There are 2 major roles in Astero:

1. **Users** : send, exchange and receive money on Astero, paying fees to the platform and arbitrators.
2. **Arbitrator**: resolve disputes between users if there are disputes.

Example Alice in the U.S. wants to send ¥100 to Lee in China, while Chen in China wants to send $15 USD to Bob in the U.S.:

1. Alice send $15 to Bob, and Chen send ¥100 to Lee.
2. Lee and Bob confirm they have received fund.
3. If there are disputes, the community would resolve the disputes on-chain and receive rewards.

This example is illustrated below.



2 Goals

The two major goals of our designs are:

1. **Safety** : Users do not lost their own funds using Astero, which often times happens on underground banks.
2. **Efficiency**: Users spend less costs and time than using legacy financial service.

There are several existing challenges to achieve these goals:

1. **Anti-fraud** : If a user claims funds have been already sent but the other user claims otherwise, how should we resolve these disputes? What if arbitrators are bribed by a user to rule in favor of the briber despite facts presented by the other party? How do we settle disagreements among arbitrators?
2. **Protection of privacy**: If users agree to upload evidence of transfer during dispute resolution, how do we protect the privacy of users? What if arbitrators misuse the private information of users?

3 Design

We sketch one possible design to achieve these goals.

3.1 Process of money transfer

The protocol is designed for crypto-crypto transfer, crypto-fiat transfer and fiat-fiat transfer.

1. **Crypto-crypto transfer** : Both party would send money to the contract first. If money is received from both party, the contract would send money to recipients automatically. No arbitration is needed.
2. **Crypto-fiat transfer**: The crypto would be send to the contract. If the recipient of fiat confirms, the crypto is released. If there are disputes, users can originate arbitration process.
3. **Fiat-fiat transfer**: The user with higher reputation points receive money first, then the user send money to another user. If there are disputes, users can originate arbitration process.

This process encourages crypto-crypto transfer since no arbitration is ever needed. It also favors crypto holders because the user would receive fiat first and the probability of losing crypto sent to contracts are low if the arbitration mechanism works. This also favors users with high reputation points because they receive money first.

3.2 Reputation-based arbitration mechanism

Reputation is defined as a function of honesty, volume, and contribution to the protocol. Similar to the practice of stackexchange, reputation is at the core of arbitration mechanism.

All users would start with 0 reputation and grow their reputation as they actively using the protocol. This leads to a cold start problem: if all users are considered 0 reputation at the very beginning, how could they trade with each other and grow their reputation? The protocol would provide 2 ways as solutions: 1. users could choose link their twitter profile with the protocol and get social verification. 2. users could collateralize with cryptos that worth more than the money they receive.

Arbitrators are elected by the rank of the reputation. To prevent spams, all dispute submitted require a dispute resolution fees paid by the originator of dispute. Arbitrators would comment on evidence of both sides, and they could comment on each others' comment. If one comment is considered to be wrong by other arbitrators, the comment would get down voted by others: the original commenter would lost reputation points. To prevent spams, the downvoters would also lost reputation points but much smaller than that of the original commenter. If an arbitrator has great contribution to resolve the dispute, then upvotes are given by other arbitrators. Upvoters would gain reputation points but much smaller than that of the original commenter.

4 Examples

4.1 E-commerce

Lee located in China is a cross-border e-commerce owner on Shopify. He does not have a U.S. bank account but he has large amounts of USD on Shopify. The protocol can match him with another user who wants to exchange USD for Yuan. Suppose he has higher reputation points since he is a frequent user. He would receive Yuan on his local bank first. Then he would send money to the other user. This is a fiat-fiat transaction.

4.2 Oversea employees

Alice resides in Japan and she works for an American crypto company, paying her USDC. She can get matched with another user who needs USDC in exchange of Japanese Yen. She could send her USDC to the contracts and release USDC once she confirms. This is a crypto-fiat transaction.

4.3 Decentralized OTC

Two anonymous users want to have a OTC trade for a low-liquidity coins. They both send funds to the contracts and the contracts would handle the rest.

References