computing conference 2017

A Blockchain based Peer-to-Peer Framework for Exchanging Leftover Foreign Currency

Rituparna Bhattacharya, Martin White, Natalia Beloff

Department of Engineering and Informatics, University of Sussex

1. Introduction

Almost every traveller possesses some amount of leftover foreign currency, either as actual cash or on a travel currency card, at the end of any international trip. However, the means to exchange this leftover currency, coins in particular, is largely inconvenient often leading to considerable amounts discarded or left unused. Research from Zopa suggests that British travellers alone have an estimated £2.9bn of LFC lying around across the UK. Scaling this problem up globally reveals a significant amount of global wealth lying around in travellers' wallets, purses and drawers at home! We explore here how distributed ledger technology, i.e. blockchain, could be applied to the problem of utilizing this leftover foreign currency. We portray here the drawbacks of the existing systems of foreign currency exchange and delineate the requirements of a potential mobile web application for exchanging this currency by integrating smart kiosk based systems, particularly for handling cash, with a peer-to-peer currency exchange technique based on blockchain that could help to bring such currency back into circulation efficiently.

2. Background Research

Recently, a number of new systems have come onto the market that allows cash based Leftover foreign currency (LFC) exchange via post such as Cash4Coins and LeftoverCurrency and kiosk based exchange such as FourEx and TravelersBox. However, the former suffers from the drawbacks of associated postal order charges and time delay. And, in both cases, whether exchange via post or kiosk, the exchange rate is decided by the converting agency to their advantage, they operate with a limited set of currencies, and they are not ubiquitous.

A new disruptive way of exchanging money could be to exploit a P2P currency exchange. Here, there are broadly two different categories of P2P currency exchange systems: the first one allows currency exchange without any associated crypto-currencies and the second one uses a virtual crypto-currency system for exchange. The former do not accept cash currency. The transfer and/or exchange fees for the P2P systems are not suitable for low amounts to be exchanged. In the second method, crypto-currency based exchange platforms have emerged, where some are built on the concept of blockchain technology. Bitcoin, Stellar, A.I.Coin are some such examples. However, they do not alleviate the problem of physical currency exchange for cash based LFC, i.e. currency carried back home, particularly, low value amounts.

3. Blockchain

Traditional digital transaction systems are built on a trust-based model where payments are processed by third parties such as banks, thus incurring service charges of varying kinds. In some applications it may be desirable to eliminate this intermediary or third party and perform transactions between ourselves, i.e. peer-to-peer (P2P). To enable digital payments to be sent directly from one party to another, a decentralized P2P system emerged around 2009, called Bitcoin, which was a first in a series of what is often called a cryptocurrency (decentralized digital currency), where cryptographic hashing is used for the generation and transaction of virtual currency. With Bitcoin, the generation and transactions of cryptocurrencies are recorded in a shared public distributed ledger that is accessible to all the peers in the network. This distributed ledger technology is maintained as a blockchain, which is a chain of blocks threaded sequentially in linear, chronological order. All transactions recorded in this ledger are supposedly irreversible, thus providing a new secure and potentially private framework for digital transactions. Prior to the advent of blockchain technology, it was not possible to prevent double spending of digital money without a trusted third party because digital assets can be copied to any extent. Another problem in this context is the Byzantine Generals' Problem. Bitcoin solves both the problems with the implementation of Blockchain.

4. Requirements

Users must be able to login into the P2P LFC mobile application with their credentials, and further use their mobile device or associated wearable using a secure NFC mechanism for accessing a deposit kiosk. User should be able to deposit and withdraw cash LFC at the smart kiosk and get a receipt for the transaction. Users must be able to select currencies, amounts and destination currency, check available exchange rates for those currencies and perform exchange. Users should also be able to advertise their preferred exchange rate for currency selected in case they do not find a suitable exchange rate. The users will receive notification when the exchange is done. There would be a provision for auto-exchange where exchange will be done based on a system decided exchange rate. It is usual to offer the option to donate currency to charity or buy articles from participating merchants with their LFC. A user should be able to transfer selected currency balances to their bank account or the accounts of friends and family. Users can see previous exchanges done, open advertised rates, amounts donated, gifts purchased and money transferred from/to user's bank accounts or that of friends and family. Users should be able to recharge the multicurrency P2P LFC account by transferring money from their bank account.

5. Proposed System

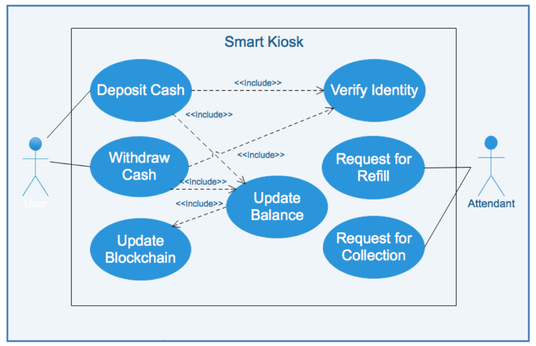

Fig 1: Smart Kiosk Use Case Diagram

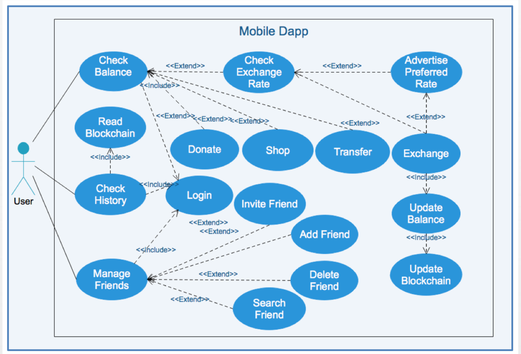

Fig 2: Mobile distributed application

6. Development and Future Work

Our work so far is focused on defining the requirements as discussed above and experimenting with blockchain and smart contract development at the backend. Experimentally, so far, we are implementing the deposit, exchange and withdraw scenarios of P2P LFC application using Solidity to write smart contract on the Ethereum blockchain in a Embark based environment.

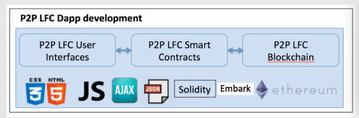

Fig 3: P2P LFC Exchange Architecture

Our observations currently indicate that there are certain complexities associated with blockchain development such as asynchronous function calls, unsuitability for real-time applications, cryptography and transaction ownership, out of gas exceptions and transaction fees, no fixed point mathematics or the inability to pass strings between Solidity functions, which make blockchain and smart contract development a non-trivial task.

Contact Email: rb308@sussex.ac.uk, m.white@sussex.ac.uk, n.beloff@sussex.ac.uk