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

Rituparna Bhattacharya
Department of Engineering and Informatics
University of Sussex
Brighton, United Kingdom
rb308@sussex.ac.uk

Martin White
Department of Engineering and Informatics
University of Sussex
Brighton, United Kingdom
m.white@sussex.ac.uk

Natalia Beloff
Department of Engineering and Informatics
University of Sussex
Brighton, United Kingdom
N.Beloff@sussex.ac.uk

***Abstract*—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. In this paper, we explore 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.**

Keywords—Blockchain; Currency Exchange; Internet of Things; Smart Kiosk

I. INTRODUCTION

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 (e.g. banks) and perform transactions between ourselves, i.e. peer-to-peer (P2P). However, before Bitcoin arrived, around 2009, there was only one successful form of P2P transaction, and that was peers exchanging cash, goods or services of some value face to face. What's more such peer-to-peer transactions can be done in secret, without the interference of any third party such as a bank (charging the peers).

To eliminate these intermediaries and 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 [1] 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 [1]. 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 such as a bank to mediate, because digital assets can be copied to any extent. A particular difficulty associated with providing a trust model in a decentralized digital transaction system or network can be illustrated by the Byzantine Generals' Problem [2]. Bitcoin apparently solves this 'lack of trust' problem with its implementation of blockchain, which is based on a decentralized trustless P2P network. Here, a solution for the consensus (i.e. the majority of generals agreeing to attack) mechanism could be provided through the implementation of blockchain technology, an approach based on cryptography that enables the decentralized system (e.g. Bitcoin) to function successfully without any third party.

In this paper, it is studied how Leftover Foreign Currency (LFC) exchange between peers can be accomplished using a semi decentralized network based on blockchain, where the blockchain's cryptography based consensus mechanism provides the security and trust without the third party, e.g. a bank's currency exchange service.

II. BACKGROUND RESEARCH

International travel is increasing with a jump of 20% reported in travel weekly for 2015 [8]. Along with this rise in international travel is a consequential increase in the amount of LFC. For example, research from Zopa suggests that British travellers alone have an estimated £2.9bn of LFC lying around across the UK [4]. Scaling this problem up globally reveals a significant amount of global wealth lying around in travellers' wallets, purses and drawers at home! A cost effective and efficient solution is needed to exchange both small amounts of cash and larger digital LFC to bring these potential billions of LFC back into the global economy.

The most common ways of disposing of LFC are exchanging it through an agency or bank, shopping at the airport, donating it to charity, exchange with friends, retain as souvenirs, or exchange via a buy back guarantee. However, physically visiting a bank for exchanging cash on a day when the exchange rate is favourable is often not convenient. Furthermore, travellers may not want to go to an exchange bureau to exchange cash based LFC if they do not consider the amount significant. In cases where the original transaction that provided the destination country's currency has a buy back guarantee, the LFC can be sold back at the same exchange rate

978-1-5090-5443-5/17/$31.00 ©2017 IEEE

[3]. Again, this may not be applicable to coin based LFC. Further, if a person visits multiple countries in a single trip, upon return they may have a combination of different currencies in their LFC such that the buy back guarantee will not work for all of them. In addition, coins are often not accepted by most of the exchange bureaus and even if they are accepted, these coins must be of a certain currency type and have a value greater than a specific denomination, for example, coins having value greater than or equal to 1 GBP. Not all travellers may be willing to use their LFC for donation, shopping or as souvenirs.

Recently, a number of new systems have come onto the market that allows cash based 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 key challenge, particularly for small amounts of cash based LFC is to efficiently physically deposit the cash into a digital system. However, FourEx and TravelersBox are already addressing this challenge.

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 first method needs users to transfer money from their bank accounts to the P2P exchange system and then match and exchange directly with a peer requiring currency in the opposite direction [9]. A key advantage of the P2P currency exchange is the ability for peers to decide the exchange rate, even if it is as simple as exchanging at the rate the peers originally bought the currency or agreeing on a standard advertised rate. However, if the amount is too small or too big, it would be difficult to obtain a match thus forcing the customers to opt for a higher exchange rate than anticipated. Also, this does not act as a payment medium [10]. These systems 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 [1], facilitating a decentralized P2P communication utilizing a shared distributed time-stamped ledger that is updated based on consensus between the participating nodes. Bitcoin [1], Stellar [5], A.I.Coin [6] 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.

III. REQUIREMENTS

In order to enable travellers to use their LFC productively taking into account the issues and challenges described above, a mobile P2P LFC application (app) is essential with the following specific functional and general requirements.

A. Specific Functional P2P LFC App Requirements

A basic set of P2P LFC app requirements are envisaged:

1) Login —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. Standard kiosk login, same as the mobile login, should also be available.

2) Deposit — User should be able to deposit cash LFC at the smart kiosk and get a receipt for the transaction. The money deposited will get added to their multi-currency account.

3) Check Balance — User must be able to check their currency balances upon logging into the application.

4) Exchange — 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 if any other user exchanges currency at their advertised rate. The currency balance will be updated to reflect the exchange. An open published rate would automatically get adjusted the next day based on updated mid-market rates. In case, the user does not want to select or publish an exchange rate, there would be provision for auto-exchange where the system would allow exchange based on a system decided exchange rate.

5) Donate — It is usual to offer the option to donate currency to charity. There will be an auto-charity option that if turned on, would donate any fractional currency balance less than a unit automatically to charity.

6) Shop — The user will be able to buy articles from participating merchants with their LFC.

7) Transfer — A user should be able to transfer selected currency balances to their bank account or the accounts of friends and family.

8) Friends — A user should be able to search, invite, add, and delete friends from the application.

9) Withdraw — Users should be able to withdraw available currencies in their accounts from smart kiosk.

10) View History — This allows a user to 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.

11) Recharge Account — Users should be able to recharge the multicurrency P2P LFC account by transferring money from their bank account.

B. General Functional P2P LFC Requirements

The P2P LFC framework will enable users to deposit currency and then wait for a profitable rate and exchange with a peer — note that a profitable rate could simply be the rate at which they originally purchased their LFC.

978-1-5090-5443-5/17/$31.00 ©2017 IEEE

Unlike existing systems for cash currency exchange where users cannot select the exchange rate, in this system, users can select the exchange rate. Also, users do not need to visit an exchange agency to exchange their cash LFC. Instead, they can wait for a suitable rate after depositing in a smart kiosk (e.g. Fourex) their cash LFC and exchange when the preferred rate is available. User can also publish their preferred rate and wait for someone to exchange.

Cash currencies in the form of both notes and coins should be acceptable. Upon depositing currency in the kiosk the kiosk or users P2P LFC app will display the total amount entered, both notes and coins, and add this amount to the user's multi-currency account. Similarly, during withdrawal of currency from a kiosk options to pay for the requested currency from the users' multicurrency account will be provided. No cryptocurrency is required for such an application.

The LFC framework will exploit distributed ledger technology (blockchain) to maintain the users' credentials and all transactions. Algorithms such as SHA256 can be applied to users' credentials such that their passwords cannot be recovered from the encrypted value and a match is found by applying SHA 256 algorithm to the user provided password against a username. If a correct password is entered, the encrypted value would match with the one stored against the same username in the ledger. Such a blockchain would be permissioned with restricted read and write access.

Any advertised open exchange rate can be maintained on the blockchain. All currency exchanges would be accomplished via smart contracts and private-public key cryptography and recorded in the blockchain. A user can use their private key to sign off the exchange transaction and transfer amount to someone through the latter's public key. Additionally, any deposit, transfer and withdraw type transactions of cash LFC can also be governed by a smart contract and recorded in the blockchain. The history of all exchanges, donation and shopping can be stored and made available through blockchain technology. Other details such as list of friends of the user can be maintained in the blockchain as well.

While the operation of smart kiosks cannot be decentralised as the fiat currency refill and collection from the smart kiosks has to be governed by some kind of human based ecosystem similar to FourEx or TravelersBox, transactions such as transfer or exchanges or preferred rate publishing can follow a trustless decentralized approach. It should also be noted that a blockchain and smart contract based LFC framework using a mobile app with NFC payment functionality like Apple Pay could function in a decentralised P2P manner taking care of LFC left in the digital system — we often return from travel abroad with LFC on a travel currency card, for example.

IV. Proposed System

In this section, we outline a cash based LFC exchange model that follows a P2P exchange framework utilizing Internet of Things (IoT) (for interconnectivity), smart kiosks (for deposit and withdraw), blockchain (for financial ledgers) with certain aspects of the system centrally controlled and regulated.

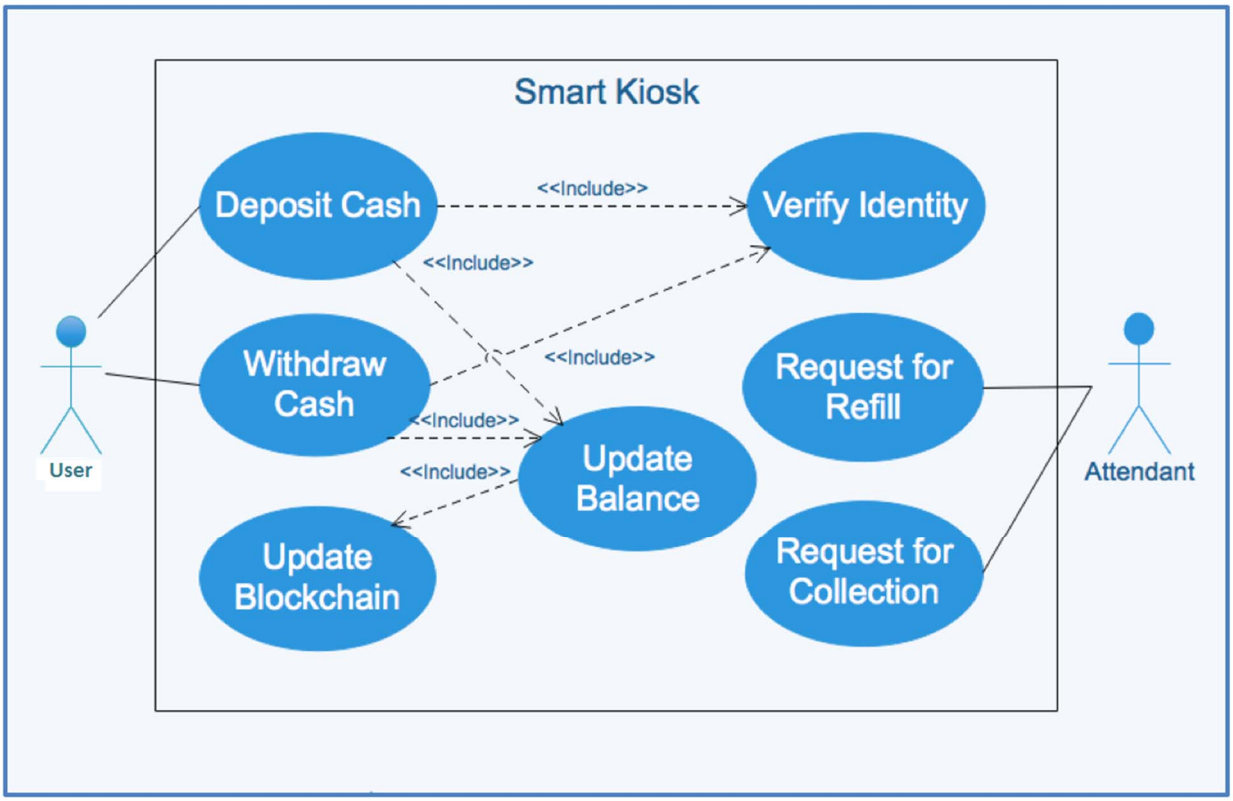

Fig. 1. Smart Kiosk Use Case Diagram

978-1-5090-5443-5/17/$31.00 ©2017 IEEE

Figure 1 illustrates the proposed smart kiosk use case where a user can deposit or withdraw cash from the smart kiosk that would lead to updating of the balance in the user's multicurrency account. This would also require updating of the blockchain with the transaction. Smart kiosk operation such as refilling, collection of cash, maintenance is anticipated to be part of a Fourex type ecosystem, beyond the scope of this research and likely to be simulated as the research progresses.

In Figure 2, we illustrate the use case for a mobile distributed application where the user needs to login to the distributed mobile app and check their balance. They can select currency type, amount and check available exchange rates and then decide to exchange or publish at their own rate. Exchanges as well as advertised rates will be subsequently updated in the blockchain.

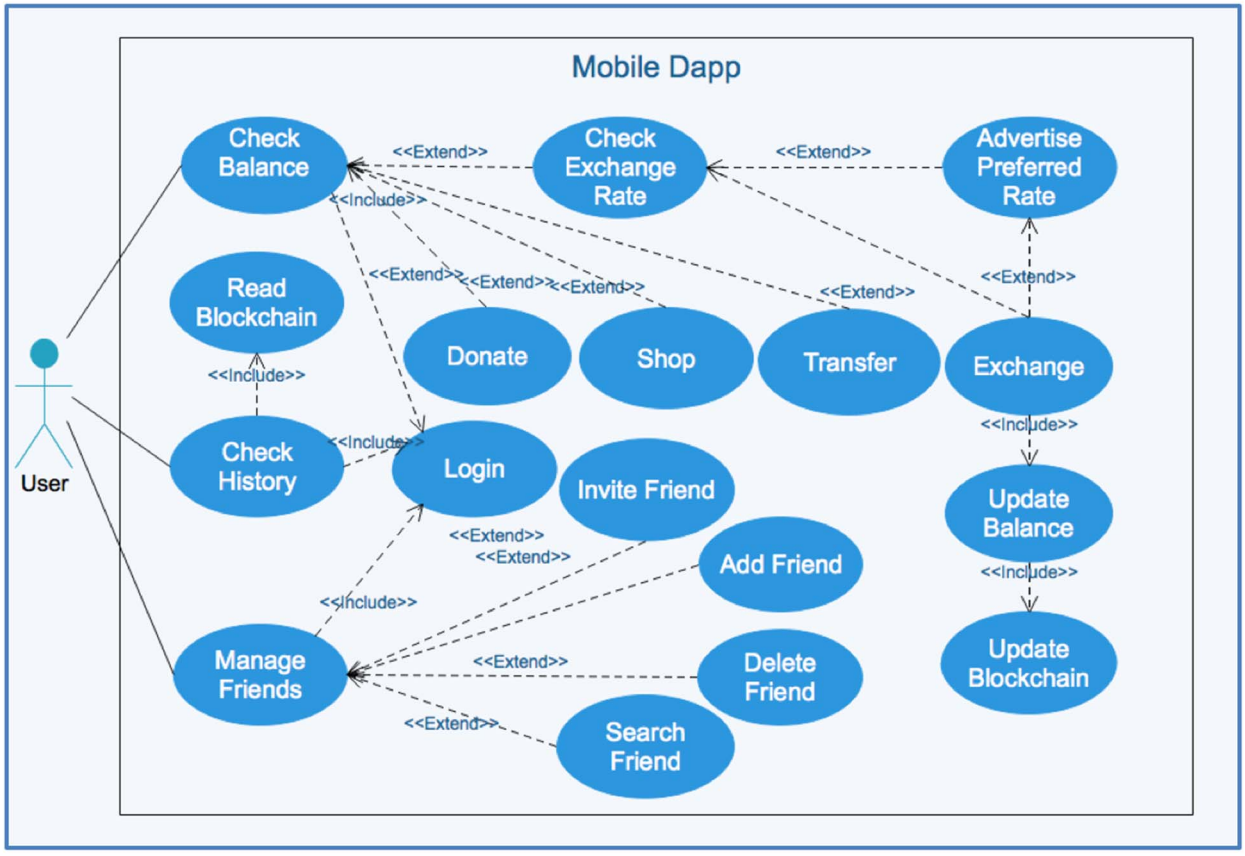

Fig. 2. Mobile distributed application

User can also decide to donate, shop or transfer with their P2P LFC app. Each activity would be recorded in the blockchain. Later on, user can check history of exchanges, open advertised rates, money donated or spent for shopping or transferred to a bank account by reading from the blockchain. User can also search for friends, add, delete or invite friends from Social Networking Sites such as Facebook.

V. Observations on Blockchain Development

Our work so far is focused on defining the requirements as discussed above and experimenting with blockchain and smart contract development at the backend. Figure 3 illustrates our architecture approach, which also indicates the development environments.

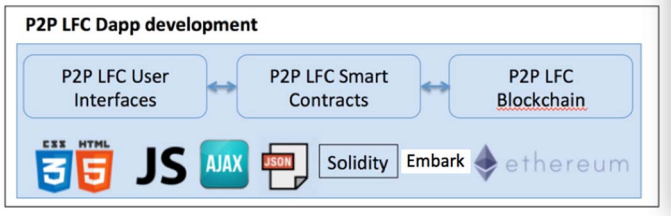

Fig. 3. P2P LFC Exchange Architecture

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. Our observations

978-1-5090-5443-5/17/$31.00 ©2017 IEEE

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. In addition, exchanging currency requires money first to be converted to Ether and then to the target currency. Besides this, the 'Verify Identity' use case in Figure 1 leads to certain queries. For instance, shopping necessitates identity verification but that would insert centralization in the application instead of a P2P approach.

VI. CONCLUSION

In this paper, we presented a proposal for a new P2P LFC exchange framework exploiting blockchain technology that could solve or alleviate the challenges of bringing left over foreign currency back into circulation. While this system, as described, cannot be operated as a completely decentralized P2P network because, for example, smart kiosks for depositing cash based LFC has to be provided and managed. As the number of users participating in the system increases, exchange rates should become more competitive such that the user may choose from a list of exchange rates and amounts. Ideally, the system we described requires the user to deposit LFC at the smart kiosks before departing from the country because LFC will not be accepted if smart kiosks present in the destination country are configured, for efficiency, only to accept currency local to the country where they are placed.

One solution can be using multi-currency kiosks similar to the ones designed by FourEx [7] accepting multiple currencies and allowing money to be withdrawn in specific local currencies.

The main advantages of the system proposed lie in its ability to exchange cash based LFC with easy money submission and withdrawal processes. As every cash transaction is governed by identity verification, and recorded on the blockchain, the range of money exchanged can be substantial without the risk of money laundering.

The main purpose of this paper is to provide a basis for future research in the area of P2P LFC utilization. There are a number of research questions that can be explored such as the possibility of making this application completely P2P and trustless, which we assume is not feasible at the moment. Additionally, how do we overcome the constraints of blockchain development as identified in section V?

Our subsequent endeavours would also include the construction of the system on a prototype level with in-depth evaluation and address these queries. In this regard, we have started development on the IBM BlueMix. Our future attempts would include building up the P2P LFC exchange application based on blockchain leveraging the blockchain service in Bluemix.

ACKNOWLEDGEMENTS

We would like to acknowledge American Express Technologies UK for their support and partial sponsorship of this research work.

REFERENCES

[1] Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System." 12 11 2015 <https://bitcoin.org/bitcoin.pdf>.

[2] Leslie, L., Robert, S., and Marshall, P. "The Byzantine Generals Problem." ACM Transactions on Programming Languages and Systems 4.3 (1982): 382-401.

[3] Jackson, R. (2015, 7 8). Leftover foreign currency: what to do with it. Retrieved 10 30, 2015 from THE WEEK: http://www.theweek.co.uk/prosper/60131/what-to-do-with-leftover-foreign-currency

[4] Cable, S. (2014, 9 30). Britons hoarding £3 BILLION in unused foreign currency at home, with just 13% bothering to exchange money after a holiday. Retrieved 11 23, 2015, from MailOnline: http://www.dailymail.co.uk/travel/travel_news/article-2774741/Britons-hoarding-3BILLION-unused-foreign-currency-home-just-13-bothering-exchange-money-holiday.html

[5] How Digital Money Works. Retrieved 1 13, 2016 from Stellar: https://www.stellar.org/learn/

[6] About A.I. Coin. Retrieved 11 1, 2015 from AI COIN Artificial intelligence: http://www.ai-coin.org/

[7] Fourex world money exchange. Retrieved 11 1, 2015 from Fourex World Money Exchange: http://www.fourex.co.uk/

[8] Tunney, D. (2015, 8 17). International trips on the rise, but air travel dropping. Retrieved 11 23, 2015, from TRAVEL WEEKLY: http://www.travelweekly.com/ConsumerSurvey2015/International-trips-on-the-rise-but-air-travel-dropping

[9] Support Centre. Retrieved from CurrencyFair: https://www.currencyfair.com/support/centre/

[10] Narasimhaiah, N. and Sam, R. P. (2015). Emerging Rails and Cashless Payments. International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering. 66-76.

978-1-5090-5443-5/17/$31.00 ©2017 IEEE