2018 International Conference on Computing, Power and Communication Technologies (GUCON)
Galgotias University, Greater Noida, UP, India. Sep 28-29, 2018

An Interoperable and Secure E-Wallet Architecture based on Digital Ledger Technology using Blockchain

Karan Singh
Computer Science Engineering
Bennett University
Greater Noida, India
karansinghkachwah@gmail.com

Nikita Singh
Computer Science
Banasthali University
Banasthali, Rajasthan, India
nikitasinghk@gmail.com

Dharmender Singh Kushwaha
CSED
MNNIT Allahabad
Allahabad, UP, India
dsk@mnnit.ac.in

Abstract- **Governments and financial Institutions worldwide are in deep need to reduce the payment, clearing and settlement cycles of various transactions thereby eliminating operational and financial inefficiencies and mitigating risks. Various consortia have been formed in order to lay the foundation stones, standards to create industry acceptable solutions. Seamless transactions and information sharing between different banks and financial institutions is still a distant dream. This paper presents a novel architecture to seamlessly integrate e-wallets of different banks and participating institutions using blockchains that shall act as a foundation of Digital ledger technology (DLT) for financial sector in India. A swarm based peer-to-peer network is designed for the proposed e-wallet system. The proposed solution shall minimize the load on the Core Banking Solution of the banks thus reducing the load on the servers at the data centers.**

Keywords- E-Wallet, Blockchain, Digital ledger technology, Core Banking Solution, Peer to Peer Network

I. INTRODUCTION

Currently all the banks have their own Core Banking Solution (CBS) for their operation needs. For this, each bank has to maintain a huge data center with expensive skilled manpower requirements. These data centers consume large energy, thus contributing to increased carbon emission. All the inter-bank transaction incur load on the CBS of the two involved banks, thus increasing the load further. As such, petty cash digital transactions are done for day today needs and transactions involving large sum are only few in number. If all the petty cash transactions can be moved out of the CBS to blockchain architecture, the load on CBS shall substantially reduce. Also the clearing time shall reduce to nearly real time.

As of date, banks in India don't allow inter e-wallet transactions. Hence, there is a dire need to provide this inter-operability that shall provide customers with agility too.

II. STATE-OF-THE-ART

Satoshi Nakamoto, the researcher who laid stone for bitcoin has proposed that "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution" [4]. Ober et al. [7] propose that for any bitcoin participant, it makes no difference if it receives a bitcoin that once belonged to him or from any other

participant as long as the amount of bitcoins remains the same. Authors in [8] discuss about transacting with shared bitcoins. Moser [9] proposes that mixing of services can use the concept of a shared wallet and increase anonymity of transactions. Zheng et al. [5] presents a comprehensive overview on blockchain technology and its architecture. They compare some typical consensus algorithms used in different blockchains besides technical challenges and recent advances are briefly listed [5].

Caytas [11] discusses about simplifying the payment transfer mechanism and clearing system. He proposes the use of private blockchains. The author discusses legislative and policy challenges. It is proposed that pre-selection of participant's enables additional access limitations for security and other purposes. Rapid digital innovations in banking and finance sector that is loosely termed as "fintech", has been able to attract attention of financial sector. Distributed ledger technology (DLT) is one such innovation that is evolving. It is perceived as a means of transforming payment, clearing, and settlement (PCS) processes. This includes how funds are transferred and how securities and derivatives are cleared and settled [1]. Dhar et al. [10] propose that "Financial sector innovations involving technology-enabled business models that can facilitate disintermediation; revolutionize how existing firms create and deliver products and services; address privacy, regulatory and law-enforcement challenges; provide new gateways for entrepreneurship; and seed opportunities for inclusive growth".

DLT (also known as blockchain technology or distributed database technology) has attracted significant interest and funding in the financial services industry in recent years. Several large financial institutions have established dedicated teams to explore the technology, and some market participants have formed consortia to create industry standards. According to a 2016 report by the World Economic Forum, over the past three years more than $1.4 billion has been invested in this technology to explore and implement uses in the financial services industry" [2]. India's largest lender State Bank of India will roll out beta launches of blockchain-enabled smart contracts by next month, according to Sudin Baraokar [3], head of innovation, SBI. Blockchain-enabled Know Your Customer (KYC) will soon follow suit. These applications are part of BankChain, a community of 27 banks, which have joined hands to explore and build blockchain solutions for banking [3].

The above discussion about the various research proposals in the recent past establish a need for a comprehensive architecture based on Digital Ledger Technology using Blockchain for the banking and financial

industry. The next section discusses our proposed architecture for "An Interoperable and Secure E-Wallet Architecture based on Digital Ledger Technology using Blockchain".

III. Proposed Architecture

Currently, cash transfer between two different e-wallets is not allowed in India. An architecture to solve this issue along with Blockchain based DLT architecture is proposed in this paper. Figure 1 illustrates an architecture wherein three different banks are arranged as peers over a network. Each of these banks provides an e-wallet to its customers. Each of the banks has one or more miner. This miner is a high end computation server that is granted access to certain attributes of the customer table in the central database of the bank. Each of the banks has definite trust agreements with each other. The idea is to use Proof of Stake (PoS) as consensus mechanism. Since the banks agree to collaborate, each of these shall ensure that any malicious activity shall directly or indirectly harm their own database and transactions.

IV. Network Architecture

The proposed network architecture is swarm based peer to peer network. Each of the participating banks shall have certain number of miners. These miners can be considered as super nodes that shall be persistent (permanent) and fault tolerant. Any customer seeking e-wallet from his bank shall be provided with the network address of all the miners. This customer shall send the join message to the miners. During registration process, a public key and a private key shall get generated. This public key gets updated with the miner.

When any offline customer becomes live for performing any transaction, the e-wallet app shall get synchronize the cashbook of the customer with the entries of the Blockchain.

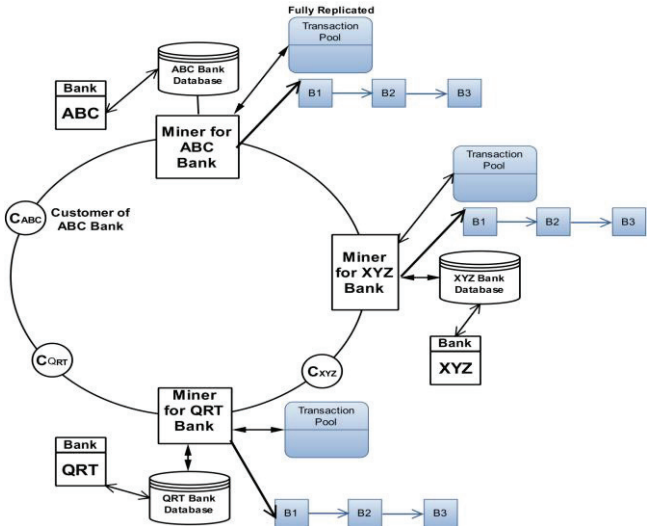

Fig. 1. Architecture illustrating bank , miner and e-wallet

A transaction in this work represents a cash or amount or payment that is digitally signed with the private key of the initiator who is making payment or vice versa with the use of its public key specified in the transaction [6]. Miners record these transactions in a Blockchain and carry out the task for the following three major scenarios:

a) Transferring cash from home bank account into the e-wallet,

b) Transfer of cash between two different e-wallets and

c) Transfer of cash from e-wallet to bank account.

Implementation and architecture for each of the above listed three scenarios is discussed in detail here.

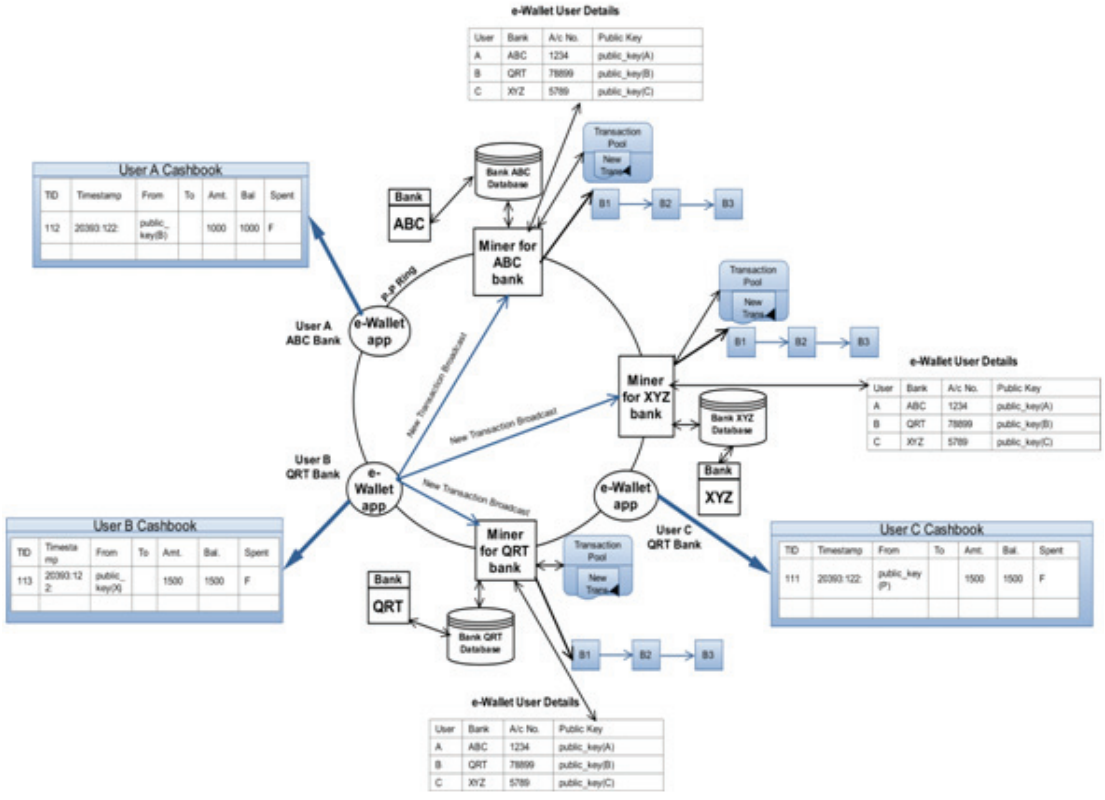

Fig. 2. Generation of transaction forTransferring cash from bank account into e-wallet

A. Transfering cash from home bank account into the e-wallet

When a client transfers cash from his home account into the e-wallet, a transaction is generated as shown in figure 2, and the same is multicast to each of the miners. This transaction gets placed in the transaction pool. This is also placed into transaction pool. This scenario is illustrated in figure 2.

As evident from figure 3, each of the miners has certain number of transactions in the transaction pool. Depending on the size of the block chosen, any miner can initiate the task of creating the new block with certain number of transactions.

Let a client having wallet of QRT Bank (CQRT) initiate a transaction to transfer Rs. 1000=00 to ClientABC having wallet from ABC Bank. The various steps involved at the miners end before it becomes an immutable content of a block (to be appended into the block chain) are:

a) The miner uses the public key of client to trace the previous blocks of the blockchain to ascertain whether the client has Rs. 1000=00 in his wallet. This amount is deducted from the account balance of the client.

b) The miner searches the blockchain for the current balance of client ClientABC and adds Rs. 1000=00 to its balance.

Similarly, other pending transactions in the transaction pool are verified and a new block is created and appended to the blockchain as shown in figure 3. This newly created block is multicast to all the miners. All these miners append this block B4 to the existing blockchain. The same is illustrated in figure 4.

Transfer of cash from e-wallet to bank account

Each client has a cash book in its e-wallet app that maintains all valid transaction details (credit and debit) of that user. When this client say Punpun of ABC Bank wishes to transfer some cash into his savings account (for cash withdrawal), the Miner of ABC bank shall specify all those credit transaction id from where he has received the amount.

Referring to the cash book as shown in figure 5, the client wishes to transfer Rs. 10,000=00 from his e-wallet to bank account. Bitcoin makes use of the concept of "unspent transaction output" while spending or receiving bitcoins [12].

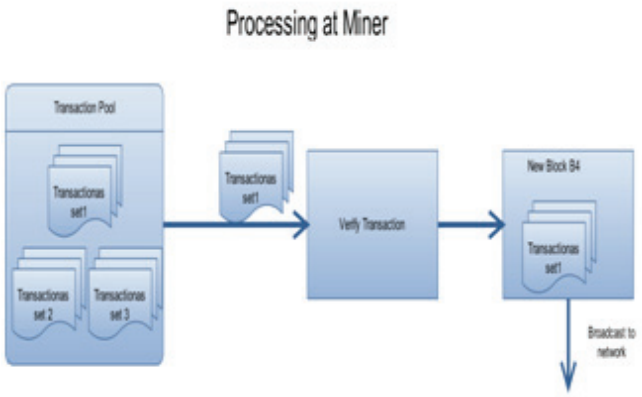

Fig. 3. Creating a new block

When certain amount has to be spent or transferred to some other wallet, it selects transactions of sufficient value that satisfies the amount we want to send and thus creates two new transaction outputs comprising of one for the receiver and one for the change we receive back to our wallet.

The change becomes a new Transaction Identifier (TID) in our wallet. Referring to figure 5 and figure 7, attribute "Spent" represents whether the amount listed in transaction is spent with flag T (true) or unspent with flag F (false).

These flags are used for verification of valid transactions and avoiding double spending.

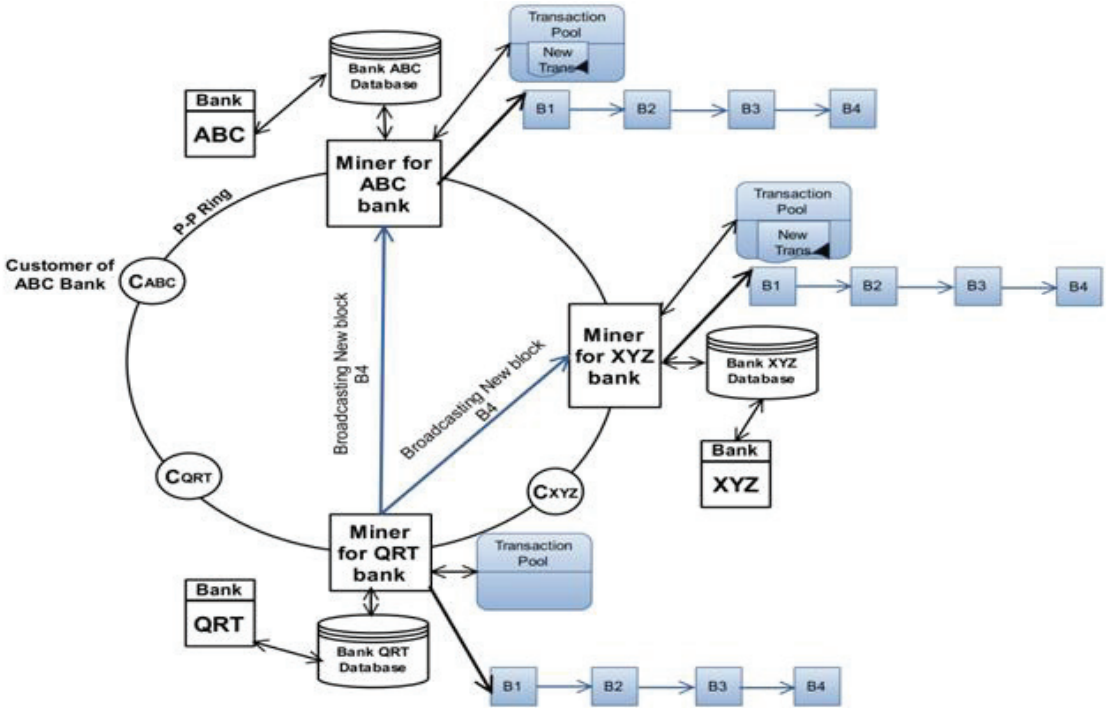

Fig. 4. Adding a new block to existing blockchain

So id 242 (the latest transaction) showing Rs. 6000=00 is selected but shall not suffice. Hence clubbing of id 236 (previous to the last one) fulfills the requirement of Rs 10000=00. Rs. 6000=00 shall be withdrawn from the concerned bank of transaction id 242 and Rs. 11000=00 from id 236. The same is illustrated in figure 6.

Miner of ABC Bank shall identify the details of these two transactions and following actions shall be performed:

a) Receivables and liabilities shall be intimated to CBS (Core banking Solution) of transactions involving these two banks. The CBS shall perform the required action.

b) The Miner shall perform Account to e-wallet transaction of surplus Rs. 7000=00 to be transferred from the home bank of id 236.

c) Cash book of Punpun shall show id's 236 and 242 as spent and

d) A new Transaction id gets added stating that Rs. 7000=00 has been transferred from the home bank of id 236 with a new transaction id 244.

User Punpun Cashbook

TID	Timestamp	From	To	Amt.	Bal.	Spent
123	2017:12:02 :	public_key (A)		2000	2000	F
170	2018:01:01	public_key (B)		7000	9000	F
236	2018:01:05	public_key (C)		11000	20000	F
242	2018:01:10	public_key (A)		6000	26000	F

Fig. 5. Cashbook details before transaction

B. *Transfer of cash between two different e-wallets*

When any client makes any payment to other person having e-wallet of some other bank or receives payment, a transaction is generated and is multicast to all the miners. This scenario is discussed in this section.

TID	Timestamp	From	To	Amt.	Spent_trans.
243	2018:01:15	Public_key (Punpun)	A/c	17000	236,242
244	2018:01:15	A/c	Public_key (Punpun)	7000	

Fig. 6. Current transaction processing

At the application level, a client may wish to transfer or make payment from his e-wallet to any other e-wallet, as illustrated in figure 8.The client shall select the public key of the beneficiary, amount and those unspent transaction ids such that the amount is equal to or more than the amount to be spent. The procedure is same as the one discussed in section "Transfer of cash from e-wallet to bank account".

V. IMPLEMENTAION

The proposed e-wallet system is implemented using interplanetary file system (IPFS) [13]. IPFS is the open source decentralized hypermedia protocol that is designed to create content based peer-to-peer network. IPFS provides the functionality of distribution of file in form of blocks. This facility can be extended to designing of blockchain network. In IPFS each block is addressed by its SHA-256 hash value thus each block is immutable. By using IPFS a swarm based peer-to-peer network can be designed for proposed e-wallet system.

User Punpun Cashbook

TID	Timestamp	From	To	Amt.	Bal.	Spent
123	2017:12:02 :	public_key (A)		2000	2000	F
170	2018:01:01	public_key (B)		7000	9000	F
236	2018:01:05	public_key (C)		11000	20000	T
242	2018:01:10	public_key (A)		6000	26000	T
243	2018:01:15	Public_key (Punpun)	A/C	17000	9000	T
244	2018:01:15	A/C		7000	16000	F

Fig. 7. Updated cashbook after Transfer of cash from e-wallet to bank account

In the proposed implementation each type of node of the system i.e. miner, e-wallet app has to implement IPFS as core level that forms IPFS swarm. The verified transaction is kept in blocks implemented as a file. Each block shall contain SHA-256 hash value of previous block along with the list of transaction. This is recorded in Inter-Planetary naming System (IPNS).

VI. CONCLUSION

A Common Secure E-Wallet Architecture based on Digital Ledger Technology using Blockchain has been proposed in this work. The proposed architecture is first of its kind for implementing blockchain architecture for e-wallets. It also introduces the architecture for inter-operability between e-wallets from different banks or entities. The proposed solution shall minimize the load on the CBS of the banks, reduce the load on the servers and decentralize the processing activities thus harnessing the idle capacities at other centers.

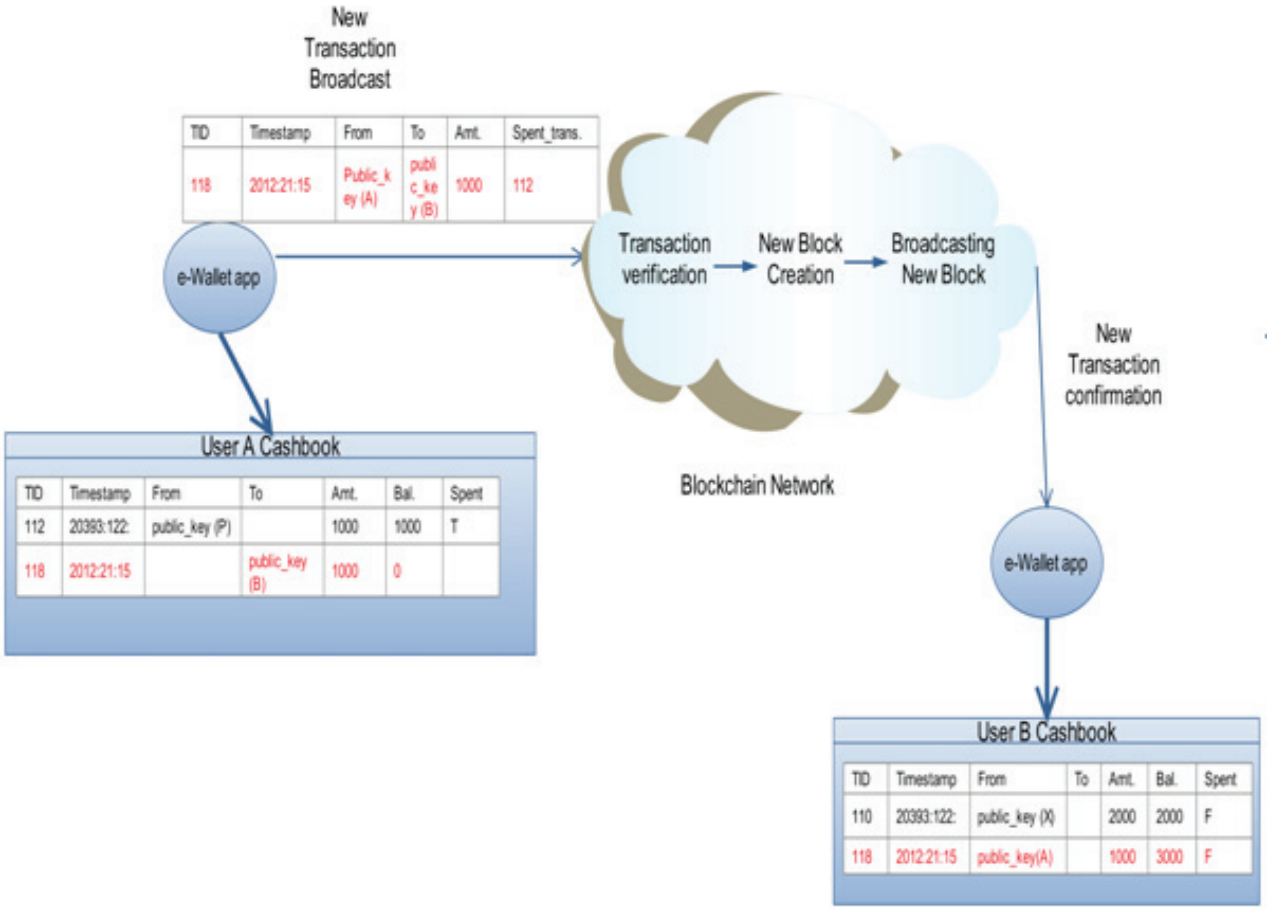

Fig. 8. Scenario illustrating transfer of cash between two different e-wallets

REFERENCES

[1] D. Mills et al., "Distributed ledger technology in payments, clearing, and settlement," *Finance and Economics Discussion Series 2016-095*. Washington: Board of Governors of the Federal Reserve System, https://doi.org/10.17016/FEDS.2016.095.

[2] The Financial Industry Regulatory Authority Report, http://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf, January 2017

[3] http://economictimes.indiatimes.com/articleshow/61715860.cms?utm_source=contentofinterest&utmmedium=text&utm_campaign=cppst, November 2017.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system, 2009," 2012. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[5] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang., "An overview of blockchain technology: Architecture, consensus, and future trends." *In 2017 IEEE International Congress on Big Data (BigData Congress), 2017* Jun 25 (pp. 557-564). Honolulu, USA, DOI: 10.1109/BigDataCongress.2017.85

[6] https://en.bitcoin.it/wiki/Transactions (visited on 05/28/2013).

[7] M. Ober, S. Katzenbeisser, and K. Hamacher., "Structure and Anonymity of the Bitcoin Transaction Graph". *Future internet*, 5(2):237–250, May 2013.

[8] http://blockchain.info/de/wallet/send-shared (visited on 05/31/2013).

[9] M. Möser , "Anonymity of Bitcoin Transactions" , An Analysis of Mixing Services . *Münster Bitcoin Conference (MBC),* 17–18 July '13, Münster, Germany.

[10] V. Dhar and R. Roger, "FinTech Platforms and Strategy " MIT Sloan Research Paper No. 5183-16. Available at SSRN: https://ssrn.com/abstract=2892098 or http://dx.doi.org/10.2139/ssrn.2892098

[11] J. Caytas "Developing Blockchain Real-Time Clearing and Settlement in the EU, U.S., and Globally" *Columbia Journal of European Law* 2016). Available at SSRN: https://ssrn.com/abstract=2807675

[12] https://www.ccn.com/bitcoin-transaction-really-works/.

[13] https://raw.githubusercontent.com/ipfs/papers/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf