

Offline Rig - Offline and Cashless Payment

Hari. R,
Department of Computer Science,
SRM Institute of Science and Technology,
Chennai, India

D. Punitha,
Department of Computer Science,
SRM Institute of Science and Technology,
Chennai, India

Abstract—The study of a new form of payment that is both cashless and offline and yet tackles the problems of black money and is very secure, is what is introduced here. We can call this an open loop, stored value card system. The aim is not to replace cash or banks which we can never do. Every user is registered and given an NFC card, and a respective pin code. This card can be in any form like a credit card, or also simply a ring. This card performs the same role as a wallet performs to cash. The difference here is that this wallet is highly secure and money can be taken out only by the owner of the money. The money is stored inside the card in the form of an electronic record. We will store Rupee directly in the card. Money is transferred into the card from the bank, using an ATM like device that uses Internet connection. After the withdrawal, the amount is stored in the card locally (no database online). The transaction needs to have a third party (a POS device). This transaction would be both offline and cashless. The whole transaction also happens in a cryptographically secure way that there can be no hacking possible. The Internet is needed only for getting money from the bank (withdrawal). (abstract)

Keywords—Offline payment, cashless payment, NFC payment (key words)

I. INTRODUCTION

Money [3] is an essential part of any human civilisation. In the earlier days, we had the barter [4] system. Here, people attribute some value to consumable items they have and exchange that to what they want. But this had many flaws. For instance, this will cause a cyclic dependency where one person wants rice, but is exchanging that with wheat and the person selling rice doesn't want wheat, but something else that the buyer does not have.

To avoid all of that, people introduced small objects and attributed value to it; called it money. This money could be anything. It had a temporary value, as it can't be consumed directly by the consumer. Instead, they could exchange this temporary value with any other object that the consumer can consume. Thus, this money forms a layer in the barter system. As time passed, money took a lot of forms, from metal coins to printed currency notes or temporary tokens.

Then people came with the idea of money banks. People could 'deposit' their money in the bank, and 'withdraw' the money any time later, thus making the bank a temporary store of their money. The bank also performs other operations like 'lending' money to people temporarily for an 'interest' amount. Soon, several money related crimes started happening (like counterfeit money [5], or black money [6] based operations). Also, people didn't pay taxes [7] properly to the government for all the income they had, and there was no way of finding out the actual income a person had. But when transactions happened within the bank, from one person to another (one account to another), we could easily track

exactly who pays what amount to which person. This data would be very critical for government agencies and the police to catch people who commit frauds. Therefore, transacting money from within the bank was made as the legal way of transacting money. The terms 'Black Money' and 'White Money' were introduced. 'White Money' is any money that the holder can prove the source, or the holder has paid his taxes. Some examples are withdrawal from a bank, or the money in the bank. 'Black Money' is any money that the holder cannot prove the source. This indicates that the money transaction that led to the money being in possession of the holder, is not accounted anywhere, and which means that the holder may also not pay an income tax for that amount (There wouldn't be any trace for the governments to find out that the holder has had that income). Thus avoiding black money is critical to functioning of the society. Wherever there is physical cash, there is always the danger of printing counterfeit cash.

On the other hand, the Internet is becoming very cheap and more accessible to everybody, and the idea of paying remotely through the internet picked off. Thus banks started offering an online and remote means of access. People could start to pay from one account to another account by accessing the bank through the internet. Banks also started to give 'credit' [8] cards and 'debit' [8] cards. These could be used by the consumer to access their bank accounts directly and pay to a merchant processing an POS [2] device that supports the reading of data present in the cards, through immediate loans, or through their bank accounts directly.

Virtual wallets like PayTM [9] also started to bloom. These are nothing but glorified banks again. They maintain a database with the amount of money present in every account and make it seem to us like a wallet. We can access this wallet from the internet through the applications developed by them. Thus, money in these cases takes the form of an electronic record. Upon giving and taking this electronic record, we exchange the temporary value of money, with which we can buy any consumable articles.

II. LITERATURE SURVEY

A. *Providing security for NFC based Payment Systems Using a Management Authentication Server [11]*

1. Provides a secure way of communication between POS and bank
2. Requires active Internet Connection and Database

B. *A Secure Lightweight and Fair Exchange Protocol for NFC Mobile Payment Based on Limited-Use of Session Keys [12]*

1. Lightweight algorithm for Secure information transfer

2. Requires active Internet

C. For Small Merchants: A Secure Smartphone-Based Architecture to Process and Accept NFC Payments [13]

1. Uses the processing power of smart phones and convenience
2. Requires Smartphone, which is an Active Device

D. KerNeeS - A protocol for mutual authentication between NFC phones and POS terminals for secure payment transaction [14]

1. The most flexible in the list and one of most secure
2. Requires Smartphone, Internet and a Database

E. Touch-based Magnetic Communication through Your Hand [15]

1. Provides an alternative method to passage of magnetic signals from NFC
2. This method increases security and convenience
3. The problem is that this does not guarantee that the payment will be offline or online

F. Overview of a Payment Solution for NFC- Enabled Mobile Phones [16]

1. Provides a better method than customer-merchant NFC payment method: payment between two NFC enabled smartphones
2. Still requires an active Internet connection
3. Also needs a cloud database

G. Swing-Pay: One Card Meets All User Payment and Identity Needs [17]

1. Provides a novel method of payment that enables NFC based active wallets that everybody can carry
2. Secured with a fingerprint scanner in each wallet. Each wallet can communicate with each other.
3. There is no need of any intermediate POS device
4. There is still a need for the Internet and customers need to maintain an active device with themselves.

III. EXISTING PAYMENT METHODS

Money and transactions, in the current state of this world, take the following forms.

Offline payment

- Cash

Online Payment

- Bank Account to Account Transfer
- Debit Card, Credit Card
- UPI
- Digital Wallets (Like PayPal [10], Paytm)
- Crypto currencies

A. Advantages

- a. Cash

Cash based payments do not require the internet or an electronic device. Any common man can have this as his mode of payment. This is also the most convenient for small transactions. If the holder is able to prove the source of the cash, the cash is called 'white' money. As the transaction happens truly offline, there can be no hacking possible. Since it is truly offline, nobody can track the transactions that a person makes, and therefore, transactions can be fully anonymous.

- b. Bank A/C transfer

This is one of the whitest and cleanest forms of money transfer. Stealing money from a bank is very difficult. Nowadays, with the internet boom, this is also one of the easiest modes of transfer of money. This is not geographically constraining upon the entities

- c. Debit/Credit Cards

Very similar to a bank account to account. But the only difference is that here, the transactions can happen only to a merchant and not peer to peer. The merchant needs to have a special POS (Point of Sale Device). The consumer need not have any active device with him.

- d. UPI

This is exactly the same as that of a Bank account to account transfer. The only difference is that the transactions happen almost instantly. Nobody needs to reveal anything about the bank accounts of any other details.

- e. Digital Wallets

These are also exactly the same as that of Bank Account to Account money transfer. These behave like a separate bank itself. They provide many new means of user interaction (Like QR codes). These also make sure that the personal details of the people involved in the transactions are not revealed. The consumer to merchant transactions also become really easy

- f. Cryptocurrencies

Provides total anonymity.

B. Disadvantages

- a. Cash

The main problem with cash is black money. Also, it is very difficult for the consumer to tender the exact change at the time of the payment. Another issue is that the cash can be easily stolen. If the holder is not able to prove the source of the cash, it is called 'Black Money'.

- b. Bank A/C transfer

It needs an active Internet connection, with any active device that is capable of accessing it. It also takes some time for the transaction to happen. The money based details of all the consumers are stored in the bank's database. So a carefully planned attack could erase all. Since the transaction happens online, even though the methods of protection and encryptions are on the rise, hackers will manage to hack money transactions. All the transactions are recorded and therefore, we do not have anonymity.

- c. Debit/Credit Cards

Needs an active Internet connection. The transactions can happen only to a merchant and not peer to peer.

- d. UPI

Needs an active Internet connection.

- e. Digital Wallets

Carries the same disadvantages of a bank to bank transfer

f. Cryptocurrencies

Needs an active Internet connection and is not easily accessible.

possible and the geographical constraint imposed is not avoidable.

IV. THE STUDY

A. Procedure

If 'A' wants to transfer some money to 'B', using the POS device, they can perform the transaction locally, offline and cashless, from card to card (wallet to wallet). This POS device that is built, also authenticates the payer as well as the payee's wallets by prompting for a pin code that would be given along with the card. Therefore, if the wallet gets stolen, nobody would be able to access the money inside. This method cannot be removed or changed, as otherwise we may need to create money out of nowhere and that would lead to a lot of problems. Just like physics says that energy cannot be created, we cannot create money. Instead, we transfer money from one form to another, or exchange it with something else with which we attribute the same amount of value.

First the payer would enter his pin and the money to transfer. Then the POS would store the money inside it. After the payee enters his pin and places his/her wallet in the POS, the money would be transferred to the POS to the wallet of the payee.

B. Setup

There are three parties involved in every transaction - Payer, Payee and the POS. As the payee and the payer carry passive wallets with them (NFC [1] cards), they need a POS device to ensure a communication between the wallets. Note that for this operation, the Internet connection is not required, as everything happens locally

The POS device must also allow for withdrawal and deposit of money from or to a bank. The POS also contains a display for users to view the status and a keypad for the users to interact.

a. C. Advantages

Compared to cash transactions, here are the problems that are solved. Black money is abolished. The reason is that money can only be stored in the wallets that are issued to people, and these wallets are given to people only after registration, to make sure that one person has only one wallet. These wallets have a top limit of the money that can be stored. Therefore, the person cannot keep storing data in the card as high as needed. Nobody can steal the money present in the card. This is because a transaction can be made only in the POS device that we have made, that too only after pin authentication. Every transaction is therefore pin authenticated

Compared to online transactions, here are the problems solved. This is offline, so secure. This provides to some extent anonymity to the user, yet ensuring there is no Black Money. Transactions happen locally, so there can be no hacking. There is no Database that has the list of all the money that a person has (so there is no central point of attack possible). The transaction is also instantaneous.

b. D. Disadvantages

The only disadvantage of this method is that there can be a transaction only in the presence of a 'POS' device. Though the device needs a very low power and can be powered by extremely simple mechanisms (even a solar panel, or a dynamo), transactions can happen only in places that have the POS. But since our problem statement is to provide Offline, yet cashless payment, there needs to be a presence of some electronic (active device), and so this is the best solution

REFERENCES

- [1] https://en.wikipedia.org/wiki/Near-field_communication
- [2] https://en.wikipedia.org/wiki/Point_of_sale
- [3] <https://en.wikipedia.org/wiki/Money>
- [4] <https://en.wikipedia.org/wiki/Barter>
- [5] https://en.wikipedia.org/wiki/Counterfeit_money
- [6] https://en.wikipedia.org/wiki/Indian_black_money
- [7] <https://en.wikipedia.org/wiki/Tax>
- [8] https://en.wikipedia.org/wiki/Debits_and_credits
- [9] <https://paytm.com/>
- [10] <https://www.paypal.com/>
- [11] Ali Al-Haj and Mayyadah Adnan Al-Tameemi, "Providing Security for NFC-Based Payment Systems Using a Management Authentication Server", 4th IEEE International Conference on Information Management, 2018
- [12] Chalee Thammarat, Werasak kurutach, "A Secure Lightweight and Fair Exchange Protocol for NFC Mobile Payment Based on Limited-Use of Session Key", 17th International Symposium on Communications and Information Technologies (ISCIT) 2017
- [13] Nour El Madhoun, Emmanuel Bertin and Guy Pujolle, "For Small Merchants: A Secure Smartphone-Based Architecture to Process and Accept NFC Payments", 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering, 2018
- [14] Ugo Biader Ceipidor, Carlo Maria Medaglia, Antonella Marino, Serena Sposato and Alice Moron, "KerNeeS - A protocol for mutual authentication between NFC phones and POS terminals for secure payment transactions", 9th International ISC Conference on Information Security and Cryptology, 2012
- [15] Arvind Allawadi, Kaikai Liu, "Touch-based Magnetic Communication through Your Hand", IEEE International Congress on Internet of Things, 2018
- [16] Deepali Kayande, Elsa Rebello, Shweta Sharma, Monica Tandel, "Overview of a Payment Solution for NFC- Enabled Mobile Phones", IEEE, 2016
- [17] Shirsha Ghosh, Joyeeta Goswami, Alak Majumder, Abhishek Kumar, Saraju P. Mohanty, Bidyut K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs", IEEE Consumer Electronics Magazine, 2017