Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8882655, 6 pages
https://doi.org/10.1155/2020/8882655

Research Article

Using the Same PayWord Chains Associated with a Single Account from Multiple Mobile Devices

Tao-Ku Chang[1] **and Fu-Hao Yeh**[2]

[1]*Department of Computer Science and Information Engineering, National Dong Hwa University, Hualien 97401, Taiwan*
[2]*Department of Information Technology and Management, Fooyin University, Kaohsiung, Taiwan*

Correspondence should be addressed to Tao-Ku Chang; tkchang@mail.ndhu.edu.tw

Received 15 September 2020; Revised 25 October 2020; Accepted 3 November 2020; Published 21 November 2020

Academic Editor: Zhili Zhou

Customer awareness and interest in mobile payments are increasing. However, security and privacy risks remain major barriers to their adoption, with customers worrying about their personal data being hacked or intercepted. In this paper, we present the design of a secure scheme for mobile payments that can guarantee mutual nonrepudiation between the customer, merchant, and banker. A customer can use the proposed scheme to make a payment with the same PayWord chains of a single account from multiple devices.

1. Introduction

Smartphones are being increasingly used to replace keys, cameras, and televisions, and further convenience would result from their use as tools for making payments. A mobile payment has been defined as "any payment where a mobile device is used in order to initiate, activate, and/or confirm this payment" [1]. Although large-scale mobile payment systems are still under development, several mobile financial and mobile commerce applications (e.g., the Starbucks app, iTunes, and Google Wallet) are encouraging more users to take advantage of the convenience they afford in making mobile payments.

Mobile payment technology can provide benefits to both customers and merchants relative to traditional payment methods [2, 3]. An electronic payment can be classified as either a macro- or micropayment depending on its amount. Macropayment schemes are used by most e-commerce websites, and they employ complex encryption techniques to conform with rigorous security requirements [4, 5]. In contrast, micropayment schemes only need low-overhead hashing functions and are suitable for specific mobile commerce applications associated with low-value and high-volume purchases [6, 7]. However, a major problem of micropayment schemes is implementing solutions that ensure authentication, nonrepudiation, and privacy. The development of mobile payments is further limited by the current high startup costs and complicated configurations.

Rivest and Shamir proposed a scheme called PayWord in 1996 that offered a more efficient scheme for micropayments [7], and many subsequently developed efficient micropayment schemes are based on it [8–12]. Until now, PayWord-based micropayment schemes have used PayWord chains of a single account from one device. However, since customers often use more than one mobile device, in the present study, we considered the situation where multiple client devices need to access PayWord chains associated with a single account. For example, consider a customer who has both a smartphone and a tablet. He/she generates hash-chain coins with his/her smartphone and makes payments with them. The inability to use the tablet to pay using the remainder of the hash-chain coins is inconvenient for the customer. This situation motivated us to design a scheme whereby customers can register the hash-chain coins of a single account and pay with them from multiple devices.

The remainder of this paper is organized as follows: Section 2 gives an overview of related work and technologies, Section 3 presents the proposed scheme for mobile payments, Section 4 presents a security analysis, and

conclusions about the work described in the paper are drawn in Section 5.

2. Related Work and Technologies

Many consumers now carry a smartphone more often than a wallet or purse. Moreover, it typically takes 5–6 hours for someone to realize he/she has lost a wallet, while only around 15 minutes typically passes before realizing that a smartphone is missing [13]. However, security and privacy risks are major barriers to the adoption of mobile payments, with customers worrying about their personal data being hacked or intercepted. Many people consider mobile transactions to be less secure than credit- and debit-card transactions, even though mobile payments can be equally secure or even more secure than traditional payment methods. When customers are offered a secure online payment environment that works via advanced mobile Web systems, they are freed from the burden of providing physical currency each time they want to make a mobile purchase or pay a bill online.

A survey performed by the Consumer Research Section of the Board of Governors of the Federal Reserve System revealed that more than half of customers believed that mobile contactless payments would become a major form of payment within the next 5 years, and more than one-third of the survey subjects indicated that they would use the method if it were made available [14]. Mobile payments are expected to become a mainstream payment method, with an Allied Market Research report projecting that their value will reach $12.06 trillion by 2027 [15].

Different types of mobile payments can be differentiated based on various characteristics, including the technology used and the transaction size, location, and funding mechanism [16]. The type of payment can be categorized into one of two types based on the underlying technology: proximity or remote payments. Proximity payments generally refer to contactless payments employing near-field communication [17–19], while remote payments are made via a mobile Web browser or a smartphone application, in which the smartphone is used as a device to authenticate personal information that is stored remotely. Such payments utilize services such as SMS (Short Message Service) to initiate or authorize a payment. The funding mechanisms for payments made in mobile payment systems have previously been differentiated into the following types: bank accounts, credit cards, and telecommunication company billing, or into an account, real-time, prepaid, postpaid, smart card, credit card, mobile POS, mobile wallets, and P2P payments [1, 16, 20, 21].

The increasing interest in mobile payments and commerce is also increasing the importance of privacy and security to customers, which continue to constitute major obstacles to widespread adoption. The specific security issues identified have varied between surveys. Some customer reservations about mobile payments stem from fears of payment account information being intercepted, the threat of unauthorized parties accessing personally identifiable information, and the receipt of unsolicited promotional material [14, 22]. A First Data mobile payments study found that more than half of the customers surveyed believed a smartphone payment to be less secure than payments made in person or credits [23]. Regardless of the specific reasons for these security concerns and their validity, security issues must be addressed in order to achieve the mass adoption of mobile payments.

3. The Proposed Micropayment Scheme

We present a new novel micropayment scheme based on using the same PayWord chains of a single account from multiple devices [6] in order to address the problem where a customer wishes to use multiple devices for payments and all of the involved entities can store attestations. The proposed scheme involves the following entities: a customer (C), merchant (M), and banker (B), which have the following public and private key pairs: ($pri(C)$, $pub(C)$), ($pri(M)$, $pub(M)$), and ($pri(B)$, $pub(B)$), respectively. $[O]_{pri(x)}$ and $[O]_{pub(x)}$ are used to denote a digital signature and the encryption of data object O that is generated by the private and public keys of a subject x, and data objects within square brackets that are separated by commas are first connected and then have cryptographic operations performed on them. Let $h(x)$ denotes a cryptographically strong hash function: calculating $y = h(x)$ is easy, whereas calculating the inverse $x = h^{-1}(y)$ is infeasible. ID_C and ID_M represent the identities of C and M. The scheme comprises three phases: a registration phase, a transaction phase, and a redemption and remittance phase.

3.1. Registration Phase. Figure 1 shows the following steps and message exchanges involved in the registration phase:

(1) C sends CSR = $[ID_C, IMEI]_{pub(B)}$ to B. Tell B the identity of C and the IMEI number of the device

(2) B decrypts $[ID_C, IMEI]_{pub(B)}$ using $pri(B)$ and registers a customer account with $[ID_C, IMEI]$, and then sends an ACK to C to indicate that the registration is successful

(3) C sends $PSR = [ID_C, ID_M, n, m, s, IMEI]_{pub(B)}$ to B. Tell B the identity of C and the $IMEI$ number of the device, and request three PayWord chains of M: E, F, and E^*, whose lengths are n, m, and s, respectively. B decrypts $[ID_C, ID_M, n, m, s, IMEI]_{pub(B)}$ using $pri(B)$ to obtain the customer's information. B checks if the $IMEI$ number of the device has already been registered and rejects the request if it has not been. If there are PayWord chains that are not redemptive or not expired in the customer's account, B sends the existing PayWord chains to C directly

(4) B generates PayWord chains E-chain, F-chain, and E^*-chain with two denominations, d_E, d_F, and d_{E^*} ($d_E < d_F$, $d_E = d_{E*}$), as follows:

$$\begin{aligned} E &= (e_0, e_1, e_2, \cdots, e_n), \\ F &= (f_0, f_1, f_2, \cdots, f_m), \\ E^* &= (e^*{}_0, e^*{}_1, \cdots, e^*{}_s), \end{aligned} \tag{1}$$

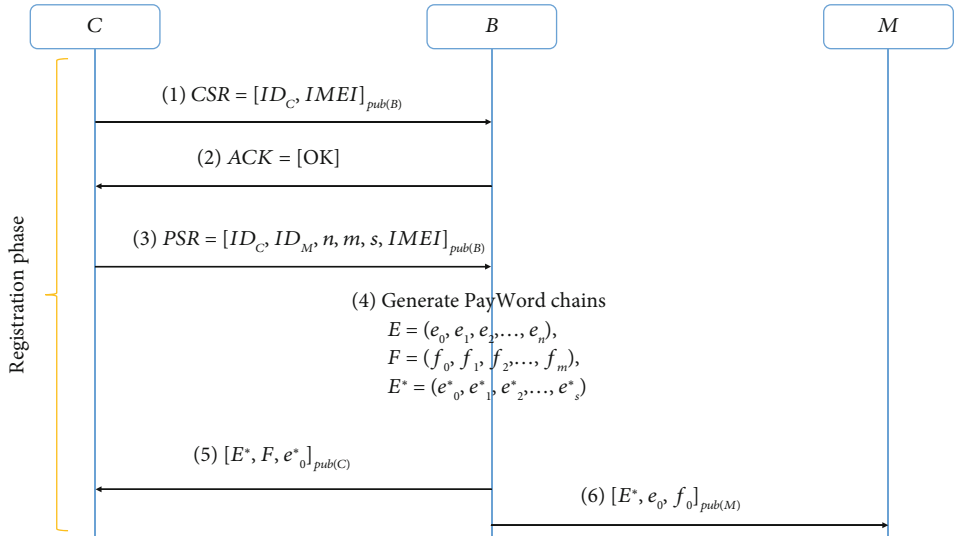

Figure 1: The message exchanges of the registration phase.

where

$$e_i \text{ satisfies } e_i = h(e_{i+1}),\ i = n-1, n-2, \cdots, 0$$
$$f_i \text{ satisfies } f_i = h(f_{i+1}),\ i = m-1, m-2, \cdots, 0$$
$$e^*_i \text{ satisfies } e^*_i = h(e^*_{i+1}),\ i = s-1, s-2, \cdots, 0$$
$$e_0 \text{ and } f_0 \text{ are anchors used by the merchant to verify each chain.}$$
$$e^*_0 \text{ is an anchor used by the customer to verify the return} - \text{change chain.} \quad (2)$$

(5) B sends $[E, F, e^*_0]_{pub(C)}$ to C. C decrypts this using $pri(C)$ to obtain PayWord chains E-chain and F-chain, as well as e^*_0, which is used to verify E^*-chain

(6) B sends $[E^*, e_0, f_0]_{pub(M)}$ to M. M decrypts this using $pri(M)$ to obtain return-change chain E^*. Note that the merchant should pay money for E^*-chain

3.2. Transaction Phase. In the transaction phase, it could be that the customer is using electronic coins for the first time, or that the electronic coins have already been used previously. The following steps (depicted in Figure 2) are involved when a customer wants to make a payment with E-chain and F-chain of the electronic coins.

(1) M tells C the total payment amount. C sends a payment message $[e_{p'}, f_{q'}, e_{p'+a}, f_{q'+b}, a, b]$ to M, where the numbers of coins obtained from E and F are "a" and "b," respectively, $e_{p'}$ and $f_{q'}$ represent the anchors of the last payment, and $e_{p'+a}$ and $f_{q'+b}$ represent the anchors of the most-recent payment

(2) M receives the payment message $[e_{p'}, f_{q'}, e_{p'+a}, f_{q'+b}, a, b]$. Check whether E-chain and F-chain have been used before by e_p and f_q. If they have been used before, check whether or not anchors ($e_{p'}$ and $f_{q'}$) from C are the same as those of the last payment. If the anchors are not the same, send $[e_p, f_q]$ to C, and C substitutes the anchors of E-chain and F-chain with e_p and f_q. Step 1 is then performed again. If the anchors are the same, verify that e_p is equal to $h^a(e_{p'+a})$ and f_q is equal to $h^b(f_{q'+b})$. M then substitutes anchors e_p and f_q with $e_{p'+q}$ and $f_{q'+b}$ to complete the payment

(3) M sends a return-change message $[e^*_r, e^*_{r+1}, \cdots, e^*_{r+c}]$ to C. C verifies that e^*_r is equal to $h^c(e^*_{r+c})$ in order to accept the returned change $(e^*_{r+1}, e^*_{r+2}, \cdots, e^*_{r+c})$. The return-change chain (E^*-chain) could be used when E-chain—which is the same denomination of E^*-chain—is used up. However, the merchant cannot use E^*-chain to return change again

3.3. Redemption and Remittance Phase. In the described scheme, each PayWord chain has a duration scope. Merchant M may redeem the money from banker B after the expiration date or at the end of a certain period. The details of the message exchanges in the redemption and remittance phase illustrated in Figure 3 are as follows:

(1) M sends $[ID_C, ID_M, e_{p+a}, f_{q+b}]_{pub(B)}$ to B

(2) B decrypts $[ID_C, ID_M, e_{p+a}, f_{q+b}]_{pub(B)}$ using $pri(B)$. If anchors e_{p+a} and f_{q+b} are valid, B remits the money $((p+a) \times d_E + (q+b) \times d_F)$ to M and deducts this amount from the account of C. B stores anchors e_{p+a} and f_{q+b}. In the next period, B receives and verifies the redemption $[ID_C, ID_M, e_{p+a+c}, f_{q+b+d}]_{pub(B)}$ successfully, where $(p+a+c) \le n$ and $(q+b+d) \le m$, and then remits the money $((c-a) \times d_E + (d-b) \times d_F)$ to M and also deducts this amount from the account of C

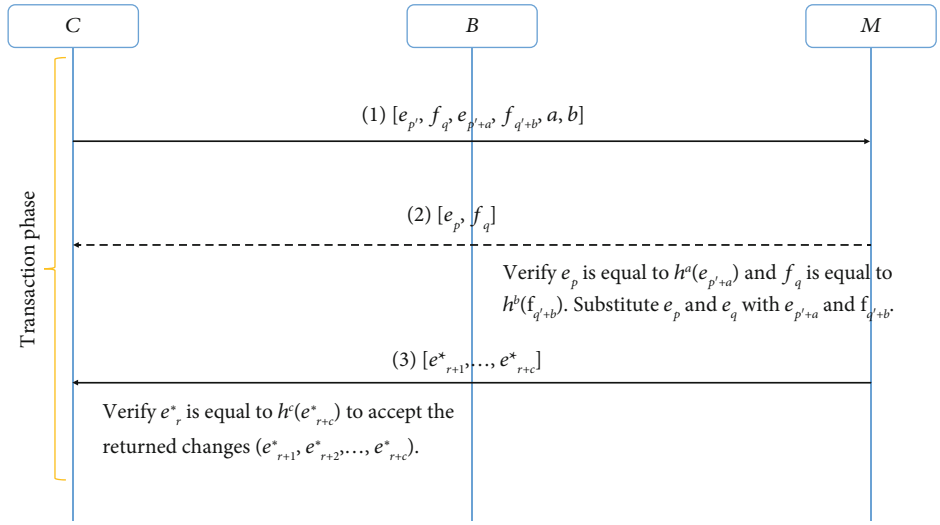

Figure 2: The message exchanges of the transaction phase.

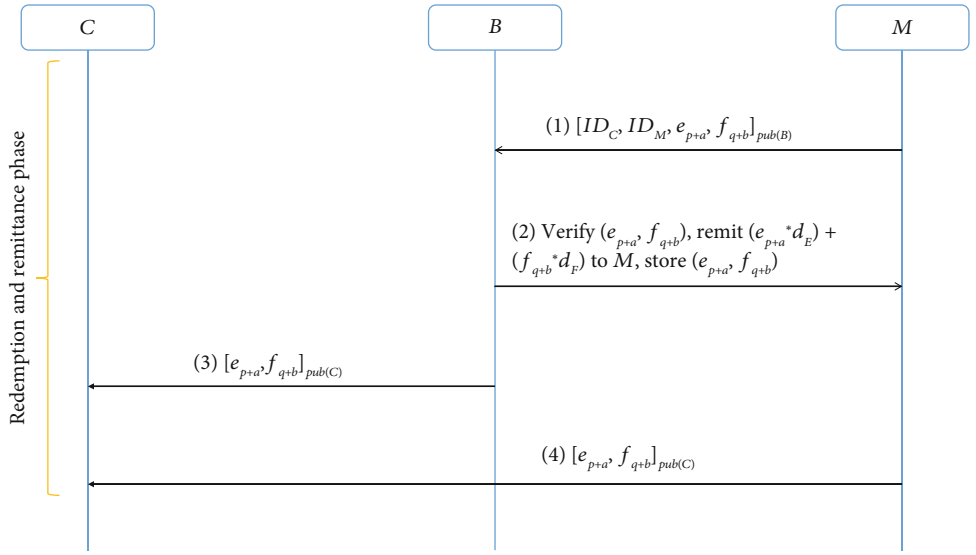

Figure 3: The message exchanges of the redemption and remittance phase.

(3) B sends $[e_{p+a}, f_{q+b}]_{pub(C)}$ to C. C decrypts this using $pri(C)$ to obtain anchors e_{p+a}, and f_{q+b}, and then verifies whether or not these two anchors are valid

(4) M sends $[e_{p+a}, f_{q+b}]_{pub(C)}$ to C. C decrypts this using $pri(C)$ to obtain anchors e_{p+a} and f_{q+b}, and then verifies whether or not these two anchors are valid. C checks if these anchors from B and C are the same or different

4. Security Analysis and Discussion

In this study, we made no assumption about the honesty of the customer, merchant, and banker. The main goal of the proposed scheme is to prevent the problems associated with counterfeiting and reusing PayWord chains. The required security and privacy features were implemented as follows:

(1) *Confidentiality and Authentication*. The proposed scheme employs the SSL protocol to authenticate the server and to cryptographically protect the channel used for communication between the client and the server. The client must provide the username and password of the customer's account, as well as the IMEI number of the device to the authorization server. An attacker could potentially guess the account username and password. However, he/she cannot use the mobile device to obtain the IMEI number

(2) *Attacker-Counterfeit Attack*. If an attacker does not obtain the anchor of a PayWord chain and the hash function generating a PayWord chain, an attacker cannot counterfeit any PayWord chain

(3) *Customer-Counterfeit Attack*. A customer has access to PayWord chains $E = (e_0, e_1, e_2, \cdots, e_n)$

Table 1: Comparison of the proposed scheme and other two PayWord-based micropayment schemes.

	The proposed scheme	MSRC [6]	PayWord [7]
Attacker-counterfeit protection	Yes	Yes	Yes
Customer-counterfeit protection	Yes	Yes	Yes
Merchant-counterfeit protection	Yes	Yes	Yes
Banker-deduction attack	Yes	Yes	Yes
Single account from multiple devices	Yes	No	No

and $F = (f_0, f_1, f_2, \cdots, f_m)$, but he/she cannot obtain $e_i\ (i > n)$ and $f_i\ (i > m)$ due to the one-way property of a hash function. This means that an attacker cannot counterfeit any PayWord chain. A customer receives the change $(e^*_1, e^*_2, \cdots, e^*_s)$ from the merchant. However, he/she cannot counterfeit $(e^*_{s+1}, e*_{s+2}, \cdots)$ due to the one-way property of a hash function

(4) *Merchant-Counterfeit Attack*. The merchant has the return-change chain $E^* = (e^*_0, e^*_1, \cdots, e^*_s)$ and verifies it. However, the merchant cannot obtain $e^*_i (i > s)$ and counterfeit the return-change chain due to the one-way property of a hash function. The merchant receives PayWord chains $e_i\ (i \geq 1)$ and $f_i\ (i \geq 1)$ from a customer and verifies them using the hash function, and obtains $(e_0, e_1, e_2, \cdots, e_i)$ and $(f_0, f_1, f_2, \cdots, f_i)$. However, the merchant cannot counterfeit any valid anchors after a PayWord chain due to the one-way property of a hash function

(5) *Customer Reuse and Overspend Attack*. The merchant updates the anchor of a PayWord chain when each payment is finished. If the customer makes a payment using a previously used PayWord chain, the merchant can verify this by checking the newest anchor. The customer does not overspend because he/she cannot counterfeit a PayWord chain

(6) *Merchant Reuse and Overspend Return-Change Attack*. The customer updates the anchor of the return-change chain when the merchant returns the change to the customer. If the merchant returns the previously used change, the customer can verify this by checking the anchor of the return-change chain. The merchant does not overspend because he/she cannot counterfeit the return-change chain

(7) *Merchant-Redemption Attack*. The banker updates the anchors of all PayWord chains after the merchant redeems the money from the banker. If the merchant attempts to redeem the money more than once or make a fraudulent redemption, the banker can verify this by checking the newest anchors. Also, the merchant cannot make a fraudulent redemption because the merchant cannot counterfeit a valid PayWord chain

(8) *Banker-Deduction Attack*. The banker sends the anchors of all PayWord chains redeemed by the merchant. The customer can verify this by comparing the anchor that is stored by the banker with the one that the merchant sends last to the customer when the banker deducts more money from the customer

Theorem 1. *The proposed scheme is secure even though attackers intercept the values of* $e_{p'}$, $f_{q'}$, $e_{p'+a}$, *and* $f_{q'+b}$ *(see Figure 2) sent from a device.*

Proof. Suppose that we have m various devices, and that the final payment anchors for each device are $\{e_{p_i}, f_{q_i}\}, 1 \leq i \leq m$. Obviously, the newly updated payment anchors $\{e_p, f_q\}$ in merchant M are the newest and should be the largest anchors from the anchors $\{e_{p_i}, f_{q_i}\}, 1 \leq i \leq m$. Via the one way property of hash function, we can derive $\{e_p, f_q\}$ from $e_p = h^a(e_{p_i})$ and $f_q = h^b(f_{q_i}), 1 \leq i \leq m$. Thus, attackers do not have any additional information from the intercepted values $\{e_{p_i}, f_{q_i}, e_{p_i+a}, f_{q_i+b}\}, 1 \leq i \leq m$.

According to the above analysis and proof, we compared the proposed scheme with other two PayWord-based micropayment schemes [6, 7] shown in Table 1.

5. Conclusion

This paper has presented a PayWord-based scheme for micropayments, in which a customer uses mobile devices to obtain PayWord chains as electronic coins. The proposed scheme not only includes authentication, confidentiality, and integrity but also guarantees mutual nonrepudiation between the customer, merchant, and banker. Moreover, we have shown that the proposed scheme allows the customer to make a payment with the same PayWord chains of a single account from multiple mobile devices.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors are indebted to the anonymous reviewers for their careful reading and suggestions to enhance the quality

of this paper. This work is supported by the Ministry of Science and Technology, Taiwan (Grant no. MOST 104-2221-E-259-012).

References

[1] S. Karnouskos, "Mobile payment: a journey through existing procedures and standardization initiatives," *IEEE Communications Surveys and Tutorials*, vol. 6, no. 4, pp. 44–66, 2004.

[2] N. Mallat, "Exploring consumer adoption of mobile payments - a qualitative study," *The Journal of Strategic Information Systems*, vol. 16, no. 4, pp. 413–432, 2007.

[3] N. Mallat and V. K. Tuunainen, "Merchant Adoption of Mobile Payment Systems," in *Presented at the Proceedings of the International Conference on Mobile Business*, Sydney, NSW, Australia, 2005.

[4] M. Bellare, J. A. Garay, A. Herzberg et al., "iKP - A Family of Secure Electronic Payment Protocols," in *Presented at the WOEC'95 Proceedings of the 1st Conference on USENIX Workshop on Electronic Commerce*, New York, NY, USA, 1995.

[5] B. Cox, J. D. Tygar, and M. Sirbu, "NetBill Security and Transaction Protocol," in *Presented at the WOEC'95 Proceedings of the 1st Conference on USENIX Workshop on Electronic Commerce*, New York, NY, USA, 1995.

[6] C.-N. Yang and C.-C. Wu, "MSRC: (M)icropayment (S)cheme with ability to (R)eturn (C)hanges," *Mathematical and Computer Modelling*, vol. 58, no. 1-2, pp. 96–107, 2013.

[7] R. L. Rivest and A. Shamir, "PayWord and MicroMint: Two Simple Micropayment Schemes," in *Presented at the Proceedings of the International Workshop on Security Protocols*, Cambridge, United Kingdom, 1996.

[8] Y. Mu, V. Varadharajan, and Y.-X. Lin, "New Micropayment Schemes Based on Pay Words," in *Presented at the the Australasian Conference on Information Security and Privacy*, Sydney, NSW, Australia, 1997.

[9] C.-T. Wang, C.-C. Chang, and C.-H. Lin, "A new micropayment system using general Payword chain," *Electronic Commerce Research*, vol. 2, no. 1/2, pp. 159–168, 2002.

[10] V. Patil and R. K. Shyamasundar, "An Efficient, Secure and Delegable Micro-Payment System," in *Presented at the the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service*, Taipei, Taiwan, 2004.

[11] Z. Yang, W. Lang, and Y. Tan, "A New Fair Micropayment System Based on Hash Chain," in *Presented at the IEEE International Conference on, e-Technology, e-Commerce, and e-Services*, Taipei, Taiwan, 2004.

[12] X. Dai, O. Ayoade, and J. Grundy, "Off-Line Micro-Payment Protocol for Multiple Vendors in Mobile Commerce," in *2006 Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06)*, Taipei, Taiwan, 2006.

[13] *A Mobile Wallet: Cash, Credit, Or Cellphone?*, NPR, 2012, https://www.npr.org/2012/01/27/145990092/a-mobile-wallet-cash-credit-or-cell-phone.

[14] M. B. Gross, J. M. Hogarth, and M. D. Schmeiser, *Consumers and Mobile Financial Services*, Board of Governors of the Federal Reserve System, 2012, https://www.federalreserve.gov/econresdata/mobile-device-report-201203.pdf.

[15] P. Borasi and S. Khan, *Mobile Payment Market by Payment Type, Transaction Mode, End User, Purchase Type, and Application: Opportunity Analysis and Industry Forecast, 2020–2027*, Allied Market Research, 2020, https://www.alliedmarketresearch.com/mobile-payments-market.

[16] V. K. Raina, U. S. Pandey, and M. Makkad, "A user friendly transaction model of mobile payment with reference to mobile banking in India," *International Journal of Information Technology*, vol. 18, 2012.

[17] P. Agrawal and S. Bhuraria, "Near field communication," *SETLabs Briefings*, vol. 10, pp. 67–74, 2012.

[18] *Near Field Communication-White paper*, Ecma Internation, 2005, http://www.ecma-international.org/activities/Communications/tc32-tg19-2005-012.pdf.

[19] *NFC-Forum*http://www.nfc-forum.org/home/.

[20] A. S. Lim, "Inter-consortia battles in mobile payments standardisation," *Electronic Commerce Research and Applications*, vol. 7, no. 2, pp. 202–213, 2008.

[21] C. TOMA, "M-payments issues and concepts," *Informatica Economică*, vol. 16, pp. 117–123, 2012.

[22] *Consumers and Convergence V: The Converged Lifestyle*, KPMG, 2012, https://home.kpmg/ru/en/home/insights/2012/02/consumers-and-convergence-v-the-converged-lifestyle.html.

[23] *Consumers Going Mobile: The Transformation of Payments, First Data*, 2011, https://www.firstdata.com/downloads/thought-leadership/Consumer-Payment-Insights-Consumers-Going-Mobile-WP.pdf.