南　華　大　學
資訊管理學系
碩士論文

一個"安全不可追踪之離線電子現金系統"的改善方法

Improvement on "Secure untraceable off-line electronic cash system"

研 究 生：周秀雲
指導教授：周志賢 博士

中華民國 106 年 1 月 5 日

南 華 大 學

資 訊 管 理 學 系

碩 士 學 位 論 文

一個"安全不可追蹤之離線電子現金系統"的改善方法

Improvement on "Secure untraceable off-line electronic cash system"

研究生：周秀雲

經考試合格特此證明

口試委員：劉建人

[illegible]

周志賢

指導教授：周志賢

系主任(所長)：[illegible]

口試日期：中華民國 106 年 1 月 5 日

南 華 大 學 碩 士 班 研 究 生

論 文 指 導 教 授 推 薦 函

資訊管理學 系碩士班 周秀雲 君所提之論文

Improvement on "Secure untraceable off-line electronic cash system"

係由本人指導撰述，同意提付審查。

指導教授 周志賢

106 年 1 月 7 日

南華大學資訊管理學系碩士論文著作財產權同意書

立書人：周秀雲之碩士畢業論文

中文題目：一個"安全不可追踪之離線電子現金系統"的改善方法

英文題目：Improvement on "Secure untraceable off-line electronic cash system"

指導教授： 周志賢 博士

學生與指導老師就本篇論文內容及資料其著作財產權歸屬如下：

- [x] 共同享有著作權
- [ ] 共同享有著作權，學生願「拋棄」著作財產權
- [ ] 學生獨自享有著作財產權

學 生：周秀雲（請親自簽名）

指導老師：周志賢（請親自簽名）

中 華 民 國 106 年 1 月 7 日

誌　　　謝

碩士在職專班的日子即將隨著這篇誌謝的完成來到尾聲。

感謝洪銘建教授來我們學校開學分班，才有緣進入南華大學就讀，也感恩南華大學提供優良的師資、優雅的校園環境和舒適平靜的學習氛圍。

首先感謝系上老師們的教導與包容，更感恩周志賢教授的費心指導論文。雖然不是每位老師的課都有修，但在請益、閒聊之中，總是能感受到師長的好。

其次最要感謝的是同事也是同學的鴻生和素卿，感謝鴻生這段日子開車接送，讓我得以不中斷的學習;也感謝素卿的陪伴、提醒和督促。這一年半的上下學共乘，三個人沿途說說笑笑，我稱我們三個人是南華生命共同體。

最後感恩班上月珍姐、素月姊、正哥等15位同學這一年半來的陪伴，在相互經驗交流及打趣之下，讓學習的過程格外有趣。

另外感恩口試老師:

南華大學資管系指導教授:周志賢 博士

高苑科大資管系副教授: 劉建人 博士

南華大學資管系教授: 王昌斌 博士

周秀雲 謹誌

2017/01/06 朴子

一個"安全不可追踪之離線電子現金系統"的改善方法

學生：周秀雲　　　　　　　　　　　　指導教授：周志賢 博士

南　華　大　學　資訊管理學系碩士班

摘　　要

最近，Baseri 等人 提出了一種安全的，不可追踪的離線電子現金系統。他們聲稱，他們的計劃可以實現電子現金系統的安全要求，如不可追踪性，匿名性，不可連接性，雙重花費檢查，不可偽造性，日期附加性和防止偽造硬幣。 他們進一步證明了通過使用解離散對數問題的難度而達到不可偽造性的安全特徵。 然而，在密碼分析後，我們發現該方案不能滿足不可追踪性的安全要求。 因此，我們修改該方法以期達到具有這項功能，這在電子現金系統中是相當重要的。

關鍵詞：數字簽名，離散對數問題，密碼分析，RSA，電子商務和支付

Improvement on "Secure untraceable off-line electronic cash system"

Student：JOU, SHIOU-YUN Advisors：Dr. CHOU, JUE-SAM

Department of Information Management
The Graduated Program
Nan-Hua University

ABSTRACT

Recently, Baseri et al. proposed a secure, untraceable off-line electronic cash system. They claimed that their scheme could achieve the security requirements of an e-cash system, such as untraceability, anonymity, unlinkability, double-spending checking, unforgeability, date-attachability, and preventing forging coins. They further proved the unforgeability security feature by using the hardness of discrete logarithm problem. However, after cryptanalysis, we determined that the scheme could not satisfy the untraceability security feature requirement. Therefore, we modified the method to include this desired functionality, which is considerably important in an e-cash system.

Keywords: digital signatures, discrete logarithm problem, cryptanalysis, RSA, electronic commerce and payment

目　　錄

List of Table

List of Figures

Improvement on “Secure untraceable off-line electronic cash system”

1. Introduction

There have been many cryptographic scientists working within the field of e-cash system design [1-33] since Chaum [11] in 1982 first proposed the concept of e-cash. E-cash’s properties are similar to paper cash such as anonymity, verifiability, and unforgeability. An e-cash system typically contains three roles: customer, bank, and merchant; and three protocols: withdrawal, payment, and deposit. In the protocol design principle, the user’s identity cannot be revealed to the outside world to ensure his purchasing privacy. It can only be disclosed when double-spending or an illegal transaction occurs. In an off-line e-cash scheme, the bank cannot prevent double-spending on-line. Therefore, it must have the ability to revoke the anonymity of an illegal user. In 2013, Baseri et al. [27] pointed out that Eslami et al.’s untraceable off-line electronic cash system [17] is flawed. It is vulnerable to three attacks: double-spending attack, expiration date forgery, and frauds on the exchange protocol. Further, they proposed an excellent, untraceable off-line e-cash system and claimed that their scheme exhibits anonymity, double-spending detection, unforgeability, date attachability properties, and forgery prevention. Meanwhile, they demonstrated the reasons why their scheme was immune to the three vulnerable faults of the Eslami et al.’s scheme. However, upon a closer examination, we discovered that it does not support the untraceability property. Therefore, to enhance its security, we modified their scheme to include this feature. We demonstrate the enhancement in this article.

The remainder of this paper is organized as follows. In Section 2,we review Baseri et al.’s scheme. In section 3 ,we show the weakness of their scheme. Section 4 modified the scheme to include the untraceability property. Section 5 analyzes it security, and Section 6 makes a conclusion.

2. Review of Baseri et al.'s scheme

Baseri et al.'s e-cash scheme [27] consists of four participants: a central authority, a bank, a spender, and a merchant. It contains five phases: initialization, withdrawal, payment, deposit, and exchange. They use Chaum's signature to design the scheme and adopt a RSA-based method to attach time to the structure of the signature. In this article, we only review the withdrawal and payment protocols to illustrate its weakness. As for the definitions of the notations used, please refer to the original article.

2.1 Withdrawal protocol

The central authority sets specific public parameters that includes two publicly known elements, g_1, g_2, and the bank's two RSA public/private key-pairs $(((e_B, n), 1/e_B))$ and $((e_B^{'}, n), 1/e_B^{'})$, such that $e_B \geq e_B^{'}$. Before withdrawing a coin, the spender must prove his account ownership to the bank. The spender proves his identity in a manner similar to a classical withdrawal from an account. In addition, the bank periodically publishes the fresh time by using two parameters, t and $e_B * t \pmod{\phi(n)}$, where t is a constant during the period and is used to synchronize the customers, and $e_B * t$ acts as a public key for the bank and is chosen in such a manner that its reverse exists. The coin is represented by a six-tuple $(A', B, s_1, s_2, s_3, t)$. The withdrawal protocol is described as follows and also shown in Fig. 1.

Step 1. The spender S:

(a) Chooses three random numbers, $x_1, x_2 \in_R Z_{e_B}^{*}$ and $s \in_R Z_n^{*}$, and two blinding factors, $b_1, b_2 \in Z_n^{*}$.

(b) Computes: $A' = A^s \pmod{n}$, $B = g_1^{x_1} g_2^{x_2} \pmod{n}$, $w_1 = B b_1^{e_B^{'}} \pmod{n}$, and $w_2 = (A^{'} + B) b_2^{e_B * t} \pmod{n}$.

(c) Sends w_1, w_2, t to the bank.

Step 2. The bank B:

(a) Checks the validity of the Date/Time slip.

(b) Signs w_1, w_2 by computing:

$O_2 = w_1^{1/e_B^{'}} \pmod{n}$, $O_3 = w_2^{1/(e_B * t)} \pmod{n}$.

(c) Sends O_2 and O_3 to the spender.

Step 3. The spender S:

(a) Verifies the signatures of the bank on A', w_1, w_2.

(b) Obtains the signatures of the bank on A', B, and $A' + B$, that are signed with private keys $1/e_B$, $1/e'_B$, and $(1/(e_B * t))$, respectively:

$s_1 = O_1^s \pmod n = \text{sign}_B(A')$,

$s_2 = O_2 / b_1 \pmod n = \text{sign}_B(B)$,

$s_3 = O_3 / b_2 \pmod n = \text{sign}_B(A' + B)$.

The coin is $(A', B, s_1, s_2, s_3, t)$.

spender		**bank**
$s \in_R Z_n^*$, $x_1, x_2 \in_R Z_{e'_B}^*$		
$b_1, b_2, \in Z_n^*$		
$A' = A^s \pmod n$		
$B = g_1^{x_1} g_2^{x_2} \pmod n$		
$t = (Date/Time)$		
$w_1 = B b_1^{e'_B} \pmod n$		
$w_2 = (A' + B) b_2^{e_B * t} \pmod n$	w_1, w_2, t $\longrightarrow$	
		Check $Date/Time$
		$O_2 = w_1^{1/e'_B} = B^{1/e'_B} b_1$
	O_2, O_3 $\longleftarrow$	$O_3 = w_2^{1/(e_B * t)}$
$s_1 = O_1^s \pmod n = \text{sign}_B(A')$		
$s_2 = O_2 / b_1 \pmod n = \text{sign}_B(B)$		
$s_3 = O_3 / b_2 \pmod n = \text{sign}_B(A' + B)$		
coin $= (A', B, s_1, s_2, s_3, t)$		

Fig. 1: The withdraw protocol of Baseri et al.'s scheme

2.2 Off-line payment protocol

The off-line payment protocol is described as follows and also depicted in Fig. 2.

Step 1. The spender S:

(a) Sends $(A', B, s_1, s_2, s_3, t)$ to the merchant M.

Step 2. The merchant M:

(a) Verifies whether $A' \neq 1$,

(b) Checks the coin's expiration date,

(c) Verifies the signatures s_1, using the public key e_B, s_2 using the public key $e_B^{'}$, and s_3 the public key $(e_B * t)$,

(d) Computes the challenge $d = H(A', B, ID_M, date \,||\, time)$, where H is the hash function determined in the initialization phase, ID_M is the merchant's identity, and $date \,||\, time$ represents the transaction's date and time.

(e) Sends d to the spender.

Step 3. The spender S:

(a) Computes:

$r_1 = dus + x_1 \pmod{e_B}$,

$r_2 = ds + x_2 \pmod{e_B}$.

(b) Sends r_1 and r_2 to the merchant.

Step 4. The merchant M:

(a) Accepts the coin if $g_1^{r_1} g_2^{r_2} = A'^d B$.

spender		**merchant**
	A', B, s_1, s_2, s_3, t →	Verify $A' \neq 1$
		Check the coin's expiration date
		Verify the signature s_1, s_2, s_3
	← d	$d = H(A', B, ID_M, date \,||\, time)$
$r_1 = dus + x_1 \pmod{e_B}$		
$r_2 = ds + x_2 \pmod{e_B}$	r_1, r_2 →	$g_1^{r_1} g_2^{r_2} = A'^d B$
		Accepts the coin

Fig. 2: The payment protocol of Baseri et al.'s scheme

3. Weakness of this scheme

An insider can collect the transmitted message on the Internet and obtain information as follows:

(1) From the messages in a withdrawal protocol execution, the attacker can acquire the values, w_1, w_2, t, O_2, and O_3.

(2) From the messages in an off-line payment protocol, the attacker can acquire the coin $(A', B, s_1, s_2, s_3, t)$.

Assuming that the attacker has gathered all *m* (with $m \le 2^q$, where q is the security parameter, e.g., q = 80) coins $(A_i', B_i, s_{i1}, s_{i2}, s_{i3}, t_i)$ for *I* = 1 to *m*, he then can launch an off-line attack for the *m* coins using the following methods:

(1) He computes $O_2^{e_B'} = w_1 = Bb_1^{e_B'} (\bmod n)$. From this equation, he obtains $b_1^{e_B} = O_2^{e_B} / B (\bmod n)$. Although, he cannot determine the correct value of *B*, with the help of the m observed coins $(A_i', B_i, s_{i1}, s_{i2}, s_{i3}, t_i)$, he can compute $b_{i1}^{e_B'} = O_2^{e_B'} / B_i (\bmod n) = w_1 / B_i (\bmod n)$, for I = 1 to m. Then, he randomly chooses $a, f \in z_n^*$, forms the value $w_{i1} = a^{e_B} b_{i1}^{e_B} (\bmod n)$, and executes the withdrawal protocol by sending w_{i1}, *f*, and *t* to the bank for acquiring, $O_2' = w_1^{1/e_B'} = ab_{i1} (\bmod n)$, $O_3' = f^{1/e_{B*t}} (\bmod n)$. Then, he can deduce b_{i1} using the value $a^{-1} (\bmod n)$.

(2) By computing, he determines if $O_2' = s_{i2} \cdot b_{i1}$.

If equation (2) is true, the insider knows that the e-cash $(A_i', B_i, s_{i1}, s_{i2}, s_{i3}, t_i)$ is related to the parameters w_{i1}, w_{i2}, t, O_2', and O_3' in a specific withdrawal protocol. Otherwise, he continues through the remaining *m*-1 coins. Obviously, he will determine one coin that satisfies the equation. Therefore, the feature of untraceability is violated. Even if $m \ge 2^q$, the attacker can use the parameter *t*, observed in the withdrawal protocol, to filter the coins that have the same time *t*, and then launch the two-step attack shown above.

4. Modification

From the weakness found in Section 3, we note the key point is that the insider can use $b_{i1}^{e_B'}(=O_2^{e_B'}/B_i(\bmod n))$ to produce w_{i1} (equals to $a^{e_B'}b_{i1}^{e_B'}(\bmod n)$) and send it to the bank for obtaining b_{i1}, to see if $O_2' = s_{i2}\cdot b_{i1}$ holds. To further disguise the relationship between O_2' and s_{i2} in the original scheme, we introduce two new parameters, $b_3 \in z_n, x_3 \in z_n^*$, and modify $w_1 = b_3^{e_B'} B b_1^{e_B'}(\bmod n)$ which is $Bb_1^{e_B'}$ in the original scheme, add another parameter $w_{11} = (b_3 x_3)^{e_B'}(\bmod n)$. Then, the spender sends w_1, w_{11}, w_2, t to the bank in the withdraw phase. The bank will return O_2, O_{22}, and O_3. O_2 from the bank will now become $w_1^{1/e_B'}(\bmod n) = b_3 B^{1/e_B'} b_1$ .Subsequently, the original value $s_2 = O_2/b_1(\bmod n) = B^{1/e_B'}$ will be modified to $s_2 = O_2\cdot O_{22-x3}/b_1 b_3^2(\bmod n) = B^{1/e_B'}$. For clarity, we show the definitions of used notations in Table 1 and show the modification result of the withdraw protocol in Fig. 3.

Table 1. The definitions of used notations

$A' = A^s(\bmod n)$ $B = g_1^{x_1} g_2^{x_2}(\bmod n)$ $w_1 = b_3^{e_B'} B b_1^{e_B'}(\bmod n)$ $w_{11} = (b_3 x_3)^{e_B'}(\bmod n)$ $w_2 = (A' + B) b_2^{e_B * t}(\bmod n)$ $O_2 = w_1^{1/e_B}(\bmod n) = b_3 B^{1/e_B'} b_1$ $O_{22} = w_{11}^{1/e_B}(\bmod n) = b_3 x_3$	$O_3 = w_2^{1/(e_B * t)}(\bmod n)$ $O_{22-x_3} = b_3$ $s_1 = O_1^s(\bmod n) = sign_B(A') = A'^{1/e_B'}$ $s_2 = O_2 \cdot O_{22-x_3}/b_3^2 b_1(\bmod n) = sign_B(B) = B^{1/e_B'}$ $s_3 = O_3/b_2(\bmod n) = sign_B(A'+B) = (A'+B)^{1/e_B' * t}$ coin=$(A', B, s_1, s_2, s_3, t)$

5. Security analysis

If an attacker launches the above attack on our modification.

(1) He randomly chooses $a, f \in z_n^*$, forms the value $w_{i1} = a^{e_B} b_{i3}^{e_B'} b_{i1}^{e_B'}(\bmod n)$,

$w_{i11} = b_{i3}^{e'_B} x_3^{e'_B} (\bmod n)$, $w_{i2} = f (\bmod n)$, and executes the withdrawal protocol by sending w_{i1}, w_{i11}, w_{i2}, and t to the bank for acquiring $O'_2 = w_1^{1/e'_B} = ab_{i3}b_{i1} (\bmod n)$, $O'_{22} = b_{i3}x_3 \ (\bmod n)$, $O'_3 = f^{1/e_{B*t}} (\bmod n)$ .Then, although he can acquire the multiplication $b_{i3} \cdot b_{i1}$ with the value of a^{-1} , however, he can not deduce b_{i3}, b_{i1}, x_3 individually.

Spender		bank
$s, x_3 \in_R Z_n^*,\ x_1, x_2 \in_R Z_{e'_B}^*$		
$b_1, b_2, b_3 \in Z_n$		
$A' = A^s (\bmod n)$		
$B = g_1^{x_1} g_2^{x_2} (\bmod n)$		
$t = (Date / Time)$		
$w_1 = b_3^{e'_B} B b_1^{e'_B} (\bmod n)$		
$w_{11} = (b_3 x_3)^{e'_B} (\bmod n)$		
$w_2 = (A' + B) b_2^{e_B * t} (\bmod n)$	w_1, w_{11}, w_2, t →	Check $Date / Time$
		$O_2 = w_1^{1/e'_B} (\bmod n) = b_3 B^{1/e'_B} b_1$
		$O_{22} = w_{11}^{1/e'_B} (\bmod n) = b_3 x_3$
	← O_2, O_{22}, O_3	$O_3 = w_2^{1/(e_B * t)} (\bmod n)$
$s_1 = O_1^s (\bmod n) = sign_B(A')$		
$s_2 = O_2 \cdot O_{22-x3} / b_3^2 b_1 (\bmod n) = sign_B(B)$		
$s_3 = O_3 / b_2 (\bmod n) = sign_B(A' + B)$		
$coin = (A', B, s_1, s_2, s_3, t)$		

Fig. 3: The withdraw protocol after modification

(2) Although, he knows $s_2 = O_2 \cdot O_{22-x3} / b_3^2 b_1$, however, without x_3^{-1} from $O'_{22} (= b_{i3} x_3)$,

he cannot deduce the value of b_{i3}. Without the knowledg of b_{i3}, he therefore cannot determine the value b_{i1} from the acquired multiplication $b_{i3} \cdot b_{i1}$.

In short, although he knows $b_{i3} \cdot b_{i1}$, however, without the value of b_{i3}, he cannot determine the values b_{i1},and without b_{i3}, he cannot deduce the value x_3 from O'_{22}. Accordingly, the modification defeat the weakness which we found in Baseri et al.'s scheme, and therefore we successfully enhance its security of untraceability.

6. Conclusion

In this paper, we showed that Baseri et al.'s untraceable off-line e-cash scheme is flawed, because it suffers from traceability. We modified the scheme to avoid this security weakness. From the security analysis shown in Section 5, we see that we have corrected the security issue.

References

[1] Choo, Kim-Kwang Raymond. "New payment methods: A review of 2010–2012 FATF mutual evaluation reports." *Computers & Security* 36 (2013): 12-26.

[2] Chen, Yalin, and Jue-Sam Chou. "Cryptanalysis on" Secure untraceable off-line electronic cash system"." IACR Cryptology ePrint Archive 2014 (2014): 63.

[3] Aszalós, László, and Andrea Huszti. "Payment approval for PayWord." International Workshop on Information Security Applications. Springer Berlin Heidelberg, 2012.

[4] Tan, Garry Wei-Han, et al. "NFC mobile credit card: the next frontier of mobile payment?." Telematics and Informatics 31.2 (2014): 292-307.

[5] Žilka, Roman, Vashek Matyáš, and Libor Kyncl. "Four authorization protocols for an electronic payment system." International Doctoral Workshop on Mathematical and Engineering Methods in Computer Science. Springer Berlin Heidelberg, 2011.

[6] Pour, Mohammad Mehdi Hossein, and Halina Mohamed Dahlan. "BESTCASH: A new -cash for micropayment." Innovation Management and Technology Research (ICIMTR), 2012 International Conference on. IEEE, 2012.

[7] Hinterwälder, Gesine, et al. "Efficient e-cash in practice: Nfc-based payments for public transportation systems." International Symposium on Privacy Enhancing Technologies Symposium. Springer Berlin Heidelberg, 2013.

[8] Tiwari, Mayank, et al. "An Efficient and Secure Micro-payment Transaction Using Shell Cryptography." International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness. Springer Berlin Heidelberg, 2013.

[9] Hinterwälder, Gesine, Christof Paar, and Wayne P. Burleson. "Privacy preserving payments on computational RFID devices with application in intelligent transportation systems." International Workshop on Radio Frequency Identification: Security and Privacy Issues. Springer Berlin Heidelberg, 2012.

[10] Rahman, Nor Azlina Bt Abd, Khalida Shajaratuddur Bt Harun, and Yusnita Bt Yusof. "SMS banking transaction as an alternative for information, transfer and payment at merchant shops in Malaysia." Information Technology and e-Services (ICITeS), 2013 3rd International Conference on. IEEE, 2013.

[11] Ogata, Wakaha, and Kaoru Kurosawa. "Oblivious keyword search." Journal of complexity 20.2 (2004): 356-371.

[12] Chaum, David, Amos Fiat, and Moni Naor. "Untraceable electronic ash." Proceedings on Advances in cryptology. Springer-Verlag New York, Inc., 1990.

[13] Brands, Stefan. "Untraceable off-line cash in wallet with observers." Annual International Cryptology Conference. Springer Berlin Heidelberg, 1993.

[14] Brickell, Ernest F., Peter Gemmell, and David W. Kravitz. "Trustee-based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change." SODA. Vol. 95. 1995.

[15] Camenisch, Jan, Ueli Maurer, and Markus Stadler. "Digital payment systems with passive anonymity-revoking trustees." Journal of Computer Security 5.1 (1997): 69-89.

[16] Fujisaki, Eiichiro, and Tatsuaki Okamoto. "Practical escrow cash systems." International Workshop on Security Protocols. Springer Berlin Heidelberg, 1996.

[17] Eslami, Ziba, and Mehdi Talebi. "A new untraceable off-line electronic cash system." Electronic Commerce Research and Applications 10.1 (2011): 59-66.

[18] Frankel, Yair, Yiannis Tsiounis, and Moti Yung. "Fair off-line e-cash made easy." International Conference on the Theory and Application of Cryptology and Information Security. Springer Berlin Heidelberg, 1998.

[19] Wang, Hua, Jinli Cao, and Yanchun Zhang. "A flexible payment scheme and its role-based access control." IEEE Transactions on knowledge and Data Engineering 17.3 (2005): 425-436.

[20] Fuchsbauer, Georg, David Pointcheval, and Damien Vergnaud. "Transferable constant-size fair e-cash." International Conference on Cryptology and Network Security. Springer Berlin Heidelberg, 2009.

[21] Gaud, Matthieu, and Jacques Traoré. "On the anonymity of fair offline e-cash ystems." International Conference on Financial Cryptography. Springer erlinHeidelberg, 2003.

[22] Hufschmitt, Emeline, and Jacques Traoré. "Fair blind signatures

revisited." International Conference on Pairing-Based Cryptography. Springer Berlin Heidelberg, 2007.

[23] Juang, Wen-Shenq. "D-cash: A flexible pre-paid e-cash scheme for date-attachment." Electronic Commerce Research and Applications 6.1 (2007): 74-80.

[24] Ashrafi, Mafruz Zaman, and See Kiong Ng. "Privacy-preserving e-payments using one-time payment details." Computer Standards & Interfaces 31.2 (2009): 321-328.

[25] Chen, Yalin, et al. "A novel electronic cash system with trustee-based anonymity revocation from pairing." Electronic Commerce Research and Applications 10.6 (2011): 673-682.

[26] Fan, Chun-I., Vincent Shi-Ming Huang, and Yao-Chun Yu. "User efficient recoverable off-line e-cash scheme with fast anonymity revoking." Mathematical and Computer Modelling 58.1 (2013): 227-237.

[27] Baseri, Y., B. Takhtaei, and J. Mohajeri. "Secure untraceable off-line electronic cash system." Scientia Iranica 20.3 (2013): 637-646.

[28] Stalder, Felix. "Failures and successes: notes on the development of electronic cash." The Information Society 18.3 (2002): 209-219.

[29] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[30] Zorpette, Glenn. "The beginning of the end of cash [Special Report]." IEEE Spectrum 6.49 (2012): 27-29.

[31] Peck, Morgen. "The cryptoanarchists' answer to cash." IEEE Spectrum 6.49 (2012): 50-56.

[32] Miers, Ian, et al. "Zerocoin: Anonymous distributed e-cash from bitcoin." Security and Privacy (SP), 2013 IEEE Symposium on. IEEE, 2013.

[33] Reid, Fergal, and Martin Harrigan. "An analysis of anonymity in the bitcoin system." Security and privacy in social networks. Springer New York, 2013. 197-223.