# 해쉬체인을 이용한 은행 전용의 전자화폐에 관한 연구

강서일*, 이임영

*순천향대학교 정보기술공학부

# A Study on Bank exclusive Electronic Cash Using the Hash Chain

Se-Il Kang*, Im-Yeong Lee

*Division of Information Technology. Sonnchunhyang Univ.

## 요 약

전자 상거래의 발달로 인해 전자 화폐의 개발 및 연구는 현재 활발하게 진행되어지고 있다. 전자화폐는 고액과 소액의 금액 단위 및 보안 요구 사항으로 위조 방지, 익명성, 분할성, 이중사용 방지 등의 다양한 요구를 만족 시켜야 한다. 이에 본 논문에서는 해쉬체인을 이용한 소액의 은행 전용의 전자화폐에 관하여 연구하였다. 보안 요구 사항으로는 분할성, 위조 방지, 이중사용 방지를 제공해 주고 있다. 기존의 해쉬 체인의 경우 사용자가 발행하여 은행으로부터 정당성을 증명하는 경우가 대부분이나 본 논문에서는 은행이 사용자의 요청으로 인해 해쉬체인을 생성하여 제공한다. 이로 인해 인출 프로토콜의 통신횟수가 줄어들었다.

## I. 서론

전자상거래의 발달로 인해 전자화폐의 개발 및 연구는 활발하게 진행되어져 왔다. 소액에 대한 지불 방식으로 다양한 방식의 연구가 진행되고 있다. 본 논문에서는 해쉬체인을 이용한 소액 지불 시스템을 제안한다. 해쉬체인의 경우 소액 지불에서 많은 연산이 필요하지 않으며, 간단하게 생성할 수 있다. 이에 소액 지불에서 유용하게 사용할 수 있는 방법이다. 해쉬체인은 하나의 값을 정한 횟수까지 연속적으로 해쉬를 취한 값을 이용한다. 이와 같은 경우 앞의 값을 알고 있다면, 다음 값을 유추 할 수 있는 취약성을 가지고 있지만, 해쉬체인을 이용하는 경우에 있어 역으로 지불함으로써 마지막 값으로부터 순차적으로 앞으로 이용하게 된다. 본 논문의 본문에서는 첫 번째로 전자화폐의 보안 요구 사항에 대해서 간략하게 분석하고, 두 번째로 해쉬체인을 이용한 기반 연구에 대해 기술한다. 세 번째에서는 본 논문의 제안하는 해쉬체인을 이용한 은행 발급 전용 전자화폐에 대해 자세히 기술한다. 네 번째에서는 앞에서 언급한 보안 요구 사항을 가지고 본 제안 방식을 분석하고, 마지막으로 결론 및 향후 방향으로 본 논문을 마치도록 한다.

## II. 본론

### 1. 전자화폐의 보안 요구 사항

전자화폐는 전자적으로 이루어지는 거래에서 편리성을 제공하는 디지털 정보로써 화폐의 가치를 저장하고 있기 때문에 다음과 같은 보안 요구 사항을 만족하여야 한다.[3]

- 익명성 : 전자화폐의 지불 과정에서 물품 구입 내용과 사용자 식별 정보가 어느 누구에 의해서도 연계될 수 없어야 한다.
- 위조 방지 : 발행된 전자화폐를 위조, 변조 등의 부정한 사용을 할 수 없도록 해야 한다.
- 분할성 : 발행된 전자화폐의 경우 일정한 금액 내에서 자유롭게 분할하여 지불할 수 있어야 한다.
- 이중사용 방지 : 한 번 사용된 금액은 다시 사용되어서는 안 된다.

이외에도 다양한 보안 요구 사항이 요구되나 본 논문에서는 위의 사항을 중심을 분석 제안하도록 한다.

## 2. 기반 연구

이번 장에서는 해쉬체인에 대한 연구 및 해쉬 체인을 이용하는 소액 지불 시스템에 대해 알아보겠다.

1) 해쉬체인

해쉬체인은 하나의 값에 연속적으로 해쉬를 취하는 것으로 앞에서 해쉬를 취한 값에 해쉬를 취해 다음의 값을 얻는 것을 말한다.

$$C_i = H(C_{i-1})$$

해쉬 함수는 충돌 회피의 일방향성 해수 함수를 말한다. 해쉬 체인의 경우 $C_i$의 값을 알아도 $C_{i-1}$의 값을 알기는 매우 어렵다는 것이다. 역방향 함수가 존재하지 않으므로 그 값을 알아내기는 어려운 것을 이용한다.

2) 해쉬 체인을 이용한 전자 화폐 시스템

가. 해쉬 체인을 이용한 새로운 오프라인 전자 화폐

해쉬 체인을 이용한 전자 화폐 시스템으로 익명성을 제공하기 위해 은닉서명을 이용하고, 분할성을 제공한다. 다음의 그림 1은 인출 프로토콜의 흐름도를 보여준다.[4]

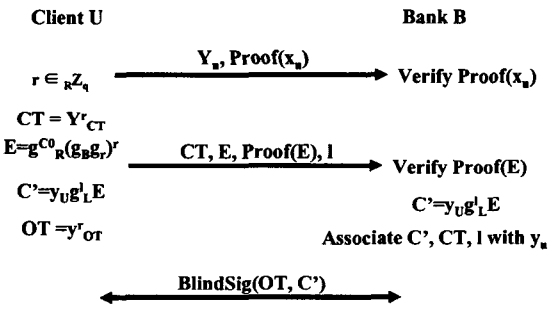


그림 1. 인출 프로토콜의 흐름도

그림 1. 인출 프로토콜은 사용자가 해쉬 체인을 생성하여 자신의 신원 정보와 함께 은행에 전송하면 영지식을 이용하여 자신의 정보를 은행에 확인시키고, 은행의 은닉 서명을 받아 온다.

나. 이중해쉬체인에 기반한 분할 가능 전자화폐의 설계

이중해쉬체인을 이용한 논문의 기반 기술은 이중해쉬체인으로 사용자가 선택한 해쉬체인과 은행의 선택한 해쉬체인을 쌍으로 만들어 이용하는 것으로 하나의 해쉬 체인을 이용하는 경우, 중간 값을 유추하여 사용할 수 있는 취약성에 대처하고 있는 것이다.[5]

또한 분할하는 경우를 예상하여, 은행으로부터 대리 서명을 할 수 있는 인자 값을 가지고 있다. 이로 인해 각각의 분할로 지급되는 경우 은행의 대리 서명이 이용된다.

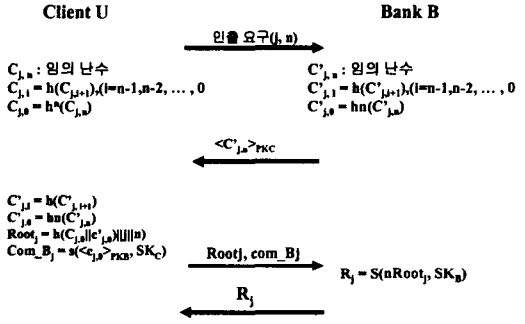


그림 2. 이중해쉬체인의 인출 프로토콜의 흐름도

그림 2와 같은 인출 프로토콜은 사용자가 은행에 인출을 요구하면 은행은 하나의 해쉬체인을 생성하여 사용자에게 제공한다. 사용자는 두개의 해쉬체인을 이용하여 root를 생성하고 은행의 서명을 요구하면 은행은 서명을 해서 사용자에게 전송한다.

지급 방식에서 분할 지급을 하기 위해서는 은행의 대리 서명을 이용한다.

이와 같이 해쉬체인을 사용자가 생성하여 이용하는 경우 은행이나 지불 브로커 또는 신뢰기관으로부터 자신이 생성한 화폐가 정당한지를 확인 받기 위해 통신 회수가 최소 3회를 이상을 가져야 한다. 이는 정당성의 확인은 2회로 가능하나 섬명을 받아서 다시 사용자에게 전송을 해주어야 하기 때문이다.

## 3. 제안 방식

제안 시스템은 해쉬체인을 이용하여 은행에서 구성하는 전용화폐로써 다음과 같이 구성된다.

1) 제안 시스템의 계수

본 시스템에서 사용된 계수는 다음과 같다

- U : 사용자(user)
- B : 은행(Bank)
- S : 상점(shop)
- * : 각각의 객체(사용자, 은행, 상점)
- PK*[] : *의 공개키로 암호화
- Sig*() : *의 개인키 서명
- R* : *가 선택의 임의 난수
- h(*) : *의 내용에 대한 충돌회피의 일방향 함수
- $x_*$ : *의 개인키
- $y \equiv g^{x^*} \bmod p$ : *의 공개키
- root : 해쉬 체인의 최종 값
- M : 금액의 정보
- n : 해쉬 체인의 회수
- T_data : 동전 발행 시간
- $g^S$ : 상점의 식별자

2) 제안 방식

전자화폐 시스템의 경우 인출, 지불, 이체 프로토콜로 나누어 볼 수 있다. 인출은 사용자와 은행, 지불은 사용자와 상점, 이체는 상점과 은행의 거래로 볼 수 있다.

본 논문의 제안 방식은 인출 프로토콜과 지불 프로토콜 두 개로 나누어 말한다. 인출 프로토콜은 은행과 사용자 사이의 통신으로 전자화폐를 은행이 발행한다. 지불 프로토콜은 은행으로부터 발급 받은 돈을 가지고 물건의 구입대금으로 지불한다. 이체에 대해서는 은행에서 발급되는 전자화폐이므로 은행은 이중 사용의 검출만 하면 된다.

가. 인출 프로토콜

㉠ 사용자는 은행에게 인출을 요구한다. 사용자가 인출 할 금액과 해쉬를 몇 번 취할 것인지 등의 정보를 은행에 알려 준다.

U -> B : M, n

㉡ 은행은 사용자의 공개키를 가지고 와서 선택한 랜덤 수로 C와 root를 생성하여 서명하여 보낸다.

B -> U :

$$g^{R_B},\ PK_U[\ Sig_B(\text{root}, T-data), T-data]$$

$$C = g^{X_U R_B} \quad (1)$$

$$\text{root} = h(\ g^{X_U R_B})^n \quad (2)$$

$$Sig_B(\text{root}, T-data) \quad (3)$$

㉢ 사용자는 은행으로부터 받은 값을 자신의 개인키와 해쉬 체인을 이용하여 확인한다.

$$C' = g^{X_U R_B} \quad (4)$$

$$\text{root}' = h(\ g^{X_U R_B})^n \quad (5)$$

$$\text{root} \stackrel{?}{=} \text{root}' \quad (6)$$

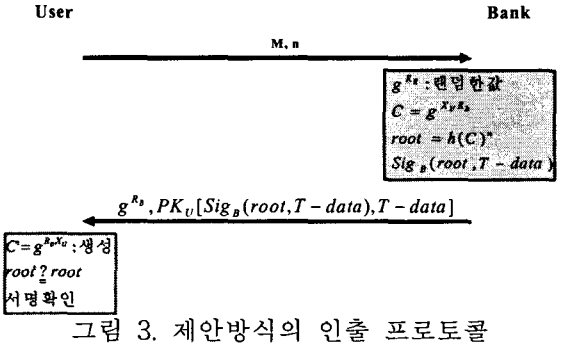


그림 3. 제안방식의 인출 프로토콜

나. 지불 프로토콜

발급 받은 전자화폐를 분할하지 않고 전체다 이용하는 경우를 보겠다.

㉠ 상점은 자신의 식별자 값과 물건의 금액에 대해서 알려 준다.

$$S \rightarrow U : g^S, M$$

㉡ 사용자는 다음과 같이 값을 생성해서 상점에 보낸다.

$$U \rightarrow S:$$
$$g^{sx_u}\,[\,Sig(root, T-data), T-data, C, n\,]$$

㉢ 상점은 사용자에게 받은 값을 다음과 같이 확인한다.

$$h(C)'' = root() \qquad (7)$$

$$root \triangleq root'$$

다. 분할의 경우

사용자는 자신의 해쉬 체인의 첫 번째로 n부터 j까지를 이용하였다. 이후에 분할 사용을 위해 사용자는 j 값과 $h(C)^{n-j}$ 값을 저장한다. 두 번째 사용시의 k만큼 지불한다면 사용자는 다음과 같이 계산하여 지불하여야 한다.

$j+k$, $h(C)^{n-j-k}$의 값을 상점에 전송하여 지불한다.

## 4. 제안 방식 분석

본 장에서는 앞에서 말한 것과 같이 제안한 방식에 대하여 1장에서 언급한 보안 요구사항에 대해 알아본다.

㉠ 위조 방지

은행에서 해쉬 체인을 발급하므로 인해 사용자는 은행이 만든 임의의 난수를 다른 것으로 대체할 수 없게 되는데 그 이유는 수식 (2)의 root값을 증명을 할 수 없기 때문이다. 또한 (1)에서 개인키를 이용해서 생성함으로 사용자 자신이 아니면 화폐를 생성해서 이용할 수 없다.

㉡ 이중 사용 방지

이중 사용을 방지하기 위해 상점의 제공하는 값들은 은행이 저장하고 있으면서 같은 값의 해쉬 체인이 나오면 지불을 하지 않고 각 상점의 식별자 값을 제외시켜 난수로써 사용자를 확인한다. 사용자의 공개키를 이용하여 발급하였기 때문에 사용자가 생성하는 경우에는 개인키를 이용하도록 된다. 이에 사용자가 전자화폐에 대해서 부인 할 수 없게 되고, 이중 사용시에 사용자를 알아 낼 수 있다.

㉢ 분할성

사용자는 해쉬 체인의 특성을 이용하여 분할 지급할 수 있다. 단, 해쉬 체인의 값들은 일정한 금액을 나타내고 있으며, 그 금액의 아래로는 분할할 수 없다.

## Ⅲ. 결론 및 향후 방향

본 논문에서는 은행에서 발급하는 전용 전자화폐로써 은행은 개인의 공개키를 이용하여 전자화폐를 발급하였다. 이로 인해 기존의 방식인 사용자가 생성하고 정당성을 입증하여 서명을 받는 방식보다 간편하고 통신의 회수를 줄일 수 있다. 인증도 자신의 개인키를 이용하기 때문에 다른 절차가 필요 없다.

향후 발전 방향으로 본 논문의 경우 익명성에 대한 제공을 언급하지 않고 있다. 또한 은행의 전용 전자화폐로써 익명성 제공에 대한 방안이 필요하며, 가치 이전의 서비스를 제공하는 경우는 난수의 값과 개인키의 값 둘 중 하나의 값이 공개되어야 하는 취약성을 가지고 있다. 향후 익명성의 제공과 가치이전에 대해서 연구가 계속되어져 할 것이다.

## 참고문헌


[1] R.Sai Anand, C.E.Veni Madhavan, "An Online, Transferable E-Cash payment system", INDOCRYPT 2000, LNCS 1977, pp 93~103, 2000

[2] Markus Stadler, Jean-Marc Piveteau, Jan Camenisch, "Fair Blind signatures", EUROCRYPT'95, LNCS 921, pp 209~219, 1995

[3] 장석철, "분할성 및 익명성 제어를 갖는 네트워크형 전자화폐 시스템에 관한 연구", 석사학위논문, 순천향대학교 정보기술공학부, 2001년

[4] 김상진, 오희국, "해쉬 체인을 이용한 새로운 오프라인 전자화폐", 정보과학회논문지, 제 30 권 제 2 호, pp207~221, 2003년 4월,

[5] 용승림, 이은경, 이상호, "이중 해쉬 체인에 기반한 분할 가능 전자화폐의 설계", 정보과학회논문지, 제 30 권 제 8 호, pp408~416, 2003년 8월

[6] 이임영, " 전자 상거래 보안 입문", 생능출판사, 2001년