공인인증서 대체를 위한 블록체인 기반 개인인증 방안 연구

김진석*, 강정호**, 전문석* 김은환**
*숭실대학교 컴퓨터학과
**숭실대학교 평생교육원 정보보안학과
*e-mail:dooleya@ssu.ac.kr

A Study of Blockchain based Personal Authentication Scheme for the Accredited Certificate

Jin-Seok Kim*, Jungho Kang**, Moon-Seog Jun*, Eun-Hwan Kim**
*Dept of Computer Science & Engineering, Soongsil University
**Dept of Information Security, Soongsil University Life-Long Education

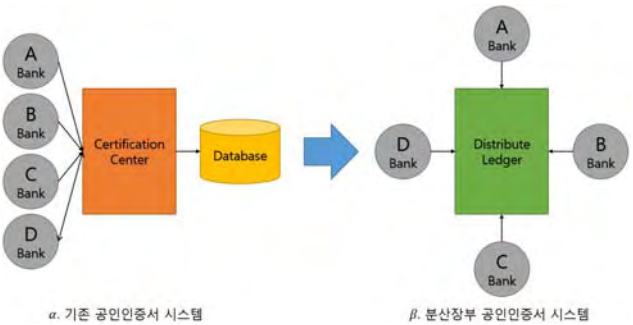
요 약

기존의 공인인증서는 한번 은행에서 발급 후 다른 은행에서 사용하려면 다시 등록해야 하는 번거로움이 존재한다. 또한 중앙 기관에서 공인인증서를 관리하기에 공격을 당했을 경우 개인정보 유출의 위험이 있다. 이에 대한 해결방안으로 은행 간에 블록체인을 사용하여 공인인증서를 발급 및 관리할 것을 제안한다. 블록체인은 다른 누구나 네트워크에 참여할 수 있고, 참여자 모두가 블록에 대한 검증을 하는 분산원장(Distribute Ledger) 기술을 사용하고 있다. 분산원장 기술로 공인인증서를 관리하면 사용자의 편의성 증대 및 보안 위협으로부터 안전할 것이다.

1. 서론

최근 비트코인의 가치가 상승함에 따라 전문 업계 종사자뿐만 아니라 일반인들의 비트코인에 대한 관심 역시 증가하고 있다. 비트코인은 2013년 키프로스 경제위기 이후 가치를 잃는 유로화 대신 가상화폐의 중요성에 대한 재조명을 받아 그 가치가 2013년 1BTC당 약 140불에서 2017년 9월 14일 기준 약 4000불까지 30배 이상 치솟았다. 비트코인은 누구나 네트워크에 참여할 수 있고, 참여자 모두가 블록에 대한 검증을 하는 분산원장(Distribute Ledger) 기술을 사용하고 있다. 이러한 분산원장 기술은 블록체인의 특징이기도 하다. 분산원장 기술을 사용하면 중앙 시스템이 필요 없으며 기록의 작성 시점을 객관적으로 알 수 있다. 또한 기록의 타당성을 모든 참여자에게 검증받게 된다. 이러한 블록체인의 장점은 중앙 시스템 없이 기관 간 24시간 거래가 가능해야 하며 거래에 대한 객관적인 검증이 필요한 금융권에서 유용하게 쓰일 수 있다. 그래서 2015년 국제 금융 기업 UBS(Union Bank of Switzerland)와 영국의 Barclays 은행 등 세계적인 금융기관들은 블록체인 기술 연구를 시작한다는 입장을 발표했다.

또한 블록체인은 공인인증서를 대체할 기술이기도 하다. 기존의 공인인증서는 금융결제원(Yessign), 한국전자인증(Crosscert) 등의 중앙기관에서 발급과 관리를 하고 있다. 그림 1의 α와 같이 A, B, C, D로 표기된 각각의 은행들에게서 개인이 금융서비스를 이용하고자 할 경우 하나의 은행에서 인증을 완료한 후 타 은행에서 금융서비스를 이용할 때에는 추가적인 등록이 필요하다. 또한, 이러한 중앙 시스템이 공인인증서를 관리하는 경우 공인인증서를 저장하고 있는 서버가 공격당하면 개인정보가 유출될 수 있는 위험이 있다.



(그림 1) 기존 공인인증서 시스템과 제안하는 분산장부 공인인증서 시스템

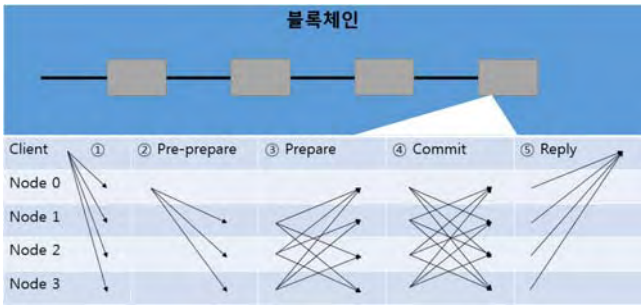
따라서 그림 1의 β와 같이 A, B, C, D 은행들이 블록체인의 분산원장 기술을 활용하여 공동으로 공인인증서를 관리하게 되면 사용자는 A, B, C, D 은행 중 한곳에서 한 번의 인증으로 다른 모든 은행에서 금융서비스를 추가등록 없이 사용할 수 있다. 사용자의 편의성 증대 및 공격으로부터 안전한 분산장부 형태의 인증 방법을 제안한다.

2. 블록체인 기술의 분류

<표 1> 블록체인 기술의 분류

	공용(Public)형	개인(Private형)	컨소시엄형
노드형	제한 없음	제한 가능	제한 가능
블록체인 검색	제한 없음	제한 가능	제한 가능
블록 생성시	높은 난이도 필요	임의	임의

블록체인 기술은 사용되는 네트워크와 용도에 따라 표 1과 같이 세 가지로 나누어진다. 첫 번째는 누구나 참여 가능한 공용(Public)형이다. 공용형의 경우 노드에 제한이 없다. 누구나 자유롭게 네트워크에 참여할 수 있으며 모든 참여자는 동등한 권리를 부여받아 언제 어떤 블록이 생성되었는지 검색이 가능하다. 비트코인이 사용하는 알고리즘인 PoW(Proof of Work)가 공용형 블록체인의 알고리즘으로써 사용된다. PoW는 블록을 만들어 배포한 후 더 많은 참여자가 사용하는 것을 올바른 블록으로 정의한다. 그렇기에 블록 생성시 높은 난이도를 요구하며, 해결 보상으로 비트코인을 지급하는 형식이다. 반면 네트워크의 상태에 따라 블록체인의 한 부분에 문제가 생긴 경우 블록을 확정짓는 파이널리티(Finality)가 불확실하다는 단점이 있다. 첫 번째 블록 생성 후 다음 블록이 모든 구성원들로부터 인정받기 위해서는 약 6개 정도의 블록이 더 쌓여야 가능하다. 두 번째는 개인(Private)형이다. 개인형 블록체인은 하나의 주체가 내부 전산망을 블록체인으로 관리하는 형태다. 개인형 블록체인은 내부 네트워크를 구성할 때 주로 사용되므로 참여 노드의 제한이 가능하다. 또한 구성원들이 검색할 수 있는 범위도 직급과 권한에 따라 제한할 수 있다. 블록을 생성할 때에는 공용형 블록체인과 달리 이미 신뢰받는 구성원들로 네트워크가 이어져 있기 때문에 보상을 지급할 필요가 없다. 개인형 블록체인은 악의적인 사용자에 대한 대비보다는 처리 속도와 파이널리티의 확실성에 중점을 두고 있다. 마지막으로 컨소시엄형의 경우 여러 기업들이 운영하고 미리 선정된 주체들로만 구성하는 블록체인 기술이다. 한명의 주체를 가지는 개인형과는 달리 여러 주체들이 참여하고 주체들간 합의된 규칙을 통해 네트워크를 운영한다. 그렇기에 네트워크의 확장이 용이하고 거래 속도가 빠르다는 장점이 있다. 컨소시엄형이 사용하는 알고리즘으로는 PBFT(Practical Byzantine Fault Tolerance)가 있다. PBFT는 네트워크의 모든 참가자를 미리 알고 있어야 한다는 전제가 붙는다. 그림 2를 보면 Node 0이 리더가 되고 자신을 포함한 모든 참가자에게 요청을 보낸다. 그 요청에 대한 결과를 집계하여 다음 블록을 결정한다. 만약 부정 노드 수가 f개라고 하면 전체 노드 수는 3f+1개여야 하며, 확정에는 f+1개 이상의 노드가 필요하다. PBFT의 동작구조는 그림 2와 같다.



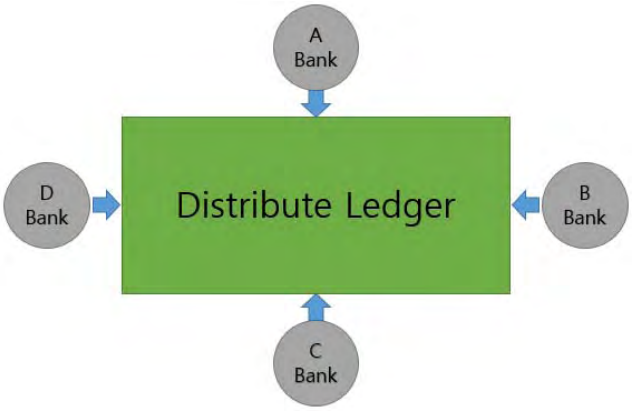
(그림 2) PBFT 알고리즘의 구조

① 클라이언트가 모든 노드에 요청을 보냄
② Node 0이 리더가 되면 다른 노드에 순서대로 명령을 전달
③ 각 노드들은 리더의 명령을 받으면 리더(Node 0)를 포함한 모든 노드에 회신
④ 각 노드들은 ③에서 전달된 명령을 일정 수 이상(2f) 수신하면 리더(Node 0)를 포함한 모든 노드에 수신한 신호를 전송
⑤ 각 노드들은 ④에서 보낸 명령을 일정 수 이상(2f) 수신하면 명령을 실행하고 블록을 등록해 Client에 Reply를 반환

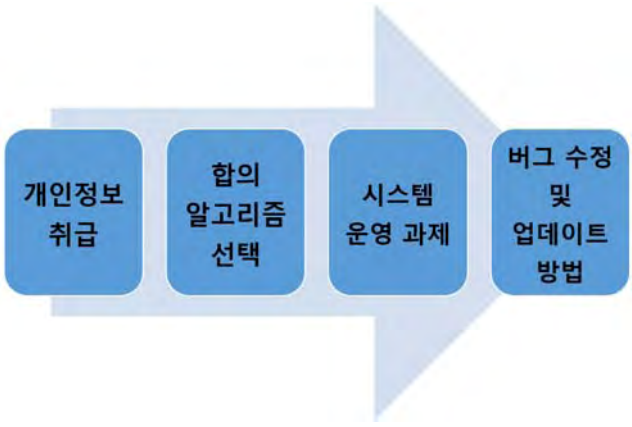
3. 블록체인 기반 개인인증

3.1 블록체인 기반 개인인증 기술

제안하는 시스템에서 그림 3의 A, B, C ,D 은행은 사전합의를 통해 컨소시엄형 블록체인 기술로 공인인증서의 분산장부를 만들기로 약속한다. 금융서비스를 사용하는 사용자는 주거래은행에 관계없이 같은 분산장부를 공유하는 은행 중 한곳에 가서 공인인증서를 발급받을 수 있다. 그림 3의 은행은 개인인증을 통해 공인인증서를 사용자에게 발급하고 그 내용을 분산장부에 저장한다. 분산장부에 저장된 인증서는 모든 은행이 공유하는 정보가 되어 사용자는 인증서를 등록한 은행뿐만 아니라 같은 분산장부를 공유하는 타 은행에서도 금융서비스를 수행할 수 있다. 또한 악의적인 목적으로 네트워크에 침입한 공격자가 한곳의 은행을 공격하여 개인정보를 조작하여도 분산장부에 저장된 인증서가 변조될 위험은 없다.



(그림 3) 블록체인 기반 개인인증 기술



(그림 4) 블록체인 기술 도입에 앞서 해결해야 할 과제

3.2 해결과제

이처럼 블록체인 기술을 활용하면 사용자의 편의성 증대 및 보안 위협으로부터 안전하다. 하지만 그림 4에서 보이는 것처럼 아직 해결해야 할 문제가 남아있다. 첫 번째, 개인 정보의 취급에 대한 부분이다. 블록체인 기술은 저장되는 정보를 암호화함으로써 정보 은닉 요구를 만족한다. 하지만 블록체인의 특성상 정보는 참여하고 있는 모든 노드들과 공유되기 때문에 은닉된 정보라고 할지라도 모두에게 전달되게 된다. 따라서 중요한 정보는 철저한 감시와 더불어 아예 블록체인에 저장하지 않는 것도 방법이 될 수 있다. 두 번째는 합의 알고리즘의 선택이다. 본 논문에서는 신뢰할 수 있는 기업들만이 참여하는 PBFT 알고리즘을 제안하였고 이러한 경우에 따라서는 중요도가 낮다고 할 수 있다. 세 번째는 시스템 운영의 과제이다. 비트코인 시스템이 이미 보여주듯이 블록체인 기술은 예기치 않은 변수 및 장애에 강하다. 하지만 동시다발적인 공격이 이루어진다면 데이터의 정당성을 구성원 전체에게 검증받을 수 없다. 따라서 사전에 시스템다운 등의 문제에 대비하여야 한다. 네 번째는 버그 수정 및 업데이트 방법이다. 블록체인 기술은 미리 설정해놓은 값을 갱신하는 것에 대해서는 쉽지만 새로운 프로그램의 추가나 기존 프로그램의 업데이트가 어렵다. 따라서 예기치 못한 문제가 발생했을 때의 해결방법에 대해 구성원들이 미리 합의해놓아야 한다.

4. 결론

비트코인을 시발점으로 이더리움(Ethereum), 리플(Ripple) 등의 다양한 가상화폐들이 쏟아져 나오며 많은 기관들이 안전한 시스템을 구축하면서도 유지비용을 최소화 할 수 있는 블록체인 기술에 대해 연구하고 있다. 이중 사전에 신뢰받는 기관들이 모여 블록체인 네트워크를 구성하는 컨소시엄형 블록체인은 본 논문에서 제안하는 개인인증 뿐만 아니라 무역, 의료 분야에도 다양하게 쓰일 수 있다. 하지만 한번의 개인인증으로 같은 네트워크를 구성하는 모든 은행에서 사용할 수 있다는 장점은 곧 2차 피해의 방지를 어렵게 만들 수도 있다. 공격자가 인증서 탈취에 성공할 경우 한 번의 공격으로 같은 분산장부를 이용하는 은행들 전체의 사용자 계정에서 피해가 발생할 수 있다. 그렇기에 향후 평소 거래량에 비해 큰 금액의 입출금시 거래가 일시정지 되거나 오랜 기간 쌓여온 블록과 신규 블록간 신뢰도의 차별을 두는 등 강화된 개인인증 방법에 대해 연구할 예정이다.

참고문헌

[1] 박성준. (2017). 블록체인패러다임과 핀테크 보안. 한국통신학회지(정보와 통신), 34(3), 23-28.

[2] 이동영, 박지우, 이준하, 이상록, 박수용. (2017). 블록체인 핵심 기술과 국내외 동향. 정보과학회지, 35(6), 22-28.

[3] 김신정, 김하은, 염용진. (2017). 블록체인의 금융업에 상용화에 따른 이슈. 한국통신학회 학술대회논문집, 602-603.

[4] 이지언. (2017). 블록체인의 이해와 금융권에서의 활용. 금융포커스 26권 5호. 12-14.

[5] 아카하네 요시하루, 아이케이 마나부. (2017). 블록체인 구조와 이론. 위키북스.