무선모바일 보안 환경에서 블록체인 암호기술의 동향

홍동성 · 조영복*

대전대학교 정보보안학과

Trends of Block Chain Cryptography in Wireless Mobile Security Environments

Dong-sung Hong · Young-bok Cho*

Daejeon University

E-mail :hds5664@gmail.com

요 약

IT기술의 발전과 함께 대두된 블록체인 기술은 단순히 비트코인과 같이 디지털 통화와 연관된 기술로 알고만 있었지만, 최근 들어 보안에서 새로운 기술로 떠오르고 있다. 특히 모바일 환경의 보안에서도 생체인식기술과 블록체인이 연계된 연구가 다양하게 진행되고 있고 무선모바일환경의 IoT기반에서도 각 다양한 디바이스간의 블록체인 기반의 인증들이 제시되고 있다. 본 논문에서는 현재 진행되고 있는 블록체인 기술과 무선모바일 환경에 적용 사례와 보안요구사항을 분석하여 향후 블록체인 연구를 진행하는데 가이드라인을 잡고자 한다.

ABSTRACT

Blockchain, which emerged with the development of IT technology, has emerged as a new technology in security in recent years, although it has only been known as a technology associated with digital currencies, such as bitcoin. In particular, various studies have been conducted involving biometric technology and blockchain in the security of the mobile environment, and blockchain-based certifications between different devices are also presented in the IoT base of the wireless mobile environment. In this paper, we want to analyze the trends that are currently being applied to various wireless mobile environments and set up guidelines for future blockchain research.

키워드

FIDO(Fast Identity Online), 블록체인, IoT(Internet of Things), 스마트 그리드

I. 서 론

블록체인이 최초로 공개된 지 어느덧 10년이 다 되었다. 초기에 공개되었을 때는 암호 화폐에서만 사용되는 기술인 줄 알았으나, 다양한 분야에서 사용이 되고, 4차 산업혁명을 맞이하여 이제 모바일, 사물인터넷, 스마트 그리드와 접목해 한창 연구가 진행되고 있다. 모바일에선 기존의 생체인식에 블록체인을 접목하여 서버를 거치지 않고 인증정보를 공유 할 수 있는 연구인 블록체인 기반 FIDO(Fast Identity Online) 범용 인증 시스템이 있다. 이 연구에서 여러 도메인의 응용 서비스를 사용자의 FIDO 인증 정보를 한번만 등록하고 추가적인 등록과정을 거치지 않고 다른 응용 서비스의 FIDO 인증 서비스를 이용하며, 공인된 제 3기관을 거치지 않고 사용자의 FIDO 인증 정보를 안전하게

* corresponding author

공유할 수 있다. 또한 블록체인에 IoT를 접목하여 IoT 장치의 펌웨어(firmware)를 인증하는 연구가 등장했다. 블록체인 기반 펌웨어 인증은 IoT 장치가 펌웨어 업데이트를 수행할 때 업데이트 기록을 블록체인에 저장하는 방법을 제안했다. 그러나 이 연구는 무결성을 제공하는데 필요한 블록체인의 구성에 대한 고려가 없다. IoT 환경의 보안을 높이기 위한 연구로서 ChainVeri가 있다. ChainVeri는 블록체인의 무결성을 위해 블록체인을 구성하는 방법에 대해 고려하고 있다. 하지만 ChainVeri에 펌웨어 업데이트 기록을 위해 IoT 장치간, IoT 장치와 블록체인을 관리하는 노드 간에 정보를 교환할 때 메시지 및 데이터가 노출되는 문제가 있다. 펌웨어 관련 정보를 공격자가 수집하게 된다면, 공격자는 펌웨어 정보를 기반으로 알려진 취약점을 조사하고 공격 대상을 정하는 등 악의적인 공격에 사용될 수 있다.

본 논문에서는 다양한 환경에서 적용되고 있는 블록체인 기술의 동향을 분석해보고 향후 블록체인 연구에 활용한다.

Ⅱ. 모바일 환경에서 적용되는 블록체인 기술 동향

2.1 블록체인기술

블록체인은 거래정보를 특정 기관이나 중앙서버 등에 저장하지 않고 네트워크에 분산 저장하여 참여자 공동으로 기록, 관리하는 기술로, 모든 거래 정보를 포함하는 분산 원장 기술이다.

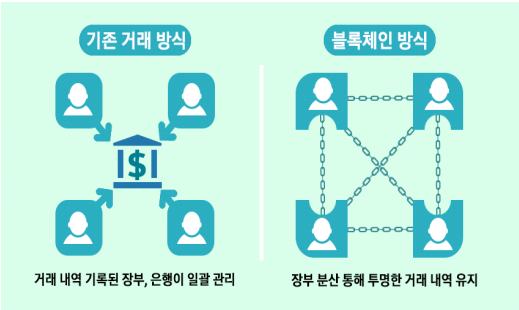

그림 1. 블록체인의 거래 방식

처음 블록체인이 등장 했을 때, 암호 화폐를 거래하는 과정에서 발생할 수 있는 해킹이나 위·변조를 막는 기술로 활용되어 관심을 받기 시작했다. 이제는 금융 분야뿐만 아니라 다양한 산업 영역으로 확장하고 있고, 4차 산업 혁명의 혁신기술로 주목 받고 있다. 특히 유통/물류, 에너지, 의료 그 외에 사물인터넷 등 이와 같이 다양한 분야에서 활용되어 사회적으로 큰 변화를 가져올 것으로 예상한다[1]. 아직까지 블록체인은 완성된 기술이 아니며 현재까지도 한계가 존재한다. 블록체인은 데이터의 무결성은 보장하지만, 네트워크의 참여자가 많아질수록 검증해야 될 데이터가 많아지면서 그만큼 네트워크 참여자들 간의 합의에 도달하는 시간이 늘어나게 된다. 또한 참여자간에 거래내역을 공유하기 위해서 필요한 데이터 저장 공간이 부족해 기술적으로 해결해야 될 과제기도 하다. 블록체인에 한번이라도 기록된 데이터는 임의로 변경 및 수정이 불가하고, 누적되어 블록에 저장되는 데이터 용량이 늘어날 수밖에 없다. 이 때문에 데이터 저장문제로 블록체인은 대용량 데이터를 기록하는 분야에서는 활용되기 어렵다는 비판이 존재한다.[2] 이 부분은 향후에 블록체인의 탈중앙화 규모를 줄이고, 새로운 합의 알고리즘 개발 및 거래 처리 속도를 높이는 방향으로 발전할 전망이다.[2] 또한 거래를 할 때 블록체인 데이터들은 삭제를 하지 않고 외부에 블록체인 데이터를 저장하는 방식으로 저장문제를 해결할 수 있고 차후에 블록체인에 저장되는 데이터 용량은 점차 줄어들 것으로 전망했다. 즉, 대용량의 데이터는 블록체인 외부서버에 보관하고 해당 데이터의 참조 값 과 접근 권한 정보, 데이터 무결성을 파악을 위한 키 값 등은 불록체인에 저장하여 외부서버에 저장된 데이터를 관리하는 방향으로 연구될 것이다.

2.2 IoT 환경에 적용한 블록체인기술

사물인터넷은 우리 생활속에 여러 사물들이 인터넷에 연결 가능한 기기로 발전해 오면서 인터넷을 통해 연결 가능한 사물들을 연결하여 사물과 사물 간에 정보를 교류하고 상호 소통하는 지능형 플랫폼이다. 각각의 사물은 목적에 따라 센서들이 연결되어 있고, 이러한 센서를 통해 사물은 데이터를 수집하고, 각각의 사물은 인터넷을 통해 사물인터넷 플랫폼에 보낸다. 그리고 사물인터넷 플랫폼은 이러한 데이터를 기반으로 생활에 도움이 될 수 있는 서비스를 제공한다. 하지만 사물인터넷 플랫폼은 대부분 중앙 집중형 플랫폼으로 확장성, 보안성, 안정성에 대한 단점이 존재하여 해킹, 단일 장애점 등 여러가지 한계를 보인다. 기존 사물인터넷 플랫폼은 여러가지 단점이 존재하며 최근 이러한 단점을 극복하기 위해 사물인터넷 플랫폼에 블록체인을 접목시키기 위한 연구들이 진행되고 있다. 이렇게 블록체인을 접목시킨 사물인터넷 플랫폼은 IoT 블록체인이라고 불리며, 기존 사물인터넷 플랫폼에서 확장성, 보안성, 안정성이 모두 개선된 플랫폼으로 이러한 IoT 블록체인의 예로는 IOTA[4]를 예로 들 수 있다.

IoT 블록체인에 저장되는 IoT 데이터의 경우 주로 개인 정보로 분류되기 때문에 허가된 노드만이 참여할 수 있는 프라이빗 블록체인으로 구축된다. 기존 블록체인은 누구나 참여 가능한 퍼블릭 블록체인이기 때문에 언제든지 새로운 노드가 참여할 수 있으며, 각 노드의 상태를 확인하지 않아도 된

다. IoT 블록체인의 경우 각 노드에서 IoT 플랫폼의 중요한 목적인 IoT 데이터 수집을 트랜잭션에 저장하여 블록체인에 저장하기 때문에 각 노드들의 상태와 블록체인 네트워크의 상태를 확인하는 것이 매우 중요하다.

2.3 스마트 그리드 환경에 적용된 블록체인

알파그리드(alphagrid)는 전력산업의 환경 변화로 인한 불확실성에 선제적으로 대응하는 미래형 스마트 그리드를 의미한다. 정보통신기술을 통해 주로 전력계통의 자동화와 효율성을 추구하는 스마트 그리드는 스마트 기기와 같은 쌍방향적인 통신 기술을 활용하지만 프로슈머인 인간에 대한 깊은 이해를 반영하지 않는다. 알파그리드는 인간적 요소로 인한 불확실성을 진지하게 고려한다는 점에서 진보된 스마트 그리드이다. 딥러닝과 빅데이터, 전기차, 신재생에너지, 사물인터넷, 스마트 기기, 블록체인 등 첨단 기술에 힘입어서, 국지적인 소규모 전력망을 의미하는 마이크로그리드가 활성화될 것이며, 절전과 신재생에너지 발전을 통해 비축했던 전기를 거래하는 개인 대 개인(P2P) 전력시장이 등장 할 것이다. 개인은 최선을 다해 자신의 이익을 추구하는 합리성과 함께 편향과 감정 같은 비합리성을 동시에 가진다. 사람들은 사회정치적 영향을 많이 받는 에너지 정책에 자신의 정치적 취향에 따라 비합리적인 태도를 보이기도 하는데, 이는 갈등을 증폭시켜 큰 사회적 비용으로 이어질 수 있다[3].

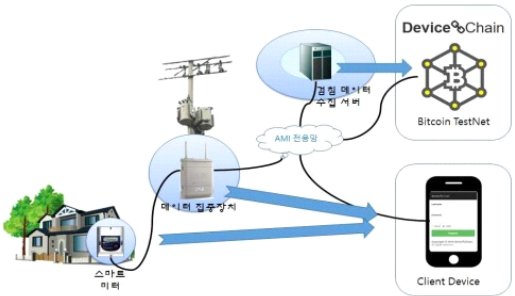

그림 2. DeviceChain 적용한 환경도

구현된 DeviceChain의 수행 절차는 그림2와 같다. 먼저 검침 서버와 AMI기기에서 DeviceChain을 통해서 Bitcoin TestNet 공개키 쌍을 각각 만든다. 검침 서버에서는 등록 대상 AMI 기기의 정보를 입력하고, AMI 기기에서는 자신의 기기 정보를 생성하고 해당 정보로 검침 서버에 기기 등록을 요청하면 검침서버에서는 기기정보를 확인하고 DeviceChain에 기기를 등록한다. 마지막으로 AMI 기기에서 검침 서버에 접속 테스트를 요청하면 검침 서버에서 DeviceChain을 통해 해당 기기의 인증 상태에 따라 인증 결과를 보여준다.

2.4 모바일 환경에 적용한 블록체인 기술

최근 모바일 단말에 지문과 홍채, 얼굴과 같은 생체 인식 기술이 탑재되면서 사용자의 생체 정보를 활용한 사용자를 인증할 수 있는 FIDO(Fast Identity Online)기술이 확산되고 있다. FIDO 인증 기술의 기본 개념은 사용자 단말에 적용되어 있는 인증 수단들을 온라인 서비스의 사용자 인증 수단으로 사용이 가능하도록 지원하고, 이를 위해 사용자 확인, 인증 프로토콜 및 인증 서버를 그림과 같이 분리하였다.

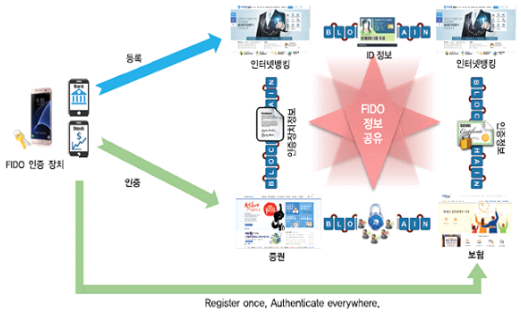

그림 3. FIDO 인증기술

FIDO 인증 시스템의 동작을 요약하면 처음에 사용자 확인 단계에서 FIDO 인증장치가 지원하는 인증수단을 이용하여 해당 인증 장치에 등록된 사용자인지 확인을 한다. 그다음 FIDO 인증 장치와 서버간의 인증단계가 여기서 공개키 기반 구조 인증기법을 사용한다. 여기서 서명을 위한 개인키와 검증을 위한 공개키가 필요하고, 두 키들은 FIDO 인증 장치에서 사용자 확인이 정상적으로 완료되었을 때만, 자체적으로 생성하고 관리한다. 그리고 FIDO 인증장치는 생성된 공개키를 FIDO 서버에 등록하고, 이후 FIDO 인증 장치가 개인키로 서명한 인증 정보를 FIDO 서버에 등록되어 있는 공개키로 검증하는 방식이다. 결국 사용자가 FIDO 인증 서비스를 이용하기 위해 최초 한번의 FIDO 등록과정이 필요하다. 이런 구조적 특성은 사용자 측면에서 다양한 인증수단들을 사용할 수 있고, 사업자 측면에선 한 번에 서버에서 다양한 사용자의 인증 수단들을 수용할 수 있는 장점을 갖고 있다. 또한 사용자의 확인은 해당 디바이스 내부에서만 동작하여 사용자의 생체 정보 유출에 의한 프라이버시 문제에서도 자유롭다[4].

Ⅲ. 국내외 무선모바일환경에서 블록체인 연구의 동향

사물인터넷 플랫폼에 블록체인을 적용한 블록체인 기반 사물인터넷 플랫폼에 대한 연구가 활발히

진행되고 있다. 이에 따라 사물인터넷 플랫폼을 감시 및 분석할 수 있는 시각화 도구가 필요하여. 전자화폐를 위한 기존 블록체인의 시각화 도구들은 블록체인 관점에서 블록체인 내부 데이터를 시각화한 경우, 블록체인에 블록이 생성되는 시각화한 경우, 그리고 블록체인 네트워크의 정보를 시각화한 경우를 찾아볼 수 있다. 이를 기반으로 시각화 방법과 함께 사물인터넷에 맞는 시각화 방법을 추가한 블록체인 기반 사물인터넷을 감시 및 분석하기 위한 시각화 도구를 연구하고 있다[4].

Ⅳ. 결 론

블록체인 기반의 FIDO 범용 인증 시스템은 모든 응용 서비스의 사용자 ID만을 이용하여 블록체인에 기록되어 있는 사용자의 FIDO 인증 정보를 조회할 수 있는 ID연결방식이다. 이를 통해서 사용자는 FIDO 등록과정을 단 한번 수행하고 추가적인 FIDO 등록 과정 없이 타 응용 서비스의 FIDO 인증 서비스를 이용할 수 있고, 서비스 제공자는 제3의 기관을 거치지 않고 사용자의 FIDO 인증 정보를 안전하게 공유 및 활용이 가능하기에 FIDO 서버설치비용과 유지보수비용을 줄일 수 있을 것으로 기대된다. 이는 단순히 모바일에서가 아닌 PC에서도 신속한 인증서비스가 가능해져 다양한 인증서 도입의 촉매제가 될 것이다.

또한 블록체인과 FIDO 기술의 진화에 힘입어 인증서 시장이 단순한 ‘보안’ 위주가 아닌 ‘강력한 보안을 전제로 한 효율성과 편리성’ 중심으로 재편될 전망이다.

References

[1] M.H Lim, “The Influence and Implications of Blockchain Technology." *Weekly Technology Trends,* pp. 2-13 Dec. 14. 2016.

[2] J.Y Lee, C.W Woo "Prospects and Limits of Blockchain Technology and Its Implications" Future Horizon pp. 12-15 no. 4 Dec. 31. 2018.

[3] S.H Lee, K.J Kim "Device authentication in Smart Grid System using Blockchain" *Conference on Information Security and Cryptography*, Seoul, pp. 1-4, Dec. 2018.

[4] S.H Kim, S.Y Heo, Y.S Jo, S.R Jo, S.H Kim “FIDO Universal Authentication System Based on Blockchain” *Electronic communication trend analysis,* vol. 33 no. 1 Feb. 2018.

[5] J.H Song, J.H jung, H.K Seok, J.H Nang "Design and Implementation of Visualization Tool for Blockchain based Internet of Things Platform." *Korea Computer Congress 2018*, Jeju pp.1684-1686 Jun. 2018.