블록체인에서 디지털서명 국내외 동향 분석

나장호[1], 김혜영[2]
[1]홍익대학교 대학원 게임학과(공학계열)
[2]홍익대학교 게임학부 게임소프트웨어전공
jang1na2@gmail.com, hykim@hongik.ac.kr

An Analysis on Trend of Digital Signature in Blockchain

Jangho Na[1], Hye-Young Kim[2]
[1]Major in Games, Graduate School, Hongik University
[2]Major in Game Software, School of Games, Hongik University

요 약

본 논문은 블록체인에서 사용 중인 디지털서명을 국내외 동향으로 분석하여 향후 기존 디지털서명 기술이 새로운 대안의 디지털서명으로 대체될지 전망을 분석하였다. 디지털서명의 국내외 동향은 해시함수, 타원곡선, 디지털서명 알고리즘 등으로 구별하여 파악하였다. 디지털서명의 해외 동향에서는 ECDSA 외에 몇몇 새로운 알고리즘 도입이 진행 중에 있었지만 국내 동향에서는 단 하나의 사례도 찾기 힘들 정도로 여전히 대부분 업체에서는 ECDSA를 사용 중에 있었다. 아직까지 국내에서는 ECDSA의 채택률이 압도적이지만 해외에서는 조금씩 새로운 디지털서명을 채택 중에 있었다. 향후에는 ECDSA의 채택률이 줄어들고 새로운 디지털서명의 채택률이 올라갈 것으로 예상된다.

1. 서론

비트코인[1]은 영향력을 계속해서 확장해나가고 있으며 이미 여러 나라에서는 비트코인이 보여준 블록체인 기술의 가능성과 새로운 모습의 전자결제 시스템은 디지털 세상에 거대한 변화를 가져오고 있다. 특히, 세계적으로 블록체인은 2015년 비탈릭 부테린(Vitalik Buterin)이 개발한 이더리움(Ethereum)[2, 3]이라 불리는 2세대 블록체인 플랫폼을 시작으로 다양한 기술을 접목하여 급속도로 발전하고 있다. 이러한 발전에서 블록체인 트랜잭션의 핵심 요소인 디지털서명이 중요한 역할을 하고 있다. 디지털서명[4]이란 첨단 기술로 보안이 강화된 전자서명의 한 종류로서, 개인키와 공개키를 이용한 전자서명이다. 블록체인에서 기록되는 데이터의 보안 및 무결성을 보장하는 중요한 요소 중 하나이다. 이러한 중요한 요소인 디지털서명 기술이 현재 블록체인에서 어떤 것을 채택 중이고 향후에는 어떤 새로운 디지털서명으로 대체될 것인지 아닌지 그 전망을 분석하였다. 디지털서명 현황을 국내 및 해외로 분석하여 해시함수, 타원곡선, 디지털서명 및 특징 등으로 표로 정리하였다. 정리한 국내외 동향 분석을 통해 기존 디지털서명 알고리즘과 새롭게 제안된 디지털서명 알고리즘의 향후 전망을 예상하였다.

2. 블록체인 디지털서명 해외 동향

현재 블록체인 업계에서는 디지털서명을 무엇을 사용하고 있는지 그 현황을 <표 1>로 정리하였다. 표의 구성은 블록체인별로 출시일, 해시함수, 타원곡선, 디지털서명, 특징을 조사했다. 대부분의 블록체인 업체에서 타원곡선암호를 사용 중이였고 그 중에서도 ECDSA 디지털서명체계를 채택중이다. <표 1>은 현시점으로 시가총액이 7조원 이상이며 세계 20위권 안에 들어가는 블록체인 암호화폐들 중에서도 현재 활발히 거래되어 사용량이 많은 대표적인 업체들만 정리하였다.

비트코인은 사토시 나카모토(Satoshi Nakamoto)에 의해 2008년에 출시되었으며 처음으로 암호화폐 개념을 만든다. 이 때 암호학적 배경을 ECDSA로 채택하고 해시는 SHA-256을 사용하며 타원곡선은 secp256k1을 처음 사용한다. 그 후 많은 블록체인 플랫폼에서 비트코인 디지털서명을 기반으로 암호화폐를 구축한다[1].

이더리움은 비탈릭 부테린(Vitalik Buterin)에 의해 2015년에 출시되었으며 해시는 SHA-256, 타원곡선은 secp256k1, 디지털서명체계는 ECDSA를 채택중이다. 특징으로는 현재 블록체인을 대표하는 플랫폼 중 하나라는 것이고, 스마트컨트랙트, EVM 등 2

세대 블록체인 기술이 시작된 플랫폼이다[2, 3].

카르다노(Cardano)는 찰스 호스킨슨(Charles Hoskinson)와 제러미 우드(Jeremy Wood)가 2017년에 출시했으며 ADA라는 암호화폐를 사용한다. 해시는 SHA-512, 타원곡선은 Curve25519, 디지털서명체계는 Ed25519를 사용 중이다. 특징으로는 대부분 업체들이 ECDSA를 채택할 때 카르다노는 Edwards 타원곡선을 채택했다는 것이고 미래에는 BLISS-B 디지털서명을 통합하여 양자 컴퓨터에 저항 가능한 서명을 추가하는 방향성을 갖고 있다[5, 6].

트론은 저스틴 선(Justin Sun)이 2017년에 출시했으며 디지털서명체계는 이더리움 기반으로 ECDSA를 사용한다. 특징으로는 이더리움 블록체인에서 독립하여 자체적인 네트워크를 구성하였다. 또한, 트론은 EVM을 사용하지 않고 따로 트론가상머신(Tron Virtual Machine)을 사용한다[7].

크로노스는 크리스 마자렉(Kris Marszalek)과 바비 바오(Bobby Bao)가 2016년 모나코라는 이름으로 처음 출시했고 그 후 이름을 변경해 2018년에 발행되었다. 2022년 현재는 크로노스로 이름을 또다시 변경하였다. 디지털서명체계는 이더리움 기반으로 ECDSA를 사용한다. 특징으로는 자체적인 API를 운영하고 크로노스 메인네트워크(Cronos Mainnet)를 따로 사용하여 이더리움 네트워크와 호환되게 하였다. 전자결제 블록체인 플랫폼이다[8].

솔라나는 아나톨리 야코벤코(Anatoly Yakovenko)가 2020년인 최근에 출시했으며 디지털서명체계는 이더리움 기반으로 ECDSA를 사용한다. 특징으로는 리눅스 커널 커뮤니티에서 만든 가상머신인 BPF(Berkeley Package Filter)를 사용한다는 것이다. 핵심기술로는 역사증명(Proof of History)을 합의 알고리즘으로 채택하고 있다[9].

폴카닷은 이더리움 공동창시자인 개빈 우드(Gavin Wood)가 2020년인 가장 최근에 만들었으며, 해시는 Blake2b를 사용하고, 타원곡선은 sr25519, 디지털서명체계는 Schnorr 서명을 사용 중이다. 특징으로는 서로 다른 블록체인을 연결하는 인터체인 프로젝트이다[10].

<표 1>를 보면 대부분의 블록체인 업체들은 이더리움에서 사용 중인 ECDSA 디지털서명체계를 사용한다. 타원곡선은 secp256k1이며 해시함수는 SHA-256를 사용 중이다. SHA-256은 keccak-256 해시함수라고도 불린다. 현재 다른 디지털서명체계를 채택하고 있는 블록체인들을 보면 카르다노는 Ed25519 디지털서명을 채택하고 Edwards 타원곡선을 사용한다. 블록체인 업체들 중에 가장 최근 출시된 폴카닷만이 Schnorr 디지털서명을 채택중이였다. 해외 동향에서는 조금씩 ECDSA를 대체하는 새로운 디지털서명이 나타나고 있었다.

<표 1> 블록체인에서 디지털서명 해외 동향

업체명	출시일	해시함수	타원곡선	디지털서명	특징
비트코인	2008	SHA256	secp256k1	ECDSA	사토시 나카모토가 만든 최초의 블록체인 개념을 확립한 가상화폐이다.
이더리움	2015	SHA256	secp256k1	ECDSA	현재 블록체인을 대표하는 플랫폼이며 스마트컨트랙트 기술을 활용하여 2세대 블록체인을 시작하였다.
카르다노	2017	SHA512	Curve25519	Ed25519	대부분 이더리움 기반으로 개발이 되지만 카르다노는 Ed25519 디지털서명체계를 채택한다.
트론	2017	SHA256	secp256k1	ECDSA	이더리움 네트워크에서 분리되어 독자적인 네트워크를 구성하였으며 트론 가상 머신을 사용한다.
크로노스	2018	SHA256	secp256k1	ECDSA	크로노스는 독자적인 API와 크로노스 메인넷을 사용 중이며 이더리움 네트워크와 호환이 된다.
솔라나	2020	SHA256	secp256k1	ECDSA	리눅스 커널 커뮤니티에서 만든 가상머신 Berkeley Package Filter(BPF)를 사용한다.
폴카닷	2020	Blake2b	sr25519	Schnorr	폴카닷은 이종 블록체인을 연결하는 인터체인이며 Schnorr 디지털서명 체계를 채택하고 있다.

3. 블록체인 디지털서명 국내 동향

국내 블록체인 업계에서는 디지털서명을 무엇을 사용하고 있는지 그 현황을 <표 2>로 정리하였다. 표의 구성은 그 이전의 <표 1>과 같다. 국내에서는 블록체인 업체가 해외에 비하여 수가 적기 때문에 발전이 더딘 경향을 보인다.

메디블록은 현직 의사 출신인 이은솔과 고우균 대표가 2017년 공동 창시하였고 분산된 의료정보를 수집하여 제공하는 개인 맞춤형 의료 데이터 플랫폼이다. 메디블록은 이더리움 기반으로 설계되었으며 해시함수는 SHA256, 타원곡선은 secp256k1, 디지털서명 체계는 ECDSA를 채택하고 있다[11].

모스랜드는 손우람 대표와 노정석 이사가 2018년에 출시하였으며 현실 세계의 랜드마크들을 소재로 하는 가상 부동산 게임 플랫폼이다. 위치기반의 AR(Argument Reality) 모바일으로 증강현실 서비스가 지원된다. 모스랜드는 이더리움 기반으로 설계되었으며 해시함수는 SHA256, 타원곡선은 secp256k1, 디지털서명 체계는 ECDSA를 채택하고 있다[12].

클레이튼은 주식회사 카카오의 자회사인 그라운드엑스가 2019년에 개발하여 출시한 블록체인 플랫폼이다. 클레이튼은 카카오와는 다른 독립적인 플랫폼이며 이더리움에 비해 탈중앙화를 약화시키고 대신 디앱(Dapp)에 실용성을 강화했다. 클레이튼은 이더리움 기반으로 설계되었으며 해시함수는 SHA256, 타원곡선은 secp256k1, 디지털서명 체계는 ECDSA를 채택하고 있다[13].

휴먼스케이프는 장민후 대표가 2019년에 정식 출시하였고 블록체인 기반의 환자 커뮤니티를 위한 의료 데이터 플랫폼이다. 카카오 블록체인 플랫폼인 클레이튼의 의료분야 첫 번째 서비스파트너이기도 하다. 휴먼스케이프는 이더리움 기반으로 설계되었으며 해시함수는 SHA256, 타원곡선은 secp256k1, 디지털서명 체계는 ECDSA를 채택하고 있다[14].

밀크는 조정민 대표가 2019년에 출시하였고 블록체인기반 여행용 플랫폼이다. 주식회사 야놀자와 파트너 제휴를 맺고 있으며 다양한 이벤트를 제공한다. 밀크는 이더리움 기반으로 설계되었으며 해시함수는 SHA256, 타원곡선은 secp256k1, 디지털서명 체계는 ECDSA를 채택하고 있다[15].

플레이댑은 최성원 대표가 2020년에 출시하였고 블록체인 기술을 장착한 게임 서비스 플랫폼이다. 플레이댑은 출시한 디앱 게임들간에 거래를 가능하게 지원한다. 플레이댑은 이더리움 기반으로 설계되었으며 해시함수는 SHA256, 타원곡선은 secp256k1, 디지털서명 체계는 ECDSA를 채택하고 있다[16].

국내 블록체인 업체들은 따로 독자적인 디지털서명을 개발하여 사용하고 있지 않으며 대부분 업체들이 이더리움에서 사용하고 있는 ECDSA 디지털서명 체계를 기반을 개발하여 사용 중에 있었다. 현재까지 국내에서는 단 하나의 사례도 찾을 수 없었지만 해외 동향에서 최근 ECDSA 디지털서명을 대체하려는 연구 및 개발을 하고 있어 국내 블록체인 디지털서명도 그 추세를 따라갈 듯하다.

<표 2> 블록체인에서 디지털서명 국내 동향

업체명	출시일	해시함수	타원곡선	디지털서명	특징
메디블록	2017	SHA256	secp256k1	ECDSA	현재 환자 의료정보의 주체가 병원이지만 관리 권한을 환자 본인에게 부여한다.
모스랜드	2018	SHA256	secp256k1	ECDSA	AR 위치기반 기술을 활용하여 모바일에서 사용하는 가상 부동산 플랫폼이다.
클레이튼	2019	SHA256	secp256k1	ECDSA	카카오 자회사에서 개발하였지만 카카오와는 다른 독립적인 플랫폼이다.
휴먼스케이프	2019	SHA256	secp256k1	ECDSA	환자 의료데이터 플랫폼으로 카카오 블록체인 플랫폼 클레이튼에 서비스파트너이다.
밀크	2019	SHA256	secp256k1	ECDSA	여행용 플랫폼으로 주식회사 야놀자와 파트너 제휴를 맺고 있다.
플레이댑	2020	SHA256	secp256k1	ECDSA	플레이댑 플랫폼에 출시된 게임들 간에 자유로운 아이템활용 및 거래를 지원한다.

4. 결론 및 향후 방향

본 논문에서 우리는 타원곡선암호에 기반을 둔 디지털서명 체계가 현재 블록체인 업계에서는 무엇이 채택되어 사용 중인지 그 국내외 현황을 파악했다. 기존의 ECDSA 디지털서명이 여러 문제점들을 안고 있고 해외에서는 여러 가지 새로운 디지털서명 알고리즘을 이용하여 해결책 및 우수성을 갖는 미래 대안 디지털서명을 찾는 중이다. 국내에서는 아직까진 단 한 사례도 파악되지 않았지만 결국은 ECDSA 채택률이 낮아질 것으로 예상된다. 우리는 향후 제시된 새로운 디지털서명 알고리즘들과 기존 알고리즘인 ECDSA를 비교분석하여 데이터 수치 값을 얻는 연구를 하려고 한다. 더 나아가, 우리는 기술적 측면을 더욱 깊이 파고들어 블록체인에서 새로운 미래 대안 디지털서명으로 활용 할 수 있는 다양한 가능성을 찾는 연구를 계속 할 것이다.

Acknowledgement

이 논문은 2019년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2019R1A2C1008533)(2016R1A2B4012386) 또한 “이 논문은 2022학년도 홍익대학교 학술연구진흥비에 의하여 지원되었음”

참고문헌

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[2] A. M. Antonopoulos and G. Wood, “Mastering Ethereum,” O’ Reily Media, Inc. 2018.

[3] V. Buterin, “Ethereum white paper,” Ethereum Foundation, 2013.

[4] Hash Net,, Digital Signature [Internet], http://wiki.hash.kr/index.php/%EB%94%94%EC%A7%80%ED%84%B8%EC%84%9C%EB%AA%85.

[5] C. Hoskinson, “Cardano white paper : Why we are building Cardano,” Cardano Foundation, 2017.

[6] L. Ducas, “Accelerating BLISS: the geometry of ternary polynomials,” Cryptology ePrint Archive, 2014.

[7] J. Sun, “Tron white paper v_2.0,” Tron Foundation, 2018.

[8] K. Marszalek, B. Bao, “Crypto.com white paper v_1.03,” Crypto.com Foundation, 2020.

[9] A. Yakovenko, “Solana white paper: A new architecture for a high performance blockchain,” Solana Foundation, 2018.

[10] D. Salman, “Polkadot white paper: Cryptography Explainer,” Polkadot Foundation, 2021

[11] Hash Net, Medibloc [Internet], http://wiki.hash.kr/index.php/%EB%A9%94%EB%94%94%EB%B8%94%EB%A1%9D#.ED.8A.B9.EC.A7.95

[12] “Mossland white paper v2.2,” Mossland Ltd., 2018.

[13] “Klaytn white paper v2.1,” Ground X, 2019.

[14] “Humanscape white paper Ver 1.1.0,” Humanscape foundation, 2019.

[15] “The White Paper of Mileage Point Integration Platform in Lifestyle Sectors version 0.9.7,” Mil.k foundation , 2019.

[16] “PlayDapp white paper: From dApp to Blockchain-Powered Gaming Entertainment Ecosystem,” PlayDapp foundation, 2019.