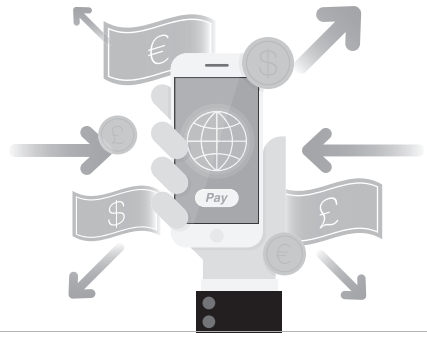
블록체인패러다임과 핀테크 보안



박성준 동국대학교 국제정보보호대학원 블록체인연구센터 센터장

1. 머리말

2008년 사카시 나까모도의 P2P 기반 암호화폐(cryptocurrency)인 비트코인(bitcoin)의 이중지불 방지(double spending)를 위해 창안된 블록체인(blockchain) 기술은 탈중앙화된 신뢰시스템 특성으로 인해, 현재 전 세계적으로 미래 세상을 견인할 혁신 기술로 주목받고 있다[1]. 이후 많은 블록체인 기반의 다양한 응용서비스가 개발되었으며, 핀테크 산업이 대표적인 응용분야 중 하나이다.

그러나 비트코인에서 사용한 블록체인 기술은 P2P 암호화폐시스템에 적합하도록 제한적이었다. 블록체인을 컴퓨터 개념으로 확장한 것은 이더리움을 창시한 부탈린이다[2]. 이더리움은 비트코인에서 이용한 블록체인을 모든 응용서비스가 가능하도록 암호화폐 기능에만 제한을 두지 않고 확장하였다. 이더리움 블록체인의 비전 및 목표는 P2P 네트워크 기반 하나의 글로벌 신뢰컴퓨터를 만드는 것이다.

이후 현재까지 다양한 블록체인이 개발되고 있으며 목적과 비전에 따라 다양한 특성을 지니게 된다. 블록체인 기술은 이해도에 따라 다양한 시각이 있으나 크게 다음의 5가지 관점에서 정의할 수 있다.

① 분산 장부(Distributed ledger)
② P2P 신뢰네트워크(P2P trusted network)
③ 스마트계약 플랫폼(Smart contract platform)
④ 글로벌 신뢰컴퓨터(Trust world computer)
⑤ 제2의 인터넷 또는 가치의 인터넷(Internet of value)

현재는 각 비즈니스 영역의 특성(속도, 정보보호 특성 등)에 따라 다양한 블록체인 플랫폼이 개발되고 있는 실정이며 각 블록체인은 자체의 비전과 목표를 가지고 있다.

블록체인을 구성하는 방법에 따라 블록체인은 크게 퍼블릭(public) 블록체인과 프라이빗(private) 블록체인으로 구분된다. 먼저 P2P 신뢰네트워크 참여자들의 제한 여부에 따라 permissionless와 permissioned로 구분된다. Permissionless 블록체인은 네트워크 참여에 제한을 두지 않는 블록체인을 의미하며, permissioned 블록체인은 네트워크 참여에 제한을 두는 블록체인이다. 그리고 P2P 네트워크의 신뢰성(trust)을 확보하는 방법에 따라 퍼

블릭과 프라이빗으로 구분된다. 네트워크의 신뢰성을 확보하는 네트워크 참여자들의 자격에 제한을 두지 않는 경우가 퍼블릭 블록체인이며, 제한을 두는 경우를 프라이빗 블록체인(또는 consortium)이라고 한다. 따라서 크게 봐서는 4가지 블록체인이 존재하게 된다. 그러나 일반적으로 퍼블릭 블록체인은 퍼블릭, permissionless 블록체인을 통칭하며, 프라이빗 블록체인은 프라이빗, permissioned 블록체인을 통칭한다.

대표적인 퍼블릭 블록체인으로는 비트코인, 이더리움, 카르다노[3] 등이 있으며, 프라이빗 블록체인에는 하이퍼레져 패브릭(hyperledger fabric)[4], 리플(ripple)[5], R3[6] 등이 있다.

무엇보다도 블록체인 기술의 핵심 요소기술로는 바로 네트워크 참여자 간의 합의(consensus) 메커니즘으로 볼 수 있다. 물론 합의 메커니즘은 퍼블릭 블록체인과 프라이빗 블록체인에 따라 다양한 방식이 존재한다. 퍼블릭 블록체인의 대표적인 합의 메커니즘으로는 컴퓨팅 파워에 의존하는 작업증명(PoW, Proof of Work), 암호화폐 보유량에 의존하는 지분증명(PoS, Proof of Stake), 평판(reputation) 및 투표(vote)에 의해 일종의 국회를 구성하는 방식인 위임지분방식(DPoS, Delegated Proof of Stake) 등이 있다. 프라이빗 블록체인 합의 방식으로 대표적인 것이 비잔틴장군문제를 해결하는 솔루션인 PBFT(Practical Byzantine Fault Tolerance) 방식이다[7].

블록체인의 탈중앙화 및 정보공유 특성은 정보보호 문제를 야기한다. 블록체인에서 의미하는 보안성은 블록체인에 저장된 정보의 무결성(integrity), 또는 원본성(immutability)을 보장한다는 것이다. 그러나 무결성은 기본적인 정보보호 4대 서비스인 비밀성(encryption), 인증(authentication), 무결성 및 부인방지(nonreputation) 중 하나일 뿐이다. 특히, 블록체인은 개인정보보호 측면과는 모순되는 특징을 가지고 있다.

이를 해결하기 위해서는 블록체인 기술을 활용한 응용서비스를 개발할 경우 기존의 중앙화된 모델에서와 같이 정보보호 서비스 개발을 독립적으로 개발하는 해야 한다. 그러나 이는 블록체인 기술의 활성화에 장애요인이 될 수 있다. 따라서 블록체인 기술에 기본적인 정보보호 기능을 내재하는 것이 필요하다.

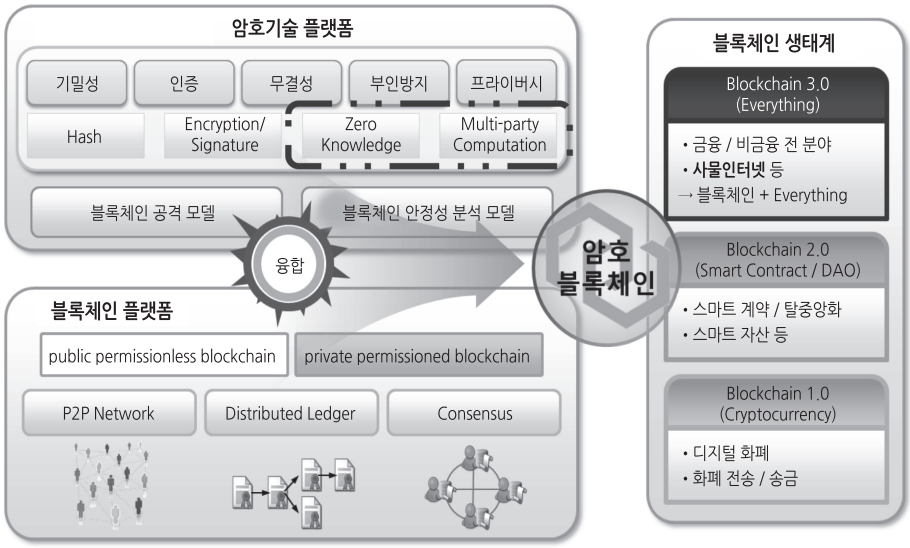
2. 암호블록체인

블록체인 기술의 장점을 극대화하고 정보보호 문제를 해결하기 위해 먼저 암호기술을 이해해야 한다. 보통 우리는 암호기술 하면 평문을 암호화하여 암호문을 생성하는 암호알고리즘과 인터넷뱅킹에서 활용하는 신원확인 및 전자서명 기술을 떠올린다.

그러나 암호기술 분야는 매우 광범위하고 다양하다. 일반적으로 암호기술은 크게 7가지 분야로 구분할 수 있다.

① 비밀성(encryption)
② 전자서명(digital signature)
③ 의사난수(pseudorandomness)
④ 영지식 대화형 증명시스템(ZKIPs, Zero Knowledge Interactive Proof system)
⑤ 안전한 다자간 계산(SMPC, Secure Multi-Party Computation)
⑥ 정보은닉(information hiding)
⑦ 다른 학문과의 융합(카오스, 인공지능 등)

비밀성 기능을 갖는 암호화기술, 인증기능을 갖는 전자서명기술, 랜덤성을 확보하는 의사난수기술(Pseudorandomness) 등은 이미 실현되어 활용하고 있는 분야이다. 현재 인터넷뱅킹의 보안을 확



[그림 1] 암호블록체인 개념

구분	인터넷	블록체인인터넷	암호블록체인인터넷
비밀성	X	X	O
인증	X	X	O
무결성	X	O	O
부인봉쇄	X	△	O
개인정보보호	-	-	O

[그림 2] 암호블록체인과 정보보호

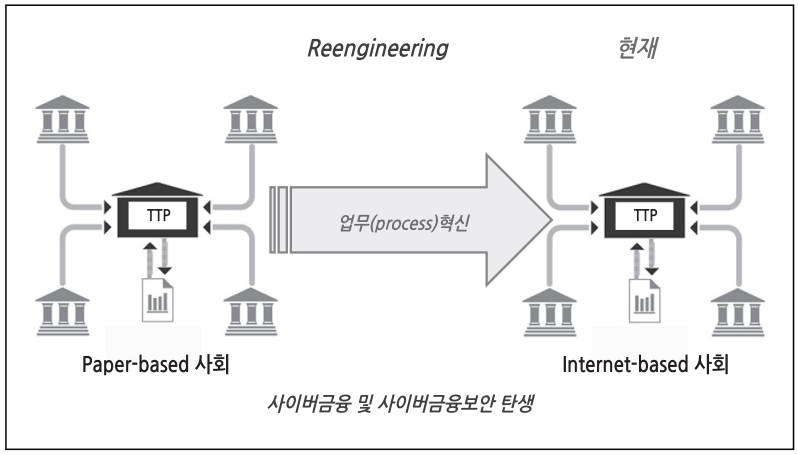
보하기 위해 사용하는 일회용비밀번호(OTP, One Time Password)가 의사난수를 이용하고 있다. 특히, 비트코인의 경우 계정 및 거래 생성을 위해 전자서명기술을 사용하며 각 계정의 공개키 및 개인키 생성을 위해서는 의사난수기술을 사용하였다.

블록체인의 정보보호 문제 및 개인정보보호를 해결하기 위해서는 비트코인에서 사용한 3가지 기술(비밀성, 전자서명, 의사난수)외에 영지식대화형증명시스템 및 안전한 다자간 계산이 중요한 역할을 담당하게 된다[8][9].

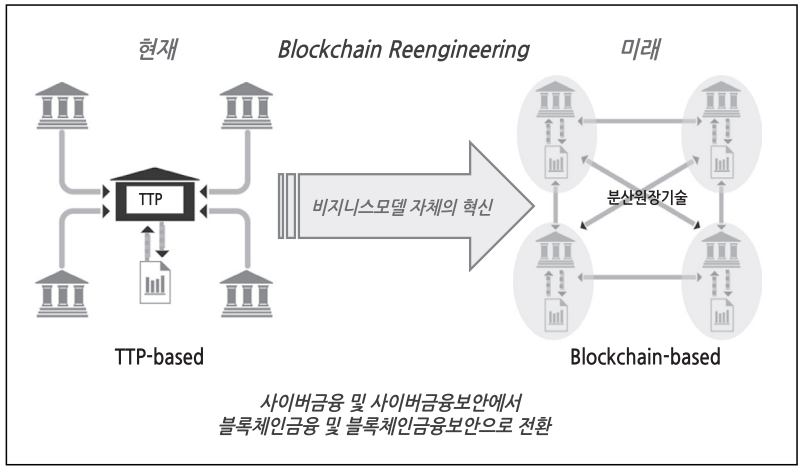
특히, 블록체인 기술의 정보보호문제 및 개인정보보호 문제를 해결하는 방법으로 암호기술을 블록체인 아키텍처의 기본 모듈로 내재하고 있는 실정이다. 블록체인 기술과 암호기술을 융합(통합이 아닌)한 블록체인을 암호블록체인이라 명명하였다([그림 1]).

암호기술과 융합된 암호블록체인 기술은 블록체인의 기본적인 기능 외에도 정보보호 4대 서비스인 비밀성, 인증, 무결성, 부인봉쇄 기능뿐 아니라 가장 중요한 개인정보보호 기능 또한 내재한다([그림 2]). 그리고 현재 상용화되고 있는 대부분의 블록체인은 사실 완전하지는 않지만 암호블록체인의 기본적인 특징을 내포하고 있다고 보면 된다.

본고에서는 블록체인과 암호블록체인을 특별한 경우를 제외하고는 동일시 하는 것으로 한다.



[그림 3] 사이버패러다임과 리엔지니어링



[그림 4] 블록체인패러다임과 블록체인 리엔지니어링

3. 블록체인패러다임

필자는 20여 년 전 한국정보보호센터(현, 한국인터넷진흥원) 기반기술팀(암호기술 담당) 팀장 시절에 사이버패러다임을 역설하면서 사이버세상(또는 인터넷 세상)의 도래에 대비하기 위해 사이버보안 필요성을 강조하였으며, 특히 암호기술의 대중화를 위해 다양한 활동 및 정책 지원을 수행하였다. 이러한 활동이 전자서명법 제정과 더불어 여러 분야의 공개키기반구조(PKI, Public Key Infrastructure)가 구축되어 인터넷뱅킹 활성화의 초석이 되었다. 사이버보안이란 기존 종이문서에 기반을 둔 사회의 보안 개념을 인터넷 및 전자문서에 기반을 둔 보안 개념으로 바꾸는 것이다. 사이버패러다임으로 인한 업무 혁신 과정이 리엔지니어링(reengineering)이다([그림 3]).

이제 우리는 새로운 블록체인패러다임에 의한 블록체인 리엔지니어링을 해야 하는 시기에 직면해 있다. 사이버패러다임이 기존의 종이 기반 비즈니스 모델을 인터넷에 기반을 둔 전자문서 활용 비즈니스 모델로의 전환을 의미했다면, 블록체인패러다임은 인터넷 기반의 모든 비즈니스 모델을 블록체인 기반으로 전환하는 것을 의미한다([그림 4]).

특히, 사이버패러다임과 블록체인패러다임은 본질적인 측면에서 큰 차이를 나타낸다. 사이버패러다임은 기존 중앙집중적인 비즈니스 모델(신뢰기관 가정)은 유지하면서 업무 프로세스를 혁신하는 것이라면, 블록체인패러다임은 신뢰기관을 제거하는 특성으로 인해 업무 프로세스 혁신뿐 아니라 비즈니스 모델 자체의 혁신이기도 하다. 이런 연유로 블록체인 기술은 파괴적인 기술 또는 혁명적인 기술이라고도 한다.

블록체인패러다임에 의해 정보보호 측면에서도 혁신이 필요하다. 사이버패러다임에 의해 사이버보안이 탄생했듯이 블록체인패러다임에 따른 블록체인 보안이 필요하게 된다. 블록체인 보안이란 기존의 중앙집중식 비즈니스 모델의 정보보호 관점이 아닌 탈중앙화 신뢰시스템인 블록체인 기반 비즈니스 모델의 정보보호 관점을 연구하는 것으로 정의할 수 있다.

한편으로는 블록체인패러다임에 의한 블록체인 세상을 실현하기 위해서는 아직 해결해야 할 문제들이 존재한다. 가장 중요한 문제 중 하나는 성능이다. 그러나 오늘날 사이버세상이 탄생하는 과정을 돌이켜보면 초기의 많은 문제는 다양한 전문가가 연구한 결과 대부분 해결되었다는 것을 알 수 있다. 중요한 것은 장점은 극대화시키고 단점들은 개선하는 노력을 경주하여야 한다는 것이다. 블록체인의 성능 문제 또한 빠르게 해결되고 있는 실정이다.

2016년에 일본은 블록체인 기술을 활용한 자국 은행 간 지급결제 시스템에 대한 실험 및 검증을 한 결과 초당 1,500건의 충분한 거래 속도를 확보하였다(일본의 은행 간 속도 조건: 1,388건)[10].

4. 핀테크 보안

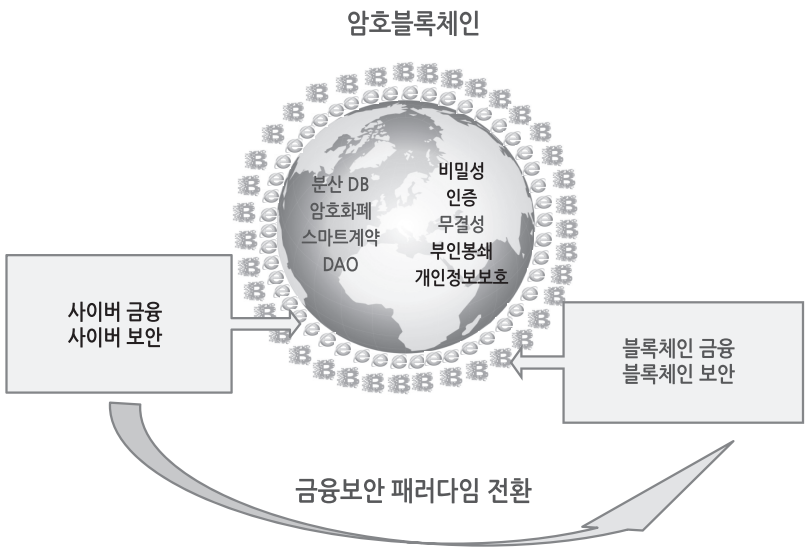
핀테크 산업은 블록체인패러다임이 금융 산업에 적용된 대표적인 블록체인 응용 사례로 볼 수 있다. 즉, 핀테크 산업은 기존의 인터넷 기반의 금융 산업을 블록체인 기반으로 전환한 것이다.

이제 핀테크 보안 분야도 블록체인패러다임에 의해 인식의 대 전환이 필요하다.

현재 핀테크 보안의 대부분이 기존 인터넷 기반 금융보안이라는 중앙집중적인 관점에서 연구되고 있는 것에 대한 인식의 대전환을 요구한다. 가까운 미래의 핀테크 보안은 인터넷 기반의 보안이 아닌 암호블록체인 기반의 탈중앙화된 관점의 보안을 고려하여야 한다. 예를 들어, 기존 핀테크 보안의 경우 신뢰기관을 가정한 중앙집중화된 금융산업의 정보보호 관점에 집중적으로 치중되어 있다. 그러나 암호블록체인 기반의 핀테크 산업은 신뢰기관이 존재하지 않는다. 따라서 기존의 정보보호 관점에서 다루기에는 한계가 존재한다.

공격 대상인 서버(신뢰기관)가 없는 블록체인 기반 핀테크 산업의 경우 해커는 서버가 아닌 네트워크와 경쟁해야 한다. 비트코인 또는 이더리움을 해킹한다는 것은 무엇을 의미하는 건가? 비트코인 및 이더리움에 대한 다양한 해킹 소식이 전해질 때마다 안타까운 것은 해킹의 의미에 대한 오해다. 예를 들어, 비트코인을 해킹했다는 것은 비트코인 자체가 아닌 클라이언트 지갑을 해킹한 사례이다. 이는 내 지갑에 있는 돈을 도난당했다는 것이며, 돈 자체 시스템에 대한 문제는 아닌 것이다.

가장 중요한 핵심은 상호 비교가 될 수 없는 금융생태계(현재의 중앙집중식 금융생태계와 탈중앙화된 금융생태계)를 같은 잣대로 분석해서는 안 된다



[그림 5] 암호블록체인패러다임과 핀테크 보안

는 것이다. 필자는 탈중앙화된 암호블록체인 기반의 핀테크 보안을 크게 다음의 2가지 관점에서 분석해야 한다는 것을 제안하고자 한다.

① 암호블록체인 자체의 안전성 증명
- 핀테크 산업의 인프라 관련 안전성 증명

② 암호블록체인 기반 금융서비스의 해킹 모델 정립 및 안전성 증명
- 핀테크 서비스 레벨에서의 안전성 모델 및 증명

또한, 앞서 이야기했듯이 기존 인터넷은 단순한 정보통신망 역할이었으나 암호블록체인의 경우 무결성을 보장하는 분산 DB, 암호화폐, 그리고 스마트계약 등 기본적인 데이터 및 거래에 대한 무결성 보장 기능 외에, 비밀성, 인증, 부인봉쇄 등 기본적인 4대 정보보호 기능과 개인정보보호 기능까지도 내포하고 있다. 이는 암호블록체인 기반의 핀테크 보안에서 상당 부분은 서비스 레벨이 아닌 인프라 레벨인 암호블록체인 기능으로 보장할 수가 있다는 것을 의미한다.

따라서 핀테크 보안이란 기존의 인터넷 기반의 금융보안과는 달리 암호블록체인이 보장하는 정보보호서비스를 제외한 핀테크 서비스 특성에 따른 보안에 집중하여야 한다. 대표적인 부분이 스마트폰 보안 분야로 생각할 수 있다. 즉, 서버보안이 아닌 클라이언트 보안 부문이다.

특히, 현재 다양한 관점에서 제기되고 있는 핀테크 보안은 암호블록체인으로 상당부분 해결할 수 있다고 생각한다.

5. 맺음말

본고에서는 암호블록체인패러다임에 의한 핀테크 보안의 대전환을 역설하였다. 핀테크 산업이란 인터넷 기반의 금융 산업을 암호블록체인패러다임에 의한 암호블록체인 기반의 금융 산업을 의미한다([그림5]).

암호블록체인은 기존 인터넷 인프라와는 달리 탈중앙화된 신뢰시스템으로 암호화폐 및 스마트계약

등의 기능을 가지고 있으며, 또한 기본적인 정보보호 4대 서비스와 개인정보보호서비스를 내포하고 있는 보안적으로 매우 우수한 차세대 인프라이다.

사이버패러다임에 의해 사이버보안을 고려했다면, 이제 블록체인패러다임에 의한 블록체인 보안을 연구해야 한다. 이는 블록체인패러다임에 의해 정보보호 관점도 재조명되고 인식의 대 전환을 요구 한다는 것이다.

암호블록체인상의 핀테크 보안은 블록체인이 가지고 있는 근본적인 정보보호 기능 외에 핀테크 산업의 다양한 서비스에 필요한 정보보호 조건들을 다시 분석하고 블록체인 인프라와 병행하여 정립해야 한다는 것이다. TTA

[참고문헌]

[1] 'Bitcoin: A Peer-to-Peer Electronic Cash System' at https://bitcoin.org/bitcoin.pdf

[2] 'Corporate website of Ethereum Foundation' at https://www.ethereum.org/

[3] Aggelos Kiayias, Alexander Russell, Bernardo David, Roman Oliynykov, 'Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol', 2016년 12월

[4] 'Hyperledger Whitepaper' at http://www.the-blockchain.com/docs/Hyperledger%20Whitepaper.pdf

[5] 'The Ripple Protocol Consensus Algorithm' at https://ripple.com/files/ripple_consensus_whitepaper.pdf

[6] 'About R3' at http://r3cev.com/about/

[7] KPMG, 'CONSENSUS', 2016년 8월

[8] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. Zerocash: Decentralized anonymous payments from Bitcoin. In S&P, 2014.

[9] G. Zyskind, O. Nathan, and A. Pentland. Enigma: Decentralized computation platform with guaranteed privacy.

[10] Blockchain Study Group, Report on Practical Experiment of Blockchain Technology in Japanese Domestic Interbank Payment Operation, Nob. 30, 2016.

정보통신 용어 해설 http://terms.tta.or.kr

스마트 홈 허브 smart home hub

가정에서 사용자의 음성 인식을 기반으로 인공 지능 서비스를 제공하는 허브.

스피커, TV, 거울 등이 매개체가 되어 가정 자동화(home automation) 서비스를 실현한다. 허브 기기에는 음성 인식 기반의 인공 지능(AI) 소프트웨어와 사물 인터넷(IoT) 기능이 탑재되어 있어, 전원이 켜져 있는 동안 마이크를 통해 사용자의 말을 듣고 처리하거나, 음성 데이터를 클라우드 서버로 전송하여 결과를 받아 작업을 수행한다. 스마트 홈 허브는 가전제품, 조명, 보안시스템 등 가정 내 기기를 사물 인터넷(IoT)으로 연결 · 제어하는 홈 허브 역할과 사용자의 음성 명령에 따라 음악을 검색하여 틀고, 실시간 교통 상황을 안내하며, 배달 음식 주문도 하고, 실내 온도를 조절하는 등 지능형 가상 비서(IPA: Intelligent Personal Assistant) 역할을 한다. 대표적인 스마트 홈 허브로 아마존 에코(Amazon echo), 구글 홈(Google Home), 애플 홈팟(Apple HomePod), SK텔레콤의 누구(NUGU) 스피커 등이 있다.