korbit
Research

Connect Wallet:
웹3 지갑의 발전상

2022.10.28

테마

Web3

관련 자산

Ethereum | ETH

Solana | SOL

작성자

정준영 | Junyoung Jeong

junyoung.jeong@korbit.co.kr

정석문 | Peter Chung

peter@korbit.co.kr

주요 자산 가격(2022.10.27)

BTC	
USD	$20,795
KRW	₩29,115,000
김치프리미엄	-0.82%

ETH	
USD	$1,563
KRW	₩2,193,000

웹3 지갑과 새로운 아이덴티티

가상자산 지갑 서비스는 통상적으로 블록체인 네트워크상의 공개 키와 개인 키를 생성, 관리하는 기능을 제공한다. 가상자산 자체는 네트워크상의 장부 기록으로 존재하며 사용자는 개인 키를 통해 자신이 소유한 자산에 접근하고 처분할 수 있다. 가상자산 지갑은 블록체인 서비스와 유저가 만나는 접점이 되며 가상자산 주소 및 계정은 웹3 환경에서 사용자의 신원(identity) 역할을 하기도 한다. 기존 인터넷에서 신원 정보가 특정 서비스 제공자 각각의 데이터베이스에 저장되는 데 반해 웹3 주소와 활동 내용은 특정 주체가 아닌 탈중앙화 네트워크 자체에 기록된다. 한편 웹3 계정에 활동 이력에 따른 평판과 신용(credit)을 부여하려는 시도도 이루어지고 있으며 이는 아이덴티티의 역할을 더욱 확장하는 계기가 될 수 있다.

지갑 서비스의 향후 발전 방향

월렛 서비스들은 그 기능적인 중요성에도 불구하고 유저 경험 측면에서는 개선 과제를 안고 있다. 키의 관리와 보관성, 유저 경험과 인터페이스, 체인간의 상호운용성 등이 개선 과제의 예이다. 이에 따라 유저 경험을 개선한 애플리케이션과의 통합, 멀티체인 지원 등의 개발이 이루어지고 있다. 향후 지갑 애플리케이션은 기존 서비스와 자연스럽게 연결되는 사용 경험을 추구하며 웹3 서비스에 접속할 때의 관문이자 종합 포털의 역할을 할 것으로 보인다. 또한 타깃 유저의 특성에 따라 높은 탈중앙성을 지닌 셀프 커스터디, 보안성, 혹은 접근 편의성 등 각 요소 간의 균형점을 찾아갈 것이다.

인프라로서의 가상자산 지갑

가상자산 지갑은 웹3의 대중 수용이 네트워크 효과의 변곡점(inflection point)에 도달하기까지 필요한 주요 인프라 중 하나이다. NFT의 인기와 친화적인 인터페이스로 단기간에 약 300만 개의 지갑을 생성한 레딧은 흥미로운 대중 도입의 사례를 보여준다. 단 정부 보조금을 활용한 높은 비트코인 지갑 보급률에도 실제 사용률이 낮았던 엘살바도르의 예시가 보여주듯, 인프라의 양적인 보급률 자체보다는 수용자에게 소구력을 가지는 용례와 지속적인 사용성을 창출하는 것이 더욱 중요하다. 향후에는 특히 SNS, 게임 등 수용층이 넓고 실생활에 밀접하게 닿아 있는 사용처가 웹3 월렛의 보급을 견인하는 선행적인 애플리케이션이 될 수 있다.

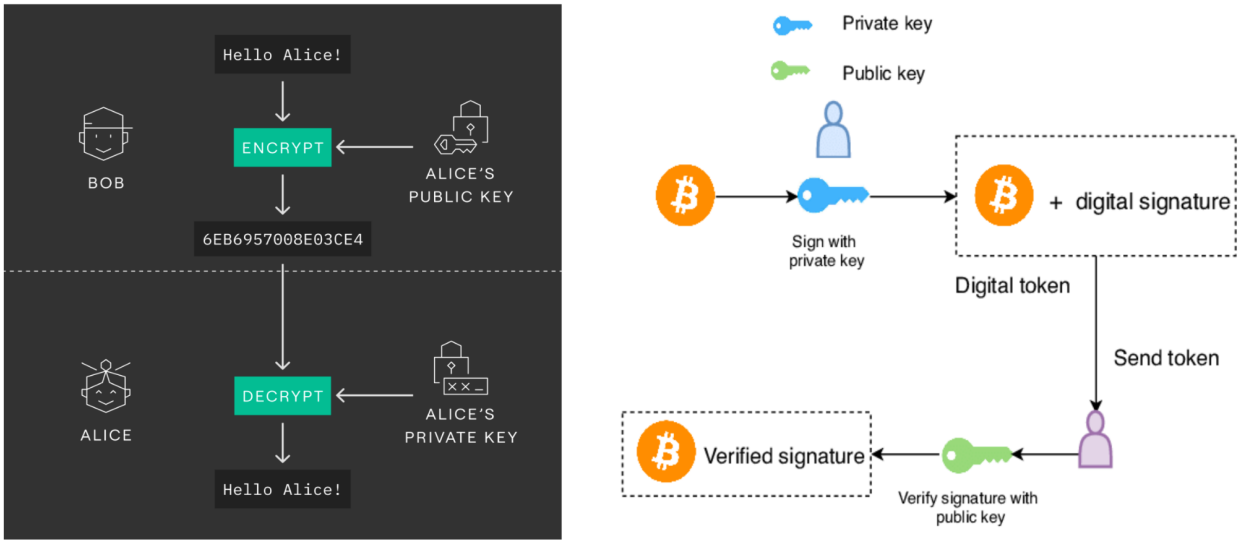
웹3 지갑의 개요

지갑의 작동 원리: 가상자산 지갑 서비스는 통상적으로 블록체인 네트워크상의 공개 키와 개인 키를 생성, 관리하는 기능을 제공한다. 가상자산 지갑에 실제 가상자산이 보관되어 있는 것은 아니다. 가상자산 자체는 네트워크상의 장부 기록으로서 존재한다. 지갑을 생성할 때 타인에게 공개되어 송금 등을 할 수 있게 하는 공개 키와 자신만이 알고 있는 개인 키가 함께 생성되며 개인 키를 통해 블록체인 네트워크상의 가상자산에 접근하고 처분할 수 있다. 개인 키는 루트 시드(root seed)로부터 함수화를 거쳐 임의로 생성된 난수 형태로 만들어진다. 대부분 루트 시드는 사용자 친화적인 12개 혹은 24개의 단어 형태의 니모닉으로부터 생성된다. 공개 키는 개인 키로부터 생성되지만 공개 키로는 개인 키를 유추할 수 없다.

비트코인을 포함한 많은 블록체인 네트워크들은 트랜잭션의 보안성을 위해 두 개의 서로 다른 키를 이용하는 '공개 키 암호화'라는 방식을 사용하고 있다. 공개키 암호화 방식에서 메시지는 수신자의 공개 키를 사용해 암호화를 거친다. 수신자의 공개 키로 암호화된 메시지는 수신자의 개인 키를 통해서만 복호화가 가능하다. 블록체인 상에서 자산 전송 등의 트랜잭션을 수행할 경우, 송신자는 자신의 개인 키를 활용해 트랜잭션을 서명(sign)하고 검증자들은 송신자의 공개키를 이용해 서명의 유효성을 확인할 수 있다. 즉 누구나 공개 키로 서명의 유효성을 검증할 수 있지만 서명을 수행하는 것은 개인 키를 통해서만 가능하다.

수탁 지갑과 비수탁 지갑: 수탁지갑(custodial wallet)과 비수탁지갑(noncustodial wallet)은 개인 키를 보관하는 주체에 차이가 있다. 가상자산 거래소에 계좌를 만들고 자산을 거래할 경우 일반적으로 해당 지갑에 대한 개인 키 및 보유 자산을 거래소라는 수탁자가 관리한다. 은행 서비스와 마찬가지로 수탁자가 자산에 대한 보관과 수탁을 제공하고 자산 인출 및 송금 등이 필요할 경우 이용자가 수탁자에게 전송해달라고 요청한다. 한편 비수탁지갑인 메타마스크의 경우 개인키 접근과 관리의 주체가 각 이용자이며 따라서 제삼자의 의사 및 운영방침에 관계없이 자신의 자산에 대한 통제권을 가질 수 있다. 이에 따라 개인키 관리의 권리와 책임은 모두 개인에게 귀속된다. 이처럼 제 3자의 중개 및 수탁 없이 자신이 개인 키의 관리에 대한 권한과 책임을 갖는 방식을 셀프 커스터디(self custody)라고도 한다.

Figure 1: 공개키 암호화를 통한 블록체인 트랜잭션 과정 출처: Coinbase, Anastasios Kalogeropoulos



지갑의 기능과 역할

가상자산 지갑은 공개 키와 개인 키를 관리하는 공간인 동시에 가상자산의 전송과 거래를 위해서 필요하기 때문에 웹3 서비스와 유저 간의 접점이 된다. 예를 들어 이더리움 네트워크에서 유니스왑 등의 디앱 서비스를 사용하기 위해서는 이더리움 네트워크에서 가상자산 지갑을 생성하고 지갑을 통해 네트워크에 접속(connect)한 후 디앱에서 보유한 ETH를 사용하는 과정을 거치게 된다. 가상자산 네트워크 이용에는 별도의 승인 절차가 필요하진 않으며 지갑과 함께 생성된 공개 키 혹은 지갑 주소(address)가 네트워크에서 상호작용의 주체가 된다. 즉 가상자산 지갑이 관리하는 주소 및 계정은 웹3 환경에서 사용자의 ID에 대응되는 신원(identity) 역할을 하기도 한다.

대표적인 가상자산 지갑으로 컨센시스(Consensys)사가 개발한 메타마스크를 들 수 있다. 메타마스크는 2022년 3월 기준 월간 활성 거래자 수 3천만 명을 기록하였으며 일간 스와프 거래 수는 지난해 말 2만 건을 넘어서며 최고치를 기록하기도 했다. 최근 약세장에 접어들면서 활용 지표들 역시 조정되는 모습을 보이고 있으나, 일간 스와프 거래 수는 여전히 7-8천건 수준을 유지하고 있다. 이외에도 솔라나 체인에서 주도적으로 사용되는 팬텀(Phantom) 월렛, 코스모스 네트워크에서 주로 사용되며 멀티체인 계정 관리, 스테이킹, 거버넌스 참여 등 기능을 제공하는 케플러(Keplr) 월렛, NFT 거래에 친화적인 인터페이스를 가진 레인보우(Rainbow) 월렛 등이 주요 월렛의 사례이다.

Figure 2: 메타마스크 일간 스왑거래 건수

출처: Dune Analytics

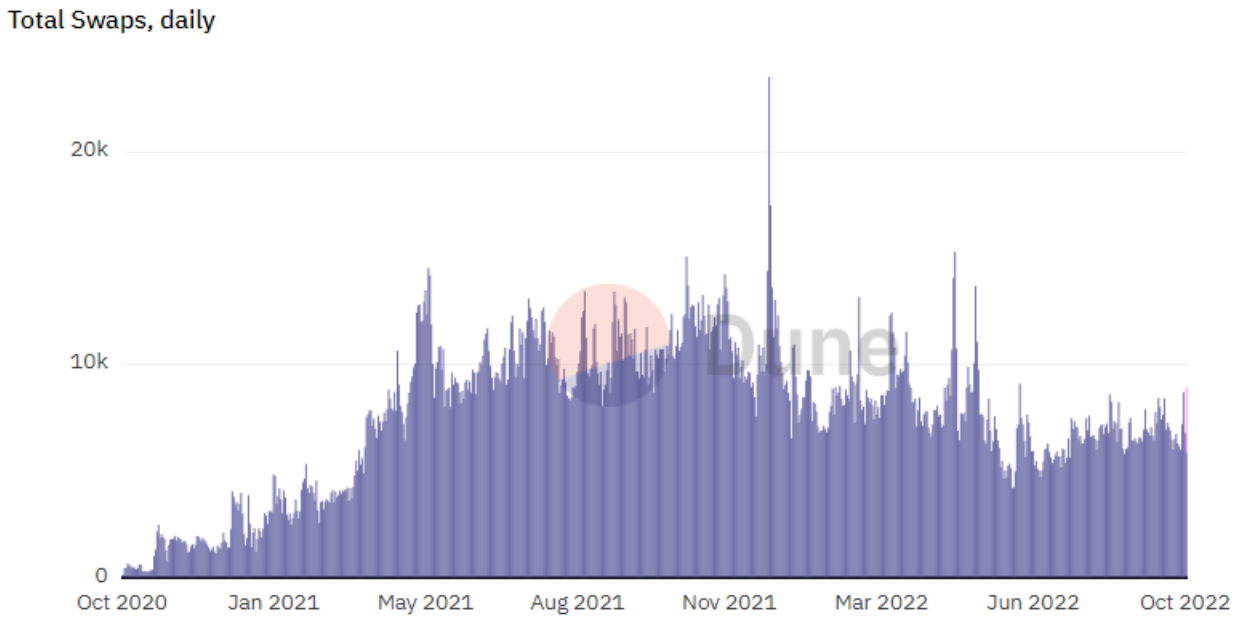


Figure 3: 케플러 월렛의 모바일 인터페이스

출처: Keplr

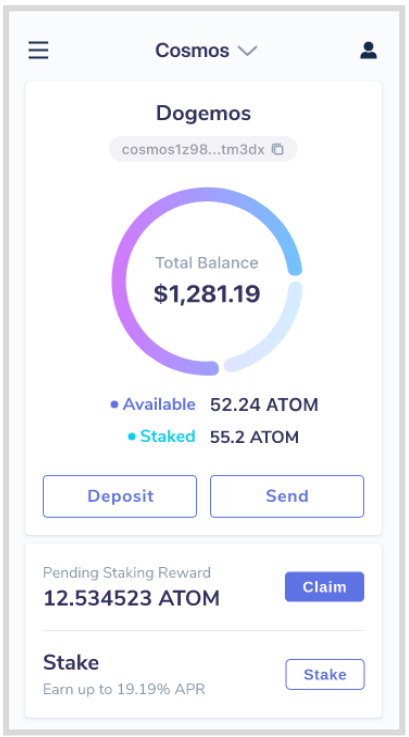
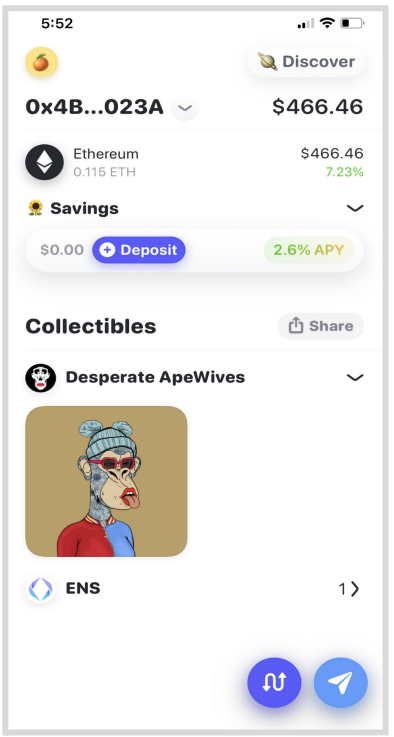


Figure 4: 레인보우 월렛의 모바일 인터페이스

출처: Howard Lindzon



웹3 지갑과 디지털 아이덴티티

‘Connect Wallet’ 후에 일어나는 일

과거 인터넷 사이트에서의 신원 인증(authentication)이 (말 그대로 신원을 뜻하는) ID와 패스워드를 통해 이루어졌다면, 웹3 환경에서는 지갑이 나타내는 주소가 곧 신원을 입증한다. 사용자는 ID나 이메일 주소, 휴대폰 인증이 아닌 ‘지갑 연결(Connect Wallet)’을 통해 블록체인 상의 디앱에 접속한다. 자산과 거래 기록은 지갑에 담겨있는 것이 아닌 블록체인 네트워크에 기록되어 있으며, 사용자는 지갑을 연결함으로써 자기 개인 키로 네트워크에 기록된 자산의 소유자임을 증명하고 자산을 사용하거나 처분할 수 있다.

이러한 신원 인증의 개념은 (비록 사이트마다 ID와 비밀번호를 설정할 필요가 없다는 점은 유사하나) 구글이나 페이스북 계정으로 여러 사이트를 로그인하는 SSO(single-sign-on) 방식과는 다른 형태이다. 기본적으로 웹2 환경에서의 신원 정보는 구글, 메타 등 각 서비스 제공자의 데이터베이스에 저장되며 서로 다른 업체의 데이터베이스는 일반적으로 분절(disconnected)되어 있다. ‘지메일로 로그인’은 공통의 일반 표준(OAuth 등)을 따르는 웹사이트에서 구글 데이터베이스상의 특정 인적 정보를 호출하는 것을 승인함으로써 가능하다.

유튜브나 인스타그램과 같이 (거의) 무료인 서비스를 제공하는 대신 사용자의 정보와 활동 기록을 수집하고, 이를 제삼자에게 제공하거나 광고를 포함한 다른 서비스에 연동하여 매출을 발생시키는 방식은 인터넷 기업들의 일반적 사업 모델이 되었다 (조지 길더, ‘구글의 종말’). 예컨대 페이스북의 개인정보처리방침은 페이스북이 유저의 활동 기록, 연결 관계, 기기 정보, 제삼자로부터 제공받은 정보(예컨대 ‘페이스북으로 로그인’한 다른 쇼핑몰에서의 구매 기록 등)를 수집하고 있으며, 수집한 정보를 “광고 등 맞춤화된 환경을 제공하기 위해, 그리고 설명된 다른 목적으로” 이용한다고 규정하고 있다. 즉 서비스 제공자가 개인이 생성한 정보를 수집하고 사용하는 주체가 되며, 그들의 데이터베이스는 수집된 데이터가 모이는 일종의 ‘저수지’가 된다.

반면 웹3 환경에서 지갑 주소는 특정 업체의 데이터베이스나 서버가 아닌 블록체인 네트워크 자체에 기록되어 있다. 활동 내역 등의 정보 역시 수집, 저장하는 특정 주체가 존재하는 것이 아니라 탈중앙화 네트워크 자체에 기록된다. 이는 서비스 제공자의 통제 없이 네트워크상에 존재하는 서비스를 하나의 아이덴티티로 장벽 없이 이용할 수 있게 하며 서로간에 정보와 디지털 소유권을 자유롭게 공유 및 전달 가능하게 해준다.

Figure 5: 웹 신원인증 방식의 변화

출처: Medium

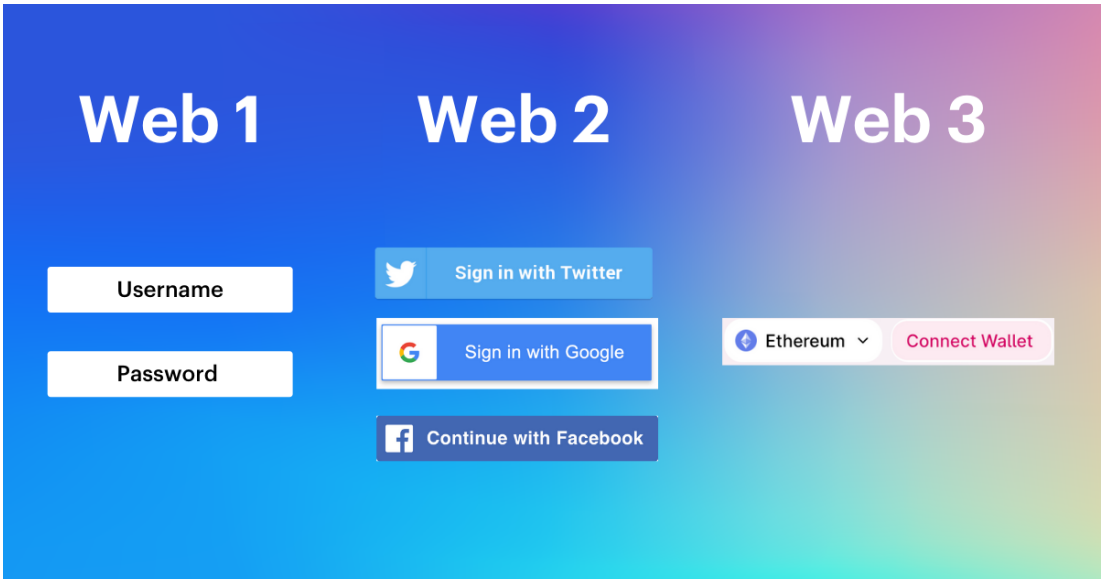
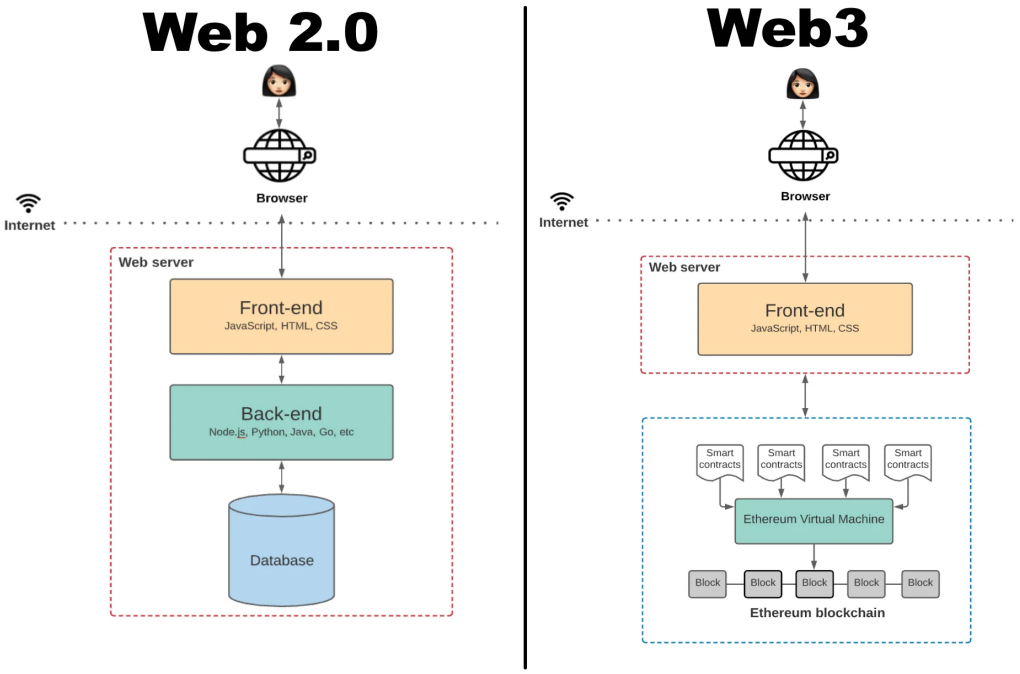


Figure 6: 웹2 vs 웹3의 데이터베이스 구조

출처: Preethi Kasireddy



계정과 주소를 웹3 아이덴티티의 기본 단위라고 한다면 각 계정이 트랜잭션 등 활동을 수행하며 집적되는 데이터는 개별 주체들을 구별하는 특성을 부여한다. 웹3 환경에서 아이덴티티는 대중적 수용을 이끄는 데 중요한 요인 중 하나로 여겨진다. 예를 들어 기존 금융에서 대출을 포함한 경제 활동은 많은 부분 신용(credit)을 기반으로 하고 있는 데 비해 디파이 서비스에서(특히 개인 이용자를 대상으로 한) 신용 기반 거래는 아직

제한적으로만 이용되며, 대부분의 대출이나 레버리지 활용은 상당 규모의 담보 자산을 요구하고 있다. Maple Finance 등 신용기반 대출을 제공하는 디파이 프로토콜이 존재하지만 Pool Delegate의 대출자에 대한 오프체인 실사(due diligence)에 상당 부분 의존하고 있다. 이는 현재로서 온체인상에서 각 계정의 신용도, 지불능력, 악의적인 행동을 할 위험 등을 평가할 '온체인 평판(on-chain reputation)'에 대한 충분한 데이터와 적절한 평가 방법이 없기 때문이다.

부테린은 가상경제에서 계정에 아이덴티티와 신뢰성을 부여하기 위한 방법 중 하나로 양도 불가능한 NFT를 뜻하는 소울바운드(soulbound) 토큰이 사용될 수 있다고 보았다. 출석 증명(proof of attendance) NFT가 가장 기본적인 활용 사례가 될 수 있다. 이에 더해 신용 기반 거래에 필요한 계정의 거래 내역, 대출에 대한 상환 이력 등이 계정에 대한 신뢰성을 제공해줄 수 있으며, 더 나아가 거버넌스 투표 등 계정 자체를 아이덴티티의 주체로 한 다양한 활용 사례가 모색될 수 있다. 옵티미즘은 시티즌 하우스라는 거버넌스 기구에 대한 시민권을 소울바운드 토큰으로 부여하겠다는 계획을 밝혀 이에 대한 실제 적용 가능성을 제시하고 있다. 하지만 여기에는 부정적인 낙인효과 가능성에 대한 비판과 함께 부테린 자신도 지적하듯 다중계정을 사용하거나 계정에 대한 소유권 자체를 매매하는 등 시스템의 허점을 이용할 수 있다는 우려가 함께 존재한다. 그는 계정 소유자 본인에 대한 증명(proof of humanity)을 도입하지 않고도 양도 가능성을 제한하기 위해 보안과 편의 사이에서의 절충안이 선택될 것으로 보았다. 또한 영지식증명 (zero-knowledge proof) 기술 등의 도입이 계정에 집적된 여러 개인정보를 직접 공개하지 않고도 특정 자격에 부합하는지 여부를 증명하게 할 수 있게 해 낙인효과에 대한 우려를 일부 완화할 수 있을 것으로 전망했다.

Figure 7: Maple Finance의 신용대출 기준은 KYC와 오프체인 실사를 요구 출처: Maple Finance

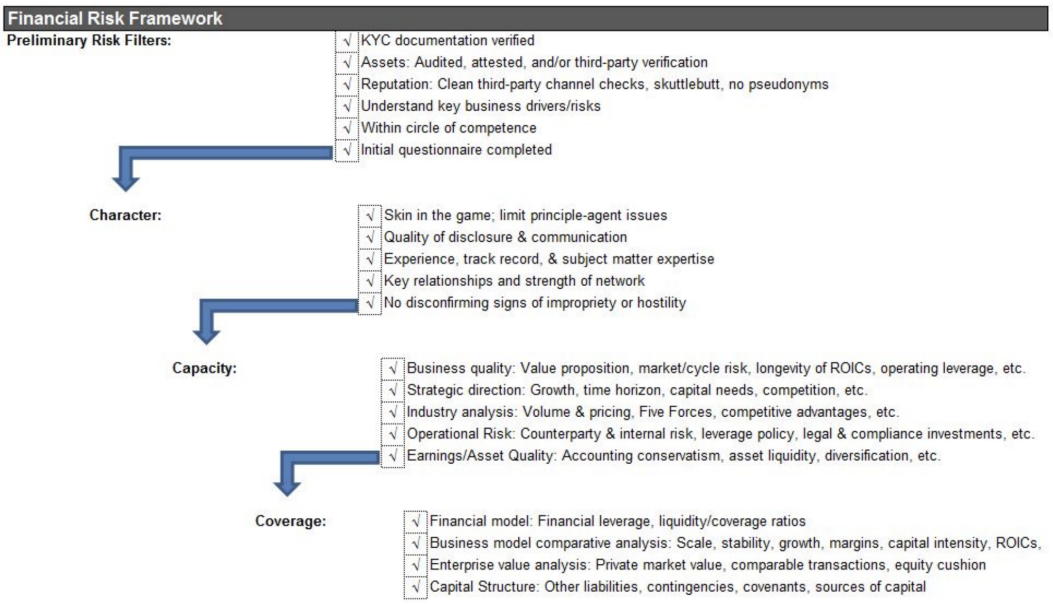


Figure 8: 소울바운드 토큰 활용 예시

출처: Crypto Times

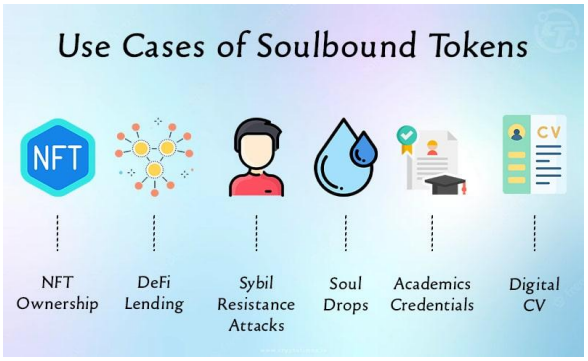
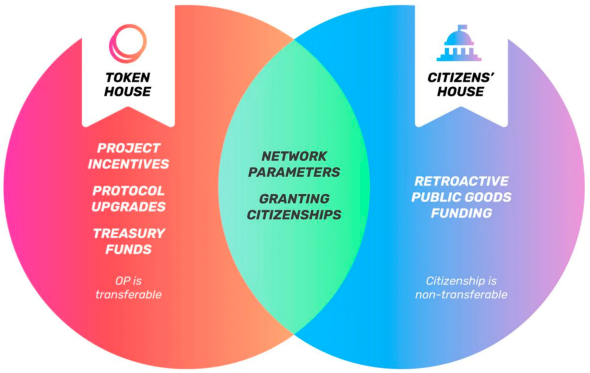


Figure 9: 옵티미즘의 거버넌스 기구

출처: Optimism



탈중앙화 신원증명 (DID)

디지털 방식의 신원 증명은 이미 예방접종에서부터 호텔 체크인에 이르기까지 일상 생활의 광범위한 영역에 퍼져있다. 팬데믹 기간 중에는 여러 국가에서 공공 장소나 민간 장소를 방문할 때 반드시 신원 확인 절차를 거치도록 하는 사례도 발생했다. 한편으로는 신원 정보의 중앙화 뿐 아니라 신원 정보 자체의 미비가 문제가 되기도 한다. 세계은행은 99개국을 대상으로 한 설문조사를 바탕으로 전 세계적으로 10억 명 가량이 주민등록을 포함한 신원에 대한 공식적 기록이 없으며, 투표권 및 법률, 사회보장제도의 혜택을 받지 못하고 있다고 추정하였다.

월드와이드웹 컨소시엄(W3C)은 탈중앙화 신원인증 (Decentralized Identifier, DID) 개념에 대해 "중앙화된 등록 기관을 필요로 하지 않는 유일하고 영구적인 신원 인증 수단으로 많은 경우 암호학적으로 생성 혹은 등록되는 것"으로 정의한다. 정의와 같이 DID는 반드시 블록체인 기술을 기반으로 하는 것은 아니지만, 블록체인은 분산화된 검증과 ID의 지속성을 가능하게 하고 데이터의 관리 권한을 개인에게 부여한다는 점에서 DID의 효과적인 구현 수단이 될 수 있다. 이는 KYC (고객확인절차)나 AML(자금세탁방지) 규정 준수가 필요한 서비스, 성인인증 등 유저에 대한 특정 정보가 필요한 서비스 등에 적용 가능하다.

여러 기업 및 프로젝트들이 블록체인을 활용한 실생활에서의 DID 구현 솔루션을 개발 및 제공하고 있다. Civic은 지갑 소유자의 개인 정보를 온체인상에 저장 및 보호함으로써 특정 기관에 개인 정보를 의탁하지 않으면서 컴플라이언스 사항을 준수할 수 있는 솔루션을 제공한다. 지갑 연결 후 최초의 KYC 과정으로 Civic Pass를 생성한 뒤 디앱 및 CEX에서의 신원 인증에 사용할 수 있다. SelfKey는 신원 데이터는 개인이 오프체인상에 보관하되 지갑 보유자에게 고유한 자체 주권(self-sovereign)의 신원 인증 키를 발급해 KYC 등에 사용할 수 있도록 한다. 마이크로소프트가 개발한 ION은 가장 신뢰성 있는 블록체인으로 여겨지는 비트코인 네트워크 상의 트랜잭션 실행 레이어로서 신원 인증이 가능하게 하고 있다. 국내에서도 SK텔레콤, LG CNS, 라온시큐어 등이 DID 개발 및 상용화에 참여하고 있다.

Figure 10: 미등록 인구(unregistered population)에 대한 세계은행 조사 출처: World Bank, Messari

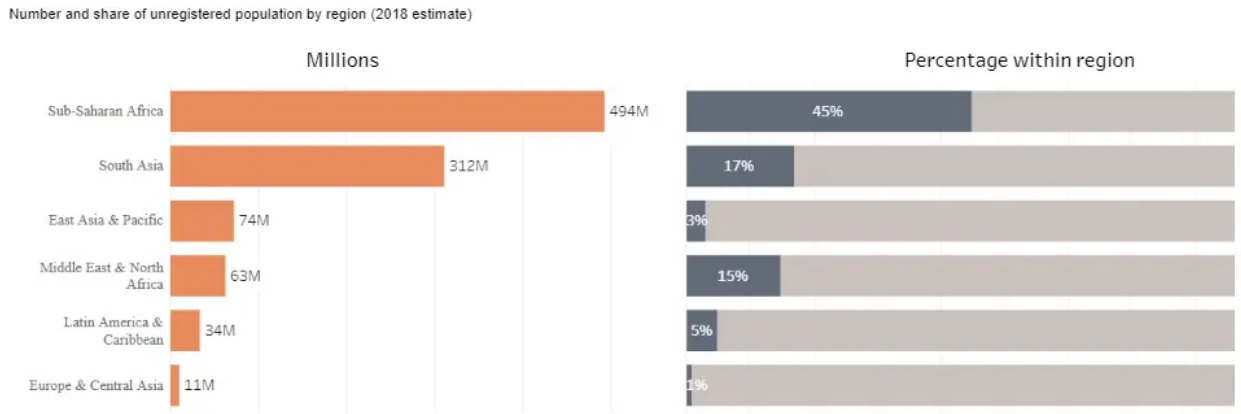
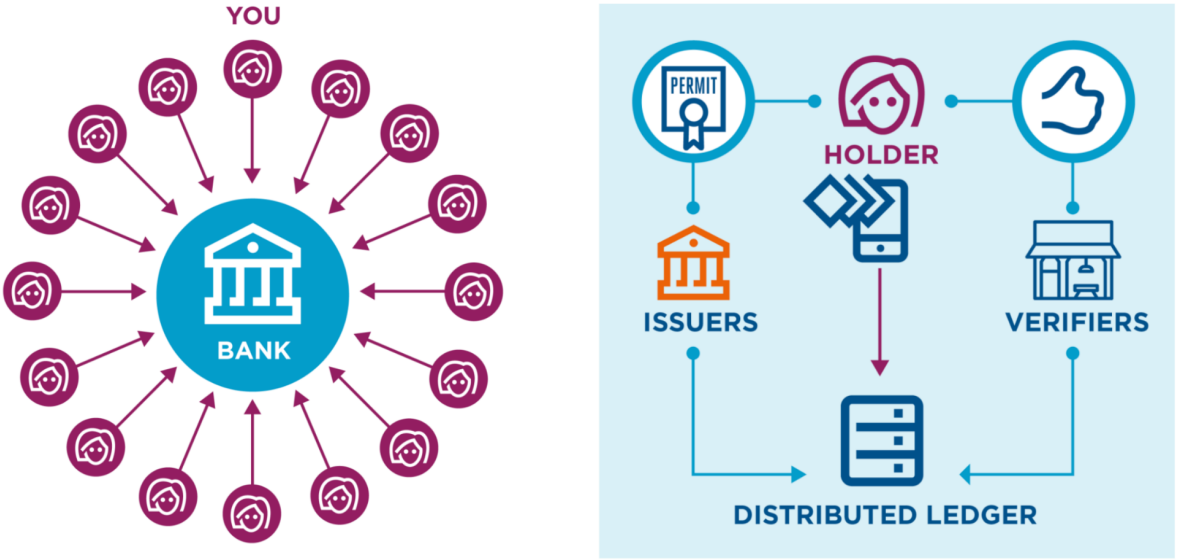


Figure 11: Centralized ID(좌)와 Decentralized ID(우)의 개요 출처: GSMA



지갑의 개선점과 발전 방향

월렛 서비스들은 그 기능적인 중요성에도 불구하고 유저 경험 측면에서는 많은 개선 과제를 안고 있다. 개발자이자 블로거인 Cory Hymel은 웹3 수용 확대를 위해 필요한 가상자산 지갑의 개선점으로 1)통합과 상호운용성, 2)온보딩 과정의 단순화, 3)유저 경험과 인터페이스의 개선, 4)보안성과 개인정보보호의 강화 요소 등을 꼽았다. 개선을 위해 해결해야 할 문제점을 다음과 같이 보다 자세히 들여다볼 수 있다.

키의 관리와 보안성: 비수탁 방식의 가상자산 계정은 별도의 중개 기관이 없기 때문에 분실할 때 사실상 복구 방법이 없으며, 개인정보를 요구하지 않기 때문에 개인 키나 시드 구문이 노출될 경우 타인이 쉽게 악용할 수 있다. 온라인에서의 정보 노출을 막기 위해 지갑 서비스 제공자들은 구문을 종이에 적거나 폴라로이드 사진으로 보관하는 등 아날로그적인 보관방식을 추천하는데, 대형 기관투자자의 경우에도 커스터디 사업자에 위탁하지 않는 계정은 여전히 아날로그적인 보관이 선호된다. 이러한 특성 때문에 7천 개의 비트코인이 담긴 USB 하드월렛의 비밀번호를 분실해 접근 방법을 잃어버린 사람의 케이스처럼 웃지 못할 일도 벌어지곤 한다.

이외에도 현실에서는 다양한 사유로 인해 자산 피해 사례가 발생한다. 시드 구문이 PC에 저장돼 있거나 이메일로 전송할 때 등의 해킹 피해, 개인 키 노출 유도, 실제와 다른 트랜잭션에 승인 유도, 피싱 사이트를 이용해 해커의 계정으로 자산 전송을 유도하는 것 등이 대표적인 사례이다. 개인 키에 대한 접근 권한을 내가 보유하고 있는 한 모든 트랜잭션은 본인의 서명과 승인이 필요하지만, 암호화 구문이 담긴 서명 안내문을 읽고 자신이 정확하게 어떤 트랜잭션을 서명하고 승인하고 있는지 파악하는 것은 때로는 가상자산에 익숙한 투자자들에게도 쉽지 않은 일이다.

너무 많은 체인과 지갑: 메타마스크가 지원하는 스왑(swap) 기능은 일종의 애그리게이터로서 한 체인 내에서 토큰 간의 교환을 편리하게 한다. 그럼에도 서로 다른 체인들을 이용 시의 상호운용성 및 UX 미비, 브릿지 이용의 불편 등은 멀티체인 환경에서 지갑 사용자 경험을 저해하는 요인의 하나이다. 예컨대 메타마스크는 이더리움, 아발란체, BNB체인 등 (주로 EVM과 호환되는) 수많은 체인들을 지원하지만 Rust 언어를 쓰는 솔라나 체인은 지원하지 않는다. 때문에 솔라나 체인에서 거래를 하는 사용자들은 팬텀(Phantom) 월렛 등을 별도로 사용해야 한다. 코스모스, 폴카닷, 클레이튼 네트워크 등 역시 각자 체인에서 주로 사용되는 월렛을 별도로 보유하고 있다. 사용자가 여러 체인을 함께 이용하기 위해서는 체인마다 다른 월렛을 설치하고 UX에 적응해야 하며 이는 체인 간의 자유로운 자산 교환과 전송에 있어서 사용자의 경험을 분절시키게 된다.

Figure 12: 메타마스크 서명 요청 사례

출처: Scopelift

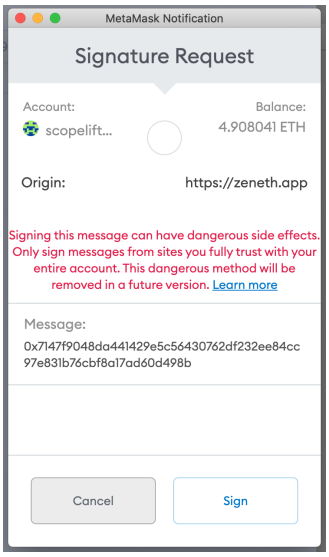


Figure 13: 솔라나 Slope Wallet에서의 자금 탈취

출처: Coindesk

지갑의 발전방향

정보 관리 편의성과 심리스(seamless) 유저 경험: 개인 키와 시드 구문의 관리 문제를 해결하고 편의성을 개선하려는 다방면의 접근이 이루어지고 있다. 한 예로 해치랩스의 Face Wallet은 '웹3 게임에 특화된 인게임 소셜 로그인 지갑'을 표방한다. 이는 시드 구문을 2개로 나누어 각각 사용자의 기기와 운영팀의 저장소에 나누어서 보관하여, 게임 인앱에서의 PIN 코드 접속 및 SNS 등을 통한 소셜 로그인 등이 가능하게 하는 형태로서 일부 개인정보 요구와 중앙 관리 요소를 도입하되 그 부작용을 최소화하고 non-custodial 구조를 유지하려는 시도로 판단된다.

토큰프루프(TokenProof)는 지갑 서비스가 아니면서도 지갑 사용 시 유저 경험을 개선하는 애플리케이션의 하나이다. 사용자는 모바일 앱에서 1회 서명으로 지갑의 실소유주임을 인증한 뒤에는 별도의 서명 절차 없이 QR코드 등으로 신원 인증이 가능하다. 추가적인 트랜잭션을 수행하지 않고 신원 인증 기능만을 수행하므로 지갑에 보유한 NFT를 이벤트 참여, 멤버십 인증, 온라인 쇼핑 등 실생활에서도 추가 서명이 필요없이 사용이 가능하다.

끊어짐 없이 자연스럽게 연결되는(frictionless) 유저 경험은 향후 지갑 애플리케이션의 중요한 추구 방향이 될 것으로 보인다. 더 나아가서는 월렛의 존재가 드러나지 않고(seamless) 유저가 월렛 서비스를 이용하고 있다는 것을 인지하지 못할 정도의 사용 설계도 가능하다. 게임을 예로 들면 외부 지갑 소프트웨어 설치 및 실행 필요 없이 인앱에 내재된 지갑 사용은 게이머들이 플레이 도중 지갑 사용을 위해 게임을 이탈하는 일이 없게 하여 직관적인 유저 경험에 기여한다. 또 다른 사례인 스타벅스는 폴리곤 체인 기반 멤버십 NFT 발행 계획을 밝히면서 별도의 지갑 앱

설치가 필요 없으며 기존 멤버십 앱 이용자들이 “NFT나 블록체인에 대해 아무것도 몰라도” 직관적으로 이용 가능한 서비스가 될 것으로 언급했다. 이는 향후 스타벅스 애플리케이션 자체에 지갑이 인앱 기능으로 내장되어 NFT의 보관 및 전송이 가능하게 하는 형태가 될 것으로 예상된다.

레딧 역시 사용자들이 볼트(Vault) 지갑을 생성해 NFT와 커뮤니티 토큰을 보관할 수 있게 했다. 최근 출시된 컬렉터블 아바타 NFT는 사용자가 직접 디자인하고 프로필로 설정할 수 있으며, 오픈시 등 다른 NFT 마켓플레이스와도 연동 가능하다. 볼트 지갑은 별도 앱 설치 없이 레딧 앱이나 웹사이트에서 신규 지갑 비밀번호 설정으로 생성될 수 있으며 신용카드로 토큰 구매 기능도 제공한다. 또한 레딧 사용자 간에 서로 커뮤니티 토큰이나 아바타 NFT를 전송할 수 있다. 레딧의 전체 일간 활성이용자는 약 5천만 명에 달하며, NFT를 보유하고 있는 볼트 지갑 수는 10월 말 현재 300만 개를 넘어서 상당한 이용률을 보이고 있다. 국내에서 신규 출시되는 서비스들 중에서도 월렛이 인앱에 내재되어 있는 경우를 찾아볼 수 있다. 한 예로 최근 런칭된 팬 기반 K-Pop NFT 마켓인 모먼티카 역시 자체 메인넷과 월렛을 지원해 NFT 컬렉팅과 공유를 보다 간편하게 하고 있다.

애플리케이션뿐 아니라 디바이스 자체에 월렛이 임베딩되기도 한다. 솔라나가 7월 런칭한 스마트폰 Saga는 안드로이드를 OS로 사용하면서 SMS(Solana Mobile Stack)라는 웹3 개발을 위한 오픈소스 SDK를 내장하고 있다. SMS에는 안드로이드 앱과 가상자산 지갑의 상호작용을 가능하게 하는 모바일 월렛 어댑터가 포함되며, 또한 솔라나 페이(Solana Pay)를 통해 지갑에 보유한 가상자산으로 QR코드 및 NFC 기반 실생활 결제도 수행할 수 있다.

Figure 14: Face Wallet 작동원리

출처: Face Wallet Docs

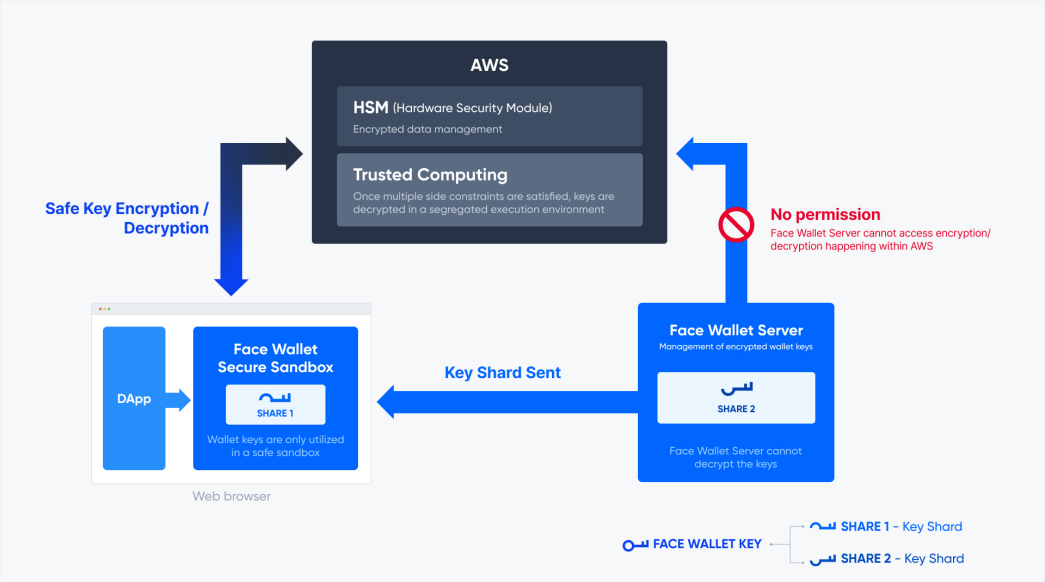


Figure 15: 레딧 NFT 보유 Vault 지갑 개수

출처: Reddit, Twitter @JuhyukB

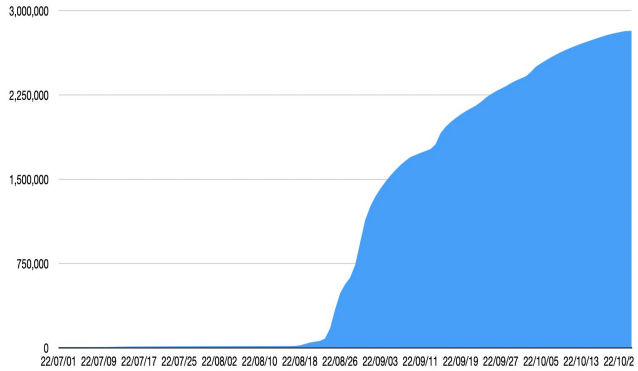


Figure 16: 다른 거래소 및 지갑과 호환되는 레딧 NFT

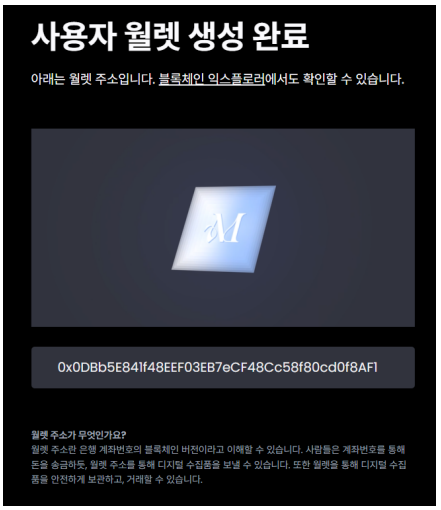
출처: Twitter @rainbowdotme

Figure 17: 솔라나의 Saga 스마트폰

출처: GizGuide

Figure 18: 인앱 지원 월렛의 사례 (Momentica)

출처: Momentica



멀티체인 지갑과 게이트웨이로서의 역할: 솔라나 네트워크에서 시작한 팬텀 지갑이 이더리움 네트워크를 지원하기 시작하는 등, 월렛 서비스들은 보다 더 많은 체인들을 지원하는 방향으로 나아가고 있다. Trust Wallet은 비트코인, 이더리움 네트워크뿐 아니라 메타마스크에서 지원하지 않는 폴카닷, 코스모스 체인을 함께 지원하여 지갑에서 관리할 수 있다. 국내 업체인 디센트의 디센트 월렛 역시 니어, 솔라나, 코스모스를 포함해 50개 이상의 체인을 지원하고 있으며, 이에 더해 콜드월렛과 소프트웨어 월렛을 하나의 앱에서 관리가 가능하도록 한다.

다만 멀티체인을 지원하는 월렛들도 월렛 자체에서 서로 다른 체인 간 메시지 및 자산 전송, 교환에 대한 구현은 아직 충분하지 않은 수준이다. 메타마스크가 DEX에서의 스왑 가격을 취합하는 애그리게이터 기능을 앱 내의 스왑 기능으로 내재화하였듯이 향후에는 체인 간의 메시징 및 브릿지를 통한 자산 전송 등도 지갑 자체에서 임베딩되어 이용가능하게 될 수 있다.

지갑 서비스는 웹3 환경에 접속하기 위해 이용자가 거치는 관문(gateway)의 역할을 한다는 점에서 웹브라우저와 유사한 점이 있다. 메타마스크가 크롬 브라우저의 확장 기능을 지원한 것은 사용자가 웹2 및 웹3 페이지를 보다 자유롭게 오가는 편의성을 제공하여 초기 성공에 기여한 요인의 하나가 되었다. 브레이브 월렛(Brave Wallet)은 이에 더해 월렛 기능을 포함한 자체 웹브라우저로서 디앱 이용과 개인정보보호에 보다 최적화된 환경을 제공한다.

현재의 월렛이 네트워크로의 기능적 접근성과 인터페이스를 제공하는 점에서 브라우저에 가깝다면 향후의 월렛은 더 나아가 네이버, 구글과 같은 포털과 유사한 역할로서 큐레이션과 검색 기능 등을 함께 제공하게 될 수 있다. 또한 현재 메타마스크 지갑이 스왑 수수료에서 대부분의 수익을 창출하고 있다면 향후에는 월렛 서비스가 사용자에게 여러 체인들과 디앱들을 발견하고 선택 및 접근할 수 있는 편의성을 제공하고 대신 수수료를 수취하는, 일종의 자체적인 마켓플레이스로 진화할 수 있다.

기관 대상 지갑: 기관투자자 및 기업들의 가상자산 진출 수요에 따라 기업들의 요구에 특화된 지갑 서비스들이 나오고 있다. 기관 및 기업들은 특정 목적을 위해 대규모 자산을 보유, 사용하며 보안성과 안전한 커스터디에 대한 수요가 더욱 높다. Ledger 등의 하드웨어 지갑들은 핫 월렛(hot wallet)에 비해 보안성이 높고 혹시 모를 해킹 위험을 방지할 수 있다는 점을 강조하고 있다. 메타마스크는 2021년 기관 사용자들에게 특화된 메타마스크 인스티튜셔널(Metamask Institutional)을 출시하였다. 컨센시스에 의하면 이는 콜드월렛에 비해 트랜잭션 과정을 간소화하고, 키 보관, 커스터디 서비스, 멀티시그 관리 등 기능을 강화하며 기업에 요구되는 수준의 높은 보안성 및 컴플라이언스 기능을 제공하고 있다.

탈중앙화 월렛: 컨센시스에 의해 운영되는 메타마스크를 포함해 많은 지갑 서비스들이 일반 사기업에 의해 운영되는 것에 비해 커뮤니티가 운영하는 탈중앙화 지갑에 대한 시도도 있다. 탤리 호(Tally Ho)의 Tally Wallet이 그 사례 중 하나로 Tally Wallet의 코드는 오픈소스로 공개되어 있으며 DAO 구성원들이 지갑에서의 스왑 수수료를 분배받고 거버넌스 제안 및 투표에 위임을 통해 참여할 수 있다. 자체 토큰인 'DOGGO'는 유니스왑에서 거래 가능하다.

기존 기업들의 진출: 월 활성 이용자(MAU) 2천만 명 이상을 기록 중인 주식 거래 플랫폼 로빈후드는 9월 자체 웹3 지갑의 베타 버전을 출시한다고 밝혔다. 로빈후드에서 USDC의 거래를 지원한 데 이어, 지갑

서비스를 매개로 한 가상자산 거래와 디파이 거래까지를 추구하고 있는 것으로 보인다. 국내에서도 삼성, SK텔레콤 등이 웹3 지갑 개발을 진행하고 있다. 한편 메타는 개발을 추진하던 디엠 스테이블코인의 상용화를 염두에 두고 코인베이스와 협력해 가상자산 지갑 서비스인 노비(Novi)를 파일럿으로 공개해 왔으나, 올해 7월 서비스 종료를 밝혀 상반된 모습을 보였다.

Figure 19: 메타마스크 인스티튜셔널

출처: Consensys

Figure 20: 디센트 월렛

출처: 디센트

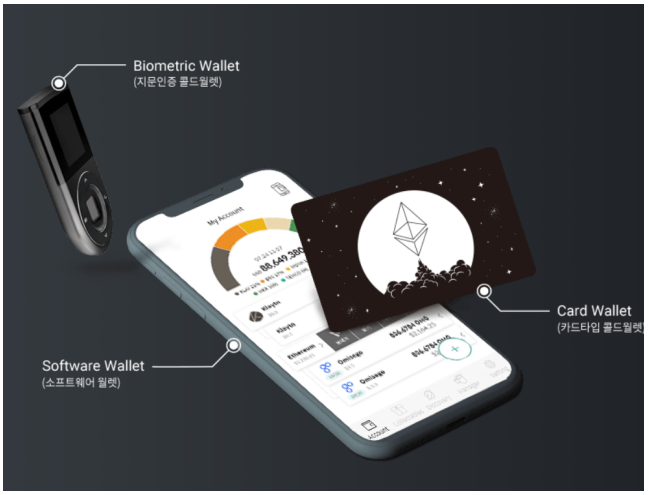
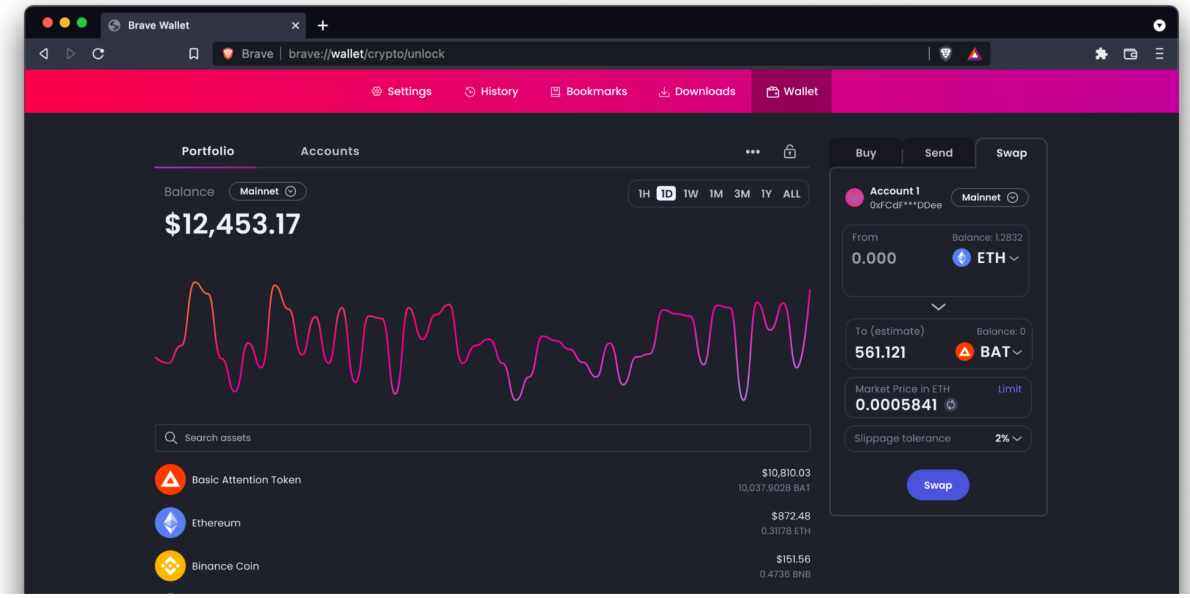


Figure 21: Brave의 브라우저 월렛

출처: Brave



인프라로서의 가상자산 지갑

인프라 보급의 임계 지점

비즈니스 운영에 있어 인프라가 가지는 영향에 대해 제프 베이조스는 다음과 같이 언급했다. “제가 아마존을 시작했던 1994년에는 아마존이 필요로 하는 모든 대형 인프라가 이미 마련되어 있었습니다. (...) 우리가 컴퓨터를 발명해야 했을까요? 아닙니다. 대부분 가정에는 이미 컴퓨터가 있었죠. 주로 게임을 하기 위한 것이긴 했지만 말입니다. 몇 십억 달러가 필요한 통신망을 건설해야 할 필요가 있었을까요? 아닙니다. 주로 장거리 전화를 위해 AT&T와 같은 전 세계 회사들이 만들어놓은 통신망이 존재했던 덕이죠. 이렇듯 인프라는 기업가들이 놀라운 일을 할 수 있게 해줍니다.” (제프 베이조스, ‘발명과 방황’)

네트워크적인 효과를 갖는 기술이 대중적으로 수용되는 과정에는 임계 지점에 도달하기 전 일정 수준의 보급 이후 확산이 가속화되는 변곡점(inflection point)을 거치게 된다. 이는 인프라와 애플리케이션 양측 모두에 적용된다. 가상자산 계정과 지갑은 NFT 거래를 포함해 블록체인 네트워크에 참여하고 애플리케이션들을 이용하기 위한 관문이 된다는 점에서 웹3 대중화를 위한 주요 인프라의 하나이다. 즉 가상자산 지갑의 대중화가 웹3 대중화의 충분조건은 아닐지라도 필요조건의 하나가 되며, 웹3 사용층 확산의 임계 지점은 지갑의 보급 확대와 동행할 것으로 전망할 수 있다.

예컨대 레딧의 볼트 지갑은 편의성과 아바타 NFT의 인기에 힘입어 10월 말 기준 NFT 보유 지갑 수 300만 개를 돌파해, 오픈시의 누적 활성 계정 수(약 230만 개)를 넘어섰으며 레딧의 전체 DAU 5천만 명과 비교해도 상당한 보급률을 보이고 있다. 볼트 지갑은 월렛의 패스워드와 레딧 계정의 패스워드를 분리시켜 보안성 문제를 방지하되 crypto-native가 아닌 가상자산에 낯선 일반 이용자들에게 보다 용이한 접근성을 제공한다. 온보딩된 사용자들은 평소와 같은 SNS 활동을 지속하면서도 아바타를 꾸미거나 커뮤니티 포인트와 토큰(MOON)을 획득 가능하고, 계정 간 상호작용을 경험할 수 있으며, 더 나아가서는 다른 거래소에서의 NFT 거래, 디파이 등 다양한 디앱에의 접근 등의 잠재적인 수요층이 되어 활동 범위를 점차 확장할 수 있다.

이외에도 향후 웹3 계정의 보급을 견인하는 애플리케이션은 실생활에 밀접하게 맞닿아있는 사용처가 보다 선행할 것으로 생각된다. 게임 분야도 그 사례가 될 수 있다. 이는 이용자들의 저변이 넓고 시장 규모가 크다는 점(Dataprot는 전세계의 게이머 인구 수를 32억명으로 추산), 캐릭터, 아이템, 레벨과 능력치 등의 요소들로 구성되어 NFT 등 웹3 요소 접목이 용이하다는 점, 많은 게이머들이 이미 게임 내 경제 활동 및 유료 결제의 경험을 보유하고 있다는 것 등의 장점이 있다. P2E 게임 Axie Infinity는 일간 활성 유저 수는 가장 높았을 때 270만 명에 달했다. 한편 성공적인 기존 게임들의 경우 포트나이트의 최대 일간 활성 이용자는 3,500만 명,

로블럭스는 5,000만 명을 넘어섰다. 향후 수집 욕구를 부르는 성공적인 게임 NFT를 인앱 지갑에 보유하게 될 게이머는 자신도 모르게 블록체인 네트워크와 상호작용하고 있는 셈이며 아이템을 계정 간에 전송, 판매, 대여하면서 자연스럽게 블록체인 경제 활동의 일원이 될 수 있다.

Figure 22: 인터넷의 인프라 구축과 서비스 발전과정

출처: Michael Dempsey

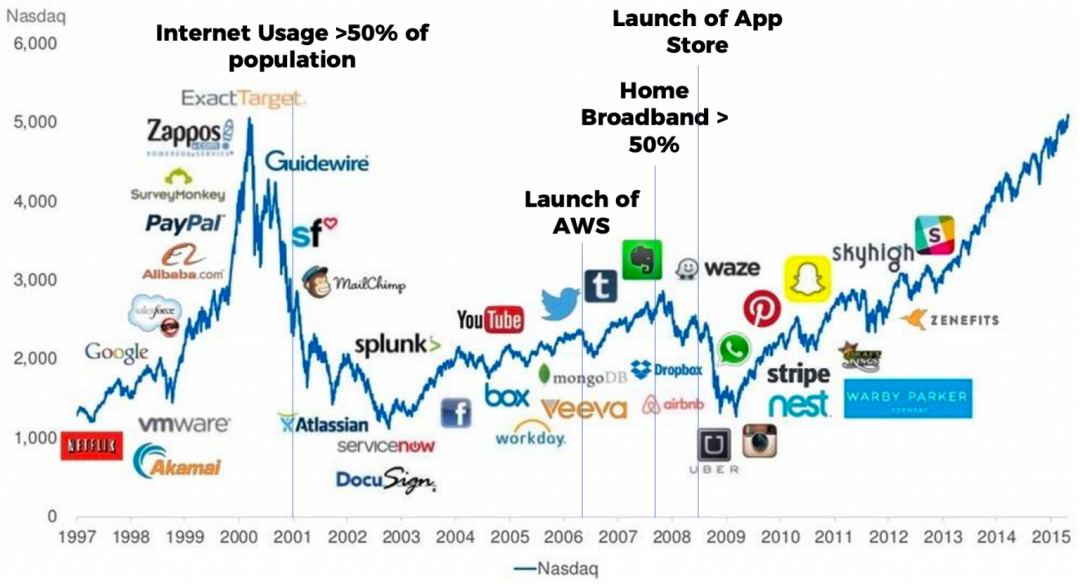


Figure 23: 웹 브라우저 점유율 추이

출처: Statista

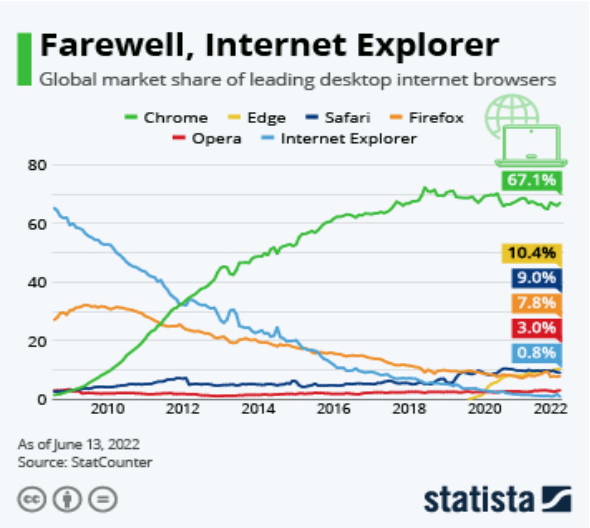
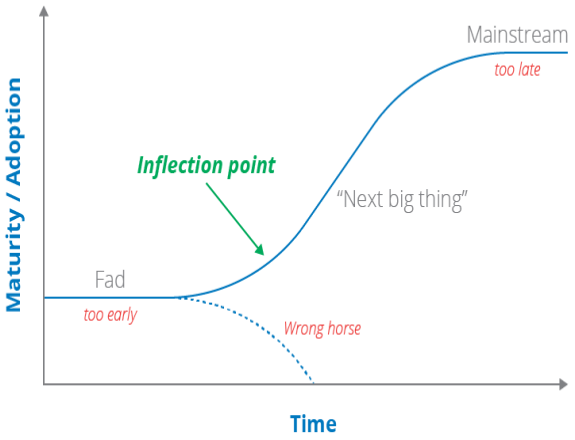


Figure 24: 대중 수용의 inflection point

출처: Michael Dempsey



탈중앙성의 희생 혹은 생태계의 확장

이러한 온보딩 과정을 목표하는 서비스들은 상당수의 경우 (흔히 웹2.5라고 불리는) 기존 비즈니스와 크립토 기반 활동을 접목하여 균형점을 찾아나가는 형태를 추구하고 있다. 그러나 이는 어느 정도 우려와 논쟁의 여지를 내포한다. 편의성을 위해 개인 키나 개인 정보를 일부 위탁할 경우 애초의 탈중앙성과 셀프 커스터디의 가치를 희석시킬 수 있다는 우려와 함께, 편의성과 대중 수용만이 강조될 경우 과연 기존 웹2 방식과의 차이가 무엇인가라는 질문이 상존할 수 있기 때문이다. 이러한 우려가 일부 유효할 수 있음에도 불구하고 웹3 요소 도입은 사용자에게 블록체인 네트워크에서 인정받을 수 있는 디지털 소유권과 데이터 의사결정권, 서로 다른 플랫폼을 오가는 상호운용성의 경험을 가능하게 한다. 이는 기존 시스템에서 구현되지 않는 새로운 효용을 가져올 수 있으며 개발자들에게 보다 창의적인 서비스 설계의 도구를 제공한다. 또한 분산화 데이터베이스, 영지식증명 등의 기술의 도입은 개인정보의 집중이나 노출을 최소화하는 데에 추가로 기여할 수 있다.

다른 서비스들과 마찬가지로 월렛 서비스 역시 이용자 특성에 따라 기업 및 기관투자자, 트레이더, NFT 수집가, 혹은 가상자산을 처음 접하는 대중적 소비자층까지 어떤 이용자를 타깃하는가에 따라 그 주가 되는 특성이 다르게 강조될 것이다. 크립토에 익숙한 트레이더에게는 자신 외의 누구에게도 키가 노출되지 않는 완벽한 셀프 커스터디를 보장하는 월렛이 더 매력적인 선택이 될 수 있고, 기업 이용자에게는 멀티시그 방식의 보안성과 만일의 사태에 자산의 안전을 보장할 수 있는 커스터디를 지원하는 엔터프라이즈 대상 월렛이 합리적일 수 있다. 반면 웹3에 지식이 없어도 단지 게임을 즐기거나 NFT를 수집하기 바라는 이용자들은 편의성을 위해 자신의 이메일이나 SNS 정보를 연동하는 방식을 더 선호할 수 있으며 혹은 아예 월렛의 존재가 드러나지 않는 사용 경험을 통해 보다 자연스럽게 웹3 서비스에 온보딩되는 효과를 거두는 것이 가능해진다. 이는 상호 배타적인 관계가 아닌 생태계의 확장 과정에서의 다양한 스펙트럼을 구성하게 된다.

인프라는 가치 창출과 동행되어야

당연하게도 월렛을 포함한 인프라의 확산은 대중 수용의 충분조건이 아님을 다시금 상기할 필요가 있다. 프로젝트들의 목표는 단지 인프라의 양적 확장이 되어서는 안된다. 스마트폰에서 다운로드되는 애플리케이션의 23% 만이 설치 3일 이후에도 이용된다는 통계가 보여주듯, 유저들은 익숙한 사용 패턴으로 돌아가는 경향을 가지고 있으며 새로운 애플리케이션이 지속적인 사용성을 창출해내는 것은 어려운 과제이다. 모바일 메신저 틱톡이 과거에 무려 2천만 명 이상의 가입자를 확보하였음에도 가입자 수와 실제 이용에서의 점유율이 동행하지 못했던 사례도 월렛 서비스가 실제로 수용되려면 단순한 보급 이상의 요인이 필요하다는 시사점이 될 수 있다.

2021년 비트코인을 법정화폐로 도입한 엘살바도르의 경우 국가가 앞장서서 치보 월렛(Chivo Wallet)을 다운로드하는 국민에게 30달러의 비트코인 보조금을 지급하면서 가상자산 및 지갑 보급에 나섰다. 그러나 전미경제연구소(NBER)의 조사에 따르면 인구의 3분의 2 이상이 월렛을 다운로드 받았음에도 보조금 사용 후에도 월렛 이용을 계속하는 사람의 비율은 전체 응답자의 20%에 불과했으며, 치보에 대해 알고 있는 응답자의 75%는 비트코인 보조금이 아니었다면 다운로드할 필요성을 느끼지 못한다고 밝혔다. 이러한 조사 결과는 사용자 가치 제공과 동행되지 않는 인프라 보급은 의미가 크지 않을 수 있다는 중대한 교훈을 준다. 개발자들은 월렛이 가지는 웹3 네트워크의 관문이자 통로로서의 인프라 잠재력을 최대한 활용하는 동시에, 웹3 수용의 본질은 수용자에게 소구력을 가지는 유즈 케이스와 애플리케이션에 있음을 함께 염두에 두어야 한다.

Figure 25: 모바일 메신저 설치 후 이용률(2012)

출처: 아이티데일리, 랭키닷컴

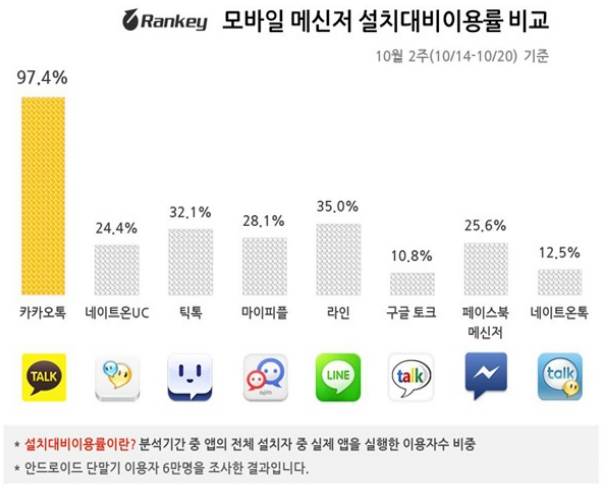
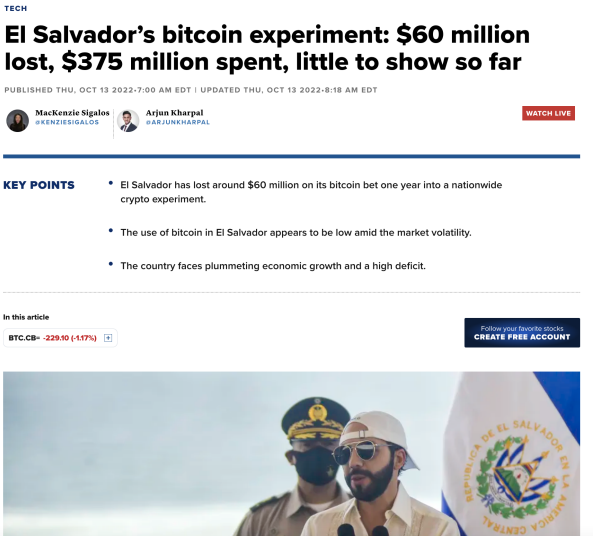


Figure 26: 엘살바도르의 비트코인 공용화폐 도입

출처: CNBC



작성자

정석문 | Peter Chung

2018년 코빗 입사. 사업개발팀을 거쳐 현재 코빗 리서치센터장 역임중. 그 전에는 커리어 대부분을 홍콩과 뉴욕 금융권에 종사. Goldman Sachs, UBS, Credit Suisse, Nomura를 거치며 top-tier 글로벌 자산운용사 들을 담당하여 아시아 주식 법인 영업을 주도했다. 학업으로는 University of Pennsylvania, The Wharton School에서 Finance 전공으로 학사과정을 졸업하였다.

정준영 | Junyoung Jeong

2022년 코빗 입사. (現)코빗 리서치센터 Research Analyst. (前)삼성증권 리서치센터, 다올투자증권 자기자본운용팀 근무. 서울대학교 농경제학과 및 경영대학 대학원 졸업.