지브렐 네트워크

2017년 5월

2차 초안

YAZAN BARGHUTHI
yazan@jibrel.network

VICTOR MEZRIN
victor@jibrel.network

요약

지브렐 네트워크는 통화, 채권, 기타 금융 상품 등 전통적인 금융자산의 디지털화, 상장, 거래를 블록체인에서 활성화시키는 것을 목표로 한다. 지브렐 탈중앙은행은 플랫폼을 통해 사용자들이 현금, 단기금융상품을 예치하거나, 사용자 소유의 암호화폐예탁증서(CryDR)를 발행하여 온/오프 체인에서 이루어지는 재정거래로 수익을 얻을 수 있도록 지원한다. 디지털 통화에 과도하게 노출된(overexposed) 탈중앙화 기관과 자금들은 포지션 위험을 분산시키고 안정적인 자산으로 자금을 보호할 수 있다. 뿐만 아니라, 지브렐 네트워크는 전통자산기반 토큰을 활용하는 거래, 투자 및 위험분산에 필요한 툴과 어플리케이션을 구축할 수 있도록 개발자들에게 완전한 플랫폼을 제공한다.

또한 지브렐 네트워크는 개인 간, 사업자 간 또는 소비자와 판매자 간에 이루어지는 법정통화 간의 트랜잭션 형태로 즉각적이고, 비용은 거의 없으며, 해외 결제 및 송금을 가능하도록 한다.

본 백서는 지브렐 네트워크를 구성하고 있는 핵심 요소와 상호작용 방식은 물론, 기존의 인프라를 활용하여 효율적으로 네트워크를 구축할 수 있는 방법을 설명한다.

1.서론

지난 2009년 비트코인이 선보인 이래[1], 블록체인이 지닌 엄청난 가치가 드러났다. 블록체인이라는 새로운 기술 덕분에 불가역적 분산원장(immutable decentralized ledger) 기반의 거래를 확인하고 실행하거나, 보다 광범위한 거래를 실행하고, 분산된 합의(decentralized consensus)에 도달할 수 있다.

이 놀라운 혁신은 믿을만한 중개자, 결제 및 청산 기관, 다양한 산업 및 산업 부문에 걸친 중개 서비스 제공자의 필요성을 감소시킴으로써 세상의 변화를 주도하고 있다.

그러나 기관 차원에서의 도입은 제한적이기 때문에 암호화폐 경제의 가치 대부분은 사용처 또는 지역별로 제각각 고립된 상태이다. 이로 인해 발생하는 병목현상 때문에 광범위한 시스템적 위험, 즉 전통 자산을 디지털 자산으로 전환하는 과정에서의 문제점과 한계점이 존재한다.

전통 경제와 암호화폐 경제 간의 단절을 고려하면, 전통 경제에서 발생하는 동일한 문제들이 암호화폐 경제에서도 발생한다. 전통 화폐 간의 전송을 원하는 사용자들은 암호화폐 교환, 전통적 금융기관 및 지급 프로세서 등을 복합적으로 이용하는 과정에서도 여전히 시간 지연 및 수수료 문제를 겪고 있다.

뿐만 아니라, 오프 체인(off-chain)에서 전통 자산의 이동을 빠르게 촉진시키는 전통적 개인 및 기관투자자들 역시 근본적인 비호환성, 특히 투명성 결여와 극심한 시장 변동성 때문에 암호화폐 경제에 대한 참여를 주저한다[2].

마지막으로, 크라우드세일을 통해 자금을 모집하는 탈중앙화 조직들은 물론, 디지털 자산과 암호화폐에 과도하게 노출된 탈중앙화 펀드 및 암호화폐 투자자들에게도 전통 자산을 다각화하는 선택지는 제한되어 있다.

위험이 한층 더 복잡해진 이유는 디지털 화폐가 다양한 역할을 수행한다는 점에서 비롯된다. 디지털 화폐는 가치를 전송하는 수단으로서 그리고 투기적 투자 수단으로서 거래 활성화에 기여한 채굴자들에게 보상을 제공하는 데에 사용되며, 특히 최근에는 크라우드펀드를 모집하고 탈중앙화 조직 및 어플리케이션을 운영하는 데에도 사용되었다(예를 들어 탈중앙화 컴퓨팅[3], 탈중앙화 저장소[4]).

전통 금융에서는 이러한 기능들을 수행하기 위하여 제각기 다른 수단들이 사용되었고 그에 맞추어 규제가 적용되었다. 이는 시스템적 위험을 관리하는 측면에서 도움이 된다. 그러나 탈중앙화된 규제 합의 프로토콜을 완전히 갖추기 전까지, 암호화폐 경제에서는 규제 대상이 아닌 거래의 형태로서의 보안 및 사기 위험, 의도된 목적을 벗어난 범위에서 사용된 암호화폐가 지닌 극단적인 변동성으로부터 비롯되는 시장 위험, 불안정한 디지털 화폐의 형태로

저장되어 있고 결과적으로 스마트 컨트랙트에 묶여있는 크라우드펀드로부터 발생하는 시스템적 위험에 노출된다[1].

본 백서는 현재 상황의 한계점과 문제점을 분석하고, 모든 이해관계자를 위한 솔루션을 제공하기 위하여 기존 인프라를 활용하는 접근법을 제시한다.

2. 전통자산기반 토큰(TRADITIONAL ASSET-BACKED TOKENS)

지브렐 네트워크 생태계의 핵심 관계자들은 암호화폐와 블록체인 기술을 이용하여 낮은 송금 수수료와 즉각적인 자금 전송 등의 이점을 이용하려는 비투자 목적의 사용자들, 떠오르는 암호화폐 경제에서 높은 수익을 얻고자 하는 전통적인 투자자들, 그리고 크라우드펀드 투자자들에게 투명성을 내보이기 위한 목적으로 온 체인(on-chain)에서 안정적으로 낮은 수익을 내는 자산을 이용하여 암호화폐 자산을 다각화하려는 탈중앙화 조직/펀드 및 암호화폐 투자자들이다.

블록체인도 전통적인 금융 상품들이 가진 안정성을 동일하게 갖출 수 있다면 모든 이해관계자의 니즈가 성공적으로 충족될 것이다. 이러한 안정성은 전통적 기초자산과 일대일로 대응하는 테더 토큰(tethered token)을 발행하는 방식으로 달성할 수 있다. 이 방식을 통해서 테더 토큰은 통화를 표시하는 데에 사용되거나[5] 심지어는 상품을 의미하는 데에도 사용될 수 있다[6].

전통 자산을 보관하고 해당 기초자산에 대한 소유권과 동일한 의미의 토큰을 발행하는 '보증인'(guanrantor)을 개발함으로써 다양한 통화, 상품, 단기금융상품, 기타 금융 수단들이 온 체인에서 공개적으로 거래될 수 있을 것이다.

3. 시스템 아키텍처

본 섹션은 지브렐 네트워크를 구성하는 핵심 요소들을 설명하고, 온 체인에서의 전통 자산 거래를 활성화하기 위하여 필요한 요소를 살펴본다.

3.1 퍼블릭 블록체인

특정 블록체인에 의존하게 되면 많은 문제점과 한계점에 직면하게 되므로, 블록체인 간 완전한 소통이 가능해지기 전까지는 안전한 퍼블릭 블록체인이 지브렐 네트워크 초기 버전에 필요하다.

3.2 암호화폐 교환

암호화폐 교환은 최종 사용자들에게 사용자들이 이용하는 법정화폐 계정과 암호화폐를 저장하는 전자지갑을 제공한다. 사용자들은 암호화폐와 법정화폐 간의 손쉬운 전환을 이용하여 디지털 통화를 구매, 거래, 또는 전송할 수 있다.

3.3 테더 토큰(Tethered Tokens)

테더 토큰은 전통자산기반 토큰을 생성하기 위해서 필요하다. 발행된 테더 토큰은 전통 자산과 일치하므로 기초자산이 매도되면 토큰은 소멸된다.

3.4 보증인

각각의 테더 토큰이 보유한 가치를 보장해줄 수 있는 보증인이 필요하다. 보증인은 전통 자산을 확보하고 있으며 전통 자산과 일치하는 테더 토큰을 발행할 뿐만 아니라, 전통적인 기초자산에 관한 소유권의 포기 또는 이전의 경우에 해당 토큰을 청산 또는 소멸시킨다.

3.5 어플리케이션 레이어, 라이브러리, 템플릿

일단 테더 토큰이 발행되면, 지급 프로세서, 송금 지갑, 거래 플랫폼 등 토큰을 활용하는 다양한 어플리케이션이 개발될 수 있다. 신속한 어플리케이션 개발을 위해서는 사용자 편의성을 갖춘 라이브러리 및 코드 템플릿을 탑재한 전용 어플리케이션 레이어가 필요하다.

3.6 소유권 이전

일단 테더 토큰이 발행되면, 기초자산은 암호화폐와 유사하게 손쉬운 거래가 가능하다. 이와 관련된 고도의 거래 프로세스는 다음과 같다.

1. 사용자가 보증인에게 법정화폐(FIAT) 송금
2. 보증인이 jFIAT 형태로 반환
3. 사용자는 jFIAT로 판매자에게 대금 지급
4. 판매자는 jFIAT 교환
5. 보증인이 법정화폐를 판매자의 계정으로 송금

테더 토큰을 보증하는 보증인이 존재하고 그 보증인이 향후 언제든 기초자산을 상환할 것을 보장하므로, 토큰은 시스템 내에서 존재하며 온 체인 및 오프 체인 결제에 사용될 수 있다.

3.7 수수료 및 요금

디지털 자산과 전통 자산 양쪽의 소유권 이전에는 관련 수수료와 요금이 발생하므로 이 점이 반영되어야 한다.

3.8 감독 및 규제

오프 체인에서의 소유권 또는 가치의 이전에 해당하는 모든 온 체인 거래는 국제 규범 및 지역 규범을 준수해야하며 그에 따라 운영되어야 한다.

올바른 관리 및 감독을 위하여 규제 프로토콜 및 관리 툴이 실행되어야 한다.

모든 거래는 KYC 및 AML 규제를 준수한다.

[1] 프로젝트들은 시장 위축으로 인해 펀딩이 감소하는 경우에 실현되지 않을 위험이 있다.

4. 지브렐 네트워크 실행

본 섹션은 지브렐 네트워크를 구성하는 요소들이 각각 어떤 방식으로 실행되는지를 설명한다.

4.1 이더리움(Ethereum) 블록체인

선택된 블록체인은 채굴 보상과 시스템 참여자 간 실제 거래를 분리해야 한다. 이러한 이유로, 이더리움은 지브렐 네트워크의 기본 아키텍처 기반을 형성하는 데에 아주 적합하다. 채굴 보상은 이더리움 '가스'의 형태로 제공되는 한편, 테더 토큰은 채굴 과정에 포함되지 않는다[7].

비트코인의 옴니 프로토콜 기반에도 지브렐 네트워크가 적합하나 이 접근에 대한 설명은 본 백서의 범위를 넘어선다.

4.2 암호화폐예탁증서 (CryDR)

암호화폐예탁증서(CryDR)는 지브렐 네트워크가 확보한 전통적 기초 자산의 소유권을 의미한다. 본 백서에서 기초 자산은 jAsset(예를 들어 jUSD, jEUR, jGBP) 형태로 표시된다. 소유권 해지 시, 지브렐 네트워크는 여섯 가지 법정화폐와 두 가지 단기금융상품을 지원하며, 향후 다른 금융 상품도 추가할 계획이 있다.

4.2.1 통화 / 법정화폐

지브렐 네트워크 초기 버전에서는 미국 달러화(USD), 유로화(EUR), 영국 파운드화(GBP), 러시아 루블화(RUB), 중국 위안화(CNY), 아랍에미리트 디르함(AED)을 지원하는 것을 목표로 하며, 향후 전략적 교환 파트너들의 참여가 늘어남에 따라 지원 가능한 통화는 점진적으로 확대될 것이다.

4.2.2 단기금융상품

안정적인 낮은 수익률을 내는 자산은 지브렐 네트워크가 핵심적으로 제공하는 상품이며, 암호화폐 투자자들은 미국 국채, 제로쿠폰 양도성 예금증서에 해당하는 토큰을 구매할 수 있다. 지브렐 네트워크의 초기 버전에서는 모든 단기금융상품에 대하여 자동 롤오버(automatic rollover) 또는 누적 메커니즘(accrual mechanism)이 적용된다. 이는 만기가 도래한 투자로부터 받은 법정화폐가 유사한 자산에 자동으로 재배치되는 것을 의미한다. 비슷한 방식으로, 기초자산의 만기가 도래하거나 기초자산이 매도될 때까지 배당금 또는 이자는 누적될 것이다. 지브렐 네트워크의 향후 버전에서는 단기금융상품에 대한 재설정이 가능할 것이다.

4.2.3 기타 금융 상품

향후에 전통적 금융 기관들이 지브렐 플랫폼에 참여함에 따라서 상장주식, 사모펀드 등 기타 금융 상품에 대한 총체적인 지원책이 마련될 것이다.

4.2.4 스마트 컴플라이언스

암호화폐예탁증서(CryDR)는 완전한 프로그래밍이 가능하므로 규제사항도 내장될 수 있다. 법정화폐는 제한받지 않을 것이나, 기타 다른 자산을 구매하거나 재판매하는 경우에는 해당 유형과 지역에 따라서 규제 사항을 완전하게 준수해야한다. 이러한 로직은 각각의 암호화폐예탁증서에 내장된다.

4.3 지브렐 '탈중앙'은행 (JDB)

지브렐의 탈중앙은행은 소유자들을 대신하여 전통 자산을 수령 및 확보하며 그와 일치하는 CryDR을 발행하여 소유자의 전자지갑으로 전송한다. 토큰 상환 시에는 토큰이 소멸되고 기초자산은 토큰 보유자에게 이전된다.

지브렐 탈중앙은행은 완전한 분권화를 목표로 하고 있으나, 전통적 금융 기관들이 온 체인 거래에 완전하게 통합되기 전까지는 지브렐 네트워크의 대다수 구성 요소들이 오프 체인으로 운영될 필요가 있다. 오프 체인 활동은 지역 및 국제 규제당국의 조언 및 감독을 받게 될 것이다.

따라서 이해관계자 간 거래는 투명성과 신뢰도에 손상없이 완전한 규제 준수를 보장하는 방식으로 올바르게 운영되어야 한다. 이는 각 지역에서 해당되는 규제를 완전하게 준수하면서 운영되는 특수 독립체인 자산 포털(asset portal)을 통하여 달성될 수 있다.

4.4 자산 포털

자산 포털은 전통 자산을 온 체인의 디지털 자산으로 전환하기 위하여 필요한 법적인 금융 관련 절차를 수행하는 데에 이용된다.

법정화폐 포털(fiat portals)은 단순한 암호화폐 교환을 의미할 것이다. 기존의 교환과는 전략적 파트너십이 형성될 수 있으며, 다른 한편으로는 다양한 지리적 접근성을 갖춘 지브렐 교환 네트워크가 구축될 것이다. 또한 기존의 교환에서 지브렐의 법정화폐 준비금의 일정 부분을 보관해둠으로써 자금 이전에 수반되는 시간 및 수수료를 상당부분 감소시키는 것은 물론, 교환에 필요한만큼의 유동성을 제공한다.

비법정화폐 포털(Non-fiat portals)에서는 필요한 실사(due diligence)를 수행하고 비법정화폐 예금의 소유권을 보유할 수 있는 오프 체인 기관이 존재해야한다.

대다수 지역에서 자산 포털은 중개업과 송금업 자격증을 요구한다. 규제 강도가 높은 지역이나 정교한 금융 상품에 관련되는 경우에 규제 당국의 철저한 개입과 감독이 이루어질 수 있다.

규제가 변화함에 따라서 향후 자산 포털은 분권화되어 커뮤니티가 자체적으로 운영하는 방식으로 변화할 수 있다. 기관투자자들과 기타 금융 기관들은 지브렐 플랫폼을 이용하여 보유하고 있는 전통 자산을 온 체인에서 상장할 수 있을 것이다.

4.5 지브렐 네트워크 토큰 (JNT)

비법정화폐 포털은 법정화폐 형태로 오프라인 수수료를 청구할 것이며, 지브렐 탈중앙은행의 온 체인 수수료와 커미션은 지브렐 네트워크 토큰(이하 JNT)의 형태로 부과될 것이다.

JNT는 ERC20기준에 부합하는 교환 목록에 포함될 것이다.

5. 인프라

사용자의 잔액, 거래 내역 등 중요한 데이터는 블록체인에 저장되고 기타 데이터는 개발 서버에서 관리된다.

탈중앙화 어플리케이션의 빠른 개발을 위한 몇 가지 개발환경, 툴, 프레임워크 등은 이미 개발되어 있다[8]. 지브렐 네트워크는 CryDR의 광범위한 도입과 유통을 위하여 기존과 유사한 개발자 컴포넌트, 툴, 프레임워크를 개발할 필요가 있다.

인프라는 두 가지 주요 영역인 온 체인 API와 오프 체인 APIs/Utils에 걸쳐 필요할 것이다.

5.1 온 체인 인프라

네트워크의 효율적인 운영을 위해서는 오직 네 가지 핵심 스마트 컨트랙트만이 필요할 것이다.

5.1.1 암호화폐예탁증서(CryDR) 스마트 컨트랙트

지브렐 탈중앙은행에 등록된 각각의 자산들은 스마트 컨트랙트 형태로 발행된 CryDR를 보유하게 된다. CryDR스마트 컨트랙트는 ERC20 기준에 부합한다. 사용자 계정 간 CryDR 전송은 다른ERC20토큰을 전자지갑 간 전송하는 방식과 유사하다.

5.1.2 지브렐 탈중앙은행 스마트 컨트랙트

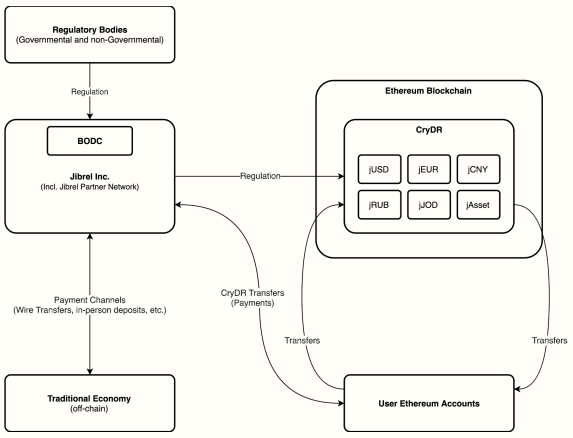
지브렐 탈중앙은행용 스마트 컨트랙트가 CryDR 스마트 컨트랙트의 운영을 관리할 것이다.

5.1.3 스마트 컨트랙트 이사회 (BODC)

스마트 컨트랙트 이사회는 지브렐 탈중앙은행 컨트랙트와 상호작용을 하고 영향을 미치는 유일한 메커니즘이다.

스마트 컨트랙트 이사회는 투표로 관리되며, 이사회 구성원들은 이사회의 활동에 관한 투표를 하기 위해 이더리움 계정을 이용한다. 개인 키의 보관 및 사용은 이사회 구성원들 각자의 책임 하에 있다. 이사회는 암호화폐에 걸맞는 사고방식을 가진 리더들과 금융 서비스 전문가로 구성되는 것이 가장 바람직하다.

도표 1. CryDR – 전반적인 흐름도



5.1.4 Helpers / Utils (보조 스마트 컨트랙트)

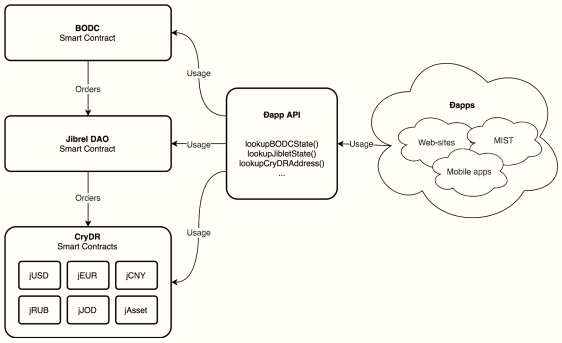
각기 다른 버전에서 운영되는 컨트랙트 간의 전환, 부가적인 API 기능 추가 등 보조적 기능을 수행할 수 있는 몇 가지 보조 스마트 컨트랙트를 생성할 필요가 있다.

이에 관한 구체적인 설명은 본 백서의 범위를 넘어선다.

5.2 오프 체인 인프라

거래, 투자 및 위험분산 수단인 CryDR의 광범위한 도입을 촉진시키기 위하여 어플리케이션 개발자들에게는 사용자 편의성을 갖춘 라이브러리 및 코드 템플릿이 제공될 것이다.

도표 2. 지브렐 탈중앙화 어플리케이션 API 흐름도



5.2.1 라이브러리 및 템플릿

개발자들은 기존의 라이브러리를 이용하여 이더리움 블록체인(예, JS web3)과 상호작용하게 될 것이다. 지브렐 네트워크는 지브렐 탈중앙은행과 스마트 컨트랙트 간의 상호작용을 보다 단순화할 수 있는 라이브러리와 코드 샘플에 대한 래퍼(wrapper)를 제공할 것이다.

5.2.2 CryDR 익스플로러

생성된 오픈 소스 익스플로러를 통하여 사용자들은 CryDR 관련 메타데이터를 확인하고 스마트 컨트랙트 이사회와 상호작용할 뿐만 아니라 지브렐 탈중앙은행이 보유한 기초자산의 소유권을 직접 확인할 수 있다.

5.2.3 이사회 툴킷

CryDR Ltd의 내부 IT 인프라와 이더리움 블록체인이 상호작용할 수 있도록 하는 툴이 개발될 것이다. 이는 특히 스마트 컨트랙트 이사회와 이사회 구성원들간의 상호작용을 조직하고, 지브렐 시스템 상황을 효과적으로 모니터링하기 위한 것이다.

6. 스마트 규제 실행

본 섹션에서는 지브렐 네트워크 내에서의 CryDR, 스마트 규제, 스마트 컴플라이언스의 실행을 다룬다.

6.1 CryDR 아키텍처

CryDR 자체가 이더리움 블록체인에 배포되는 스마트 컨트랙트에 해당한다. 견고하고 측정가능한 시스템을

구축하기 위하여 CryDR는 다음과 같은 다양한 요구조건을 충족해야 한다.

높은 호환성: 이미 존재하는 토큰 관리 툴과의 호환성을 위하여 ERC20 인터페이스를 갖추어야 함
업데이트 가능한 비지니스 로직: 변화하는 실제 규범과 규제에 맞추어 업그레이드가 용이해야 함
불가역성: 일단 배포되고 나면 변경이 불가능해야 함
이동가능성: 이벤트(Events)와 스토리지(Storage)는 분리되어 저장되어야 함
쌍방향성: CryDR는 서로 간 상호작용이 가능해야 함.

6.2 기존 방법론

이러한 기술적인 요구조건들은 현재 이더리움 생태계 내에서 사용가능한 툴만으로는 달성하기가 어렵다. 업그레이드가 가능한 스마트 컨트랙트는 실행이 쉽지 않으며, 특정 툴과 방법론은 존재하나 각각 한계점을 가지고 있다.

6.2.1 EVM DELEGATECALL

가능한 첫 번째 접근법은 이더리움 가상 머신(Ethereum Virtual Machine, EVM)의 작업 코드 `DELEGATECALL` 을 이용하는 것이다.

이 작업 코드는 비지니스 로직을 업데이트할 수 있는 강력한 툴이지만 몇 가지 단점을 가지고 있다. 특히, 일단 한 번 배포되고 나면 스마트 컨트랙트 원본의 스토리지 구조가 업데이트 과정 내내 유지되어야 한다. 따라서 이 방법은 간단히 업그레이드가 가능한 컨트랙트 실행 시에만 적용될 수 있으며 지브렐 네트워크의 사용처에서는 이용할 수 없다.

6.2.2 스마트 컨트랙트 가지치기

또다른 솔루션은 컨트랙트를 가지치기하고 이벤트와 상태(State)가 보존되는 동일한 주소로 새로운 컨트랙트를 배포하는 것이다. 이는 지브렐 네트워크에 대한 이상적인 솔루션이 될 수 있지만, 이더리움 가상 머신에서는 아직 실행되지 않았다.

6.3 지브렐 네트워크 접근법

지브렐 네트워크를 구축하는 과정에서는 지루하기는 하지만 전체론적인 솔루션이 활용된다. 시스템 전체를 서로 상호작용하는 다수의 정교한 스마트 컨트랙트로 해체하지만, 업그레이드 및 업데이트를 원활하게 제공할 수 있다.

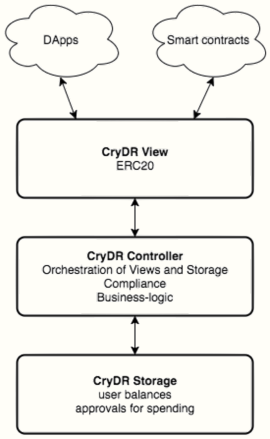
네트워크의 실행은 더 복잡한 과정을 거쳐야하나 이 접근법은 지브렐의 탈중앙화 어플리케이션(DApps)에 강력한 백엔드(backend)를 제공한다.

6.3.1 CryDR의 3중 시스템

CryDR는 다음의 세 가지 핵심적인 구성 요소로 해체된다.

스토리지(Storage) – 모든 데이터 저장
뷰(View): 제 3자 컨트랙트와 웹 어플리케이션을 위한 인터페이스
컨트롤러(Controller): 컴플라이언스와 비지니스 로직을 실행하고 스토리지와 컨트랙트 뷰를 조직함.

도표 3. 계층형 아키텍처

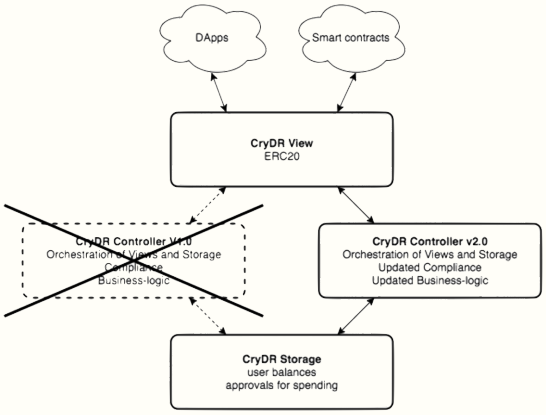


6.3.1.1 컴플라이언스 업데이트

이 구조 내에서 새로운 CryDR 컨트롤러 컨트랙트를 손쉽게 배포하고 뷰와 스토리지 컨트랙트를 설정하여 새로운 컨트롤러를 사용할 수 있다.

이를 통해 효율적인 방식으로 컴플라이언스 및 CryDR을 강력하게 하는 비지니스 로직을 손쉽게 업데이트할 수 있으며, 우리는 이것을 스마트 규제로 명명한다.

도표 4. 컨트롤러 업데이트

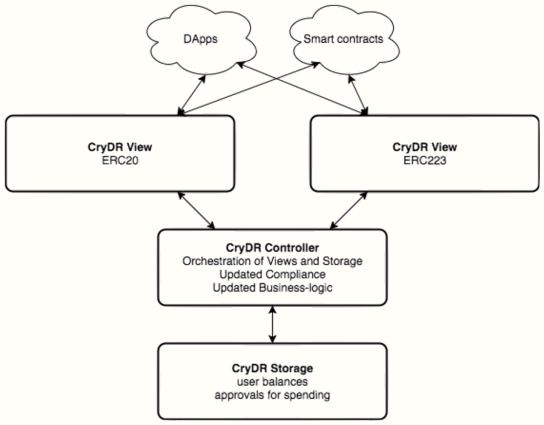


지브렐 네트워크는 비지니스 로직을 업데이트하는 프로세스를 활성화함으로써 토큰이 현실 세계에서 변화하는 규제 내용에 완전히 부합되도록 보장할 수 있다.

6.3.1.2 인터페이스 업그레이드

이 아키텍처를 이용하여 새로운 토큰 기준(예, ERC223)에 대한 추가적 지원을 제공하는 등 토큰 인터페이스도 원활하게 업그레이드할 수 있다.

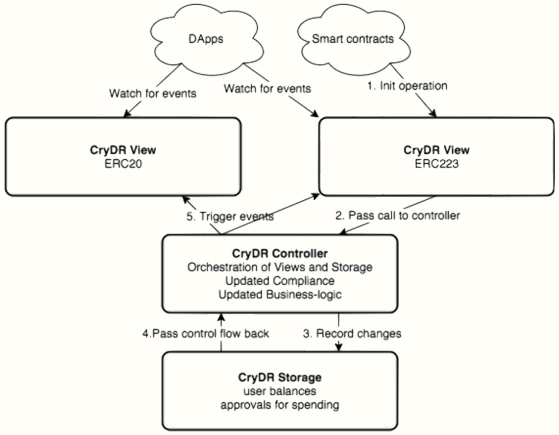
도표 5. . 뷰 업그레이드



업그레이드 수행 시, CryDR 스토리지는 변경되거나 영향을 받지 않는다.

뷰는 컨트롤러보다 앞서는 레이어로서 동작하므로, 업데이트 과정에서 모든 이벤트는 변경되지 않고 그대로 보존된다. 컨트롤러가 성공적으로 수행되면, 연결된 모든 뷰에 유발(trigger)되어 클라이언트는 모든 이벤트를 수신할 수 있다.

도표 6. 이벤트 유발



6.3.2 스마트 규제 아키텍처

KYC 및 AML기준을 준수하려면 엄격하고 구체적으로 계정 허가를 관리해야 한다.
스마트 컨트랙트에는 내재된 한계점이 있고, 무엇보다도 온 체인 데이터 접근은 설계 상 제한된 제3자 서비스에 대한 요청에 의해서만 가능하다.

오프 체인 데이터에 접근하려면, 해당 데이터는 우선적으로 트랜잭션의 형태로 블록체인 영역에 진입되어야 한다.

간단히 말하자면, 모든 컴플라이언스 준수는 스마트 컨트랙트를 통하여 온 체인에서 실행되어야 한다.

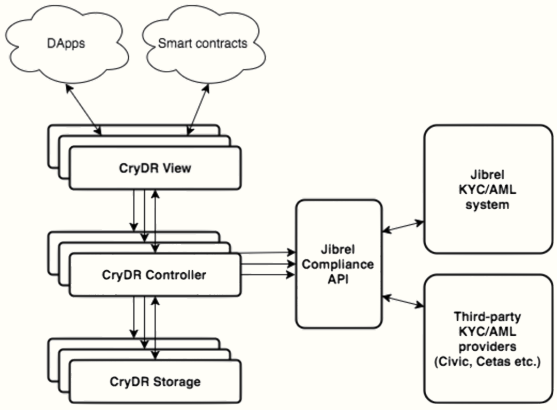
KYC 및 AML기준을 준수하려면, 다음과 같은 두 가지 솔루션이 실행될 필요가 있다.

데이터 저장소: 온 체인에서 사용자 데이터 저장
규정 실행: KYC/AML 규정을 트랜잭션마다 적용

Civic, uPort를 포함한 대다수 프로젝트들이 이러한 솔루션을 다룬다. 그러나 이 솔루션들은 적응성과 다목적성을 갖도록 구축되었고, 결과적으로 제도적 수준의 KYC/AML 프로세스에서 요구되는 조건을 충분히 만족시키지 않아도 되는 일반 사용자 정보만 저장할 수 있을 뿐이다.

이러한 이유 때문에 지브렐 네트워크는 KYC/AML 전용 지브렐 모듈 및 현재 이용가능한 제3자 솔루션과 모두 연계되는 전용 컴플라이언스 API를 구축할 것이다.

도표 7. 지브렐 컴플라이언스 API



6.3.3 지브렐 네트워크 토큰의 역할

지브렐 네트워크의 핵심 비지니스 조건은 모든 CryDR이 기초자산에 연동(tethered)된 상태가 유지되어야 한다는 점이다. 이를 위해서는 오프 체인 자산이 우선적으로 증권화 되어야하며, 따라서 가상 교환 통화(virtual exchange currency)가 필요하다. 이는 지브렐 네트워크를 통하여 거래를 하고, 오프 체인 수수료 지급을 용이하게 하기 위해서이다.

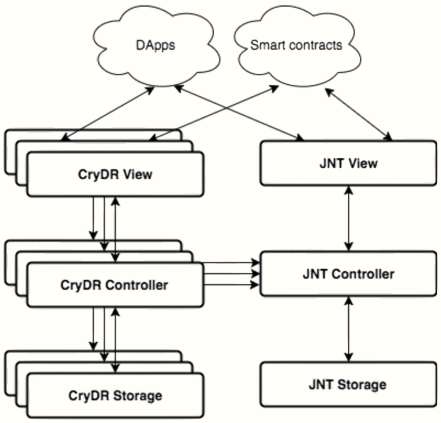
비트코인, 이더리움 등 기존의 암호화폐들은 화폐 가격의 변화가 지브렐 네트워크의 유용성과는 무관하기 때문에 적합하지 않다. 이러한 단절로 인해 시장 및 신용 리스크가 발생한다. 뿐만 아니라, 앞으로 전용 체인을 제공하는 것이 지브렐 네트워크의 목표라면, 전용 토큰은 원활한 마이그레이션 프로세스를 촉진시키는 데에 필요할 것이다.

CryDR 자체는 이러한 솔루션에 적합하지 않다. 현실 세계의 기초자산에 연동된 상태를 유지해야하며, CryDR을 지급의 일부로서 사용할 경우 단절이 발생하여 시스템 불안을 야기할 것이기 때문이다.

지브렐 네트워크 토큰(JNT)은 지브렐 네트워크의 '연료' 또는 '가스'로서 역할을 할 것이다. JNT는 지브렐 네트워크 및 지브렐의 탈중앙화 어플리케이션(DApp)을 통해서 제공되는 모든 기능에 대한 보편적인 접근을 허용할 것이다.

JNT는 모든 CryDR이 해당하는 기초자산에 연동된 상태가 언제나 유지된다는 점을 보장하며, 컴플라이언스의 추가적인 레이어를 부가한다.

도표 8. 지브렐 네트워크 토큰의 상호작용



7. 완전한 탈중앙화 운영

중단기적으로, 물리적 자산을 디지털 자산으로 변환하려면 필요한 법률적인 금융 관련 실사를 수행하는 오프 체인 활동이 필요하다. 또한 이사회 구성원들은 완전한 투명성 및 규제 컴플라이언스를 확보하도록 지브렐 탈중앙은행을 감독해야 한다.

장기적으로, 규제는 자산 소유권을 온 체인에서 확인할 수 있는 방식으로 진화할 것이며, 이에 따라서 지브렐 네트워크는 탈중앙화 자율 조직(decentralized autonomous organization, DAO)이 될 것으로 기대된다.

7.1 셀프서비스 포털

기술적인 한계점, 즉 온 체인 계산 능력, 복잡한 영지식 증명(zero-knowledge proofs)[2][9]의 현실성, 관련 허가 취득에 대한 규제 장벽 등의 문제가 해결되기만 한다면, 지브렐 네트워크는 셀프서비스 포털(예를 들어, 전통적인 교환 플랫폼으로서 온 체인에서 호스트되고, 지브렐 네트워크와 소통가능한 포털)을 운영할 수 있다.

이러한 포털의 구축은 지브렐 네트워크가 완전한 탈중앙화를 이루기 위한 결정적인 요소이다.

7.2 온 체인 디지털 신분증 / KYC 및 AML

현재 수많은 온 체인 디지털 신분증과 KYC 솔루션이 존재하지만 기능은 제한되어 있다. 셀프서비스 포털을 운영하려면 보다 개선된 신분 증명 솔루션이 필요하다.

7.3 DAO이사회

일단 운영이 안정적인 상태로 접어들면, 이사회는 해체되고 지브렐 탈중앙은행의 운영을 감독하는 자율적인 규제 조직으로 대체될 수 있다.

2 확률적으로 검사 가능한 증명의 효율성을 입증하기 위해 상당한 연구가 이루어졌으나 아직은 현실성이 없음

8. 사용처

교환이 용이한 전통자산기반 토큰은 광범위한 사용처를 제공한다.

8.1 전통/디지털 자산 교환

플랫폼이 전통 자산과 디지털 자산 간의 거래가 자유롭게 이루어지도록 함으로써 자체적으로 발전하고, 투자자들과 안정적인 디지털 자산을 찾는 주체들을 대상으로 하는 전통적인 투자 상품의 대량 판매를 통하여 기관투자자들이 낮은 위험과 높은 수익을 얻을 수 있도록 한다.

8.1.1 투자 플랫폼

투자은행은 단기금융상품이나 상품들을 지브렐 탈중앙은행에 예치한 후 해당CryDR을 탈중앙화 조직과 펀드에 프리미엄을 받고 매도하여 **온 /오프 체인 재정거래**에서 수익을 얻을 수 있다.

8.1.2 위험을 분산하는 토큰

탈중앙화 자율 조직과 펀드는 단기금융CryDR (money market CryDR)을 구매한 후 온 체인에 저장하여 완전한 투명성과 자금의 안정성을 보장받을 수 있다. 탈중앙화 자율 펀드는 다양한 전통 자산 중에 선택하여 디지털 포트폴리오를 완성하고 암호화폐경제의 침체로부터 자산을 보호할 수 있다.

8.2 해외 전송

플랫폼은 자산기반 토큰을 제공함으로써 (안정적이고 전세계적으로 통용되는) 전통 자산과 (불가역성, 전송의 용이성, 신뢰도를 갖춘) 디지털 자산 양쪽의 바람직한 특성을 모두 보유한 토큰을 제공할 수 있다.

이러한 토큰을 통해 지급결제대행, 송금 채널, 기타 현금 전송이 실행될 수 있다.

8.2.1 송금

지브렐 네트워크는 트랜잭션 실행 시 암호화폐 인프라를 이용하는 법정화폐 간의 전송을 가능하게 하여 송금을 실행할 수 있도록 한다. 사용자들은 자금을 추가하고 전세계의 누구에게든 그 자금을 전송할 수 있으며, 이 과정에서 디지털 통화를 통한 낮은 수수료와 동시에 전통 화폐의 안정성, 안전성 및 보안성도 계속 누릴 수 있다.

8.2.2 유니버설 지갑(Universal Wallet)

모든 통화에 통용되는 지갑이 생성되고, 이 지갑을 통하여 사용자들은 통화의 종류, 장소, 대상에 상관없이 통화를 자유롭게 변환하여 자금을 전송할 수 있고, 일반적으로 이러한 트랜잭션에서 발생하는 과도한 수수료가 없다.

8.3 해외 결제

이와 마찬가지로, 지브렐 네트워크는 해외 결제를 가능하게 할 것이다.

8.3.1 통화 API

전통자산기반 토큰을 통하여 지브렐 네트워크는 통화간 변환을 자유롭게 해주는 통화 API를 사용자들에게 제공할 수 있다.

8.3.2 판매자 API

지브렐 네트워크는 판매자들에게 간단하고 손쉬운 지급결제대행을 제공하여 결제를 받은 후 통화 종류에 상관없이 해당 지역 화폐로 인출할 수 있도록 하며, 이 과정에서 교환 또는 전송 수수료는 발생하지 않는다.

지브렐 네트워크가 구축되면 판매자들은 사용자 편의성을 갖춘 지브렐의 라이브러리와 API를 이용하여 통화 종류에 상관없이 지급결제대행 서비스를 구축하게 된다.

9. 참고자료

[1] Nakamoto, Satoshi, *Bitcoin: A peer-to-peer electronic cash system*, 2008 - URL - {https://bitcoin.org/bitcoin.pdf}

[2] Brennan and Lunn, Credit Suisse Equity Reports - *Blockchain - The trust disruptor: Shared ledger technology and the impact on stocks*, 2016 - URL {http://www.the-blockchain.com/docs/Credit-Suisse-Blockchain-Trust-Disrupter.pdf}

[3] Golem, *The Golem Project: Crowdfunding White Paper*, 2016 - URL {http://golemproject.net/doc/DraftGolemProjectWhitepaper.pdf}

[4] Wilkinson, Shawn, *Storj Project: A Peer-to-Peer Cloud Storage Network*, 2014 - URL {https://storj.io/storj.pdf}

[5] Tether Ltd, *Tether: Fiat currencies on the Bitcoin blockchain*, 2016 - URL {https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf}

[6] Eufemio, Chng and Djie, *Digix: The Gold Standard in CryptoAssets*, 2016 - URL {https://dgx.io/whitepaper.pdf}

[7] Buterin, Vitalik, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2013 - URL {http://ethereum.org/ethereum.html}

[8] Solidity, *Solidity: A contract-oriented, high-level language for the Ethereum Virtual Machine*, Release 0.4.10 Documentation - URL {http://solidity.readthedocs.io/en/v0.4.10/}

[9] Ben-Sasson, Chiesa, Garman, Green, Miers, Troma and Virza, *Zerocash: Decentralized Anonymous Payments from Bitcoin*, 2014 - URL {http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf}