PENTA

블록 체인 연결

테크놀로지 화이트 페이퍼

Penta Network

V1.0.24 | 2018

들머리

블록 체인 기술이 왕성히 발전하면서 다양한 블록 체인 체계를 구축하였다. 그러나 그 체계들은 서로 관통하지 않아 오프 체인 장면에서의 인터랙티브도 부족하기에 현실 세계와 블록 체인 세계의 유효 연결에 영향을 미친다. 차세대 블록 체인 네트워크의 목표는 다양화의 블록 체인 생태를 바탕으로 탈중심화 블록 체인 세계와 집중형의 현실 세계를 연결하는 것이고 블록 체인과 미래의 모든 것을 연결하는 것이다.

PENTA ("PENTA Network" 또는 "PNT"라고도 불린다)는 차세대 블록 체인 네트워크이다. PENTA 는 펜타 쿠르에서 유래했으며 "다섯차 인터레이스" 라는 것을 상징하고 있다.사물의 인과 관계를 탐구하고 네트워크의 역사 궤적와 발전 결과를 추적하며 미래의 블록 체인 세계를 탐색한다.

PENTA 은 주체, 트러스트, 가치, 장면, 유통이라는 다섯개의 차원을 구축함으로써 많은 블록 체인 체계 및 집중형 체계와 연결하다. 이는 블록 체인 세계와 현실 세계의 연결은 보다 더 효율적이고 블록 체인 기술은 더 보급하고 최종적으로 미래의 블록 체인 세계와 연결하는 것을 실현한다.

PENTA 네트워크 미래를 이끌어 낸다!

목차

1. 개요

PENTA("PENTA Network" 또는 "PNT" 라고도 불린다)는 차세대 블록 체인 네트워크와 프로토콜이다. 다섯 가지 차원(주체, 트러스트, 가치 유통 상황)에 근거하여 세 개의 연결(블록 체인과 블록 체인 연결/블록 체인과 중심화 시스템의 연결/ 오프 체인과 온 체인 연결) 을 실현하는 것이다. 이를 실현하기 때문에 10 개의 코어 기술 전략을 작성했다.

PENTA 팀의 핵심 멤버는 NASA, Wiki Leaks, Google, Morgan Stanley, 네덜란드 은행, 독일 은행 등 글로벌 톱의 과학, 금융 기구로 구성되어 있다. 과학 기술, 사회, 경제 발전에 대해서 깊은 인식을 가지고 있다. 블록 체인은 미래의 세계를 만드는 중요한 열쇠이기 때문에 미래의 궁극의 블록 체인 세계의 모습을 탐색하는 것은 PENTA 의 초심이다.

그리스 철학자 아리스토텔레스는 우주 만물은 네 개의 보편적으로 존재하는 요인으로 묶인다고 지적했다. 즉 "형식 인 ","질료 인","동력 인","목적 인"이다. 그 가운데 "목적 인"은 가장 중요한 "궁극 인" 이라고도 할 수 있다. PENTA 는 처음으로 블록 체인"사인설"을 제언했다. 트러스트는 블록 체인 형식 인이며 분산 식은 블록 체인의 질료 인이며 권력 분산화는 블록 체인의 동력 인이다. "보세"는 블록 체인"목적 인"에서 가장 중요한 "궁극 인"이다.

본고는 PENTA 의 프레임워크 및 대응하는 주체, 트러스트, 가치, 유통, 장면과는 다섯 가지 차원의 연결에 대해서 소개한다.또 PENTA 는 어떻게 요행 체인들을 연결하여 미래의 블록 체인 세계를 만드는지 설명한다.

2. 블록 체인 “사인설”

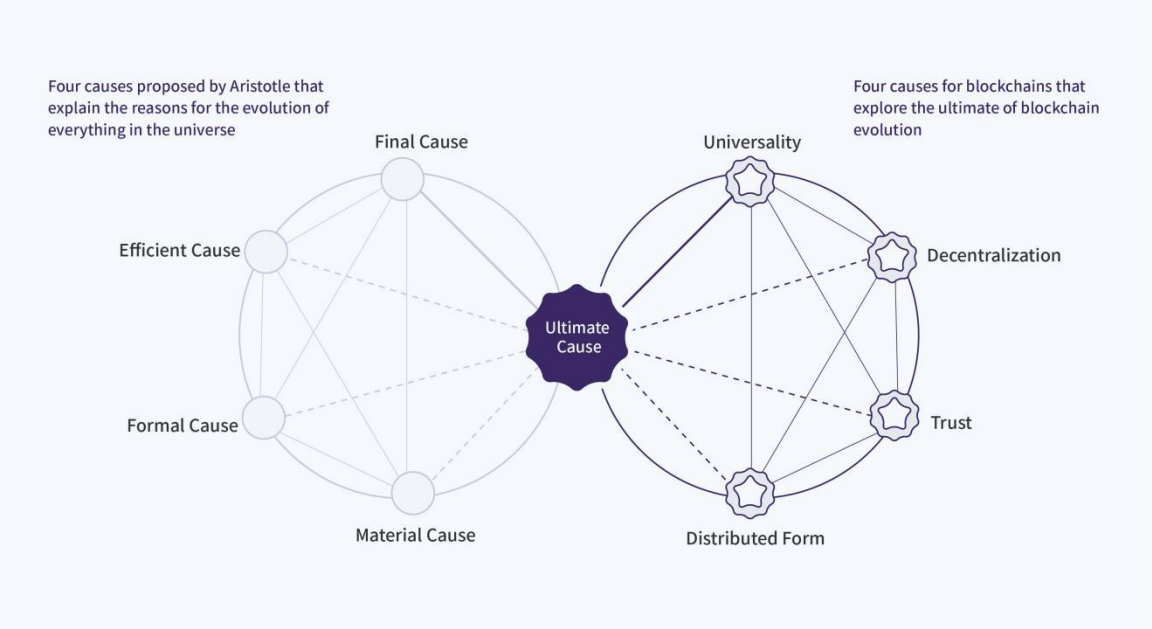
우주 만물의 탄생, 변화, 발전, 종결에는 반드시 원인이 있다. 사물의 진화와 종결은 필연적이다. 사물이 발전하는 궁극의 현 의의를 찾아 학설 중에서 고대 그리스의 철학자 아리스토텔레스의 사인설은 집대성의 것으로 평가받았다. 아리스토텔레스의 사인설은 자연 철학에 대한 새로운 투시로, 기존의 시각을 크게 바꾸고, "게슈탈트 변환 스위치"를 가져왔다. 아리스토텔레스는 우주 만물의 존재는 넷 개의 보편적인 요인으로 묶인다고 지적했다. 즉"형식 인 ","질료인","동력 인","목적 인"이다. 이 네 가지 요인이 공동으로 사물의 발전을 촉진한다. 그 가운데"목적 인"은 가장 중요하고 궁극적인 것으로 모든 사물을 발전시키는 근원이다.

아리스토텔레스의 사인설에 근거하여 PENTA 는 처음으로 블록 체인"사인설"을 제언했다. 탈중심화, 분포식 전산, 조작 방지는 블록 체인의 핵심 사상이다. 이들의 특성을 통해 블록 체인 네트워크는 "신뢰 관계를 강화하는" 기계가 되었다. 블록 체인의 인과 발전을 분석하고 트러스트는 블록 체인의 형식 인이라는 것을 제기한다. 분산 식은 블록 체인의 질료 인이며 탈중심화는 블록 체인의 동력 이며 "보세"는 블록 체인의 "목적 인” 즉 가장 중요한 "궁극 원인"이다.

2.1 궁극의 블록 체인

만약 탈중심화(동력 인)은 궁극적인 원인으로서 중심화의 세계를 뒤집으

면 편견의 블록 체인이 될 것이다. 분포식(질료인)은 궁극적인 원인으로서 분포 식을 구석구석까지 침투시킨다면 협의의 블록 체인이 될 것이다.



트러스트 체계, 즉"형식 인 "은 궁극적인 원인으로서 일방적으로 변혁을 추진하겠다고 하면 편향된 블록 체인이 될 것이다. 보세 생태 균형"목적인"을 만들어 블록 체인의 분포식이고 탈중심화의 세계와 기존의 중심형의 세계를 연결하는 것은 블록 체인의 궁극 원인이다.

2.2. 편견의 블록 체인

PENTA 는 탈중심화는 "블록 체인 사인설"속의 "동력 인"이라고 생각하고 있다."동력 인"은 수동자를 움직이는 것, 변화를 일으키는 것이다. 블록 체인의 탄생 이후 탈중심화는 블록 체인의 핵심 개념으로 되었다. 많은 지지자는 이 특질이 세계를 혁신하는 중요한 힘이라고 믿고 있다. 심지어 이 특질은 반드시 기존의 중심형의 세계를 뒤엎겠다는 생각하는 사람도 있다.

그 때문에 탈중심화는 동력 인이지만 블록 체인의 궁극이 아니다. 현실 세계를 보면 풍부한 인터넷 애플리케이션의 대부분은 중심화 시설로 제공하고 있다. 안전 및 편리 두 중에 하나를 반드시 선택하라고 하면 편리를 선택하는 사용자가 더 많을지도 모른다. 일방적으로 탈중심화를 강조하면 현존의 기술 생태를 동화할 수 없다. 그래서 분산 블록 체인의 궁극 원인을 강조하는 것은 일종의 편견이라고 본다.

2.3. 협의의 블록체인

PENTA 는 분포식은 "사인설"의 "질료 인"으로 본다. "질료 인"은 "사물에서 형성되어 계속 사물 속에 존재하는 것이다. 이는 탈레스를 비롯한 밀레토스 학파 및 레우키 포스와 데모크리토스의 원자론에서 유래한다. 블록 체인은 특수한 분포식 구조이며 누구나 서버를 만들어 네트워크에 가입하고 블록 체인 네트워크의 어느 노드가 될 것이다. 이는 탈중심화의 특성을 구축한다. 그래서 분포식은 "질료 인"이다. 그러면 분포식은 블록 체인의 궁극이 될 수 있는가? 알다시피 분포식 시스템은 블록 체인 탄생 이전 이미 존재했다. 분포식 시스템에서 한 독립한 컴퓨터는 사용자에게 하나의 정체처럼 보인다. 시스템은 대부분 통용된 물리 및 로직 리소스를 갖고 다이나믹하게 작업을 배포할 수 있다. 그리고 분산형의 물리 및 로직 리소스는 컴퓨터 네트워크에 의해서 교환한다. 그러나 이는 분포식 시스템에 블록 체인 같은 사상과 기술 혁신을 가져오지 못했다. 분포식 노드는 블록 체인의 위조 방지의 간접 원인에 불과하다. 블록 체인의 발전 과정에서 일

방적으로 분포식 구조를 강조하는 것은 협의적이다.

2.4. 편향된 블록 체인

PENTA 는 트러스트는 "블록 체인 네 인설" 속 "형식 인 "이라고 본다. 형식 인은 사물의 모델, 즉 본질을 나타낸 정의이다. 이것은 피타 고라스 학파의 "수"와 플라톤의 "아이디어"에서 유래하고 있다. "수"와 "아이디어"를 만물의 기원으로 "통신 식"의 작용을 강조한다. 트러스트는 사회 체계, 인문 발전과 경제 네트워크를 만드는 핵심이다. 여러 방법으로 트러스트 관계를 강화하는 것은 각 조직, 국가 전략 목표이다. 블록 체인 기술은 탈중심화 및 변조 방지등의 특성은 트러스트 네트워크를 쉽게 구축할 수 있기에 블록 체인은 "형식 인" 이라고 한다. 블록 체인 기술과 산업의 발전으로 블록 체인 네트워크 및 체계의 수는 갈수록 늘고 있으나 이들의 블록 체인 체계는 각각 자신의 "트러스트 네트워크"만 만들고 있다. 그러나 이들의 네트워크는 협력하지 않고 혹은 그 협력의 효율이 낮다. 트러스트를 블록 체인 발전의 궁극적인 목표라고 여기면 일방적인 생각이다.

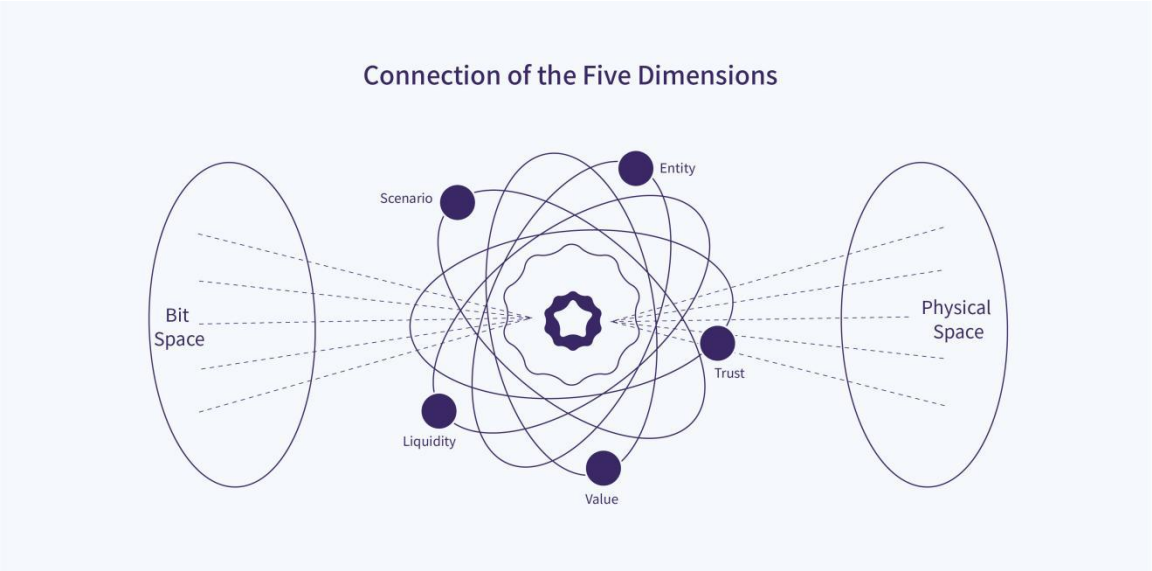
2.5. 본질의 블록체인

PENTA 는 보세라는 특성을 "블록 체인 사인설" 속 "목적 인"이라고 여긴다. "목적 인"는 사물의 "최선의 종결", 즉 "종결 인"이다. 이 생각은 파르메니데스의 “존재” 와 아낙사고라스의 "이성"를 거슬러 올라갈 수 있다. 왜냐하면, 영원한 "존재"로 하는 만물의 기원은 인과의 동일성을 강조하나 "이

성"은 만물의 질서를 유지하는 "선"으로 만물의 궁극적인 방향을 보다 더 잘 나타낸다. 블록 체인의 각 특성은 트러스트 관계를 강화하는 기계이다. 사람들은 트러스트 세상 혹은 트러스트 관계를 구축 비용이 낮은 이상적 세상을 원한다. 그럼 블록 체인을 이용하여 이를 실현하기 위하여 블록 체인 기술은 진짜 기반 인프라로 되어야 한다. 기반 인프라의 건설의 핵심은 모두에게 이익을 나누는 것이다. 즉 블록 체인 세계의 각 퍼블릭 체인과 제휴 체인을 로우 코스트로 연결하여 협력하도록 하는 것이다. 또 블록 체인 세계와 오프 체인 세계의 중심형 체계를 연결하도록 하는 것이다. 최종적으로 멀티 레벨의 세상을 만드는데 온체인 과 오프체인 상태를 막론하고 모두 힘을 발휘하고 이상적인 차세대 블록 체인 세계를 만들어 낼 것이다. 그래서 "모두에게 이익을 가져오는 것"은 미래 블록 체인 세계의 발전의 궁극 인이다.

3.다섯 차원의 연결

PENTA 는 "펜타 쿠르"(PENTAcle)에서 유래하고 있다. 고대 이집트, 고대 바빌로니아, 셀틱 전설, 피타 고라스 학파는 모두 펜타 쿠르를 숭배한다. 펜타 쿠르는 "다섯차 인터레이스"의 탄생을 상징하고 있으며 사물의 인과 관계를 탐구하여 역사와 발전을 추구하며 세계의 생물의 생명과 미래의 부호이기도 한다.



PENTA 의 중심 구조에 대응하는 다서 차원은 주체, 트러스트, 가치, 유통, 장면이다. 이는 차세대 블록 체인 세계의 커넥터로 미래 블록 체인 세계를 더 쉽게 만든다.

3.1. 주체

모든 참가자는 모든 인간, 사물, 조직 시스템을 포함한다. PENTA 에서 통일한 신분 표식을 사용한다. PENTA 는 신분 표식을 사용하여 수권 관리와 업무 처리를 실시한다. PENTA 은 주체의 멀티 신분 표시 관리를 지원한다.

신분 표식은 탈중심화로 관리한다. 신분 표시의 생성, 사용, 검증, 스토리지 등을 포함한다. 이를 통하여 사생활 보호와 안전 거래를 실현할 수 있다.

- 생성:신분 표식은 PKI 메커니즘에 의한 공개의 주소 정보를 생성한다. 신분 표시의 소유자는 주소와 개인 키를 보관한다. 그 외에 일부분의 주체는 특정 디지털 인증 센터가 발행한 증명서를 표시할 수 있다.
- 사용: 신분 표시의 주체는 개인 키 정보를 통해서 PENTA 에서의 디지털 자산을 거래하거나 PENTA 에 요청할 수 있다.
- 검증: PENTA 는 권익 검사와 거래를 검증하고 통과하면 합의에 이른다.
- 스토리지: 생성된 신분 표시와 대응하는 공개 정보는 PENTA 의 분산형 대장에 저장된다.

이 외에 신분 표식은 스마트 콘트랙트의 확장을 지지한다. 더 풍부한 신분 표시 관리를 실현하고 다른 업무 영역의 신분 관리 요구를 만족한다. 예로 들면 금융 영역에서는 자산을 거래할 때 관리 측의 KYC 수요를 만족해야 한다. 확장한 스마트 콘트랙트를 이용하여 KYC 의 설치와 스토리지를 할 수 있다.

3.2. 트러스트

블록 체인의 번영과 발전에 관해서 비교적으로 중요한 원인의 하나는 블록 체인 기술에 의한 탈중심화 트러스트 메커니즘을 실현하고 블록 체인을 "트러스트의 머신"로 되었다.PENTA 은 트러스트 주체, 트러스트 네트워크, 트러스트 인터랙티브를 이용하여 분산형 트러스트 메커니즘을 구축한다.

● 트러스트 주체

PENTA 속의 주체는 모두 PKI 을 이용함을 통하여 신분 표시를 만든다. 또한 분산형 대장을 통하여 정보 공개와 스토리지를 실시한다.인증 증명서를 통해 일부 운영 주체를 관리할 수 있다.

● 트러스트 네트워크

합의 알고리즘을 이용하고 거래를 확인하고 대장에 기록한다. 확인하자 어떤 방법으로도 취소할 수 없다.

● 트러스트 인터랙티브

다른 블록 체인 플랫폼 혹은 집중형 시스템은 암호화 키 혹은 인증 증명서를 사용하여 수권할 수 있다. 이를 통하여 크로스 체인 트랜잭션를 진행한다. PENTA 는 스마트 콘트랙트에서 크로스 체인 트랜잭션을 실시하는 것을 지지한다. 관계 체인 또는 시스템에서 합의를 실현하여 인터넷 전체의 합의를 실현한다. 이로써 트러스트 인터랙티브의 통제와 관리를 실현한다.

3.3. 가치

블록 체인은 탈중심화 디지털 자산 전이를 실현한다. PENTA 에 등록된 모든 재산은 특정 가치의 형태로 존재하고 있어 주체 간의 거래에 참여하여 가치의 전이를 실현한다. PENTA 의 가치 관리는 가치 생성, 가치 교환, 크로스 체인 거래를 포함한다.

PENTA 에서의 가치는 매번 공감를 달성할 때부터 PNT 형식으로 합의에 참가한 노드에 배포한다. 그 외 진입한 주체는 오프-라인 상태에서 코체인을 매핑하다.

가치 자산은 PENTA 에 의해서 가치 교환하며 PENTA 는 소프트 익스체인지 어댑터를 사용하여 다른 체인과 가치 교환을 지지한다. 그리고 스마트 콘트랙트를 통하여 거래를 잠그고 관리하다.

3.4.장면

PENTA 는 각 블록 체인 시스템, 분산형 중심화 시스템, 주체 사이의 연결을 지지하여 비즈니스 장면의 지지와 연결을 실현한다. PENTA 는 가치 교환의 중추로서 클라우드 컴퓨팅, 빅 데이터, AI 등과 결합하여 다양한 비즈니스 상황에 대응하여 지지한다. 제 다섯 장은 PENTA 는 일부분 업무 영역에서 어플리케이션 방식에 대해 자세히 소개한다.

3.5. 유통

Penta 는 차세대 블록 체인 세계를 연결 커넥터로 새로운 비즈니스 장면을 지지할 뿐 아니라 전통의 비즈니스 상황에서도 유통이 가능한다. 이로 블록 체인과 모든 비즈니스를 연결하는 미래의 비즈니스에 트러스트와 가치 교환의 기초를 제공한다.

이를 실현하기 위하여 Penta 는 Dapp 모듈과 SDK 를 제공하고 Dapp 의 개발을 쉽게 한다. 개발자는 블록 체인의 기초 지식이 없어도 조합된 툴킷에서 Dapp 를 개발할 수 있다. 또한 Penta 는 체인점을 제공함을 통하여 Dapp 의 사용과 보급에 플랫폼을 제공한다.

4. PENTA 네트워크

4.1 PENTA 기술의 프레임위크

PENTA는 모듈화된 기반 구조를 채택하기에 유저들이 블록체인앱이나 섭체인을 만들 때 대부분 모듈들이 레고처럼 상호 인용을 통해서 어셈블리할 수 있다. 모든 모튤들이 플러그형 기술을 지지한다. 예를 들면 합의 모듈은 POW、POS、dPOS、PBFT 를, 암호화 알고리즘은 RSA, State Encryption Algorithm 등을 지원한다. 그리고 유저들이 거기다가 확장도 가능하다.

저장모듈과 커뮤니케이션 모듈은 블록체인 시스템의 기본 모듈들이다. 커뮤니케인션 부분에서는 PENTA 는 P2P 네트워크를 실현할 뿐만 아니라 분산식 사설망과 유연성 체인 계약 (상세한 내용은 기술 부분 참조) 도 동시에 확장한다. 뿐만 아니라 PENTA 는 기업체 유저들의 재해 복구 및 데이터 검색을 동시 만족하기 위해 보통 불록 뿐만 아니라 세상 상태와 블록 데이터 저장, 그리고 관계성 데이터 저장 등의 모듈을 만들었다.

보안 모듈 면에서 PENTA 는 스마트 계약, 디지털 재산, 격려 메커니즘, 멤버 관리, 그리고 권한 관리 등 스마트 계약과 블록체인 앱 개발 시 꼭 필용한 기반 모듈들을 제공한다.

응용 모듈 면에서 PENTA 는 스마트 계약, 디지털재산, 격려메커니즘, 멤버관리와 권한 관리 등 스마트 계약와 블록 응용을 개발하는 데 필요한 기초적인 모듈을 제공한다.

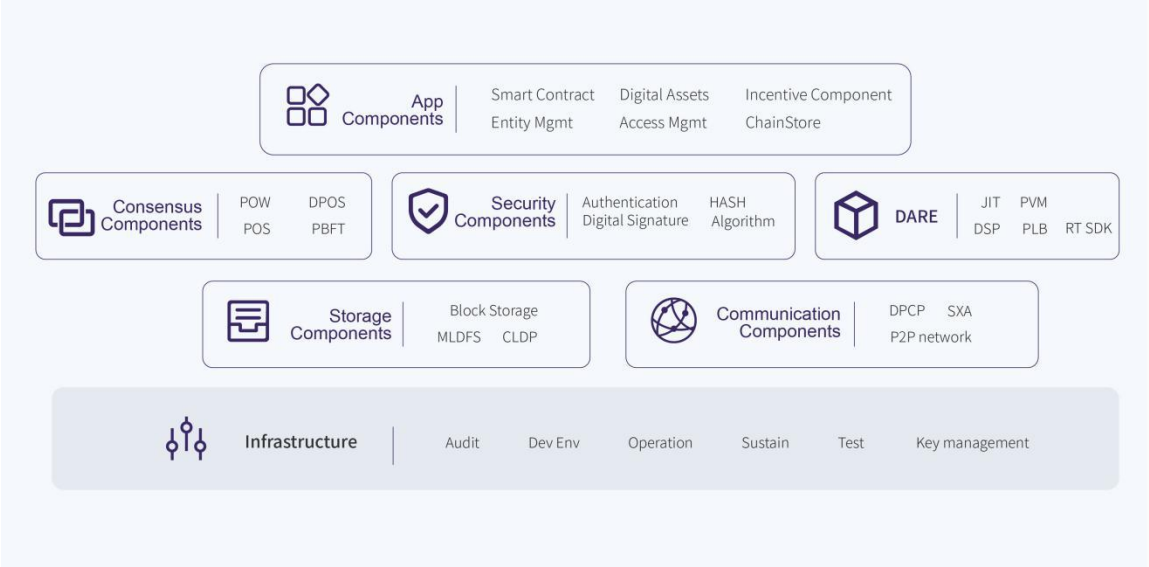


그림 3 PENTA 기술 프레임위크 예시

4.2 PENTA 네트워크 DAPP

PENTA 네트워크에서 DAPP(볼록체인 애플리케이션)은 PENTA 네트워크 상황 응용 서비스를 실행하는 핵심이다. 보통 ui 레이어, 업무로직 레이어, 데이터 레이어으로 나누어진다.

DAPP 데이터 레이어에서 DAPP 시행시 산출된 상태 데이터는 PENTA 네트워크 원장에 저장된다. 데이더는 PENTA 내의 파일이나 데이터 베이스의 형식으로 각 노드에 저장되기에 PENTA의 서버는 보통 블록 데이터만 동기화한다. 블록 데이터는 DAPP 상태 데이터의 버전 번호 및 지문 정보만 포함되고 DAPP 의 상태 데이터가 들어가지 않는다. 유저들이 PENTA 서버의 Chainstore 에서 DAPP 를 다운로드 받아야 해당 DAPP 의 상태 데이더가 다른 노드에서 로컬로 동기화 가능해진다.

DAPP 업무 레이어는 간단한 스마트 계약일 수도 있고, 복잡한 업무 DAPP 응용서비스의 핵심일 수 있다. 업무 레이어의 외부 인터페이스는 보

통 콘트롤류(초기화, 메타데이터 등), 검색류(수정 불가하고 검생용만의 데이터), 그리고 변경 데이터(업무 로직은 데이터 레이어의 데이터를 수정할 것이니 기록노드의 합의가 있어야만 데어터 활성화 가능)3 가지로 나누어진다.

DAPP UI 레이어는 PENTA 클라이언트에서 운용할 때 유저들과의 인터랙션를 담당한다. UI 레이어 개발은 해당 개발 규칙과 프레임 요구에 만족해야 클라이언트에서 적용된다. PENTA 에서의 DAPP UI 레이어는 MVVM 프레임을 작용하여 UI 구조과 전단 로직 처리의 유효적 분리를 통해 UI 레이어 코드의 유지 가능성을 높인다. DAPP 는 인터페이스 패턴으로 서비스를 제공할 수 있으며 ui 프레이가 없어도 된다.

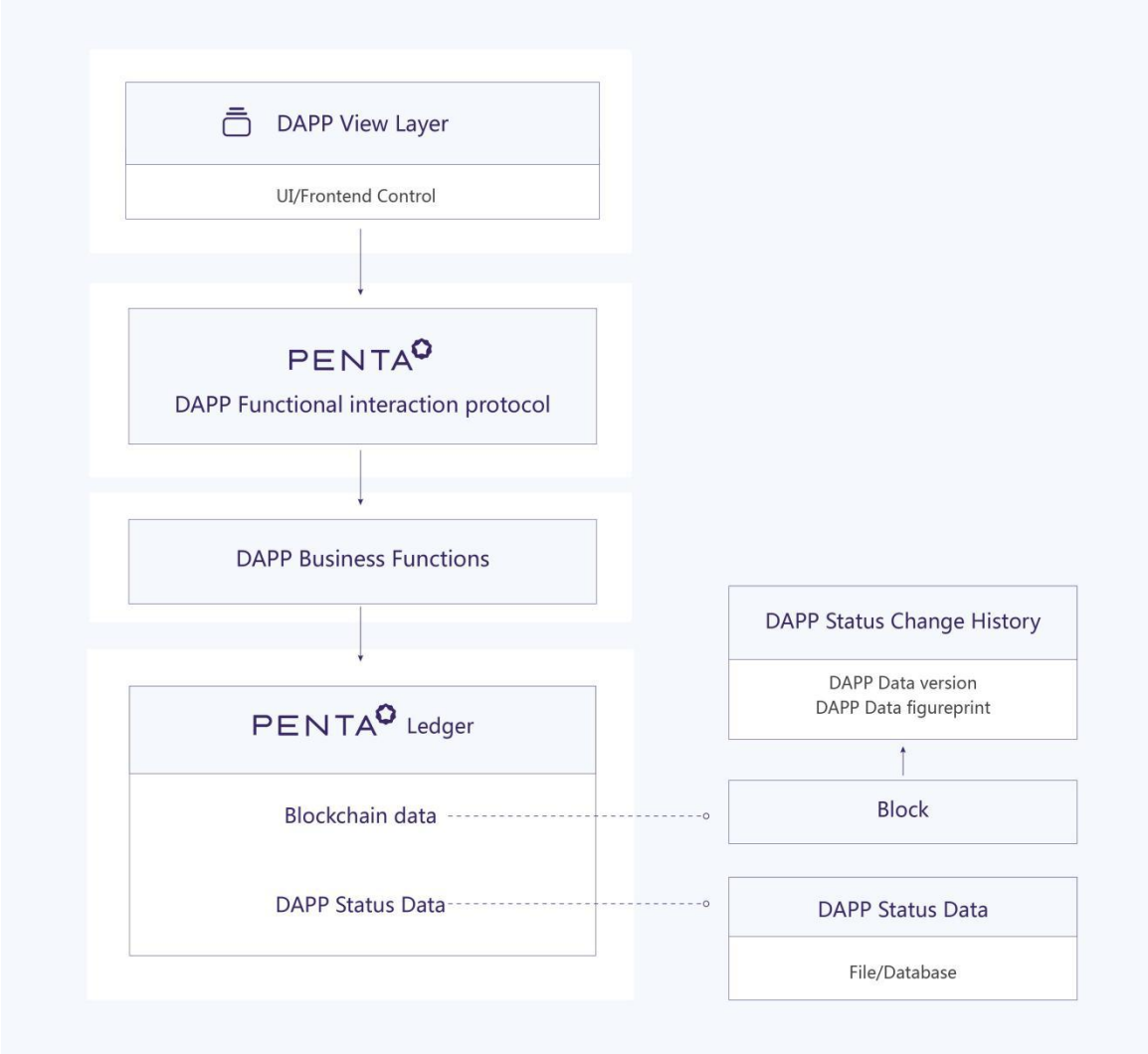


그림 4 PENTA 네트워크 DAPP 구조 원리 예시

4.3 PENTA 체인 스토어(PENTA chain store)

PENTA 체인 시토어는 PENTA 네트워크에서의 로그인 체인과 체인 서비스 (스마트 계약, 기타 DAPP 애플리케이션 등 포함)의 정보 센터다. 체인스토어의 데이터는 부분적으로 PENTA 체인 원장에 저장되어 있고 UI 로직은 PENTA 의 클라이언트 쪽에서 제공한다. 유저들이 PENTA 클라이언트의 체인 애플리케이션 스토어에서 DAPP 를 다운로드 받고 체인스토인에서 등록된 DAPP 정보에 따라 DAPP UI 프로그램을 다운로드 받으면서 동시에 DAPP 의 상태 데이터를 로컬로 자동 동기화시킨다.

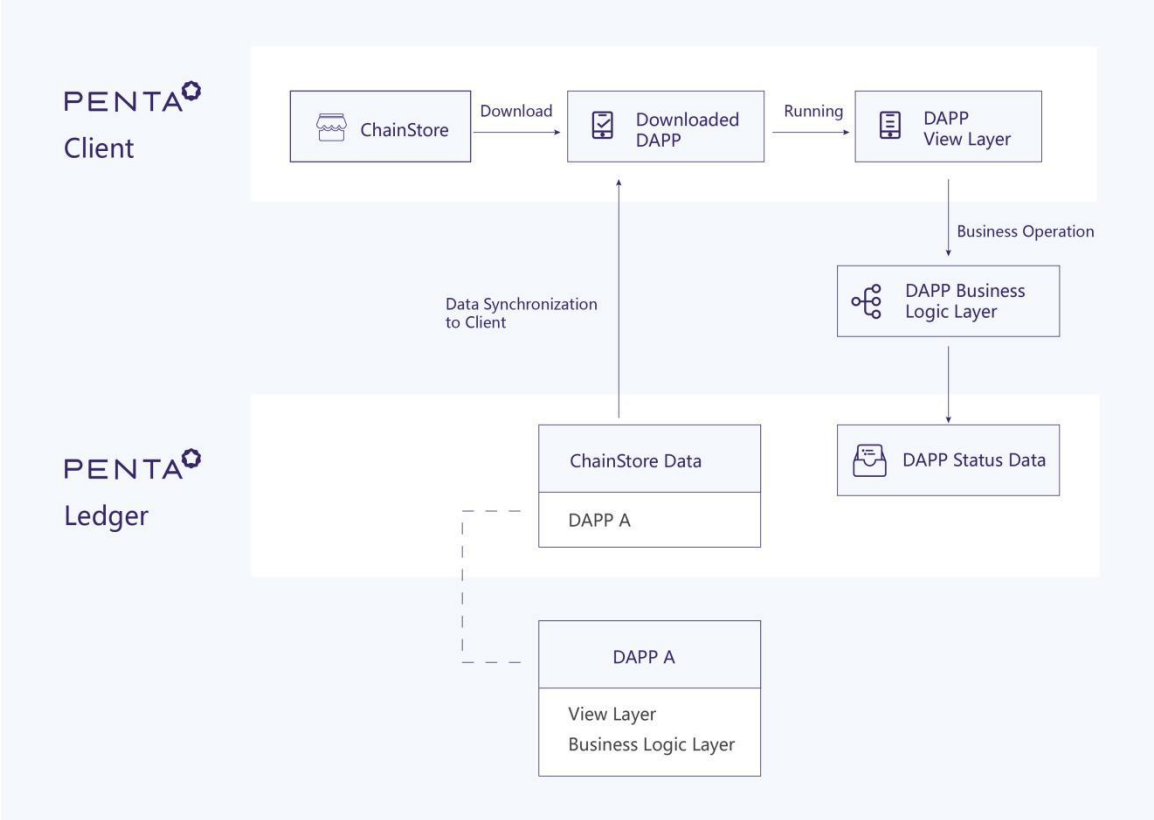


그림 5. PENTA 체인 체인 스토어 원리 예시

4.4 주쇠결합(Interchain) 서비스 합력 기슬 시스템

주쇠결합(interchain)서비스 합력 계약은 체인과 체인, 체인과 기존센터시스템 간의 협력이 가능하게 해 주고 연성 업무 메커니즘을 지원하여 분산식 응용이 업무 컨트롤을 할 수 있게 한다. DAPP SDK PENTA 의 핵심 실행 플랫품으로서 다른 체인을 호출하는 표준 API, 기존 주요 블록체인 플랫폼(BTC、ETH、Ripple、Stellar、NEO、Dash、 Hyperledger 등)의 API 를 제공한다. DAPP 에서 개발자가 해당 API 를 호출하면 다른 체인이나 기존 센터시스템하고 인터랙션를 실현할 수 있다. 기능 모듈 레이어는 통합 ID 인증, 체인서비스 로그인, 체인 서비스 검색, 체인 서비스 평가 등을 제공하여 체인 서비스 간, 체인과 기존 중앙 시스템이 제공한 서비스와의 협력 운행을

실현하다. 또한 PENTA 네트워크는 통합적 UX 를 만족하기 위해 주요 블록체인 클라이언트 (BTC、ETH、Ripple、Stellar、NEO、Dash、Hyperledger 등) 와의 컨버전스 서비스도 제공한다. 그와 동시에 위의 체인들을 방문할 때 통일된 api 표준도 같이 제공한다. 그래야 기타 체인들은 클라이언트 컨버전스를 통해서 통일된 방식으로 PENTA 체인과 타체인 간의 연결 및 협력을 아주 쉽게 실현할 수 있다.

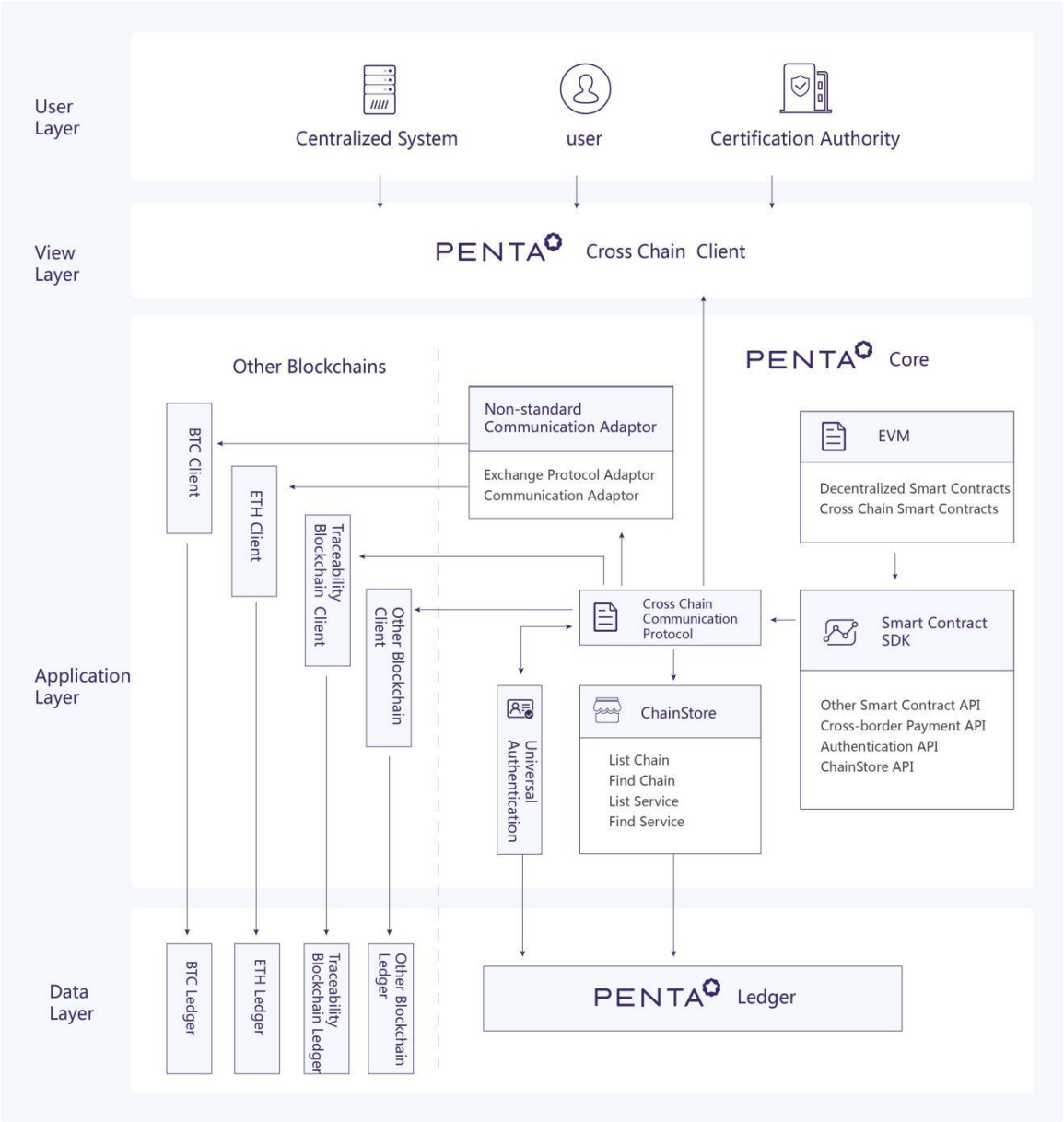


그림 6 주쇠결합(interchain) 서비스 합력 계약 원리 전시도

4.5 기술적 세부 사항

PENTA 네트워크는 미래 세계의 커넥터(Connector)를 만드는 데 목적이 있다. 향후 더욱 복잡한 탈중심화 혹은 중심화 앱들이 나타나서 유저들에게 서비스를 제공한다. 그러나 기존 블록 체인 플랫폼은 DAPP 지원 불가하든가, 아니면 간단한 DAPP 만 지원 가능하기에 그로 인한 부족한 성능이 유저들의 요구를 만족하지 못한다. 이런 문제를 해결하기 위해 PENTA 네트워크는 고성능 스마트 계약 플랫폼을 개발하는 데 그 목표가 있다.

PENTA 네트워크는 이더리움을 비롯한 퍼블릭 블록체인들, 그리고 하이퍼레저(Hyperledger)로 대표되는 연매체인의 수많은 장점과 저층 블록체인으로의 다년간에 쌓여진 PENTA 자신의 경험을 결합하여 10 가지 핵심 기술을 개발하였다.

4.5.1 DSC

PENTA 네트워크에서 메인 체인의 블록은 동적 권한을 기반으로 한 합의 계약을 채택하여 동적 선거를 통해서 어느 정도 기록자를 뽑아내고 해당 규칙에 따라 그 중의 일부 기록자를 선정하여 기록에 참여시킨다. 선정된 기록자들이 PBFT 알고리즘을 이용하여 거래 합의를 한다. 기록자로서 누구나 참여 기회를 가지고 있지만 매번 합의는 과다한 기록자가 참여하지 않도록 한다. 이렇게 하면 합의 성능을 효율적으로 높일 수 있다. Pbft 알고리즘은 Miguel Castro 와 Barbara Liskov 두 사람이 1999 년에 공동 발표한 것

이고 PBFT(Practical Byzantine Fault Tolerance) 초기 알고리즘의 저효율 문제를 해결하여 복잡도이 기하급에서 다항식으로 낮춤으로써 pbft 알고리즘은 실제적으로 실행 가능할 수 있도독 하였다. Pbft 알고리즘은 n 개의 합의 노드로 이루어진 합의 시스템에게 f=⌊(n-1)/3⌋의 고장 허용 능력을 제공할 뿐 더러 강한 지속성이 가지고 있으므로 거래가 한번 확인되면 취소나 롤백이 발생하지 않을 것이고 갈래도 나눠지지 않는다.

PENTA 는 여러 합의 알고리즘이 공존하는 매커니즘을 채택하여 스마트 계약 진행과 블록 생성은 각각 독립적인 합의 체계를 가지고 있으므로 블록 생성 때 부담을 덜 해주고 플랫폼 자원을 더욱 합리적으로 이용해서 전체적인 합의 성능을 높인다. 합의 참여자들은 기록자 장려를 받을 것이고 저층 사용 합의 커머니즘은 두 가지의 합의가 통일한 상태로 유지할 수 있다. 또 더 많은 사람들이 저장 자원을 공유하기를 격려하기 위해 특정한 저장 자원에 대해 데이터 합의 알고리즘을 채택하고 소비자에게 일정한 PNT 를 받아 자원 제공자에게 장려한다.

PENTA 네트워크는 다 볼록체인 기술을 지원한다. PENTA 는 플러그 합의 알고리즘을 지원하기 때문에 여기서 만든 부속 블록체인들은 응용 상황에 따라 적절한 합의 프로토콜 (POW, POS, dPOS, PBFT, POC 등)을 선정 가능하다.

POW 는 컴퓨터에 의해 수학 알고리즘을 진행하여 기록권을 얻는 합의 프로토콜이다(마이닝) .

POS 는 노드의 기록권 획득 난이도는 노드의 권익과 반비례되는 합의 프로토콜이다

dPOS 는 노드들이 대리인을 투표 선정하고 대리인이 검증과 기록을 담당하는 합의 프

로토콜이다.

PBFT 는 허가 두표를 통해 다수결의 원칙에 따라 선정된 리더가 기록하는 합의 프로토콜이다.

POC 는 용량에 따라 합의를 진행하는 프로토콜이다.

4.5.2 탈중앙화 응용엔진

DARE 는 분산식 알고리즘 엔진으로서 패러렐 버추얼 머신(PVM, Paraller Virtual Machine) , 부하 균형, QOS, 시행시 sdk (Software Development Kit) 등이 내장되어 있다. 그중에서 PVM 는 JVM 과 같이 범용의 버추얼 머신이며, 가상적인 컴유터로서 실제 컴퓨터에서 각종 컴퓨터 기능을 실현한다. 스마트 계약의 시행 효율을 높이기 위해 우선 JIT(Just-In-Time Compiler) 컴파일 방식을 통해 스마트 계약을 바이트 코드로 편집한다. 그 다음에 편집된 바이트 코드는 버추얼 머신에서 특정된 플랫폼의 컴퓨터 명령으로 표현되어 실행된다.

Dare 는 불록체인 응용 운행 때 버추얼 머신 환경 초기화, 초기화 및 MLDFS 걸기, 초기솨 및 CLDP 걸기, 분산식 컴퓨팅 코오디네이터 등 업무를 담당한다. 그중에 컴퓨팅이나 저장은 부산식 설치를 모두 지원한다.

4.5.3 멀티레벨 분산식 파일 시스템

멜티레벨(MLDFS)는 분산식 파일 시스템 저장 합의로서 명칭 공간이라 데이터 공간으로 나누어져 있으며, 명칭 공간은 파일 명칭을 관리하는 것이고 데이터 공간은 해당 데이터를 저장하는 공간이다. 데이터 파일은 약

간의 블록으로 나누어져서 데이터 공간에다가 저장된다. 데이터 블록에 대해서 전통적인 파일 시스템를 의해 분산식 저장도 되고 또 MLDFS 를 이용하여 저장해도 된다.

MLDFS 는 버전에 의해 파일을 저장한다. 블록체인에서 합의를 제출할 때마다 그 합의와 해당된 유일한 버전 번호를 얻을 것이고 이 번호는 해당 버전 합의의 hash 값을 검증하는 데이터로 삼는다. 각 버전은 그 버전의 변경 데이터를 기록하고, 변경된 번호는 블록에다가 기록될 것이며, 또 DAPP 상태 데어터의 일부분으로 다른 노드들에 의해 동기화된다. 그와 동시에 버전 번호는 동기화된 데이터의 무결성를 검증할 때도 쓰인다. 기타 노드들이 데이터와 시간을 유과적으로 감소하여 블록체인의 전체 성능을 높이기 위해 증분 동기화를 수행해도 된다

MLDFS 는 가상화 기술을 이용하여 각 불록체인이 시행할 때 DARE 에 의해 독립적인 파일 저장 공간을 분배하는 것이다. 그리고 모든 파일의 변경 기록은 스마트 계약이나 블록체인 응용 차원에서 관리할 것이며 저장된 파일 버전의 변경도 각 블록체인에 따라 진행된다.

MLDFS 는 분산식 업무 관리를 지원한다. 합의 참여 노드들이 블록체인 응용 시행, 결과 검증, 서명, 그리고 파일 수정 등 차례대로 진행할 때 합의를 제출하기 전에 데이터는 파일 시스템에 기록되지 못한다. 합의를 제출하고 나서야 파일이 저장되어 새로운 버전이 형성되고 최종적으로 계층화 분포로 나타날 것이다.

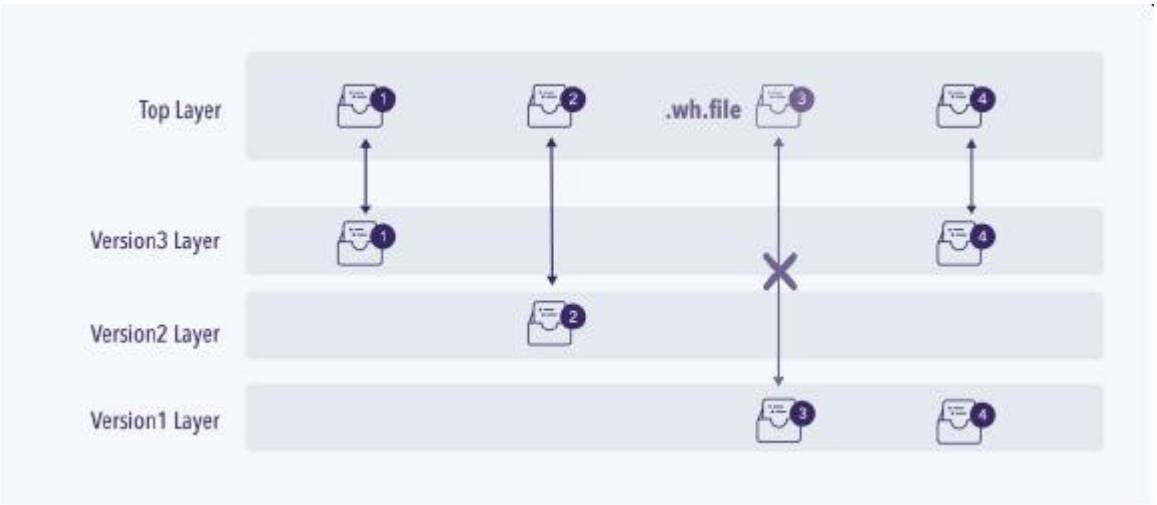


그림 7 멀티레벨 버전 분산식 파일 시스템 예시

4.5.4 켄테이너 레벨 데이터베이스 프로토콜

켄테이너 레벨 데이터베이스 프로토콜은 PENTA 네트워크를 위해 개발한 분산식 데이터 베이스 저장 엔진이다. CLDP 는 데이터 세트를 대상으로 관계형 데이터 베이스와 비관계형 데이터 베이스의 장점을 겸비할 뿐 아니라 동시에 SQL 엔진을 제공하여 블록체인 응용 개발을 감소화시킨다. 스마트 계약 데이터와 랜잭션 저널을 분리하여 블록체인 응용 데이터 동기화와 복제를 효율적으로 진행하도록 버추얼 메커니즘을 제공한다. CLDP 는 설치, 활용, 저장 면에서 편의성을 가지고 있고 라이트급의 개인 유저를 넘어 헤비급의 기업체들의 수요까지도 만족할 수 있는 고성능적인 엔진이다.

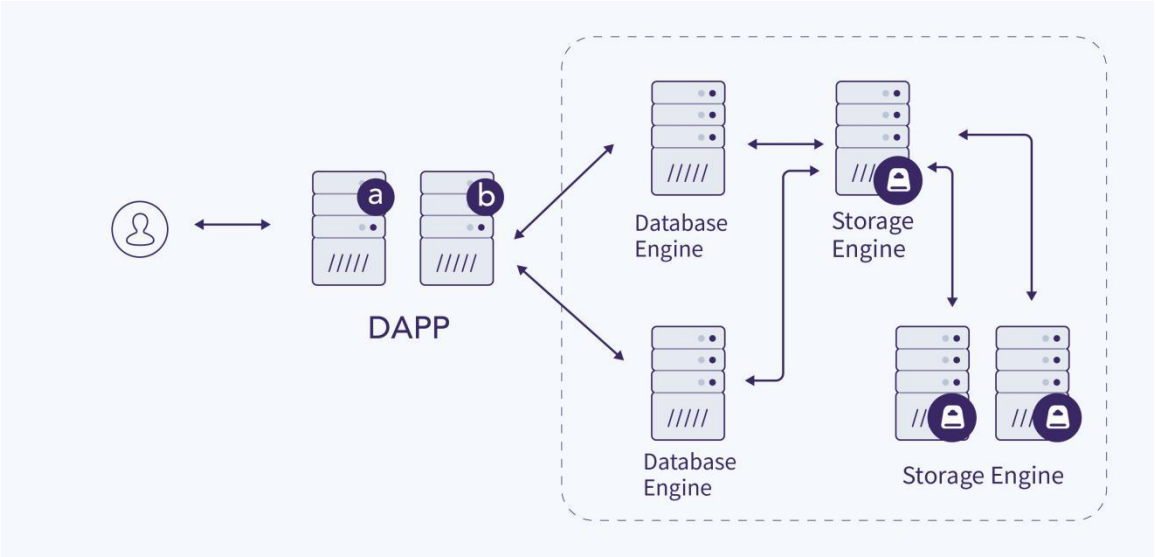


그림 8 켄테이너 데이터베이스 계약 예시

4.5.5 분산식 서비스 프로코틀

고성능 블록체인에 대한 기업체들의 요구를 만족하기 위해 PENTA 플랫폼에서 분산식 서비스 프레임워크를 개발한다. 이 플랫폼에서 서비스 정의, 서비스 등록, 서비스 감시, 원격 통신과 데이터 교호, 서비스 호출, 클러스터 결함포용 등 작업을 지원하며, DARE 분산식 메커니즘을 결합함으로써 블록체인 응용이 기업체 내부에서 분산식 클러스터 방식으로 운행하여 우수한 병행성, 고효성, 안정성, 고품질의 서비스를 제공한다.

4.5.6 PENTA Dock World(PDW)

PENTA Dock World 는 스마트 계약과 기타 블록체인 응용을 위해 버추얼 스마트가 독립적 운행 공간, 독립적인 알고리즘 소스, 데이터베이스, 파일 저장 등 응용 운행 조건을 제공한다. 블록체인 응용에서의 모든 소스에 관련된 접근 권한은 다 PDW 안에 제한되어 있고 PDW 외의 다른 블록체인

의 데이터나 파일을 접근하면 안 된다.

Pdw 에서의 알고리즘, 데이터베이스, 그리고 파일저장 소스는 각각 DARE, CLDP, MLDFS 에 의해 배정된다. 그중에서 블록체인 응용은 MLDFS 와 CLDP 를 의해 제공한 전용 API 로 소스를 접근하여 운행 완료 시 상태 버전 지문으로 생성되어 블록에다가 기록을 남는다.

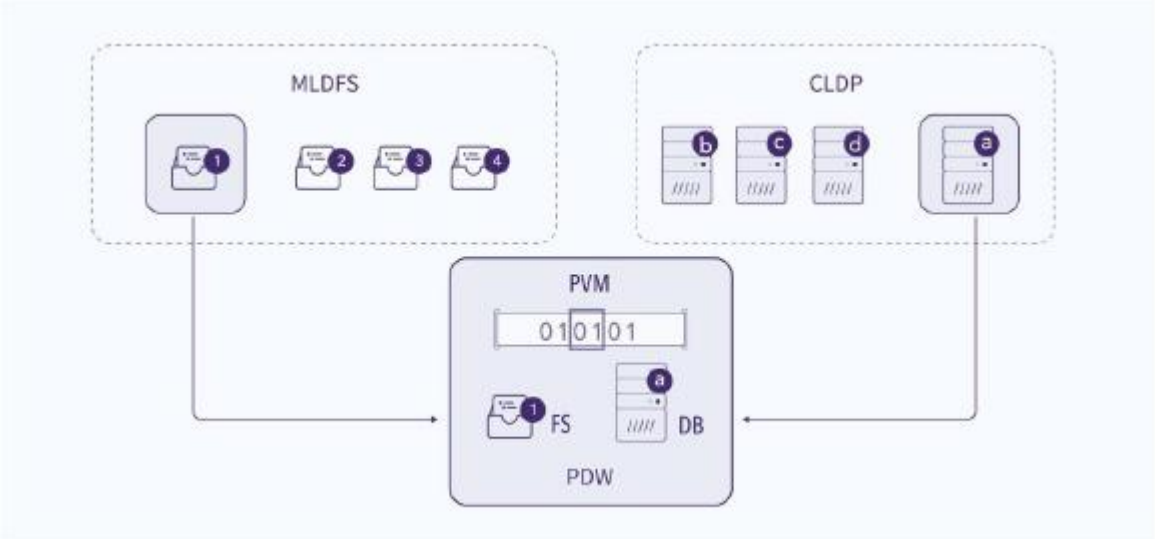


그림 9 pdw 예시

4.5.7 플렉서블 링크 계약

탈중심화 시스템으로서 블록체인 기술은 신속한 발전 속도를 보이고 있지만 블록체인 응용이 특정한 상황에만 적용된다. 또 기존 중심화 시스템이 앞으로 장기간 동안 사라지지 않기 때문에 불록체인 응용은 더욱 넓은 분야에서 기존 시스템하고 합력이 필요하다. 이런 상황 하에 더욱 안정하고 효율적으로 중심화 시스템에 접근하기 위해 플렉서블 링크 계약(SXA)이 개발된다. SXA 는 통신층, 계약층 ,업무층 등 3 가지로 나누어져 있으며 이 3 개의 계약들이 서로 협렵해서 중심화 스시템에 신속한 연결이 가능하다.

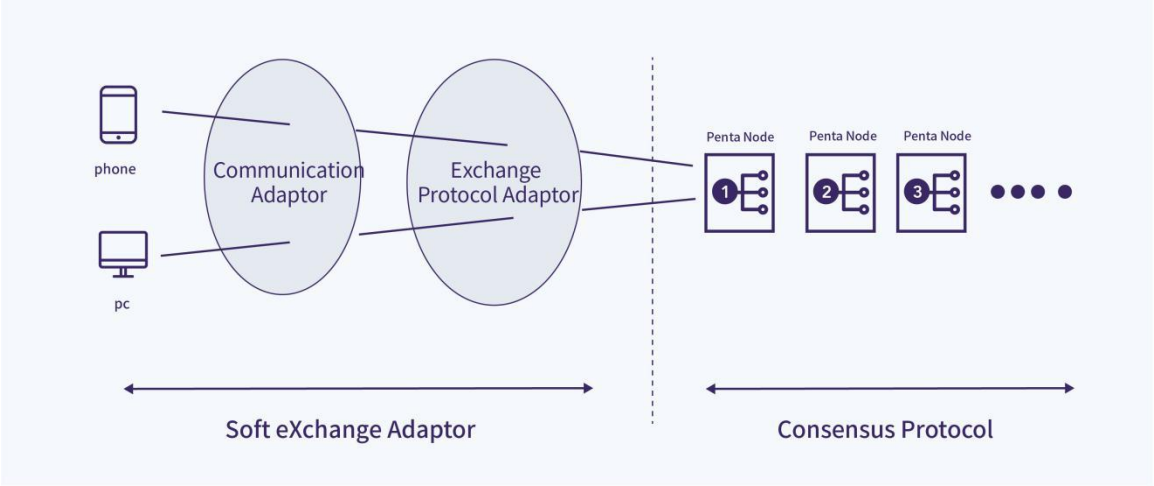


그림 10 플렉서블 링크 예시

4.5.8 분산식 PCT（Private communication protocol）

블록체인은 P2P 네트워크에서 데이터 정보가 방송될 것이고 또 방송된 데이터 정보는 모든 참여자들에게 확인 가능한 공개적 통신시스템이라는 것은 암목한다. 하지만 현실 거래 과정에서 업무 무관자에게 데이터 노출하기 원하지 않은 경우가 있는데 PENTA 는 이 문제를 해결하기 위한 것이다. PENTA 는 네트워크의 노드 사이에서 DPCP 라는 특별한 통신망을 만들 것이다. 통신망에서 연결된 노드 2 개가 사적 정보를 전송하려면

그림 11 분산식 사적 통신 계약 예시

DPCP 에서 특별한 통신 터널을 구축될 것이다. 터널를 통과하는 모든 데이터는 접근 양쪽만 볼 수 있으며 기타 제 3 방 유저들 그 누구도 엿보지 못한다. PENTA 네트워크는 라우팅, 채널 구축, 데이터 컨트롤, 증서 교환, 데이터 키 교환, 암호화 데이터 교환, 채널 폐기 등 메커니즘을 제공한다.

4.5.9 PNT 장려 방안

더 많은 참여자들이 알고리즘, 저장, 소스를 제공하기를 자극하기 위해 PENTA 네트워크는 블록 생산할 때마다 생기는 일정량의 에너지 입자(PNT)를 장려품으로 제공자에게 준다. PNT 를 이용하여 기록자 선거 출마, 계좌 이체, 스마트 계약 발표와 운행, 그리고 저장 소스 사용 등 자격을 가지게 될 것이다. 매번 합의 달성 후 받은 PNT 는 기록 노드와 소스 제공자가 각각 50%를 균분한다. Pnt 의 장려는 일정한 비율로 소진이 되 돌고 점차 줄일 것이다.

4.5.10 안티 퀀텀 보안 대책

PENTA 네트워크는 다중적 보안 대책을 마련하여 플랫폼의 안전을 보장한다. 근본적 소프트웨어 중에서 ECC, SM2 와 같은 암호 기술 선택할 수 있을 뿐더러 프로젝트 진행 상황에 따라 적시에 안티 퀀텀 알고리즘도 이용할 수 있다.

PENTA 네트어크에서 사용된 ECC 암호 알고리즘은 주류 비대칭 알고리즘 중의 하나이다. 공개 키 암호 알고리즘은 항상 어려운 수학 문제를 기반으로 한다. 예를 들면, RSA 가 기분으로 한 문제는 다음과 같다: 지정된

소수 p, q 를 곱하면 n 이 된다. 그러나 n 를 인수 분해하는 것은 오히려 상당히 어려운 것이다. 또 ECC 알고리즘은 다름과 같은 문제를 기반으로 한다:

K= kG [k, G 는 Ep(a, b) 위의 점이며, k 는 n(n 는 G 의 찻수이다) 보다 작은 정수이다]. 지정된 k 와 G 의 덧셈을 하여 K 를 컴퓨팅하는 것은 쉽지만, 지정된 K 와 G 를 가지고 k 를 컴퓨팅하는 것은 오히려 그리 쉽지 않을 것이다. 이것은 바로 타원곡선 암호 알고리즘(ecc)이 기반으로 한 문제이다. 그 중에서 G 는 기점(base point), k 는(k<n, n 는 기점 G 의 찻수다) 사적 키(privte key), K 는 공개 키(public key)라고 부른다.

ECC 알고리즘을 이용한 암호화 통신 과정은 다음과 같다:

A 는 타원곡선 Ep(a, b)을 정하여 곡선 위에 G 를 기점으로 삼는다.

A 는 사적 키 k 를 선택하여, 공개 키 K 는 kG.

A 는 Ep(a,b)과 K, G 를 유저 B 에게 보내준다.

B 는 정보를 받고 나서 발송될 평문 암호를 Ep(a,b) 위의 M 점에다가 코딩하여(코딩 방법이 많지만 여기서 논의하지 않는다.) 임의의 정수 r 를 생성한다. r(r<n)

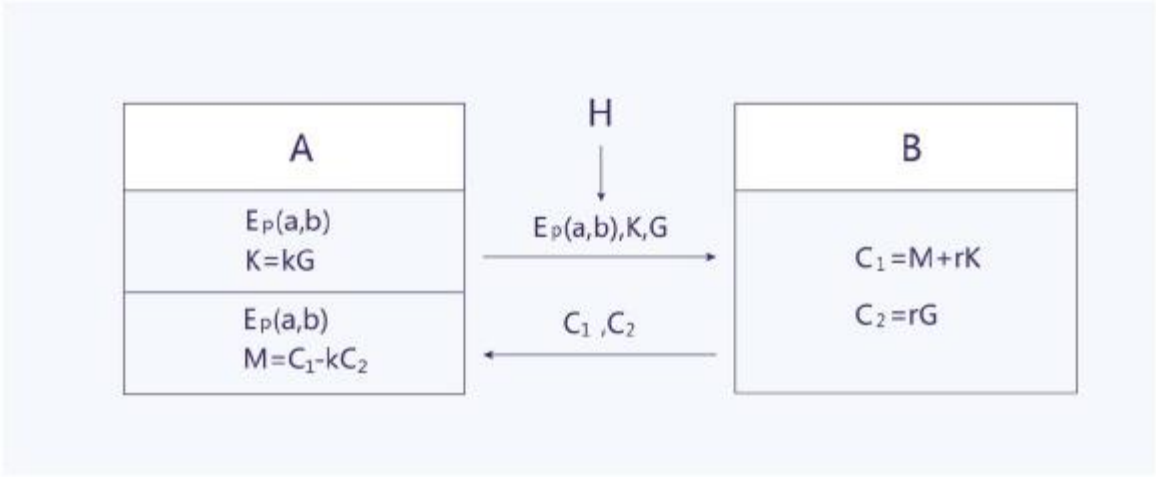
B 는 C1, C2 점을 컴퓨팅한다. C1=M+rK ; C2=rG.

B 는 C1, C2 를 A 에게 발송한다.

정보를 받은 A 는 C1-kC2 를 컴퓨팅하여 결과 M 점을 받는다. 그다음에는 C1-kC2=M+rK-k(rG)=M+rK-r(kG)=M 의 연산 방법으로 M 를 해독하면 평문 암호를 얻을 수 있다.

위와 같은 암호화 통신 과정에서 엿보는 사람 한명 있으면 그 사람이 Ep(a,b)、K、G、C1、C2 만 볼 수있다. 그러나 K, G 를 통해 k 의 값을 구하거나 C2, G 를 가지고 r 값을 구하는 것은 다 상당한 난도를 가지는 것이다. 그렇기 때문에 H 는 A, B 간에 전송된 평문 정보 확득이 불가능한 것이다.

암호 작성법에서 Fp 위의 한 타원곡선을 설명할 때 다음과 같이 6 개의



매개변수가 필요하다:

T=(p,a,b,G,n,h)

(한 타원곡선는 매개변수 p, a, b 에 의해 정해진다. G 는 기점이고, n 는 G 의 찻수다. h 는 곡선 위에 모든 점들의 갯수 m 와 n 를 나눗셈해서 얻은 결과의 정수 부분이다) 이와 같은 매개변수들의 값 암호화의 안전성에 직접적인 영향을 끼칠 것이다:

1. p 값은 크면 클수록 안정성이 더 높겠지만 알고리즘 속도도 그만큼 떨어진다. 보통 200 자릿의 값이면 일반적 안전 보장에 문제 없을 것이다.
2. $p \neq n \times h$.
3. $pt \neq 1 \pmod{n}$, $1 \leq t < 20$;
4. $4a3+27b2 \neq 0 \pmod{p}$;

5. n 는 소수다;

6. h≤4.

PENTA 네트워크에서 지원하는 SM2 알고리즘은 중국국가암호국이 ECC 알고리즘을 기반으로 개발한 것이고, 중국 비즈니스 분야에서 광범위하게 운용하고 있으며 특히 금용 영역에서 의무적인 사용이 규정되고 있다. 향후 SM2 알고리즘을 지원하는 PENTA 네트워크에서 더욱 폭넓은 분야에서 적용될 전망이다.

PENTA 네트워크가 아이디 인증 시스템을 도입함으로써 안전성, 기밀성, 그리고 참여자 신분에 대해 엄격한 요구가 있는 연맹체인이나 중심화 시스템과의 협력은 더욱 쉽게 이루어질 것이다. PENTA 아이디 인증 시스템에서는 일단 전통적으로 권위 기구에서 참여자들의 신분 정보에 대해 인증 받았고 마스킹 처리한 개인 정보와 권한 부여 정보를 PENTA 원장에다가 기록하고 다른 사용자들의 검증을 기다린다.

정보 남용, 과다한 거래 거품의 문제가 생기지 않고 플랫폼의 안정성을 높이기 위해 PENTA 네트워크는 인터넷 계죄이체와 스마트 계약 이용자 시행및 저장할 때 일정량의 PNT 를 공제한다. PNT 소유자는 투표를 해서 위와 같은 행위에 대해 PNT 공제 여부와 공제 수량을 결정한다.

5. PENTA 네트워크의 응용

지난 2 년 동안, PENTA 는 세계 각 업계의 여러 기업이나 조직과 협력하여 블록 체인 프로젝트 몇개를 시작하였다. 장래적으로는 PENTA 가 업계의 깊이를 계속 더할 거고 보다 많은 어플리케이션을 위한 굳건한 블록 체인 인프라를 제공하여 효율의 높임과 비즈니스 비용의 삭감함에 주력할 것이다.

그리고, 사회와 경제적인 차원에서, PENTA 는 블록 체인의 실제 응용 네트워크를 구축할 것이다. 인공 지능, 빅 데이터, 가상 현실(VR), 로봇, 사물 인터넷, 클라운드 소비스등 신기술과 결합하여 건강 의료, 교통 운수, IP, 신생 에너지 자동차, 유기 농업, 분산식 에너지, 패션, 식품, 비즈니스, 금융, 게임등 업종에 적용된다.

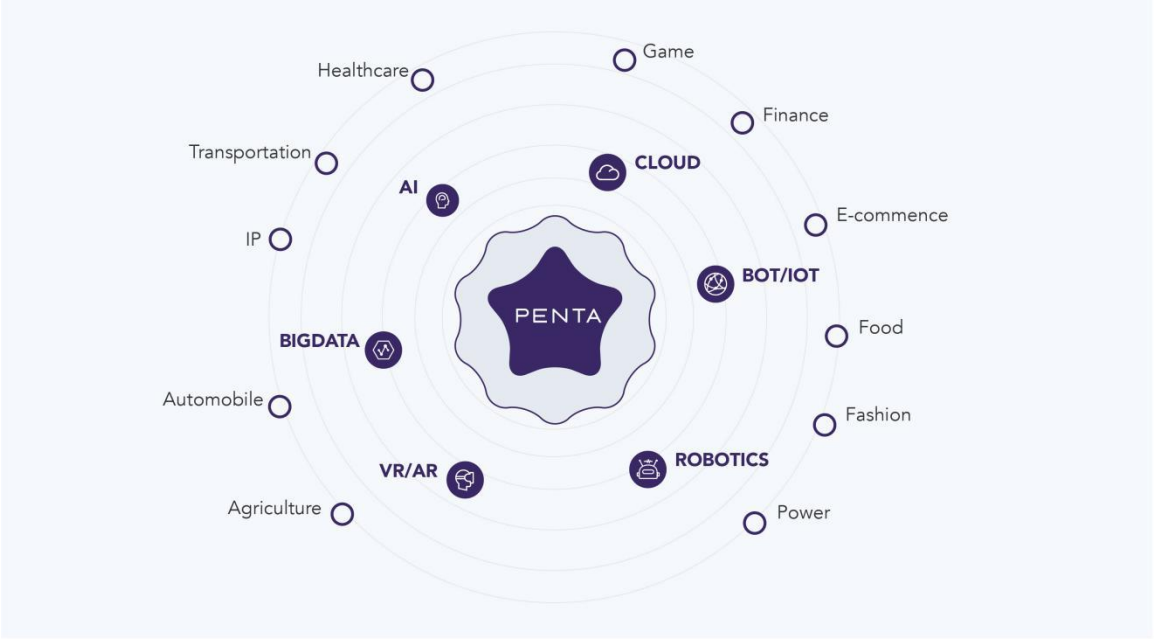


표 12. PENTA 의 응용 네트워크

5.1 사회

5.1.1 의료/건강

헬스 케어 산업에서 큰 변화를 일으키고 있다: 의약품, 설비, 서비스, 비즈니스 모델등의 다지털화를 통해 의료 시스템을 보급하고 새로운 가치도 생긴다. 대다수 나라에서는 디지털 헬스 케어를 목표로 한 정책을 출범하고 전자 건강 기록이나 전자 진료 기록등 디지털 건강 정보를 보완하고 다른 건강 진료 시스템이나 설비도 부단히 갱신하다.

보안성, 완전성, 퍼스널라이즈 헬스 데이터에 대한 접근 권한에 관한 제한은 헬스 케어 이노제이션을 실현하는 열쇠 되었다. 헬스 케어 업계에서는 리스크와 보상의 균형을 잡기가 힘든데 블록 체인 기술의 운용은 이런 긴박 소구를 완화하는 해법을 제공하였고 아래에서 언급할 여러 처원에서 의료 업계에 도움도 될 것이다.

1) 데이터 보안

기존의 보안 체계와 달리, 블록 체인은 내장된 안호 기술을 이용하고 분산식 네트워크에서 운행하여 기술 차원의 데이터 변경 불가함을 보증할 수 있다. 그리하여 의료 체계, 의료 설비 업체와 의료 기술 기업은 블록 체인 기술을 활용하여 설비 관리 기능을 강화하여 환자의 건강 데이터에 선택적인 접근을 제공한다.

2) 헬스 케어 데이터 교환

헬스 케어 데이터 공유는 정보 교환 뿐만 아니라 2 개 혹은 2 개 이상의 체계 또는 주체 간의 상호 신뢰에 근거하는 책임 정보의 사용이다. PENTA

는 변경 불가하고 신뢰할 만한 워크 플로우를 제공하여 헬스 케어 데이터의 교환 과정에서 "단일적인 데이터 소스"를 형성하고 체계와 모델의 완정성을 보증하게 된다.

3) 의약품의 안전성

블록 체인 기술을 기초한 분산식 의료 시스템을 채택하여 약품 위조 방지의 강화와 약값의 공표등이다.

4) 정밀한 치료

제약 기업은 그의 의약품 가치를 증명하는데 갈수록 높아진 스트레스를 직면하고 있다. 왜냐하면, 업계의 예측에 따르면 매년 약 3000 억 달러의 약품이 예상된 효과를 달성하지 못하니 결국 낭비가 되었고 환자에게도 해로운 부작용에 시달리고 있다. 그래서 제약 업체는 환자 위주의 약품 개발 패로다임(paradigm)으로 이행해야 미래의 표적 치료를 실현할 수 있다. 정밀 의학 개념은 헬스 케어 분야의 패러다임 변화를 예고하였다.

블록 체인 기술은 그의 완비한 보안 인프라에 의한 연속적인 데이터 교환으로 보다 규모가 더 큰 유전자 연구를 촉진하여 정밀 의료의 발전도 촉진하였다. 의약품 개발 업계가 정밀 의학에서의 계속 투자를 하면서 불록체인에 기초한 변경 불가한 기록은 임상 시험 데이터 수정로 인한 부담과 코스트 배제할 가능성이 있을 거고 연구 성과의 공유도 촉진할 것이다.

미래에 PENTA는 헬스 케어 업계의 융합과 비즈니스 프로모션을 통해 의료 체계의 운행와 관리의 효율을 높일 거고 믿음직한 투명、안전한 의료 제도를 구축한다.

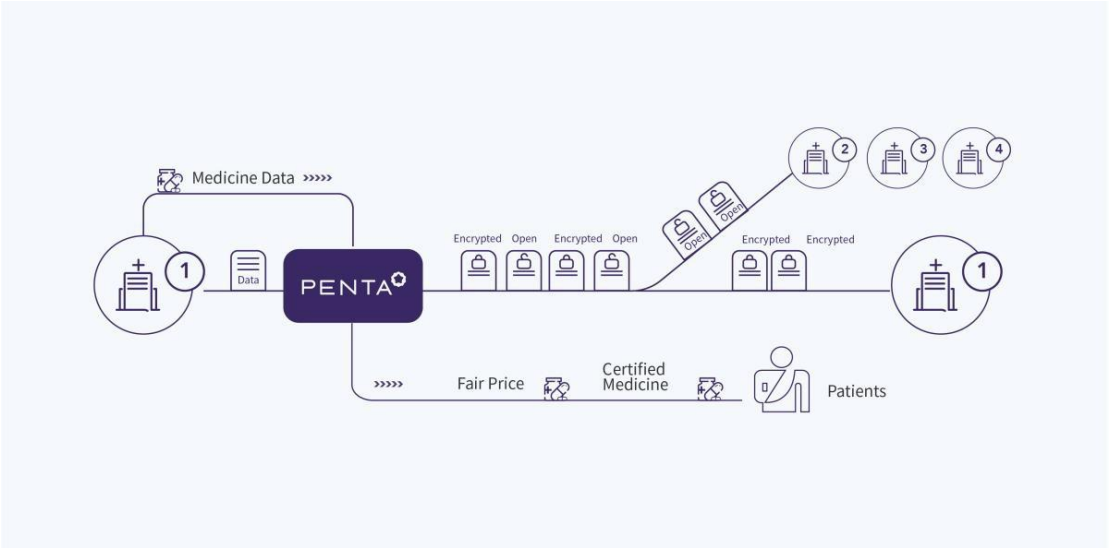


표 13. PENTA 블록 체인의 약품 적용 체계

5.1.2 에너지

전통적인 에너지 부족과 환경 오염은 세계적인 과제가 되었고 , 인간은 재생 가능한 에너지 자원(풍력.태양 에너지등)을 이용하는 기술이 선숙해지고 있으나 널리 사용되는 정도 아니다. 어떤 설문에 따르면 발전 총량에서 차지하는 비율은 풍력 발전이 4%를 불과하고 태양 에너지가 1%만 차지하고 있다.

본질적으로 보면 전통적인 대규모 정력망(국가 전망, 중국 남방 전망등)은 집중형의 비즈니스 모델로 인하여 송배전의 상황이 복잡하고 설비도 많아 전력 조달과 컨트롤이 어려워 대규모 이용하는데 기술적인 지장와 산업적인 이익 충돌도 있다.

인터넷 통신 및 정보 처리 기술의 신속한 발전에 따라 미국 학자 제레미·리프킨은 <제 3 차 산업 혁명>에서 "에너지 인터넷"의 개념을 발표하였다. 그 후에 이 개념이 급속히 퍼져 왔다. 2016 년 중국 국가 전망 본사는 "도

시 에너지 인터넷 발전 화이트 페이퍼(2016)"를 발표했다. 전력 위주의 도시 에너지 UEI(Urban Energy Internet)를 구축하는 것을 처음으로 제안했고 도시는 하나의 자치체로서 에너지의 효율적인 구성을 달성하여 도시 에너지의 청결화, 전기화, 스마트화를 추진하다.

새로운 추세와 형세하에, 분산식 에너지의 수용, 거래,사용에 대해 우리는 미니 전력망의 관점에서 다시 사고하고 디자인해야 하며 전통적 대규모 전력망의 틀안에서 전체적으로 계획하지는 않다. "만능 인터넷, 다능 인터랙티브, 다능 접속, 다능 거래, 다능 대응"할 수 있는 에너지 인터넷 CEI(Community Energy Internet)이 형성하고 나서 CEI에 의해 UEI를 조합하고 전망와 인터랙티브하고 에너지 인터넷의 생태를 형성하다. 물건의 인터넷 분야에서의 돌파 뿐만 아니라 정보 플랫폼과 비즈니스 모델의 변경에 혁신할 필요도 있다. 중용한 돌파구 중의 하나응 분산식 전력 플랫폼 SPX(Smart Energy Exchange)의 설립에서 물리 영역의 범위 내의 에너지 공급과 소비자 간의 독립하고 투명한 거래와 정보 공유를 추진하고, Win-Win의 인센티브 매커니즘을 설정함으로써 에너지의 전달과 이용 효율을 개선하다.

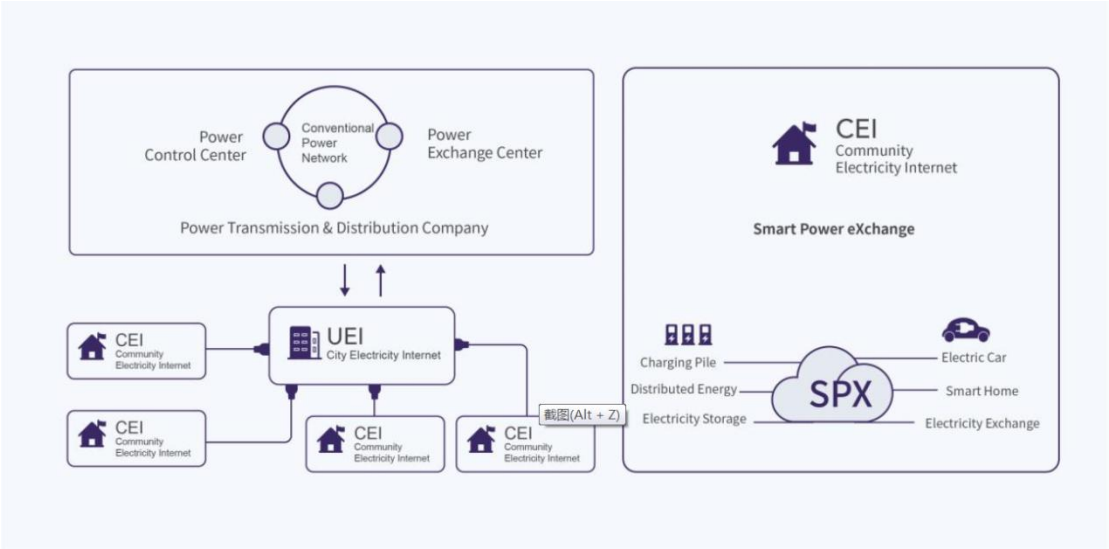


표 14. SPX 를 핵심으로 한 에너지 커뮤니티 네트워크

PENTA 에 기초한 분산식 전력 거래 플랫폼 SPX(Smart Energy Exchange)은 정보 플랫폼의 확립과 비즈니스 모델의 재구축을 통해서 한정 범위의 가상화 커뮤니티 에너지 인터넷을 구축하고자 한다. 그 애플리케이션 프레임워크는 이용 가능한 자원의 발표, 에너지의 발견과 수요의 발표, 스마트 매칭, 주문의 실행, 스마트 미터와 미터 링의 데이터 전송, e 지갑, 주문 결재 등의 기능이 포함되다.

5.1.3 물건의 인터넷

물건의 인터넷 기술, 스마트 하드웨어와 블록 체인 기술의 발전에 따른 IOT (Internet of Things) 시대는 반드시 BOT(Blockchain of Things)의 시대으로 발전한다. PENTA 는 최종적으로 사물의 자치(Things Autonomy), 가치 전송(VALUE TRANSFER), 인공 지능(AI)와 로봇(Robotics)기술의 융합등을 실현한 BOT 시대으로 발전하는 데 노력하고 있다.

표 15. PENTA 네트워크의 BOT 체계

BOT 분산형 충전소(DCP)의 응용 장면에 대해 예로 들면, 전기 자동차의 저탄소 특성 때문에, 정부 주도하의 세계적인 "탈 가솔린 차"의 파도가 형성되었다. 어느 보도에 따르면 독일은 2030 년에 휘발유와 디젤 차량의 생산을 정지할 예정이고 영국은 2040 년에 가솔린 차를 금지하는 것도 검토하는 중이다. 전동 자동차의 발전은 이미 저항할 수 없는 역사적인 경향이 되었지만 마케팅에 영향을 끼치는 요인 중 하나는 충전의 편리성이다. 언론의 조사에 따르면" 모 도시 중심부의 42 개 공공 충전 스폿에 관한 현지 조사를 보면 340 개 충전소 중에서 충전 사용중인 61 개로 17.9%를 차지하고 손상 및 기능 부전 상태인 35 개로 10.2%를 차지하며 휘발유 차량한테 무단 차지하는 게 92 개로 27%를 차지했다. 왜냐하면 이들 시설이 전력 회사, 전동 자동차 회사, 충전 스폿 운영 회사에 의해 집중 투자, 건설, 운영되는 거니 비즈니스 모티베이션 공통성과 지속적인 발전에는 단점도 적지

않고 전동 자동차 충전소에 대한 커다란 필요에도 미치지 못하였다.

충전난의 주된 이유는 충전 스폿(빠른 충전과 슬로우 충전)에 지나치게 의존하기 때문이다. 이 외에도 개인적으로 투자되는 대량의 충전 시설을 외부 사용자 한테 공유할 수 없는 것이며 다른 잠재적인 전력 공급 업체(커뮤니티 편의점이나 주차장 등)도 충전 서비스를 제공하지 못하고, 다시 말하면, 수요와 공급간의 매칭, 측정 및 결제를 포함한 효율적인 전력 거래 방식이 없는 것은 그의 근본적인 문제이다.

PENTA 를 통해서 SPX 플랫폼을 구축하여 잠재적인 전력 공급 업체로(개인 충전소 주차장, 편의점 등)스마트 미터, 스마트 퍼스트 차지, 슬로 충전 설비를 제공하고 충전 서비스를 제공하는 것을 가능하게 한다. SPX 플랫폼에서 이용 가능한 자원을 발표함으로써 유저는 각 루트(전기 자동차 회사 APP 와 SPX APP 포함)를 통해서 충전 스폿 찾아 충전하여 전기의 효율적인 전송과 이용을 크게 촉진할 수 있다.

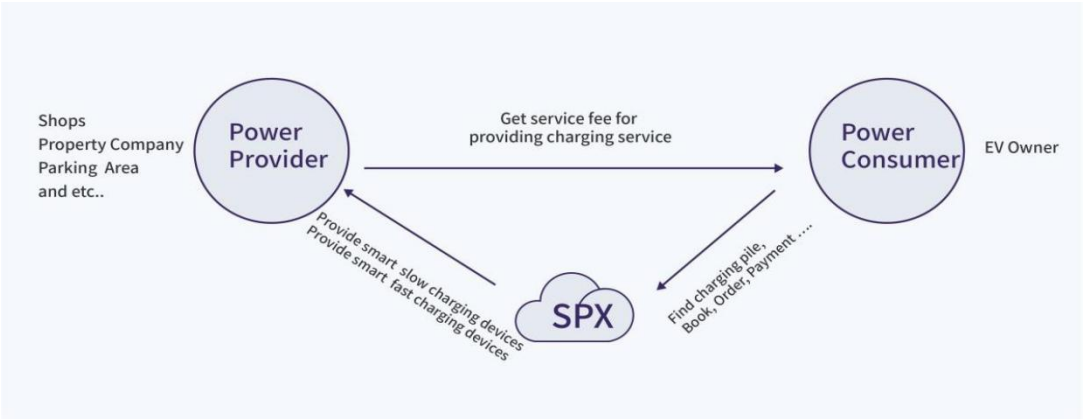


표 16. SPX 를 중심으로 한 공유 충전 모드

수요 측의 응답(DemandResponse, DR)은 상금 인센티브에의 형식으로 유저 원래의 전력 소비 모드를 변경하여 절정기 전력 부담을 감소 또는 이동시켜 전력 공급 체계의 안정성을 확보하는 것을 말합니다.

지금 전력망의 집중 관리하에 수요 응답은 이에 관여하는 조직이나 개인은 사전에 신청하고, 전력 감시 장치를 미리 설치해야 하고 전력 수요 응답 프로토콜도 미리 체결해야 하기 때문에 그 결과 복잡한 절차와 높은 리퀘스트로 수많은 소규모 사용자의 참여가 어려워져서 스케일 효과나 수요 응답의 실제 효과가 나타나기는 어렵다.

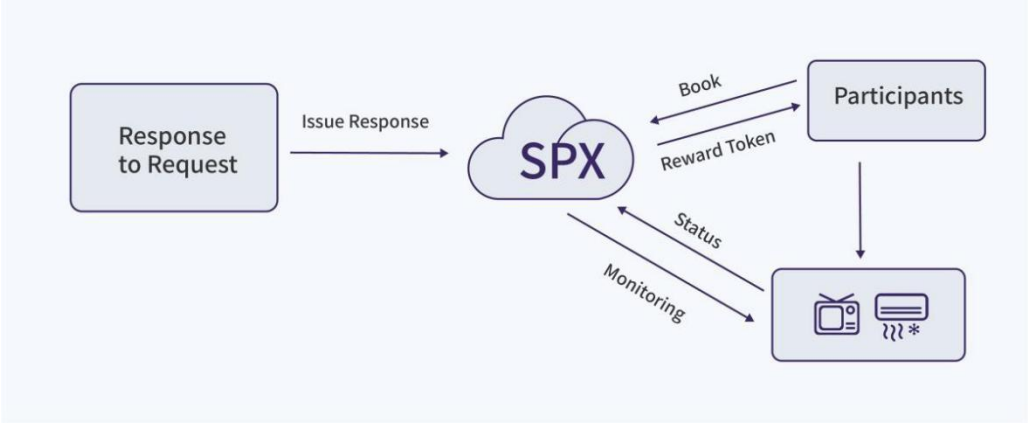


표 17. SPX 를 중심으로 한 수요 응답

분산식 전력 거래 센터 SPX 는 수요 측의 대응에 대해서 부하 인테그 레이터의 역할과 기능을 담당할 수 있다. 전력 회사로부터의 수요 응답 프로토콜과 이벤트를 취득하고 SPX 에서 스마트 콘트랙트를 설정하고 발표하여 CEI 의 서브 젝트에 주문을 로드하거나 예약하거나 한다. 이 프로세스를 통해서 SPX 는 전력 회사로부터 수요 응답의 총량을 얻고 작업 분해와 실행 주체의 분산화를 실현하고 더 많은 소규모 유저 수요 응답 과정에 참여하고 롱 테일 효과를 볼 수 있도록 하다. 또 스마트 콘트랙트 중에는 관용 기능의 함수가 설정되어 있기 때문에 소수의 위약 행위가 전체의 수요 응답의 적시성과 정밀도에는 영향을 주지 않을 것이다. 수요 응답의 실행 중에 SPX 는 미리 제공되는 무료 인텔리전트 단말기에 의해서 수요 응답 상

황을 감시하거나 신용 평가를 근거하여 인텔리전트 단말기를 설치하지 않는 경우에서도 참가자에 의한 트러스트를 바탕으로 한 적극적인 응답도 실현할 수 있다. SPX 는 부하 적분기로서 전력 회사로부터 수요 응답으로 얻은 보수를 참가자에게 토큰 형식으로 실시간 전달한다.

5.2 경제

블록체인은 차세대 기술로서 신속한 발전 속도로 보이고 있다. 금융 분야에서 신기술의 도입은 상대적 늦어지는 것이 보통 상환이지만 블록체인들의 구성원을 살펴보면 금융 분야 업체들이 제일 많고 그만큼 참여도 가장 적극적인 것으로 알 수 있다. 블록체인과 금융 분야 간에 근본적 적합성 때문에 금융 분야에서 실행 가능한 상황이 비교적 풍부하다. 예를 들면 아래와 같다.

- 자산거래 면에서 동분야 자산거래, 비즈니스 어음, 공급사슬, ABS 자산증권화 등 업무에서 활용 본격 추진.
- 지불과 결산 면에서 은행간의 결산, 국제 지불 , 포인트 적립 등 업무에서 활용 가능.
- 신용 대부 면에서 신용 등급 조회, 담보 대출, 전당 대출, 일반 대출, 공급체인대출 등 업무에서 활용 진행.
- 기타 면에서 P2P、크라우드 펀딩와 관련된 분야에서 블록체인 활용 가능.

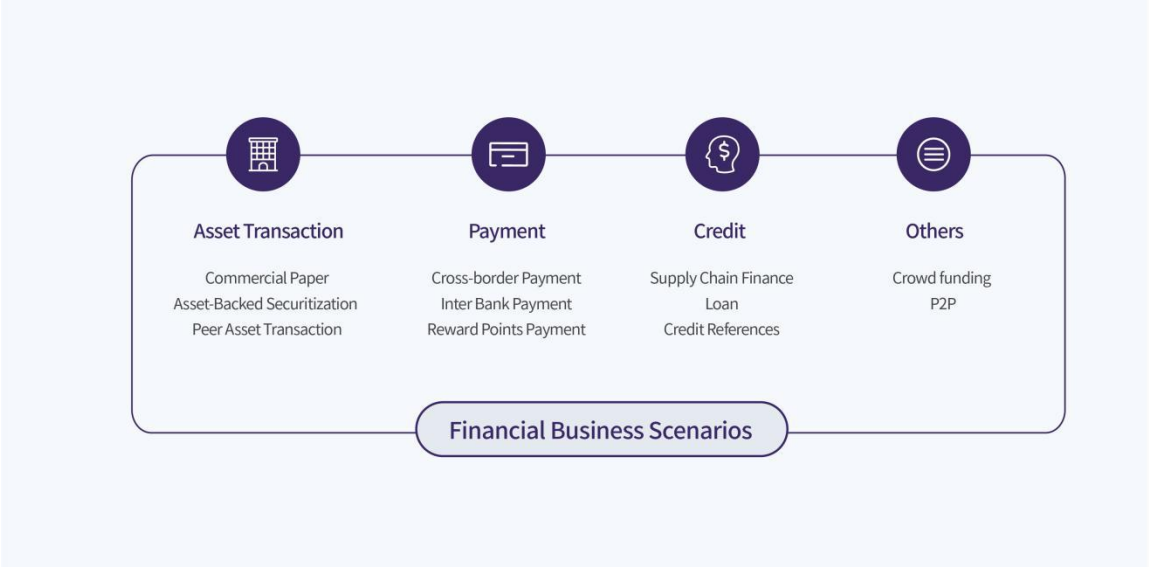


그림 17 금융상황

PENTA 네트워크는 금융 분야에서 블록체인을 활용하는 데 풍부한 경험을 쌓았고 특히 신용 등급 조회, 포인트 적립, 자산 증권화, 공급체인금융 등 업무에서 구체적인 실행 경험도 가지고 있다.

5.2.1 신용 등급 조회

근년에 들어 전세계적으로 대출 규모와 대출 인구의 상승에 따라 신용조회에 대한 수요도 그만큼 증가되어 있다. 이와 동시에 신용기술의 발전과 대중적 지지에 의해 중국 신용조회의 성장에 대한 필수적 조건이 마련되었다.

지금 중국 신용 등급 조회 시장에서 다음과 같이 몇 가지 문제가 존재한다.

1) 지금 중국중앙은행 신용 등급 조회의 문턱 값이 비교적 높은 편이다. 조회 대상은 주로 은행과 그들의 고객층만에 한하여 가능한데 소액대출업체나 금융리스업

체와 같은 경우 신용 등급 데이터를 공유하지 못한다.

2) 신용 등급 조회 업체들 간에 데어터 공유가 부족해서 업체와 유저들 간에 정보 비대칭성이 심각해 보인다.

3) 정규적 시장화 데이터 수집 방법이 한계가 있으므로 데이터 소스에 대한 경쟁이 엄청한 비용 부담이 되었다.

4) 전통적 기술 프레임워크가 새로운 요구를 만족하지 못하기에 데이터 안보 문제도 두드러진다.

블록체인은 탈중심화, 탈신뢰, 타임스탬프, 비대칭암호화, 그리고 스마트 계약 등 특성을 지니고 있으며 데이터 안전의 유효적인 보장에 통제 가능한 신용 데이터 공유 및 검증을 기술적으로 실행할 수 있다. 지금 신용 등급 조회 시장의 실정을 감안하여 블록체인은 데이터 공유 거래 분야에 집중하여 블록체인을 기반으로 한 신용등급조회 플랫폼을 구축함으로써 리스크를 낮추고 비용부담을 덜어주면서 데이터 전달, 검색, 결산을 가속화는 가능하다.

PENTA 가 블록체인을 기반으로 개발된 신용 등급 조회 플랫폼에서는 연결된 노드들이 신용 등급 조회 업체, 개인 유저, 기타 업체(소액대출업체, 은행, 보험업체, 정부기관 등 포함) 가 포함되어 있으며, 대출 업체와 신용 등급 조회 업체, 그리고 신용 등급 조회 업체 간의 정보 공유를 실현 가능하다.

신용 등급 정보 남용을 막기 위해 PENTA 는 블록체인의 스마트 계약을 도입하여 신용 등급 조회 수권 기제를 구축하였으며 블록체인의 추적 특성을 이용하여 권한 수여를 기록 및 검색 가능하다. 또 블록체인은 비가역성

때문에 대출업체들의 불당한 등급 조희 행위를 주도면밀하게 방비할 수 있다. 그 외에는 블록체인에서 기록된 민감한 정보는 이미 암호화된 상태라 관한을 허용해야만 조희 가능하다.

이 플랫폼은 출시 이후, 소액 대출 업체들이 이미 가입되어 있으며, 대출 데이터, 담보물 정보, 블랙리스트, 기타 규체기관 및 제 3 자 업체들이 제공한 데어터 전송 및 검색을 지원하고 있다. 그 밖에도 PENTA 네트워크는 포인트 적립 및 소비 메커니즘을 구축함으로써 연결된 업체들이 더욱 많은 정보를 공유하기를 장려한다.

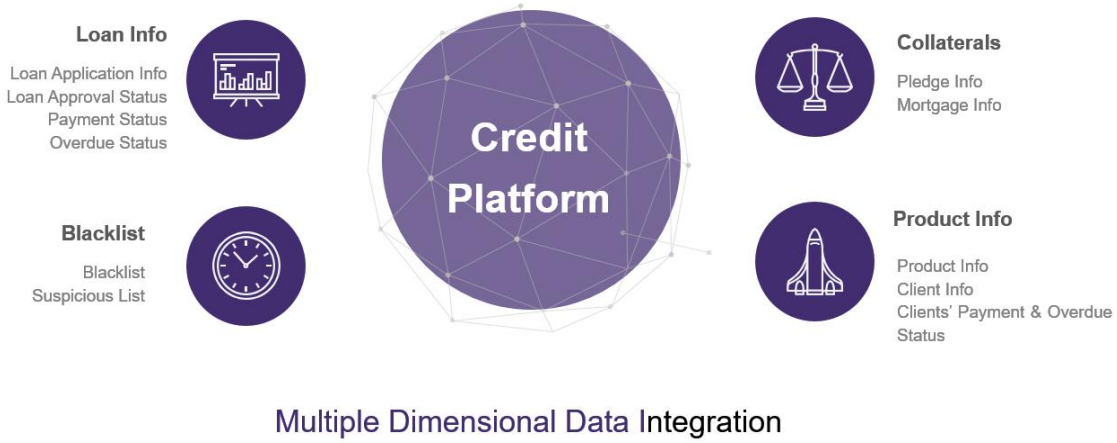


그림 18. PENTA 네트워크 블록 체인 신용 등급 조회 플랫폼

플랫폼 출시 이후 연결된 업체들과 노드는 끊임없이 늘어나고 있으며 전체적으로 잘 운영되고 있다. 블록체인을 기반으로 한 신용등급조회 플랫폼의 거래블록 감시제어 예시도는 다음과 같다.

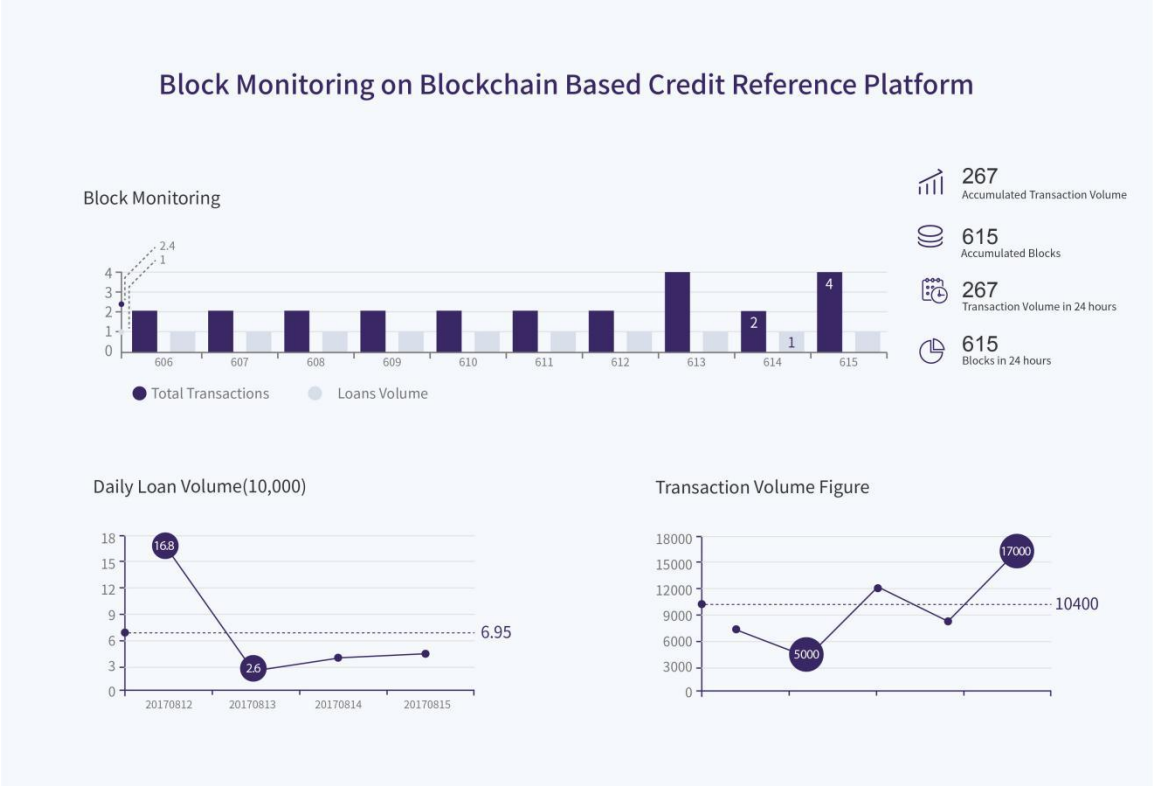


그림 19 블록체인 신용등급조회 플랫폼의 거래블록 감시제어 예시도

5.2.2 공급 체인 금융

경제 성장와 산업화 발전에 따라 각 나라의 기업들의 수취채권도 점차 늘어가고 있다. 만약 그들의 수취채권을 가지고 잠재적인 대출 담보물로 충분이 활용할 수 있다면 앞으로 공급 체인 금융시장의 잠재력이 얼마나 높은지 짐작할 수 있다.

PENTA 네트워크는 수많은 은행, 재무회사 등 금융 업체들에 공급 체인 금융 솔루션을 제공한 바 있다. PENTA 는 서비스를 제공하면서 공급 체인 금융 업무의 복작성을 충분이 느끼게 된다. 그 중에서 다수 공급자 계약, 거래, 증명 서류 등 번거로운 검증 절차 때문에 진행 과정이 장황하고 저효율적이다. 이것은 공급체인금융의 참여자가 많아 정도 인터랙션와 신뢰를 달성하기 어렵기 때문이다. 일반적 오더파이넌스를 예로 들면 그중에서

구입자, 판매자, 구입자 계죄 개설 은행, 판매자 계죄 개설 은행, 유통차, 감독기관, 세관(국가간 오더파이넌스의 경우) 등 수많은 업체들과 연관되어 있다.

그리고 공급체인금용와 관련된 서비스도 생산기획에서 화물접수, 수도결제까지 거래 과정 각 단계를 관통하고, 서비스 종류도 오더피이넌스부터 유동자금 대출, 자금결제까지 등 다양한 것이다.

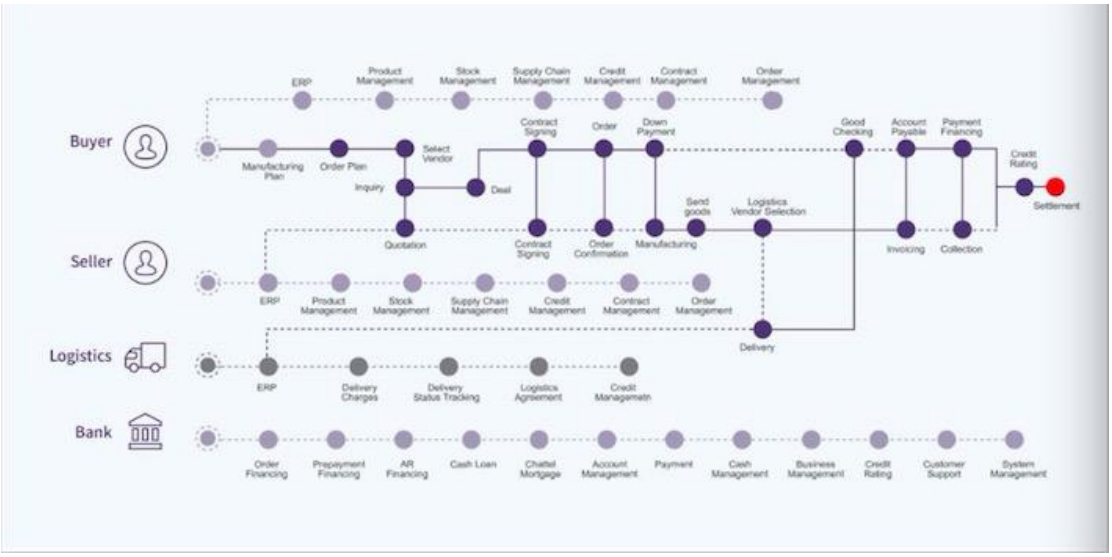


그림 20 공급 체인 금용

블록체인 기술이 공급 체인 금용 업무와의 결합을 통해 오더, 신용장, 인수증, 무역 절차 등 파일을 블록체인에다가 기록하여 블록체인을 통해 인증과 변경 불가에 대해 검증을 실행한다. 이와 동시에 블록체인의 디지털 솔루션은 종이 파일에 의해 진행된 인공적 진행 대체, 단 대 단의 완전적 공개화, 저위험과 고효율을 실행 가능하다.

PENTA 네트워크는 모 금요업체를 위해 공급체인 오더파이넌스 플렛폼을 구축하였다. 그중에 업무 상황와 블록체인 기록 처리 로직은 다음과 같다.

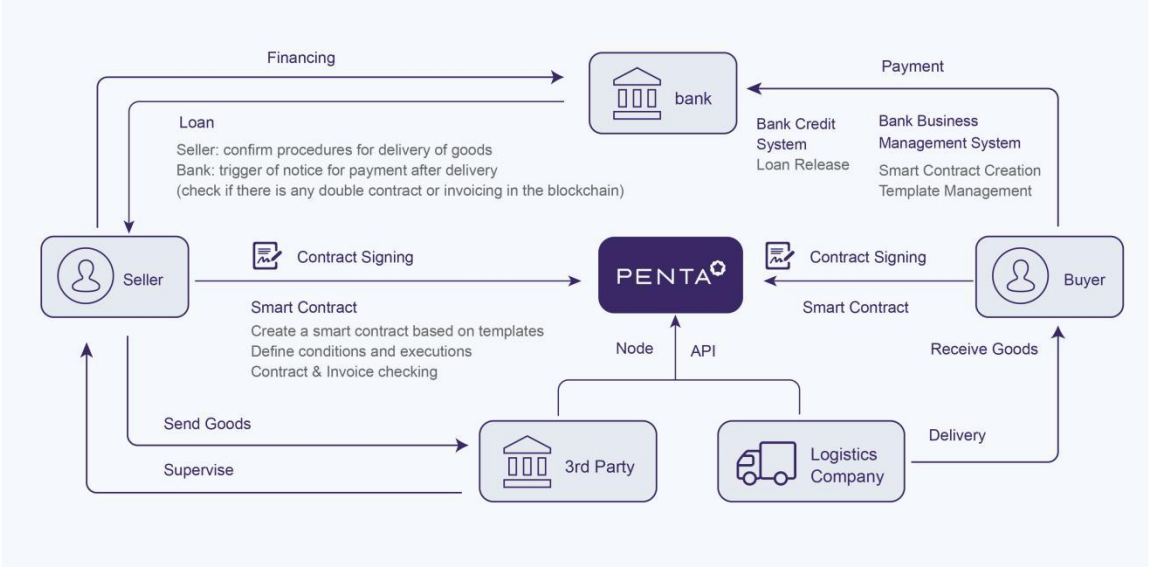


그림 21 오더 파이넌스 상황

위와 같은 상황에서 참여자들은 매매쌍방, 양측 계좌 개설 은행, 유토사, 제 3 방 감독기관 등이 포함되어 있다. 구체적 절차는 다음과 같다.

1) 오더파이넌스상황 계약 체결 때 계약 조항은 스마트 계약에 기록한다.

2) 금융기구는 계약과 화물 출하 상황에 따라 차별화하게 신용공여와 대출을 진행한다.

3) 구매자는 오더에 따라 파이넌스를 진행되 시간이되면 스마트계약은 자동적으로 지불 진행한다.

4) 거래 과정에서 유통사와 감독업체도 업무 처리 상황을 수시로 블록체인에서 업데이트한다.

5.2.3 자산의 증권화

자산의 증권화 과정은 절차가 번거롭고 참여자도 많기 때문에 전문적인 SPV(특별자금관리사)를 설치하여 주체적인 리스크를 면하도록 한다. 일번적인 자산 증권화 거래 구조가 다음과 같다.

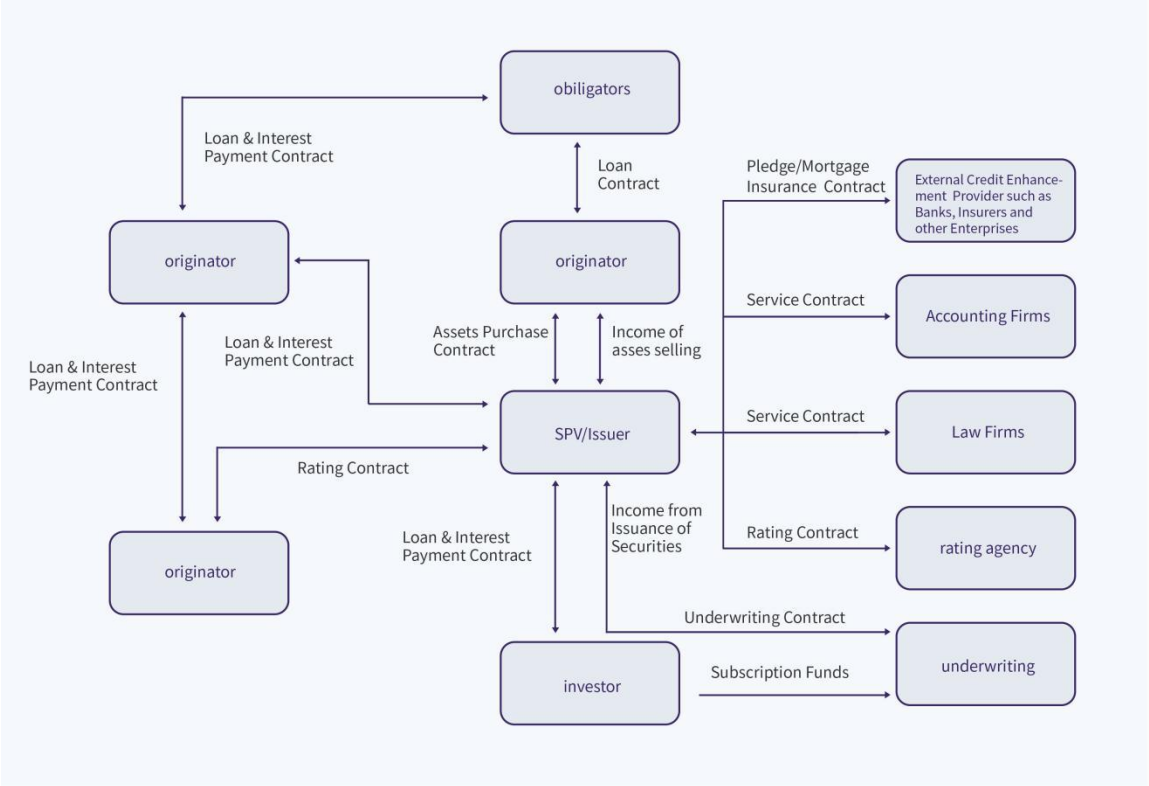


그림 24. 기본적 거래 구조 예시

위와 같은 상황에서 SPV(Special Purpose Vehicle)、발기인, 원채무인, 투자자, 공탁자, 서비스 제공 업체, 회계사무소, 로펌, 신용등급평가기구, 증권 발행 대행상 등 수많은 관계자들이 연결되어 있기 때문에 상호간의 정보 인터랙션의 비용 부담이 비교적 높고 정보 검증도 더 오래 시간이 소모될 것이다. 블록 체인에서는 B 단의 모든 업체들와 C 단의 투자자를 연결시키고, 자산패킷 (asset package) 의 신뢰성을 보장하며, 각 참여자들의 주체적 자산 분배 상황을 검색 가능하고, 또 3 자간의 등급 평가 결과의 공개성도 보장할 수 있다. 체인에서 연결된 데이터에 대한 믿음을 보증하면 업체들 간의 인터랙션와 검증 부담을 유효적으로 덜어주기도 하고, 더욱 유력한 투자자들이 정확한 정보를 참고하여 벤처 투자할 때 적절한 결정을 내릴 것이다.

위의 목적을 이루기 위해 PENTA 네트워크는 블록체인을 기반으로 한 스

마트 자산 증권화 플랫폼을 구축한 바 있다. 블록체인을 이용함으로써 기본 자산을 관리하여 매번의 자산 평가, 회계 감사, 거래 내역 등 정보를 블록체인에서 기록한다. 이처럼 사산 정보의 투명성은 자산 증권화 업무이 순조롭게 발전하고 감독 부담을 덜어주는 데 유리하다.

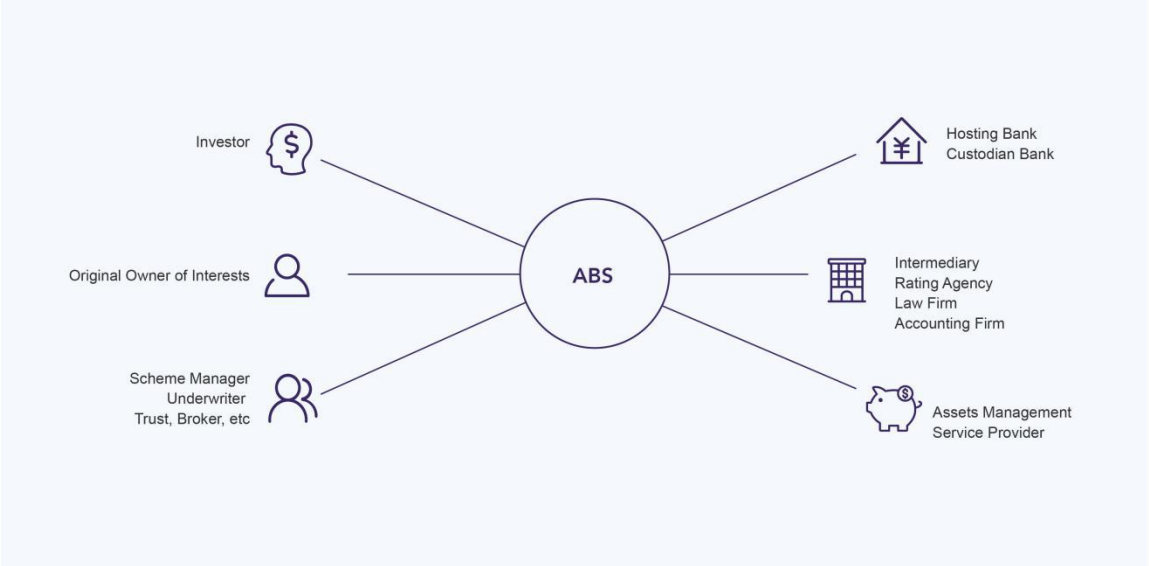


그림 25. 자산증권화 스마트 클라우드 플랫폼 예시

블록체인을 기반으로 한 스마트 자산증권화 플랫폼은 모든 참여자들이 관리하고 실행하는 것을 지원한다. 데이터 신뢰성을 높이도록 각 업체들이 자신만의 데이터 기록 노드를 만들 수 있다.

6. 전문 용어

1) 비트코인(BitCoin): 비크코인은 2009 년에 사토시 나카모토(Satoshi Nakamoto)라는 필명의 프로그래머는 오픈 소스 소프트웨어의 형식으로 발표한 암호화 가상 통화이다.
2) 이더리움(Ethereum): 스마트 계약을 제공하는 퍼블릭 블록체인 플랫폼이다.

3) 하이퍼레져 패브릭(Hyperledger Fabric): IBM 이 연맹 체인들을 위한 오픈 소스 기반의 서브 프로젝트이다.

4) 이더리움 가상머신: 이더리움 가상머신이란 P2P 네트워크의 모든 노드들이 공유하는 가상머신이다. 블록체인에서 진행 가능한 코드와 데이터를 읽고 쓸 수 있을 뿐더러 데이터 서명 검증도 가능하고 완전하지 못한 언어로 code 를 실행 가능하다. 또 이더리움 가상머신은 서명 완성된 메시지를 받아야만 코드 실행이 가능하다. 그리고 블록체인에 저장된 정보는 적당한 행위를 구분할 수 있다.

5) 튜링 완전한 언어: 튜링 컴퓨팅 가능한 함수를 컴퓨팅할 수 있는 모든 컴퓨터 시스템은 튜링 완전 기계라고 부른다. 튜링 완전한 프로그래밍 언어라면 튜링 기계(Universal Turing Machine)와 동일한 컴퓨팅 능력을 가진다는 의미이다. 그것도 현대 프로그래맹 언어가 가질수 있는 최고의 능력이라고 할 수 있다.

6)스마트 계약: 스마트 계약이란 time-driven 방식을 채택하고 상태가 있으며 공유 원장에세 운행 가능하고 또 원장 재산을 저장할 수 있는 프로그램이다.

7) 기호화폐 : 비트코인 제외된 기타 가상 화폐이다.

8) 퍼블릭 블록체인: 퍼블릭 블록체인이란 어느 누구도 어디서도 거래 가능하고 또 유효적 확인을 얻을 수 있으며, 모든 사람들이 합의 참여 가능한 블록체인이다.

9) 연맹체인: 개방도와 탈중심화 정도는 퍼블릭 블록체인보다 제한이 받았지만 참여자들 간에 이미 합의가 이루어졌고 서로간의 신뢰감을 형성

된 체인이다

10) POW(Proof of Work 작업증명): 작업증명이란 일한 채굴자의 노력 정도에 따라 코인을 주는 방식이다. 비트코인이나 라이트코인과 같은 대부분의 가상 화폐는 POW 방식을 채택한 것이다.(연산략이 높으면 높을수록, 채굴 시간이 많으면 많을수록 모아진 코인도 그만큼 많아진다.)

11) POS(Proof of Stake 지분증명): 참여자의 소지 금액과 보유시간(coinage)에 따라 이자를 주는 방식이다. POS 의 방식을 책용할 경우, 코인 하나가 하루에 1 coinage 증가된다. 예를 들면, 100 개 코인을 30 일 정도 보유하면 총 coinage 는 3000 이다. POS 블록을 발견하자 보유자의 보유신간을 초기화한다.

12) PBFT(Practical Byzantine Fault Tolerance 실용 비잔틴 장애 허용): 1999 년에 Miguel Castro 와 Barbara Liskov 가 공통 제기한 PBFT 알고리즘은 초기 비잔틴 장애 허용 알고리즘의 저효율 문제를 해결하여 지수급 컴퓨팅 복잡도를 다항식급으로 낮추게 함으로써 이 알고리즘이 실제 시스템에서도 적용이 가능케 한다.

13) QOS (Quality of Service 서비스 품질): 서비스 품질이란 네트워크에서 각종 기초 기술을 실행할 수 있고 지정된 네트워크의 통신에 대해 더욱 좋은 서비스를 제공 가능한 능력이다. 그리고 QOS 는 또한 보안 메커니즘으로서 네트워크에서 지연이나 혼잡 문제 등을 해결하는 기술이다.

14) RSA: 1977 년 론 리베스트(Ron Rivest)와 아디 셰미르(Adi Shamir), 레오

나르드 아델만(Leonard Adleman) 등 3 명의 수학자에 의해 개발된 국제 통용 알고리즘이다. RSA 는 키 하나만 이용하는 대칭암호로서 치환이나 대체가 아닌 수학 함수를 기반으로 한다. 비대칭 암호로서 RSA 는 공개 키와 개인 키를 독립적으로 사용하기 때문에 키 쌍 체계라고 할 수도 있다. 그증에서 공개 키는 공개 가능하기 때문에 공개 키 알고리즘이라고도 한다.

15) 국가 암호화 알고리즘: 중국국가암호국에서 인증 받는 중국산 암호화 알고리즘으로서 주로 SM1 , SM2 , SM3 , SM4 등이 포험되어 있다. SM1 는 대칭 암호 알고리즘이다. 암호화 강도는 AES 에 해당된다. SM1 는 공개되지 않기 때문에 클리퍼 칩의 인터페이스를 통해 호출 가능하다. SM2 는 이미 공개된 비대칭 암호 알고리즘이다. ECC 를 기반으로 개발되어 있기 때문에 서명 속도와 암호키 생성 속도는 RSA 보다 빠른 편이다. ECC 256 비트(SM2 가 기반으로 한 알고리즘은 바로 ECC 256 비트 중의 하나이다) 의 안전강도는 RSA 2048 보다 높을 뿐더러 속도도 RSA 보다 빠르다. SM3: 검증결과는 256 비트로, 이미 공개된 암호컴퓨팅법이다, MD5 를 참조해서 이해하면 된다. SM4: 무선 랜 표준의 블록 데이터 알고리즘이다. 대칭 암호화 알고리즘으로서 키 길이와 블록 길이는 똑같이 128 비트가 된다.

16) 부하 균형(Load Balance): 기존 네트워크에서 구축되어 있고, 저렴하고 공개된 방법으로 네트워크 설비와 서버의 대역폭 확장, 데이터 스루풋 증가, 데이터 처리 능력 강화, 네트워크의 유연성 강화 등의 기능을 동시에 갖추고 있는 것이다.

17) P2P(peer- to – peer): 인터넷에서 개인과 개인 간에 업무와 적업량을 분배하는 분사식 응용 프레임워크임으로서 P2P 컴퓨팅 모델이 응용 레이어에서 형성된 네트워킹이나 네트튀크이다. 'Peer'이라는 단어는 영어에서 '대등자, 또래, 개인' 이라는 의의를 가지고 있기 때문에 표면적으로 대등 컴퓨팅이나 대등 네트워크라고 이해해도 된다.

7. 참고 문헌

[1]G. Ateniese, R.Burns, R.Curtmola, J.Herring, O.Khan, L.Kissner, Z. Peterson, and D.Song. Remote data checking using provable data possession. ACM Trans. Info. & System Security, 14(1), May 2011.

[2]M.T.Goodrich, M.Mitzenmacher, O.Ohrimenko,and R.Tamassia.Privacy- preserving group data access via stateless oblivious RAM simulation. In SODA, 2012.

[3]H.Shacham and B.Waters. Compact proofs of retrievability. Proc. Asiacrypt 2008.

[4]C.Huang, H.Simitci, Y.Xu, A.Ogus, B.Calder, P.Gopalan, J. Li, and S. Yekhanin. Erasure coding in Windows Azure storage. In G. Heiser and W. Hsieh, editors, Proceedings of USENIX ATC 2012. USENIX, June 2012.

[5]L.Rizzo. Effective erasure codes for reliable computer communication protocols. ACM SIGCOMM Computer Communication Rev., 27(2):24–36, Apr. 1997.

[6]M.Liskov, R.Rivest, and D. Wagner. Tweakable block ciphers. J. Cryptology, 24(3):588–613, July 2011.

[7]V. Buterin. Ethereum, Apr. 2014.

[8]V.T.Hoang, B.Morris, and P.Rogaway. An enciphering scheme based on a card shuffle. In R.Safavi-Naini, editor, Proceedings of Crypto 2012, LNCS. Springer-Verlag, Aug. 2012. To appear.

[9]Nakamoto, S.31 October 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System". Also known as the Bitcoin whitepaper.

[10]Kyle Randolph. "A Next-Generation Smart Contract and Decentralized Application Platform". Also known as the Ethereum whitepaper.

[11]Christopher Ferris. "Hyperledger fabric Protocol Specification".

[12]Miguel Castro, Barbara Liskov. "Practical Byzantine fault tolerance and proactive recovery".

[13]Hal, F. "Reusable proofs of work" http://www.finney.org/~hal/rpow/.

[14]Tushar Deepak Chandra, Vassos Hadzilacos, Sam Toueg. "The Weakest Failure Detector for Solving Consensus".

[15]Manos Kapritsos, Yang Wang, Vivien Quéma, Allen Clement, Lorenzo Alvisi, Mike Dahlin: All about Eve."Execute-VerifyReplication for Multi-Core Servers"