블록체인4.0, 큐브체인 플랫폼을 위한 Open APIs와 Service Model

Open APIs and Service Model for Block Chain 4.0, CubeChain Platform

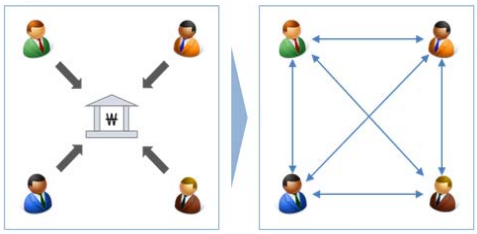
남 상 엽**, 김 동 오**

목 차

1. 세대별 블록체인 동향분석

1.1 블록체인 1세대 '비트코인'

블록체인 1세대, 블록체인 1.0은 비트코인에 적용한 기술로써 약 4000개의 거래 정보를 담을 수 있는 1MB크기의 블록이 10분에 하나씩 생성돼 연결되도록 설계되었고 초기 설계 값을 변경할 수 없도록 만들어 졌기 때문에 중간에 비트코인의 발행량과 속도 등을 변경하기가 불가능하다.



〈그림 1〉 블록체인 1.0의 P2P 분산형 구현기술

1.2 블록체인 2세대 '이더리움'

블록체인 2세대, 블록체인 2.0은 이더리움에 적용한 기술로써 블록생성 속도를 1분 이하로 개선하고 블록 크기를 늘리고 자동 계약 기능을 통해 거래 참여자가 합의된 내용이 특정 시기가 되면 발효되도록 설정한 스마트 계약(Smart Contract)이라는 새로운 기능이 추가 되었다.

또한 계약이 성립하기 위한 규칙을 정하고 조건에 맞으면 해당 초기 값을 변경이 가능하도록 생성 속도와 발행량도 수정이 가능하도록 하였다.

1.3 블록체인 3세대 '블록체인 컨소시움'

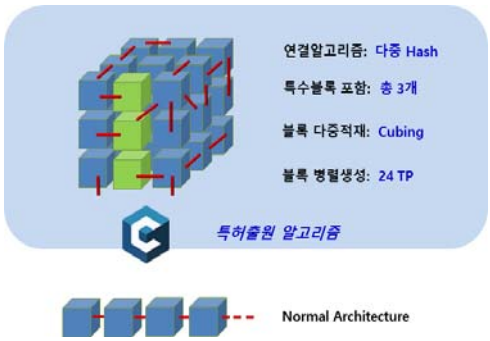
블록체인 3세대, 블록체인 3.0은 사회전반의 서비스를 보다 편리하게 이용할 수 있고 의사결정 기능 및 지분증명방식(PoS)의 뛰어난 거래처리 성능 등 기술이다. 이것은 플랫폼 생태계 구축과 서비스 표준화를 통하여 블록체인 컨소시움인 R3CEV와 고객의 정보외 각각의 서비스 정보를 담고 있는 블록체인과 연결하여 다양한 서비스를 보다 효율적으로 운영하는 플랫폼인 리눅스 재단과 IBM이 주도하는 하이퍼 레저(Hyperledger) 프로젝트, EOS, NEO, IOTA, Qtum, Boscoin 등이 있다.

1.4 블록체인 4세대 'Cube Chain '

큐브 체인(Cube Chain)은 기존의 블록체인보다 더욱 빠르고, 정밀한 데이터 처리 및 강화된 보안시스템을 가진 차세대 블록체인 플랫폼이다. 큐브 체인(Cube Chain)은 생성된 27개의 블록을 하나의 큐브로 형성하고, 큐브와 큐브를 연결하여 데이터를 보관하는 신개념 블록체인 원천기술이다. 큐브 엔진(Cube Engine)은

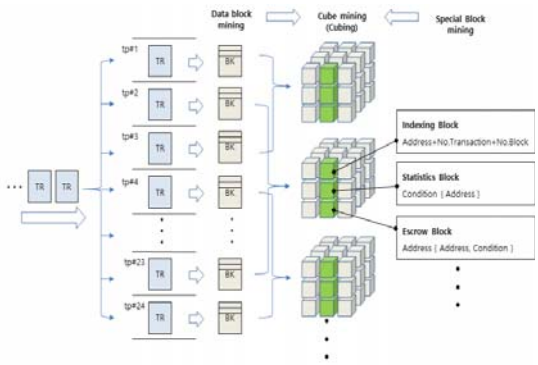
* 국제대학교 컴퓨터정보통신과 교수
** 큐브시스템 대표이사

큐브 체인(Cube Chain)의 코어 기술로서, 블록을 큐브화(Cubing)시키고, 큐브를 이루는 27의 블록 중 3개의 특수한 기능을 가진 블록을 형성하여 기존의 블록체인보다 우수한 성능을 가진다. 또한, 블록화와 큐브화를 거치는 2중 암호화 방식으로 인터넷이라는 신뢰가 형성되지 않은 공간에서 신뢰를 만들어 데이터를 이동시킬 수 있는 혁신적인 암호화 기술이다.



〈그림 2〉 큐브체인의 특징

블록체인이 기존의 데이터베이스를 제대로 대체하려면 속도의 개선과 사용의 편리성 등 기존 데이터베이스가 가지고 있는 기술적 기능들이 동반되어야 한다. 블록체인 기술이 지속적으로 발전하여 데이터베이스를 대체할 수 있는 수준이 된다면 데이터를 기록하고 관리하는데 매우 안전한 방식으로 자리매김할 것이다. 그러한 관점에서 큐브체인은 블록대신 큐브라는 개념을 통해 데이터베이스의 기능적 요소를 확장해 갈 수 있도록 구조화 시켰다.



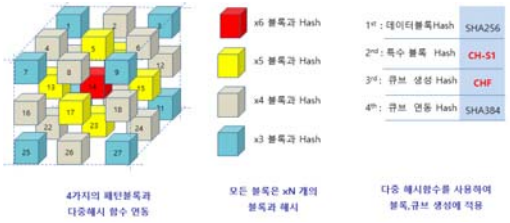
〈그림 3〉 큐브체인의 병렬처리 구조

따라서 공개 데이터베이스의 안전한 사용을 위해 기존의 블록체인이 갖는 장점을 기반으로 데이터베이스가 갖는 몇 가지 장점을 활용할 수 있도록 하였다. 큐브체인의 개발은 발전된 블록체인 원천기술을 확보하여 암호화 화폐를 발행하고 공개용 데이터베이스를 필요로 하는 다양한 온라인 서비스를 선보일 예정이다.

2. 큐브체인의 구조분석

2.1 큐브체인의 패턴블록과 다중 해시사용

큐빙을 진행할 때 암호화 방식은 독자적으로 개발한 CHF-Algorism(Cubing Hash Function Algorithm)을 사용한다. 큐브 내 27개의 블록은 각 블록의 위치에 따라 서로 인접한 블록이 각각 다르다. 육면체의 각 면의 위치에 따라 모퉁이에 위치한 블록 8개, 중심에 위치한 블록 6개, 중심을 둘러싼 블록 12개, 큐브의 정중앙 블록 1개로 구성된다. 4가지 구분에 따라서 사용하는 해시함수도 달라지고 각각 CH-B3, CH-B4, CH-B5, CH-B6으로 명명한다.



〈그림 4〉 큐브체인의 패턴블록과 다중해시 사용

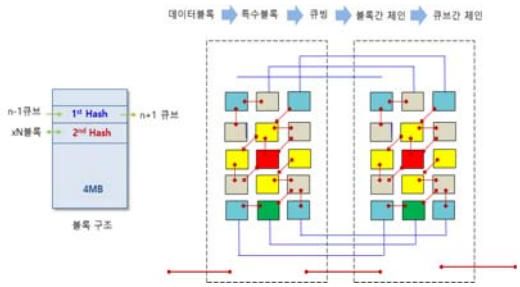
큐브체인의 4 종류의 패턴은 <그림 4>처럼 인접한 6개의 블록과 연결되는 제 1패턴, 인접한 5개의 블록과 연결되는 제 2패턴, 인접한 4개의 블록과 연결되는 제 3패턴, 인접한 3개의 블록과 연결되는 제 4패턴이 있다

2.2 큐브체인의 큐빙과 블록체인 동시연산

CH(Cubing Hash)는 큐빙 해시함수를 뜻하며 뒤의 B(Block)는 위치한 블록에서 큐브 내 바로 인접한 블

록의 개수를 뜻한다. 큐빙 해시함수는 인접한 블록의 해시값을 이용하여 또 다른 해시값을 만들어낸다. 이렇게 해서 27개 블록의 각각 해시값을 얻는다. 큐빙 해시값이 블록 해시값과 다른 특징은 블록데이터를 기반으로 한 것이 아니라 관계된 블록 해시값을 기반으로 했다는 점이다. 큐빙 해시값을 통해 현재블록과 전체 블록을 검증하며 27블록이 개별적으로 사슬관계를 만들어 검증을 한다.

<그림 5>처럼 큐브체인의 컴퓨팅 연산은 데이터블록, 특수블록, 큐빙, 블록간 연결, 큐브간 체인 순으로 진행한다.

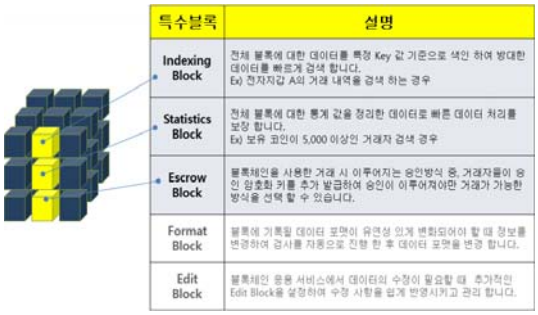


〈그림 5〉 큐브체인의 컴퓨팅 처리과정

2.3 큐브체인의 특수블록

큐브 체인의 특수블록은 데이터 블록에 기반으로 하여 재가공 된 데이터나 반영될 데이터이다. <그림 6>처럼 필수 특수블록으로 채택되는 3개의 특수블록은 데이터 블록의 재가공 데이터라 할 수 있다. 특수블록이 생성되기 위해서는 먼저 데이터 블록이 있어야 한다. 따라서 최초의 첫 번째 큐브에서는 특수블록이 생성되지 않는다.

두 번째 큐브부터 특수블록이 생성되는데, 특수블록의 생성시점은 이전 큐브가 만들어지고 현재 큐브가 형성되는 시점에서 진행된다. 그래야만 특수블록을 생성하느라 큐브가 완성되는데 지연되는 시간을 없앨 수 있다. 첫 번째 큐브가 완성되면 바로 두 번째 큐브에 포함될 특수블록을 생성하기 시작한다. 이때 특수블록은 이전 특수블록과 이전 데이터에서 추출된 내용을 합쳐서 생성함으로 누적 반영을 쉽게 처리할 수 있다. 즉, n번째 큐브의 특수블록은 n-1번째 큐브까지의 데이터를 담고 있다. n-1번째 큐브가 완성되는 시점에서 n-2번째 큐브의 데이터를 담은 특수블록과 n-1번째 데이터를 합쳐서 만들어지기 시작하며, n번째 큐빙이 이루어질 때, 데이터 블록과 유기적인 관계를 형성하게 된다. 특수블록은 큐브와 큐브가 체인화가 이루어지는 시간동안 생성됨으로 기능적 요소는 확장되지만, 이로 인한 지연되는 시간은 없다. 또한 특수블록의 암호화는 자체개발한 CH-S1 함수를 이용하여 데이터 량에 비해 매우 빠른 속도로 해시 값을 얻을 수 있다.



〈그림 6〉 큐브체인의 특수블록

2.4 큐브체인의 성능 분석

2.4.1 큐브체인의 성능

큐브체인의 성능은 <그림 7>처럼 큐브생성이 30초가 소요된다. 그리고 트랜젝션 1개의 사이즈가 260바이트이므로 1개의 큐브는 387,166 트랜잭션이 발행함으로 1개 블록의 트랜잭션이 12,905(TPS) 트랜젝션 수가 발생한다. 그러므로 블록 생성시간은 30초/24=1.25초이고 확정시간은 30~165초에 확정이 이루어진다.

〈그림 7〉 큐브체인의 성능

2.4.2 큐브코인의 확정

큐브코인의 확정은 <그림 8>처럼 블록이 한 개의 경우는 30초이고 최대 5개의 블록이 생성시 확정시간이 165초이다.

코인명	TPS	확정횟수
리플	2~10초	1 컨펌
이오스	9초~45초	15 컨펌
큐브체인	30초~165초	5 컨펌
이더리움	14초~6분	12 컨펌
대시	150초~15분	6 컨펌
모네로	60초~20분	10 컨펌
퀀텀	120초~30분	10 컨펌
이더리움클래식	12초~24분	120 컨펌
라이트코인	150초~30분	12 컨펌
제트캐시	2.5분~60분	24 컨펌
비트코인골드	10분~60분	6 컨펌
비트코인캐시	10분~60분	2 컨펌
비트코인	10분~60분	6 컨펌

〈그림 8〉 큐브코인의 확정

2.4.3 큐브체인의 다른 기술과의 비교분석

<그림 9>처럼 큐브체인과 다른 기술들과의 비교분석을 하였다. TPS는 블록체인 소프트웨어의 설계뿐 아니라 블록체인을 구동하고 블록을 생성/검증하는 하드웨어 성능, 네트워크 성능에 따라서 달라질 수 있다. 또한 트랜잭션의 종류에 따라서 달라질 수 가 있다. 블록생성시간 및 확장시간의 지표에서 좋지 않으면 실제 사용자에게 느리게 느껴질 가능성이 존재한다. TPS, 블록생성시간 및 확장시간의 통하여 비트코인, 이더리움, EOS 등을 포함하여 다양한 블록체인들의 이론적 속도를 평가할 수 있다.

	합의 알고리즘 (컨센서스)	대역폭 (TPS)	블록생성 주기(초)	확정횟수	확정시간 (초)
큐브체인	POH (POW+POS)	12,900	1.25	5	165
EOS	DPOS	500~1,000	3	15	45
비트쉐어/스팀	DPOS	3,300	3	15	45
네오	DBFT	100	15-20	1	15-20
이더리움	POW	15	14	12	180
비트코인	POW	7	600(10분)	6	3600

〈그림 9〉 큐브체인의 다른 기술과의 비교

3. 큐브체인의 Open APIs와 서비스 모델

3.1 큐브체인의 비즈니스 모델

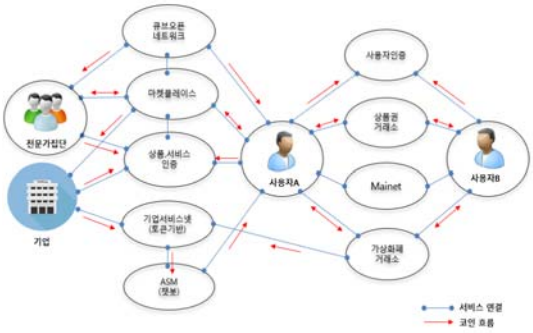
큐브체인 비즈니스 서비스 모델은 <그림 10>처럼 5개 분야인 사용자 인증, 상품/서비스 인증, 메시지/마켓플레이스, SNS/전문가그룹 등으로 비즈니스 모델을 구현하고자 한다.

〈그림 10〉 큐브체인의 비즈니스 모델

이러한 큐브체인 비즈니스 서비스 모델을 구현하기 위하여 <그림 11>처럼 다양한 워킹 그룹인 의료공공, 서비스 결제, DNA의료, P2P거래, 전자상거래 등 E-Commerce 분야의 큐브체인 플랫폼을 구축하고 있다.

〈그림 11〉 큐브체인의 비즈니스 플랫폼 구현 예시

<그림 12>처럼 큐브체인의 5가지 서비스 모델의 구현을 통하여 서비스 연결과 코인의 흐름을 확인할 수 있다.



〈그림 12〉 큐브체인의 서비스 토폴로지와 코인 흐름도

3.2 큐브체인 플랫폼의 OPen APIs와 서비스 모델

규브체인 플랫폼을 위한 OPEN API와 서비스 모델은 <그림13>처럼 5가지이다. 5가지 OPEN API와 서비스 모델은 큐브체인기반 사용자 인증 로그인 서비스인 OneID 서비스, 큐브체인 기반 상품 인즌 서비스인 Cube Chain Product, 큐브체인 기반의 SNS플랫폼인 Cube Open Network, 큐브체인 기반 메신저 서비스와 마켓플레이스인 Cube Chat, 큐브체인 기반 기업 콜센터용 챗봇 서비스인 ASM 이다.

〈그림 13〉 큐브체인 기반 서비스 모델과 Open API

3.2.1 One ID Service

큐브체인의 One ID Open APIs를 사용하는 모든 서비스에 별도 가입 없이 로그인 가능하다.

생체 인증 (지문 인식) 을 추가하여 개인 정보 보안과 인증을 강화하고 블록체인 기반의 사용자의 신원을 인증하는 패스포트 역할을 할 수 있다.

〈그림 14〉 One ID Service

<그림 14>처럼 사용자 정보를 해시하여 큐브체인에 저장하고 Open APIs를 사용하는 모든 서비스에 로그인 할 수 있게 한다.

3.2.2 Cube Chain Product Service

큐브체인을 이용하여 온,오프 라인 가맹점 사업이 가능하다. 구매자의 중고거래, 재판매 거래 시 상품 신뢰성을 확보하고 거래 결제를 지원하고 판매자의 상품 정보를 보호하고 재판매 시 매출/마진 확보 등이 가능하다. <그림 15>처럼 온 오프 라인 상 유통되는 디지털 상품의 진위 여부를 판별할 수 있도록 상품 판매 정보를 큐브체인에 담을 수 있다.

〈그림 15〉 Cube Chain Product Service

3.2.3 Cube Open Network Service

Cube Open Network은 블록체인 기반의 플랫폼으로 <그림 16>처럼 전문가들과 Follower 들의 지성 집단들의 창작활동을 지원하여 생성된 콘텐츠를 Follower가 인정하면 평가에 의하여 콘텐츠를 큐브체인의 정식 블록으로 인정 (채굴)하고 생성과 평가에 참여한 사용자에게 토큰과 평가 점수를 보상하는 서비스이다.

〈그림 16〉 Cube Open Network Service

3.2.4 Cube Chat Service

Cube Chat Service는 기업과 개인, 개인과 개인간의

온오프상의 거래를 지원하는 메신저 기반의 P2P 간 거래와 결제가 가능한 마켓 플레이스이다. <그림 17>처럼 큐브 오픈 네트워크와 연계하여 전문가들의 스몰 비즈니스를 지원한다. 메신저 데이터를 노드에 저장 할 수 있도록 하여 개인 정보를 보호하고 큐브체인의 원장, 지갑, 토큰, 에스크로 기능을 통하여 실시간 결재를 진행할 수 있는 혁신적인 시스템이다. 인스턴트 메세지와 Live 방송을 이용하여 전문가 그룹의 스몰 비즈니스를 지원한다.

〈그림 17〉 Cube Chat Service

3.2.5 AI Service Manager Service

AI Service Manager Service는 기업의 고객 대응을 위하여 빅데이터를 분석하고 이것을 바탕으로 고객에게 대응을 할 수 있는 인공 지능형 맞춤 서비스이다. <그림 18>처럼 기업의 콜센터를 채봇 서비스로 대신하여 기업은 비용 절감과 고객에겐 스마트 계약을 통한 코인 보상을 서비스 한다. 이 서비스를 통하여 콜센터 구축 운영 유지 보수에 필요한 비용을 절감할 수 있고 데이터 마이닝과 머신 러닝을 통하여 고객 질문에 대응하는 챗봇 서비스를 구현 할 수 있고 챗봇 서비스를 통하여 예약과 계약 (Smart Contract)을 진행하고 고객에게 토큰을 보상할 수 있다.

〈그림 18〉 AI Service Manager Service

4. 고찰 및 결론

큐브체인은 4세대 블록체인 플랫폼으로 기존 블록체인 서비스의 최대 단점으로 부각 되고 있는 블록생성과 합의 인증에 필요한 데이터 접근과 업데이트 속도를 큐빙(Cubing) 기술을 이용하여 업 그레이드 함으로써 검색속도, 이중암호화, 데이터통계, 지급보증을 위한 에스크로 기능을 시스템이 직접 제공하는 신개념의 블록체인 기술이다.

큐빙 데이터는 기존 블록체인 생성에 필요한 암호화와 더불어 큐빙에 필요한 암호화가 추가되어 이중 보안을 실현한다. 큐브체인 서비스플랫폼에서 필요한 다양한 APIs 와 스마트 계약을 위한 프로그래밍적인 구현을 지원하며, 큐브체인 코인(QUB)를 발행하고, 전자지갑, 분산원장, 에스크로 기능을 제공하여 P2P 간의 거래를 가능토록 해준다. 블록체인이 기존의 데이터베이스를 제대로 대체하려면 속도의 개선과 사용의 편리성 등 기존 데이터베이스가 가지고 있는 기술적 기능들이 동반되어야 하는데 그러한 관점에서 큐브체인은 블록대신 큐브라는 개념을 통해 데이터베이스의 기능적 요소를 확장해 갈 수 있도록 구조화 시켰다.

따라서 공개 데이터베이스의 안전한 사용을 위해 기존의 블록체인이 갖는 장점을 기반으로 데이터베이스가 갖는 몇 가지 장점을 활용할 수 있도록 하였으며 큐브체인의 개발은 발전된 블록체인 원천기술을 확보하여 암호화 화폐를 발행하고 공개용 데이터베이스를 필요로 하는 다양한 온라인 서비스를 구현하고 있다.

큐브체인 플랫폼 상에 구축되는 큐브체인 서비스 플랫폼은 다양한 P2P 참여자의 자발적인 거래를 지원하여 기업과 개인 모두 블록체인의 참여자로서 새로운 서비스 혜택을 받게 하는 구체적인 비즈니스 모델로 사용자에게 블록체인 서비스가 어떠한 미래 가치를 갖고 생활을 바꿀 수 있는지 선명하게 제시 하였다.

참 고 문 헌

[1] 남상엽외 3인, “블록체인기술활용”, 상학당, 2018.04
[2] 남상엽외 4인, “인터넷뱅킹과 결재플랫폼”, 상학당, 2018.01
[3] 남상엽외 3인, “차세대 블록체인 4.0, 큐브체인의 구성 및 응용,” 한국인터넷정보학회지 제19권제1호, 2017.04

[4] 김동오외 2인, “큐브체인의 데이터 연결구조 및 연결 방법,” 특허출원번호(P180114) 2018.04.02.
[5] 김동오외 2인, “큐브체인 형태의 데이터 관리 엔진 및 데이터 관리 방법,” 특허출원번호(P180115) 2018.04.02.
[6] 김동오외 2인, “큐브체인을 활용한 사회관계망 서비스 시스템,” 특허출원번호(P180116) 2018.04.02.
[7] 김동오외 2인, “블록체인 기반 리모트 채널변경 인식을 통한 시청률 조사시스템 및 방법” 특허출원번호(P180154) 2018.05.02.
[8] 김동오외 2인, “통계 블록을 포함하는 큐브체인 형태의 데이터 관리 엔진 및 데이터 방법,” 특허출원번호(P180127) 2018.06.04.
[9] 김동오외 2인, “색인 블록을 포함하는 큐브체인 형태의 데이터 관리 엔진 및 데이터 방법,” 특허출원번호(P180128) 2018.06.04.
[10] 동오외 2인, “에스크로 블록을 포함하는 큐브체인 형태의 데이터 관리 엔진 및 데이터 방법,” 특허출원번호(P180129) 2018.06.04.
[11] 김동오외 2인, “큐브 체인의 암호화 방법 및 큐브 체인을 이용한 코인거래를 확인 방법,” 특허출원번호(P180130) 2018.06.04.
[12] -http://www.cubechain.io

◐ 저 자 소 개 ◑

남 상 엽
2002년 단국대학교 대학원 컴퓨터(공학박사)
1984년~1992년 삼성종합기술원 주임연구원
1992년~1998년 모토로라반도체통신 책임연구원
1998년~현재 국제대학교 컴퓨터정보통신과 교수

김 동 오
1990년 인하대 컴퓨터공학(공학사)
1990년~2000년 삼성SDS
2017년~현재 큐브시스템 대표이사