CUBE
CHAIN

Cube Chain

Technical White Paper

Contents

큐브체인 기술백서

Cube Engine Version 2.0

1. 개요

1.1 개요

블록체인은 데이터를 일정한 시간 단위로 모아 데이터 블록을 생성하고, 블록을 암호화한 해시값을 통해 데이터를 검증하고, 이렇게 기록되는 데이터를 분산 서버에 저장하는 시스템이다. 암호화를 통한 데이터 검증과 동일한 데이터를 분산 저장하여 데이터의 신뢰와 안정성을 확보하기 위한 시스템이다. 기존에 사용되던 데이터베이스에 비해 블록체인의 장점은 데이터를 시간순으로 암호화 검증하여 비가역적이고, 이를 P2P 방식으로 동일 데이터를 공유하여 저장함으로써 데이터를 매우 안전하게 보호하고 유지할 수 있다는 점에 있다. 다수의 사용자로부터 신뢰를 얻어야 하는 디지털 화폐 기술에 블록체인이 사용되면서 오늘날 암호화 화폐 시장의 기반 기술로 자리 잡은 데에는 이와 같은 이유가 있다. 블록체인이 암호화 방식과 P2P 방식을 사용하여 독특한 데이터 기록 방식을 구현하여 새로운 기술의 지평을 열었지만 여전히 기술적인 한계는 가지고 있다. 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 블록 대신 큐브라는 개념을 통해 데이터베이스의 기능적 요소를 확장해 갈 수 있도록 구조화했다. 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 데이터베이스가 있어야 하는 다양한 온라인 서비스를 선보일 예정이다.

1.2 기본정보

Cube Chain (QUB)

코인 이름 : Cube Chain
총발행량 : 120 억개
알고리즘 : SHA256,CH-S1,CHF,SHA384
보상방식 : POH (Proof of Hybrid: POW+POS)
POS 참여조건 : 지갑에 최소 5,000 개 이상의 큐브체인 보유
개발 시작 : 2017 년 1 월

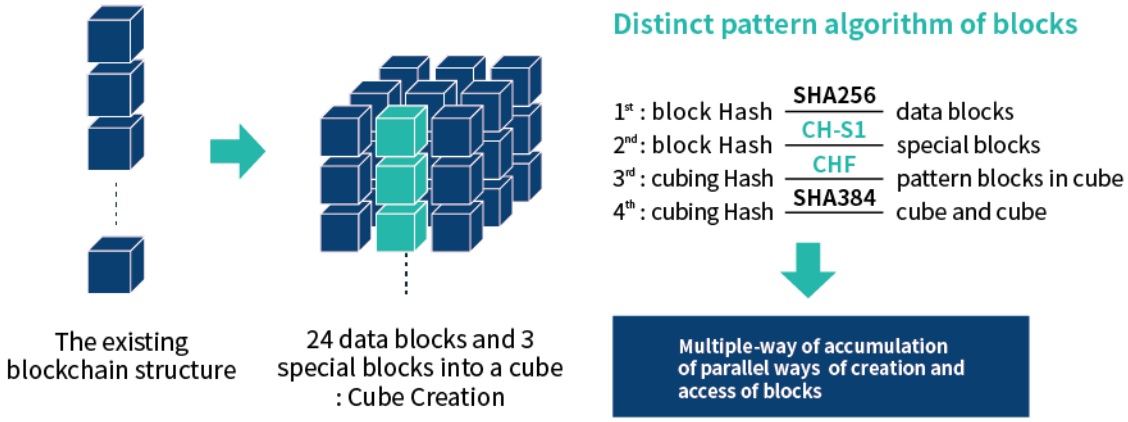
2. 큐브체인의 특징

우선 블록체인의 핵심이자 암호화 기술 용어인 해시에 대해서 아래와 같이 설명한다. 암호화 해시의 한 종류인 SHA256 에 대한 정의이다. 해시는 '특정한 데이터를, 이를 상징하는 항상 같은 길이의 데이터로 변환하는 행위'를 의미한다. 여기에서 상징 데이터는 원래의 데이터가 조금만 달라져도 확연하게 달라지는 특성이 있어 무결성을 지키는 데 도움을 준다. 예를 들어 'A'라는 문자열의 해시와 'B'라는 문자열의 해시는 고작 한 알파벳이 다를 뿐인데 그 결과가 천차만별이라는 것이다. 예를 들어 대표적인 해시 알고리즘인 SHA256 은 어떠한 입력 값을 넣든 항상 256bit 의 다른 64 자리의 16 진수 값을 반환한다.

[그림 1]

2.1 Cubing

큐빙(큐브화)은 27 개의 블록을 모아 블록의 집합체인 하나의 큐브로 만드는 큐브화 기술을 뜻한다. 거래장부를 기록한 24 개의 일반블록과 3 개의 특수블록이 합해져 하나의 큐브를 생성한다. 단순한 Grid 개념이 아닌, 병렬로 동시에 블록이 생성되는 기술이다. 27 개의 블록이 생성됨과 동시에 큐빙(큐브화)은 진행되며, 생성된 큐브는 또 하나의 해시값을 만든다. 이후 기록되는 모든 장부는 지속해서 큐브를 만들고, 해시값은 블록과 블록이 아닌 큐브와 큐브를 잇는다. 이는 블록이 연결되면서 생기는 1 차 암호화, 큐브가 연결되면서 생기는 2 차 암호화 현상을 만들어내며, 기존의 블록체인보다 훨씬 강력한 암호화 기술의 블록이 생성됨과 동시에 큐브화는 진행되며 생성된 큐브는 또 하나의 해시값을 만든다. 큐빙으로 인해 큐브의 해시값이 만들어짐으로 블록의 해시값과 함께 이중으로 검증되는 데이터 시스템을 구축할 수 있다.



[그림 2]

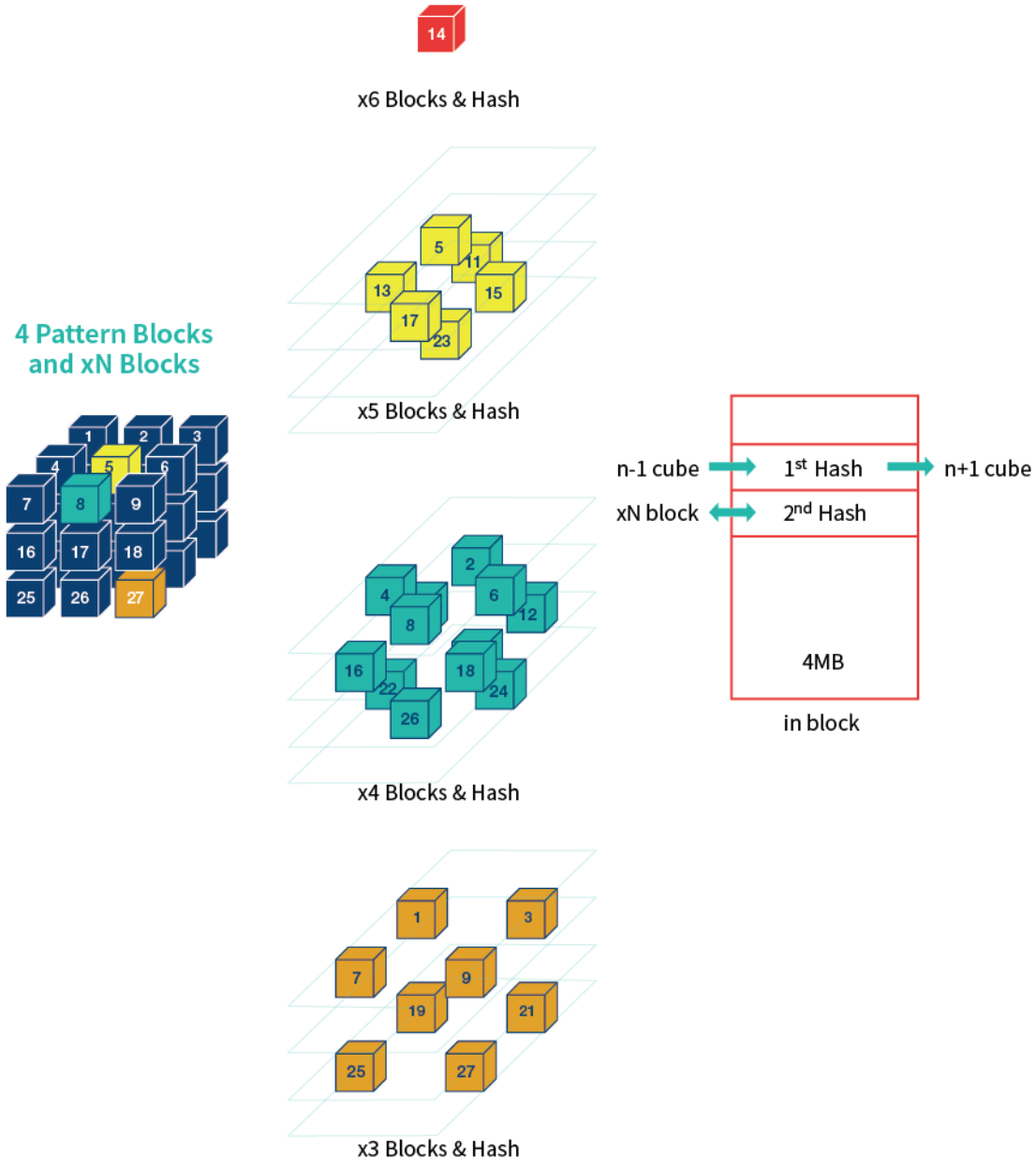
기존의 일렬 연결 구조로 인한 속도 저하와 확장성 문제를 해결하기 위해 24 개 트랜잭션 풀을 통해 병렬 구조로 데이터 블록을 신속하고 안전하게 생성한 것이 큐브체인이다. 트랜잭션 풀에서 동시에 생성된 24 개의 데이터 블록이 큐브로의 적재까지 이어져 빠르고 안전한 처리가 가능하다. 큐빙이라는 기술을 통해 많은 양의 데이터 블록의 병렬 처리를 관리하며 이중 해시 함수와 패턴블록 구조를 통해 블록 간의 빠른 접근이 구현할 수 있도록 설계하였다.

블록이 1 개의 큐브로 합쳐질 때 4 개의 해시함수를 사용하여 보안성을 강화했다. 여기에서 사용된 해시함수는 SHA256, CH-S1,CHF,SHA384 이고 SHA256, SHA384 는 공개된 해시알고리즘이다. 아래의 독자 개발된 해시알고리즘에 관해서 설명한다. CH-S1(CubeHash Special Version 1)는

특수블록이 생성 시 해시함수를 만들 때 사용하는 자체개발된 알고리즘이고, CHF(CubeHash Function)는 큐빙의 과정에서 패턴블록으로 해시함수를 만들 때 사용하는 자체 개발된 알고리즘이다.

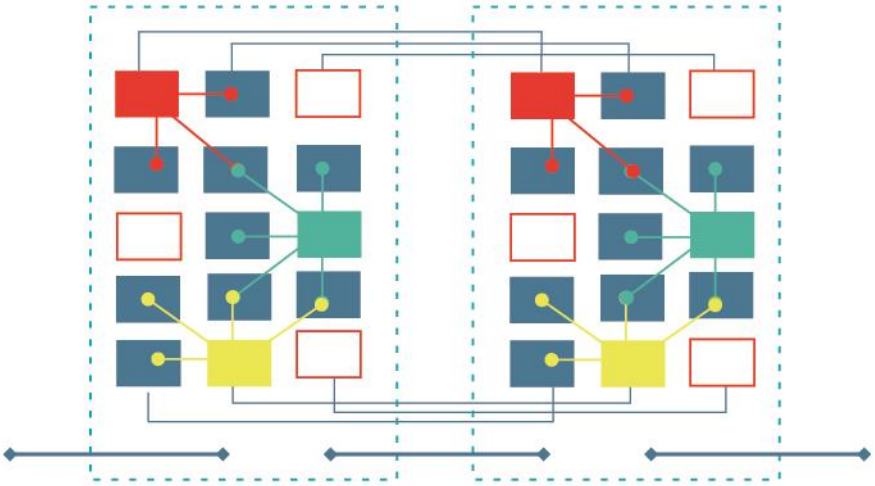
구조분해와 설명

큐브체인은 다중 방식의 블록적재와 병렬식 블록을 생성 및 접근하여 속도를 향상시키는 구조를 가진다.



[그림 3]

큐브를 분해하면 위와 같은 4 가지의 블록패턴이 존재한다.



[그림 4]

각 패턴 블록은 이전 큐브의 가장 근접한 블록과 연결되고 [그림 3]의 2nd Hash 에 xN 블록의 해시값이 저장된다.
큐빙으로 인한 큐브 연결은 직전에 생성된 큐브의 해시값이 [그림 3]의 1st Hash 에 저장됨으로 인해서 직전에 생성된 큐브와 연결된다. 이로 인해 각 블록과 블록이 연결되고, 큐브와 큐브가 연결된다. 각 패턴으로 연결된 블록의 해시값은 큐브에 저장된다.

2.2 Indexing Block

Indexing Block 은 전체 블록에 대한 방대한 데이터를 일목요연하게 정리하여 검색기능이 강화된다. Indexing Block 은 전체 거래에 포함된 전자지갑을 주소별로 거래가 이루어졌던 큐브높이(기존 블록체인의 블록높이)를 정리한 데이터 블록이다. 따라서 Indexing Block 만으로 해당되는 데이터를 더욱 빠른 시간내에 찾을 수 있다.

예를 들어, A 라는 주소: 20c (20 : 20 번째 큐브, c : 3 번째 블록) ,32a, 105h, 201j, 302r 큐브 블록 위치, B 라는 주소: 3b, 102v, 201s, 1001q 큐브 블록 위치, C 주소 5c, 34e, 56g, 234k, 456y 큐브 블록 위치 등 위와 같이 모든 주소를 주소값 순서대로 정리한 후, 해당하는 블록높이를 주소값에 맞게 정리한다.

검색자가 B 주소 내 특정거래를 검색하고 싶을 때, Indexing Block 내 정리된 B 주소와 같이 특정 거래를 빠르게 찾아낼 수 있다. Indexing Block 의 목적은 특정 주소에 대한 이력을 빠르게 찾고 쉽게 관리할 수 있도록 도와준다.

[기존 블록체인 방식]
특정 지갑 주소 거래 내역 검색 시 모든 데이터를 검색
(모든 큐브 1,000 개 큐브 생성 시 1,000x24=24,000 개의 블록 검색)
시간복잡도 = $O(B \log 2\ T)$

[큐브체인 방식]
지갑 주소, 큐브 높이와 블록 위치에 대한 정보만을 가지고 있고, 해당 데이터를 가지고 전체블록을 스캔할 필요가 없고, Indexing Block 에서 지갑주소만 검색하면 해당 데이터를 취득할 수 있다.
시간복잡도 = $O(\log 2\ I + \log 2\ T)$
예)특정 지갑 주소 거래 내역 검색 시 인덱싱 블록만 검색 (1 개의 블록 + 1 개의 큐브)

2.3 Statistics Block

Statistics Block 은 전체 블록에 대한 통계 값을 정리하여 응용서비스와 각종 API 에서도 빠른 로직 구현과 다양한 활용성을 제공한다. Statistics Block 은 매우 빠른 데이터 처리를 보장한다. 예를 들어 Statistics Block 내에서 POS 대상자가 5,000 이상이므로 잔고 5,000 이상인 전자지갑 주소에 대한 데이터, 잔고가 많은 전자지갑 상위 리스트 1,000 개, 이체 횟수가 100 회 이상인 전자지갑 리스트를 모아둘 수 있다. 이외에도 사용성이 많은 통계 데이터를 모아두어, 언제든지 필요할 때 리스트를 빠르게 출력할 수 있다.

이러한 통계는 전체 블록에 대한 통계값으로 정리된 내용이 없다면 검색 시 많은 시간이 필요한 부분이지만 Statistics Block 을 이용하면 빠른 시간내에 서비스 처리가 가능하다. 잔고가 많은 전자지갑 상위 리스트 1,000 개, 이체 횟수가 100 회 이상인 전자지갑 리스트 등 자주 사용되는 출력 데이터들을 모아 놓는다면 효과적인 검색을 이루어 낼 수 있다. 결과적으로 해당하는 응용서비스의 API 를 매우 빠르게 구현할 수 있다.

예) 큐브 높이에 따른 POS 대상자 찾기 위한 검색 블록

[기존 블록체인 방식]

큐브 높이 1,000 일 때 : 1+2+3+ … +998+999+1,000=500,500x24=12,012,000 블록

큐브 높이 10,000 일 때 : 1+2+3+ … +9,998+9,999+10,000=50,005,000x24=1,200,120,000 블록

[큐브체인 방식]

큐브 높이 1,000 일 때 : 1+1+1+ … +1+1+1=1,000 개 블록

큐브 높이 10,000 일 때 : 1+1+1+ … +1+1+1=10,000 개 블록

큐브가 1,000 개만 쌓여도 검색해야 하는 블록의 개수는 10,000 배이상 차이가 난다. 리스트를 정리하는 과정과 해당 내역을 검색하는 과정을 고려하면 이 보다 더 큰 차이가 발생할 것이다. 현재까지 고려하고 있는 기능은 단일 거래로 1000QUB 나 2000QUB 이상이 거래되는 내역에 대한 통계, 잔고 랭킹 1~1000 등 까지의 통계, 전체 거래량/전체 거래 횟수에 대한 통계, 미승인 에스크로에 대한 통계이다.

2.4 Escrow Block

에스크로(escrow)는 상거래 시에, 판매자와 구매자의 사이에 신뢰할 수 있는 중립적인 제삼자가 중개하여 금전 또는 물품을 거래하는 것을 의미하며 거래의 안전성을 확보하기 위해 이용된다. 구체적으로는 판매자·구매자·제삼자의 사이에서 다음과 같은 절차로 진행된다.

구매자는 제삼자에게 대금을 맡긴다. 판매자는 제삼자에게의 입금을 확인하고 구매자에게 상품을 발송한다. 구매자는 송부된 상품을 확인하고 제삼자에게 상품이 도착했음을 알린다. 애초의 거래 내용과 다른 경우는, 상품을 반송하거나 거래를 파기할 수 있다. 제삼자는 판매자에게 대금을 송금한다. 판매자는 대금을 수령한다(거래의 종료). 중개하는 제삼자는 일정한 수수료를 받는 것으로 수익을 얻는 것이 일반적인 에스크로 거래방식이다.

큐브체인에서의 에스크로 거래는 거래체결이 되더라도 받은 지갑에서 즉시 사용할 수 없는 상태가 되고 반드시 승인이 이루어져야만 사용할 수 있다. 일반거래는 24 개의 데이터에 분산되어 기록되지만, 에스크로 거래 시에는 에스크로 블록에 기록된다.

암호화폐 에스크로 이체 시 승인 암호화키를 만들어 거래할 수 있고 승인 암호화키를 송신인과 수신인이 암호화 키를 통해 승인 처리를 할 수 있다. 이때 승인 암호화키는 자동 생성 방식과 송신인이 만들어서 보내는 방식이 있다. 암호화키 승인 허용 방식에서도 송신인만 승인할 수 있도록 혹은 수신인측에서 승인할 수 있도록, 송신인과 수신인 둘 다 허용해야 승인 가능한 방법으로 처리할 수

있다. 또한, 일정 기간 후 자동승인 방식도 있는데 이때 승인키로 자동승인을 해제하지 않는 한 일정 기간 후 승인되어 수신인에서 사용 가능한 상태가 된다. 이때 자동승인 해제를 하면 송신인 측에서 승인을 허용하는 방식으로 전환되며 에스크로 상태 허용 시까지 유지된다. 그렇게 되면 수신인은 거래를 취소할 수는 없지만 송신인이 사용할 수 없기 때문에 지속해서 거래나 계약을 지키도록 요청할 수 있다. 승인키 허용방식에서 수신인 승인 허용방식은 송신인 측에서 이 메일이나 메신저 등의 통신 수단을 통해 승인키를 전달하면 된다. 기존의 에스크로 거래는 중계자가 거래자 간의 중간에서 거래의 매개 역할을 했다면 에스크로 블록은 중계자가 없는 에스크로 기능이 특징이다. 물론 서비스 구현에 따라 기존의 방식처럼 제삼자가 중간매개 역할도 가능하지만 직접 당사자 간 거래로만 에스크로를 도입할 수 있다는 큰 특징이 있다. 온라인 쇼핑몰, 오픈마켓뿐만 아니라 쇼핑몰이 없는 개인 간의 직거래에서도 간편하고 안전한 거래가 이루어지게 하는 획기적인 방법이 될 수 있다.

에스크로 블록에는 Double authorization data system(이중승인방식)을 도입하여 데이터를 저장한다. 일반 데이터는 24 개의 데이터 중 하나로 기록되지만, 에스크로 데이터는 별도로 보관 관리된다. 에스크로 데이터는 이중승인이 이루어지는 시점에서 일반 데이터로 재기록 된다.
Double authorization data system(이중승인방식)이란 일반적인 블록체인을 사용한 거래 시 이루어지는 전자서명 외에 암호화키를 추가 발급하고 승인하여야 거래가 가능한 방식을 말한다.
에스크로 블록을 사용한 이러한 방식은 암호화폐에서 거래체결이 되더라도 받은 지갑에서 즉시 사용할 수 없는 상태가 되며, 제삼자가 중계하는 에스크로의 형태가 아닌 거래 당사자 간의 거래를 보호하는 기능을 부여할 수 있다. 블록체인을 기반으로 하는 에스크로 기능인 것이다.
또한 에스크로 블록은 소유자가 암호를 통해 데이터를 보호할 때 사용할 수 있다. 데이터를 오픈된 형태로 사용하는 것이 아니라 암호화를 통해서 암호를 알고 있는 사용자만이 데이터를 확인할 수 있게 되는 것이다.

일반블록과 특수블록의 크기와 생성까지의 소요시간

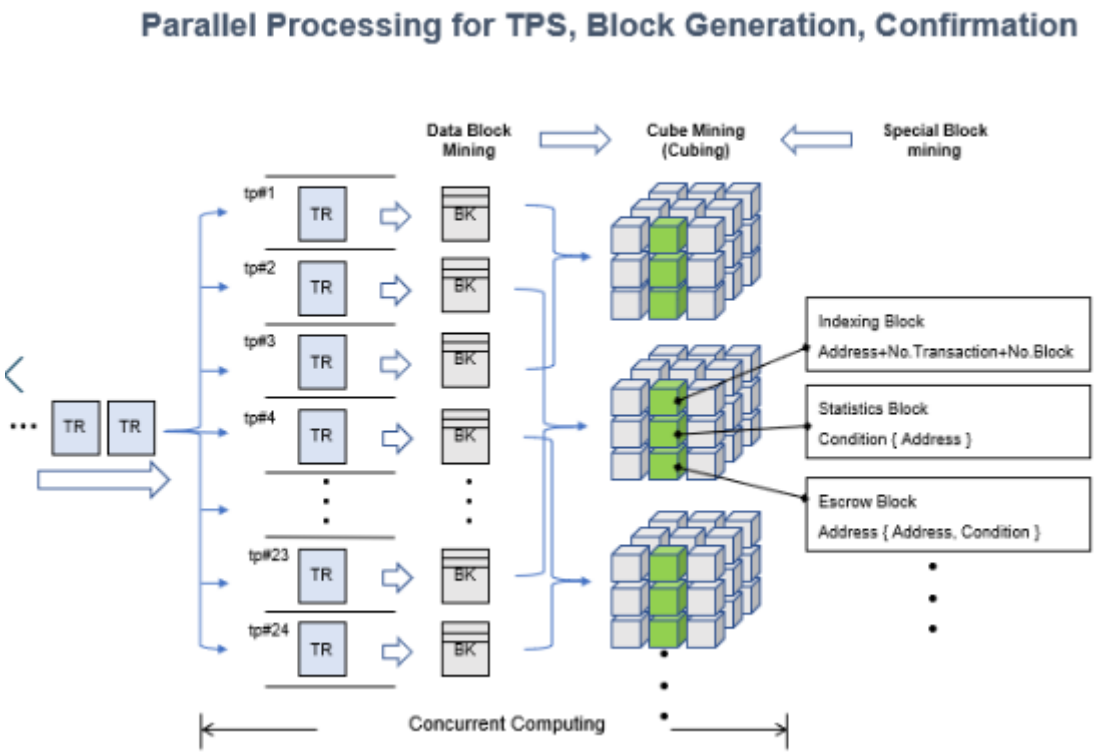
일반블록 : 1 개의 블록은 4MB 이다.
특수블록 : 3 개의 특수블록의 용량은 가변적이고, 큐빙으로 일반블록이 만들어질 때 생성된다.

큐브의 크기 : 특수블록은 특정 크기가 정해진 것이 아니기 때문에 α 라고 정한다. 1 큐브=24 블록*4+α, 즉 1 큐브는 96+α MB 의 크기를 가진다.

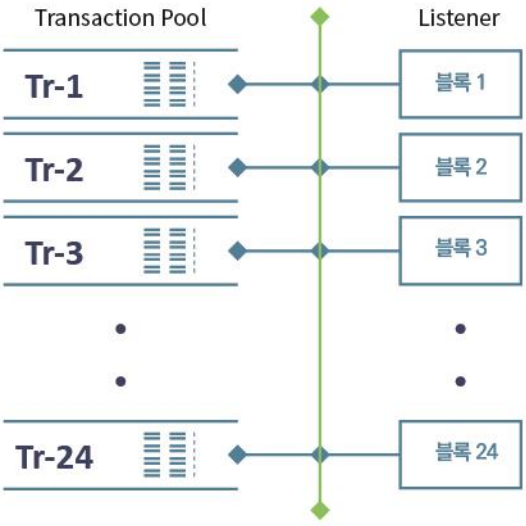
트랜잭션풀에 데이터 도착에서부터 큐브생성까지의 과정

트랙잭션풀에 거래내역 또는 기타정보(입력되는 데이터의 종류가 복수 존재가능, 단 모든 데이터는 해시(암호화)처리되어 데이터의 길이와 사이즈는 동일)가 도착하면 트랜잭션풀에서

Tr1~Tr24 까지의 데이터가 순차적으로 할당되어 일반블록을 생성한다. 특수블록은 이전 큐브가 생성됨과 동시에 이전 큐브의 특수블록이 복사되어 우선적으로 생성된다.



[그림 5]



[그림 6]

각 블록은 각 4MB 의 최대크기를 가지나 경우에 따라서는 4MB 이하일 수도 있다. 4MB 이하의 크기를 가지는 경우, 트랜잭션풀에 데이터가 들어오는 순서는 블록순서대로 들어오고, 1 건의 트랜잭션이 1 개의 블록에 할당되며, 이러한 방식으로 병렬처리가 이루어진다. 채굴자는 24 개의 블록 중 자원이 허락하는 한도에서 중복으로 선택하여 채굴에 참여할 수 있다. 예를 들어, 24 개의 일반블록 중 채굴 선택에서 2,3 번 블록을 선택하여 채굴할 수 있고, 특수블록도 선택해서 채굴할 수 있다.

2.5 POH (Proof of POW+POS hybrid)

POW+POS Hybrid 방식을 채택하여 마이너의 네트워크 참여를 유도하면서 전력 낭비를 줄인다. POW 와 POS 혼용 시 POS 를 계산하여 지급하는 데 시간이 오래 걸리는 단점이 있으나, Statistics Block 통계기능으로 계산에 대한 단점을 없애고 POW 와 POS 비율을 확정했다. POS 참여 조건은 지갑에 최소 5,000 개 이상의 Cube Chain 을 보유하고 있어야 하며, 조건에 부합되는 대상자에게 잔고 비율에 따른 코인보상 지급을 한다. POH 는 POW 와 POS 를 결합한 방식으로, POW 는 프로토콜(컴퓨터 간에 정보를 주고받을 때의 통신방법에 대한 규칙과 약속)이자 프로그램 함수이다. 이는 Proof-of-Work 의 줄임말로 작업 증명 방식을 의미한다.

POW 는 많은 해시(Hash)를 보유한 사람이 코인을 얻을 수 있는 블록을 더 많이 발견할 수 있는 시스템을 의미한다. 서비스 거부 공격과 네트워크상에서 스팸과 같은 서비스 남용들을 처리시간을 요구하는 서비스 요청으로 몇 가지 작업을 요구함으로써 마음을 접게 만드는 경제적인 수단이다.

현재 '채굴'이 가능한 모든 코인은 POW 이며, 현재 가장 대중적이며, 시장이 크고, 인프라가 지속적으로 확대되고 있는 코인들은 대부분 POW 방식이다. 비트코인, 라이트코인, 도지코인 등 알고리즘을 풀어서 코인을 보상으로 얻는 개념의 모든 코인은 다 POW 코인이다. 암호화폐가 POW 코인인 비트코인에서 출발했기 때문에 현재 주류는 당연히 POW 코인이고, 시장의 규모는 POW 가 POS 보다 압도적으로 크다. POS 는 POW 의 가장 큰 문제인 '채굴에 들어가는 많은 비용 및 유지비 (전력사용, 장비 구입비) 절약', '해시의 독점으로 인한 보안상의 문제'를 해결하고자 만들어진 방식이다. POS 의 경우 인터넷이 연결된 PC 1 대만 있으면 모든 준비가 끝나며, 더 좋은 CPU 더 좋은 GPU 같이 더 이상 추가적인 장비가 필요 없다. 코인을 얻는 방법은 각 코인마다 얻은 방식, 양은 다르지만 기본적으로 POS 는 가지고 있는 코인양이 많을수록 더 많은 코인을 지속적으로 얻게 된다. (이자와 같은 개념)

POS 라는 이름과 같이 전체 코인에 대한 많은 지분(Stake)을 보유한 사람이 추가로 발행되는 코인에서 많은 분량을 가져가게 되는데, POW 에서는 '해시'가 이러한 기능을 했다면, POS 는 보유한 '코인'의 양이 기준이 된다. 그래서 POS 방식에는 보안을 위해서 대규모의 해시가 필요하지 않고, 각 개개인이 코인을 보유하고, 지갑을 연동시켜 놓는 것만으로 강한 보안 장벽을 만들어낼 수 있는 것이다. 또한 출시 초기에 대량의 코인이 단기간에 발행되며 차차 줄어드는 POW 와는 다르게 늘 일정한 양이 조금씩 발행되기 때문에 가격이 큰 폭으로 상승 또는 하락하는 경우가 더 적다는 장점이 있다. 또한 채굴에 소모되는 대량의 전기 및 채굴기가 필요 없기 때문에 더 많은 사람이 쉽게 코인을 접하고, 사용할 수 있다. 하지만 가격의 상승 폭이 크지 않기 때문에 '대량의 자금'이 유입되지 않았다는 점(지금 보유할

필요가 적기 때문에), '자금'이 많은 사람이 쉽게 독점할 수 있다는 점, 지분을 통한 이득이 POW 보다 적은 점, 초기 코인의 유포가 공평하지 못한 점 등의 이유가 약점으로 존재한다.

큐브체인은 POW 와 POS 비율이 7:3 으로 시작되어 시간의 흐름에 따라 POS 비율이 높아지고 결국에는 POS 로만 유지되도록 하였다. 초기에 POW 를 높여서 네트워크가 안정적으로 구축되도록 하였고 POS 를 높여가며 네트워크 자원 및 전력 낭비를 줄이는 방식을 사용하였다. POW 와 POS 혼용 시 POS 를 계산하여 지급하는 데 시간이 오래 걸리는 단점이 있으나, 큐브체인의 Statistics Block 을 이용한다면 매번 반복적으로 계산하는 비효율성을 획기적으로 줄일 수 있다. 초기에는 채굴자가 생태계를 조성하는 역할을 하므로 POW 의 비중을 높이지만, 자원낭비 문제가 심각하고 경쟁을 통한 비효율성이 증대되는 문제가 있어서 POW 를 처음에는 높게 가져가지만 점차 비율을 조정하여 POS 로만 가능하게끔 한다. POW 와 POS 의 장점을 시간적으로 배분해서 적정한 장점을 취하게 한다.

3. 암호화 방식

3.1 지갑의 생성

지갑의 생성에서 가장 많이 사용하는 방식은 비대칭형(공개키, 개인키) 암호화 방식이다. 비대칭 암호화 방식은 두 개의 키를 쌍으로 가지며 하나의 키로 암호화하면 다른 키로 복호화 할 수 있다. 두 개의 키 중에 하나는 공개키는 지갑 생성 시 공개키는 지갑 주소로 사용되며, 또 하나는 개인키로 이체 시 비밀번호로 사용된다. 큐브체인은 지갑의 주소와 암호의 생성에서 비대칭형 암호화 방식(Asymmetric Cryptographic Technique)인 RSA(Rivest Shamir Adleman)알고리즘을 사용한다.

3.2 디지털 서명

지갑을 통해 이체하게 되면 디지털 서명의 과정을 거치게 되는데, 이때 암호화 방식은 대칭형 암호화 방식(Symmetric cryptographic technique)인 AES256 을 사용한다.

지갑의 주소와 암호를 생성하는 RSA Algorithm 의 비대칭형 암호화 방식은 키를 노출하여도 해킹할 수 없는 암호전달의 문제를 해결하였지만, 속도가 느린 단점을 가지고 있다. 그래서 키의 교환 상에 어려움이 있지만, 암호화와 복호화 속도가 빠른 장점이 있는 AES256 방식과 혼합하여 RSA 의 단점을 보안 할 수 있도록 한다.

데이터의 크기가 작다면, RSA 로 생성된 공개키와 개인키를 이용하여 디지털 서명 암호화 키를 생성하는 데이터 암호화 처리 방식에 대한 개선이 효율적이지 않을 것이다. 그러나 데이터의 크기가 커질수록 그 개선 효율성은 훨씬 증대될 것이다.

3.3 블록 해시함수

해시함수는 데이터를 고정된 일정 길이의 해시값으로 변환하여 출력하는 함수이다. 이 변형된 데이터는 원본 데이터를 복구하는 복호화는 되지 않고, 데이터의 무결성을 검증하거나 암호를 인증하는 데 사용한다. 블록체인에서 n 번째 블록의 해시값은 n-1 번째 블록의 해시값과 연결된다. 큐브체인에서는 해당 블록 내의 27 개 각 블록의 해시값을 만드는데, 이때 데이터블록에 사용되는 해시 함수는 SHA-256 을 사용한다.

특수블록은 일반 데이터 블록보다 데이터가 점차 더욱 증가하기 때문에 기존의 해시함수와는 다른 해시함수가 쓰여야 하며, 그것은 자체 개발된 CH-S1 함수를 사용한다. 기존의 해시함수를 사용할 시 심각한 속도저하가 일어날 수 있다. 이러한 속도저하를 방지하기 위해 기존과 다른 데이터 추출/압축과정으로 해시 처리 과정 속도를 획기적으로 높인 CH-S1 해시함수를 사용한다.

3.4 큐빙 해시 함수

큐빙을 진행할 때 암호화 방식은 독자적으로 개발한 CHF-Algorism(Cubing Hash Function Algorithm)을 사용한다. 큐브 내 27 개의 블록은 각 블록의 위치에 따라 서로 인접한 블록이 각각 다르다. 육면체의 각 면의 위치에 따라 모퉁이에 위치한 블록 8 개, 중심에 위치한 블록 6 개, 중심을 둘러싼 블록 12 개, 큐브의 정중앙 블록 1 개로 구성된다.

4 가지 구분에 따라서 사용하는 해시함수도 달라지는데, 각각 CH-B3, CH-B4, CH-B5, CH-B6 으로 명명한다. 앞의 CH(Cubing Hash)는 큐빙 해시함수를 뜻하며 뒤의 B(Block)는 위치한 블록에서 큐브내 바로 인접한 블록의 개수를 뜻한다. 큐빙 해시함수는 인접한 블록의 해시값을 이용하여 또 다른 해시값을 만들어낸다.

이렇게 해서 27 개 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 27 블록이 개별적으로 사슬 관계를 만들어 검증한다. 큐브 내 위치 값을 통해 서로의 블록을 검증하게 되며 이때 한 개의 블록만 달라도 전체의 값이 달라진다.

3.5 큐브 해시 함수

큐빙에서 얻어진 27 개 블록의 전체 해시값과 이전 큐브의 해시값을 포함하여 현재 큐브의 해시값을 생성한다. 큐브의 해시값을 만드는데 SHA-384 함수를 사용한다.

4. 특수블록 생성과정

4.1 특수블록의 설정

큐브체인에서는 데이터만을 가지고 움직이는 것이 아니라 데이터 영역과 특수기능의 데이터를 구분하고 확장할 수 있도록 하였다. 암호화폐를 위해서는 3 개의 특수블록을 설정하였지만 다른 애플리케이션 개발을 위해서는 특수블록을 별도로 설정해서 사용할 수 있으며, 이는 Genesis 파일 설정을 통해 가능하다. 특수블록은 코어를 설치할 때 설정만으로 사용할 수 있도록 하였고, 이를 통해서 다양한 분야에 쉽게 적용하도록 설계되었다. 큐브체인에서는 다양하게 정의된 특수블록을 준비하였으며, 향후 지속해서 추가될 예정이다.

4.2 특수블록의 종류

특수블록에는 Indexing Block, Statistics Block, Escrow Block, Format Block, Edit Block 등이 있다. 이 중 3 개의 블록에 대해서는 앞에서 이미 설명했으므로 생략한다.

Format Block

Format Block 은 데이터 블록에 기록될 데이터 포맷이 유연성 있게 변화되어야 할 때 사용한다. 포맷을 결정하는 정보를 변경하면 Format Block 은 데이터의 유효성 검사를 자동으로 진행하며 이를 통해 잘못된 데이터가 담기는 것을 방지하며 사용자나 프로그램의 오류를 방지한다. 데이터형식에 대한 데이터만 보관할 뿐 사용자가 사용하는 일반 데이터는 사용되지 않는다.

Edit Block

Edit Block 은 기존 데이터를 수정할 목적으로 사용된다. 블록체인의 비가역성은 장점이자 동시에 단점이다. 암호화폐에서는 필수적인 요소지만 다른 응용서비스에서는 데이터의 수정이 필요할 수도 있다. 이를 위해서 Edit Block 을 설정하여 수정사항을 쉽게 반영시키고 관리할 수 있다.
수정할 데이터를 Edit Block 에 담고, 원래의 데이터를 참조할 때 Edit Block 에 있는 데이터를 반영하여 제공하는 방식이다. 블록체인의 데이터가 단순히 거래이력으로써의 데이터만 아니라 수정 및 삭제가 가능하게 참조값을 연결 또는 끊게 함으로써 데이터의 수정이 가능하게 된다.

단, 특수블록 중 Format Block 과 Edit Block 은 프라이빗 블록체인을 도입하고자 하는 기관이나 기업을 대상으로 하는 것이다. 24 개의 블록 중 2 개의 블록이 특수블록으로 전환되며, 이로써 22 개의 데이터 블록이 남게 된다. 실제 블록체인의 데이터를 수정하는 형태가 아닌, 수정될 데이터에 블록 데이터를 추가하고 참조할 데이터의 영역 위치를 변경하는 것으로 이해할 수 있다. 즉, 기존 데이터의 수정이 아닌 서비스나 애플리케이션에서 사용할 수 있는 데이터로 변환하는 것을 의미한다. Edit Block 과

Format 블록은 큐브체인(QUB) 발행과는 연관이 없고, 서비스 사업자의 요청에 따라 추가될 수 있는 선택사항의 특수블록이다.

4.3 특수블록이 생성되는 과정

특수블록은 데이터 블록에 기반하여 재가공 된 데이터나 반영될 데이터이다. 필수 특수블록으로 채택되는 3 개의 특수블록은 데이터 블록의 재가공 데이터라 할 수 있다. 특수블록이 생성되기 위해서는 이전 데이터 블록이 있어야 한다. 따라서 최초의 첫 번째 큐브에서는 비어 있는 데이터로 생성된다.

특수블록은 두 번째 큐브부터 생성된다. 특수블록의 생성 시점은 이전 큐브의 형성이 완료되는 동시에 생성이 시작되며, 현재 큐브에 포함될 데이터 블록들이 생성 완료되는 시점에 포함되어 큐빙이 이루어진다. 이러한 프로세스는 특수블록 생성 시간 때문에 발생하는 큐빙의 지연시간을 미리 방지하기 위함이다. 특수블록은 이전 큐브의 특수블록 데이터에서 추출된 내용과 이전 데이터 블록의 내용을 추가하여 누적 반영된다.

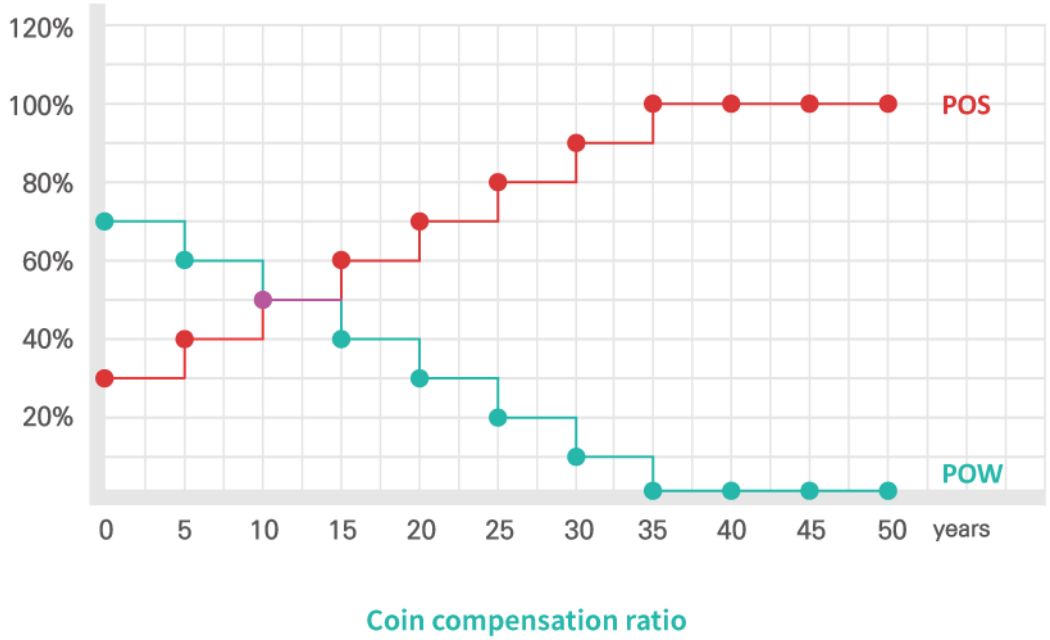
즉, n 번째 큐브의 특수블록은 n-1 번째 큐브까지의 데이터를 담고 있다. n-1 번째 큐브가 완성되는 시점에서 n-2 번째 큐브의 데이터를 담은 특수블록과 n-1 번째 데이터를 합쳐서 만들어지기 시작하며, n 번째 큐빙이 이루어질 때, 데이터 블록과 유기적인 관계를 형성하게 된다. 특수블록은 큐브가 생성되고 큐브와 큐브가 체인화가 이루어지는 시간 동안 생성됨으로 기능적 요소는 확장되지만, 이로 인한 지연되는 시간은 없다. 또한 특수블록의 암호화는 자체개발한 CH-S1 함수를 이용하여 데이터양에 비해 매우 빠른 속도로 해시값을 얻을 수 있다.

5. 합의방식

5.1 POH (Proof of POW+POS hybrid)

큐브체인의 기본 채굴방식은 POW 로 작업증명에 참여한 노드들에게 코인 보상을 한다. 그러나 POW 의 과도한 네트워크 자원 낭비와 지나친 과열 경쟁으로 인한 난이도 상승 문제를 해결하기 위해 POS 의 보상방식을 결합한 POH(Proof of POW+POS hybrid)방식을 채택하였다.

큐브체인만의 POH 방식은 POW 와 POS 를 동시에 진행하면서, 점차 POS 비율을 상승시킨다. 이는 POW 로 인한 채굴의 산업화를 방지하고, 네트워크 자원 낭비를 막는 것을 지향한다.



[표 1]

POW 채굴은 세 가지 방식으로 참여할 수 있으며, 데이터 블록생성, 특수블록생성, 큐빙 작업 시 각각의 항목별로 선택하여 참여할 수 있다.

5.2 POW 보상형태

작업증명에 참여한 노드는 매 큐브가 생성된 후 지급받을 보상이 계산되어 지급된다.

작업의 중복으로 참여할 경우 중복으로 계산되어 지급되며, 항목별로는 합산되어 지급된다.

- 데이터 블록을 생성시 해시값에 추가된 임의값을 찾아내는 연산을 수행함에 따라 보상한다. 이때 24 개의 데이터 블록에 대해서 각각 따로 보상 지급하며 중복 참여시 중복으로 지급한다.
- 특수블록을 각각 생성할 때 해시값 검증에 필요한 연산을 수행함에 따라 보상한다.

- 큐빙의 과정에서 큐빙에 사용되는 암호화 함수 검증하는 연산을 수행함에 따라 보상한다.
- 일반블록 24 개, 특수블록 3 개, 큐빙 1 개으로 구성되며 각각 따로 보상 지급되며, 중복참여시 중복으로 지급한다.

5.3 데이터 블록의 채굴 과정

- 블록의 타임스탬프와 해당 노드의 난이도를 확인한다.
- 블록의 타임스탬프가 이전 블록의 타임스탬프와 비교하여 유효범위인지 확인한다.
- 블록에 포함된 데이터나 거래에 대해 목록을 만든다.
- 블록 헤더의 머클트리를 확인하여 유효성을 확인한다.
- 이전 큐브에서 해당 블록의 해시값을 연결하고 1 차 해시값을 만든다.
- 이전 큐브의 패턴 블록을 이용하여 2 차 해시값을 만든다.
- 블록을 생성하고 노드에 블록 데이터를 전파한다.

5.4 특수 블록의 채굴 과정

특수 블록의 채굴은 큐브체인만이 가질 수 있는 채굴 방식이다.

- 특수 블록의 타임스탬프를 확인하고 해당 특수 블록의 헤더를 확인한다.
- 데이터 블록에서 특수 블록에 추가될 데이터를 추출한다.
- 데이터의 개수를 항목별 소계와 총합계를 계산한다.
- 이 계산에 대한 머클트리를 만들고 확인하여 유효성을 확인한다.
- 이전 큐브에서 해당 블록의 해시값을 연결하고 1 차 해시값을 만든다.
- 이전 큐브의 패턴 블록을 이용하여 2 차 해시값을 만든다.
- 이전 특수 블록에 추가될 데이터를 넣는다.
- 블록을 생성하고 노드에 블록 데이터를 전파한다.

5.5 큐빙의 채굴 과정

큐빙의 채굴은 큐브화라는 독특한 방식의 데이터 구조화를 위한 연산으로 채굴한다.

큐빙의 채굴 과정은 다음과 같다.

- 이전 큐브의 타임스탬프를 확인하고 27 개 블록의 해시값을 확인한다.
- 큐브의 타임스탬프가 이전 큐브의 타임스탬프와 비교하여 유효범위인지 확인한다.
- 27 개의 블록 해시값의 유효성을 확인한다.
- 27 개의 패턴블록 해시값의 유효성을 확인한다.
- 이전 큐브 해시값과 27 개의 블록 해시값을 이용하여 큐브 해시값을 만든다.
- 큐브를 생성하고 노드에 전파한다.

5.6 채굴방식의 다양화

큐브체인은 채굴방식이 다양할 뿐만 아니라 방식에 따른 채굴의 효율성과 난이도가 다르게 반영되었다. POW 는 큐브체인이 초기에 네트워크 구성을 원활하게 하기 위한 목적으로 사용됨으로 다양한 참여자가 참여할 수 있도록 참여 범위를 넓혔다. 채굴프로그램을 통해서 할 수 있고, 참여 수량과 채굴 블록을 결정해야 한다. 채굴에 필요한 연산 함수를 디코딩하는 칩이나 하드웨어 장비를 개발하여 연산 효율성을 높일 계획이다. 이렇게 되면 적은 비용으로 고효율의 채굴이 실현됨과 동시에 무한 과열 경쟁의 채굴 장비에 투자되는 비효율성을 극복할 수 있을 것이다.

5.7 POS 보상방식

POH 는 POW 의 채굴방식과 POS 의 보상방식이 결합한 큐브체인만의 참여방식이다.
큐브체인에서는 노드의 참여와 관계없이 큐브체인의 지갑에서 참여가능하다. 이전 블록기준으로 5,000 개 이상의 큐브체인(QUB) 잔고 보유자에게 보유 수량에 비례하여 지급한다. 단, POS 참여신 수량은 참여기간 동안 이체 불가능 하게 되며, 이체하고자 할 때는 참여수량을 제외하여 이체 할 수 있다. 지급 시기는 현재 블록이 생성되는 기점에 지급하며, 지급 수량은 전체 수량 대비 보유 수량 비율을 계산하여 지급한다. 큐브체인의 Statistics Block 에서 블록마다 POS 대상자의 보유 수량을 저장하기 때문에, 빠르게 보상 수량을 계산하여 각각의 지갑 주소로 전송할 수 있다.

6. 지갑서비스

큐브체인은 활용성 높고 편리한 블록체인 서비스를 목표로 한다. 이를 위해 기본 서비스를 제공하여 큐브체인 활용을 극대화하며 응용 프로그램이나 서비스 개발에 집중될 수 있는 환경을 제공하고자 한다.

6.1 지갑의 제공

큐브체인 지갑은 큐브체인을 이용한 이체 및 내역관리 등의 서비스를 지원한다. 큐브체인 지갑에서는 기본적인 이체, 거래내역 조회 서비스 외에도 여러가지 특징적인 지갑 서비스를 제공한다. 제 4 차 산업혁명을 선도하는 새로운 금융서비스로서, 애플리케이션 이용시 활용성이 높고 사용자의 편의성을 더한 서비스를 추가한 큐브체인 지갑만의 아이덴티티를 보여 줄 것이다.

지갑주소의 도메인 서비스

지갑 도메인 서비스는 한 번에 외우기 힘든 지갑주소를 사용자가 외우기 쉬운 특정 지갑이름으로 매칭해주는 서비스이다. 특정 아이피 주소를 지정된 도메인 주소로 연결시키듯, 사용자가 지정한 지갑 도메인 주소로 특정 지갑주소를 연결시켜 편리성을 증대시킨다. 지갑 도메인으로는 개인이 사용하는 모바일 번호나 이메일 주소를 사용할 수 있으며, 기억하기 쉬운 주소를 사용함으로써 사용자 또는

이체를 할 상대방이 지갑 도메인 주소를 쉽게 기억하여 입력할 수 있도록 도와준다.

예) CWxhQRgBrqZUbj6fj1ftprurb2U9yAFMhu 의 형식을 가진 큐브체인 주소

Abc.com(대소문자 구분하지 않음)와 같은 단순한 문자열을 유저가 임의 선정하여 복잡한 지갑주소를 대신하여 큐브체인 지갑에서 사용할 수 있다. 그러면 Abc.com 를 알려주고 코인전송을 받을 수 있게 된다.

지갑 그룹화 서비스

하나의 지갑에 여러 지갑을 지정된 형태로 묶어주는 그룹화 서비스는, 대표 지갑 주소는 노출하지 않으면서, 연결된 지갑 주소만을 노출시키는 형태의 서비스이다. 사용자가 하나의 지갑에서 여러 개의 연결된 지갑 주소를 관리할 수 있으며, 목적에 따른 다수의 지갑을 개설 또는 분류할 수 있다. 그룹화 서비스를 활용하여 자동이체 서비스 또는 연결된 지갑 주소를 편리하고 손쉽게 관리할 수 있다.

자동이체 서비스

자동이체 서비스는 사용자가 스스로 설정한 이체조건(수취인, 입금 지갑 주소, 금액, 주기 등)에 따라 특정 지갑 주소로 주기적으로 이체해주는 서비스이다. 자동이체 서비스를 이용할 경우 따로 수취인에게 지로징표를 고지받지 않아도 지정된 날짜에 사용자의 지갑에서 지로대금을 출금하여 수취인에게 일괄 입금하고 그 내역을 통지받을 수 있다.

지갑 메시지 전달 서비스

지갑을 사용하는 사용자를 대상으로 거래 후 확인 메시지 또는 서비스 요청에 관한 메시지를 전달할 수 있는 기능이다. 이체 완료 메시지 또는 잘못된 거래에 대한 반환 요구 등의 용도로 사용 가능하며, 메시지는 애플리케이션 알림 서비스, SMS, E-mail 등과 같은 용도로 활용된다.

6.2 큐브체인 활용 기반서비스

큐브체인 활용 기반서비스는 블록체인 기반의 큐브체인 기술을 여러 분야의 비즈니스 모델로 사용할 수 있도록 기반서비스 플랫폼을 구축 후 배포되는 서비스이다. 이와 같은 목적은 기업 또는 개인이 큐브체인을 활용하여 폭넓은 큐브체인 생태계를 만들도록 개발환경을 형성하고, 더욱 확장된 2 차 큐브체인 응용프로그램 개발을 위한 초석을 제공한다. 큐브체인을 활용한 기반서비스는 비즈니스 모델을 직접 적용할 수 있는 완성된 형태로 발전시켜 나아갈 것이며, 이를 템플릿 앱 형태로 별도 배포할 예정이다.

큐브체인 개인정보 인증 서비스

범용적으로 개인의 이메일 또는 핸드폰 번호, 핀 번호 등을 큐브체인에 저장하여 사용할 수 있는 개인 인증 서비스이다. 사용자는 큐브체인에 저장된 본인 개인정보를 웹 또는 애플리케이션 상에 제공할 수 있다. 큐브체인에 저장된 개인정보는 보호된 데이터를 기반으로 본인 인증 시에만 오픈됨으로 제삼자에게 노출되지 않으면서, 개인정보를 제공하고자 하는 사용처에 안전하게 연동시킬 수 있다.

큐브체인 메시지 전달 서비스

P2P 로 서비스가 진행된다는 점에서 기존 메시지 전달 서비스와 차별된다. 주고받은 메시지 데이터는 큐브체인으로 전송되어 저장된다. 메시징 데이터는 후순위로 저장되기 때문에 사용자들은 데이터 전송 지연 없이 서비스를 이용할 수 있다. 큐브체인으로 분산 저장된 데이터들은 사생활 보호 기능이 적용되어, 인증자에게만 오픈되는 메시지로 변환시킬 수 있다. 사생활 보호 저장기능은 제삼자에게 노출 또는 해킹당하지 않는 보호 장벽으로써 사용자들이 안전한 채팅 서비스를 이용할 수 있도록 한다. 또한, API 를 통해 채팅방 개설, 참여자 설정, 참여자 대화 내용을 전달함으로 활용성을 증대를 시킬 수 있다.

큐브체인 파일저장 서비스

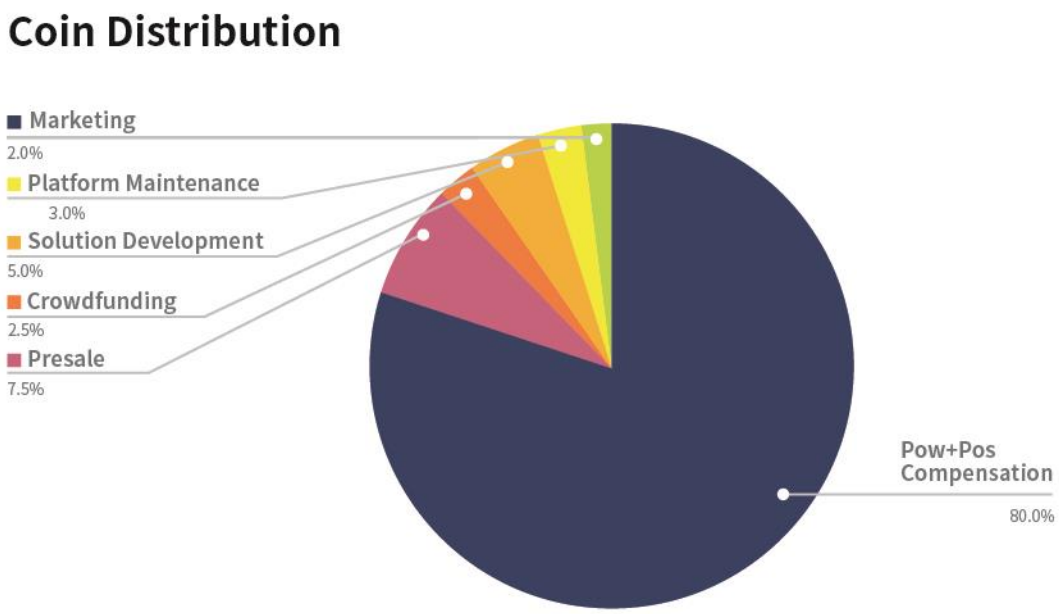
큐브체인 파일 저장 서비스를 사용하면 사용자가 특정 파일을 큐브체인을 이용하여 분산 저장하여 특정 파일을 공공의 목적으로 사용하거나 공인된 파일로 등록할 수 있다. 문서파일이나 이미지 파일을 등록하는 서비스를 통해 사용자는 중요한 파일을 안전하게 보관할 수 있다. 템플릿 앱이나 애플리케이션과 연동되는 서비스를 통해 파일의 활용성을 높일 수도 있다.

큐브체인 데이터베이스 서비스

큐브체인의 데이터베이스 서비스는 블록체인의 데이터를 데이터베이스처럼 활용성 높게 사용하기 위한 서비스이다. 큐브체인의 Edit Block 과 Format Block 을 사용하여 데이터를 구조화시켜 관리할 수 있는 장점을 제공한다. 데이터를 관리하는 것을 표준 SQL 문을 통해서 저장, 수정, 삭제가 가능하도록 API 를 제공한다. 아울러 관계형 DB 로 큐브체인 데이터의 큐브 생성 시 마다 데이터를 보내 연동시키는 기능을 제공한다.

7. 큐브체인 발행수량

7.1 큐브체인 배분



[표 2]

7.2 POH 비율

큐브체인은 50 년 동안 총 120 억 개의 코인을 발행하며 5 년 간격으로 POW 와 POS 의 비율이 조정이 된다.

구 분	5 년간 큐브체인 보상수량	POW : POS 비율	5 년간 POW 보상수량	5 년간 POS 보상수량
~5 년	960,008,400	7:3	672,005,880	288,002,520
5~10 년	960,008,400	6:4	576,005,040	384,003,360
10~15 년	960,008,400	5:5	480,004,200	480,004,200
15~20 년	960,008,400	4:6	384,003,360	576,005,040
20~25 년	960,008,400	3:7	288,002,520	672,005,880
25~30 년	960,008,400	2:8	192,001,680	768,006,720
30~35 년	960,008,400	1:9	96,000,840	864,007,560
35~40 년	960,008,400	0:10	-	960,008,400
40~45 년	960,008,400	0:10	-	960,008,400
45~50 년	960,008,400	0:10	-	960,008,400

[표 3]

8. 큐브체인 기술활용

8.1 RPC 서버

큐브체인에 참여한 노드는 RPC 서버로 사용할 수 있다. RPC 서버로 이용할 경우 원격으로 함수를 실행할 수 있기 때문에, 큐브체인을 활용하여 원격지에서 노드를 제어할 수 있다. 큐브체인 네트워크를 구성하고 있는 노드에서 RPC 서버를 사용하여, 큐브체인에 가담하지 않은 PC 나 서버를 통해 큐브체인의 데이터를 참조 또는 노드 제어를 할 수 있다. 원격지에 대한 제한 설정이나 기능의 범위 설정도 가능하여, 원격지의 통제가 가능하다.

8.2 API

큐브체인 RPC 서버와의 API 를 만들어 제공함으로 원격지에서 쉽게 노드 관리가 되도록 한다. RPC 서버의 API 의 전달과 응답 모두 기본적으로 JSON 형식을 사용한다. 상세 API 문서는 추후 큐브체인 진행 시 별도 오픈할 예정이다. API 의 사용 명령어 및 간단한 예시는 다음과 같다.

rpc_ver : RPC 서버의 현재 버전 정보를 구해 온다.
curl -X POST --data '{"callno":100,"com":"rpc_ver","vars":{},rmsg:"서버 버전 확인요청"}'

network_info : 서버의 네트워크 참여 형태와 참여 노드 및 활성화 상태에 대한 정보를 구해온다.
curl -X POST --data '{"callno":100,"com":"network_info","vars":{},rmsg:"네트워크 정보 확인요청"}'

p2p_info : p2p 관련 정보를 구해온다.
curl -X POST --data '{"callno":100,"com":"p2p_info","vars":{},rmsg:"peer to peer 정보"}'

cube_pow : POW 참여 여부에 대한 정보를 얻을 수 있다.
curl -X POST --data '{"callno":100,"com":"cube_pow","vars":{},rmsg:"POW 상태 확인"}'

cube_pos : 전달된 지갑주소의 POS 해당 여부에 대한 정보를 얻을 수 있다.
curl -X POST --data '{"callno":100,"com":"cube_pos",
"vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"POS 상태 확인"}'

cube_height : 현재 진행 체인의 높이, 즉 현재까지의 큐브 개수를 구한다.
curl -X POST --data '{"callno":100,"com":"cube_height","vars":{},rmsg:"체인수를 확인"}'

cube_balance : 전달된 지갑주소의 잔고를 확인한다.

curl -X POST --data
'{"callno":100,"com":"cube_balance","vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"지갑의 잔고 확인"}'

cube_transaction_count : 전달된 지갑주소의 거래횟수를 확인한다.

curl -X POST --data
'{"callno":100,"com":"cube_transaction_count","vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"지갑의 거래횟수 확인"}'

cube_transaction_list : 거래의 해시값 즉 거래 아이디를 추출한다. 특정 주소의 거래내역이나 특정 큐브 높이의 거래내역을 찾을 수 있다.

curl -X POST --data
'{"callno":100,"com":"cube_transaction_list","vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"거래내역 전송"}'

cube_transaction_detail : 거래의 해시값의 내역 정보를 전달한다.

curl -X POST --data
'{"callno":100,"com":"cube_transaction_detail","vars":{"tr_hash":"6e8dd67c5d32be8058bb8eb970870f072445675058bb8eb97f"},rmsg:"거래 또는 데이터 전송"}'

cube_transaction : 전달된 지갑주소간 거래를 진행한다.

curl -X POST --data
'{"callno":100,"com":"cube_transaction","vars":{"address_from":"Q9eeb85d32cf465507dd71d503d8a85d32s","address_to":"Qd2be8058bb8eb970870f0723315b60e8dd","amount":1.2,"fee":0.0001},rmsg:"거래 또는 데이터 전송"}'

cube_transaction_data : 특정 데이터를 큐브체인에 올린다.

curl -X POST --data
'{"callno":100,"com":"cube_transaction","vars":{"address_from":"Q9eeb85d32cf465507dd71d503d8a85d32s","address_to":"Qd2be8058bb8eb970870f0723315b60e8dd","data":{"no":1,"id":"cubechain","chapter":"cubechain_api","book_name":"큐브체인 백서"}},rmsg:"일반 데이터 전송"}'

9. 결론

블록체인 기술은 4 차 산업혁명을 이끌 기반 기술로 자리매김하기 위하여 발전하고 있다. 암호화폐 시장뿐만 아니라 전 산업에 걸쳐 데이터의 자유로운 공유와 안전성을 동시에 확보하는 기술로 대중화될 날이 머지않았다. 큐브체인은 기존 블록체인의 단점을 보완하여 블록체인 기술발전에 기여하고자 한다. 큐브체인이 4 차 산업혁명의 선도적 역할을 하길 기대하며 동시에 다양한 분야에 널리 활용되길 바란다.