RICH CASH

RICH CASH COIN

WHITE PAPER

2018.05.ver

목차

- RICH CASH 탄생 배경
- RICH CASH의 필요성
- RICH CASH의 On – Line 플랫폼
- RICH CASH의 비즈니스 플랜
- RICH CASH 네트워크
- RICH CASH 작업증명
- RICH CASH 블록생성과 보상체계
- RICH CASH 암호화 알고리즘
- RICH CASH 스펀지 구조
- RICH CASH INSIDE
- RICH CASH 트랜잭션의 처리 및 승인
- RICH CASH POLICY

RICH CASH의 탄생 배경 1

- 글로벌 네트워크 회사는 기존 Off - Line 마케팅 방식에서 On - Line으로 전환하는 형태로 진화되고 있다.
  기존 Off – Line의 구조는 사람과 사람의 만남 방식을 통한 유통방식으로 시간과 장소의 한계가 발생하게 된다. 이를 글로벌화 하기 위해서는 시간과 장소 비용을 절감하는 On – Line상의 마케팅 방식으로 On – Line 쇼핑몰, 각종 SNS, 오픈 마켓, 소셜 커머스 등을 통한 네트워크를 확산하고 있다. 이는 지역과 언어의 장벽을 허물며 세계가 하나가 되는 네트워크로 자리매김을 할 수 있는 구조가 된다

- 물류 및 유통은 글로벌시대에 맞추어 발전하고 있으나, 결제의 구조는 국가간의 규제와 각종 수수료 등으로 인해 시대의 발 맞춤에 편승하지 못 하는 것이 현실이다.
  이를 해결하기 위한 방안으로 RICH CASH가 지불결제 수단으로 탄생하게 된다.

- RICH CASH는 국가간 누구나 자유롭게 거래를 할 수 있는 탈 중화의 기본이 되는 지불결제 수단이다.

- 전세계 유명 대기업 조차도 가상화폐 시장에 뛰어들고 있다. 그러므로, RICH CASH는 가상 화폐를 이용한 On - Line 네트워크 회사를 설립하게 되었다.

- 네트워크 형태여서 매출에 따른 커미션이 발생한다. 매출과 커미션을 지급하는데 있어서 각 나라별 통화가 다르기 때문에 각 지역별 지사를 두어야 한다. 물론 지사 없이 달러로 지급하는 회사도 존재하지만 환전 수수료가 비싸고 여러 가지 불편한 상황이 발생하게 된다.

- 인터넷 쇼핑몰을 기반으로 하여 전 세계를 하나로 묶으며, 네트워크 마케팅 글로벌 사업의 단점 이었던 지사 설립은 On - Line 국제암호화폐거래소가 환전소 역할을 하여 매출 및 커미션 지급을 원활히 이루어 지게 하면서 해결할 수 있다.

- RICH CASH는 두 가지 마케팅의 장점을 모을 수 있는 매개체가 될 것이다.

RICH CASH의 탄생 배경 2

잘게 쪼개진 토큰 거래는 자금모금, 크라우드 펀딩, 금융상품의 블록체인 상의 거래를 활성화할 것이다. 가벼운 클라이언트를 통해서 설치 과정은 쉽게 이루어지며, 최종 사용자들의 진입장벽이 낮아진다.

'모든 가능한 블록체인 기술의 어플리케이션이 시도될 것이며 그 중 p2p 디지털 화폐의 사용 빈도가 가장 높을 것이다.' (Ryan X Charles)

우리는 유통시장에서 화폐가 가지는 유용함과 한계를 이미 경험했으며 또한 부동산개발 시장에서 금융의 중요성을 이해하고 있다. RICH CASH COIN 은 Nxt 와 Wave 코인이 제시한 방식을 응용하여 두 시장에서의 화폐가 가진 역할을 충실히 이행하며 기존의 한계를 극복하고자 한다.

기존의 한계라 함은

1. 대규모 자본 외 소규모 자본은 펀드에 참여하기 어려움
2. 펀드에 참여한 경우라도 사업진행상황을 지속적으로 관찰하기 어려움
3. 수익 배당 절차의 투명성을 담보하기 어렵고 배당 순위가 떨어짐

이 부분에서 어려운 것은

1. 유통시장과 부동산개발시장에서 사용되는 코인 또는 토큰은 각자 격리되어야 한다는 것이다. 두 시장은 위험과 수익률이 상이하기 때문이다.
2. 두 시장에서 사용되는 코인은 서로 보완 관계를 가질 수 있는가?

우리는 Ripple 과 Wave 를 통해 위에서 제시한 문제점을 해결하였고 비즈니스 플랜을 통해 RCS의 유용성을 밝히게 될 것이다.

- - 커스텀 토큰 생성, 삭제, 전송
- - 분산 토큰 거래소, 매수가와 매도가를 매칭시킴
- - 어떤 커스텀 토큰을 다른 것과 교환할 수 있다. (asset-to-asset 트레이딩). 각국의 화폐와 연동되는 토큰을 만들 수도 있으며, 따라서 전통적인 거래 인프라를 재현할 수 있다.

RICH CASH의 필요성

- 가치의 전송을 위해서 메인 네트워크 토큰을 사용하는 것은 상당히 자연스러운 일이지만, 문제점도 몇가지 발생한다. 유동성과 변동성이 큰 코인들을 사용하게 되면 판매자에게 상당한 부담이 된다.

- 분산 화폐의 가치의 저장고로써의 사용을 방해하는 불안정성을 완화하기 위해서 화폐로 사용되는 총 토큰의 양은 (적어도 기술의 개발 초기 시점에라도) 제한되어야 한다.

- 국가별로 중앙화된 블록체인 화폐를 공개적으로 만들게 되면, 외부적인 금융기관이 등장하는 셈이다. 그들의 역할은 실제 화폐 자산의 부족한 유동성을 확장해주며, KYC/AML 과정을 제공할 수 있다. 지불 인프라를 유지하는 것은 분산 블록체인으로 완전히 아웃소싱 된다.

- 국가적인 화폐를 블록체인에 기록하는 방법은 Nxt 블록체인 상에서 CoinUSD 토큰으로 시도된 적 있다. 마치 Ripple의 게이트웨이 접근방식과 유사하다. 이러한 전략이 새롭게 등장하는 블록체인과 경쟁할 수 있고, 금융기관이 열린 블록체인과 함께 일할 수 있도록 유도한다.

- 금융기관 및 기업에게 블록체인이 커뮤니티 기반 프로젝트의 기능을 구현하는 효과적인 틀이라고 생각한다. 블록체인 기술은 특성상 고빈도의 거래를 지원할 수는 없다. 중앙화된 해결책은 다량의 거래량을 순식간에 해결할 수 있을 것이다. 하지만 이것이 필수적인 것은 아니다. 블록체인은 자연스럽게 운영되어야 한다. 예를 들어 크라우드펀딩 토큰을 발행하고, 금융적인 흐름을 커뮤니티 안에서 관리해야 한다.

- 킥스타터와 같이 미래에 출시될 상품으로 일정 금액을 투자 받는 방식이 존재하고 있지만 명백한 한계가 존재한다. 기존 방식의 투자자는 투자한 만큼을 다른 누군가에게 중도에 판매하기 어렵다. 반면 블록체인 기반의 시스템에서 중도판매는 상당히 자연스러운 것이며, 블록체인에서 RCS는 교환이나 이체가 용이하다.

- 증권의 발행은 금융감독원의 규제를 받는다. 토큰들은 증권과 비교될 수 있는데, 코인의 가치가 상승할 것으로 예상되거나 이익을 배당할 것으로 예상되는 경우에 그러하다. 그러나, 블록체인은 완전히 규제되지 않는 특성이 존재하며 증권에 비해 용이하게 발행되고 거래될 수 있다.

- 코인의 가치가 각 사람 만다 다르게 느껴지는 것은 다음의 원인에 있다.
- 어떤 자산의 가치는 그 자산을 보유함으로 유입되는 기간별 현금의 흐름 예상액과 현금흐름을 각 기간의 이자율로 할인한 금액을 합한 금액이다.. 자산을 매입하여 보유하여 얻는 순이익을 공식으로 표현하면 다음과 같다.

- 위 공식에서 IRR은 내부순이익률이라 불리는데 주로 자신이 조달한 자본의 이자율로 쓰인다. 이 이자율은 위험프리미엄이 포함되며 위험을 선호하는 정도에 따라 가치가 상이하게 표현된다.
- RCS는 이 같은 가치 변동성을 완화하여 안정성을 부여하고자 한다.

RICH CASH의 On – Line 플랫폼

- 글로벌 네트워크 회사는 모든 업무를 인터넷 쇼핑몰에서 이루어 질 수 있는 플랫폼을 구축하였다.
  이 인터넷 쇼핑몰 플랫폼에서 구매, 반품, 커미션 지급 등 모든 화폐의 기능은 RICH CASH를 사용하여 결제하고 지급하는 시스템으로 일원화 시켰다.
  또한 각 국가별로 다른 통화로 발생되는 문제점들과 불편한 사항은 On - Line 국제 암호화폐 거래소 플랫폼을 사용하여 누구나 쉽게 가입하여, 국가간 외환 거래를 용이하게 하여 거래하고 시세의 차익과 이익에 대한 비전을 현실화 하며, 이를 자국통화로 현금화할 수 있도록 해결하였다.

- RICH CASH는 On - Line 쇼핑몰 플랫폼을 이용하여 전세계를 하나의 마켓으로 구현하였다. 각 나라의 상품을 플랫폼에 등재하며, 세계의 어느 나라 사람이든 질 좋고 이국적인 상품, 또는 상품화되었지만, 구매과정이 불편하고 어려워서 구매하지 못하는 제품을 쉽게 구매 할 수 있도록 만드는 플랫폼이다.
  초기 플랫폼에 등재되는 제품군은 화장품, 건강식품, 뷰티제품(케어), 명품(자동차, 가방, 시계, 지갑, 벨트 등)이며, 제품군은 점차적 확대 개발 할 예정이다.
  이런 제품들은 구매자가 구매의사를 표현하고 결제가 이루어지며, 해당 국가에서 배송되는 시스템으로 쉽게 접할 수 있도록 만들어 진다.

- 또한, 판매 방식이 일반 소비자의 계층과 네트워크 마케팅 계층에서도 사용 가능하도록 구현하였다.

- 전세계의 제품이 하나가 되고, 전세계의 구매자가 하나가 되는 플랫폼이다.
  이를 구매하는 결제 수단은 RICH CASH로 가능하게 된다.

- RICH CASH는 글로벌을 하나로 묶는 하나의 연결고리로 거듭난다.

RICH CASH의 비즈니스 플랜 1

- RICH CASH는 글로벌 네트워크 On - Line 쇼핑몰의 기축 통화로 사용되고 30만명 이상의 다국적 회원들에 의하여 사용되어 진다. 제품의 구매 및 커미션은 RICH CASH만을 사용한다.

- 현재 30만명의 회원이 주기적으로 거래하는 암호화폐는 거의 없으며 이렇게 확실한 사용처에서 충분한 거래량을 확보한 RICH CASH는 사용처가 불분명한 대부분의 알트코인들과 비교하여 경쟁 우위에 있다.
  또한, On - Line 쇼핑몰의 글로벌 네트워크 계층과 일반 계층이 하나가 되어 움직임으로 시장 경쟁력과 소비자 권익에 한걸음 더 나아가게 된다. 이는 더 많은 소비자와 회원을 만들게 되고 이 또한, RICH CASH의 글로벌 최고의 자리에 기반이 되는 구조를 만들어주게 된다.

- 네트워크 마케팅에 이은 인터넷 쇼핑몰 알리바바, 아마존닷컴 등은 인터넷 상에서 전 세계를 하나로 통합하여 별도로 지사를 운영하지 않아도 물류 유통이 가능하게 하였다.
  물론 인터넷 쇼핑몰은 네트워크 방식이 아니기에 커미션을 지급하지 않고 매출을 비자 혹은 마스터 카드로 하면 되기에 가능한 일이었다.

- 이 두 가지 마케팅의 장점만을 모아서 새로운 마케팅 플랫폼을 만들었고 매출이나 커미션을 그 지역의 통화로 바꾸어 주어야 하는 문제점은 RICH CASH를 사용하여 해결했다.

RICH CASH의 비즈니스 플랜 2

- 선 채굴 1차 발행량 200,000,000RCS는 유통시장에 사용된다. 거래에 사용될 재화의 시장 가격과 연동시킴으로써 코인의 내재가치를 유지하게 될 것이다. 우리 온라인 쇼핑몰의 소비자들은 각자가 필요로 하는 물품을 구매하는데 현금대신 RCS를 사용하게 되고 구매에 필요한 RCS가 시세를 초과하게 되면 일정한 RCS를 보유한 유저에게 Airdrop함으로써 코인을 보유한 유저는 이익을 얻고 코인의 시세는 재화의 시장가격과 같은 수준을 유지하게 된다. 쇼핑몰 운영 이익 또한 코인의 가치를 상승시키게 된다.

- 또한, 부동산개발시장에 사용된다. Target 부동산의 투자 규모를 고려하여 시장에 유통될 것이며 완성된 건물의 각 호실과 교환할 권리를 시장가치와 연동하여 부여 받게 될 것이다. 즉 유통 코인 수는 해당 타겟 부동산 개발에 필요한 자기자본과 투자로 인한 이익의 한도 내에서 발행량이 결정된다는 뜻이다. RCS 투자 부동산 1호 사업계획서에서 자세하게 논의하기로 한다.

- 두 시장에서 사용될 코인은 최초 거래 관리 지갑을 별도로 지정하여 상호간 교란되지 않도록 제한 관리하게 될 것이나, 관리자의 승인으로 상호 교환은 가능하게 된다.

- 부동산 개발 지갑을 통한 코인은 실물 부동산의 구입, 중개비, 임대료, 관리비의 납부에 사용될 예정이다.

- 일정 시기가 되어 Target 투자 부동산의 총 투자 금액이 200,000,000RCS에 이르게 되면 부동산 투자 코인은 하드포크 또는 코인 스왑을 통해 부동산 전문 코인으로 전환하게 되며 RCS는 유통전문 코인과 부동산 전문 코인으로 분리, 운영될 것이고 그 기간은 1년 6개월 내지 2년이 소요될 것으로 예상한다.

- 유통 시장에 사용될 RCS는 상장을 원칙으로 하고, 부동산 투자에 사용될 RCS는 Private sale을 원칙으로 하되 상호간 가치 warranty를 고려하여 설계한다.

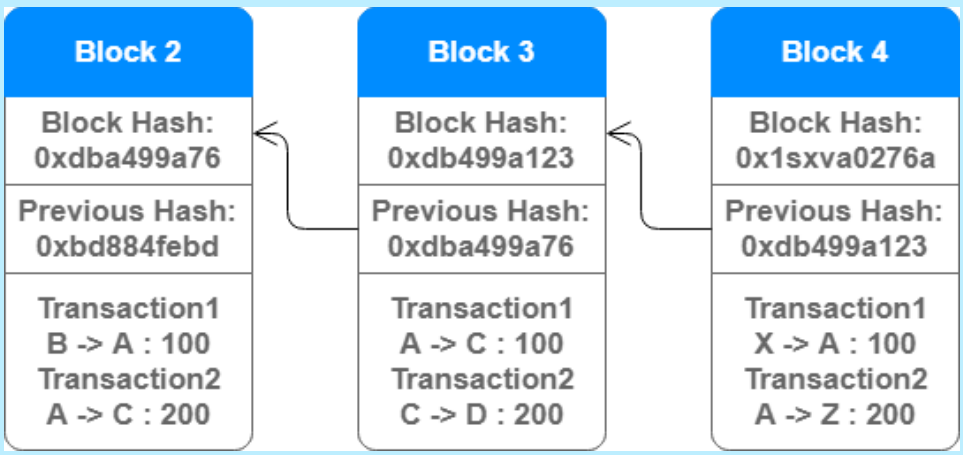
RICH CASH의 비즈니스 플랜 2

- Target 부동산
- 사업명　RCS 영등포 오피스텔 신축사업
- 위　치　서울시 영등포구 영등포동1가 121-3
- 지　구　1종지구단위(일반상업)
- 대　지　237.92평
- 연면적　1,587.52평
- 용적율　590.41%(예상)
- 호실수　상가 1실　오피스텔 162실 (9.42평 138호실, 11.37평 24호실)
- 총매출　30,153,860,000
- 토지비　9,000,000,000
- 공사비　8,173,897,000　공사관련비　1,271,919,000　제세공과금　814,439,000
- 판매비　2,850,646,000
- 보존등기　245,880,000
- 금융비　2,525,385,000
- 사업익　3.626.477.000
- 분양성　매우 우수

- 현재 상태
- 토지　토지계약완료　토지사용승낙서 발급
- 시공　아이렉스 건설㈜　트윈건설㈜　시공참여의향　공사비 견적 산출중　bidding 예정
- 금융　수협중앙회 역삼금융센터,　오케이 저축은행, 우리은행　대주단 참여 의향
- 신탁　국제신탁　하나자산신탁　무궁화신탁　코리아신탁 신탁참여의향
- 신탁비 및 금융비 절감을 위해 담보신탁 대리사무 진행예정(자기자본 50억 조건)
- 분양　2개월 판매 책임조건(미판매 물량 전액 인수) 따라서 매수 의향 있는 분은 미리 의향서 제출 요망
- 설계　5/24일 영등포구청 심의도서 접수.　담당자와 인허가 문제 구두 협의 완료한 상태
- 착공 및 분양　2018년 10월 예정

RICH CASH 네트워크

블록체인 네트워크는 크게 블록체인 노드와 블록체인 클라이언트로 구성된다.
노드는 트랜잭션을 보관, 승인하고 분산 합의의 역할을 담당하며, 클라이언트는 트랜잭션을 생성하고, 거래내역을 확인하는 역할을 한다.
노드는 두 종류의 데이터 베이스를 가지고 있는데, 하나는 올바른 트랜잭션을 모두 보관하는 블록체인 트랜잭션 보관 데이터 베이스이고, 다른 하나는 저장된 트랜잭션을 어플리케이션에 적용하는 어플리케이션 데이터 베이스이다.
노드가 가지고 있는 위의 첫 번째 DB가 바로 블록체인 이라는 특이한 구조로 설계되어 있다.
트랜잭션을 기록한 블록은 P2P네트워크를 통해 전파되며, 여러 블록 중에서 사전에 합의된 방식에 의한 올바른 블록을 이전 블록에 이어나가게 된다.



RICH CASH 작업증명

RICH CASH는 기본적으로 작업증명방식의 합의 알고리즘을 채택한다.
작업 증명은 keccak 해시 함수를 이용한 암호화 해시 값을 찾는 과정이다.
RICH CASH의 작업증명방식은 기본적으로 알려진 비트 코인의 그것과 유사하다.
하지만, 기존의 작업증명방식은 대량 트랜잭션으로 인한 한계와 블록 생성 타임 10분이라는 느린 속도의 한계를 가지고 있다.

RICH CASH은 이러한 문제점을 극복하고자 **Keccak(SHA-3) 해시 함수**를 이용하여 GPU 방식의 작업증명 방식(Proof of Work)을 채택 하였다.

단, 공개 채굴을 위한 매장된 코인의 블록 간 발생시간은 5분이며, 일일 블록 수는 288 블록이 생성되며, 블록 보상은 40 RCS이며, 1일 최대 채굴보상 수량은 11,520 RCS로 구분된다. 난이도는 1블록당 난이도를 적용한다.
RICH CASH 의 가장 큰 특징은 지불 결제 수단 으로서의 기능과 기술적인 부분에서의 5분 단위의 최대 블록 수와 블록 생성에 따른 보상수량을 정해놓아 공개 채굴이 가능하게 만들었다는 점이다.

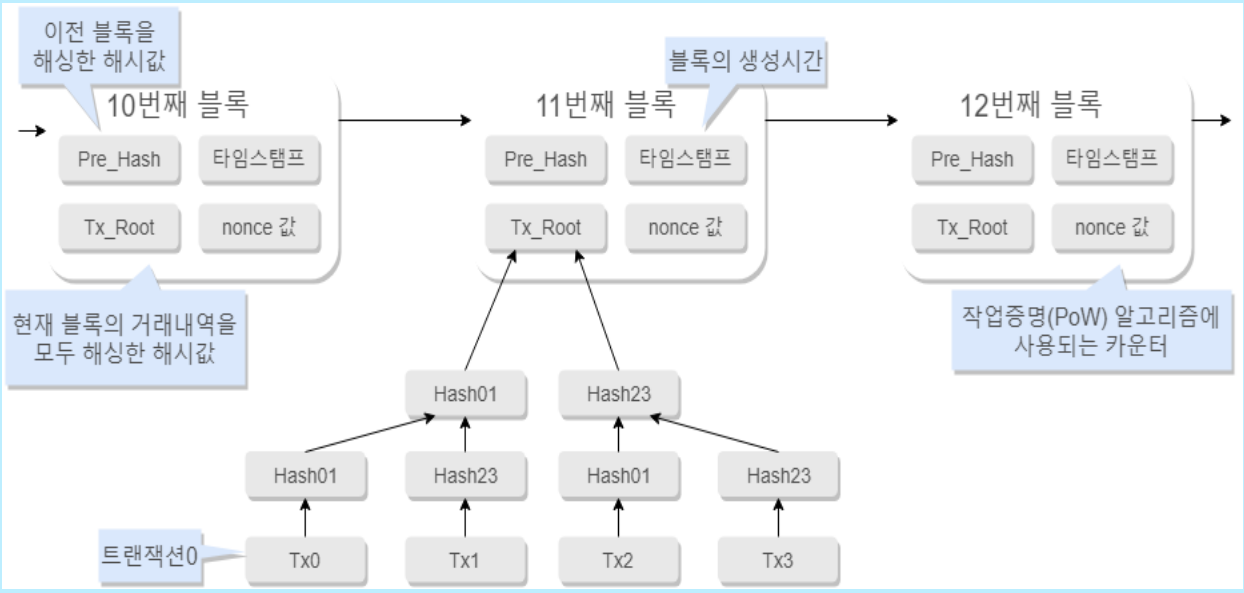
보통 지불결제 수단으로서의 코인들은 100%를 모두 선 채굴하여 사용하지만, RICH CASH는 80%만 선 채굴하며, 20%는 공개채굴을 적용한다는 점이다. 유통되고 사용되는 코인 외에 자유로운 채굴을 통해 참여를 하는 유저를 확보함을 바탕으로 두고 있다.

공개 채굴되는 2.2억 RCS의 총 채굴 기간은 약 52년으로 설계되었다.

코인의 최초 0 ~ 9번째 block까지 보상 코인은 0 RCS이며,
10번째 block의 보상이 8.8억 RCS가 된다.
11번째 이후부터 각 block 당 보상은 8 RCS로 고정된다.
채굴 코인 총액이 2.2억 RCS가 되는 순간(5,500,010 blocks)부터 각 block 당 보상 코인은 0 RCS가 된다.

RICH CASH 블록생성과 보상체계

RICH CASH 블록의 생성 시간은 5분 이내이다. 일일 블록 수는 288 블록이 생성되며, 블록 보상체계 은 40 RCS이며, 1일 최대 채굴보상 수량은 11,520 RCS로 구분되어지며, 1블록생성당 난이도는 상향 조정되어 보상을 적용하게 된다.



RICH CASH 암호화 알고리즘

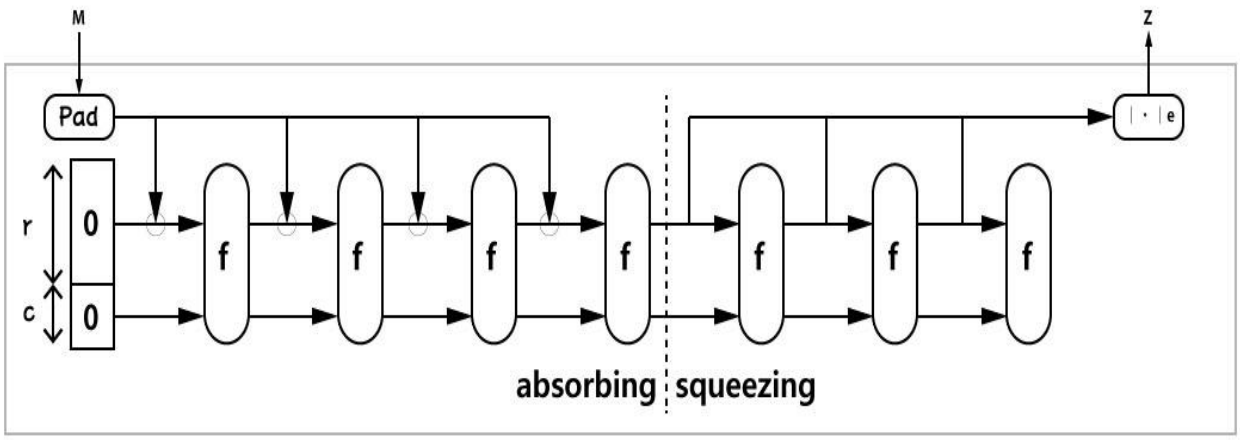
암호 알고리즘 중 해시 함수(SHA : Secure Hash Algorithm)는 메시지 무결성 코드나 전자서명 등 시큐리티의 다양한 분야에서 사용되는 필수적인 암호알고리즘으로, 1993년 SHA-0 이 발표된 이후, SHA-1, SHA-1의 변형인 SHA-2계열의 SHA-224, SHA-256, SHA-384, SHA-512 등이 발표되었다.

SHA-1은 SHA 함수들 중 가장 많이 쓰이며, TLS, SSL, PGP, SSH, IPSec 등 많은 보안 프로토콜과 프로그램에서 사용되고 있다.
SHA-1은 이전에 널리 사용되던 MD5를 대신해서 쓰이기도 한다. 하지만, SHA-0 와 SHA-2 에 대한 공격이 발생하였고, MD5의 취약성이 발견됨에 따라, SHA-1과 큰 차이가 없는 SHA-2 또한, 언제 공격받을 지 모르는 상황에 놓이게 되었다. 비트코인은 SHA-2로 분류되는 SHA-256 알고리즘을 사용한다.

이를 대비 하고자 하는 것이 바로 SHA-3이다.

SHA-3은 미국 국립표준기술연구소(이하 NSIT)가 2015년 8월에 발표한 암호화 해시 함수이다.
SHA-3는 기존 SHA-1, SHA-2 해시 알고리즘의 취약점을 보완하기 위하여 5년 동안의 공모를 통해 제출된 64건의 암호알고리즘을 비교 분석하여 가장 적합한 하나를 선정하는 과정을 진행하였는데, 그 결과 차기 SHA-3 해시 알고리즘으로 Keccak이 최종 선정되었다.

SHA-3는 SHA3-224, SHA3-256, SHA3-384, SHA3-512의 4개의 해시 함수와 SHAKE128, SHAKE256으로 불리는 2개의 확장 가능한 출력 함수로 구성되어 있으며 스펀지 구조로 이루어져 있기 때문에 스펀지 함수라고 불린다.



SHA-3의 스폰지 구조

RICH CASH 스펀지 구조

SHA-3는 스펀지 구조로서 비트의 순열을 가지는 함수와 메시지를 패딩 하는 패딩 함수를 이용하여 메시지 다이제스트를 출력한다. b 비트는 b∈ {25,50,100,200,400,800,1600}로 정해져 있고 b=r+c로 r이라는 bitrate와 c의 보안 파라미터로 나누어진다.

r은 b보다 작은 양의 정수로 f 함수의 입력 비트를 의미하고 c는 b-r값 을 갖는 양의 정수이다.
메시지는 패딩 함수를 거쳐 r의 배수 비트가 되도록 패딩 되고 이 메시지를 r비트씩 자른 값과 r 의 XOR 연산값을 f 함수의 입력으로 사용된다.

이전 f 함수의 출력 값이 메시지와 XOR된 후에 다음 f 함수의 입력 값으로 사용되는 과정이 반복되면서 메시지를 흡수하는 과정이 진행된다.

개요	Keccak 스폰지 함수
설계자	Guido Bertoni, Joan Daemen, Michaël Peeters and Gilles Van Assche
구현	확장가능 출력 함수(XOF), 즉 임의의 출력 길이를 갖는 해시 함수의 일반화
구조	스폰지 구조
프리머티브	b 가 25, 50, 100, 200, 400, 800 또는 1600 비트 인 KECCAK - f[b] 순열 중 하나입니다 . FIPS 202 및 SP 800-185 표준의 범위에서 가장 큰 순열 KECCAK - f[1600]이 사용됨. 그럼에도 불구하고 제한된 환경에서 더 작은 (또는 "더 가벼운") 순열을 사용할 수 있다.
매개변수화기준	용량 c와 비트율 r
인스턴스	인스턴스는 KECCAK [r , c] 로 표시. 용량 c 는 일반 공격에 대한 입증 된 보안 강도를 결정. 즉, 보안 수준 n 비트 인 경우 용량은 $c = 2n$ 이어야 하고, 합쳐지면 r+ c 는 25, 50, 100, 200, 400, 800 및 1600 비트 중에서 순열의 너비여야 함.
지위	3GPP TS 35.231, FIPS 202 및 SP 800-185에서 표준화 된 SHA-3 경쟁에서 우승

RICH CASH INSIDE

스폰지 구조로 되어 있는 SHA-3는, SHA-2가 출력 가능한 메시지 다이제스트의 크기를 모두 출력할 수 있고, 암호학적 함수가 지녀야 할 특성을 완전하게 갖추고 있기 때문에 기본적으로 SHA-2사용된 모든 곳에서 사용이 가능하다.

또한, SHA-3는 높은 병렬구조를 가지고 메모리 접근에 인터리빙 방식을 사용하기 때문에 효율성이 뛰어나다.

기존 SHA-2 해시 알고리즘의 취약점으로부터 비교적 안전하다.

모든 플랫폼에서 기존 SHA-2 해시 알고리즘보다 처리 속도가 빠르다.

SHA-3는 출력길이를 확장하는 것이 가능하다.

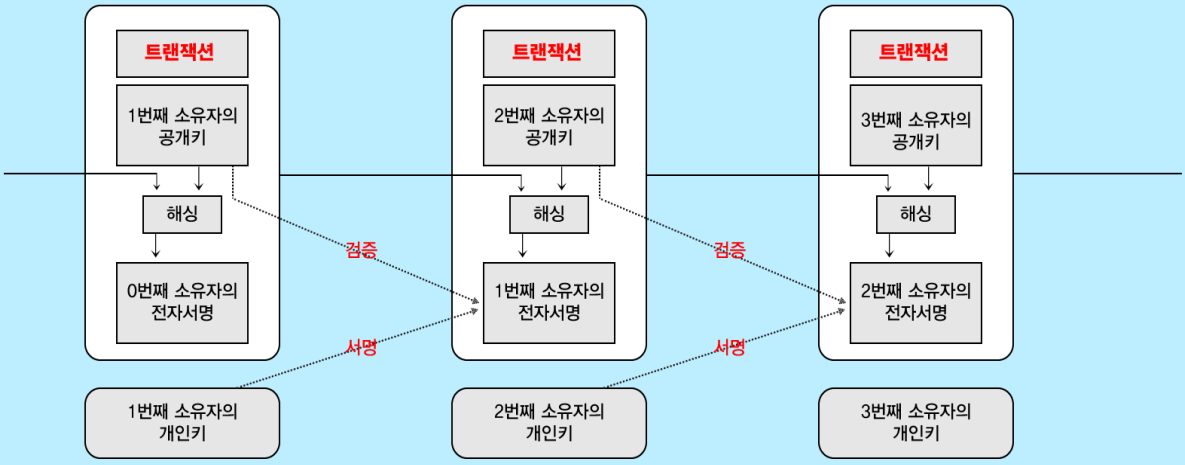
Keccak Tree 해시 함수는 MD5 해시 알고리즘보다 성능적으로 뛰어날 뿐 아니라 처리 속도에서도 비교적 동등하거나 몇몇 플랫폼에서는 우위를 점하고 있다.

Cycles / byte	Algorithm	Strength
4.79	keccakc256treed2	128
4.98	Md5	< 64
5.89	keccakc512treed2	256
6.09	Sha1	< 80
8.25	Keccakc256	128
10.02	Keccakc512	256
13.73	Sha512	256
21.66	sha256	128

주요 해시 알고리즘과의 성능 비교표

RICH CASH 트랜잭션의 처리 및 승인

네트워크에서 트랜잭션이 발생하면, RICH CASH체인은 다음과 같은 과정으로 트랜잭션을 처리한다.



1) 이용자가 개인키를 사용하여 이체 거래 A를 신청한다.

2) 이체 거래 A에 해당하는 해시값과 식별코드가 발행된다.
(TxID) – 이를 통해 이체내역은 즉시 확인할 수 있고, 식별코드를 통해 어떤 소속의 채굴자가 채굴에 참가할 수 있는지가 정해진다.

3) 이체 거래 A 내역을 채굴자가 자신의 이체 풀에 넣어 보관한다.

4) 채굴자가 목표값 해싱에 성공하여 블록 생성 권한을 얻게 되면 새 블록에 이체신청내역을 '우선순위'부터 차례로 담아 발행한다.

5) 이체 거래 A 내역을 담은 블록이 네트워크에 전파된다.

6) 이체 거래 A가 1회 확인(confirmation) 받는다.

RICH CASH 트랜잭션의 처리 및 승인

7) 네트워크를 통해 해당 블록을 전파(다운)받은 다음의 채굴자가 블록 생성 권한을 얻고 다음 블록을 생성하게 된다.
8) 이체 거래 A를 담은 블록의 '다음 블록'이 네트워크에 전파된다.
9) 이체 거래 A가 2회 확인 받는다.
10) 이체받는 주체가 이체내역을 승인하면 이체확정(Settlement)이 된다.

사토시가 설계한 비트코인 프로그램은 각 이체가 총 6번의 이체확인을 받아야 재이체(사용)가 가능하도록 설계되어 있는데, 이는 먼 거리의 노드에서 거의 동시에 블록이 생성 될 수 있음을 가정한 것이다.
먼저 생성된 블록이 도달하기 전에 새로운 블록이 생성되는 경우 체인은 분기가 발생하는데 이 경우, 더 긴 쪽의 체인이 채택되고, 더 이상 블록을 이어가지 못하는 체인은 소멸하게 되는 것이다.

비트 코인이 6컨펌 이후에 재사용이 가능하게 설계된 이유는 트랜잭션을 담고 있는 블록이 생성(1컨펌)된 이후 최소 5블록이 더 붙게 되면 그 체인은 살아 남게 되고, 해당 트랜잭션은 더 이상 문제가 발생하지 않을 것이라는 뜻이다.

이때 소멸된 블록에 담겨졌던 트랜잭션은 원래의 상태로 돌아가 다시 블록에 담기기를 기다리게 된다.
비트코인의 블록생성 시간이 평균10분이고, 이렇게 연산량이 큰 작업의 경우 거의 동시에 블록이 생성되는 경우가 많지 않다.

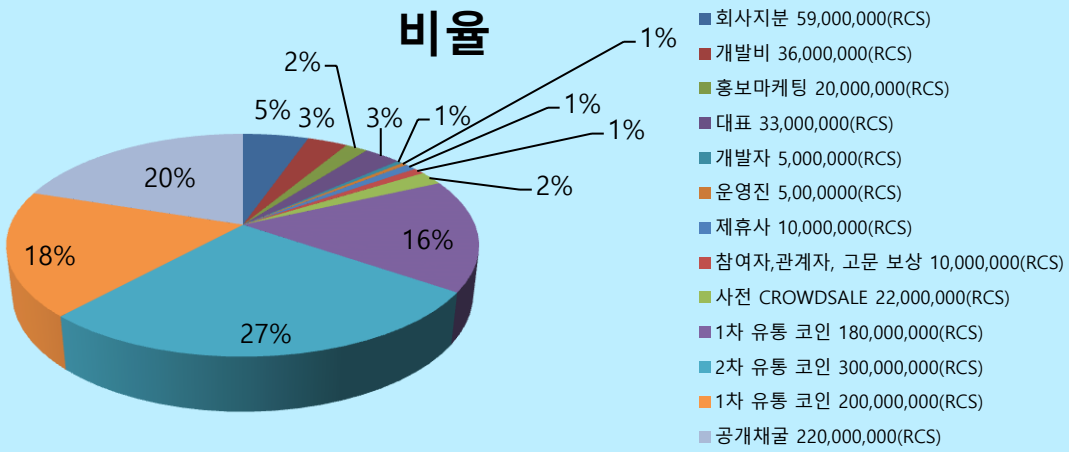
또 길이가 같은 체인이 충돌하더라도 머지 않아 블록체인의 길이가 달라져 분기에 의한 충돌이 해소된다.
실제 지난 1년간 발생한 분기는 2~3블록 이내에서 해결되고 있다.
또한, 많은 사업자들은 비즈니스 영역에서 사용자 만족을 위해 컨펌 단계를 조정해 1~2컨펌 만으로도 이체 확인이 가능하게 처리하고 있다.

RICH CASH POLICY

- COIN NAME : **RICH CASH**
- COIN 약 명 : RCS
- COIN 단위 : 소수점 이하 8자리
  RP1(소수점 1자리) ,RP2,RP3~ RP8(소수점 8자리)의 단위명으로 구분
- RICH CASH 알고리즘 : Keccak (SHA-3)
- RICH CASH 사용처 : On - Line 쇼핑몰의 지불 결제 페이 , 부동산 유통 코인
- RICH CASH 총 매장 량 : 11억 RCS
- RICH CASH 공개채굴 량 : 2.2억 RCS
- RICH CASH 선 채굴량 : 8.8억 RCS

RICH CASH COIN의 분배는 아래와 같이 세분화 된다.

구분	배분구분	코인 배분 수량	비율
코인운영자금	회사지분	59,000,000(RCS)	5.36%
	개발비	36,000,000(RCS)	3.27%
	홍보마케팅	20,000,000(RCS)	1.82%
참여자 배분	대표	33,000,000(RCS)	3.00%
	개발자	5,000,000(RCS)	0.45%
	운영진	5,00,0000(RCS)	0.45%
	제휴사	10,000,000(RCS)	0.91%
	참여자,관계자, 고문 보상	10,000,000(RCS)	0.91%
	사전 CROWDSALE	22,000,000(RCS)	2.00%
ON-LINE 결제 유통 코인	1차 유통 코인	180,000,000(RCS)	16.36%
	2차 유통 코인	300,000,000(RCS)	27.27%
부동산 유통 코인	1차 유통 코인	200,000,000(RCS)	18.18%
공개채굴		220,000,000(RCS)	20.00%



RICH CASH POLICY

RICH CASH은 keccak (SHA-3) 알고리즘을 기반으로 한다.
총 발행 수는 11억 RCS이며, 지불결제 페이로써 사용, 확산하기 위하여 8.8억 RCS는 선 채굴 한다.
RICH CASH은 거래소에 등재를 하고 RICH CASH의 가치 상승을 대비하여 2.2억 RCS는 공개 채굴할 수 있도록 설계되었다.
난이도가 올라간 상태에서 채굴을 하려면 고사양의 채굴기가 있어야 하는 점을 감안하여 누구나 쉽게 채굴이 가능하도록 하기 위하여 저 사양에서도 잘 돌아가는 keccak (SHA-3) 알고리즘을 적용하여 ETH나 LTC보다 생산성이 좋다.
채굴 시 발열하는 온도도 ETH보다 30% 정도 밖에 발생하지 않아 장시간 사용할 수 있다.

블록 간 발생시간은 5분이며, 일일 블록 수는 288 블록이 생성되며, 블록 보상은 40 RCS이며,
1일 최대 채굴보상 수량은 11,520RCS로 구분되며, 최대 블록수와 블록에 따른 보상을 적용하게 된다.
RICH CASH의 가장 큰 특징은 실물화폐로서의 기능과 기술적인 부분에서의 1 블록당 난이도를 적용하여 공개 채굴이 가능하게 만들었다는 점이다.
RICH CASH은 생활 화폐로써의 가치 창출을 위하여 빠르고 다양한 On - Line 플랫폼에서 운영되도록 하려고 한다.
RICH CASH은 분산화 된 세상을 실현하기 위해 공동체를 새롭게 정의 내리고, 정의된 공동체를 연결하며, 연결된 공동체를 통해 새로운 세상을 만들 것이다.
RICH CASH은 사회적·정치적 의미로만 존재하던 공동체(Community)에 경제적 관계를 결부시킴으로써 국가 단위로 정의되던 기존 경제시스템을 공동체 단위로 새롭게 정의하고, 정의된 각 공동체들을 이전보다. 더욱 밀접하게 연결시킬 것이다.
또한, 현실세계(Real world) 뿐만 아니라 가상 화폐 세계(Crypto-world)와도 연결되어 무한한 확장(Infinite scalability)이 가능해질 것이다.

Coin Name	**Richcash Coin**
Abbreviation	RCS
Algorithm	keccak (SHA-3)
Time Between Blocks	300 sec (난이도 높음)
Block Reward	40 RCS
Total Coin	1,100,000,000 (11억 RCS)
daily block count	288 blocks
mining coin per a day	11,520 RCS
Rewardable Last Block	5,500,010
Expectation time until Last Block generated	52 years 117 days 6 hours and 10 minutes
maximum block size	2M
pre-mined coin	880,000,000 (8.8억 RCS)