THE KAICOIN WHITE PAPER

블록체인과 문화의 결합
화폐가치를 변화시키는 암호화폐 플랫폼

www.kaicoin.io

Initial Ver. 1.0 : 2017-05-01
Last Updated Ver. 1.2 : 2017-08-18

목 차

1. 개요

카이코인은 한국투자자협회 회원들의 이익 증대와 국내외 관계 회사들의 컨텐츠 결제용으로 사용하기 위해 한국투자자협회에 의해서 투자되어 개발되었다. 카이코인은 비트코인과 이더리움의 기술력을 보완하고 보안과 전송속도를 10배 이상 빠르게 개발되었으며 특히 보안 중심적인 안전한 암호화폐로 평가된다. 총 채굴량이 21억 개로 제한되어 있어, 전 세계로 보급될수록 코인 자체의 희소성이 높아져 스스로 가치상승의 효과를 가져 온다.

그리고 모바일게임, e-쇼핑몰, 그리고 VR컨텐츠 등에 사용되도록 사용환경 시스템을 이미 구축하였으며 추후 카이코인의 사용 환경은 급속히 확장되어 갈 것이다.

또한, 완벽한 보안시스템을 통해 수익 실현을 추구하며, 카이코인, 비트코인, 이더리움은 물론 전세계 유수의 알트코인들의 거래가 가능하도록 통합거래시스템을 자체 운용할 것이다.

2. 배경

블록체인은 2009년 나카모토 사토시에 의해 비트코인의 핵심기술로 태어났다.

비트코인은 이중지불 문제를 해결하기 위해 블록체인을 사용하였으며 이는 개인들의 화폐전송 정보를 공개적으로 기록하는 금융거래원장으로써 블록체인을 사용하게 되는 근본 이유가 된다. 이후 블록체인 기술을 활용한 수많은 알트코인이 나타났으며 지금까지 약 800여개의 암호화폐가 상호 경쟁관계에 있으면서 전 세계적으로 활발히 거래되고 있다.

또한 컨소시움 블록체인을 도입하여 수많은 기업들과 은행들이 이 블록체인 기술에 투자하고 있다.

블록체인은 화폐를 비롯하여 금융상품, 서비스, 물류정보, 재산소유권, 지적소유권, 신원정보 그리고 모든 디지털 자산을 사용 및 관리하려는 다양한 계층에서 연구 및 개발되고 있다.

이어 2014년 7월 비탈릭 부테린에 의해 탄생된 이더리움은 "임의의 상태변환 함수 구현에 사용될 수 있는 계약"이라는 스마트 컨트랙트를 제공하는 블록체인을 핵심기술로 담고 있다. 이러한 스마트 컨트랙트 기반의 블록체인의 최대 목표는 사용자가 모든 종류의 계약(프로그램)을 블록체인에 쓸 수 있게 하는 것이며 스마트 컨트랙트는 탈 중앙형 시장, 통화거래 플랫폼 등에 사용될 수 있다.

그러나 비트코인이 갖고 있는 문제점 즉, 지연되는 전송속도(결제/송금)문제와 블록용량(1MB)의 협소성 문제 그리고 이더리움이 갖고 있는 보안 취약성(DAO) 문제들 또한 존재한다.

제 4세대 화폐인 암호화폐에 대해 국내외의 관심은 빠르게 확산되고 있으며 보다 안전하고 보다 편리하게 사용될 수 있는 코인이 요구되는 시대다. 카이코인은 비트코인과 이더리움의 결점을 보완하여 사용의 편리성과 보안성이 강화되었으며 특히 한국문화 기반의 전자상거래에 중점을 둔 블록체인 기술에 초점을 맞춰 사용자들의 편의와 수익성에 큰 도움이 되도록 개발되었다.

3. GSChain 소개

GSChain 은 조직들 사이에 특정 블록체인을 생성하고 배포할 수 있는 맞춤 플랫폼이다. GSChain 은 사용이 편리한 패키지를 통해 프라이버시와 규제를 주어, 금융권에 블록체인 기술을 전파하는데 난관으로 여겨지는 문제를 해결하는데 목적을 둔다. Bitcoin core 소프트웨어에서 파생된 GSChain 은 윈도우, 리눅스, 맥 서버를 모두 지원하며 간단한 API 와 커맨드라인 인터페이스를 지원한다. 뒷 부분에서 GSChain 첫 공개 버전과 GSChain 의 특징을 소개한다.

3-1. 프라이빗 블록체인

GSChain 은 사용자 권한을 통합 관리하여 채굴, 프라이버시, 개방성에 관련된 문제에 해결책을 제시한다. GSChain 의 핵심 목적은 다음의 3 가지로 정리된다.

1) 블록체인 활동이 선정된 참여자에게만 보이도록 함
2) 어떤 트랜잭션이 허용되는지 통제방법을 도입
3) PoW 등 관련 비용을 들이지 않고 안전하게 채굴 가능.

블록체인이 사유화될 경우 해당 블록체인 참여자들이 블록의 최대 크기를 조정할 수 있기 때문에 블록의 확장 문제는 쉽게 해결된다. 또한, 폐쇄성 시스템이기에 참여자와 관련이 있는 트랜잭션만 발생한다.

모든 암호화폐가 공개 키 암호 방식(public key cryptography)을 사용해서 신원과 보안을 관리하는 점으로 시작한다. 암호화폐 사용자들은 각자의 개인 키를 임의로 생성하고 다른 참여자에게 절대로 공개하지 않는다. 각 개인 키는 수학적으로 연관된 공개 주소가 있으며, 이는 자금을 수령할 수 있는 신원을 대신한다. 공개 주소로 자금이 송금되면 개인 키가 있어야 해당 거래를 "체결"할 수 있다. 이것은 개인 키에 접근하는 것이 곧 해당 키가 보호하고 있는 자금을 소유한다는 것을 뜻한다.

이러한 암호 방식은 자금에 대한 접근 권한을 통제하고 사용자가 특정 주소와 관련된 개인 키를 소유하고 있다는 것을 입증하기 위해 메시지에 서명할 수 있도록 한다. 이와 같은 특징때문에 GSChain 은 접근 허용 명단에 포함된 사용자만 블록체인에 접근할 수 있도록 허용하는데, 두 개의 블록체인 노드가 연결될 때 아래와 같이 서로 "확인" 하는 과정을 거친다.

블록체인 확인 과정

1) 각 노드는 접근허용명단에 공개 주소로 신원을 밝힌다.
2) 각 노드는 각자가 가진 허용명단에 상대방의 주소가 있는지 확인한다.
3) 각 노드는 상대방에 챌린지 메시지(challenge message)를 보낸다.
4) 각 노드는 받은 챌린지 메시지의 서명(signature)을 보내서 기존의 공개 주소에 해당하는 개인 키를 가지고 있음을 증명한다.

어느 한쪽 노드에서 결과가 충족되지 않으면 P2P 연결을 강제 종료한다.

권한을 공개주소와 연결시키는 원칙은 네트워크 상 다른 기능에도 적용할 수 있다. 예를 들어 송금/수령 트랜잭션 권한을 특정 명단으로 제한할 수도 있는데, 이는 트랜잭션 내역에 송금인과 수령인의 주소가 모두 명시되기 때문이다. 송금/수령인이 여럿인 경우도 있기때문에 트랜잭션에 포함된 송금인과 수령인 전원이 허용 명단에 있을 경우에만 트랜잭션을 허용하게 된다. 물론 블록체인을 완전히 공개적으로 열람할 수 있고 트랜잭션 기능만 제한할 수도 있다. 끝으로, 채굴자들이 블록에 포함시킨 코인베이스 트랜잭션에 서명란을 추가하여 GSChain 내 채굴을 비슷하게 제한할 수 있다. 이는 소수가 프라이빗 블록체인을 장악할 수 없도록 핵심적인 역할을 하며, 이는 다음 내용에 언급한다.

GSChain 권한

GSChain 에서는 특정 메타데이터를 포함한 네트워크 트랜잭션을 사용해서 모든 권한 승인과 취소가 이루어진다. '최초(genesis)' 블록 채굴자는 다른 사용자의 권한을 관리할 수 있는 관리자 권한을 포함해서 모든 권한을 갖게 된다. 관리자는 트랜잭션 출력값에 포함된 사용자 주소와 각 사용자에 주어질 권한을 명시하는 메타데이터를 통해 다른 사용자들에게 권한을 부여한다. 다른 사용자의 관리자 권한 및 채굴 권한을 변경할 때는 제약이 추가로 적용된다. 기존 관리자들이 변경 사항에 대한 동의여부를 표결해야 하고, 최소 비율이 동의해야 권한 변경이 가능하다. 이러한 표결은 별도의 트랜잭션을 통해 각 관리자가 등록하며, 충분한 합의가 이뤄졌을 때 변경 사항이 반영된다. 블록체인 생성 초기에 몇 블록은 "설정 단계"를 구성하게 되는데, 이때 한 명의 관리자가 앞서 설명한 표결을 건너뛸 수 있다. 향후 버전에서는 GSChain 에 독자적으로 권한 승인/취소가 가능한 "수퍼 관리자"를 반영할 수도 있다.

권한 수정 내용이 트랜잭션 내부 메타데이터에 내장되어 있기 때문에 네트워크에 있는 모든 노드에 빨리 전파되며, 현재 상태에 대한 합의를 도출하게 된다. 하지만 분산 네트워크인 만큼 각 노드가 다른 트랜잭션 전후로 서로 다른 시기에 권한 트랜잭션을 받을 수도 있다. 만약 대금 지불 트랜잭션 유효성이 미처 전파되지 못한 권한 변경으로 결정될 경우, 이 차이로 인해 치명적일 수 있다 – 일부 노드는 지불을 수락하고 일부는 거부할 수 있음

이러한 차이점은 블록체인에 트랜잭션이 확인되면 해결되며, 최종 순서를 고정하게 된다. 트랜잭션이 블록체인 순으로 "재생"되기 때문에 블록에 있는 각 트랜잭션은 직전의 사용자 권한에 의거하여 유효한 트랜잭션이어야 한다. 블록에 있는 트랜잭션이 유효하지 않을 경우 블록 전체가 무효 처리된다. 블록이 유효할지라도 해당 블록의 트랜잭션에 정의된 허용목록에 채굴자가 있어야 유효하게 처리된다.

단, 접속 권한의 경우 블록체인 내용과 연관이 없기 때문에 이러한 권한 관리 체계에서 제외된다. 대신 특정 주소의 권한이 취소될 경우, 모든 노드는 응답 확인 과정에서 해당 주소를 사용한 노드와 연결을 끊는다.

편의상 고정범위의 블록 번호에 임시 권한을 제한적으로 승인할 수도 있다. 이런 임시권한에 따라 이뤄지는 트랜잭션은 지정된 범위에 있는 블록 번호에만 유효하다. 권한 변경은 충분한 수의 관리자들이 해당 사용자와 권한에 맞는 블록 범위를 정확히 골랐을 때만 합의가 도출된 것으로 여긴다. 이를 통해 네트워크의 투명성을 제고하는 동시에 기간이 만료된 임시 권한을 일일이 취소해야 하는 부담을 줄일 수 있다.

블록체인이 제대로 "프라이빗" 네트워크가 되기 위해서, 모든 주소는 체인 상으로 승인되며 적어도 한 명의 관리자가 주소 소유자의 실제 신원을 꼭 알고 있어야 한다. 하지만 대부분의 참가자들이 서로의 정체를 알고 있을 필요는 없다. 블록체인의 주요 기능 중 하나가 peer-to-peer 트랜잭션인데, 두 가지 형태의 토큰을 교환하는 사례가 있다. 주소의 익명성이 보장되면 트랜잭션이 진행될 때 서로의 실제 정체를 모르고도 거래가 가능하다. 금융기관들은 여러 주소를 취급하며 이러한 트랜잭션을 처리하는데, 담당자만이 각 주소의 소유자를 알 수 있다.

3-2. GSChain 에서 채굴하기

GSChain 에서는 신원 확인이 가능한 당사자에게만 채굴권을 제공하는 것으로 한 명이 채굴권을 독점할 수 있는 프라이빗 블록체인의 딜레마를 해결한다. 이 해결책은 동일한 채굴자가 특정 기간 내에 생성할 수 있는 블록 수를 제한하면 가능하다.

제한을 구현할 때 필요한 매개변수

mining diversity (*0 ≤ mining diversity ≤ 1* 로 정의)

매개변수 활용하여 블록 유효성 검증

1) 블록 내 트랜잭션에 정의된 모든 권한 변경을 순차적으로 적용한다.
2) 변경 적용 후 허가 받은 채굴자의 수를 센다.
3) 채굴자와 *mining diversity* 를 곱하여 결과값을 반올림해서 *spacing* 값을 얻는다.
4) 해당 블록의 채굴자가 지난 *spacing*-1 블록을 채굴한 적이 있으면 해당 블록은 무효 처리된다.

이렇게 round-robin 스케줄을 적용하여 허가 된 채굴자는 각각 한 번씩 돌아가며 블록을 생성해야 유효한 블록체인이 생성되게 된다. *mining diversity* 매개변수는 엄격한 스키마 scheme 로 정의하는데 이는 네트워크를 장악하기 위해 담합해야 하는 허가 된 채굴자 비율을 의미한다. 값이 1 이면 모든 허가 된 채굴자가 순환에 포함되는데, 0 일 경우 그 어떤 제한도 없음을 뜻한다. 일반적으로 값이 클수록 안전한 네트워크로 간주되지만 1 에 너무 가까운 경우 일부 채굴자가 비활동시 블록체인 자체가 정체될 수 있다. 따라서, 중간 값으로 0.75 를 권장한다. 각 노드는 자원을 아끼기 위해 이미 채굴한 지난 *spacing* - *1* 블록을 채굴하려 하지 않을 것이다.

다양성 변수로 제약을 걸면 악의적 활동을 예방할 수 있으며, 통신 두절 등으로 인해 네트워크가 일시적으로 끊어질 때도 도움이 된다. 이때 끊어진 네트워크 구간의 노드가 다른 구간의 거래나 블록을 볼 수 없기 때문에 블록체인 내 포크가 발생할 수 있다. 네트워크가 복원된 후 체인이 가장 긴 포크를 기준으로 글로벌 합의가 도출된다. 이런 다양성 제한으로 가장 긴 블록체인이 다수의 허가 된 채굴자가 있는 구간에 속하도록 보장한다. 이때 다른 구간의 블록체인은 곧 동결될 것이다.

프라이빗 블록체인의 유용성

왜 굳이 중앙화 데이터베이스가 아닌 프라이빗 블록체인을 사용하는지 의문이 들 수 있다. 중앙화 데이터베이스도 수신 트랜잭션 수락, 분쟁 해결, 데이터베이스 상태 쿼리 답변 등이 가능한데 말이다. 이 의문에 대한 답은 3 가지로 정리된다.

1) 블록체인에서는 각 참가자가 개인 키를 통해 자신의 자산을 완전하게 통제한다. 채굴자들도 다른 참가자의 자금으로 트랜잭션을 생성할 수 없다.

2) 데이터베이스 통제권이 여러 참가자에 걸쳐 분산되어 있기 때문에 특정 개인이나 소수 집단이 트랜잭션의 유무를 단독으로 판단할 수 없다.

3) 블록체인은 중앙화 데이터베이스 체계보다 안정적이다. 서버 하나가 사라지거나 고장 나도 네트워크 전체의 트랜잭션에 영향을 미치지 못한다.

권한 기반인 채굴의 경우 PoW 는 어떻게 될까? 비트코인에서는 PoW 를 통해 채굴에 요구되는 연산작업을 어렵게 하여(즉, 비용이 많이 들게 하여) 채굴 다양성을 보장한다. 반면에 프라이빗 블록체인은 훨씬 단순한 방법을 통해 채굴 다양성을 보장하기 때문에 PoW 에 요구되는 작업은 형식적인 의미만 갖게 된다. 실제로 GSChain 의 최초 버전은 각 노드의 블록 생산율을 규제하고 랜덤화하기 위해 여전히 비트코인 스타일의 PoW 를 사용하지만, 이것도 블록체인의 보안을 위한 장치가 될 수 없다.

GSChain 블록체인에서는 트랜잭션 수수료와 블록 보상이 "0"으로 설정되어 있다. 블록 채굴비용이 무시해도 될 정도로 적다면, 채굴자들도 별도의 보상이 필요 없게 되고, 블록체인의 원활한 기능 자체에서 얻게 되는 이득을 위해 채굴을 하게 된다. 대신, 채굴자들이 네트워크 참가자를 상대로 고정된 연회비를 얻을 수도 있는데 블록체인이 아닌 제도권 내 지불 수단으로 지불한다. 블록체인의 유일한 목표가 토큰화 된 자산에 트랜잭션을 제공하는 거라면, 해당 네트워크의 암호화폐는 단순한 기술혁신 정도로 무시할 수도 있겠다. 하지만 트랜잭션의 희소성이 요망되는 상황이라면 GSChain 에서도 암호화폐가 블록 보상이나 최소의 트랜잭션 수수료 및 거래량 등으로 사용될 수 있도록 설정 가능하다. 이럴 경우 참가자는 암호화폐를 채굴자들로부터 구매해야 하며, 구매 수단에는 토큰화 된 자산 등이 있을 수 있다.

3-3. 다수의 블록체인 구동

Bitcoin Core 처럼 싱글 블록체인을 지원하는 대신에 GSChain 에서는 동시에 여러 블록체인을 구성하고 작동하는 것이 용이하다. 기관 차원에서는 특정 개발자가 아닌 시스템 관리자가 프라이빗 블록체인을 구성하고 운영할 수 있다는 측면에서 매우 유리하다. 비유하자면 Oracle 이나 SQL Server 등 관계형 데이터베이스 관리 시스템(RDBMS)에서 몇몇 SQL 명령어로 데이터베이스를 생성하고 사용할 수 있다는 것과 비슷하다. 또한, 다수의 블록체인을 지원할 때 장점은 서버가 다른 체인의 활동을 연결할 수 있다는 점이다. 예를 들어 특정 블록체인에 자금이 들어오게 되면 다른 블록체인에 송금하도록 유발시킬 수 있다.

GSChain 에서 사용자가 설정할 수 있는 블록체인의 모든 파라미터

1. 체인 프로토콜	프라이빗 블록체인 또는 순정 비트코인에 가깝게
2. 블록별 타겟 시간	1 분 등
3. 승인 권한 종류	누구나 접속할 수 있거나 일부만 송/수신이 가능

4. 채굴 다양성 (mining diversity)	예) 0.75
5. 관리자 및 채굴자를 생성/제거할 때 필요한 합의 수준, 이런 사항이 강제되지 않는 설정 단계의 기간	프라이빗 블록체인만 해당
6. 채굴 보상	예) 블록당 50 단위, 21 만 블록마다 반으로 줄도록 설정
7. P2P 연결을 위한 IP 포트와 JSON-RPC API	예) 8571, 8570
8. 허용된 거래 종류	예) pay-to-address, pay-to-multisig, pay-to-script-hash
9. 블록 최대 크기	예) 1MB
10. 거래당 최대 메타데이터	예) 4096 바이트

하나의 서버에 다수의 블록체인을 활성화할 수 있으며, 각 블록체인마다 고유의 이름과 설정 파일을 갖게 된다. 새로운 블록체인을 생성하기 위해서는 사용자는 두 가지 설정을 해야 한다.

1) 사용자는 체인명을 선택한다. 그러면 GSChain 이 기본 설정을 갖고 있는 설정 파일을 생성한다. 이 파일은 사용자가 수정할 수 있으며, 일반적으로는 기본 설정으로 충분하다.

2) 사용자가 블록체인을 실행하면 GSChain 은 최초의 블럭을 채굴해서 그 생성자에게 모든 사용자 권한을 부여하게 된다. 이때 최초 블록의 세부사항과 해당 블록체인의 파라미터 해시를 설정 파일에 내장하여 향후 실수로 변경될 때를 대비한다.

GSChain 프로세스

처음 실행되면, 블록체인은 하나의 노드로 운영된다. 노드를 추가하기 위해서 GSChain 은 다른 컴퓨터에서 3 가지 파라미터를 가지고 실행한다. (1) 목적지 블록체인명 (2) IP 포트 번호 (3) 기존 노드의 IP 주소. 사용자 편의상 이 정보를 "노드 주소"라는 형식으로 묶어 사용한다. 예) gs`chain@127.0.0.1:0000`. 프라이빗 네트워크이기 때문에 처음에는 신규 노드가 접속권한 없이 네트워크에 접속하지 못한다. GSChain 은 새로운 노드가 자체 생성한 공개 주소를 포함하여 메시지를 표시하게 되는데, 이 주소를 관리자에게 보내야 한다. 관리자는 간단한 명령어로 트랜지션을 생성하여 해당 주소에 접속 권한을 부여한다. 신규 노드는 이제 접속할 수 있게 되고 접속 시 블록체인의 특성이 정의된 설정 파일을 자동으로 다운로드한다. 나중에 동일한 블록체인으로 재 접속 시에는 체인명만 필요하고 응답 확인 절차를 통해 두 노드가 동일한 파라미터를 사용하고 있는지 확인된다.

GSChain 개선사항

차후에 반드시 개선되어야 할 사항 중 하나는 블록체인이 실행 중일 때 신뢰성 있는 관리자들이 발행한 특정 트랜지션을 통해 일부 파라미터가 변경될 수 있도록 하는 것이다. 예로, 네트워크 사용량이 증가하면서 거래량을 소화하기 위해 블록 최대 크기를 증가시킬 수 있겠다. 이와 같은 변경은 네트워크상에 있는 각 노드의 연산 역량을 함께 고려해야 한다.

3-4. 복수화폐 블록체인

CoinSpark 나 Counterparty 같은 토큰화 프로토콜을 사용하면 비트코인의 자체 화폐와 병행하여 비트코인 블록체인에서 제 3 자 자산을 발행하고 거래할 수 있음을 이미 언급했다. 이런 기법은 GSChain 에서 생성한 프라이빗 블록체인에서도 별도의 수정 없이 동일하게 사용할 수 있다. 하지만 프라이빗 프로토콜을 사용하는 블록체인에서는 제 3 자 자산을 지원하는 기능을 체인 규칙에 반영하는 것으로 더욱 개선할 수 있다.

비트코인에서는 각 트랜잭션 결과값에 내장된 비트코인의 수량을 거래마다 부호화 한다. 출력값에 부호화 된 총 비트코인보다 입력값에 반영된 비트코인이 많을 경우 해당 거래는 네트워크에서 무효화 처리되어 블록체인에 확인하지도, 전파하지도 않는다. 네트워크의 모든 노드가 소모되지 않은 트랜잭션 출력값에 있는 비트코인을 추적하기 때문에 이런 검증이 가능하다. 따라서 사용자들은 네트워크 혹은 블록체인에서 벌어지는 트랜잭션 여부 자체를 통해 트랜잭션 내용에 내재되어 있는 비트코인 수량이 정확할 것이라고 안심할 수 있다. 이 덕분에 경량("simple payment verification") 지갑이 네트워크와 안전하게 거래할 수 있으며, 블록체인 전체를 사용자 컴퓨터에 저장할 필요가 없다.

토큰화 문제점

비트코인에서 자산을 토큰화 할 경우 문제가 되는 점은 외부 자산을 인코딩하는 메타데이터가 비트코인 자체를 검증하는 네트워크 수준의 검증과정을 거치지 않는다는 점이다. 예를 들어 ABC 라는 은행이 달러를 상징하는 토큰을 발행했다고 가정하자. 악의적인 사용자가 출력값에 100 ABC 달러가 있다는 메타데이터를 가진 거래를 생성할 수 있다. 실제로 그 거래의 입력값에는 ABC 달러가 없었는데 말이다. 이런 거래는 비트코인 네트워크에서 유효 처리되고 블록체인에서도 확인이 되는데, 그 이유는 첫째, 비트코인 노드가 이 메타데이터를 읽지 못하고, 둘째, 비트코인 노드들이 ABC 달러를 추적하지 않기 때문이다.

따라서 토큰화 자산은 비트코인 블록체인에서 비트코인 자체 화폐에 비해 제 2 국민 취급을 받는다. 토큰화 자산의 존재 여부는 해당 토큰을 처음 생성한 거래부터 토큰에 영향을 주는 모든 트랜잭션 내역을 봐야 알 수 있다. 이는 "포워드 forwards" 방식으로 효율적으로 계산할 수 있다. 모든 새로운 트랜잭션이 들어올 때마다 검토하면 되는 것이다. 하지만 그렇게 하더라도 전체적인 네트워크 노드가 필요하며 토큰화 프로토콜을 경량 지갑과 쓰기엔 부적합하다.

GSChain 은 이러한 문제를 해결하기 위해 모든 자산의 식별자(identifier)와 수량을 각 트랜잭션 출력값에 부호화한다. 이때 비트코인 스크립트 언어가 제공하는 확장자(extension)를 사용한다. 이러면 거래 검증 규칙이 확장되어 트랜잭션 출력값에 있는 모든 자산의 총량이 입력값과 동일한지 여부를 검증할 수 있게 된다. 입출력값이 동일해야 하는 요구사항은 비트코인 자체의 요구사항보다 더 엄격하다. 비트코인의 경우 출력값이 입력값보다 적으면 유효 처리되는데, 이때 그 차액이 채굴 수수료로 나간다. 물론 이런 방식을 사용하기 전에 해당 블록체인이 특수 메타데이터를 지닌 최초의 거래를 통해 새로운 자산을 생성할 수 있도록 허용해야 한다. GSChain 에서는 이런 최초 거래가 블록체인 어느 지점에서 생성되는지에 따라 신규 자산에 대한 식별자를 자동으로 배정하며 사용자가 정의한 고유 식별자와 함께 사용된다.

GSChain 의 권한 시스템은 자산 생성권을 통제하기 위해 사용할 수도 있다. 더불어 향후 버전에는 자산별 권한도 도입할 수 있는데, 이를 통해 자산별로 관리자와 허용된 발송/수령자를 설정할 수 있게 될 것이다. 간결함을 위해 GSChain 의 최초 버전에는 포함되지 않은 기능이지만 이미 반영된 규칙에 간단한 확장을 통해 손쉽게 추가할 수 있는 기능이다.

3-5. 비트코인과 프라이빗 블록체인의 전환

90 년대에 인터넷 사용량이 폭발했을 때 수백만의 사람들은 새로운 패러다임에 노출되었다. 업체들은 이런 혁신 기술을 내부적으로 활용하고 싶었지만 당시만 해도 많은 업체들이 인터넷을 주요 소통 수단으로 활용하기에는 프라이버시와 신뢰성, 용량을 충분히 갖추지 않았다고 평가했다. 따라서 많은 업체들은 인터넷을 내부화 한 일명 "인트라넷"을 구축했다. 인터넷과 동일한 인프라와 기술을 사용했지만, 업체에서 완전히 통제 가능한 기술이었다. 20 여년이 지난 지금, 인터넷은 대용량의 정보를 전 세계에 걸쳐 안정적으로 전송 가능한 네트워크로 자리 잡았다. 이를 통해 많은 업체들이 VPN 을 활용하게 되었다. VPN 은 인터넷을 기본 기술로 활용하지만, 해당 조직의 통신 내용을 암호화하여 공공 통신망을

통해 전파돼도 보안을 유지할 수 있다. VPN 을 통해 인터넷처럼 누릴 수 있으면서도 외부에 데이터를 노출하지 않을 수 있게 된 것이다.

비트코인 블록체인과 프라이빗 블록체인에도 비슷한 절차가 현재 진행 중이다. 업체의 입장에서는 비트코인 네트워크는 아직 정복하지 못한 영역으로, 용량도 한정적이며 장기적인 거래 비용을 예측할 수 없다. 무엇보다 비트코인 채굴은 대부분 불특정다수가 통제하고 있고, 이 중 대부분은 기업에 반대되는 사상을 갖고 있거나 법적 제도가 취약한 국가에 있는 사람들이다. 따라서 금융기관 등 입장에서는 향후 10 년간 이러한 기술을 사용하기 위해서는 프라이빗 블록체인이 더욱 매력적인 방안일 것이다. 지금부터 20 년 후 비트코인이나 다른 블록체인이 매월 수십억 건의 거래를 매우 저렴하게 처리하고 있고 정체가 명확한 대기업들이 채굴을 통제하고 있는 상황이 된다면 그때는 비트코인이 금융기관 거래에도 매력적인 플랫폼으로 다가올 수 있겠다. VPN 처럼 옅은 암호화 층을 더하여 해당 기관의 활동 내역을 대부분의 네트워크 참가자로부터 은폐할 수도 있을 것이다.

GSChain 설계는 많은 면에서 프라이빗 블록체인과 비트코인 블록체인간 쌍방으로 전환이 가능하도록 하는 것을 목적으로 삼는다. 위의 5)번 기능을 통해 자산 토큰화와 메시징을 사용하는 애플리케이션이 있을 경우 코드 변경을 최소화한 상태로 비트코인과 프라이빗 블록체인 간에 전환이 가능하다.

1) GSChain 은 비트코인망의 공식 클라이언트인 Bitcoin Core 의 파생 버전을 기반으로 만들었다. 코드 변경은 현지화되어 향후 비트코인 개선 사항에 머징이 가능하다.
2) GSChain 은 비트코인의 프로토콜, 트랜잭션, 블록체인 아키텍처를 거의 그대로 사용한다. 유일한 차이점은 두 노드가 최초로 접속할 때 진행되는 응답 확인 절차이다. 나머지 기능은 메타데이터와 트랜잭션/블록의 유효성 규칙을 수정하여 반영하였다.
3) GSChain 인터페이스(커맨드라인, API)는 Bitcoin Core 의 인터페이스와 완전히 호환 가능하다. 일부 신규 명령어를 통해 추가 기능도 포함되었다.
4) GSChain 은 per-blockchain 설정 파일에 있는 간단한 프로토콜 설정 하나로 일반 비트코인망(혹은 비트코인 유사 네트워크)에서 노드 역할을 할 수 있다.
5) GSChain 의 복수 화폐 및 메시지 기능은 비트코인 트랜잭션을 개선하기 위한 CoinSpark 프로토콜과 매우 유사하게 작동한다.

4. 카이코인 적용 기술

4-1. 블록체인 방식

특정 단체 또는 조직이 선점 및 독점을 막기 위해 선채굴에 대한 정보와 사회환원 여부를 투명하게 명시하여 시작하며 Public BlockChain방식으로 누구나 마이닝에 참여할 수 있도록 하여 보상을 공유한다. 이로 인해 컴퓨팅 파워를 이용한 해당 암호화폐 시스템 보안은 한층 더 높아진다.
퍼블릭 블록체인의 또 다른 명칭은 '무허가형 원장(Permissionless Ledger)'이다. 따라서 누구든지 허가없이 블록체인의 데이터를 읽고, 쓰고, 검증할 수 있는데 카이코인 또한 이 방식을 따르고 있다. 또한 누구나 블록체인을 다운로드하여 어떠한 기록이 담겨있는지 조회하거나 암호서명을 이용해 기록에 참여할 수 있다.
참여자들은 어떤 데이터가 입력될지를 투표로 결정한다. 노드 수가 아니라 투입한 컴퓨팅 파워에 비례해서 투표권을 부여하는 일반적인 방식이 있다. 그러나 카이코인은 이러한 방식에서 mining diversity를 통해 컴퓨팅 파워가 강한 노드가 독점하지 못하도록 한다. 따라서, 최대한 많은 노드들이 채굴에 성공하도록 돕는다.

4-2. 블록타임과 블록사이즈

최초 사용자를(3000명~4000명) 확보한 코인으로 시작하기에 거래속도와 보안이 가장 중요한 문제이다. 따라서 블록사이즈를 최소 4Kbyte부터 최대2048Kbyte까지 동적으로 할당하여 효율적으로 노드의 전송속도를 높여 안정된 거래 속도를 보장할 수 있다.
또한 블록타임을 60초로 지정하여 평균 60초 안에 해싱된 블록헤더값을 체이닝(chaining)할 수 있으므로 기존 비트 코인의 10분 블록타임의 주기보다 10배 빠른 향상된 advanced SHA256의 해싱기법을 경험할 수 있다.
이 두가지는 우리가 추구하는 차세대 블록체인 화폐의 가장 중요한 이슈인 거래가 불발되거나 거래자체가 지연되는 현상을 막을 수 있으며 기존의 비트코인과 같은 안정성을 보장할 수 있다.
지금 한창 이슈가 되고 있는 최대 블록사이즈에 대한 부분은 가장 효율적이라고 의견이 모아지고 있는 2048Kbyte로 정하여 과거 블록사이즈 때문에 한꺼번에 많은 거래를 블록안에 담을 수 없었던 이슈를 해결하였다.

4-3. 다중 서명 스크립트

Pay to Script Hash(P2SH)는 동시에 두개의 서명이 필요한 방식의 암호화를 조금 더 쉽게 사용할 수 있도록 제공한다. P2SH의 경우 복잡한 잠금 스크립트는 암호화된 Hash값을 디지털 지문으로 대체가 가능하며 해당 거래의 크기를 줄일 수 있는 이점을 포함 시스템 내부적으로 효율적인 거래구조의 선택을 제공한다.

4-4. 반감기

반감기 1년을 기준으로 총 100년간 채굴될 수 있는 공개채굴 시스템을 제공한다. 블록타임을 1분 기준으로 총 3년 동안 약 1,576,800의 블록이 형성될 것으로 예측된다. 이는 채굴자에게 좀더 나은 채굴 환경을 보장하기 위함이고 최초 발행량 21억개를 고려해보건데 채굴의 기회와 난이도 그리고 그 기간을 충분하게 제공하지 못한다면 보안을 책임지는 블록체인

의 생태계를 안정적으로 유통시킬 수 없다고 판단하기 때문이다.
우리는 조금 더 나은 환경의 채굴환경을 만드는 것이 블록체인 기술의 원래 목적을 충실하게 이행 하는 것이라 믿는다.

4-5. 카이코인 기술 명세

- 해시 알고리즘(Hash Algorithm) : advanced SHA256
- 총 발행량 : 21억 카이코인
- 발행방식 : 채굴(Mining)
- 블록타임 : 60초
- 블록사이즈 : 2048 Kbyte

5. 카이코인 소개

5.1. 목적

카이코인은 암호화폐 시장에 해를 끼쳐왔던 기존의 낡은 환경 개선을 희망하는 카이협회 회원들의 염원에 의해 개발되었다. 카이코인은 안전성, 신속성, 투명성 있게 사용되기를 희망하는 사용자들의 바램에 적극 부응하는 암호화폐이며 특히 advanced SHA256방식을 통하여 비트코인의 단점인 결제속도 지연과 보안문제를 보강하여 태어난 채굴형 암호화폐이다.
특히 카이코인에 사용되는 블록체인은 전자상거래에 초점을 맞춰 개발되었으며 이것은 사용자들에게 보다 넓은 사용 편의성과 경제적 이점을 동시에 제공한다.
카이협회의 최종 목표인 10,000개 계열사들 간의 상호 유기적이며 협력적인 네트워크 구축하기 위하여 카이코인은 결제수단으로서의 역할을 충실히 수행하는 필요충분 매개체가 될 것이다.
카이코인은 대한민국 뿐만 아니라 전 세계에서 통용되는 전자상거래 중심의 최고 글로벌 암호화폐가 되는 것을 그 목적으로 하고 있다.
일상에서 다양하게 활용가능한 블록체인 기반 시스템을 구축하는 것으로, 한국의 특색있는 컨텐츠와 문화를 결합하여 사회문화 발전에 기여하고 나아가 국제적으로 통용되는 가상화폐로 인식시킬 것이다.

5.2. 활용 플랫폼

세계는 정보통신 기술의 급속한 발전으로 인해 과거의 방식으로는 더 이상 경쟁에서 살아남기 힘들어지고 있다. 이러한 시대적 요구에 부응하기 위해 플랫폼기반이 탄생하였으며 지금은 기업 성패의 핵심 요인으로 자리매김 하고 있다.
암호화폐 시장에서 플랫폼 기반의 초석은 비탈릭 부테린이 2015년 개발한 이더리움이 최초이다. 단순히 화폐로서의 기능을 갖고 있는 비트코인과는 개념상 차이가 있으며 추후 제 4차 산업혁명 시대를 선도함에 있어서 이더리움과 같은 플랫폼기반의 화폐가 대세를 이룰 것

이다.
카이코인 역시 플랫폼 기반의 암호화폐이며 이를 통해 한국투자자협회는 비즈니스 분야와 사회공헌분야에서 다양한 활동을 전개해 나갈 것이다.

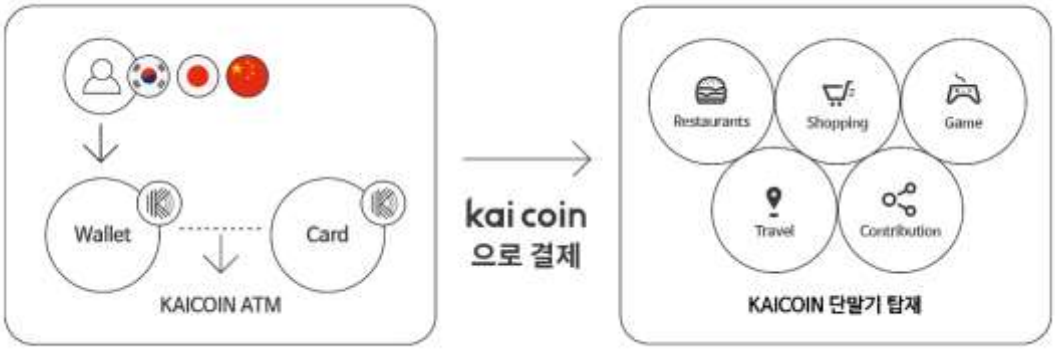
사회	- 블록체인 기술공유를 통한 사회 인프라 확장 - 사회공헌 플랫폼 구축으로 비영리활동 지원 및 NGO단체의 투명한 재정 지원
문화	- K-Culture기반 컨텐츠를 통해 중국, 일본 마켓팅 플랫폼 구축 완료 - 분산시스템을 활용한 VR 컨텐츠 및 모바일 동영상 네비게이션 사용 확장 - 음식점, 제과점, 여행사, 병원 등 오프라인 가맹점 확보 - 국내/외 온라인 쇼핑몰 지원 확대 - 온라인 게임 내부 아이템거래 지원
경제	- KAICOIN 통합거래소 KAIREX 구축 - 현금자동입출금기(ATM)로 KAICOIN 활용 - 국제거래소에 KAICOIN 등재

5.3. 상세정보

- 코인명 : KAICOIN (카이코인)
- 코인단위 : KAI
- 프리세일 기간 : (GMT+9) 2017-09-01 PM12:00 부터 2017-10-31 PM11:59
- 토큰당 가격 : 1,500 KAI = 1 ETH
- 최소구매량 : 150 KAI = 0.1 ETH 부터 가능
- 총 공급량 : 200,000,000
- 거래가능 화폐 : ETH
- 보너스 : 주차별 지급
  (~1주차 20%, ~2주차 15%, ~3주차 10%, ~4주차 5%, 5주차부터 0%)

총 공급량 **2,100,000,000**	공개채굴량	1,000,000,000
	선 채굴량	**1,100,000,000**
선 채굴량 **1,100,000,000**	한국 프리세일	600,000,000
	ICO	**200,000,000**
	사회기부	100,000,000
	투자자 보유	100,000,000
	기타	100,000,000

5.4. 사용환경



5.4.1. 게임

게임을 통해 인간이 얻을 수 있는 두 가지 장점은 스트레스 해소와 관련 기능의 향상이다. 스트레스 해소 면에서 보면 모의 경쟁, 대리만족, 창작 등을 들 수 있으며 관련 기능 향상 면에서 보면 극도의 집중력 향상(바둑), 절차기억 향상(노년층)등에 도움이 된다.
카이코인은 이러한 게임들을 이용하는 게임머니의 수단으로 사용될 것이며 국내외 여건상 많은 수요가 있을 것이다.

5.4.2. 온라인 쇼핑몰

온라인 쇼핑이란 인터넷이나 PC통신 그리고 모바일 등을 이용하여 상품을 검색하고 주문하는 행위를 말한다. 대금 결제는 신용카드나 모바일 페이를 통해서 이루어진다. 이러한 온라인 쇼핑은 정보통신의 발전과 인터넷 사용자 수의 증가, 편리성 등으로 급격한 증가 추세를 보이고 있으나 개인정보 유출과 결제시스템의 불안정과 같은 문제점을 안고 있기에 점차 암호화폐가 새로운 결제수단으로 진화되고 있다.
카이코인은 결제시스템의 불안정한 문제점 즉, 이중지불문제, 결제자의 신원 노출, 그리고 과다한 수수료 문제점 등을 해소시킬 것이다.

5.4.3. 온오프라인 가맹점

가맹점이란 하나의 사업 연맹에 속해 있는 가게나 상점을 의미하며 프랜차이즈라고도 불리운다. 가맹이란 점포와 회사 간에 맺는 영업적 계약이며 가맹점은 회사로부터 브랜드의 인지도를 통한 수익 창출과 경영 지원 등을 기대 할 수 있다.
오늘 날 가맹점 수의 증가는 가히 폭발적이며 지금도 꾸준히 늘어나고 있는 실정이다. 카이코인은 유명 브랜드를 보유하고 있는 회사들과 협력하여 전국에 위치하고 있는 가맹점에서 결제수단으로 사용될 수 있도록 노력할 것이다.

5.4.4. 모바일 서비스

- 카이코인 월렛
  카이코인을 수령하며 계좌를 관리할 수 있는 전자지갑

- KAIREX 거래소
  카이코인 및 다른 가상화폐를 거래할 수 있는 거래소 서비스
- 기부 및 기타
  국내외 카이코인 가맹점을 검색하고 선물 및 후원/기부 서비스

6. 로드맵

1차 (~2017.09)	- 카이코인 개발 - 카이코인 기부 약정 체결 - ICO 한국 프리세일 완료 - ICO 글로벌 프리세일 런칭 - 카이코인 월렛 런칭
2차 (2017.10~12)	- 카이코인 거래소 KAIREX 런칭 - 국제거래소 등재 - 벤더, PG업체와 제휴 확대
3차 (2018)	- 카이코인과 카드의 결합 - ATM기 연동 및 코인으로 간편결제 사용 - 일상 속 카이코인 사용 생활화
4차 (2019)	- 중국, 일본에 결제시스템 지원 - 오프라인 가맹점 10,000여개 이상 확보 - 여행산업 중심으로 지원확대 - 중국, 일본관광객에 특화된 편의성 제공
5차 (2020~)	- 동남아 및 유럽시장 진출 모색 - 국내외 실생활에서 활용도 높은 대표적인 화폐규약으로 인색

7. 개발사 및 제휴사

7-1. 한국투자자협회

한국투자자협회는 2010년 12월 설립되었다. 협회는 비영리 단체로서 경제교육, 투자교육 및 엔젤투자클럽을 지원하고 파트너사와 협력을 통한 주식기부 운동 및 10만 명의 건강한 투자자 양성을 목적으로 하고 있다.
한국투자자협회의 사업은 크게 네 가지로 구분된다.

첫째, 금융 교육 사업이다.

이는 재산관리 아카데미의 다양한 금융교육 프로그램을 통하여 회원들의 자산관리, 투자교육 및 청소년들에게 경제 교육 서비스를 제공한다.

둘째, 투자클럽 육성 사업이다.
이는 엔젤클럽 설립 및 운영 지원을 통해 회원들에게 가치 있는 기업을 발굴하여 투자할 수 있는 기회를 제공함으로써 회원들의 효율적인 자산관리를 돕는 사업이다.

셋째, 주식 나눔 사업이다,
이는 더불어 살아가는 사회공동체의 일원으로서 기업 활동의 사회적 책임을 실천하는 혁신적인 사회공헌 사업인 "주식 나눔 운동"에 동참할 7,000개의 자산 나눔 협력기업 네트워크를 만들어 가는 사업이다.

그리고 마지막으로 IT관련 디지털 산업 투자 및 운영 사업이다.
협회는 제 4차 산업혁명 시대에 요구되는 새로운 암호화폐와 그에 따른 결제시스템에 부응하고자 전자상거래에 필요한 안전성, 신속성, 수익성을 고려하여 협회 산하에 카이코인 사업본부를 설립하여 카이코인을 개발하게 되었다.
카이코인은 한국투자자협회와 회원 뿐만 아니라 다음과 같은 협회 파트너사 들과 함께 사용될 것이며 추후 세계적 게임사들과 온라인 쇼핑몰, 그리고 유명브랜드를 소유하고 있는 가맹점 등에서 결제수단으로 사용될 것이다.
암호화폐의 성격상 제한된 코인 양에 비해 수요가 늘어남으로써 코인의 화폐로서의 가치는 상승될 것이며 이는 카이코인을 보유하고 있는 회원들에게 상당한 금전적 혜택을 부여할 것이다.

7-2. 제휴사

KAii	WHITE STONE	allreve	INCAPO
WOWZONE	PICK:LE 일본	PICK:LE 중국	㈜비트앤퍼슨
AllStarWORLD	로젠비 메디컬	미래옥 불고기전문점	큰물참치 참치전문점

※ 홈페이지가 없는 제휴사는 표기 제외

- KAii : http://www.kaii.or.kr/default/mindex.php
- Allreve : http://www.allreve.com/mshop/main.asp
- WOWZONE : http://wowzone.co.kr/mshop/main.asp
- PICK:LE 일본 : http://ameblo.jp/pickle-japan/

- PICK:LE 중국 : http://weibo.com/u/5888766483?is_hot=1
- AllStarWORLD : http://www.allstarworld.co.kr/
- 로젠비 메디컬 : http://www.rosenbee.com/

8. 결론

한국투자자협회 산하 카이코인 사업 본부는 비트코인의 화폐가치적 기능과 이더리움의 폭넓은 플랫폼 기반을 활용하여 보다 진화된 암호화폐 개발에 목표를 두고 매진해 왔다. 특히 합리적 알고리즘과 실용적 블록체인을 기반으로 전자상거래 영역 특히 게임과 e-commercial 결제에 특화되도록 기술을 개발하였다.

카이코인 개발팀은 블록체인기술을 통해 얻을 수 있는 보안성 및 무결성을 활용하여 일상에서 다양하게 활용가능한 블록체인 기반 시스템 구축을 완료했다.

한국의 컨텐츠와 문화를 결합하여 사회문화 발전에 기여하고 국제적으로 통용되는 가상화폐로 나아갈 것이다.