J COIN

WHITEPAPER

Ver 1.0

컨슈머마켓 쇼핑몰 기반의
구매보상형 디지털결제포인트 블록체인토큰

Table of Contents

1 J-COIN의 속성

2 J-COIN의 전자지갑

3 J-COIN의 운영개념

4 J-COIN의 배분구조

5 J-COIN의 기술적 배경 (이더리움 베이스 토큰)

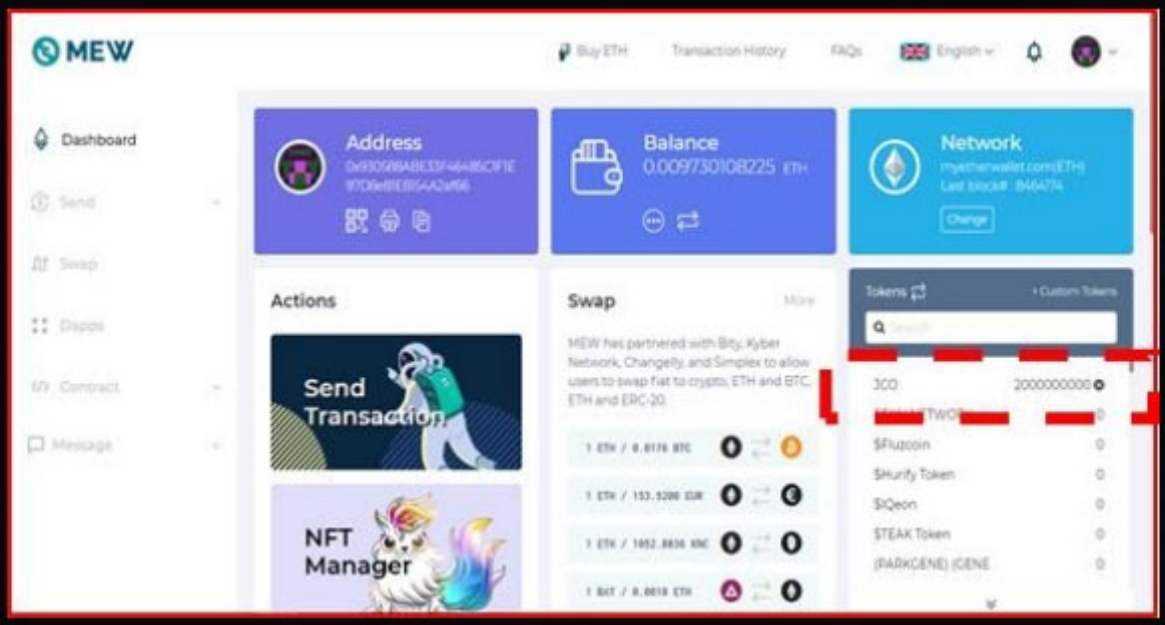
6 J-COIN의 정책

7 향후 기술 반영사항

8 참고

9 법적고지 및 면책사항

1 J-COIN의 속성



[그림1. J-COIN의 초기설립 전자지갑]

- 주소 0x930588ABE33F46485C1F1E97D8e81E8154A2af66]

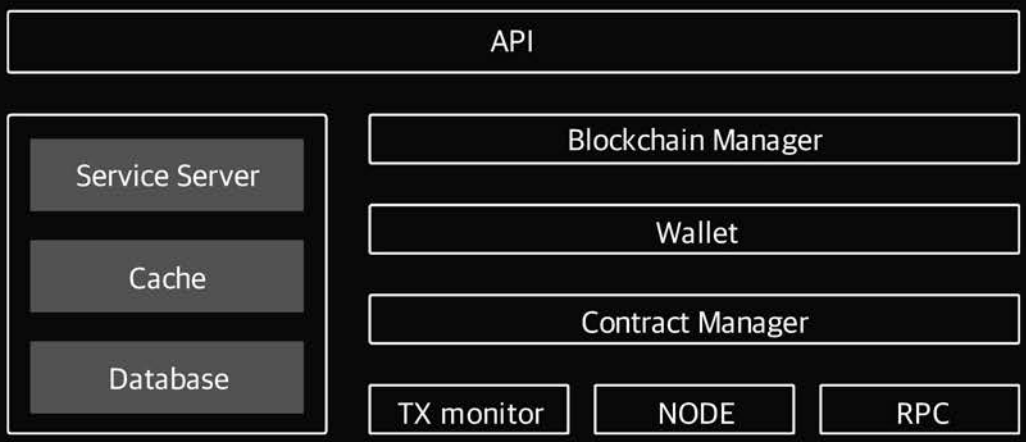
J-COIN은 ERC-20 표준을 준수하며 다음과 같은 속성을 지닙니다.

- ✓ 기초시스템 : Ethereum(이더리움) 블록체인(ERC 2.0표준)
- ✓ 이 름 : J-COIN, 심볼 : JCO
- ✓ 공 급 : 총 80억개(8,000,000,000)의 J-COIN 발행완료
- ✓ 잔 액 : Ethereum에 공개
- ✓ 계 정 : Ethereum주소의 사용
- ✓ 마이닝 : 쇼핑몰 marketdiffer.com 연동형
- ✓ 소유자 : 다중서명지갑
- ✓ 특약사항 : J-COIN의 발행자는 추가 코인을 임의로 발행 하지는 않으나 시장의 흐름에 따라 공지 후 추가 발행할수도 있으며 J-COIN 구매를 승인하고 J-COIN의 매매를 할 수 있습니다.

2 J-COIN의 전자지갑

J-COIN 전자지갑은 코인을 보관하는 공간으로서 Ethereum 블록체인에서 구매, 사용, 거래 등 모든 금융상 거래 활동을 처리할 수 있으며, 계약방식(Smart Contract)은 하단의 레이어로 도식됩니다.

J-COIN Layer



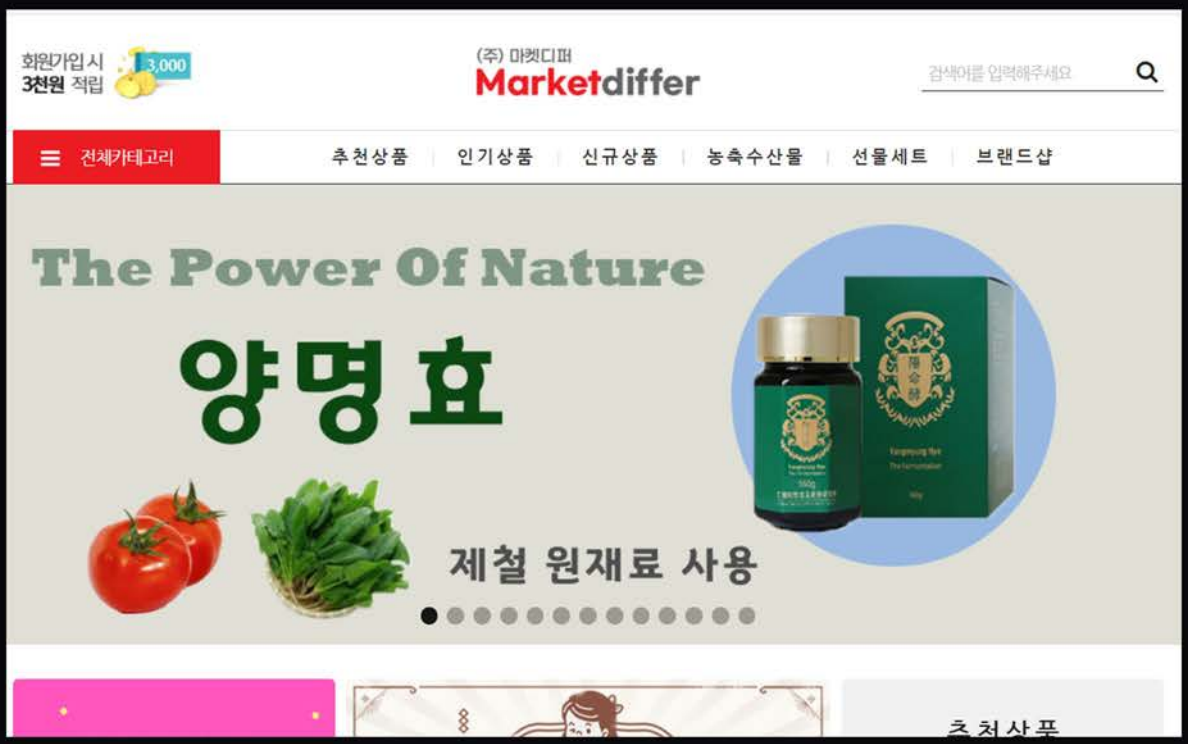
[J-COIN의 상부/하부 레이어 구조]

Blockchain Layer

[블록체인 상부/하부 레이어 구조]

J-COIN의 전자지갑은 HTML5 언어로 구성된 WEB모바일 기반의 반응형 페이지로 구축되어, iOS와 Android를 지원하는 바, 국내외 모든 상용 스마트폰에서의 거래가 용이하게 가능합니다.

3 J-COIN의 운영개념



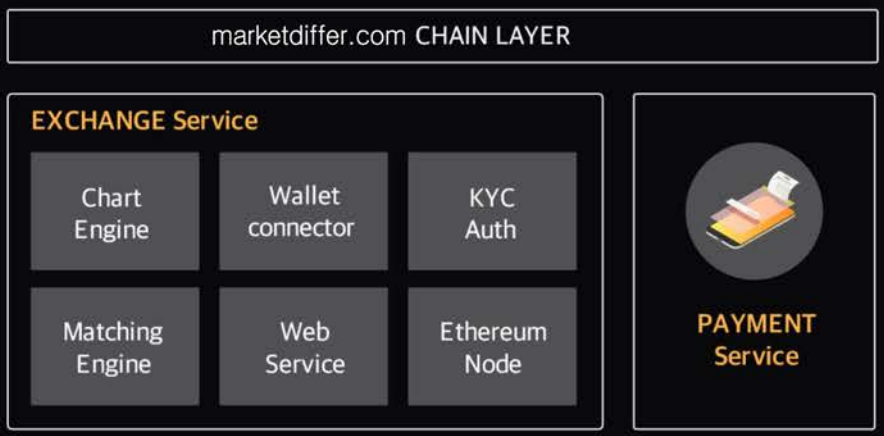
[그림4.marketdiffer.com 쇼핑몰 초기화면]

J-COIN은 컨슈머 마켓 기반의 온라인 쇼핑몰 마켓디퍼(marketdiffer.com)에서 상품을 구매결제 할 때, 지갑에 존재한 JCO는 거래소 시세에 따른 가치로 인정받아 다시 마켓디퍼에서 상품을 실제 결제목적으로 구매 사용할 수 있는 사용→회수의 선순환 메카니즘으로 운영됩니다.

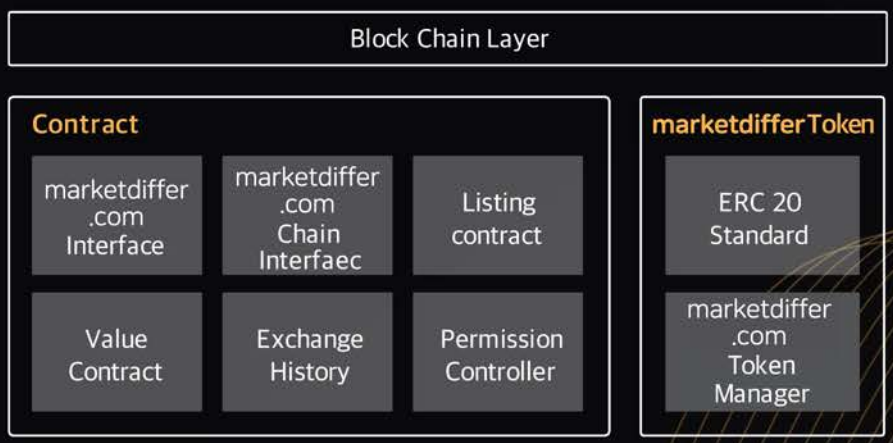
위는 다음 장에 있는 그림과 같이 도식되어집니다.

| J-COIN 선순환 메커니즘 오버 뷰

| marketdiffer.com 체인 레이어 구조



| 블록체인 레이어 구조



위와 같이 J-COIN은 marketdiffer.com에서 상품 구매를 할 수 있는 기본 구조를 채택하고 있으며, J-COIN의 가치는 그 날의 거래소 시세에 따라 인정됩니다

이는 종전 제1세대 암호화폐의 고질적 문제인 경제적 인센티브의 부존재를 해결하는 기능의 측면이 있고, 제4세대 미래형 암호화폐가 목표하는 디지털 거래 실 결제수단도 충족한다 할 것입니다

트레이드 마이닝은 미래시점까지의 보상을 포함하는 바, 거래소에서의 시세가 곧 이익의 크기가 됩니다. 이에 결국 코인 내에서도 잠재적인 디플레이션(Deflation)이 발생되며, 이는 피셔 방정식처럼 실질금리, 소비, 생산에 영향을 끼칩니다.

$$r = i_{LT} + [\text{Deflation}]$$

[Deflation] : Expected rate of deflation
(expressed asa positive number)

$$r = i_{LT} - \Pi^{e}$$

r : Real interest rate

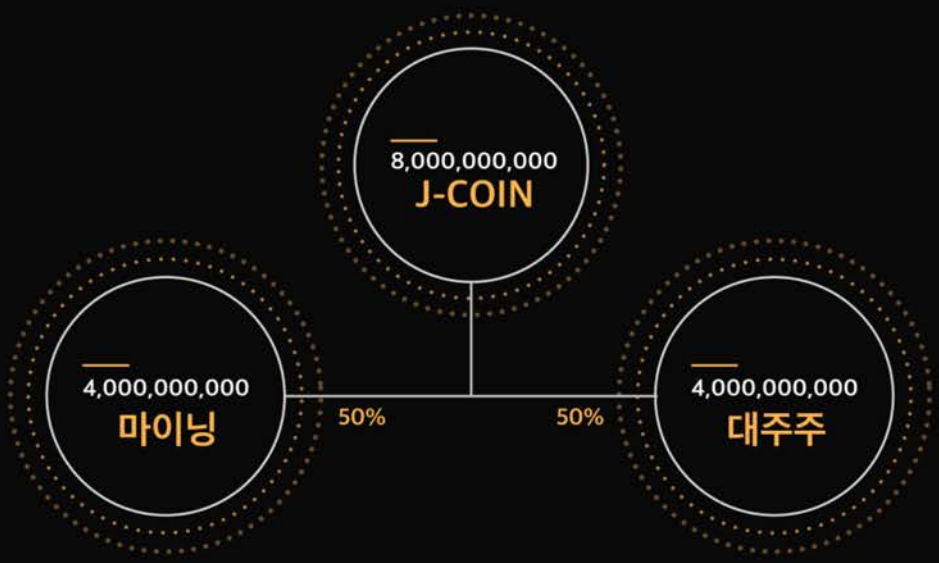
LT : Long-Term norminal interest rate

[피셔(I.Fisher) 방정식]

이에 J-COIN은 marketdiffer.com 라는 경제적 인센티브의 매개체를 적극 도입하여 메기효과를 일으키며, 이에 따라 J-COIN을 사용의 사이클에서 암호화폐 시장과 연결하는 자산(Asset) 역할의 개념으로 운영합니다

4 J-COIN의 배분구조

코인의 거래소 상장 전까지는 총 80억 개의 코인을 상품구매 마이닝 50%(40억 개) 비중으로 배분하고, 나머지 50%는 경영 대주주그룹이 1/2 비율 40억개(전체 50%) 나누어 배분합니다



코인의 거래소 상장 전까지는 총 80억 개의 코인을 상품구매 마이닝 50%(40억 개) 비중으로 배분하고, 나머지 50%는 경영 대주주그룹이 1/2 비율 40억개(전체 50%) 나누어 배분합니다.

경영 대주주그룹의 코인은 안정적인 운영과 코인 및 쇼핑몰 업그레이드를 위하여 사용되고, 특히 경영 대주주그룹 코인은 코인의 가치부양을 위하여 상장 제반비용, 공격적 마케팅 비용의 목적으로 사용되고 이외에도 공격적으로 여러 가지 사업을 진행 목표합니다.

기존 배분된 코인은 상장 후에는 일괄적으로 상장 코인화 되어 거래소 전자 유통된다.

한편, 상장 코인은 해당 거래시세의 가치대로 marketdiffer.com 에서 상품을 구매할 수 있으며, 가치의 변동은 실시간으로 결제가에 반영됩니다.

단, 상장된 J-COIN을 이용하여 marketdiffer.com 에서 상품구매시, 상품가의 5%를 추가 할인 받는 혜택(일명『에누 리매출)의 발생으로 코인 사용자는 시세가치와 별개로 상품가의 5% 가치는 최소한 담보 받게 되는 연동보장이 이루어지게 됩니다.

5 J-COIN의 기술적 배경

| 이더리움 베이스 토큰

J-COIN은 분산 어플리케이션(이른바, dApp)의 제작을 용이하게 하는 목적 프로토콜 규정이 가능한 비트코인의 업그레이드 블록체인 이더리움을 기술적 기초로 하며, 튜닝완전성(Turing-completeness)을 제공하는 이더리움 가상머신(EVM) 기반 워킹 고유언어 솔리디티(Solidity)를 이용하여 프로그래밍하였습니다.

5-1. 비트코인과의 동일 데이터 구조 활용

비트코인 데이터구조의 안전성은 이미 검증된 바이며, 이를 적극 활용하며 구조는 아래와 같습니다.

비트코인 데이터구조를 구성시키는 분산 합의과정은 트랜잭션 패키지인 이른바 블록을 연속적으로 생성하기위해 시도해야 되며, 따라서 이를 도울 노드가 필요합니다.

각 블록은 타임스탬프, 논스, 직전블록의 해시, 직후 발생 모든 트랜잭션의 목록을 가지며, 이 과정에서 범위를 확장시키는 블록체인이 형성되는데, 최신상태를 표시하기 위해 이를 계속 갱신하게 됩니다.

이 갱신의 적정여부를 확인하고자 각 블록의 유효성을 확인하는 알고리즘이 필요하고, 이는 아래와 같습니다.

가. 해당 블록으로 참조된 직전블록의 존재와 유효여부를 확인

나. 타임스탬프 값이 직전블록의 타임스탬프 값보다 큰지와 특정 유효시간 이내 범위인지의 확인

다. 작업증명(PoW) 유효여부확인

라. S[Q]을 직전블록의 마지막상태가 되도록 맞춤

마. TX 를 n 개의 트랜잭션으로 이루어진 블록 트랜잭션 목록으로 우선하고, 폐구간 Q 부터 n-1 의 i 에 대한 S[i+1]=APPLY[S[i], TX[i])집합 중 1 개 이상 오류로 확인 되면 거짓(false) 값을 반환하며 반복문에서 탈출

바. 참(True)값을 반환하고, S[n]을 블록 마지막 상태로 맞춤

위와 같이 블록의 각 트랜잭션은 유효한 상태 변위가 일어나야 하며, 원시상태(Genesis State)때부터 해당 블록까지의 모든 트랜잭션을 순서대로 적용 계산함을 알 수 있습니다.

이 때, 작업증명(PoW)이 적용됨에 따라, 블록의 이중-SHA256 해시 값이 동적 맞춤 목표 값보다 필히 작아야 하는데, 이유는 전체 블록체인에 인위적인 개입자가 생기지 않기 위함에 있습니다.

이리하여 예측불가 유사 난수 함수(Pseudorandom Function)를 만족시키기 위하여 블록 헤더의 논스 값을 증가시켜서 새 해시 값이 위를 만족하는지 반복 확인하게 됩니다.

블록은 여러 계층구조(Multi-layer data structure)에 저장되어지는데, 블록 헤더에는 타임스탬프 등을 포함해 머클트리(Merkle tree)의 루트해시 200바이트 용량의 데이터가 들어가고, 여기서 머클트리란, 바이너리 트리로서 최하위 저층에 기저 데이터가 반영된 무수의 잎 노드와 자기 자신 하위에 두 자식 노드의 해시인 중간 노드, 위 중간 노드의 최상위에 있는 루트 노드의 집합을 의미합니다.

5-2. 전자지갑의 핵심인 이더리움 어카운트 방식

각 트랜잭션이 1회만 처리되도록 하는 카운터인 논스와 이더(ether)잔고, 계약코드, 저장공간 등의 4개의 필드로 어카운트는 구성되어집니다.

위 이더(ether)는 암호연료(Crypto-fuel)로서, 트랜잭션 수수료를 지불하는 용도로 사용됩니다. 어카운트는 프라이빗키로 통제되는 외부소유 어카운트(Externally Owned Accounts)와 계약코드에 의해 통제되는 계약 어카운트(Contract Accounts)로 나누어집니다.

5-3. 거래의 핵심인 메시지와 트랜잭션 방식

메시지 수신처, 발신처 확인서명, 수신처로 보내는 이더의 양, 선택적 데이터 필드, STARTGAS 값, GASPRICE 값 등의 6개 필드로 트랜잭션은 구성되어집니다.

이 중 STARTGAS와 GASPRICE는 안티-서비스거부(anti-Dos)를 수행하는 중요 방어장치입니다. 악의적 과잉계산으로 시스템을 마비시키는 일을 계산 단계수로 제한시켜서 막습니다. 이 때 계산의 연료단위는 gas이고, 이 gas는 계산의 양에 따라 수시로 변동되어지게 됩니다.

즉, 악의적으로 시스템을 마비 시키려면 계산의 양이 현저히 많아야 하기 때문에, 따라서 그 계산을 하기 위해서는 gas도 비례하여 유상지불해야 하므로 함부로 계산을 불필요하게 할 수 없게 되는 것입니다.

한편, 메시지는 메시지 발신처, 메시지 수신처, 이더, 선택적 데이터필드, STARTGAS 값 등의 5개 필드로 구성되어집니다. 앞서의 트랜잭션과 상당히 유사한 구조입니다.

5-4. 상태변환

트랜잭션의 형식확인, 서명 유효여부확인, 논스의 발신처 어카운트 논스와의 일치 하는가 여부가 결국 이더리움 상태변환 핵심 함수인 APPLY(S, TX) →S의 기능이라고 정의할 수 있습니다.

트랜잭션 수수료는 STARTGAS * GASPRICE로 그 총액이 계산되어지며, 발신처 잔고가 부족하면 오류를 발생시킵니다.

5-5. 블록검증 알고리즘

참조 직전블록의 존재와 유효여부를 확인하고, 현재블록 타임스탬프의 참조 직전블록보다 크기가 초과되는지와 현시점 기준 15분 후보다 작은 크기인지 확인합니다.

이후, 블록넘버, 트랜잭션루트, 삼촌루트, gas 리미티드 등이 유효한지 확인하고, 블록의 포함 작업증명의 유효성을 확인합니다.

이 때, S[]을 직전블록의 마지막 상태로 우선하고, 부터 n-1에 대한 S[i+1] = APPLY(S[i], TX[i])를 적용시 오류를 반환 또는 블록소모 총 gas가 GASLIMIT을 초과하면 오류를 반환하게 됩니다. 작업참여자에게는 지불된 보상블록을 S[n]으로 붙이고, 이 머클트리의 블록헤더가 최후상태와 같은지를 확인만 하면, 블록의 유효성을 마지막 절차에 의해 검증까지 할 수 있게 됩니다.

5-6. 토큰시스템

위조불가한 블록체인의 토큰시스템은 J-COIN을 기반하고 있으며, 토큰은 1개의 오퍼레이션을 수행하는 데이터베이스 개념정도에 해당됩니다.

[토큰시스템의 상태변환 함수 적용한 코드]

```
def JCOIN Send(to, valuse):

    if self.storage[msg.sender] >= value:

        self.storage[msg.sender] = self.storage[msg.sender] - value

self.storage[to] = self.storage[to] + value
```

6 J-COIN의 정책

6-1. 생태계 (Eco-System) 구축

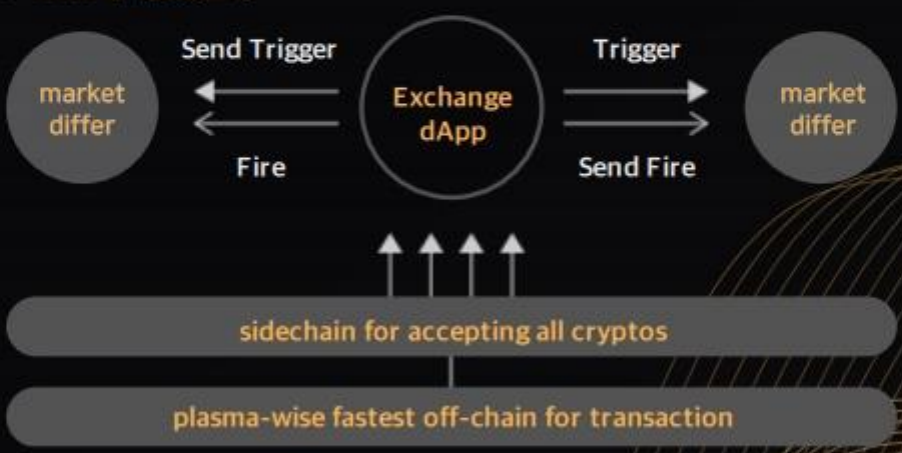
J-COIN은 다양한 계층의 개인, 기업 그리고 국가 경계를 넘는 블록체인 기반의 분산화된 생태계에서 작동되어집니다. 동등한 정보, 접근권한과 거래의 균등한 기회를 제공하고, 실질적인 결제수단으로의 활용성을 보장합니다.

J-COIN 생태계 도식

6-2. 메인넷

이더리움은 비트 코인의 스택 언어를 튜링 완전성으로 진보 시켰고, 이는 스마트 컨트랙트 개념으로 발전되어 블록체인 활용성의 세계를 지수 확장하였습니다.

J-COIN의 메인넷 도식



6-3. KYC 인증

KYC 인증을 통하여 국제 흐름대로 J-COIN은 투명한 운영 및 자금세탁 방지에 동조하며, 신원증명이 된 자는 단계별로 거래규모제한을 해제하고, 신원증명을 위해 이름과 이메일 주소, ETH주소 그리고 신분증 등의 최소정보를 기본으로 요구합니다.

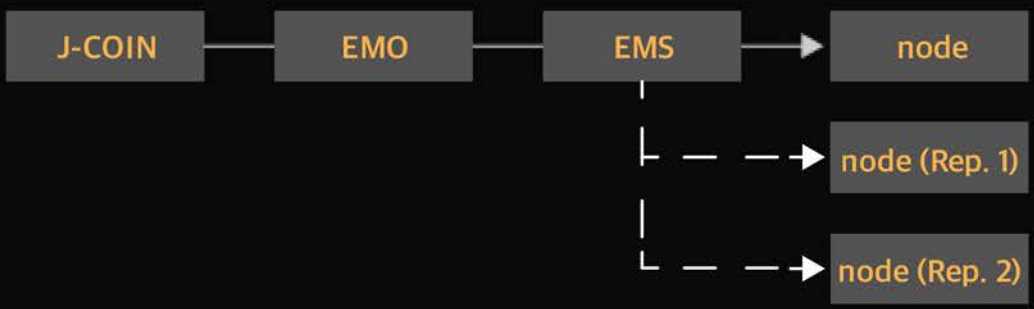
6-4. 서킷브레이커

코인의 변동성은 매우 역동적인 성격을 가지는 바, 다양한 외부요인 변수에 따른 시장충격을 흡수통제 처리하고자 J-COIN 사용자들을 위한 안전장치인 서킷브레이커를 발동할 수 있습니다.

6-5. EMS, EMO를 통한 보안

시장의 흐름과 기술의 발전으로 새로운 약점이 발견된 경우, 코인의 통상정책인 EMS(Emergency Stop)와 EMO(Emergency Off) 기능을 스마트 컨트랙트에 반영하 여 비상상황을 대처할 수 있으며, 임의조작 할 수 없도록 Multi Sig를 기본으로 하되 법률자문(Legal Advisor)의 참관 하에 투명하게 긴급조작을 승인합니다.

J-COIN의 보안정책 도식



7 향후 기술 반영사항

7-1. POST 합의 메커니즘

종전의 권익증명 합의 PoS(Proof of Stake) 합의 메카니즘을 개량한 것으로서, 작업증명 PoW(Proof of Work)의 차세대진보 방식이 POST합의입니다.

PoW 합의 참여 노드는 논스 값을 무한 해독하여, 블록의 해시 값을 일정 조건이 만족될 때까지 작업하게 되 는데, 여기에서 성공적인 블록이 생성되면 그 즉시 기록 장부를 쓰게 됩니다.

단, 이 때, 우수 기록 장부 노드가 다른 기록 장부 노드 통제권을 행사할 수도 있으므로, 노드에 대한 신용 부여가 필요하며, 이로 인해 부여된 각 노드의 신용정보를 바 탕으로 작업증명의 난이도를 조절함으로써 믿 음 가능한 노드와의 합의만을 전제시켜 합의의 신뢰성을 담보시킬 수 있습니다.

이를 POST(Proof Of Stake + Trust)로 명칭하고, 향후 J-COIN에 반영합니다

7-2. 다자간 합의 안전 알고리즘

가. 핵심노드에서 임의의 세트 수를 정함

나. 임의로 생성된 세트 수를 N으로 나눔(N=정수, 모든 사용자수 60% 이상보다 초 과)

다. 위 N으로 나누어진 수를 N명의 각 암호로 지정

라. 모든 사용자는 위 암호를 이용해 N개의 암호를 계산 마. 핵심 노드에서 모든 데이터를 수신 받는 즉시, 권한의 부여

8 참고

| 종전 합의 메카니즘의 종류

- PoW (Proof of Work)

작업증명 합의 메카니즘으로서, 블록생성을 주도하고 노드는 끊임없이 모든 블록 장부에 대응하는 블록해시 값을 계산하며 일정 조건을 만족시킵니다.

- PoW (Proof of Work)

작업증명 합의 메카니즘으로서, 블록생성을 주도하고 노드는 끊임없이 모든 블록 장부에 대응하는 블록해시 값을 계산하며 일정 조건을 만족시킵니다.

- DPos (Delegated Proof of Stake)

권리위탁증명 합의 메카니즘으로서, 투표를 통하여 일정 수량의 노드를 선출하여 일정조건을 만족시킵니다

- PBFT (Practical Byzantine Fault Tolerance)

실용 비잔틴 장애허용 합의 메카니즘으로서, 소식을 전달하는 과정에 3단계의 일 치성을 확인 후 일정조건을 만족시킵니다.

| 참고 - 문헌

- S.Nakamoto, Bitcoin : A peer-to-peer electronic cash system, bitcoin.org, 2009

- Tapscott, D.Tapscott, How blockchain is changing finance, Havard Business Review, 2017.

9 법적고지 및 면책사항

본 백서는 J-COIN(JCO) 프로젝트(이하 JCO)가 추진하고자 하는 컨슈머마켓 쇼핑몰 기반의 구매보상형 디지털결제포인트 블록체인토큰에 대한 정보를 제공하고자 작성하였습니다. 이 백서를 통해 저희 플랫폼에 투자를 권유하고자 하는 목적이 아니며 그와는 전혀 무관합니다. 또한 저희 J-COIN(JCO) 팀은 이 백서를 작성 당시를 기준으로 작성하여 제공하는 것으로서, 결론을 포함해서 백서 상의 어떤 내용도 장래 시점까지 정확하다는 점을 보증하지 않습니다.

J-COIN(JCO) 팀은 이 백서와 관련하여 여러분에게 어떠한 사항도 정확성을 진술 및 보장하지 않으며, 그에 대한 법적 책임을 부담하지 않습니다. 그 예로 J-COIN(JCO) 팀은 i) 백서가 적법한 권리에 근거하여 작성되었으며, 제 3자의 권리를 침해하지 않는지, ii) 백서가 상업적으로 가치가 있거나 유용한 지, iii) 백서가 여러분이 가지고 있는 특정한 목적의 달성에 적합한 지 iv) 백서의 내용에 오류가 있는지 등을 보장하지 않습니다. 물론, 책임 면제의 범위는 앞서 든 예에 한정되지 않습니다.

여러분이 자신의 의사결정 등 행위에 있어 이 백서를 이용(백서를 참고하거나 이를 근거로 한 경우도 포함하되 이에 한정되지 아니한다)한 경우, 그에 다른 결과는 이익, 손해 여부를 불문하고 전적으로 여러분의 판단에 따른 것입니다. 다시 말해 이 백서를 이용함으로써 여러분에게 손해, 손실, 채무 및 기타 피해가 발생하더라도 J-COIN(JCO) 팀은 그에 대한 배상, 보상 기타 책임을 부담하지 않는다는 점에 유의하시기 바랍니다.

미래 예측 진술에 대한 경고문

(a) 본 백서에 명시된 특정 표현들은 프로젝트의 미래, 미래 사건, 전망 등에 대한 예측성 진술을 담고 있습니다. 이러한 내용은 역사적 사실에 기반한 진술이 아니며 '예정,' '추정,' '믿음,' '기대,' '전망,' '예상' 등의 단어와 유사한 표현들로 식별됩니다. 본 백서 외 발표자료, 인터뷰, 동영상 등 기타 공개자료에도 이러한 미래 예측 진술이 포함될 수 있습니다. 본 백서에 포함된 미래 예측 진술은 J-COIN(JCO) 및 관계사의 향후 결과, 실적, 업적 등을 포함하지만 이에 국한되지 않습니다.

(b) 미래 예측 진술은 다양한 리스크 및 불확실성을 포함하고 있습니다. 이러한 진술은 미래 성과를 보장하지 않으며 따라서 지나치게 의존해서는 안됩니다. 리스크 및 불확실성이 현실로 구체화되는 경우 J-COIN(JCO) 및 관계사의 실제 성과와 발전은 미래 예측 진술에 의해 설정된 기대와 다를 수 있습니다. 향후 이러한 상황에 변화가 있어도 J-COIN(JCO) 및 관계사는 미래 예측 진술에 대한 업데이트를 제공할 의무가 없습니다. 본 백서, J-COIN(JCO) 및 관계사의 홈페이지와 기타 자료 등에 포함된 미래 예측 진술을 바탕으로 행동을 하는 경우 미래 예측 진술의 내용이 실현되지 않는 것에 대한 책임은 오로지 귀하에게 있습니다.

(c) 본 백서가 작성된 날짜를 기준으로 J-COIN(JCO) 플랫폼은 완성되었거나 완전히 운영 중인 상태가 아닙니다. 향후 J-COIN(JCO) 플랫폼이 완성되고 완전히 운영될 것이라는 전제 하에 설명이 작성되었지만, 이는 플랫폼의 완성 및 완전한 운영에 대한 보장 또는 약속으로 해석되어서는 안됩니다.

자금세탁방지법(AML)

구매자는 J-COIN(JCO) 팀의 J-COIN 코인 (JCO) 및 기타 관련 파생상품(있는 경우)을 통해 자금 세탁, 불법적인 통화 거래 및 기타 제한된 활동에 어떠한 형태로든 참여하지 않겠다는 데 동의해야 합니다. 각 참여자는 J-COIN(JCO) 코인 (JCO) 및 기타 관련 파생상품을 자금 세탁을 목적으로 직, 간접적 판매, 교환 및 처분할 수 없다는 사실을 숙지하여야 합니다.

중요사항

관련 정책, 법률 및 규정, 기술, 경제 및 기타 요인의 빈번한 변경으로 인해 본 백서에 제공된 정보는 정확하지 않을 수 있고, 신뢰할 수 없거나 최종적이지 않을 수 있으며, 여러차례 변경될 수 있습니다. 본 자료는 오직 참고를 위한 용도로만 제공됩니다. 저희 팀은 제공된 정보의 정확성 및 정당성에 책임을 지지 않습니다. 참여를 희망하는 사람은 본 백서에 있는 정보에만 의존해서는 안됩니다. 저희는 참여자들이 후원에 앞서 자체적으로 조사하기를 권장합니다. 본질적으로 본 백서는 사업제안서 혹은 사업 홍보 문서이며, 그 어떠한 경우에도 법적 구속력을 갖지 않습니다. 본 문서에 명시된 내용은 단지 참고용이며 J-COIN(JCO) 구매자는 스스로 추가적인 주의를 기울여야 합니다.

언어의 해석

본 문서는 한국어와 영어로 제공됩니다. 분쟁 발생 시, 저희는 국문 버전(KOREAN version)을 근거로 문제를 해결할 것입니다. 본 백서의 보다 정확한 해석을 위해서는 국문 버전을 참고하여 주시기 바랍니다.

THANKS

FOR WATCHING