
몰(MOL)
모바일네트워크의 블록체인경제

목차

1. 블록체인 편년사 1
1.1 비트코인과 블록체인 1
1.2 이더리움과 블록체인 2
1.3 DAG(방향성비순환 그래프)과 블록체인 2
2. 왜 몰체인인가? 2
2.1 소액결제 3
2.2 모바일네트워크 3
3. 몰체인의 기술적 특성 3
3.1 디자인로직 3
3.1.1 블록리스 4
3.1.2 스마트계약 5
3.1.3 토큰발행 6
3.2 컨센서스 산법: POW and DPOS 6
3.2.1 Proof of work 6
3.2.2 DPOS 6
3.3 성능 7
3.4 크로스체인 7
3.5 화폐경제 8
3.5.1 staking 이자 8
3.5.2 보상 9
3.5.3 경제모델 9
3.5.4 몰 배분 9
4. 총결 10
5. 사용환경 10
5.1 실시간결제 11
5.2 소액결제 11
5.3 포인트의 토큰화 11
5.4 게임칩 11
6. References: 11
7. Appendixes 첨부 12
7.1 몰 스마트계약 (토큰발행) 정의 및 함수유형 12
7.2 몰 MVM 에 의한 이더리움 EVM 의 변화 (명령) 13
7.3 몰체인:모바일네트워크의 블록체인경제 14

몰:모바일네트워크의 블록체인경제

Alex Qian[1] Halton Xu[2] Sandy Ye[3] Harry He[4] Eddy Guo[5]
Molecule Foundation, Singapore

개요: 성능의 평준화는 비트코인과 이더리움이 대표하는 블록체인경제의 발전의 가장 큰 걸림돌이다. 다만 산출속도 (Block rate)의 향상,블록크기(Block size)의 증가 및 컨센서스효율의 향상은 현재 지속적으로 퍼블릭 블록체인의 발전을 이끌고 있다.현재 주요 해결 방안으로는 이더리움을 포함한 스마트계약의 샤딩 혹은 Zilliqa 의 네티워크 샤딩; 레이어링, UTXO 방식의 실시간 결제 네트워크; 컨센서스 효율, 작업증명(POW)부터 권한증명(POS),비잔티움 장애 허용(BFT),DPOS 등은 모두 한계점에 이르렀다.블록을 데이터 저장의 매개로 하는 체인은 이미 탈중앙화,성능,안정성의 "불가능삼각"에 진입했다. DAG(방향성비순환 그래프)는 혁신적인 해결방안으로 IOTA 의 M2M(machine to machine) 과 Nano 의 결제방식이 바로 좋은 예시이다. 몰체인은 Nano“블록진영”에서 계발을 얻어 거래와 블록을 분리시켜 블록리스를 구현했다. DPOS 컨센서스,이더리움 EVM 방식으로 Dapp 토큰발행이 용이하고 50 밀리초 단위로 컨펌, DAG 퍼블릭 블록체인의 수수료 면제 등으로 구성되어있다.

1. 블록체인 편년사

1.1 비트코인과 블록체인 1.0

2008 년 미국발 금융위기는 기존의 독점형 금융구조의 리스크에 대해 큰 경각심을 불러일으켰으며 같은 해 발표된 비트코인 백서는 큰 관심을 불러을이켰다. P2P 개념의 탈중앙화된 경제개념을 최초로 구현한 가상화폐는 이후 전통경제학자들로부터 129 번의 "사망선고"를 받았으나 불과 몇년만에 그 가치가 수만배나 증가하는 기록을 세운다.비트코인은 설계 초기부터 안전성과 용량의 균형유지(Trade off)의 우선시 했으며

[1] Alex Qian: Blockchain developer and M.tech from IIT, Delhi, Serial Entrepreneur
[2] Halton Xu: Blcokchain architect, Full stack developer, Linux, C++, Node,
[3] Sandy Ye: Full stack and crypto wallet developer with 13 years' of coding
[4] Harry He: Full stack and blockchain engineer of MOL
[5] Eddy Guo: Blochain Engineer of MOL

용량을 희생하여 안전성을 확보했다.이것이 바로 비트코인 전송시간이 1 시간이상 걸리는 이유이다.

1.2 이더리움과 블록체인 2.0

비트코인 전문지 기자 Vitalik Buterin 는 블록체인 기술의 업그레이드는 인류를 새로운 지적 혁명의 시대로 이끌 것이라고 단언했다.비트코인의 스크립트 언어를 스마트계약으로 승화 DAO(Decentralized Autonomous Organization) [3]시켜 미래형 네트워크의 새로운 형태를 선도한다. 하지만 POW 방식의 이더리움은 역시 성능문제가 존재하며 하나의 cryptokitty 도 전체 네트워크를 마비시킬 수 있다.

1.3 DAG(방향성비순환 그래프)와 블록체인 3.0

현재 세계적으로 부유한 국가 상위 20 개국이 전세계 개인용 컴퓨터의 75%를 사용하고 있다. 즉 나머지 25%의 PC 는 178 개국에서 사용중인 것이다. 예컨대 인구대국인 인도의 경우 PC 호황기를 경험하지 못하고 직접 모바일 시대로 돌입했고 모바일 뱅킹은 아프리카 대륙에서 이미 기존의 오프라인 은행업무를 대체했다. 데스크탑 PC 기반의 서비스를 제공했던 블록체인 1.0-2.0 은 90%의 모바일 디바이스 이용자들에게는 쉽게 접근할 수 없는 장벽이었다. 몰체인 이러한 문제를 완벽히 해결 할 수 있는 모바일 기반의 블록체인 생태계이다.

기존 블록체인은 그 확장성 문제가 비트코인과 이더리움에서 파생된 분포식 경제의 확산에 큰 걸림돌이 되었다. 특히 블록체인의 크기와 생성속도 문제는 블록체인 발전에 슬럼프를 가져왔다. 현재 가장 효과적인 대안으로 떠오르는 것이 바로 방향성 비순환 그래프 (DAG) 및 라이트닝 네트워크로 실시간 과금 구현이 가능하며 특히몰체인만의 스마트 계약 을 이용해 수수료가 전혀 발생하지 않는 DAG 블록체인이 완성되었으며 최고 50 밀로초의 실시간 거래가 가능해졌다. 즉 이론적으로 네트워크 속도 환경의 영향만 받을 뿐 블록체인 자체의 딜레이는 전혀 없는 것이다.

2. 왜 몰체인인가 ?

2.1 소액결제

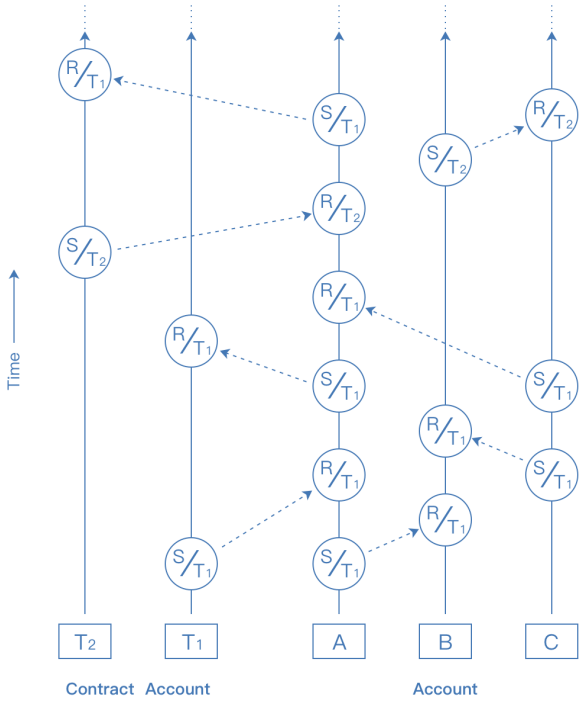
소액결제의 특징은 일상화와 대중화이다. 하지만 현재 가상화폐의 가장 큰 단점은 소액결제에 이용할수 없다는 것이다.비트코인 1 시간,이더리움 10 분이라는 전송시간 장벽이 있으며 수수료도 무려 2 달러 이상이 소요된다.몰체인은 가상화폐로서 50 밀리초라는 실시간 결제방식과 수수료 전액 면제라는 혁신적인 특징이 있다.

2.2 모바일네트워크

휴대폰으로 소액결제가 가능하기 때문에 몰체인은 탈중앙화된 블록체인 경제체계로 모바일 플랫폼의 변화를 이끌 수 있다. 다양한 콘텐츠,게임,SNS 등 다양한 서비스에서 몰체인은 실시간,수수료면제,포인트의 토큰화,새로운 가상화폐 발행 등 다양하게 사용될 수 있다.3. 몰체인의 기술특성.

3. 몰체인의 기술특성

3.1 디자인원칙



몰의 구조

MOL 몰의 구조는 모든 유저가 스마트계약을 통해 자신만의 체인을 갖고 있으며 A 유저가 이체거래 요청및 비밀키에 서명하면 전파망을 통해 B 유저가 거래를 수락하는 방식이다.

3.1.1 블록리스

블록체인과 채굴자는 근본적으로 블록체인 성능을 제약한다.전세계적으로 이를테면 비트코인 10 분,라이트코인 3.5 분,이더리움 15 초 등 최소한의 컨펌시간 필요하며 블록이라는 몰드 안에서 진행된다.또한 비트코인의 경우 약 10 분간의 POW 과정을 거쳐야 한다.

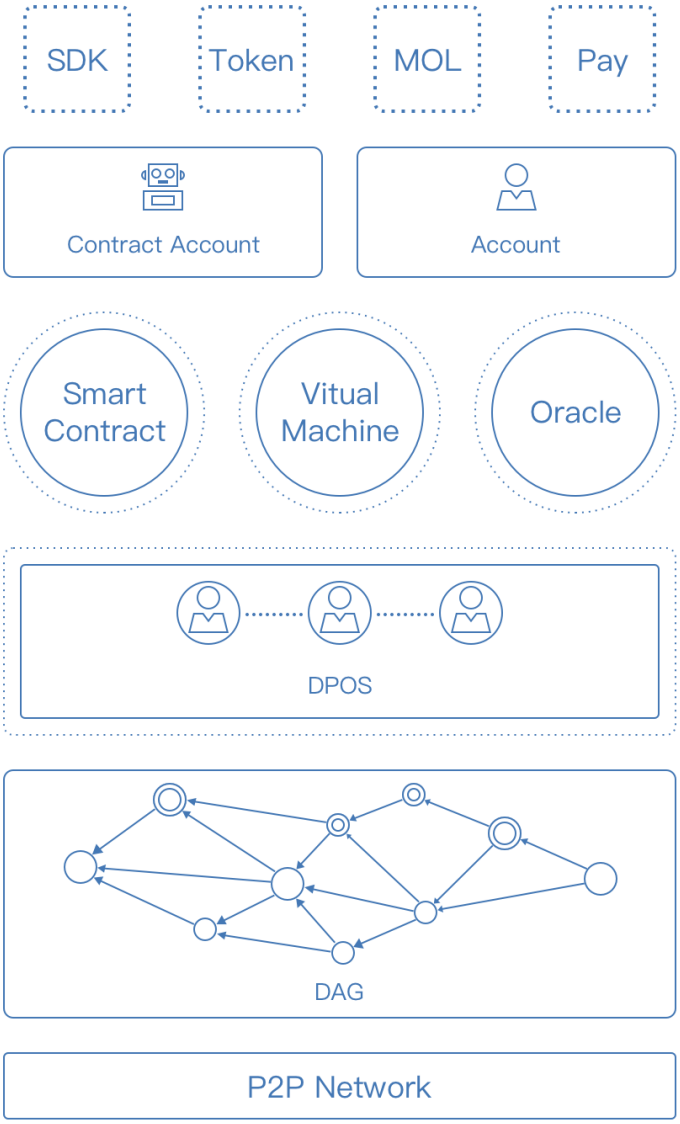
도전 :

a. 설명절 등 수억명이 계좌이체를 동시에 이용할 경우 비트코인은 1 분에 최대 3 건을 거래할 수 있지만 VISA 카드는 4700 건,알리페이는 10 만건까지 처리할 수 있다.후자들은 블록체인인의 영향을 받지 않는다.

b. 채굴자들은 블록체인의 생산량을 컨트롤 하여 블록체인 경제에 막강한 권력과 영향력을 행사한다.또한 혼잡성 때문에 최대 비트코인은 최대 100 달러, 이더리움은 최대 2 달러의 수수료가 발생하며 이는 비트토렌트가 애초에 추구하던 무료,평등의 철학(Peer-to-Peer)에 엄중이 위배된다.또한 코인 채굴을 위해 해마다 10 억달러의 컴퓨터 하드웨어 비용이 소진된다. 현재 전세계적으로 약 500 만명만이 비트코인을 보유,사용하고 있으며 만약 이 숫자가 5 천만,5 억명이 될 경우 채굴,유지비용은 큰 부담이 될 수 밖에 없다.

c. 블록 채굴자의 작업 원가는 이미 극한으로 치닫는 상태이다.비트코인과 이더리움 이 두가지 블록네트워크의 유지비만 해도 매년 10 억달러 이상의 전기사용료와 하드웨어 비용이 소모된다. 현재 전세계에서 약 500 만명만이 비트코인을 사용하며 이 인구가 5000 만 혹은 5 억으로 증가할 경우 해당 비용은 더이상 유지하기 불가능해진다. 작업증명 원가를 감소하기 위해 과거 10 년간 POW 부터 Asics-resilient Scrypt , X11 , Cryptonight 를 포함한 [5] 1.0 , 2.0 , 3.0 의 peercoin[6] , Nxt , Qutm[7], DPOS 의 BTS , Steem , EOS ,BFT 클럽 , dBFT , fBFT , pBFT 심지어 하이브리드 연산법까지 등장했다. 즉 작업증명 부분에서는 이미

창의력이 고갈된 상태이며 중앙화도 심화되고 있다. 아직도 사토시 나카모토의 원론적인 블록이론에서 벗어나지 못하고 있는 것이다. MOL 퍼블릭 체인의 경우 IOTA[8]与 Nano[9]의 블록리스 블록구조가 사용되어 근본적으로 블록의 한계에서 해탈할 수 있게 되었다.



MOL 프로토콜 스택

3.1.2 스마트계약

IOTA 와 Nano 의 디자인적 결함은 바로 스마트계약을 계약을 지원하지 않는 것이지만 MOL 은 DAG(방향성비순환 그래프)로 출발하여 혁신적인 디자인으로 계약형 계정을 개발하고 이 계정이 일반계정과 동일한 기능을 할 수 있게 구현했다. 개설,전송,수신,대표명의 전환 등 기능이 모두

가능다. 매 계약계정마다 하나의 독립적인 체인이며 초기 블록으로 시작하여 전송과 수신 거래 모두 블록리스의 블록체인이다.

3.1.3 토큰발행

유저의 콘텐츠 생성 UGC (User Generated Content) 부터 유저의 토큰생성 UGC (User generated Currency)까지, 이러한 거시적인 발전방향은 MOL 개발팀이 추구하는 완전한 탈중앙화된 Dapps 으로 토큰 발행을 구현한다는 이념과 일치하다.

a. 몰은 비교적 안정화된 이더리움 EVM 을 MOL 의 DAG 구조에 맞게 적용하여 solidity 계약을 MOL 체인으로 이식하는데 용이하다.
b. 몰은 편역기를 친구인터페이스에서 연동하여 이름,번호,발행량만 입력하면 누구나 자신만의 토큰을 발행할 수 있게 구현했다.
c. 스마트계약을 생성된 토큰은 초기 블록에서 일반계좌로 배분할 수 있으며 사전에 설계된 일정 비율에 따라 교환할 수 있다.

3.2 작업증명 : POW 와 DPOS:

3.2.1 Proof of work

는 불량정보 공격을 방지하기 위해 모든거래가 몰 네트워크로 전송되기 전 한번의 작업증명 연산과정을 거친다.불량정보 공격의 원가를 증가하기 위해 약 수초간의 시간이 연산시간이 필요하지만 이는 지갑을 여는데 필요한 몇초간의 시간으로 충분하기 때문에 체감상 실시간 거래가 가능하다.몰이 사용하는 해시산법은 ED25519&Blake2b。

3.2.2 DPOS

MOL 은 DPOS 더블스펜드처리기술(Double-spend)을 사용한다. 작업증명 효율 면에서 POW<POS<BFT<DPOS 순이며 DPOS 는 작업원가가 가장 저렴한 관계로 가장 효율적이라고 볼 수 있다. 더블스펜드는 소프트웨어에 버그 혹은 악성공격피해가 발생했을 경우에만 발생하므로 작업증명 (투표 0) 으로 처리 가능해 작업효율을 한층 더 향상할 수 있다.매 지갑노드는 자신의 대표 (Representative) 를 지정 및 변경할 수 있다.공증방법은

$$T' = \sum_{i=0}^{n} \sum_{j=0}^{m} Token$$
$$(n = sum\ of\ Representative, m = sum\ of\ account\ under\ \ each\ representative),$$
$$T = Gensis$$

예를들어 T^'>T ,

일 경우 더블스펜드 발생, 대표는 투표를 통해 2 개 혹은 여러개의 더블스펜드 중 하나를 선택할 수 있다.

3.3 성능

블록리스의 구조 설계는 거래와 네트워크 방송의 송도로 전송,컨펌된다.50 밀리초 (1 초 =1000 밀리초) 이며 거래가 병렬형태로 진행되므로 이론적으로 실시간 및 무제한 거래량 처리가 가능하다.

3.4 크로스체인

2009 에 탄생한 라이트코인은 하드포크로 Monero , Dash , Zcash 등 코인을 발행했다. 상대정으로 중앙화된 Stellar 와 Ripple 및 이더리움,Aethernity、카르디노(ADA),IOTA ,Byteball 등 DAG 체인 ,Lisk、Ark 등도 같은 방식의 코인이다. 서로 다른 블록체인에 속한 자산들은 반드시 중앙화된 거래소를 거쳐야만 전환된다.

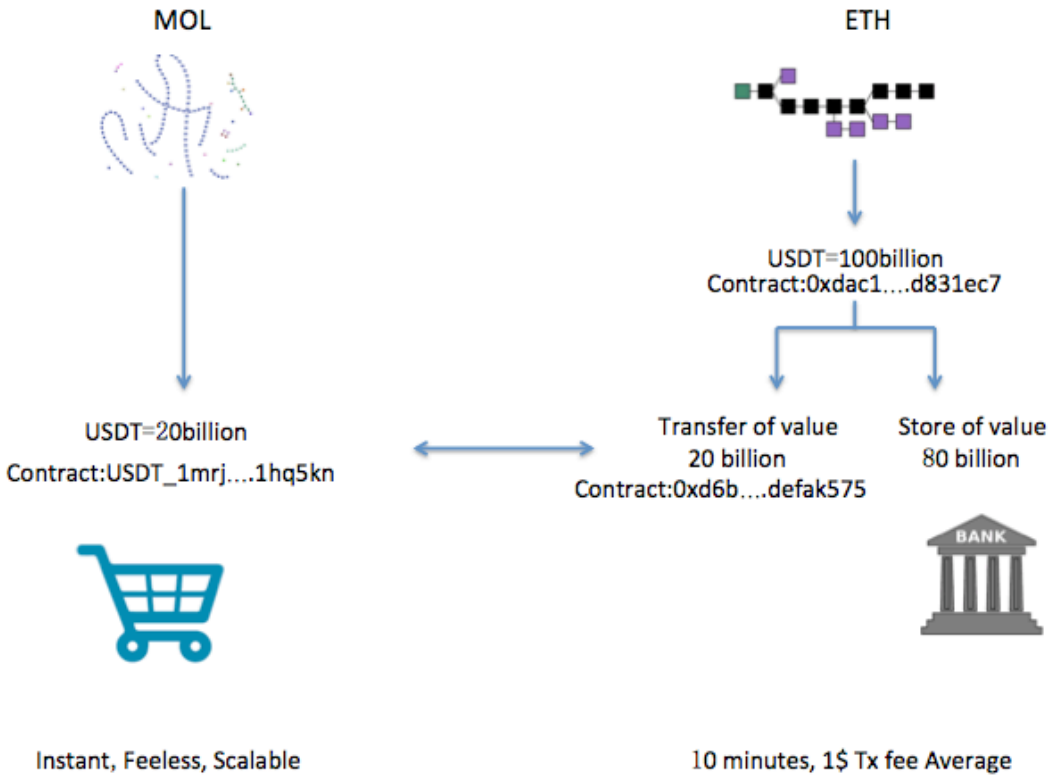
몰체인 기반및 그 스마트계약의 크로스체인기술은 아래와 같은 원칙을 적용한다:

(1) Value of Reserve 비축금

(2) 양방향 조준

(3) 스마트계약

(4) 가치샤딩



Ethereum(이더리움)기반의 USDT 의 경우, 예를들어 발행량이 1000 억개라면 그중 80%는 store of value 의 기준화폐로 체인이 아니므로 거래수수료가 발생하지 않는다.또한 USDT 의 유통가치(Transfer of Value)를 제한한다이더리움 기반의 토큰은 유통능력의 부족으로 평균 컨펌시간이 10 분, 약 1 달러의 이체비용이 발생하여 소액결제에 사용하기 부적합하다. 하지만 이더리움의 최대가치는 기업의 융자와 도와주는 기능으다.또한 이더리움 토큰은 증권의 형태로 존재하여 유통에 최적화될 필요가 없다.비트코인의 경우 소장형으로 1 시간 이상의 거래시간과 100 달러이상의 거래비용은 불합리하다고 볼수 없다. 하지만 일부 토큰, 이를테면 USDT 등 유통을 목적으로 하는 토큰의 경우 반드시 크로스체인 기술을 사용하여 그 가치를 수수료 면제의 체인으로 이전시켜야 한다. 몰체인의 경우 그 가치는 Store of value 과 Transfer of Value 분류되어 200 억의 USDT 를 이더리움-MOL 공증계약에 홀딩한다. 비축금이 준비된 후 몰체인에서 동일한 가치,동일한 금액의 USDT 를 유통시킨다.

3.5 화폐경제

3.5.1 staking 이자

네트워크 안정성을 보장하기 위해 몰체인이 무료이긴 하지만 지갑 노드는

일정기간동안 몰체인을 보유해야 하며 연간 5.5%의 이자도 발생한다.이런 과정을 일컬어 민팅 (minting) 이라고 한다.

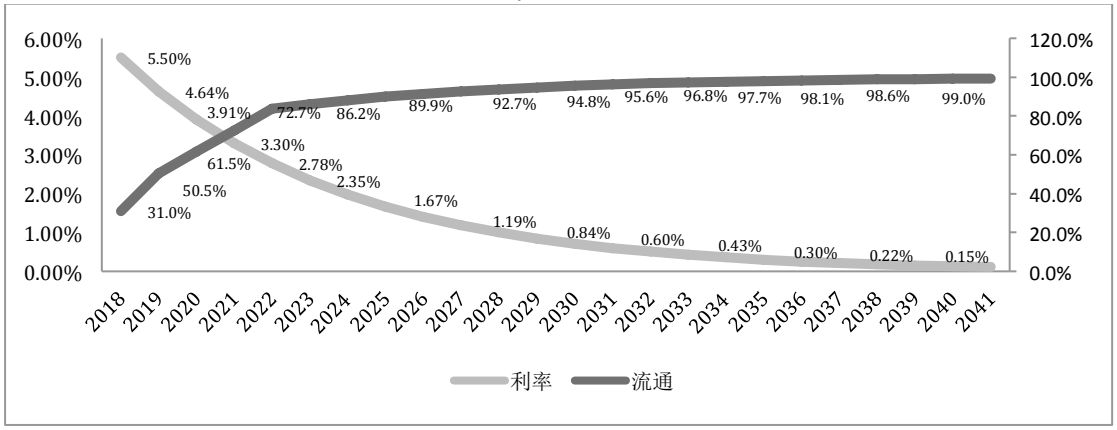
3.5.2 보상

계정이 대표를 선택하는 관계로 대표는 일명 공헌증명이라 불리는 POC (proof of contribution) 메카니즘을 이용한다. 대표가 여러 계정을 파생케 격려하고 더욱 좋은 서비스를 제공하기 위해 일부 토큰을 보상의 형태로 대표에게 지급한다.몰체인의 전체 지급량 중 일부 고정포지션 이자와 공헌보상의 형태로 단독으로 저축되며 이는 정기적으로 일정한 계산법을 거쳐 지갑과 대표의 노드로 지급된다.

3.5.3 경제모델

$$T_{n+1} = T_n * [1 + 0.8^n * 0.025]$$
$$T_0 = 0.8312$$

(주의:T 는 MOL 이 n 에서의 유통 총량이다.초기 금리는 5.5%이며 100 년 후 더이상 금리가 발생하지 않는다)



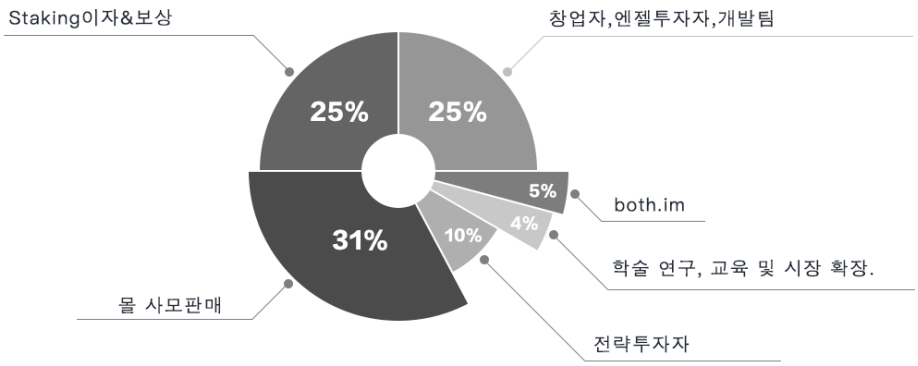
3.5.4 몰 배분

총량이 400 억개로 몰체인은 향후 4 년간 65%의 몰체인(MOL)을 커뮤니티에 배포해 진정한 오픈소프트웨어를 지향한다.

비율	배분방안	내역	설명
31%	몰 사모판매	Moore 의 사모판매 수입은 몰체인기금회의 운영,개발,마케팅,재무,법무관리 등에 사용된다.	
10%	전략투자자	몰체인의 발전에 기여한 전략투자자를 위한 보상	고정포지션 4 년,매년 1/4 씩 활성화

25%	창업자,엔젤투자자,개발팀	창업팀,엔젤투자자,개발팀은 몰체인의 발전에 큰 기여를 한 점이 인정되어 몰 코인을 그 보상으로 지급한다.	고정 포지션 4 년, 매년 1/4 씩 활성화
25%	staking 이자&보상	지갑노드는 장기간 일정수량의 MOL 을 보유할 것을 요구합니다. 보유한 MOL 은 이자를 생산하며 대표가 기타 하위 계정을 양산시키도록도모합니다.대표에게는 일정금액의 토큰이 보상으로 지급된다	
4%	학술 연구, 교육 및 시장 확장.	MOL 의 학술적 연구,개발 교육,시장 확장,몰체인 기술에 대한 인식향상및 기타 오픈소스 커뮤니티에 대한 공헌 등에 사용됩니다.	
5%	both.im	both.im 앱의운영,발전과 MOL 지갑유저에게 사용된다.	

몰(MOL)분배



4. 총결

몰체인은전복성방향성비순환그래프(DAG)와 블록리스화(Blockless)디자인으로 개발되어 50 밀리초의 거래 컨펌이 가능한 특성을 가진다.고도의 확장성과 무제한(unlimited)의 성능으로 수수료가전혀 없어 액결제,실시간결제,고액결제,사행성게임,온라인커뮤니티 등에 활용할 수 있다.증강형 이더리움 EVM 과 스마트계약 역시 MOL 퍼블릭체인으로 하여금 소액결제가 필요한 다양한 금융서비스 앱으로 파생 개발이 가능케 한다.

5. 사용환경

5.1 실시간결제

비트코인은 1 시간,이더리움및 ERC20 토큰은 10 분간의 컨펌시간이 필요하지만 몰체인은 50 밀리초의 컨펌시간으로 사실상 실시간 결제가 가능하여 오프라인 외식,엔터테인먼트(영화,개인방송,전자도서,음악)등 다양한 분야에서 결제 방식으로 사용할 수 있다.

5.2 소액결제

알리페이의 연간 거래액이 100 조위안을 돌파했지만 여전히 비트코 100 달러,이더리움및 ERC20 토큰이라는 수수료는 암호화폐가 결제시장에 설 자리가 없게 만들고 있다.하지만 몰체인은 전자들의 문제를 모두 해결하여 가장 안전하고 신속한 차세대 결제수단으로 자리매김 할 전망이다.

5.3 포인트의 토큰화

Dapp 은 기존의 해결방안을 채택, 이를테면 이더리움 포인트의 토큰화에서 가장 큰 문제점인 시간 소모를 해결해 결제수단으로서의 한계에 직면한 상황을 타개했다.

5.4 게임칩

게임(마작,포커)등은 실시간 거래가 빈번하게 일어나므로 무료,실시간 입출금은 필수이다.몰체인은 토큰을 게임 칩으로 유저들에게 지급하는 방식으로 기존의 다양한 게임서비스에 즉시 적용되어 사용할 수 있다.

6. References:

[1] Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto
[2]https://www.caseyresearch.com/they-killed-bitcoin-129-times-each-time-it-came-back-even-stronger/
[3] A next generation smart contract & decentralized application by vitalik buterin
[4] CryptoKitties craze slows down transactions on Ethereum

http://www.bbc.com/news/technology-42237162
[5] Non-Interactive Proofs of Proof-of-Work
[6] https://peercoin.net/
[7] Qtum white paper
[8]
https://www.reddit.com/r/Iota/comments/6h3sc8/what_are_the_cons_of_iota/
[9] Nano: A Feeless Distributed Cryptocurrency Network

7. Appendixes 첩부

7.1 스마트계약의새로운 정의 및 데이터구조

계좌개설

```
open {
account:mol_1ob1gzhrpxdmoka7szc9iy7jtfnuysz8kkuu3ga6fni3ypquu3e7bfi3t9cr,
source:486C0A0A13F06C5CFC01684CFC1E612050827C4C8080695524A69AD0175E37A8,
representative:mol_3ytentj15q44he4c778317r868wdttwufp96fsccjux4tuqc59ojgrwn6d4w,
work:5806aa8b5b317585,
codeHash:04F952F3BE920D09E7CD7AE648E8293A4445CC1C27F2D210E1C78EAF9952EF43,
type: open,
signature:FCDB24B64DC82AD9EFE8DAA333054E58BC4D4A2A8F61E739DB7A82901976586D1BED
ECE5B206734C770CC6FAD13A79836780AEFDBAA4D92606929D6656F03603
}
```

개설약관

```
contract {
account: mol_3mfo37obgskt7gcy4n63efie1m8r45wij5fb734se1g1soc85fza5ffpzrpm,
source:CDB5096A97665A2B95E150816360C04CD810F9088DA928459601C0CD5461B7E8,
representative:mol_3o4p44jtc6ij9i789bzzze14xdw6sx9tziejiki54u1dmrq71fkmqc7fr  o68,
work: f04f53f1d80a213b,
```

```
init: PUSH1 0 CALLDATALOAD SLOAD NOT PUSH1 9 JUMPI STOP JUMPDEST PUSH1 32
CALLDATALOAD PUSH1 0 CALLDATALOAD SSTORE
data: 2020202020
type: contract,
signature:F153D770DD834BAAEEC57BD2262C7D78CF771C899B9AC3F230C6DDFE8CE1F02C472F
2F9345A4845D6D5DA9EDED3A038149295208ED95C9CDFF894C53DD8BFA01
}
```

전송약관

```
csend {
account:mol_3xh5yoa4imaat66mmg6y7fr8baks45bnwyfytapygo8nda73aqpio3yidcgm,
source:1F022C454D2BCAD35BB4F3FF8C5B9B263B0BF016563FADF569E395DE8754B5C
E,
representative:mol_1nfdb7scmjta76qoafn1zc8ri6o9hd9k44azg8obgkbgnogxr5bt3gfyx8mk,
work: 4c71b5959ff864d5,
type: csend,
signature:05D60DFCBFA55EBFBF644CB6E801B21C2C10558D815DA5859B4C46D4C2663
264DD1FB8E52C0290FD958B099F806BB28407EA37CE40D7517B0C5A276EB2C3D107
}
```

수신약관 :

```
creceive {
account:mol_1oi8ax4kjb7hrn8un5bo3f349dsp1yme4q5ksihokdwx314gw96t856zrery,
source:BDE1AA3A6118A37E74DECF32906C372E482B5678BB3BBB635238AB42CEAE1C
FE,
representative:mol_1murykq3jduwbnojjczsgx5brqf7awnsufk6rtyxsfnbpxfzrofi66i9ezih,
work: 843f6a1593a5c1b2,
type: creceive,
signature:5CF02E89078DEAA4C34960D233B49C0468BA157544DF1AA491BDEE43EDC5B
340762DD4868BB9EE3E35A99408F7C39809DFC9D84F2B5167FBACE29A6FCD6CE70B
}
```

7.2 몰스마트계약 (토큰발행) 정의및 함수유형

Name(명칭)

```
function name() view returns (string name)
```

Symbol (기호)

```
function symbol() view returns (string symbol)
```

Decimal(소수점)

```
function decimals() view returns (uint8 decimals)
```

Total supply (총액)

```
function totalSupply() view returns (uint256 totalSupply)
```

Balanceof (잔액)

```
function balanceOf(address_owner) view returns (uint256 balance)
```

Transfer(이체)

```
function transfer(address_to, uint256_value) returns (bool success)
```

Transferfrom(출금)

```
function transferFrom(address_from, address_to, uint256_value) returns (bool success)
```

Allowance(허용한도)

```
function allowance(address_owner, address_spender) view returns (uint256 remaining)
```

Event 이벤트

Transfer (이체)

```
eventTransfer(address indexed _from, address indexed _to, uint256 _value)
```

Approval(승인)

```
eventApproval(address indexed _owner, address indexed _spender, uint256 _value)
```

7.3 몰 MVM 이 이더리움 EVM 에 대한 개변(명령집)

0s: Stop and Arithmetic Operations(정지 및 대수 연산 명령집)

명령코드	힌트키워드	EVM 어의	MVM 어의
0x00	STOP	停止	동일
0x01	ADD	덧셈	동일
0x02	MUL	곱하기	동일
0x03	SUB	차감	동일
0x04	DIV	나누기	동일
0x05	SDIV	나누기	동일
0x06	MOD	모(여)	동일
0x07	SMOD	모듈로연산	동일
0x08	ADDMOD	덧셈 후 모듈로연산	동일
0x09	MULMOD	곱한 후 모듈로연산	동일
0x0a	EXP	덮어씌기	동일
0x0b	SIGNEXTEND	기호확장	동일

10s: Comparison & Bitwise Logic Operations(비교및 비트연산 명령집)

명령코드드	힌트키워드	EVM 어의	MVM 어의
0x10	LT	비교보다 작음	동일
0x11	GT	비교보다 큼	동일
0x12	LGT	비교보다 작음(기호)	동일
0x12	SGT	비교보다 큼(기호)	동일
0x14	EQ	상등비교	동일
0x15	ISZERO	0 인여부	동일
0x16	AND	병렬	동일
0x17	OR	와	동일
0x18	XOR	와 혹은	동일
0x19	NOT	비교	동일
0x1a	BYTE	바이트를취함	동일

20s: SHA3 (SHA3 명령집)

명령코드	힌트키워드	EVM 어의	MVM 어의

0x20	SHA3	计算 SHA3	동일

30s: Environmental Information(환경정보명령집)

명령코드	힌트키워드	MVM 어의	MVM 어의
0x30	ADDRESS	계좌주소 불러오기	동일
0x31	BALANCE	잔액 불러오기	동일
0x32	ORIGIN	발송자주소 불러오기	동일
0x33	CALLER	파이선주소불러오기	동일
0x34	CALLVALUE	이체금액 불러오기	동일
0x35	CALLDATATOTAL	데이터 불러오기	동일
0x36	CALLDATASIZE	데이터크기 불러오기	동일
0x37	CALLDATACOPY	파라미터를메모리에 복사	동일
0x38	CODESIZE	코드크기 불러오기	동일
0x39	CODECOPY	코드를 메모리에 복사	동일
0x3a	GASPRICE	연료가격불러오기	다름
0x3b	EXTCODESIZE	코드크기 불러오기	동일
0x3c	EXTCODECOPY	데이터를메모리에불러오기	동일
0x3d	RETURNDATASIZE	데이터크기	동일
0x3e	RETURNDATACOPY	데이터를메모리에불러오기	동일

40s: Block Information(블록정보명령집)

명령코드	힌트키워드	EVM 어의	MVM 어의
0x40	BLOCKHASH	블록의 해시 불러오기	다름(불필요)
0x41	COINBASE	수익자주소	다름(불필요)
0x42	TIMESTAMP	타임스탬프	다름(불필요)
0x43	NUMBER	블록번호	다름(불필요)
0x44	DIFFICULTY	블록난이도	다름(불필요)
0x45	GASLIMIT	연소한도	다름(불필요)

50s: Stack, Memory, Storage and Flow Operations(스택,메모리,저장공간,조작명령집)

명령코드	힌트키워드	EVM 어의	MVM 어의
0x50	POP	데이터팝업	동일
0x51	MLOAD	메모리로딩 word(M) 동일	동일
0x52	MSTORE	word 를메모리에저장하기 동일	동일
0x53	MSTORE8	바이트를 저장하기	동일
0x54	SLOAD	로딩 1 个	동일
0x55	SSTORE	word 를하드에 저장하기	동일
0x56	JUMP	스킵명령	동일
0x57	JUMPI	조건스킵명령	동일
0x58	PC	계수기 값	동일
0x59	MSIZE	메모리크기 불러오기	동일
0x5a	GAS	가용 연소수 불어오기	다름

0x5b	JUMPDEST	목적지스	동일

60s & 70s: Push Operations(스택조작명령집)

명령코드	힌트키워드	EVM 어의	MVM 어의
0x60	PUSH1	바이트를스택에 입력	동일
…	…	…	…
0x7f	PUSH32	32 바이트를스택에입력	동일

80s: Duplication Operations(복사조작 명령집)

명령코드	힌트키워드	EVM 어의	MVM 어의
0x80	DUP1	1 대상복사	동일
…	…	…	…
0x8f	DUP16	32 대상복사	동일

90s: Exchange Operations(교환조작명령집)

명령코드	힌트키워드	EVM 어의	MVM 어의
0x90	SWAP1	1 과 2 대상 교환	동일
…	…	…	…
0x9f	SWAP16	1 과 17 의대상교환 동일	동일

a0s: Logging Operations(로그조작 명령집)

명령코드	힌트키워드	EVM 어의	MVM 어의
0xa0	LOG0	주제 설정안함	동일
…	…	…	…
0xa4	LOG4	4 개의 주제	동일

f0s: System operations(시스템조작명령집)

명령코드	힌트키워드	EVM 어의	MVM 어의
0xf0	CREATE	계약 생성	동일
0xf1	CALL	다른계약 사용	동일
0xf2	CALLCODE	계약코드 사용	동일
0xf2	RETURN	중단및 돌아가기	동일
0xf4	DELEGATECALL	code 사용 Tx 보류	동일
0xfe	INVALID	무효한 명령	동일
0xff	SELFDESTRUCT	계약상	동일