SEEKCHAIN

시크체인

자발적인 디플레이션 탈중앙화 금융 인프라

목록

시크체인(Seekchain): 자발적인 디플레이션 탈중앙화 금융 인프라

개요

시크체인(Seekchain)은 기존의 비싼 계산과 전력 자원을 장부 체계의 저장매체로 사용하는 것을 대신하여, 더 깨끗하고 경제적인 하드 디스크 자원을 사용하고 있는 탈중앙화 금융 인프라이다.

시크체인(Seekchain)은 증분연소증명(IPOB,Incremental Proof Of Burning)이란 새로운 컨센서스 메커니즘으로 분산이 가능하며, 저렴한 저장자원을 신뢰할만한 금융 협업 플랫폼으로 전환시켜 준다. 시크체인(Seekchain)은 IPOB 메커니즘을 통해 자발

적인 디플레이션 경제 모델을 구현할뿐 아니라 주기적인 인센티브로 커뮤니티 발전을 위해 마이닝풀을 자극하며, 마이닝풀의 수량이 급증함과 동시에 그룹이 더욱 분산되고, 교체반복된 체인 협치와 결합되어 시크체인(Seekchain)이 생태와 기술 측면의 이중 탈중앙화를 실현할 수 있는 것이다.

동시에 시크체인(Seekchain)은 전환가능한 컨센서스 배치 방식을 채택하여, 용량증명에서 데이터 저장 증명으로, 또한 생태중에 마이너와 마이닝풀이 적은 비용으로 메모리 마이너와 검색 마이너로의 진화가 가능하게 된다. 체인 초대 인센티브 시스템, 지분 자원 배분과 장부 자정 프로토콜, DAO 조직이 관리하는 Defi 솔루션 모음, 프라이빗 거래 등 중요한 기능들도 시크체인(Seekchain)의 생태적인 폭발력, 경제적 지속가능성, 비즈니스 리얼리티 적용성과 사용자 신분의 안전성을 극대화시켜 확장해 준다.

프로젝트 배경

비트코인의 시가총액은 수천억 달러에 이르지만 전세계 전기 사용량의 약 0.33%를, 즉 호주 전국의 전기 사용량과 맞먹는 수량을 소비하고 있는데 이 비율은 계속 높아지고 있다. 마찬가지로 ETH 1.0 의 에너지 소모도 전세계 전기 사용량의 0.03%를 차지하고 있다. 사실 블록체인 기술 자체와 커뮤니티의 컨센서스는 둘의 높은 가격을 만들어 냈을뿐만 아니라 인공 대상, 하드웨어 그리고 에너지 원가도 가격 형성 과정에도 중요한 역할을 했다.

다자간에 신뢰가 필요없는 컨센서스를 형성하는 데에 원가가 있는 것은 자명한 사실이다. BTC 와 ETH1.0 의 경우에 원가는 주로 전력과 하드웨어의 해시 레이트이며, EOS나 ETH2.0 Casper와 같은 지분증명에 기반한 방안의 경우에 코인이 스테이킹할 때 소모된 시간 비용이며, FilSEEKoin 경우에 시공간증명할 수 있고 실제 의미있는 저장 서비스 비용이다. 사실 분산형 장부가 구축 과정에서 고착화하는 자원 원가는 바로 그 장부가 공격과 분식을 저항하는 능력이기 때문에 장부를 구축하는 초기에 경제적 측면에서 우선 고려해야 할 것은 어떤 자원으로 컨센서스를 지탱하냐 하는 것이다.

Burst 팀이 POC 컨센서스 메커니즘을 통해 해시레이트 자원을 대신 하드 디스크 공간 자원의 사용방법을 채택 후, 업계에선 경제 모델이 유사한 프로젝트를 선보였으며, 이들은 모두 비즈니스와 금융 측면에서 혁신적 가치를 결핍되어 있었다. Web 3.0 기술 구조에서, IPFS 프로토콜의 커뮤니티 영향력과 분산향 비즈니스에 상상력이 점점 커짐에 따라, 투명한 통화와 탈중앙화 금용 발전 단계가 서서히 탄생했다: 하드 디스크 공간 자원에 기반하여 공간증명을 걸쳐 복제증명과 시공증명으로 진화한 후, 블록체인 기술의 발전과 성숙에 따라 점차 거대한 탈중앙화 금용 인프라를 구축할 수 있게 되었으며, 우리는 이 인프라가 시크체인(Seekchain)이라고 명명했다, 시크체인(Seekchain)은 현재 블록체인 및 암호화폐와 전통적인 금용 업계에 다음과 같이 존재하는 문제들을 해결해 나갈 것이다.

블록체인과 암호화폐가 직면한 문제

문제유형	문제내용	Seekchain 솔루션

핵심성	해시레이트와 마이닝풀의 중앙화	IPOB 증분연소증명 컨센서스 메커니즘
	협치와 개발의 중앙화	체인 협치
	해시레이트가 적은 경우의 안전성	제네시스 마이닝풀
	낮은 확장성	WASM 가장머신과 제 2 층 확장방안
연관성	고에너지 소모	저에너지 IPOB 컨센서스 메커니즘
	채굴기 폐기	IPOB 에서 IPFS 프로토콜로 전환 가능
무결성	세부화하고 완전한 솔루션 빠짐	탈중앙화 조직이 관리하는 Defi 솔루션
체험성	테스트 네트워크의 안전성과 시뮬레이션성	장부 자정 프로토콜
	프라이버시가 없음	프라이빗 거래 Private Transactions
	장부의 팽창 문제	장부 자정 프로토콜

전통 금융 산업이 직면한 문제

문제내용	Seekchain 솔루션
사용자들의 자체적 자산통	누구나 비밀계정을 만들어 자산을 스스로 통제가능

제	
자산의 글로벌화 운영과 투자	글로벌 서비스와 거래
중개소로 운영과 사용원가가 높아짐	직접적인 콘트랙트를 통하여 중개비용을 줄일 수 있다
사용자에게 차별서비스	사용자마다 자유롭고 평등하게, 모든 금용 서비스를 받을 수 있다
거래 상대방의 리스크에 영향을 받는 문제	사용자들이 직접 콘트랙트와 교호한다
투명성의 결핍	콘트랙트는 미리 작성되어 모든 사람들에게 같은 방식으로 시행하며, 분산형 장부에서 전부 확인할 수 있다
불필료한 감독과 심사	누구나 모든 금용서비스 사용 가능

증분연소증명 IPOB

IPOB(Incremental Proof of Buring) 증분연소증명 컨센서스 메커니즘은 POC(Proof of Capacity)의 확대집합이다. 시크체인(Seekchain)에서 마이너들이 IPOB를 시행해야 일정한 유효 해시레이트와 채굴 보상 수취율을 획득할 수 있으며 POC 채굴로 채굴 보상을 얻을 수 있다.

시크체인(Seekchain)은 IPOB 컨센서스를 통해 더욱 성장성있고 마이닝풀 레벨에서 더욱 탈중앙화된 커뮤니티 구조를 구축하려 한다. 해당 매커니즘은 마이닝풀이 POW 컨센서스를 채택함에 따라 피할 수 없는 중앙화는 수용하지만, 마이닝풀 에서 인센티브를 통한 경쟁성을 통해 POW 와 POC 컨센서스 분야에 오래된 중앙화 문제를 해결해 줄 수 있다.

기초 경제 개념

마이너 관리 콘트랙트

시크체인(Seekchain)에 위치하며 마이너의 상태를 관리하는 콘트랙트이다.

누적 연소 수량

마이너가 [마이너 관리 콘트랙트]로 이체하며 누구도 상환하지 못한 코인의 누적 수량이다. 해당 값이 높을수록 마이너의 유효 해시레이트와 채굴 보상 수취율이 높아지며, 마이너들이 SEEK 코인을 연소할 때마다 두 가지 사항에 영향을 끼치게 된다. 시크체인(Seekchain)에서 마이너들이 일정한 SEEK 코인을 연소해야 기초한 유효 해시레이트와 채굴 보상 수취율을 얻어 마이닝에 참여 가능하다.

채굴 보상 수취율

마이너들이 블록패킹을 작업할 경우 실제로 얻을 수 있는 채굴보상과 전액 채굴 보상의 비율이다. 해당 값이 실제함으로 인해, 블록을 패킹할 때마다 SEEK 전체 계획 발행량에서 일정한 SEEK 를 영원히 연소하여 없애는 셈이다.

유효 해시레이트

마이너들의 누적 연소 수량이 부족할 경우, 실제로 얼마나 많은 해시레이트를 가지고 있던간, 채굴 보상은 단지 누적 연소 수량에 대응하는 채굴 보상 수취율에 따라 계산될 것이다. 즉 마이너가 시초에 코인 연소 작업만 했다면 나중에 Plot 하드 디스크로 더 많은 해시레이트를 얻을 수 있어 블록패킹 확률이 높아질 것이어지만 채굴 보상 수취율이 변하지 않기 때문에, 유효 해시레이트를 늘리기 위해 들어간 비용은 새롭게 생긴 수익보다 크게 된다.

단위 유효 해시레이트 가격

마이너가 1T 해시레이트를 활성화하기 위하여 연소해야 할 SEEK 의 수량이다. 일반적으로 누적 연소 수량의 증가에 따라 해당 마이너에 대한 해시레이트 가격은 점차 낮아질 것이다.

단위 채굴 보상 수취율 가격

마이너가 채굴 보상 수취율 1%씩 올리기 위하여 연소해야 할 SEEK 의 수량이다. 일반적으로 누적 연소 수량의 증가에 따라 해당 마이너에 대해 단위당 채굴보상 수취율 가격이 빠르게 높아질 것이다.

기술 개념

Shabal / Sha256 / Curve25519

Shabal, Sha256 그리고 Curve25519 는 시크체인(Seekchain)이 주로 사용하는 암호화 해시 함수이다. Shabal 은 상당히 무겁고 느린 암호화 해시 함수로써 SHA256 등 많은 함수들과 관련이 있다. Shabal 은 용량증명 암화화폐 방안에 가장 적합한 암호

화 알고리즘이다. 이 알고리즘은 미리 계산된 해시값을 노드에 저장하도록 허용하고, 작은 실시간 검증을 수행하기에도 충분한 속도를 가지고 있기 때문이다.

Hash

해시값은 암호화 해시함수의 1회 계산 결과로 특별한 설명이 없는 경우 본 문에서 업급한 해시값은 일반적으로 32바이트로 구성되어 있다.

Plot file

마이닝할 때 마이닝 프로그램은 디스크에서 미리 계산된 해시값을 판독할 것이며, 해당 해시 값이 저장되는 것이 바로 Plot file이다.

Nonce

한 plot파일에서 일련의 nonce가 저장되어 있으며, 해시값 8192개가 한 nonce에 들어 있으며, 이 nonce의 크기는 256K 바이트이다. 각 nonce마다 독립된 길이가 8바이트인 코드가 있으며 코드의 범위가 0-18446744073709551615 (2^64)이다.

Scoop

각 nonce에 포함된 해시값 8192개가 서로 다른 4096개의 장소에 투입 될 것이며 각 Scoop마다에 해시값 2개가 투입된다.

Account ID

plot 파일을 만들 때 해당 파일은 마이너의 디지털 계정 Account ID 와 연결되어 있으며 이 ID 는 nonce 를 만들 때에 사용될 것이다. 서로 다른 마이너가 만드는 nonce 번호가 같아도 실제 nonce 가 다르게 된다.

Deadline

Deadline 은 마이닝 과정에서 서로 다른 마이너들끼리 경쟁하기 위해 사용된 값인데 이 값은 plot 파일에 있는 nonce 에 기반하여 계산된 것이다. 이 값이 지갑에 제출되면 지갑이 deadline 시간(초)내에 네트워크에 다른 노드에서 온 블록 브로드캐스팅(방송)을 수신하지 못할 경우 블록 패킹을 시작하게 된다.

Base Target

Base Target 는 지난 24 블록의 블록패킹 상황에 근거하여 계산된 것이다. 이 값에 따라 마이닝 난이도를 조정하며, 이 값이 작을수록 마이너가 작은 timeline 을 찾기가 어렵다.

Network Difficulty

네트워크 난이도를 뜻하고 약칭은 NetDiff 이다. 네트워크에 있는 마이너들의 P 디스크 파일의 총량을 평가할 수 있으며, 단위는 T 로 한다. 이 값은 각 블록에 대응하는 base target 의 변화에 따라 달라지며, 최소 가장 가까운 360 블록의 난이도 평균값이다.

Block Generator

새로운 블록이 패킹될 때 사용할 계정이 바로 block generator 이다. 즉 deadline 이 필요할 nonce 에 대응하는 계정을 찾는 것이다.

Generation Signature

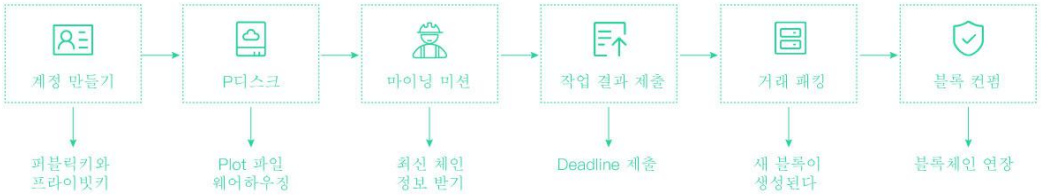
Generation signature 는 지난 블록의 generation signature 와 block generator 에 기반하여 블록 하나를 패킹하는 데에 사용되며 길이는 32 바이트이다.

Block Signature

Block signature 는 block generator 가 블록을 패킹할 때 생성되는 것이며 블록내에 있는 대부분 데이터와 block generator 의 프라이빗키를 Sha256 과 Curve25519 해시 계산으로 얻는 서명이며 길이는 64 바이트이다.

컨센서스 프로세스

IPOB 의 기본 방향은 계산을 초기 단계에 두는 것이다, 즉 해시계산의 결과를 하드 디스크에 미리 저장해 두고 시행 단계에서 저장된 데이터를 검색하는 것을 통해 POW 알고리즘에 있는 대량 해시 계산을 줄이며 소량의 해시계산만 사용할 것이다. 조건에 맞는 데이터를 더 빨리 검색할수록 해당 마이너가 블록을 패킹하는 확률이 더 높아진다.



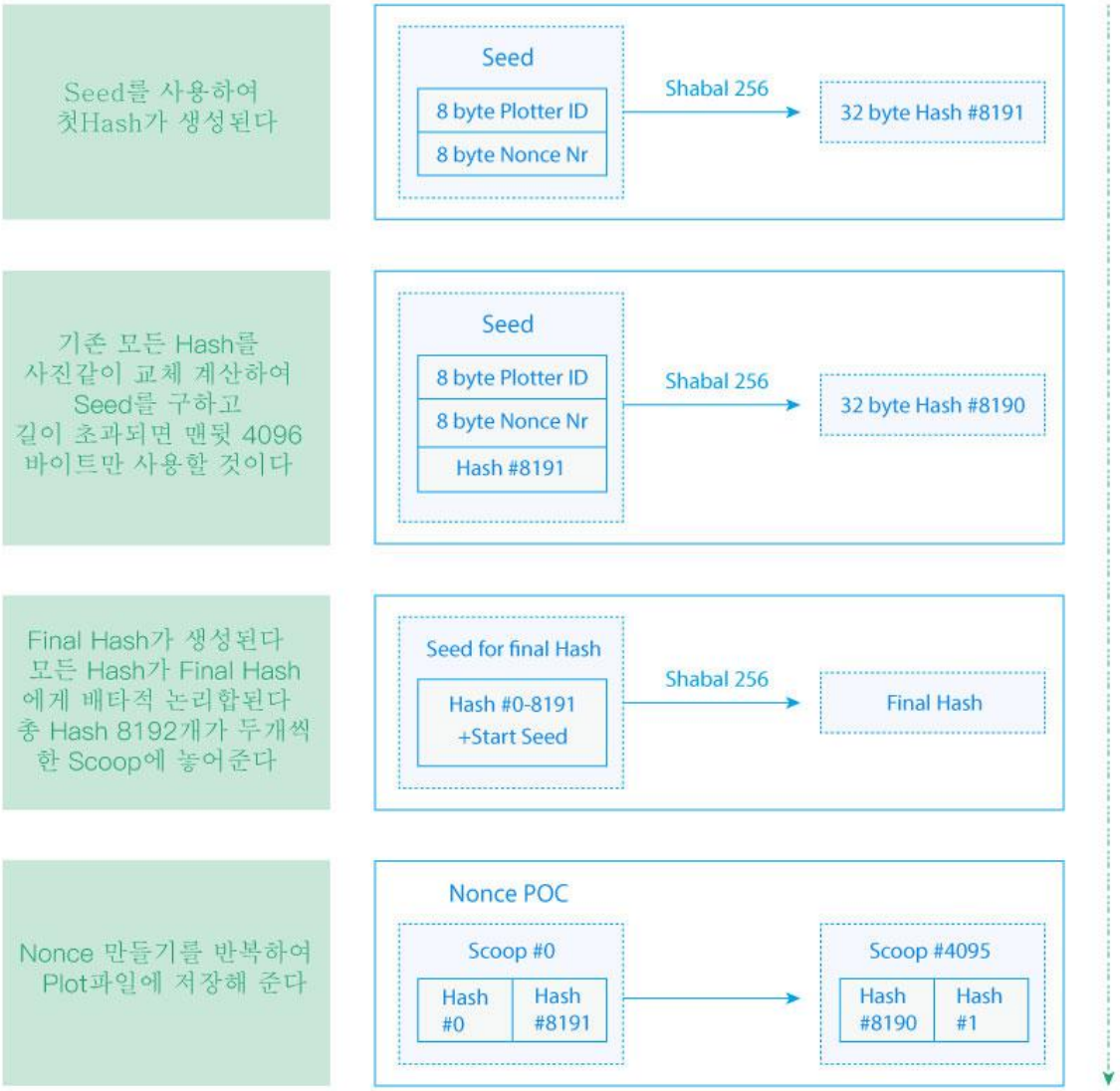
플로팅(Plotting)

마이너가 로컬 하드 디스크에서 파일 플로팅한다. Shabal256 알고리즘을 자기의 퍼블릭키와 결합하여 해시계산을 진행한 후에 결과를 디스크에서 기록한다. 마이너가 가지고 있는 플로팅 디스크 파일의 크기는 해시레이트와 동일하며, 또한 다른 마이너와 블록패킹을 하게 될 경쟁능력과 확률을 나타낸다.

플로팅을 한번 한 후 수익 계정이 변하지 않는 경우 다시 플로팅할 필요가 없다. 또한 마이닝할때 로컬 파일에서 검색만 진행 함으로 전기를 많이 소모하지 않고, 하드 디스크에게 수명을 줄일 수 있는 빈번한 작업도 하지 않을 것이다.

시크체인(Seekchain)은 최적화된 Plotting 2 방안을 사용하여 plot파일에 있는 Scoop 데이터를 다시 배열해 준다. 동일안 Scoop# 데이터를 같은 곳에 두고 마이너가 Scoop 4096 데이터를 읽으려고 할 때 순서대로 모든 데이터를 한번만 판독함으로서, 검색 시 더 효율적이고 기계식 하드 디스크의 어드레스가 느리는 특성에 적절히 부합한다.

Plotting 프로세스와 단계별 산출 안내도:



마이닝(Mining)

마이너가 지갑을 통해 최신 정보를 얻고 마이닝한다. 최신 블록 정보에는 새 Generation signature, Base target 과 Next Block height 가 포함되어 있다. 지갑이 이 정보를 발송하기 전에 Previous generation signature 를 지난 블록 생성기와 함께 서명 Generation signature 를 만들고 Shabal256 을 통해 새 Hash 를 계산한다. 마이너

가 새 32 바이트로 서명을 생성하고 8 바이트 블록 높이를 채택하고 Shabal256 의 Seed 로 같이 관리한다. 계산된 결과는 Generation hash 라는 해시값이 될 것이다.

이후에 마이너가 파일을 plot 처리하는 데에 사용할 Scoop Number 를 찾아내기 위해 해당 해시에 대해 간단한 수학 운산을 진행한다. 이는 Generation Hash 에 대해 4096 모델을 사용하여 이루어진다. 왜냐하면 scoops 가 정해진 수량만 존재하기 때문이다.

다음 단계는 모든 plot 파일에 있는 모든 Nonce 의 모든 64 바이트인 Long scoops 전체를 판독하는 것이다. 이것들은 개별적으로 Shabal256 과 새 Generation signature 를 공동처리하며, 최종적으로 Target 이라는 새로운 Hash 를 얻게 된다. 해당 Target 가 Base target 을 나누면 얻는 결과의 앞 8 바이트값이 바로 Deadline 이다.

위에 제시한 과정을 반복하여 각각 Scoop 가 계산 완료될 때까지 다시 모든 deadline 에서 최소 시간과 최소 값을 대표할 수 있는 Deadline 을 찾는다. 이 Deadline 은 지난 블록이 생성되고 나서 다음 블록이 생성되기 전까지 시스템이 기다려야 하는 시간길이를 나타낸다.

해당 시간길이 안에 아무도 다음 블록을 생성하지 못다면 기존 마이너가 블록패킹 권한을 얻게 된다. 아래 공식은 마이너가 마이닝 결과를 제출하는 방법을 제시하는 것이고, Rust 언어로 표시된다.

```rust
fn submit_work_poc(&self, nonce: H64, account_id: Address, submission_height: u64) -> Result<SubmitNonce> {
    let time_first :u64 = Local::now().timestamp_millis() as u64;
    match helpers::submit_work_detail_poc(&self.client, &self.miner, nonce) {
        Ok(_) => {
            let header :Header = self.client.best_block_header();
            let current_number :u64 = header.number();
          //  let next_number = current_number + 1;
            let isvalid_address :bool = self.provider.has_account( address: account_id);
            if isvalid_address && submission_height == current_number {
                let time_second :u64 = Local::now().timestamp_millis() as u64;
                let time_s :u64 = time_second - time_first;
                Ok(SubmitNonce {
                    result: String::from( s: "Success"),
                    request_processing_time: time_s,
                    deadline : header.deadline()
                })
            } else {
                let time_third :u64 = Local::now().timestamp_millis() as u64;
                let time_ser :u64 = time_third - time_first;
                Ok(SubmitNonce {
                    result: String::from( s: "Failure"),
                    request_processing_time: time_ser,
                    deadline :0
                })
            }
        }
```

블록 구조(Forging)

시크체인(Seekchain)은 ETH 클라이언트 Parity 에 기반하여 개발되고 튜링 컴플리트 스마트 콘트랙트를 지원하므로 블록 크기 제한은 블록의 Gas limit 에 따라 최대 8M 에 달할 수 있다. 동시에 거래당 휴대할 수 있는 Data 데이터 크기도 제한된다.

지갑은 사용자나 네트워크으로부터 받은 컨펌되지 않는 모든 거래를 먼저 수취한 후, 모든 거래가 처리완료될 때까지 혹은 제한이 걸릴 때까지 최대한 많은 블록을 패킹한다. 지갑은 판독한 모든 거래가 유효 서명과 정확한 타임스탬프를 가지고 있는지 등에 대해서 검증한다. 동시에 지갑은 모든 거래건수와 수수료도 종합한다. 블록은 각 거래의 거래 ID 와 모든 내용이 포함된 Sha256 해시값 하나만 포함할 것이며 거래는 별도로 저장될 것이다. 이 외에 블록은 많은 다른 값들의 집합을 포함할 것이다.

최장 체인 규칙 (Longest Chain Rule)

마이너가 마이닝할 때 해시값의 발생이 랜덤하게 발생하며, 네트워크가 지연되는 상황 마이너 두명이 동시에 블록을 패킹할 가능성이 존재한다. 이런 상황이 발생하게 되면 그들이 함께 장부를 기록하게 되면 블록체인 상 포크가 되는 상황이 발생하게 될 것이다.

시크체인(Seekchain)은 최장 체인 포크 선택 규칙을 채용하여 네트워크가 포크될 경우에는 마이너들이 상대적으로 긴 체인을 선택해서 마이닝을 진행한다. 모든 마이너가 최장 체인에서 마이닝 작업하기 때문에 블록체인 장부의 유일성에 도움이 된다.

제네시스 블록(Genesis Block)

제네시스 블록에는 시크체인(Seekchain)에 대한 일련의 경제와 기술 구성 매개 변수가 포함될 것이다.

```
impl From<ethjson::spec::Genesis> for Genesis {
    fn from(g: ethjson::spec::Genesis) -> Self {
        Genesis {
            seal: From::from( s: g.seal),
            difficulty: g.difficulty.into(),
            author: g.author.map_or_else( default: Address::zero,  f: Into::into),
            timestamp: g.timestamp.map_or( default: 0,  f: Into::into),
            parent_hash: g.parent_hash.map_or_else( default: H256::zero,  f: Into::into),
            gas_limit: g.gas_limit.into(),
            transactions_root: g.transactions_root.map_or_else( default: || KECCAK_NULL_RLP.clone(),  f: Into::into),
            receipts_root: g.receipts_root.map_or_else( default: || KECCAK_NULL_RLP.clone(),  f: Into::into),
            state_root: g.state_root.map( f: Into::into),
            gas_used: g.gas_used.map_or_else( default: U256::zero,  f: Into::into),
            extra_data: g.extra_data.map_or_else( default: Vec::new,  f: Into::into),
            base_target: g.base_target.map_or( default: 0,  f: Into::into),
            signature: g.signature.map_or_else( default: H256::zero,  f: Into::into),
            deadline: g.deadline.map_or( default: 0,  f: Into::into),
        }
    }
}
```

제네시스 마이닝풀과 작동 안전성

제네시스 마이닝풀은 빠르게 안정적이고 안전한 네트워크를 구축하기 위한 방침이다. 시크체인(Seekchain)은 본질적으로 보면 여전히 해시레이트로 지원해 주는 암호화폐이고 네트워크의 안전성은 네트워크에 탑재되는 해시레이트에 달려 있기 때문에 시크체인(Seekchain)은 장부 초기에 51%의 저장공간을 공격을 저항할 수단으로 확보해 지원해야 한다.

제네시스 마이닝풀은 스스로 구축한 마이닝풀보다 특별한 스펙이나 우수성을 가지고 있진 않고, 다만 POC 업종에 더 적합한 토큰 판매 방식이라고 볼 수 있다. 전체 시크체인(Seekchain) 네트워크가 여전히 강한 개방성과 탈중앙화를 갖추고 있다.

화폐 발행 체계

화폐 발행

토큰의 명칭은 SEEK 이고 총발행량은 9.7 억이며 개발팀은 제네시스 블록에서 3700 만을 미리 마이닝할 것이다.

SEEK 생성량은 4 년마다 절반으로 줄어든다.

블록 패킹 시간을 4min 로 가정하여 블록 보상 전액이 800 SEEK 로 설정할 경우, 사실 블록 패킹 수취율이 있어서 보상이 전액으로 지급되지 않는다.

분배 방안

SEEK 의 전체 산출이나 소각 상황은 아래와 같다:

• 개발 단체가 3,700 만을 미리 마이닝한다

• 채굴 보상 수취율에 의해 실제로 마이닝된 SEEK 를 계산한다

• (1-채굴 보상 수취율)에 의해 소각된 SEEK 를 계산한다

실제로 마이닝된 SEEK 는 아래와 같이 분배될 것이다:

1. 83%는 마이너가 획득.

2. 10%는 개발팀에게 분배.

3. 7%는 이급 초대자에게 지급되며 초대자가 없는 경우 해당 부분도 소각된다.

블록 보상 전액이 W 로 수취율이 e 로 가정한다면 마이너가 블록 하나를 패킹하면 블록 보상은 다음과 같은 비율로 나누어진다.

1. 마이너가 수취율에 대응하는 부분을 획득한다, 이 부분은 R= e*W*83%인 것을 가정한다.

2. e*W*10%부분은 개발팀에게 분배된다.

3. 만약 한 마이너가 이급 초대로 가입된 경우 직접 초대자는 e*W*5%의 직접 초대 보상을 받을 수 있으며 간접 초대자는 e*W*2%의 간접 초대 보상을 받을 수 있다. 초대자가 없는 경우 해당 부분이 산출되지 않는다.

4. 나머지 산출되지 못한 부분은 영구적으로 소각될 것이니 즉 한 블록이 패킹되어 소각할 SEEK 의 수량은 :

a. 최소 W * (1-e)

b. 최대 W * (1-e) + e*W*7%

블록 전액이 800 SEEK로 2급 초대로 가입되고 수취율이 20%인 마이너를 예로 들자면 한 블록이 패킹되면:

1. 마이너가 132.8 SEEK 획득한다.
2. 단체가 16 SEEK 획득한다.
3. 직접 초대자가 8 SEEK 획득한다.
4. 간접 초대자가 3.2 SEEK 획득한다.
5. 누적 소각 수량이 640 SEEK이다.

만약 마이너가 스스로 가입된다면 다음과 같이 배분될 것이다:

1. 마이너가 132.8 SEEK 획득한다.
2. 단체가 16 SEEK 획득한다.
3. 누적 소각 수량이 652.2 SEEK이다.

마이닝 모델

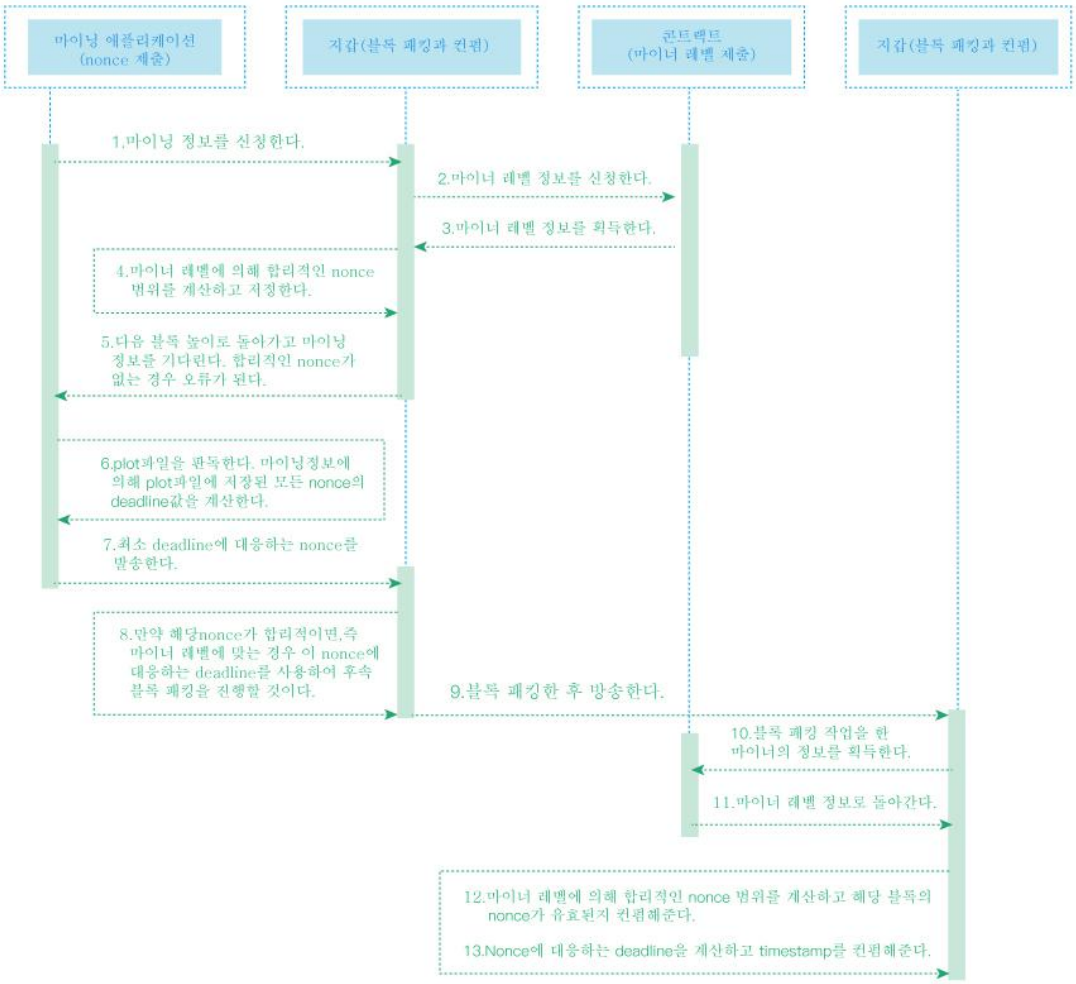
시크체인(Seekchain)에서 마이너가 다음과 같이 4가지 방법으로 SEEK 수익을 얻을 수 있다:

해시레이트로 마이닝한다

시크체인(Seekchain)은 차별 요금율을 적용하여 마이너가 연소한 SEEK 수량 G, 유효 해시레이트 P(Power)와 블록 패킹 수취율 O(Output)가격 간의 관계를 정할 것이다. 일반적으로 마이너가 연소한 SEEK 의 5%정도는 커뮤니티 예산으로 마이닝 풀에 자극하는 것 등 생태 건설에서 사용된다.

차별 요금율은 전체 네트위크의 해시레이트에 의해 주기적으로 자동 수정된다.

계정 유효 해시레이트 관제 방안은 한 계정의 레벨이나 연소 수량을 통해 해당 계정이 네트워크에 접속한 해시레이트를 컨토롤할 수 있는 것이다. 구체적인 프로세스는 아래 안내도와 같다:



시크체인(Seekchain)은 블록패킹할 때 합리적인 nonce 값의 범위에 대해 컨센서스 차원의 제한을 가한다.한 계정이 허용된 해시레이트, 즉 p 디시크 공간이 C 라고 가정하면 해당 계정의 nonce cap 에 대한 계산방법은 다음과 같다:

nonce cap = 4C*1E3*1E3

즉 초급 마이너가 네트워크에 접속할 수 있는 유효 해시레이트가 8T 라면 합리적인 블록 패킹 nonce 범위가 다음과 같다:

{1~32000000}

계정의 유효 해시레이트와 연소 요금율 변경

코인 연소를 통해 레벨을 올릴 수 있으며 마이너 레벨이 수취율, 최대 용량과 양의 상관이 된다.

마이너가 연소한 코인 수량 = 다음 레벨이 필요한 코인 기수*(현재 총해시레이트/초기 총해시레이트)

```
function levelUp() payable public {
    require(accounts[msg.sender].owner != address(0));
    uint currentHashRate = hashrate;
    uint needBurnt = burntCoinAmountToRate[accounts[msg.sender].rewardRateLevel + 1] * baseHashRate / currentHashRate;
    require(msg.value == needBurnt);
    accounts[msg.sender].burntCoin += msg.value;
    accounts[msg.sender].rewardRateLevel ++;
    intervalReward.transfer(msg.value * 500 / DecimalRate);
}
```

현재 총해시레이트의 획득 논리는 다음과 같다:

전 난이도 조정 주간(24 개 블록)의 평균 블록 난이도 값을 판독한다.

난이도 값에 의해 체인 총해시레이트를 추산한다.

해당 해시레이트값이 다음 가격 조정 주기의 블록 헤더에 기록된다(3000 개 블록마다 가격을 한번씩 조정한다).

마이너가 가입할 때마다 콘트랙트가 기록된 총해시레이트 데이터를 판독하여 해당 수치의 크기에 따라 마이너가 연소해야 할 수량을 정한다.

블록 패킹 시간 Deadling 이 4min 로 설정하며 3000 개 블록에 대응하는 조정기간은 1일 정도이다.

마이닝풀로 마이닝한다

여기서 현실에서 마이너가 마이닝하는 두가지 방법을 설명해 준다:

독립적인 마이닝은 마이너가 제출한 결과를 네트워크에 있는 기타 마이너와 마이닝풀이 제출한 결과와 비교하여 우위에 섯을 경우 모든 블록 패킹 보상을 받을 수 있는 것이다. 마이닝풀을 통해 마이닝은 마이너가 결과를 마이닝풀에 제출한 후 마이닝풀은 풀에 있는 기타 마이너가 제출한 결과를 얻고 나서 최소 deadline 값을 찾아 네트워크에 있는 기타 독립적인 마이너나 기타 마이닝풀이 제출한 결과와 비교하여 우위에 서게 되면 본인 마이닝풀의 배분 메커니즘에 의해 보상을 중앙화 방식으로 마이닝을 참여한 마이너에게 배분주는 것이다.

초대로 마이닝한다

다른 마이너를 초대하여 같이 마이닝하게 되면 상대방 블록패킹보상의 일부분을 얻을 수 있으며 해당 초대보상은 첫번째 반감기에서 한번만 조정할 것이다:

1. 초기에 직접 초대 보상은 5%이며 간접 초대 보상은 2%이다.

2. 조정 후에 직접 초대 보상은 3%이며 간접 초대 보상은 1%이다.

생태 마이닝한다

마이너들에게 다음과 같은 혁신적인 마이닝 방식도 있다:

1. 마이너들만 탈중앙화 금융 자치 위원회의 회원이 될 권리가 있으며 조직이 수익을 추가로 받아 누릴 수 있다.

2. 마이너들만 탈중앙화 거래소의 마켓 트레이더가 될 권리가 있으며 거래 수수료를 배분받을 수 있다.

3. 마이너들만 프라이빗 거래 연맹을 건립할 권리가 있으며 조직은 매매나 관리를 통해 취할 수 있다.

IPOB 에서 POD 로 진화

IPOB 컨센서스는 원가가 더 낮고 하드웨어 측면에서 더 공평한 암호화 경제 인프라를 만들었지만 더 엄밀히 말하면 이 과정에서 하드 디스크 자원의 의미가 제대로 개발되지 않았고, 디스크 자체의 데이터를 저장하는 능력은 새로운 컨센서스가 있어야 충분히 발휘할 수 있음을 알게 됐다. 데이터증명 POD (Proof of data)는 IPFS 프로토콜의 복제증명과 시공증명 두가지 저장증명 방식을 포함하는 새로운 의미가 있는 작업증명이다. 전환가능한 컨센서스에 기반하므로 POD 컨센서스가 경제적으로 실행 가능한 것으로 입증되면 시크체인(Seekchain)의 마이너들이 하드웨어 업그레이드 과정없이 바로 저장 마이너와 검색 마이너로 진화될 수 있다.

스마트 콘트랙트

가상 머신은 스마트 콘트랙트가 노드에서 실제 실행되는 환경이다. 블록 네트워크에 콘트랙트가 사용된 합법적인 거래 정보를 발송하면 각각 노드의 가상머신이 해당 콘트랙트의 코드를 실행하게 되어 실행 결과까지 기록하는데, 컨센서스 메커니즘은 모든 계산결과가 동일해야 되는 것을 요구하며 한 개의 정보만 틀려도 합

의 못하게 된다.

WebAssembly 의 약칭은 WASM 이고 이동 가능한 프로그램을 안전하고 효과적인 방식으로 실행하는 새로운 기술이다. WASM 기술을 통해 개발자는 새로운 Solidity 언어를 배울 필요없이 확실성있는 프로그래밍 규범을 따르는 것만으로도 통상적인 Go、Pyhton、Nodejs、Rust 등 프로그래밍 언어를 사용하여 시크체인(Seekchain)에서 빠르게 탈중앙화 애플리케이션을 구축할 수 있다. 그 다음 비효율적인 EVM 가상 머신보다는 WebAssembly 콘트랙트는 바이트코드로 컴파일되어 실행 효율이 더 높아진다. 동시에 현재 공학 분야에 이미 성숙한 IDE 와 컴파일러 등과 결합할 수 있다.

시크체인(Seekchain)은 WASM 콘트랙트 개발 디버킹 툴인 catalyst 를 제공한다. 해당 툴은 브라우저에서 실행되며 사용자들이 콘트랙트를 개발이나 테스트 과정에 스스로 블록체인 노드를 구축할 필요도 없고 복잡한 콘트랙트 코드 컴파일러 환경을 설치할 필요도 없다. Catalyst 툴은 WASM 콘트랙트의 개발, 컴파일, 배치와 콘트랙트 인터페이스 테스트 등의 기능을 집대성하여 개발자에게 개발와 테스트 방면에서 편리를 제공해 준다.

시크체인(Seekchain)은 또한 자주 사용되는 표준 토큰 콘트랙트 기반류를 제공하여 개발자에게 빠르게 자기자신의 토큰 콘트랙트 환경을 구축하게 해주는 편리를 제공해 준다. 스마트 콘트랙트는 생태계에서 주로 일부분 복잡한 프로토콜과 서비스에 대해 더 나은 배경을 제공한다:

1. 더 다양한 체인 관리 방식을 지원한다.

2. 다중 서명 업그레이드 콘트랙트를 지원하다.

3. 장부 자정 프로토콜을 지원하다.

4. 체인에서 프라이빗 그룹과 프라이빗 거래를 지원한다.

5. 일련의 공유 안전성과 유통성 있는 탈중앙화 금융 솔루션을 구축를 지원하다.

컨소시엄 프라이빗 거래

퍼블릭체인에 있는 거래와 콘트랙트 상태는 일반 대중들이 확인할 수 있는데 비즈니즈 비밀을 보호해 주는 기능을 제공할 수 없는 반면에 기관이나 일부 그룹들은 퍼블릭체인에서 프라이빗 거래를 만들 필요가 있을 수도 있다. 시크체인(Seekchain)의 노드는 ETH 의 Parity 지갑 위에서 구축되어 있으며, 일부분 계정이 개방된 네트워크에서 지정자에게만 확인할 수 있고 상태를 관리할 수 있도록 허용하는 프라이빗 콘트랙트를 구축할 수 있도록 지원하다. 이는 간소화된 컨소시엄 체인의 방안과 비슷할뿐 아니라 구축, 관리와 사용에는 컨소시엄 프라이빗 거래 솔루션은 더욱 경량화 되었다.

일정한 연소 요건을 충족하는 마이너만 이런 컨소시엄 콘트랙트를 진행할 수 있으며 컨소시엄 내에 있는 노드와 거래 규칙을 생성할 수 있다. 마이너는 콘트랙트를 양도하여 요금을 받을 수 있고, 요금제를 스스로 설정하여 컨소시엄 내에 거래 서비스를 사용하는 계정에 요금을 청구할 수 있다.

핵심 개념

퍼블릭 콘트랙트: 시크체인(Seekchain)에 특별히 지정된 스마트 콘트랙트이다. 퍼블릭 콘트랙트가 프라이빗 콘트랙트의 암호화폐 코드와 상태 변수를 저장한다.

컨소시엄 프라이빗 콘트랙트: 퍼블릭 콘트랙트에 저장된 스마트 콘트랙트이다. 프라이빗 콘트랙트의 상태와 코드는 공개되지 않고 특정 계정만 판독하고 수정할 수 있으며 해당 계정들은 모두 퍼블릭 콘트랙트가 생성되는 동안에 지정해 놓은 계정이다.

메인 검증자와 검증자 리스트: 메인 검증자는 프라이빗 콘트랙트 상태를 변경할 수 있게 허용된 계정이다. 검증자 리스트는 퍼블릭 콘트랙트가 생성되는 동안 메인 검증자인 마이너가 지정한 계정이며 이는 검증자 리스트에 들어가도록 설정할 수 있다.

컨소시엄 프라이빗 거래: 암화화폐 데이터와 수정된 프라이빗 콘트랙트 상태를 포함하는 스페셜 메일이며, 이는 사용자가 지정해놓은 비율 혹은 모든 검증기가 서명을 해야 변경할 수 있다.

퍼블릭 거래: 일반 계약이 퍼블릭 계약으로 전용 되는 것이며, 그에 따른 변경은 프라이빗 콘트랙트에 저장된다.

비밀 상점

비밀 상점은 노드에게 프라이빗키를 만들고 관리하는 서비스를 제공하는데, 이는 퍼블릭 콘트랙트와 연관된다. 해당 프라이빗키는 검증자의 서명을 수집하는 거과

같은 프라이빗 프로토콜의 상태와 노드간의 거래한 정보를 암호화해 준다. 프라이빗 사무 시스템에 참여하는 각각 Parity 노드를 위해 확실한 Secret Store URL 을 지정해 준다. 라이선스 콘트랙트는 어느 계정이 어느 콘트랙트의 비밀키를 방문할 수 있는지에 대하여 설명한다. 비밀 상점은 구체적으로 다음과 같은 서비스를 제공한다:

1. 분산된 타원곡선 비밀키 페어 생성-비밀키는 다방면 특수한 암호 프로토콜을 사용하여 생성되므로:

➢프라이빗키는 여전히 모든 사용자에게 알려져 있지 않다.

➢퍼블릭키 부분은 모든 면에서 계산될 수 있으며 외부에 안전하게 노출될 수 있다.

➢각각은 프라이빗키의 “지분”을 가진다.

➢t+1 의 그룹의 모두 연합이 가능하며 , 비밀키의 프라이빗 부분을 회복시킬 수 있다.

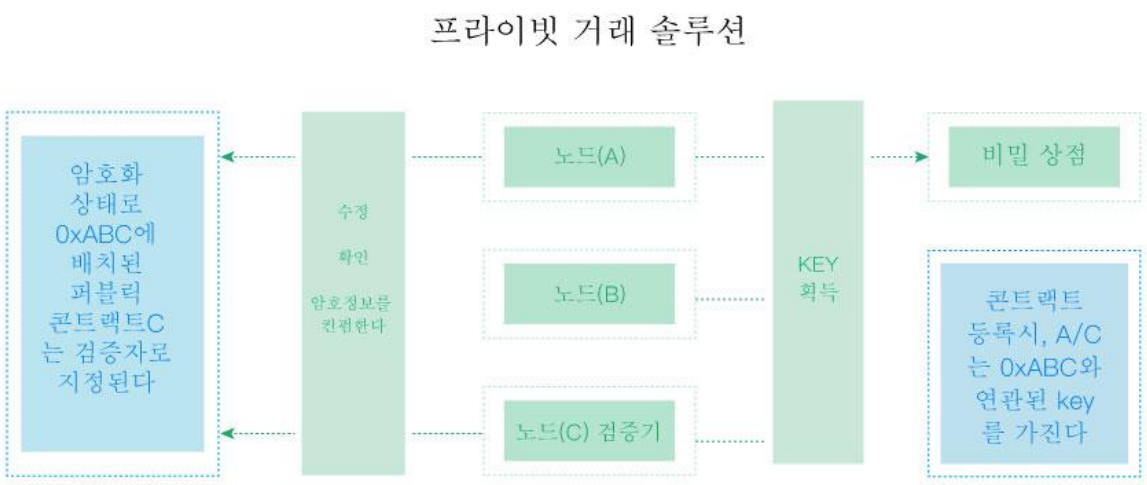
➢t+1 보다 적은 당사자의 어떤 부분 자집도 비밀키의 프라이빗 부분을 회복할 수 없다.

2. 분산형 비밀키 저장-프라이빗키 공유는 각각 따로 저장하며 다른 쪽이나 외부 실체에게 절대 노출되지 않다.

3. 블록체인 권한에 의한 역치 검색 -모든 프라이빗 키가 필요로 하는 조작은 적어도 t+1 각 측의 “권한 계약”상태를 동의해야 한다.

거래 프로세스

다음 예시에서: 노드 A와 C는 프라이빗 콘트랙트의 비밀키를 방문할 수 있지만 노드 B는 안된다. 단 노드 C는 시스템 검증자 리스트에 지정되어 있다.



우리는 간단한 프라이빗 콘트랙트를 예시로 사용한다:

contract Test1 { bytes32 public x; function setX(bytes32 _x) { x = _x; } }

setX에 이미 배치된 프라이빗 콘트랙트를 호출하기 위해 사용자가 다음과 같이 진행해야 한다:

1. 콘트랙트를 호출하도록 하는 일반적인 업무를 작성하려면, 예시에서 SetX(42)로 정한다:

curl--data'{"method":"parity_composeTransaction","params":[{"from":"0xcf9e2287227c5c
c5978e7bdbbdaf293fe4992a24","to":"0x52f5f1b8c785ab1c0e892b4c46b080fde9ad992b
","data":"0xbc64b76d2a0000000000000000000000000000000000000000000000

000000000000000000"}],"id":1,"jsonrpc":"2.0"}' -H "Content-Type: application/json" -X POST localhost:8549

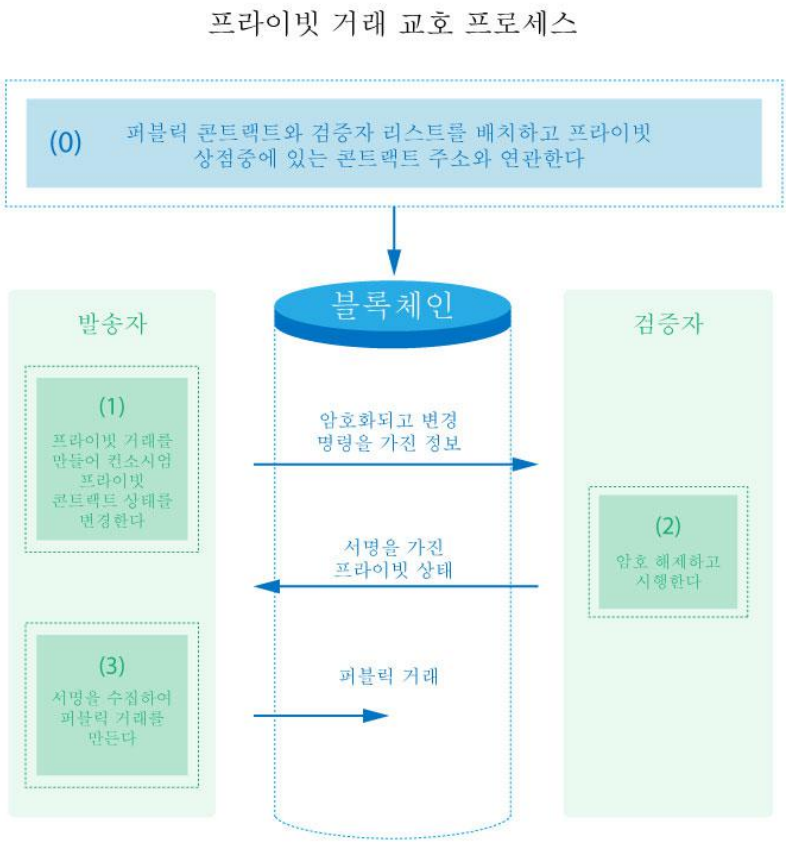
2. 거래를 서명한다.

3. private_sendTransactionAPI 방법으로 서명 업무를 발송한다:curl --data '{"method":"private_sendTransaction","params":["0xf88407...1137"],"id":1,"jsonrpc":"2.0"}' -H "Content-Type: application/json" -X POST localhost:8549

이 중 0xbc64b76d2a...00000000 는 임의 파라미터 42 를 사용하여 SetX 을() 튜닝하는 데 대응합니다.0xf88407...1137 은 이전에 만들어진 서명 사무소가 있는 해시 주소입니다.

이 중 0xbc64b76d2a...00000000 은 아무 파라미터를 사용하여 SetX()를 호출하는 것에 대응한다. 0xf88407...1137 은 이전에 만들어진 서명 업무가 있는 해시 주소이다.

후속 프로세스



자치 금융 조직

Defi DAO —Dcententralize Autonomous Oganization For Dentralized Finance.

시크체인(Seekchain)은 일련의 공유 안전성과 유통성이 있는 탈중앙화 솔루션을 제공하는 것에 초점을 맞추고, 비즈니스 생태를 빠르게 확장할 것이다. 이런 솔루션의 연구, 제품설계와 애플리케이션 개발은 탈중앙화 조직에 의해 추진되며 각 단체는 세분화된 탈중앙화 솔루션을 지원한다.

다만 마이너만 이런 DAO 자치조직의 위원이 되도록 신청할 수 있다.

체인 관리

이런 메커니즘을 실현하기 위해 시크체인(Seekchain)은 DAO 조직에게 Coops 탈중앙화 자치 조직 프로토콜을 Seekchain 에 배치하 것 등과 관련된 관리 도구를 제공한다. 이는 교체가 가능하고 쉽게 사용할 수 있는 체인관리 구조이다. 마이너들은 위원회 구성원으로써 이 구조를 통해 구성원 관리, 조직 재무 관리, 임무와 보상 관리 등 일상 업무를 실현할 수 있다. 체인관리의 임무는 일반적으로 기술 업그레이트, 제품 출시, 문제 복구 등을 포함한다. 그리고 관리 방식은 주로 프로토콜 구조와 콘트랙트 구조가 포함된다.

Defi DAO 에서는 관리의 과정은 다음과 같다.

1.지속적인 의사소통, 문제점 발견 및 고객니즈 반영 과정

2.지속적인 의사소통, 의사결정 및 기획방안 형성 과정

3.콘트랙트 개발, 검수 후 배치 완료

관리에 참여하는 대상은 다음과 같다:

1.코인 보유자, 의견과 제안을 제출하여 보상을 받거나 구성원의 합법성을 투표로 결정할 수 있다.

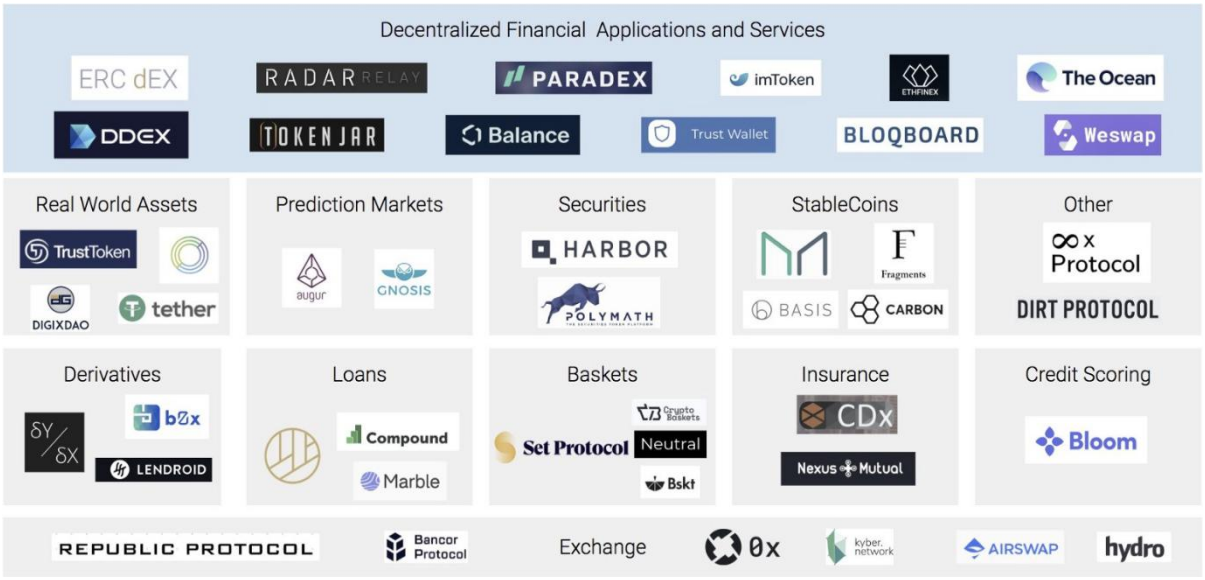
2.마이너, 위원회 구성원이 되어 일상 사무를 위해 투표하여 솔루션의 서비스 수수료를 배분받을 수 있다.

3.커뮤니티 오피니언 리더, 의견을 수집하고 고객 니즈 제안을 제출하여 실적에 따라 보상을 받을 수 있다.

4.개발 인원, 콘트랙트를 개발하고 체인에 등록 하여 보상을 받을 수 있다.

탈중앙화 금융

탈중앙화 금융은 시크체인(Seekchain)이 중심적으로 확장하고 있는 분야이며 현재 커뮤니티에서 자발적으로 형성된 탈중앙화 금융 형태에 기반하여 솔루션의 배치를 진행할 것이다.



시크체인(Seekchain)의 탈중앙화 금융 솔루션과 자치 조직은 다음과 같거나 더울 늘어날 예정이다.

포인트 to 포인트 지불

지불은 가장 중요한 금융 인프라들 중에 하나이며 IPOB 컨센서스에 의해 구축된 시크체인(Seekchain) 장부는 실제 상업 장면에서 초당 백만에 달하는 거래 요청을 뒷받침할 라이트닝 네트워크 구축을 지원한다.

자산을 블록체인과 결합한 것 및 주식 시스템화

현실에 있는 자산은 유통성이 부족하고 글로벌 거래를 실현함에 많은 어려움이 있다. 이에 시크체인은 블록체인과 연결된 후 사용자가 언제 어디서나 전세계의 투자자와 포인트 투 포인트 투자를 할 수 있다. 자산을 블록체인화 하는 것과 주식화 하는것의 자세한 내용은 아래 자세히 서술 할 예정이다.

풀 스탠더드 토큰 탈중앙화 거래소

비동질적인 ERC721 표준 토큰 및 동질적인 ERC20 표준 토큰과 같은 거래 가능한 암호화폐는 모두 시크체인(Seekchain) 탈중앙화 거래소에서 유동성을 얻을 수 있을 것이며, 이러한 유동성은 정액제를 갖춘 계약에 의해 제공되거나, 상태방이 제공할 수도 있다. 다만 마이너만 탈중앙화 거래소의 마켓 트레이더가 되어 수수료 배분을 받을 수 있다.

담보대출

암호화폐가 발행된 후 담보로 대출받을 수 있으며 저당자가 갚지 않으면 담보한 자산의 소유권은 대출 서비스를 제공하는 자에게 이전된다.

신탁 기계와 시장 예측

신탁 기계와 시장 예측은 확실한 스마트 콘트랙트가 불확실한 외부 세계에 반응하는 것을 허가한다. 이것은 콘트랙트가 외부와 데이터를 주고 받을 수 있는 유일한 경로이고 블록체인이 현실 세계와 데이터를 주고 받는 인터페이스이기도 한다.

장부 자정 프로토콜

시크체인(Seekchain)에서 배치된 모든 콘트랙트는 일정한 마크가 있는데 해당 콘트랙트가 정식건인지 테스트건인지 표시해 줄 것이다. 테스트 콘트랙트의 경우, 배치자는 블록 높이가 어느 높이에 도달하면 이 콘트랙트와 관련 데이터가 무효되도록 하는 삭제 규칙을 설정할 수 있다.

이 정화 메커니즘은 매우 중요한 역할을 2가지가 있다. 우선, 개발자에게 매우 좋은 개발 경험을 제공하고 현재 블록체인이 안전한 네트워크를 구축하기 어려운 문제를 해결하여 테스트 네트워크가 정식 네트워크인 것을 구현한다. 그 다음, 자정 프로토콜은 장부 데이터가 빠르게 팽창하는 것을 막고 쓰레기 데이터를 줄이는 것에 도움된다.

로드맵

시크체인(Seekchain)은 빠르게 진화하는 인프라이며 제품, 해결방안, 사용자 수량과 사용자 활성을 나타낼뿐만 아니라 시대와 기술에 따라 능동적인 기술 연구 개발을 해 나갈 것이다. 전체적으로 시크체인(Seekchain)의 로드맵은 메인넷의 컨센서스 메커니즘에 따라 2가지 부분을 나누어져 있는데 각각은 IPOB와 POD 단계이다.

IPOB 단계

- ❑ 2019 - 09 월　　프로젝트가 네트워크와 인센티브 계획을 테스트

- ❏ 2019 - 09 월 제네시스 마이닝풀 예매
- ❏ 2019 - 10 월 정식적인 네트워크
- ❏ 2019 - 10 월 체인 마이닝풀의 성장 보조 장기 이벤트 제 1 회 시작
- ❏ 2019 - 12 월 체인 자칙 조직과 Defi 솔루션을 발표하여 마이너 위원회 구성원 선거
- ❏ 2019 - 12 월 프라이빗과 체인그룹 기능을 발표하여 마이너가 프라이빗 거래 컨소시엄 생성 가능
- ❏ 2020 - 01 월 탈중앙화 거래소를 상장하여 마이너가 DEX 자칙 조식의 마켓 트레이더로 진화하기 시작
- ❏ 2020 - 02 월 장부 자정 프로토콜을 배치
- ❏ 2020 - 03 월 생태 개발자 대회를 열어 애플리케이션 시장을 개발
- ❏ 2020 - 05 월 글로벌 밋업과 Hackathon 등 기술과 시장 홍보 활동을 진행

POD 진화단계

- ❏ 2020 - 07 월 라이트닝 지불 네트워크가 배치완료
- ❏ 2020 - 09 월 저장시장과 검색시장을 발표하여 테시트 시작
- ❏ 2020 - 11 월 새로운 노드 클라이언트를 발표하여 IPOB 마이너에서 POD 저장과 검색 마이너로 전화하기

단체

진동규

중국정법대학교 국제법학과 졸업후 , 한국 재경부 산하의 산업 재생관련 기관 운영관리로 일하며 이를 토대로 귀금속 무역 및 보세 무역을 통한 영역으로 범위를 넓혔다.

2017 년초 가상화폐 재정거래를 시작으로 가상화폐에 진입하였으며 , 각 기업의 캐피털과 솔루션 프로세스를 연결짓는 프로젝트로 큰돈을 벌었다.

2018 년 2 월 Eos 계열의 Mono Dapp 를 개발하며 50 만트래픽을 달성하며 , 많은돈을 펀딩받았다.

현재 Seek chain 의 Ceo 로 운영과 마케팅관련한 모든일을 총괄하여 지휘중이며 , 한국 VC 의 100 만달러에 달하는 기금을 모금하였다.

오준하

반기문 Un 사무총장이 졸업한 한국의 국립대학인 서울대 컴퓨터 공학과를 졸업하였고 , 현재 Seek Chain 의 기술을 책임지는 Cto 로 일하고있다, 수년의 소프트웨어 기술 개발이력과 , 보안프로젝트 담당 경력을 갖고있으며 , 특히 분포식 데이터 처리시스템 , 암호화 처리기술에 대하여 해박한 지식을 갖고있다. 거래화를 프로세스화 시키는데 뛰어난 기술과 지식으로 Seek Chain 의 발전에 전략적 책임을 지고 있다.

투자

蛮子基金 MANZIFUND

참고

BTC Data : https://digiconomist.net/bitcoin-energy-consumption#assumptions

Proof of space : https://eprint.iacr.org/2013/796.pdf

Burst wiki : https://burstwiki.org/en/burst-wiki/

Parity wiki : https://wiki.parity.io/Parity-Ethereum

Proof of burn : https://en.bitcoin.it/wiki/Proof_of_burn