마이크로비트코인(MBC): 마이크로 경제를 위한 탈중앙화된 P2P 결제 플랫폼

초록. 마이크로비트코인은 소액 결제를 위해 사용되는 탈중앙화된 블록체인 네트워크입니다. 비트코인(BTC) UTXO를 상속받아 초기에는 하드포크의 형태로 구현되었습니다. 초기 네트워크 런칭 이후 약 1년이 지난 후, 비트코인 네트워크에서 상속된 광범위한 크기의 블록체인과 블록 유효성 검사 중에 PoW 알고리즘의 성능이 저하되는 몇 가지 제한사항이 발생하기 시작했습니다. 2019년 10월 9일에 이러한 문제를 해결하기 위해 커뮤니티는 기존 네트워크를 근본적으로 버리고, 새로운 네트워크로 전환했습니다. 새로운 마이크로비트코인 네트워크는 UTXO 스냅샷, 작은 블록 사이즈, 새로운 블록 보상 공식 및 CPU 중심의 PoW 알고리즘을 갖추고 있습니다.

1. 새로운 네트워크 시작의 전제 조건

최초의 마이크로비트코인 네트워크는 2018년 7월 11일 비트코인 네트워크의 하드포크로 시작되었습니다. 소액 결제에 더 적합하도록 ASIC[1] 저항과 빠른 블록생성시간에 주안점을 두었습니다. 통화 단위와의 상호작용을 쉽게하기 위해 1 BTC를 10,000 MBC로 4자리 이동시켰습니다.

최초의 마이크로비트코인 블록은 2018년 7월 11일에 채굴되어 기본 sha256d 해시 함수를 NIST SHA-3 Groestl [2] 알고리즘으로 대체하여 하드포크를 발생시켰습니다. 그 당시에는 ASIC 구현이 없었기 때문에 ASIC에 방어하는 내성을 지닌 것으로 알려져 있었습니다. 시간이 흐르면서 Baikal이 2018년 10월 26일에 Groestl을 지원하는 BK-G28을 출시한 후로 이것이 무너졌습니다. 이 때 이후로 BK-G28 채굴자들이 네트워크의 해시 파워의 주요 원천이 되면서 근본적인 마이크로비트코인의 탈중앙화를 손상시켰습니다. 광범위한 연구 끝에 우리는 Bill Schneider의 Rainforest [4] PoW 알고리즘을 통해 이것을 중단시켰습니다. 2019년 3월 6일에 마이크로비트코인 네트워크는 Rainforest로 하드포크되었고, 2019년 5월 7일에 알고리즘의 일부 결함을 수정시킨 Rainforest (RFv2라고도 함)의 두번째 버전으로 강화되었습니다.

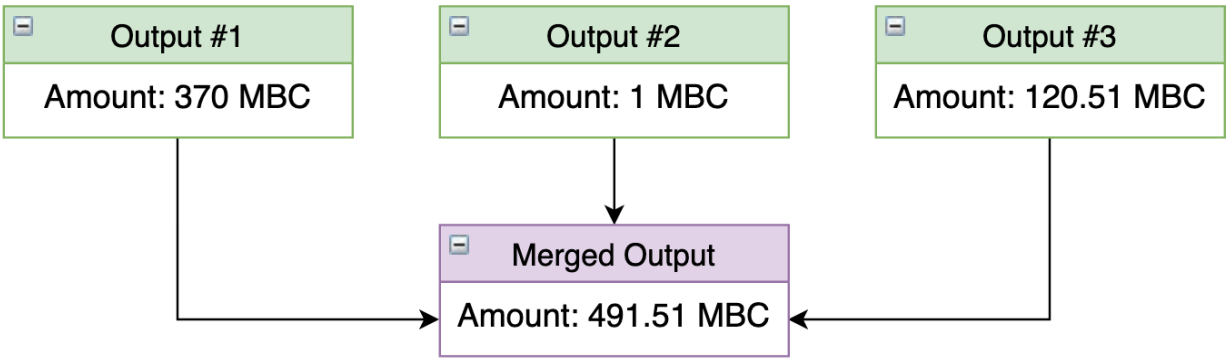
얼마 지나지 않아 PoW 유효성 검사 단계에서 Rainforest v2(RFv2) 알고리즘이 느려지고, 200GB 이상의 큰 블록체인 사이즈가 마이크로비트코인의 전체 노드를 싱크하고, 유지시키는데 매우 어렵게 만들었으며 본질적으로 네트워크의 탈중앙화의 손상을 야기할 수 있게 되었습니다. 이러한 상황이 새로운 네트워크가 시작된 주요 원인이 되었습니다.

2. 스냅샷

마이크로비트코인 네트워크는 최종 주소 잔액이 기본적으로 사용되지 않은 모든 출력값의 합인 UTXO[5] 모델에서 작동하기 때문에 한 네트워크에서 다른 네트워크로 균형을 옮기는 것은 단순한 작업입니다.

우리는 **525,000** 블록 (첫번째 MBC 블록)부터 **1,137,200** 블록까지 모든 UTXO를 가져와서 복사했습니다. 예를 들어, 기존 네트워크에서 주소에 3개의 미사용 출력값이 있는 경우 금액의 합계를 사용하여 하나의 출력값으로 병합하였습니다.

예시:



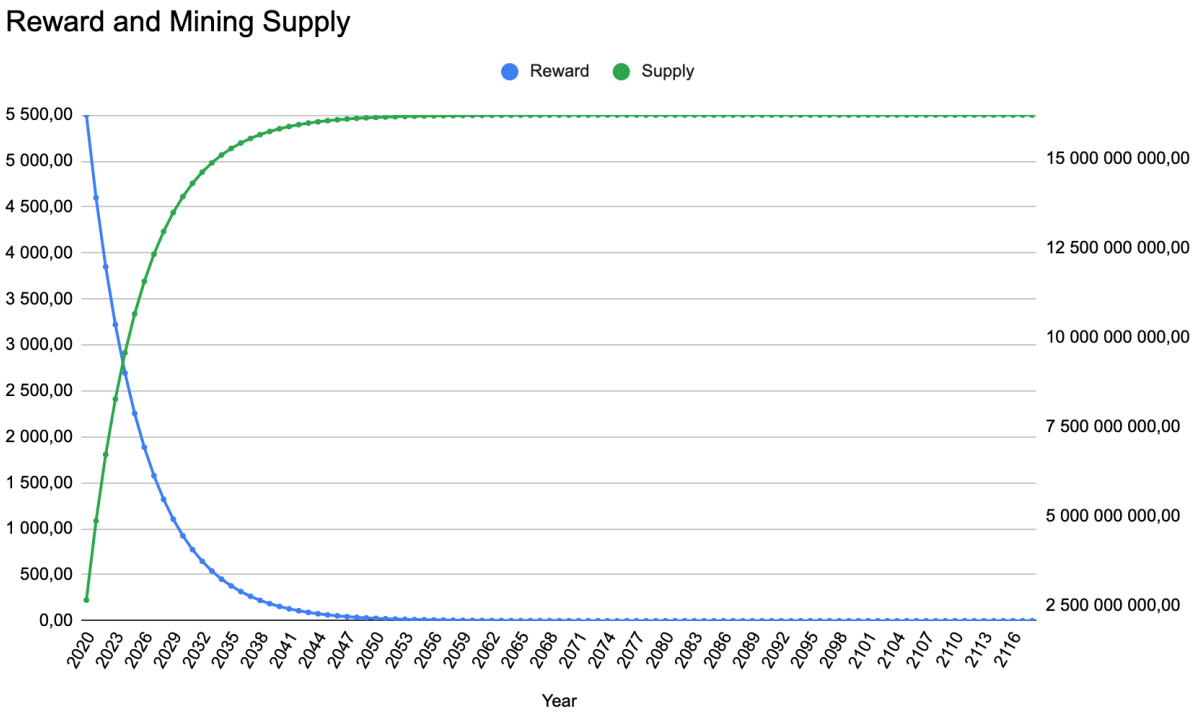
모든 스냅샷 출력값들은 새로운 마이크로비트코인 제네시스 블록[6]에 있으며 마이크로비트코인 익스플로러 에서 확인할 수 있습니다.

3. 공급과 보상

새로운 네트워크 런칭 시점에 현재 사용자 층에 대한 총 공급이 과도하게 줄어든 이후, 많은 자금이 하드포크 이후로 이동되지 않았습니다. 이러한 상황을 개선하기 위해 **525,000** 블록(초기 네트워크 시작 블록) 이후 이동되지 않은 코인은 스냅샷에 포함되지 않았으며, 더 이상 활성화 할 수 없도록 소각되었습니다. 총 **44,386,397,362.4252** MBC가 활성화 되었고, 약 **2,700,000** BTC가 하드포크 이후 MBC로 활성화되었습니다.

새로운 코인의 더 나은 분배를 위해 블록 보상 일정이 조정되었습니다. 4년마다 50%씩 블록 보상을 감소시키는 반감[7] 대신, 새로운 보상은 매번 새로운 블록 보상을 부드럽게 감소시킵니다. 기본 보상은 약 2년마다 30%씩 줄어듭니다.

보상 및 채굴 공급량에 대한 그래프:



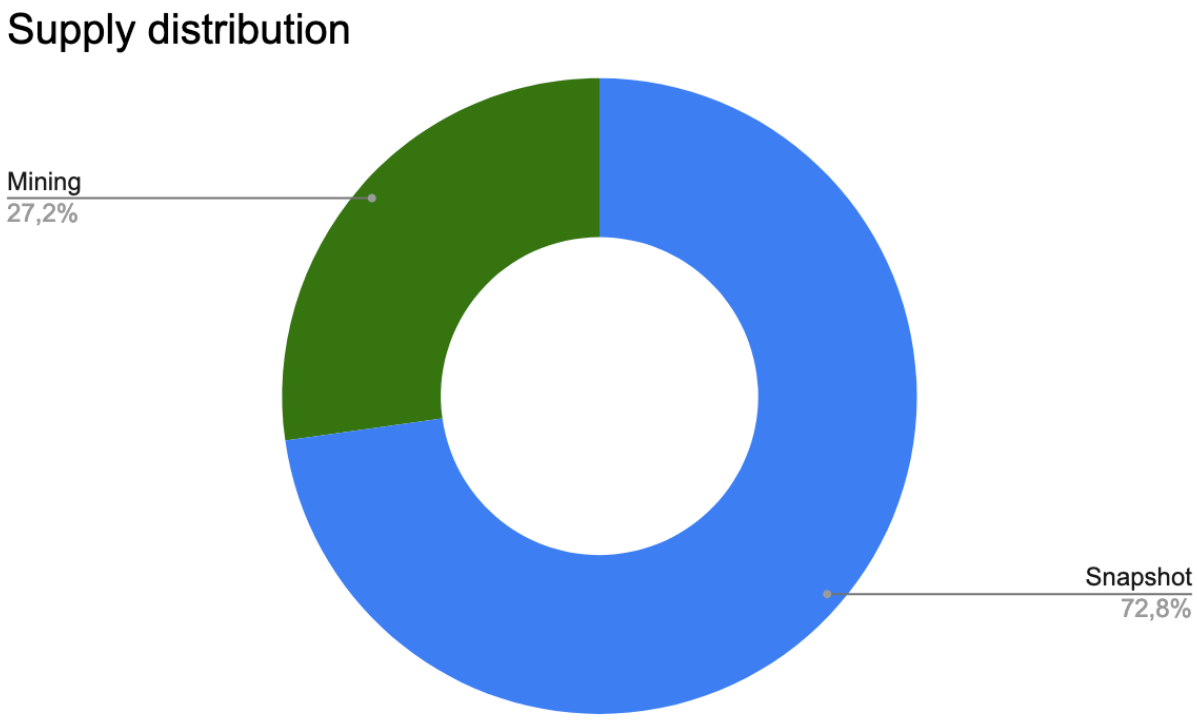
Reward formula implementation in C++.

```
#include <iostream>
#include <cmath>
```

```
// Amounts of satoshit per coin
const int64_t COIN = 10000;

int64_t reward(int height) {
  // Initial reward per block
  const int64_t reward = 5500 * COIN;
  // Reward decreasing epoch (2 years)
  const int epoch = 525960 * 2;
  // Decrease amount by 30% each epoch
  const long double r = 1 + (std::log(1 - 0.3) / epoch);
  return reward * std::pow(r, height);
}
```

총 공급량은 **61,000,000,000** MBC로 제한되며, 이 중 **44,386,397,362.4252** MBC는 이전 네트워크 스냅샷을 통해 활성화된 양입니다. 나머지 **16,613,602,638** MBC는 향후 100년 동안 채굴될 것입니다.



4. 블록 크기

네트워크의 안정성을 높이기 위해, 블록 스패밍을 방지하고, 분당 1 블록의 관점에서 더 좋고 공정한 수수료 시장을 만들기 위해서 블록 크기를 **300kb**로 줄였습니다. 이것의 구현은 Bitcoin Core 개발자 Luke Dashjr의 제안에서 영감을 얻었습니다[8].

5. Power2B 작업 증명(PoW) 알고리즘

사토시 나가모토가 제안한 비트코인의 초기 백서에서의 "1 CPU - 1 Vote"에 대한 분산과 아이디어를 장려하기 위해 CPU에 친화적이고, 반-GPU적으로 설계된 YesPower[10] 해시 함수를 수정시킨 Power2B[11]를 사용했습니다. 계산 속도가 높고 순차적인 메모리 하드 해싱을 결합하여 GPU 속도를 CPU와 같은 속도로 낮추고, FPGA 및 ASIC의 잠재적인 이점을 제한합니다. 지금까지 YesPower는 수십 개의 서로 다른 암호화폐에 보안을 제공함으로써 적절한 CPU 중심 알고리즘이라는 것이 입증되었습니다.

우리의 Power2B 수정은 SHA256 기반 PBKDF2 및 HMAC를 본질적으로 blake2b[12] 기반 구현으로 대체하여 YesPower의 독창적인 디자인을 그대로 유지합니다. 이는 원래 YesPower 용 FPGA 및 ASIC을 Power2B와 호환되지 않도록 구현하기 위해 수행되었던 것입니다. 이를 위해서는 개발자가 마이크로비트코인의 소프트웨어/하드웨어의 특정 구현과 네트워크 보안을 강화해야 합니다.

6. 난이도 조정 알고리즘

마이크로비트코인 네트워크는 zawy12가 작성한 LWMA3[13] 난이도 조정 알고리즘을 사용합니다. 가장 최근의 난이도와 계산 시간으로 현재의 해시레이트를 추정하여 난이도를 설정합니다. 평균 난이도를 계산 시간의 선형 가중 이동 평균(LWMA)으로 나눕니다. 이를 통해 최신 계산 시간에 더 많은 가중치를 부여할 수 있습니다. 타임스탬프 조작 및 해시 공격에 대한 작은 규모의 코인 보호를 위해 설계된 것입니다. 기본 공식은 다음과 같습니다.:

```
next_difficulty = average(Difficulties) * target_solvetime / LWMA(solvetimes)
```

7. 다른 비트코인 하드포크 코인과의 비교

다음은 다른 비트코인 하드포크 코인들과 마이크로비트코인을 비교한 차트입니다.

	Bitcoin	BitcoinCash	BitcoinGold	MicroBitcoin
Total Supply	21M	21M	21M	**61B ***
PoW Algorithm	SHA256	SHA256	Equihash	**Power2B**
Mining Hardware	ASIC	ASIC	CPU/GPU	**CPU**
Block Creation Interval	10min	10min	10min	**1min**
Difficulty Adjustment	Bitcoin DAA	SMA	LWMA2	**LWMA3**
SegWit	Yes	No	Yes	**Yes**
Block Size	1mb	32mb	1mb	**300kb**

> 마이크로비트코인은 비트코인의 소수점 **8** 자리 대신 소수점 **4** 자리를 갖습니다. 따라서 Satoshi 단위의 관점에서 마이크로비트코인의 공급은 비트코인의 공급보다 **3** 배 더 큽니다.

8. 앞으로의 로드맵

이 섹션에서는 마이크로비트코인 프로토콜 및 생태계의 추가 개발에 대한 몇 가지 계획과 아이디어를 간략하게 설명합니다.

대체 노드 구현

네트워크의 분산화를 지원하기 위해 대체 네트워크 노드 구현을 위해 노력할 것입니다. 이를 통해 네트워크를 강화하고 특정 구현 한 번으로 중앙 집중화를 방지할 수 있습니다. 좋은 예는 Satoshi의 노드 구현을 계속하는 Bitcoin Core[15]와 Golang에서 처음부터 작성된 btcd[16]입니다.

소프트웨어 개발 키트 공개 및 공개 API

개발자는 커뮤니티에서 매우 중요한 부분이며, 삶을 더 쉽게 만들기 위해 Node.js 및 Python과 같은 다른 언어에 대한 마이크로비트코인 SDK를 만들고 게시할 것입니다. 이를 통해 네트워크와 간단하고 편리하게 상호작용할 수 있습니다.

또한 개발자가 풀 노드를 실행하는 것이 불편하므로 RESTful 및 Socket 인터페이스를 사용하여 빠르고 안정적인 공개 API를 작성해야 합니다. 지갑 주소들의 잔고, UTXO 세트, 네트워크의 정보 등과 같은 중요한 정보들을 제공합니다.

락업

일부 실제 계약에는 특정 기간 동안의 락업이 필요합니다. **OP_CHECKLOCKTIMEVERIFY**[17] opcode를 사용하여 이러한 계약을 생성하기 위한 즉시 이용 가능한 솔루션을 구현할 것입니다. 이것이 지정된 타임스탬프 또는 네트워크 블록 번호까지 MBC 락업을 가능하게 할 것입니다.

가벼운(Light) 지갑

마이크로비트코인 네트워크에 대한 접근성을 높이기 위해 장치에 전체 블록체인을 저장하지 않고, UTXO 세트에 접근하기 위해 위에서 언급한 공개 API를 사용할 필요가 없는 다양한 플랫폼을 위한 경량 지갑을 만들 것입니다.

References

[1] https://en.bitcoin.it/wiki/ASIC
[2] https://www.groestl.info
[3] https://bitcointalk.org/index.php?topic=5057818.0
[4] https://www.slideshare.net/bschn2/the-rainforest-algorithm
[5] https://www.investopedia.com/terms/u/utxo.asp
[6] https://en.bitcoin.it/wiki/Genesis_block
[7] https://en.bitcoin.it/wiki/Controlled_supply
[8] https://github.com/bitcoin/bitcoin/compare/v0.17.1...luke-jr:example_300k-0.17
[9] https://bitcoin.org/bitcoin.pdf
[10] https://www.openwall.com/yespower/
[11] https://github.com/MicroBitcoinOrg/Power2B
[12] https://blake2.net/
[13] https://github.com/zawy12/difficulty-algorithms/issues/3
[14] https://en.bitcoin.it/wiki/Satoshi_(unit)
[15] https://bitcoincore.org/
[16] https://github.com/btcsuite/btcd

[17] https://github.com/bitcoin/bips/blob/master/bip-0065.mediawiki

Links

Official Website: https://microbitcoin.org
GitHub: https://github.com/MicroBitcoinOrg/
Explorer: https://microbitcoinorg.github.io/explorer/#/
Web Wallet: https://microbitcoinorg.github.io/wallet/#/
API: https://api.mbc.wiki/
Discord: https://discord.gg/8zg2nTV
Telegram: https://t.me/microbitcoinorg Twitter: https://twitter.com/MicroBitcoinOrg
Forum: https://bitcointalk.org/index.php?topic=3982489.msg37769108
Reddit: https://www.reddit.com/r/MicroBitcoinOrg/