BULWARK

CRYPTOCURRENCY

Cryptocurrency Whitepaper

Bulwark Core Team:

Eatbatterys (프로젝트 관리자)

Jack (마케팅)

SerfyWerfy (블록체인 개발자)

Frogman (커뮤니케이션 리더)

Patrick (브랜드 및 디자인 담당)

Stu (생태계 개발자)

Bulwark Core Team:

December 2017

이 백서에 제공된 모든 자료는 The bulwark Core Team 의 소유임을 밝힙니다.
정보가 다른 출처에서 파생된 경우 Attribution 에 표시되어 있음을 밝힙니다.

요약

Bulwark (표기:BWK)는 마스터노드 (masternode) 개인정보보호 코인 공간안의 일반적으로 관찰되는 불공정한 관습을 타개하고자 탄생한 공동체 중심의 코인입니다. 신중하고 공정한 출시 전략은 참가자들이 전도유망한 프로젝트의 시작에 참여할 수 있는 기회를 제공해줄 것입니다. 저희는 거창한 약속대신 간단하지만 가치 있는 제안을 제시합니다. 저희는 DASH 와 PIVX 의 모범 사례를 본 받아 현재뿐만 아니라 미래에도 활용될 개인 정보 보호 코인을 제공해줄 것입니다. 기대한 만큼의 결과를 내놓지 못할 수도 있고 화려한 비전이 있는 것은 아니지만, 미래사회를 지탱해줄 플랫폼내 활용될 가치있는 코인입니다. 이것은 저희의 계획이 혁신적이지 않다는 것이 아니며, 과장된 광고대신 실제 결과를 내놓겠다는 의미입니다. 현재 실질적 가치는 없이 과장광고로 포장된 많은 코인들이 있으며, 저희는 이러한 과장되고, 실질적 가치와 결과가 없는 코인들의 흐름에 동참하지 않을 것입니다. ICO 없이, 소프트 런치 보상, 소규모의 선(先)채굴, 그리고 채굴자 중심 블록 보상 할당을 기반으로 Bulwark 참여자들은 마스터노드의 혼합을 제공하는 개인정보보호코인의 기반 참여를 할 수 잇는 것은 물론 의미있는 개발 로드맵과 함께 최고의 개인정보보호 코인 기술을 경험하게 될 것입니다. 마스터노드들은 출시될 때 사용가능하며 제 기능을 할 것이고 이 코인의 비전에 기본적인 부분을 담당하게 될 것입니다. 또한 마스터 노드들은 가상화폐의 순환을 안정화시키고 네트워크 보안을 강화하고 중요한 기능성을 제공해줄 것입니다.

감사의 말

Bulwark 는 Bitcoin, Peercoin, Blackcoin, Talkcoin, Dash 그리고 PVIX 팀들의 존경할 만한 선행 결과가 없었다면 가능하지 않았을 것입니다. 오픈 소스 소프트웨어와 이의 기여자들 또한 새롭고 흥미로운 혁신으로의 길을 지속적으로 열어주고 있습니다. 정보와 지식이 자유로이 공유될 수 있을 때, 사회 전반에서 보탬이 될 것 입니다. 저희가 이러한 생태계의 성장에 기여할 수 있는 기회를 제공해준 선행자들에 대해 감사의 말을 드립니다.

Table of Contents

1 장. 가상화폐에 대한 간략한 설명

1.1 배경지식

2009 년, Satoshi Nakamoto 는 *Bitcoin: A Peer-to-Peer Electronic Cash System* 이라는 제목의 논문을 발표했습니다. Nakamoto 의 비전은 해시 (hash) 기반 작업증명 (proof-of-work)의 지원을 받는 개인 대 개인간의 통화 유통 시스템을 구체화했습니다. 네트워크는 계속 작업중인 장부에 거래내역을 해시하는 방식으로 거래내역을 타임스탬프 (timestamp) 하며, 이러한 장부는 다시 작업증명을 하지 않는 한 바뀔 수 없습니다. 노드들(Nodes)은 해싱파워의 가장 큰 풀에 의해 관찰되는 사건의 증명으로서 가장 긴 체인을 선택합니다. 51%이상의 네트워크 해싱 파워가 공격을 용이하게 하지 않으려는 노드들에 의해 제어되는 한, 그 체인은 가장 긴 상태를 유지합니다 (Nakamoto 2009).

1.2 The Block 블록

네트워크에 있는 모든 블록은 80 byte 헤더와 함께 이전 블록 헤더의 SHA256 해시, merkle root (블록에 있는 모든 해시에서 파생된 SHA256 더블 해시), 작업증명이 시작되었을 때의 타임스탬프, 헤더의 해쉬가 지향하는 난이도 목표(less-than or equal to), 채굴자가 난이도 목표를 도달했을 때의 nonce 를 포함하고 있습니다. 따라서, 어떠한 블록에서 거래정보를 바꾸려는 행위는 네트워크의 채굴자에 의해 거부가 될 것습니다. (Bitcoin Core Team 2017)

1.3 The Blockchain 블록체인

거래내역의 그룹들은 블록으로 형성되며 그 블록들은 시간 순으로 블록 체인을 형성하는 체인내에 저장됩니다. 블록체인은 네트워크상의 모든 활동들에 대한 움직이는 기록이 되며, 언제, 어떤 거래내역인지 확인이 되는 분산된 합의 모델로서의 역할을 수행합니다 (Crosby et al. 2015).

1.4 Proof-Of-Work 작업증명

작업증명은 채굴자가 전기, 하드웨어 비용과 같은 유형의 자원을 투자하여 임의의 확률론적 단어 문제를 푸는 증명 시스템입니다. 누군가 악의를 갖고 거짓된 거래내역으로 블록체인을 교란시키기 위해선, 현 시점까지의 모든 작업증명을 완료해야 합니다 (Okupski 2016).

2 장. Bulwark 에 대한 소개

2.1 확고한 기반

튼튼한 집을 짓기 위해선 확고한 기반이 필요하며, Bulwark 또한 다르지 않습니다. Bulwark 는 유명한 DASH 가상화폐에 기반한 PIVX 를 기반으로 만들어졌습니다. 모든 코인의 근원은 본래의 Satoshi Core 로 귀결되긴 하지만 각각의 프로젝트들은 그들이 제공하고자 하는 공동체를 나타내는 사상과 목적을 갖고 특정방향으로 나아갑니다. 저희는 새로운 기술을 탐구하며 선행 플랫폼의 개인정보보호 코인의 특성을 강조하고 확장해나가는 한편, 현재 플랫폼 기술에도 Bulwark 가 통합되도록 다양한 기술을 창조해낼 것입니다.

2.2 공동체를 위한 팀

몇몇 프로젝트에서 공동체를 우선순위에 두지 않고 뒷전으로 생각하는 경우가 있습니다. Bulwark 의 첫번째 우선순위는 바로 공동체입니다. 경품, 콘테스트, 활발한 토의 플랫폼 그리고 신규 가입을 막는 것에 대한 제로관용정책에 기반하여, Bulwark 는 다양한 최종수혜자들을 위한 가상화폐가 되고자 합니다. 저희 유저베이스 (userbase) 팀원들은 이미 유용한 스크립트와 가이드를 제공하여 사용자들이 더 나은 경험을 할 수 있도록 노력하고 있습니다.

2.3 공정함과 균형 잡힘

이 글을 작성하는 현재, 하나의 비슷한 기반을 가지는 많은 가상화폐들이 유입되었습니다. 기반 기술은 견고하지만, 사양 및 블록체인 매개변수들에 대해 자세히 검토하면 종종 공정하지 않은 방식이 드러납니다.

2.4 선(先) 채굴방식에 대한 문제

2.4.1 사례 연구: FooBarBazCoin

가상화폐 영역에 대한 최근 추세는 임의의 미래 날짜를 선택하고 해당 날짜의 통화 유통에 대한 선 채굴 퍼센트를 정하는 것입니다. 가상 FBC (FooBarBaz Coin)인 DASH fork 를 예를 들어보도록 하겠습니다:

- 블록 보상: 15
- 블록 시간: 2.5 minutes
- POW/Masternode 분할: 50/50%
- 초기 난이도 알고리즘: KGW

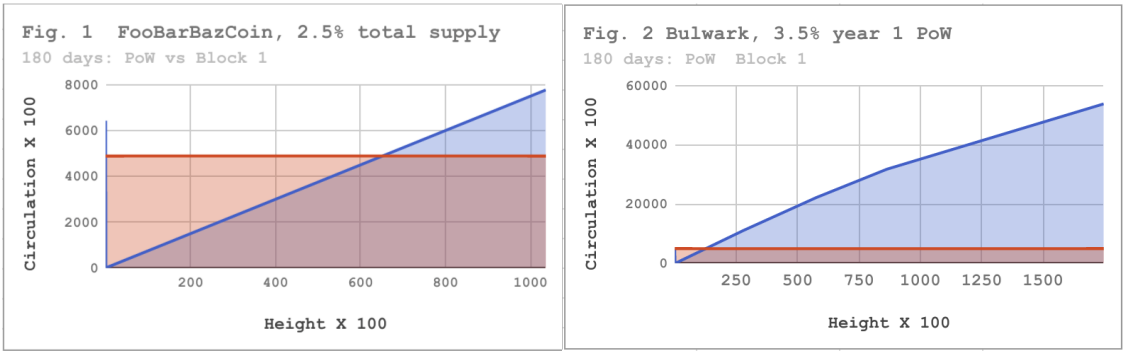
- 배당금 (subsidy) 매년 12% 감소
- 최대 코인 공급량: ~2500 만개
- 2.5% 채굴

이 사례에서, 일반 사용자에게 643,000 코인 (전체 2500 만개 중)에 해당하는 2.5% 사전채굴량은 합리적으로 보입니다. 그러나 PoW 및 마스터노드 보상이 개발자가 보유한 코인과 일치하기 위해서는 약 43,000 개의 블록이 요구됩니다. 블록 당 2.5 분을 목표로 하기 위해선, 같은 양의 코인을 채굴하기 위해 약 150 일 (또는 전체적으로 75 일)이 소요됩니다. 75 일 후, 개발자는 존재하는 코인의 절반을 여전히 보유하고 있습니다.

2.5 더 공정한 대안

Bulwark 팀은 이러한 문제점을 인식, 투명한 자세로 임하기로 했습니다. 489,720 코인 (3.5%)의 사전 채굴량은 PoW 채굴 12 일 또는 전체 생산 10 일 이상을 의미하여, 희망적으로 공동체에 안정감을 주어 특정 시점 이후 핵심 팀이 보유한 코인으로 인해 본 코인 시장이 크게 평가 절하되지 않도록 할 것입니다. 아래 그림은, 각 시나리오에서 180 일간의 예상결과를 보여주며, 그 차이는 극명합니다. 본 개발팀은 이와 같은 솔직한 방식으로의 접근이 우선순위를 정하고, 공동체 전체에 도움이 되기를 희망합니다.

2.5.1 두 접근법의 비교



2.5.2 Instamine 과 저희의 접근법

Dash (Darkcoin)은 인스타마인(instamine) 보호에 대한 필요성 관점에서 흥미로운 사례 연구 대상입니다. 소수 적극적인 사용자에 의해 코인 도입 초기 수 일 내에 10~15%의 Dash 코인이 생산되었습니다 (Wieko 2017). 본 개발팀의 인스타마인 문제에 대한 대응방식은 크게 두 가지로 나뉩니다. 저희는 첫 960 개 (1 일)의 블록들이 선형적으로 증가하도록 하였고, 전체 채굴량 100%가 채굴자들에게 배당되도록 하였습니다. 역사적으로, 이러한 방식은 특정 블록 높이에서 보상량이 소규모 보상에서 원래 보상량으로 바뀌는 보상방식으로 접근되어왔지만, 종종 풀이 고의적으로 DDoSed 되거나 신규 채굴자 유입을 감당하지 못하는 결과를 낳았습니다. 보상을 선형적으로 증가시키는 방식은, 채굴자나 풀 관리자가 자금을 수득하는데 방해받는 일이 없도록 할 것입니다.

2.5.3 ICO? 아이씨-노(NO)!

글을 쓰는 지금도 수많은 ICO 가 넘쳐나고 있습니다. ICO 는 가상화폐생태계에서 그들만의 합법적인 지위를 갖고 있지만, 종종 ICO 는 부가 일부에게 집중되게 합니다. Bulwark 가 마스터노드 보상, 그리고 두 번째 단계로 proof-of-stake 보상을 제공한다는 점을 고려하면, 이러한 부의 집중은 거대한 시장 변동을 야기할 수 있으며 지배(governance) 시스템이 가장 초기의 (가장 부유한) 구매자들에게 유리하게 기울수도 있을 것입니다. 전체적으로 부의 집중은 불가피 하지만, 저희는 공평함을 유지할 수 방법이 있다면 그게 어떠한 방법이라도 고려할 만하다고 믿습니다. 저희는 계량된 블록 보상 전략을 선택하여, Bulwark 가 많은 유저들에게 폭 넓게 분배되도록 하여, 이상적으로는 다른 프로젝트에서 쉽게 발생하는 부의 집중을 방지할 것입니다.

2.6 빠르고 실용적

90 초의 블록시간, 마스터노드 합의 그리고 거래내역 잠금을 기반으로 하며 합리적인 출시 계획, 그리고 커뮤니티 친화적 staking 을 가지고 있는 Bulwark 는 빠르고 기능적인 가상화폐가 되기를 희망합니다.

3 장. 저희의 블록체인 변수들

3.1 Bulwark Specifications at a Glance

Table 3.1: At a glance specifications for Bulwark

Specification	Descriptor
Ticker	BWK
Algorithm	NIST5
RPC Port	52541
P2P Port	52543
Block Spacing	90 Seconds
Difficulty Algorithm	Dark Gravity Wave v3.0
Block Size	1MB
Mined/Minted Maturity	67 Blocks (~100 Minutes)
Confirmation	6 Blocks (~9 Minutes)
Circulation (1 Year)	14,505,720 BWK
Circulation (5 Years)	27,668,220 BWK
PoW Period	*nHeight* ≤ 345,600
PoS Period	*nHeight* ≥ 345,601
Protocol Support	IPV4, IPV6, TOR
PoS	Blackcoin v3.0 PoS, PIVX SeeSaw rewards

3.2 SlowStart

저희의 공정한 시작점은 다음의 코드 Snippet 으로부터 시작합니다 (Zcash 로부터 가져옴)

```
int64_t nSlowSubsidy = 50 * COIN;

if (nHeight < 960 / 2) {      // If block height less than 480,
    nSlowSubsidy /= 960;              // Set nSubsidy to .05208333
    nSlowSubsidy *= nHeight;          // Multiply present height by .05208333
} else if (nHeight < 960 {    // ex: Block 200, BR will be 10.41666600
    nSlowSubsidy /= 960;              // Credits: ZCASH Team
    nSlowSubsidy *= nHeight;
```

3.3 Dark Gravity Wave 3.0

Dark Gravity Wave 는 PoW 난이도를 재조정 하기위한 방법으로서 초기단계부터 도입되었습니다. 이것은 급격한 해시 증가 또는 감소에 대응하기위해 간단한 동적 평균을 사용합니다. 이것은 멀티 풀에 의해 종종 야기되는 “stuck block effect” 위험을 줄이고 개인이 상당한 양의 컴퓨팅 능력으로 즉각적으로 여러 블록의 문제를 푸는 것을 방지합니다.

4 장. 블록 보상

4.1 PoW Block Reward

Table: PoW Period Block Reward Specifications

Subsidy	Block	PoW	MN	Circulation
489720	1	100%	NA	489200
~25(avg)	2-960	100%	NA	513150
50.000	961-28800	80%	20%	1953150
50.000	28801-57600	75%	25%	3393150
50.000	57601-86400	66%	33%	4833150
43.750	86401-172800	50%	50%	8613150
37.500	172801-2 59200	50%	50%	11853150
31.250	259201-345600	50%	50%	14553150

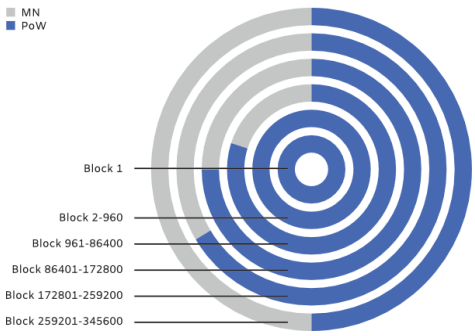


Figure 4.1: PoW Period Block Reward

4.2 PoS Block Rewards

Table 4.2: PoS Period Block Reward Specifications

Subsidy	Block	Budget	PoS/Masternode	Note
25.000	345601-432000	10%	SeeSaw	Year 2
21.875	432001-518400	10%	SeeSaw	Year 2
18.750	518401-604800	10%	SeeSaw	Year 2

15.625	604801-691200	10%	SeeSaw	Year 2
10.250	691201-777600	10%	SeeSaw	Year 3
10.938	777601-864000	10%	SeeSaw	Year 3
9.3750	864001-950400	10%	SeeSaw	Year 3
7.8120	950401-1036800	10%	SeeSaw	Year 3
6.2500	1036801-1123200	10%	SeeSaw	Year 4
5.4690	1123201-1209600	10%	SeeSaw	Year 4
4.6880	1209601-1296000	10%	SeeSaw	Year 4
3.9060	1296000-1382400	10%	SeeSaw	Year 4
3.1250	1382401-1468800	10%	SeeSaw	Year 5
2.7340	1468801-1555200	10%	SeeSaw	Year 5
2.3440	1555201-1641600	10%	SeeSaw	Year 5
1.9530	1641601-1728000	10%	SeeSaw	Year 5
1.6250	1728000+	10%	SeeSaw	In perpetuity

5 장. NIST5 Hashing

5.1 왜 NIST5 인가

NIST5 hashing 알고리즘은 2014 년에 TalkCoin 으로 인기를 얻어, 대중적으로 사용되어왔습니다. NIST5 는 다양한 소비자들이 살 수 있는 CPU 뿐만 아니라 AMD, Nvidia GPU 를 사용하여 채굴할 수 있습니다. NIST5 는 다른 알고리즘만큼 ASIC 내성이 있지는 않지만 이런 메모리를 많이 사용하는 알고리즘보다 높은 시스템 안정성, 낮은 소비 전력을 가지기에 이러한 트레이드 오프가 정당화된다고 생각합니다. PoW 기간이 끝나기 전에 ASICs 가 펌웨어 업데이트를 통해 NIST5 를 지원하기 시작하면 저희는 대체 알고리즘을 준비해 놓은 상태입니다. 이럴 경우 행동의 절차(가 있다면)에 관해 커뮤니티 투표를 요청할 것이고 그에 따라 시행할 것입니다. 저희의 짧은 PoW 기간과 채굴 알고리즘을 바꾸려는 의지가 ASIC 제조업체에 불리하다고 생각하며 추후에 문제를 일으킬 것이라고 생각하지 않습니다.

5.2 5 개의 최종 후보들 (NIST SHA-3 Competition)

NIST5 를 만든 5 개의 hashing 알고리즘은 NIST Hashing Competition (Chang et al. 2012)에서 뽑힌 5 개의 최종 후보들입니다.
Blake (Aumasson 2013), Grøstl (Gauravaram1 et al. 2012), JH (Wu 2012), Keccak (Bertoni et al. 2012), and Skein (Ferguson et al. 2010).

5.3 새로운 SHA-3 기준

결국 Keccack 이 마지막 라운드를 통과하여 새로운 SHA-3 hash 기능으로 이름을 얻었습니다. 나머지 4 개 알고리즘은 (암호학의 관점에서 봤을 때 안전하다고 여겨짐에도 불구하고) 몇 개의 작은 문제에 의해 점수를 잃었습니다. 저희는 새로운 SHA-3 기준과 더불어 다른 후보들을 조합함으로써 더 빠르고, 안전하고, 인정받는 hashing 알고리즘을 제공할 수 있을 것이라고 생각합니다.

5.4 가능한 채굴 소프트웨어

현재, 채굴자한테 몇 개의 선택지들이 있습니다:

이름	플랫폼	링크
SGMiner-5.0	OpenCL	

ccminer-2.2.2	CUDA
cpuminer-opt	CPU

6 장. 특징

6.1 마스터노드

근본적으로 마스터노드는 Bulwark 네트워크를 제공하는 컴퓨터들의 탈중앙화된 집합체입니다. 마스터노드들은 중요한 네트워크 기능을 수행하고 블록 보상의 일부분을 받습니다. 코인 공급 안정화, 거래의 진행 그리고 네트워크의 보안화를 통해 Bulwark 생태계를 이끌어갑니다. 마스터노드를 만들기 위해 5000 BW 와 함께 어느 정도의 기술적인 지식을 필요로 합니다. 5000 BW 를 보관하는 어느 지갑으로도 마스터노드를 설정할 수 있습니다.

6.2 코드 난독화 / 코인 믹싱

Bulwark 는 CoinJoin 을 기반으로 하지만 더 다양하고 개선된 난독화 기능을 제공합니다. 이는 마스터노드들의 네트워크에 의해 촉진된 분산 방식으로 한 코인 믹싱을 통해 이루어집니다. 이것은 거래에 한 층 강화된 프라이버시를 제공합니다. 완벽하게 익명성을 보장하지는 않지만, 노드 믹싱을 통한 난독화는 표준 비트코인 거래보다 훨씬 뛰어납니다. 예를 들어, 모든 비트코인 거래는 공개되어 있지만, Bulwark 에서는 악의적인 행위자는 마스터 노드의 50%를 제어한다고 하더라도 8 번의 코드 난독화를 거친 단일 거래의 정보를 볼 확률이 0.5% 미만이 됩니다. (Kiraly 2017b). 이 중요한 특징은 코드 난독화를 한 BWK 사용자들에게 높은 수준의 익명성을 제공합니다.

6.3 SwiftTX

SwiftTX 는 거래를 위한 잠금과 합의 권한을 가진 마스터노드들을 제공합니다. 거래가 네트워크에 전송될 때, 마스터노드 그룹이 이 거래를 유효화시킬 것입니다. 만약 마스터노드들이 거래의 유효성에 대한 합의에 도달하면, 거래는 추후에 블록체인에 도입기위해 잠겨질 것이며 이는 기존의 시스템 (블록 시간이 10 분이고 여러 번의 유효화가 필요한 비트코인과 같은)에 비해 거래 속도를 크게 향상시킬 것입니다. 이 시스템은 Dash 의 InstantSend 기술에 기반합니다 (Kiraly 2017a).

6.4 Sporks

Bulwark 네트워크는 “sporking”이라는 여러 단계를 통해 이루어지는 포크 매커니즘을 사용합니다. 이를 통해 BWK 네트워크는 배포 도중 의도하지 않은 네트워크 포크의 가능성은 최소화하며 새로운 기능을 도입할 수 있습니다. Spork 변경은 네트워크를 통해 배포 할 수 있으며 필요에 따라서 노드 소프트웨어를 업데이트하지 않고도 켜고 끌 수 있습니다 (strophy 2017). 이 기능은 매우 유용하며 네트워크가 보안 취약성에 신속히 대처할 수 있게 합니다.

6.5 TOR & IPV6 마스터노드

Bulwark 는 사용자들이 Onion 주소 또는 IPV6 주소에서 전체 노드 또는 마스터 노드를 돌릴 할 수 있게 합니다. 저희는 TOR 네트워크 자체에 대한 강화와 함께 TOR-only 모드를 사용하는 사용자 경험을 높이기 위해 TOR 노드를 추가하려고 노력하고 있습니다. TOR 마스터노드 만의 특별한 기능은 마스터노드를 TOR 숨김 서비스로써 작동시킬 수 있는 것입니다. TOR 노드는 안정된 인터넷 연결을 통해 사용자들이 자신들의 위치가 노출되는 사생활 침해, 홈 네트워크에 대한 공격 또는 침입의 에 대한 위험을 최소화 시킵니다.

6.6 커뮤니티의 중요성과 관리 시스템

Bulwark 커뮤니티는 프로젝트의 장기간 성공에 있어서 가장 중요한 요인이고 코인의 미래에 미칠 수 있는 영향이 매우 큽니다. 따라서, PoW 단계가 끝나면 네트워크에서 예산 superblock 을 활성화 시킬 계획입니다. 매달 지급되는 superblock 은 커뮤니티가 Bulwark 의 개발, 브랜드 존재 및 커뮤니티 문제에 대해 통제를 할 수 있게 합니다. 이 시스템의 활성화가 지연되면 긍정적인 사용자 경험에 필요한 기본 프레임워크를 개발할 수 있는 시간을 갖게 되고 채굴자와 마스터노드들에서 사용할 수 있는 블록 보상을 최대화할 수 있게 됩니다.
저희는 제안서를 작성하고 제출할 때 다-단계 프로세스를 활용할 것입니다. 각 단계는 완전히 완료되어야 할 것입니다. 약술된 단계를 완료하지 않으면 제안이 활성화되지 않습니다. 이 단계들의 기본 개요는 다음과 같습니다 :

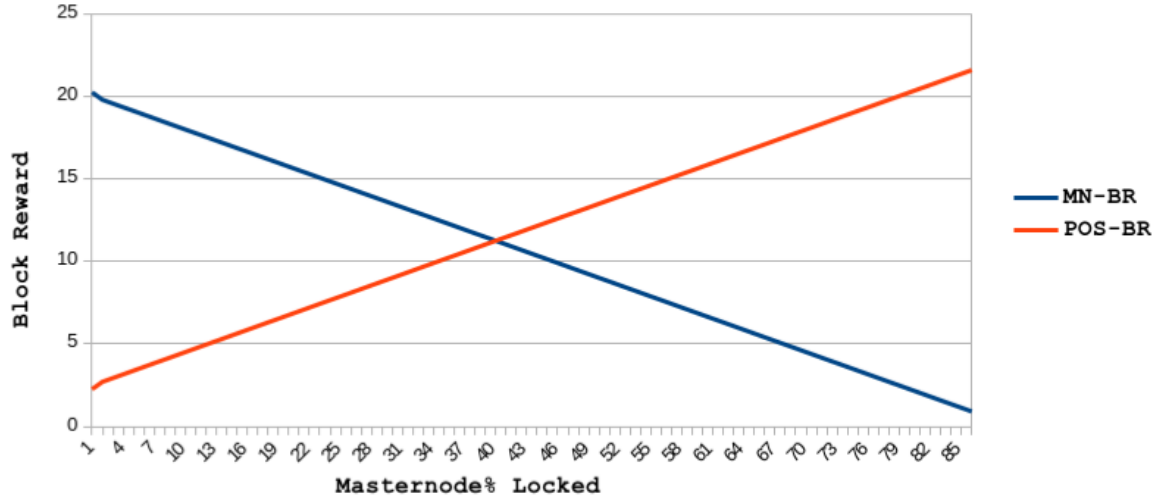
- 저희의 디스코드 채팅방에서 경험 많은 사용자들과 이야기를 나눕니다. 흥미를 판단하고 만약 반응이 긍정적이면 다음 단계로 넘어갑니다.
- 여러 소셜 미디어 플랫폼을 활용해서 토론하고 피드백을 받습니다. Bulwark 는 다양한 사용자 기반과 다양한 수준의 관리 참여를 지니고 있으며, 사용자 기반의 일부분에 도달하기 위해서는 종종 대응이 필요합니다. 이러한 토론을 기록하고 공식 사전 제안서에 인용할 수 있도록 해야합니다. 제공되는 인용 수가 많을수록 더 나은 결과를 얻을 수 있습니다.
- 커뮤니티와 개발자의 의견을 열린 마음으로 들어야 합니다. 융통성 있게 당신의 제안서에 외부의 아이디어등을 넣는 것에 대해 긍정적으로 생각해야 합니다.
- 웹사이트의 Governance -> Pre-Proposal 란에 공식 사전 제안서를 작성해야 합니다. 이전 단계에서 일어난 모든 토론에 대한 서지 정보를 제공해야 합니다. 투표를 위해 사전 제안서를 블록 체인에 제출하는 것처럼 다루어야 합니다.
- 이런 단계들을 완료하면, 제안서를 블록 체인에 제출하게 됩니다. 제출 시에 지불할 수수료와 블록체인에 제안서를 활성화시키는 개발자에게 지불할 투표 비용으로 2 개의 수수료가 청구됩니다. 제출 비용은 환불되지 않으며, 투표 비용은 제안 승인 및 활성화시에만 지불됩니다.
- 모든 사람들은 두 비용의 상환 비용을 포함하도록 제안서를 자유롭게 조정할 수 있습니다. 정식 제안서에 귀하가 요청한 급여액을 상환한다고 명시되어 있는지 확인해야 합니다.
- 귀하의 아이디어가 통과 될 수 있도록 이야기를 나눈 모든 사람과 다시 연락하는 걸 잊지 마세요. 제안이 통과되기 위해서 자격을 갖춘 마스터노드의 10%가 제안서에 대해 동의 해야합니다. 10%의 합의를 받는 과정은 생각보다 훨씬 어려울 수 있습니다. 따라서 제안이 통과되기 위한 표를 확보하기 위해 성실하고 유익하며 타인을 존중하여야 합니다.

6.7 SeeSaw PoS/마스터노드 보상

저희는 PIVX (jakiman 2017)에 의해 대중화된 SeeSaw 보상 시스템을 활용하기로 결정했습니다. SeeSaw 보상 시스템은 9:1 블록 보상 비율 (마스터노드 선호)로 시작하고 동전 유통량의 약 41.5%가 마스터노드에 고정 될 때까지 staking/노드 운영자 보상 비율을 부드럽게 조정합니다. 최종적으로 staking 보상은 마스터노드 보상보다 조금 더 유리하게 작용합니다. Seesaw 에서 staking 보상을 더 선호하는 이유는 높은 물가 변동성과 낮은 유동성과 같은 문제들을 피하고 싶기 때문입니다. 이런 문제들은 주로 유통량의 높은 비율이 노드에 고정되어 있는 코인에 많이 발생합니다. 이 전략은 코인 공급에 대한 사용자의 불만을 완화하고 강력하고 우수한 네트워크의 유지시켜 줄 것입니다. 저희의 목표 중 하나가 익명의 상업을 위한 플랫폼이기에, 거래 채결력은 Bulwark 를 받아들이는 사람들과 Bulwark 를 갖고 있는 사람들에게 매우 중요한 요소 중 하나입니다.

Fig 3. SeeSaw @ Height 345601 - 432000

(after budget percentage)



7 장. 미래

7.1 Bulwark 도구 상자

도구상자는 Code snippet, API, libraries, 스크립트, 정보등을 모아놓은 시장-느낌의 환경을 제공합니다. 여기서 개발자들은 정보, 지식, 코드를 교환함으로써 자신의 암호화폐 프로젝트에 대한 지원을 받을 수 있습니다. 저희는 개발자들에게 이러한 도구를 제공하는 것이 목수에게 흥미롭고 훌륭한 대작을 만드는 데 필요한 도구를 제공하는 것과 유사하다고 믿습니다.
A collection of code snippets, APIs, libraries, scripts, and knowledge that will serve to encourage a bazaar-like environment where developers who may be seeking the addition of cryptocurrency support in their projects are free to exchange knowledge, information, and code.

7.2 프라이버시와 소프트웨어 향상

저희는 사용자의 프라이버시를 향상시키는 새로운 프로토콜을 적용 할 것을 약속합니다. 현재 평가 중인 여러가지 방법이 있으며 2018 년 상반기에 내부 테스트 및 개발을 시작할 계획입니다. 이는 다음의 업그레이드를 포함합니다:

- I2P 프라이버시 네트워크
- Zerocoin 프로토콜 또는 Stealth 주소 도입 (이 해법에 대해 확신이 들 때 도입 예정)
- 코드베이스를 비트코인의 메인라인과 가깝게 동기화
- QT 지갑의 간소화 및 업데이팅
- Libtox 지원
- 추가적인 보안 층을 추가하기 위해 Bulwark 지갑의 가상화 및 컨테이너화

7.3 Bulwark Secure Home Node

저희는 CAD 전문가와 협력하여 소형의 내장형 home Bulwark 노드를 설계 할 것 계획입니다. 사용자들은 이것을 홈 네트워크에 연결하고 웹 UI 를 사용하여 구성할 수 있을 것입니다. 저희가 활성화하려는 기능은 다음과 같습니다:

- 안정적인 인터넷 연결을 가지고 있는 사람들을 위해, TOR 숨김 서비스를 사용하여 완전히 onionized 된 마스터노드 (또는 전체 노드)를 쉽게 설정할 수 있습니다.
- TOR 네트워크 전체에 대한 개선을 위한 릴레이 옵션

- TOR/I2p 네트워크를 통한 트래픽을 라우팅하는데 사용할 수 있는 VPN 및/또는 프록시
- 가상화 또는 부가 장치를 통한 Bulwark staking

탈중앙화를 염두하며, 3D 인쇄가 가능한 파일들과 모든 소스코드들은 집에서 사용 가능하게끔 하기 위해 커뮤니티에 공개될 것입니다.

7.4 브랜드의 확장

저희는 계속해서 브랜드를 확장하고 저희와 동일한 열정과 이상을 공유하는 하드웨어 공급 업체 및 시스템 통합 업체와 협력할 계획입니다. 5 년이내에 저희는 'Bulwark'이라는 이름을 암호화폐뿐만 아니라 개인 정보, 보안, 및 사용자의 자유에 대한 존중과 동의어가 되기를 원합니다. Bulwark 의 주된 목적은 프라이버시를 통한 선택의 자유를 제공하는 것입니다.

7.5 디자인과 영상

Bulwark 의 연구 및 개발을 통해 저희는 암화화폐 시장에서의 다른 경쟁상대와 차별화되는 디자인 언어를 만드는 것을 목표로 하고 있습니다. 저희의 디자인 팀은 최상의 사용자 환경을 제공하는 매체와 아름다운 미학을 찾고, 현재의 UI/UX/Branding 을 혁신하고 실험하여 우수한 디자인을 만들 예정입니다. 이는 경쟁상대에 대한 조사와 더불어 최신 기술 및 표준에 대한 동향 파악, 새롭고 흥미로운 결과물을 최종 사용자에게 제공함으로써 이루질 것입니다

8 장. 결론

8.1 요약

Bulwark 는 마스터노드, 관리 및 진화하는 생태계의 도구를 지닌 프라이버시 지향적인 코인입니다. 이 프로젝트는 공정한 출시와 광범위한 코인 유통에 초점을 맞추어 시작했습니다. 느린 시작, 블록 보상 분배 및 hashing 알고리즘은 높은 커뮤니티 참여도를 창출하기 위해 신중하게 선택되었습니다. Bulwark 는 다양한 프라이버시 기능을 가지고 시작했으며 개발팀은 새로운 기능을 도입하고 기존의 기술을 기반으로 새로운 기술을 만들어 내는 데에 최선을 다하고 있습니다. Bulwark 는 프라이버시를 통해 공정한 투표권을 부여하는 것을 목표로 하고 있으며 이를 위해 최대한의 노력을 기울일 것입니다.

8.2 향후 계획

마스터노드-프라이버시 코인 생태계는 투자에 대해 말도안되는 수익률 보장, 지키지 못한 약속들로 가득 찬 거대한 로드맵, 공간 내의 실질적 개선 보다는 마케팅에만 집중하여 새로운 사용자들을 유치하려고 하는 코인들로 넘쳐나고 있습니다. Bulwark 는 이와는 반대로 과대광고를 줄이고 실질적인 결과물을 내놓을 계획입니다. 프로젝트의 현재 및 미래의 목표는 구체적이고 측정 가능하며, 달성 가능하고, 관련성이 있어야하며 시간을 맞춰야한다는 공식을 따를 것 입니다.

참고자료

Aumasson, L.M., Jean-Phillipe Henzen, 2013. SHA-3 proposal: BLAKE. Available at: .

Bertoni, G., Daemen, J., Peeters, M. & Van Assche, G., 2012. The keccak sha-3 submission. Available at: .

Bitcoin Core Team, T., 2017. Bitcoin developer reference. Available at: .

Chang, S.-J., Perlner, R., Burr, W.E., Turan, M.S., et al., 2012. Third-round report of the sha-3 cryptographic hash algorithm competition. Available at: .

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., et al., 2015. BlockChain technology. Available at: .

Ferguson, N.L., Schneier, S., Whiting, B., Bellare, D., et al., 2010. The skein hash function family. Available at: .

Gauravaram1, P., Knudsen, L.R., Matusiewicz, K., Mendel, F., et al., 2012. Grøstl – a sha-3 candidate. Available at: .

jakiman, 2017. PIVX purple paper. Available at: .

Kiraly, B., 2017a. InstantSend. Available at: .

Kiraly, B., 2017b. PrivateSend. Available at: .

Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system. Available at: .

Okupski, K., 2016. Bitcoin developer reference., pp.3–4. Available at: .
strophy, 2017. Understanding sporks. Available at: .
Wiecko, R., 2017. Dash instamine issue clari cation. Available at: .

Wu, H., 2012. The hash function jh. Available at: .