BULWARK

CRYPTOCURRENCY

# Cryptocurrency Whitepaper


Bulwark Core Team:

Eatbatterys (Koordineytor ng proyekto)

Jack (Direktor ng Marketing)

SerfyWerfy (Nagpapaunlad ng Blockchain)

Frogman (Pinangungunahan ang Komunikasyon)

Patrick (Tatak at Disenyo)

Stu (Nagpapaunlad ng Ecosystem)

Ang Bulwark Core Team


December 2017

*Kami, ang Bulwark Core Team, ay kinukumpirma na ang gawain na ipinakita sa whitepaper na ito ay amin. Na kung saan ang impormasyon ay galing sa sources, kinukumpirma namin na ito ay nakalagay sa attributions.*

# Diwa

Bulwark (ticker: BWK) ay coin na nakikibagay sa komunidad, nabuhay mula sa mga karaniwang hindi pantay na gawi  sa loob ng masternode privacy coin space. Ang aming pinagisipang mabuti na pantay na istratehiyang paglulunsad ay pinapayagan ang mga sumasali ng oportunidad sa isang magandang proyekto. Kami ay nag-aalok ng simpleng may halagang panukala na walang engrandeng pangako: maghahatid kami ng privacy coin na gagana ngayon at sa hinaharap sa pamamagitan ng tulong mula sa pinakamagagaling na gawi mula sa DASH at PIVX. Walang imahinatibong paningin na may limitadong pag asam ng paghatid, ngunit isang coin na gumagana sa working platform na may pag-suporta sa hinaharap.  Hindi ibig sabihin nito na wala kami plano sa hinaharap, subalit maghahatid kami ng resulta kesa hype. Sobrang dami ng coins na pinapagana ng hype-ngunit walang wala sa sangkap-at ayaw naming makisali sa lumalaking grupo ng coins na pinatatakbo ng matatamis na salita ngunit kulang sa gawa. Walang  ICO, isang soft-launch na reward ramp, maliit na premine at pinapaboran ng miner ang alokasyon sa pabuya ng block, Ang tumatanggap sa Bulwark ay magkakaroon ng ground-floor access sa pribadong coin na nag-aalok ng halong masternodes at pagkakaroon ng pinakamagandang teknolohiya ng pribadong coin kasama ng makabuluhang pagunlad sa roadmap. Magkakaroon ng mga masternodes na gagana sa paglunsad na saligang parte ng pananaw ng coin at matatag na sirkulasyon, pirming network, at magbigay ng importanteng gawain.

# Mga Pagkilala

Ang Bulwark ay hind magiging possible ng walang naunang pagkilos ng mga respetadong grupo ng Bitcoin, Peercoin, Blackcoin, Talkcoin, Dash at PIVX. Bukas na pinanggagalingan ng software at mga kontribyutor ay parating nagbubukas ng daan para sa bago at nakakasabik na pagbabago. Kapag ang impormasyon at kaalaman ay libreng maitatayo, ang buing pamayanan ay mag-bebenepisyo. Nagpapasalamat kami sa aming mga hinalinhan para sa oportunidad na makatulong dito sa yumayabong na sistema.

# Mga nilalaman

# Kabanata 1

# Maikling Introduksyon sa Cryptocurrency

## 1.1 Pinagmulan

Noong 2009, si Satoshi Nakamoto ay naglabas ng papel na may titulong *Bitcoin: A Peer-to-Peer Electronic Cash System* na nagsasaad sa kanyang pananaw sa komersyo. Dinetalye ng pananaw ni Nakamoto ang sistema ng kaperahan ng peer-to-peer at base sa Hash patunay-sa-paggawa. Ang network ay itatala ang mga transakyon sa pamamgitan ng pag-hash nito sa ledger na hindi mababago ng walang pagsagawa muli ng patunay-sa-paggawa. Ang Nodes ay mamimili ng pinakamahabang chain bilang patunay ng mga pangyayari na nasaksihan ng pinakamalaking pool ng kapangyarihan ng hashing . Hangga't ≥ 51% ng network ng kapangyarihan ng hashing ay kinokontrol ng nodes na hindi sinasadyang magsagawa ng pag-atake, ang chain na magagawa nila ay ang pinakamahaba. (Nakamoto 2009).

## 1.2 Ang Block

Kada block sa network ay pinangungunahan ng 80 byte header na may dobleng SHA256 hashed na kopya ng nakaraang header ng block, merkle root ( dobleng SHA256 pinangungunahan ng lahat ng hashes na nangyari sa block. Ang time stamp kung saan ang Proof-of-work ay nagumpisa, ang target na kahirapan ng header's hash ay dapat na mas mababa o pantay, at ang isahang pag-gamit na kung saan ang mga miners ay naabot na ang target na kahirapan at. Dahil dito, anumang tangha na baguhin ang kahit na anong transaksyon sa kahit na anong block ay magreresulta sa pagtanggi ng block ng mga network miners. (Bitcoin Core Team 2017).

## 1.3 Ang Blockchain

Ang grupo ng transaksyon ay nabuo sa blocks, at ang blocks ay sinasaayos ayon sa pagkakasunod-sunod-na tinatawag na blockchain. Ang blockchain ay lumilikha ng talaan ng lahat ng pangyayari sa loob ng network at nagsisilbing modelo ng pinamahaging kasunduan na maaring patunayan kahit anong oras. (Crosby et al. 2015).

## 1.4 Proof-Of-Work

Proof-of-work ay isang sistema ng pagpapatunay na kung saan ang miners ay dapat pagukulan ang mga nasasalat na kayaman(elektrisidad, presyo ng hardware) para malutas ang isang pagkakataon o tsansa ng *word puzzle*. Upang madungisan ng isang masamang nilalang ang blockchain sa pamamagitan ng mapanlinlang na transakyon, dapat makumpleto nya ang lahant ng proof-of-work hanggang sa kasalukuyan (Okupski 2016).

# Kabanata 2

# Ipinapakilala ang Bulwark

## 2.1 Isang matatag na pundasyon

Bawat bahay ang kailangan ng matibay na pundasyon, ang Bulwark ay walang pinagkaiba. Ang Bulwark ay ginawa mula sa *PIVX*, na kung saan ito ay gawa din mula sa pinakasikat na *DASH* cryptocurrency. Habang ang pinanggalingan ay matutuklasan lahat mula sa Satoshi Core, bawat proyekto ay namili ng partikular na direksyon na may mga layunin at ideya na kumakatawan sa komunidad na kanilang pinagsisilbihan. Lalawak kami at maglalagay ng diin sa tampok na seguridad ng coin ng aming hinalinhan na platform sa pamamagitan ng pag-galugad ng makabagong teknolohiya, habang gumagawa ng panibagong tool sets at oportunidad para sa pagsasama-sama nito sa kasalukuyang platform ng teknolohiya.

## 2.2 Ang Grupong dedikado sa komunidad.

Sa ibang proyekto, ang komunidad ay saka na lang iisipin. Ang unang priyoridad ni Bulwark ay ang komunidad. communities are an afterthought. Bulwark's number one priority is the community. May libreng bigay, paligsahan, masiglang diskusyon na platform at zero-tolerance na patakaran sa panliligalig sa mga baguhan, ang bulwark ay nagsisikap magin cryptocurrency sa lahay ng uri ng gagamit. Ang myembro ng aming userbase ay kasalukuyan ng nag-aambag ng magagamit na scripts at gabay upang lalong umunlad ang karanasan ng gagamit.

## 2.3 Patas at balanse

Sa panahon ng pagsusulat nito, may mga At the time of writing, may ma dumaloy na cryptocurrencies na gumagamit ng kaparehong pundasyon. Habang ang pinagbabatayah na teknolohiya ay matibay, madalas, ang malalim na pagsusuri ng kanilang spesipikasyon at blockchain parameters ay nagsisiwalat ng less-than-fair na gawain.

## 2.4 Gulo sa mga gawi ng pre-mine

### 2.4.1 Pag-aaral: FooBarBazCoin

May sumusulong na takbo sa cryptocurrency na kung saan mamimili ng petsa sa hinaharap at ibabase ang porsyento ng premine sa umiikot na panustos sa petsang iyon. Tignan natin ang likha na FBC (*FooBarBaz Coin*), isang *DASH* fork.

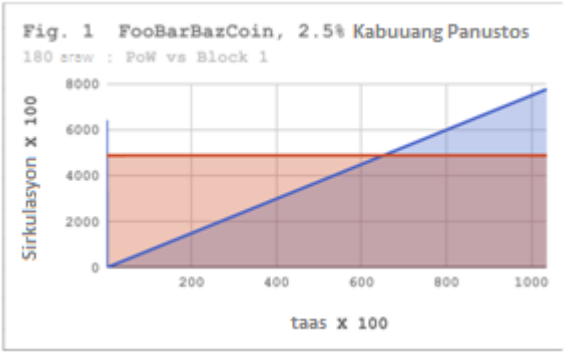
- Pabuyang Block: 15
- Oras ng Block: 2.5 minuto
- POW/Masternode Split: 50/50%
- Paunang hirap ng algorithm: KGW
- Tulong na salapi ay mababawasan ng 12% kada taon
- Pinakamalaking panustos na Coin supply: ~25 Milyon
- 2.5% pre-mine

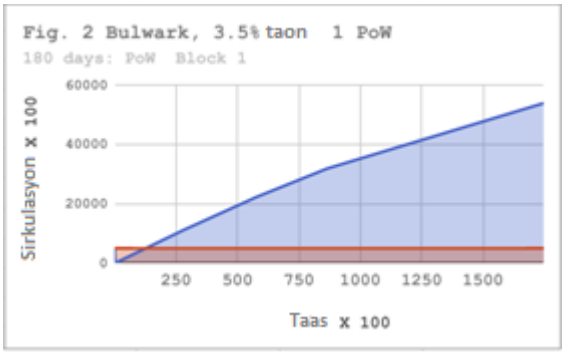
Sa halimbawa na ito, ang anunsyo na 2.5% pre-mine na masasalin sa ~643,000 coins (mula sa ~25 Million) ay mukhang makatwiran sa kaswal na tagapagmasid. Ngunit, para sa PoW at Masternode na pabuya upang tumugma ang coin na hawak ng mga nagpapaunlad, ito ay maaring tumagal ng tinatayang 43,000 blocks. Sa target na 2.5 minuto kada block, ito ay tatagal ng tinatayang roughly 150 araw para sa miners (o 75 araw sa pangkalatan)upang makagawa ng parehong dami ng coin. Pagkatapos ng 75 araw, ang mga nagpapaunlad ay mananatiling may control sa kalahati ng pag-iiral ng coin.

## 2.5 Mas pantay na alternatibo

Ito ay kinikilala ng koponan ng Bulwark, at nag-desisyong maging tapat. Ang aming premine na 489,720 coins (3.5%) ay kumakatawan ng humigit-kumulang 12 araw ng PoW mining o bahagyang mahigit na 10 araw ng pangkalahatang produksyon. Sana ito ay mag-silbi upang lumagay sa mapayapang pagiisip ng komunidad, na pagkatapos ng tiyak na puntoang pamilihan ay hindi basta mawawalan ng halaga resulta ng mga coins na hawak ng core team. Kung pagmamasdan ang mga figure sa baba, parehong nagsasaad ng 180 araw ang bawat senaryo, and pagkakaiba ay maliwanag. Umaasa kami na ang pagpapaunawa sa subject sa lantad na paraan ay magse-set ng priyoridad at magsisilbing benepisyo sa komunidad sa kabuuan.

### 2.5.1 Pagkumpara ng dalawang approach




### 2.5.2 Instamines at ang aming approach

Ang Dash (Darkcoin) ay naglalahad ng kawili-wiling case study sa pangangailangan sa proteksyon ng instamine. Tianatayang 10-15% ng kabuuang panustos ng Dash ay ginawa

ilang araw mula ng lumabas ang coins, salamat sa ilang handa sa hirap na mga gumagamit. (Wiecko 2017). Ang aming pag-unawa sa isyu ng instamine ay dalawang bahagi. Ginagamit namin ang tulong na salapi kung saan ang unang 960 blocks (1 araw) ay umangat sa buong pabuya ng block na may 100% block na pabuya ay napunta sa mga miners sa araw din na iyon. Sa kasaysayan, ito ay nilapitan ng pinakamaliit na pabuya ng block na biglang lumilipat sa tiyak na taas papuntang buong pabuya na block. Ngunit, kadalasan ito ay nag reresulta sa pools na sadyang nakakakuha ng DDoSed o nilalamon ng panibagong miner traffic. Ang linyang padagdag ng padagdag ng pabuya, walang pupuntahan para magtangka na pigilan ang mga miners o pool operators para makakuha ng salapi.

### 2.5.3 ICO? Mas gusto namin, IC-NO!

Harapin natin, sa panahon ng pagsusulat kami ay patuloy na pinipigilan ng *ICO*s. .Habang sila ay may lehitimong pwesto sa cryptocurrency ecosystem, madalas sila ay nagsisilbi na makagawa ng concentrated pockets ng yaman. Sa pagsaalang-alang na ang Bulwark ay parehong nag-aalok ng pabuya sa Masternode at sa ikalawang bahagi, pabuya mula sa proof-of-stake, ang konsentrasyon ng yaman ay maaring magdulot ng malakihang market swings, at patagilidin ang sistema ng pamumuno na sobrang pabor sa sinauna (at mayayaman) adopters. Bagama't ang konsentrasyon sa yaman ay hindi maiiwasan sa kabuuan,naniniwala kami na kahit anong oportunidad na maari naming kunin para malaro ng pantay ang field, ay isang oportunidad na makukuha. Kami ay naglunsad ng may scaled block reward strategy, isang patas na launch mechanic upang himukin ang malawak na pamamahagi ng Bulwark sa kabila ng madaming gumagamit, iniiwasan ang ilan sa konsentrasyon ng yaman na kita sa ilang proyekto.

## 2.6 Mabilis at gumagana

Sa oras na 90 segundo ng block, masternode consensus at pagkandado ng transaksyon, makatwirang iskedyul ng paglabas, at eco-friendly na pagtataya, ang Bulwark ay naghahangad upang totoong mabilis at gumaganang crytocurrency

# Kabanata 3

# Parametro ng Blockchain

## 3.1 Espisipikasyon ng Bulwark

*Table 3.1: Silip sa Espisipikasyon ng Bulwark*

| Specification | Descriptor |
|---|---|
| Ticker | BWK |
| Algorithm | NIST5 |
| RPC Port | 52541 |
| P2P Port | 52543 |
| Block Spacing | 90 Segundo |
| Difficulty Algorithm | Dark Gravity Wave v3.0 |
| Block Size | 1MB |
| Mined/Minted Maturity | 67 Blocks (~100 Minuto) |
| Kompirmasyon | 6 Blocks (~9 Minutes) |
| Pagpapalaganap (1 Year) | 14,505,720 BWK |
| Pagpapalaganap (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

An aming patas na pag-umpisa ay may sumusunod na code snippet (credit *ZCash*):

```
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
} elseif (nHeight <960 {      // ex: Block 200, BR will be 10.41666600
    nSlowSubsidy /= 960;            // Credits: ZCASH Team
    nSlowSubsidy *= nHeight;
```

## 3.3 Dark Gravity Wave 3.0

Ang Dark Gravity Wave ay empleyado ni Bulwark mula sa umpisa bilang pamamaraan na ma retarget ang PoW difficulty. Gumagamit ito ng simpleng paggalaw na maaring sumagot sa malawakang karagdagan sa nethash o drop-offs sa ilan lamang na blocks. Ito ay kakalma sa "stuck block effect" na kadalasan ay mula sa multipools at pumipigil sa isang tao na magdagdag ng malaking halaga ng computing power mula sa mabilisang paglutas ng higit pa sa kaunting blocks.

# Kabanata 4

# Pabuya sa Block

## 4.1 Pabuya sa PoW Block

*Table: Espisipikasyon ng PoW Period Block Reward*

| Tulong na salapi | Block | PoW | MN | Sirkulasyon |
|---|---|---|---|---|
| 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 |

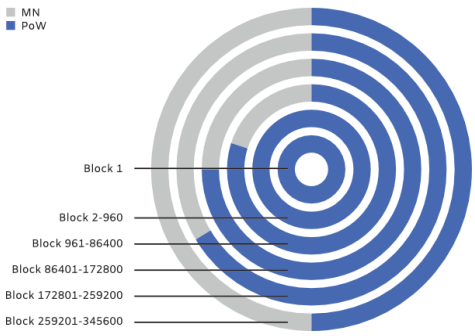



Figure 4.1: PoW Period Block Reward

## 4.2 Pabuya sa PoS Block

*Table 4.2: Espisipikasyon ng PoS Period Block Reward*

| Tulong na salapi | Block | Badyet | 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 | pamalagian |

# Kabanata 5

# NIST5 Hashing

## 5.1 Bakit NIST5

Pinatanyag ng TalkCoin noong 2014, ang NIST5 hashing algorithm ay kinakitaan ng pangunahing aktibidades sa paggamit. Ang NIST5 ay maaring i-mine sa malawak na hanay ng consumer-grade hardware kasama ang CPUs, ganon din ang AMD at NVidia GPUs. Ang NIST5, ay hindi lumalaban sa ASIC na gaya ng ibang memory hard algorithms, ngunit naniniwala kami na ang trade-off ay katanggap-tanggap para bumuti ang tatag ng sistema at mabawasan ang pagkonsumo ng enerhiya ukol sa memory hard algorithms. Sa mga pagkakataon na ang firmware ay mag-update sa pagdagdag ng NIST5 ng suporta sa ASIC ay lumutang bago ang pagtatapos ng aming Pow period, kami ay handa sa alternatibong algorithm bilang kapalit. Magsasagawa kami ng community vote sa loob ng pagkilos (kung meron man) at isagawa ng naayon. Nararamdaman namin na ang aming maikling panahon sa PoW at pagkukusa na palitan ang algorithm ay pahihinain ang loob ng aming ASIC Manufaturers at di nakikita ang mga isyu na maaring lumabas.

## 5.2 Ang Limang Finalists (kompetisyon sa NIST SHA-3)

Ang limang hashing algorithms na bumubuo sa NIST5 ay mga finalists mula sa NIST Hashing Competition (Chang et al. 2012). Sila ay (sa pagkakasunod ng blocks na na-hashed):

**Blake** (Aumasson 2013), **Grøstl** (Gauravaram1 et al. 2012), **JH** (Wu 2012), **Keccak** (Bertoni et al. 2012), and **Skein** (Ferguson et al. 2010).

## 5.3 Ang Bagong pamantayan sa SHA-3

Sa bandang huli, ang Keccak ay pumasa sa wakas upang mapangalanan na pinakabagong SHA-3 hashing na katungkulan, subalit ang ibang apat na algorithms (na kung saan masasabi din na cryptographically secure) ay natalo sa ilang puntos mula sa mga hurado dakil sa mga ilang maliit na technicalities. Naniniwala kami na ang kombinasyon ng bagong pamantayan ng SHA-3 kasama ang iba pang finalist na pinili ay magbibigay ng mabilis, ligtas, at matatag na hashing algorithm.

## 5.4 Magagamit na Mining Software

Sa oras ng pagsusulat nito, maraming pagpipilian ang miners:

| Pangalan | Platform | Link |
|---|---|---|
| SGMiner-5.0 | OpenCL | GitHub |
| ccminer-2.2.2 | CUDA | GitHub |
| cpuminer-opt | CPU | GitHub |

# Kabanata 6

# Mga Tampok

## 6.1 Masternodes

Ang Masternodes ay mahalaga, isang desentralisadong samahan ng mga Kompyuter na pinagsisilbihan ang network ng Bulwark. Ang masternodes ay ginagampanan ang importanteng tungkulin at tumatanggap ng parte ng pabuya ng block. Pinagsisilbihan nila ang Bulwark ecosystem sa pamamagitan ng pagpapatatag ng panustos na coin, magproseso ng transaksyon, at panatilihing ligtas ang network. Ang Masternodes ay nangangailangan ng 5000 BWK at saktong kaalaman sa teknolohiya upang gumana. Kahit anong wallet na may kontrol ng 5000 BWK ay maaring mag set-up ng masternode.

## 6.2 Obfuscation / coin-mixing

Ang Bulwark ay may tampok na Obfuscation, base sa CoinJoin ngunit may iba't ibang pagpapa-unlad mula sa orihinal, at ginagawa sa pamamagitan ng paghalo ng coin sa desentralisadong paraan gamit ang metwork ng masternodes. Ito ay magbibigay ng karagdagang seguridad sa mga transakyon. Datapwa't hindi perpektong hind Makita, Obfuscation sa pamamagitan ng paghalo ng node, mas mainam naman ito kaysa sa karaniwang pamantayan na transakyon ng bitcoin. Halimbawa, lahat ng transaksyon ng Bitcoin ay naaninag. Para sa Bulwark, ang isang karumal-dumal na aktor ay kinakailangang na makontrol ang 50% ng gumaganang masternodes upang magkaroon ng mas mababa sa 0.5% tsansa ng paglalantad ng isang transaksyon na nahalo ng walong beses ng Obfuscation Kiraly 2017b). Itong importanteng tampok ay angbibigay ng mataas na lebel ng di pagkakakilanlan sa mga gumagamit ng BWK na piliin na ilito ang kanilang transaksyon.

## 6.3 SwiftTX

Ang SwiftTX ay nagbibigay ng masternodes na may locking at pinagkasunduan awtoridad para sa transaksyon. Kapag ang transaksyon ay isinumite sa network, ang grupo ng masternode ay patutunayan ang transaksyon. Kapag ang mga masternodes ay dumating sa pagkakasundo na tunay ang transaksyon, ito ay ila-lock para sa mayamayang pagpasok nito sa blockchain, na syang higit na nakakadagdag sa bilis ng transaksyon kumpara sa conventional systems (gaya ng  Bitcoin 10 minuto na block na beses na may maraming pagkukumpirma). Ang SwiftTX ay ginagawang possible para sa maramihang transaksyon na mangyari bago ang block sa network ay i-mine sa parehong input. Ang sistemang ito ay base sa Dash's InstantSend (Kiraly 2017a).

## 6.4 Sporks

Ang bulwark network ay naghahatid ng multi-phased work mechanism na kilala sa “sporking”. Ito ay pahihintulutan ang BWK network na isakatuparan ang mga bagong tampok nito habang nililimitahan ang mga tsansa ng hindi sinasadyang network fork tuwing rollout. Ang mga pagbabago sa spork ay magagamit sa pamamagitan ng network at maaring buksan at patayin, kung kinakailangan ng indi na maghahanap ng node software upates (strophy 2017).ang tampok na ito ay sobrang nagagamit at pinapayagan ang network na mabilis na kumilos sa mga kahinaang panseguridad.

## 6.5 TOR & IPV6 Masternodes

Ang Bulwark ay pinapayagan ang mga gumagamit na patakbuhin ang kanilang buong node o masternode mula sa onion address o IPV6 na address. Kami ay nagttrabaho upang makapagdagdag ng buong TOR nodes upang palakaisn ang mismong TOR Network, at ang karanasan ng gumagamit ng Bulwark nag nagpapagana sa TOR mode lamang. Ang kakaibang tampok ng TOR masternode ay ang pagkilos ng iyong masternode bilang nakatagong TOR na serbisyo. Ang TOR nodes ay papayagan ang may mga matatag na koneksyon ng internet para mag-operate ng masternode ng labas sa kanilang home network ng walang implikasyon sa privacy ng paglalahad ng kanilang lokasyon o panganib ng paglalahad sa kanilang home network sa mga potensyal na pag-atake o makompromiso.

## 6.6 Importansya ng komunidad at sistema ng pamamahala.

Ang komunidad ng Bulwark ang pinakaimportanteng dahilan sa likod ng mahabang panahon na tagumpay ng proyekto, at ang kanilang abilidad na maimpluwensyahan ang hinaharap ng coin ay mahalaga sa lahat. Bilang tulad, sa dulong bahagi ng PoW, binabalak namin na aktibahin ang badyet para sa superblocks sa network. Ang mga superblocks na ito, na babayaran kada bwan, ay magagawang ang komunidad ay magsikap na ma-kontrol sa lahat ng aspeto ang pagunlad ng Bulwark, presensya ng pangalan, at kapakanan pang komunidad. Ang pagpapatagal sa pag aktiba ng sistema na ito ay magbibigay sa atin ng oras na paunlarin ang napapailalim na balangkas na kailangan para sa positibong karansan sa paggamit at palawakin ang pabuya ng block na meron para sa mga miners at masternodes.

Gagamitin natin ang multiphase na proseso para sa paggawa at pag-sumite ng proposal. Bawat hakbang ay dapat na makumpleto. Pag nabigong makumpleto ang mga hakbang ay magreresulta sa hindi pag-aktiba ng proposal. Ang pangunahing mga hakbang ay ang mga sumusunod:

- Magumpisa sa ating discord chat, at makipagusap sa ilan sa mga seasones users. Sukatin ang interes at kung positibo ang sagot, magpatuloy sa susunod na hakbang.
- Gamitin ang multimedia platforms para magdiskusyon at kumuha ng feedback. Alalahanin na ang Bulwark ay may malawak na userbase at iba-bang lebel ng partisipasyon ng pamamahala, ang pag abot sa bahagi ng userbase ay madalas mangangailangan ng footwork. Alalahanin ang mga diskusyon na ito at masabi sa pormal na pre-proposal. Mas madaming mabanggit, mas mabuti.
- Maging bukas sa mga suhestyon galling sa komunidad at tagapag-paunlad. Matutong mag adjust at maging maluwag sa kalooban na dalin ang mga ideya at suhestiyon galing sa labas sa iyong proposal.
- Gumawa ng pormal na pre-proposal sa Governance->Pre-Proposal section n gaming website. Magbigay ng citation mula sa mga diskusyon galling sa naunang step. Tratuhin ang iyong pre-proposal na parang ito ay ipapasa sa blockchain para iboto.
- Kapag nakumpleto na ang hakbang na ito, isusumite mo na ang iyong proposal sa blockvhain. Maging handa sa 2 bayarin, una sa oras ng pagsusumite at ang bayad sa balota na babayaran sa tagapag-paunlad na mag aaktiba ng iyong proposal sa blockchain. Ang bayad sa pagsumite ay hindi na maaring isauli at ang bayad sa balota ay babayaran lamang kapag na aprubahan na at naaktiba ang iyong proposal.
- Lahat ay libreng i-adjust ang proposal para maisama at maisoli ang naguguol na mga bayad ng dalawang ito. Siguraduhin lamang na sa iyong pormal na proposal na nakasaad na ikaw ay magdadagdag ng pagsasauli sa nagugol na salapi sa sahod na hinihiling. Siguraduhing makausap na muli ang lahat ng nakausap mo ng sa gayon ang iyong ideya ay iboboto. Para sa mga proposal na babayaran na, 10% ng mga

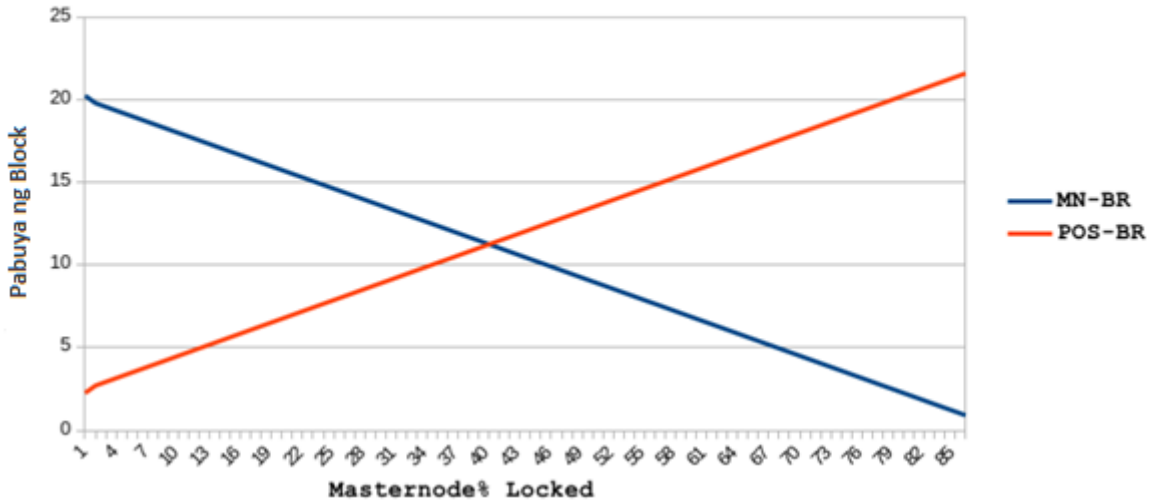
karapat dapat na masternodes ay dapat bumuto ng “yes” sa iyong proposal.ang proseso na ito na pagkuha ng 10%bilang kasunduan ay mas mahirap, kaya maging masigasig, nakapagtuturo at ma-respeto sa pagboto na kailangan upang mabayaran sa proposal. .

## 6.7 SeeSaw PoS/Pabuya sa Masternodes

Nagdesisyon kami na gamitin ang SeeSaw sistema ng pabuya na pinakilala ng PIVX PIVX (jakiman 2017). Ang SeeSaw sistema ng pabuya T ay naguumpisa sa 9:1 block reward ratio (pabor sa masternodes), at dahan dahang ma adjust ang ratio ng pabuya sa pagitan ng pagattaya at operator ng nodes hanggang sa tinatayang 41.5% ng coins na nasa sirkulasyon ay mala-locked sa masternodes, na kung saan sa oras ng pagtataya ng pabuya ay magkakaron ng bahagyang kalamangan sa masternodes base sa coin-by coin. Ang kadahilanan kung bakit mayroon kaming SeeSaw na bahagyang pinapaborang ang pabuya sa pagtataya ay dahil sa gusto naming iwasan ang problema, gaya ng makabuluhang pabago bago na presyo at mababang palit. Ayon ay tatama sa coins na may sobrang taas na porsyento ng kanilang umiikot na panustos na naka-lock sa nodes. Ang istratehiyang ito ay pagagaanin ang pag-kabigo mula sa sobrang access sa panustos ng coin at mapanatili ang kaugnayan n gating robust network. Bilang isa sa aming mga layunin na maging well-supported platforms,para sa hindi alam na komersyo, ang pagtatransaksyon ay ang pinakaimportante doon sa tumatanggap sa Bulwark at para doon sa nagtatabi nito.

**Fig 3. SeeSaw @ Height 345601 - 432000**

*(porsyento ng badyet pagkatapos)*



# Kabanata 7
# Ang Hinaharap

## 7.1 Ang Bulwark Tool Chest

Ang koleksyon ng code snippets, API's, libraries, skrip at kaalaman na magsisilbi upang himukin ang bazaar-like na kapaligiran na kung saan ang tagapag-paunlad na maaring naghahanap ng karagdagang susuporta  sa cryptocurrency na proyekto nila ay libreng makakapagpalitan ng kaalaman, impormasyon at code. Naniniwala kami na sa pagbibigay ng ganitong kagamitan ay sumasalamin sa isang karpentero sa mga kagamitan na kailangan nila upang makagawa ng kapanapanabik at dominanteng mga proyekto.

## 7.2 Pagsasapribado at Pagpapahusay sa Software

Kami ay nakatuon sa pagtanggap ng bagong plano upang mas mapaganda ang pagiging pribado ng aming userbase. Maraming mga daan ang aming inaaral sa kasalukuyan at plano na umpisahan ang aming panloob na pagsubok at pagpapaunlad nito sa unang kalahati ng taon 2018. Ang ilan sa mga pagpapaganda ay ang mga sumusunod:

- I2P privacy network.
- Zerocoin protocol o pagtugon sa Stealth (kapag kami ay tiwala sa maturity ng solusyon).
- Isabay ang aming  codebase  ng mas malapit sa bitcoin mainline.
- Pinadali/i-update ang QT Wallet.
- Pagsasama-sama ng Libtox.
- Birtuwalisasyon /containerization ng Bulwark wallet upang magkaroon ng dagdag seguridad.

## 7.3 Ligtas na Bulwark Home Node

Kami ay makikipagtulungan ng trabaho sa espesyalista ng CAD para mag-disenyo ng maliit, may sariling lagayan, bahay ng Bulwark node. Ang mga gumagamit ay maaring maikonekta ito sa kanilang home network at magkompigura gamit ang Web UI. Ang mga gusto naming paglaanan na mailunsad ay ang mga sumusunod:

- Para sa mga may matatag na koneksyon ng internet, ay madaling i-set-up na buong onionized masternode o (buong node) gamit ang TOR natatagong serbisyo.
- Opsyon na gumana bilang relay upang mapabuti ang kabuuang TOR Network.
- VPN at/o kinatawan na maaring gamitin upang mairuta ang trapiko sa home internet gamit ang TOR/I2P network.
- Pagtataya sa Bulwark sa pamamagitan ng birtwalisasyon o karagdagang serbisyo.

Sa ngalan ng desentralisasyon, In keeping with the spirit of decentralization, the 3D printable files and all source code will be available to the community for home assembly.

## 7.4 Paglaki ng aming pangalan

Magpapatuloy kami sa pagpapalawak ng aming pangalan at balak na makipagtulungan sa mga nagbebenta ng hardware, at mga nagsasama sama ng sistema na nakikiisa sa kagustuhan at mga ideya namin. Sa loob ng limang taon, gusto namin na ang 'Bulwark' ay mangahulugan hindi lamang sa cryptocurrency, kundi pribado, kaligtasan, at respeto sa kagustuhan ng mga gumagamit. Ang pangunahing layunin ng Bulwark ay magbigay ng kalayaan ng pamimili sa pamamagitan ng pagiging pribado.

## 7.5 Disenyo at Biswal

Sa pamamagitan ng pagsasaliksik at pagpapaunlad, pakay naming na gumawa ng biswal na disenyo para sa Bulwark na mamumukod-tangi mula sa kompetisyon sa pamilihan ng Crypto. Ang grupo sa pag disenyo ay nagpla-plano gumawa at mag-ekspiremento sa kasalukuyang UI/UX/Branding upang sa huli ay marating nito ang pinakamahusay na disenyo sa pamamaitan ng paghahanap ng daluyan na nagpapahintulot ng pinakamagandang karanasan ng mga gumagamit, at estetika na makabago at maganda. Ito ay magagawa sa pamamagitan ng pananaliksik sa aming mga ka-kumpitensya, panatilihing nangunguna sa kasalukuyang nauuso sa teknolohiya at pamantayan, at patuloy na makibaka upang makapag-bigay ng bago at nakakapanabik na biswal sa mga end-users.

# Kabanata 8

# Konklusyon

## 8.1 Buod

Ang Bulwark ay privacy-oriented coin na meron masternodes, pamamahala, at ang pagbabago sa ecosystem ng tools. Ang proyektong ito ay nag simula ng meron patas na paglabas at naka focus sa malawak na pamamahagi ng coin. Ang mabagal na simula, paghati ng pabuya ng block, at hashing algorithm ay sadyang pinili para makagawa ng opportunidad na may-kabuluhan sa pakikipagtulungan sa komunidad. Ang Bulwark ay inilabas ng my ibat-ibang importanteng privacy coin na nilalaman at ang development team ay masisipag para mag pakilala ng mga bagong nilalaman at magbuo pa sa mga teknolohiyang meron na. Ang Bulwark ay naglalayon na mapalakas ang pagpili sa pamamagitan ng privacy at magpokus sa napakalaking pagsisikap hanggang sa dulo.

## 8.2 Mga gawain sa hinaharap

Ang masternode privacy coin ecosystem ay kamakailan inundated ng coins na naghahanap para hikayatin ang mga bagong gagamit sa pamamagitan ng pangakong matibay na pagbalik ng puhunan, malahiganteng pagdadaanan na meron mapapaganda pang maibibigay, at ang pangkalahatang pokus sa marketing kaysa sa mismong pagpapaganda sa laman nito. Plano ng Bulwark na maging kabaliktaran: mababa sa hype ng pag gawa at mataas sa mismong pag gawa. Ang kasalukuyan at hinaharap na mga layunin para sa proyekto ay susunod sa pormula ng pagiging specific,nasusukat,nakukuha, tugma at naayon sa oras.

# Mga pinagsipian


Aumasson, L.M., Jean-Phillipe Henzen, 2013. SHA-3 proposal: BLAKE. Makikita sa: https://131002. net/blake/blake.pdf.

Bertoni, G., Daemen, J., Peeters, M. & Van Assche, G., 2012. The keccak sha-3 submission. Makikita sa: https://keccak.team/files/Keccak-submission-3.pdf.

Bitcoin Core Team, T., 2017. Bitcoin developer reference. Makikita sa: https://bitcoin.org/en/ developer-reference#block-headers.

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. Makikita sa: http://nvlpubs.nist.gov/nistpubs/ir/2012/ NIST.IR.7896.pdf.

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., et al., 2015. BlockChain technology. Makikita sa: http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.

Ferguson, N.L., Schneier, S., Whiting, B., Bellare, D., et al., 2010. The skein hash function family. Makikita sa: http://www.skein-hash.info/sites/default/files/skein1.3.pdf.

Gauravaram1, P., Knudsen, L.R., Matusiewicz, K., Mendel, F., et al., 2012. Grøstl – a sha-3 candidate. Makikita sa: http://www.groestl.info/Groestl.pdf.

jakiman, 2017. PIVX purple paper. Makikita sa: https://pivx.org/wp-content/uploads/2017/03/ PIVX-purple-paper-Technincal-Notes.pdf.

Kiraly, B., 2017a. InstantSend. Makikita sa: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/ 1146928/InstantSend.

Kiraly, B., 2017b. PrivateSend. Makikita sa: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/ 1146924/PrivateSend.

Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system. Makikita sa: https://bitcoin.org/ bitcoin.pdf.

Okupski, K., 2016. Bitcoin developer reference., pp.3–4. Makikita sa: https://lopp.net/pdf/Bitcoin_ Developer_Reference.pdf.

strophy, 2017. Understanding sporks. Makikita sa: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/128319489/Understanding+Sporks.

Wiecko, R., 2017. Dash instamine issue clari cation. Makikita sa: https://dashpay.atlassian.net/wiki/spaces/OC/pages/19759164/Dash+Instamine+Issue+Clarification.

Wu, H., 2012. The hash function jh. Makikita sa: http://www3.ntu.edu.sg/home/wuhj/research/jh/ jh_round3.pdf.