BULWARK

CRYPTOCURRENCY

Tehnička dokumentacija kriptovalute Bulwark

Bulwark *core* tim:

Eatbatterys (Koordinator projekta)

Jack (Direktor marketinga)

SerfyWerfy (*Blockchain* developer)

Frogman (Direktor komunikacija)

Patrick (Marka i dizajn)

Stu (Developer ekosistema)

Bulwark *core* tim

Prosinac 2017

Mi, Bulwark core tim, potvrđujemo da su podaci izneseni u ovom dokumentu u našem vlasništvu. Tamo gdje informacije potiču iz drugih izvora, ti izvori su navedeni.

Sažetak

Bulwark (oznaka: BWK) je valuta koja je iznikla kao posljedica generalno nepoštenih prakticiranja u *masternode* novčanim kriptosistemima. Naša odmjerena i pravedna strategija uvođenja dozvoljava svim sudionicima sudjelovanje u obećavajućem projektu od njegova samoga početka. Mi nudimo jednostavan i vrijedan prijedlog, ali bez grandioznih obećanja: mi nudimo privatni tip novca koji zadovoljava današnje i uvjete budućnosti upotrebom dosada najboljih rješenja iz DASHa i PIVXa. Ovdje nema utopijskih vizija sa gotovo nepostojećom mogućnosti ispunjavanja istih tih vizija, nego funkcionalan tip novca baziran na funkcionalnoj platformi sa aktivnom podrškom za budućnost. To ne znaci da se ne planira razvoj i inovacija – to samo znači da ćemo ispuniti svoja, realna obećanja. Različite druge kriptovalute obećavaju jako puno, a čine to bez realne mogućnosti dostizanja zadanih ciljeva – u tome mi ne želimo sudjelovati. Bez ICOa, malo količinom već izrudarenih jedinica i rudarima prilagođenim alokacijama *block* nagrada, sudionici imaju pristup kriptovaluti koja nudi *masternode* tehnologiju i najbolje moguću privatnost uparenu sa razumnim razvojnim planom. Funkcionalni *masternodovi*, koji su nosioci vizije ove kriptovalute i služe stabilizaciji i održavanju sigurnost mreže, će biti dostupni od samog početka.

Zahvala

Bulwark ne bi bio moguć bez uloženog truda timova koji su radili na Bitcoinu, Peercoinu, Blackcoiun, Talkcoinu, Dashu i PIVXu. Softver otvorenoga koda i njegovi pomagači kontinuirano rade na novim i uzbudljivim inovacijama. Kada su informacija i znanje slobodno dostupni, cjelokupno društvo je na dobitku. Mi smo zahvalni svojim prethodnicima na mogućnosti sudjelovanja u gradnji ovog rastućeg ekosistema.

Sadržaj

Poglavlje 1

Kratak uvod u kriptovalute

1.1 Osnove

Tijekom 2009 objavljen je rad Satoshi Nakamotoa pod nazivom *Bitcoin: A Peer-to-Peer Electronic Cash System* u kojem je opisana njegova vizija trgovanja. Ta vizija se zasniva na *peer-to-peer* valutnom sistemu poduprtom *hash*-baziranom *proof-of-work* tehnologijom. U tom sistemu mreža vremenski označava transakcije i „uračunava" u lanac koji se ne može promijeniti bez ponavljanja *proof-of-work* izračuna. *Masternodovi* mreže biraju najduži lanac kao referentni odnosno kao valjani dokaz slijeda događanja. Dokle je 51% računalne snage mreže kontrolirano *masternodovima* koja nemaju namjeru izvesti zločudne promjene, lanac koji oni generiraju je najduži i time referentan lanac (Nakamoto 2009).

1.2 Definicija *blocka*

Svaki *block* na mreži predvođen je zaglavljem od 80 *byteova* koji sadrži dvostruku SHA256 izračunatu kopiju zaglavlja prethodnog *blocka*, *root merkle* (dvostruka SHA256 izračunata derivacija svih izračuna koji su se pojavili u *blocku*), vremensku oznaku početka *proof-of-work*, nivo teškoće od kojeg zaglavlje ovoga izračuna mora biti manja od ili njemu jednaka, i trenutak u kojem su rudari dostigli ciljanu težinu. Svaki pokušaj manipulacije bilo koje transakcije u bilo kojem *blocku* rezultirat će odbijanjem *blocka* od strane mreže rudara (Bitcoin Core Team 2017).

1.3 Definicija *blockchaina*

Grupe transakcije se formiraju u *blockove* koji se stavljaju kronološki u lanac tvoreći time *blockchain*. *Blockchain* sadrži sve vremenski poredane aktivnosti u mreži i služi kao konsenzusni model kojim se u bilo koje vrijeme može provjeriti bilo koja transakcija (Crosby et al. 2015).

1.4 *Proof-Of-Work*

Proof-of-work (skraćeno: PoW) je sistem provjere u kojem rudari moraju uložiti određena sredstva (struja, troškovi računalnog hardvera) da bi riješili proizvoljne probalističke slagalice riječi. Jedini način da se u *blockchain* ugradi neispravna transakcija, je da se ponovi kompletan *proof-of-work* od početka do današnjeg dana (Okupski 2016).

Poglavlje 2

Uvod u Bulwark

2.1 Čvrsti temelji

Svaki dom treba solidne temelj – Bulwark u tom smislu nije drugačiji. Bulwark je izgrađen na bazi PIVXa, koji je pak izgrađen na temelju DASH kriptovalute. Unatoč povezanosti različitih valuta sa originalnom Satoshi jezgrom, svaki projekt se kreće svojim putem sa ciljevima i idealima koji predstavljaju zajednicu kojoj služe. Mi ćemo proširiti odnosno staviti naglasak na osobine vezane uz privatnost kriptovalute i to kontinuiranim istraživačkim radom praćen stvaranjem alata i mogućnosti za integraciju Bulwark-a u moderne tehnološke platforme.

2.2 Tim privržen zajednici

Za neke projekte zajednice nemaju veliku važnost. Bulwarkov prioritet broj jedan je zajednica. Sa natječajima, donacijama, funkcionalnom platformom za diskusije i nikakvom tolerancijom prema maltretiranju (novih) članova, Bulwark teži biti kriptovaluta za sve vrste ljudi. Naši članovi već pridonose zajednici pišući skripte i različita uputstva kako bi se poboljšalo korisničko iskustvo.

2.3 Pošten i uravnotežen

U trenutku pisanja ovog dokumenta, povećava se broj kriptovaluta građenih na sličnim temeljima. Iako je njihova tehnologija relativno dobro građena, često se temeljno analizom njihovih specifikacija i *blockchain* parametara otkrivaju ne tako razumna odnosno poštena prakticiranja.

2.4 Problemi vezani uz *pre-mine*

2.4.1 Primjer: FooBarBazCoin

Povećava se broj kriptovaluta koje izabiru proizvoljan datum daleko u budućnosti i na osnovu toga datuma odnosno proračunatoj ukupnoj količini valute u tom trenutku definiraju *pre-mine* postotak. Uzmimo za primjer fiktivni FBC (FooBarBaz valuta), baziran na DASHu.

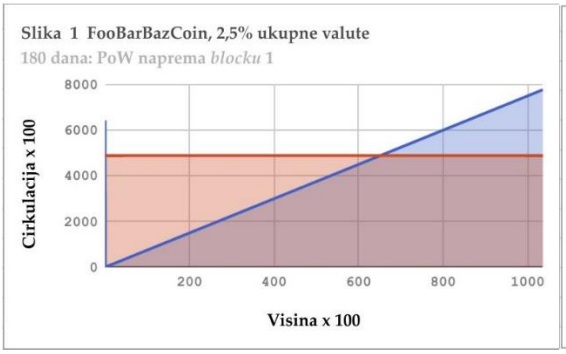
- Nagrada *blocka*: 15
- Vrijeme *blocka*: 2,5 minuta
- POW/*Masternode* podjela: 50/50%
- Početni težinski algoritam: KGW
- Subvencija se smanjuje svake godine za 12%
- Maksimalna količina valute: ~25 milijuna
- 2.5% *pre-mine*

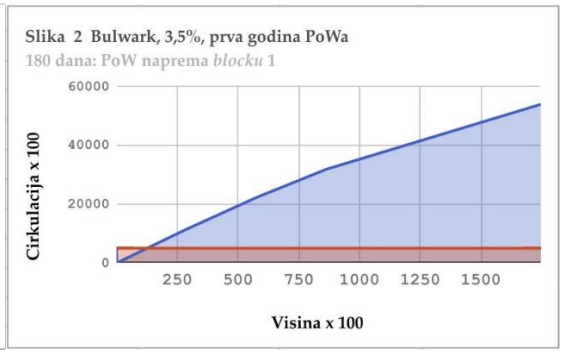
U ovom primjeru, spomenutih 2.5% *pre-minea* znači otprilike 643.000 jedinica valute (od ukupnih 25 milijuna), što se na prvi pogled čini razumnim. Da bi se PoW i *masternode* primanjima dosegla količine valute u rukama razvojnog tima, treba se doseći otprilike *block* 43.000. S obzirom na vrijeme *blocka* od 2,5 minute, rudarima bi trebalo oko 150 dana (odnosno 75 dana uključujući sve opcije) da se generira ista količina valute. Čak i nakon 75 dana, razvojni tim bi posjedovao više od 50% jedinica valute.

2.5 Razumna alternativa

Bulwarkov tim je prepoznao probleme iz primjera u prethodnoj sekciji i odlučio staviti karte na stol: naš *pre-mine* od 489,720 (3,5 %) odgovara 12 dana PoW rudarenja ili nešto više od 10 dana sveukupne generacije. Nadamo se da to će to povećati osjećaj sigurnosti u zajednici, jer nakon određene točke vrijednost cijelog tržišta više ne može biti ozbiljno umanjeno kao posljedica jedinica valute u posjedu Bulwarkovog tima. Kao što se vidi iz dolje priloženih grafika, od kojih oboje predstavljaju vremenski period od 180 dana, razlika je više nego jasna. Nadamo se da je ovim, otvorenim pristupom temi postavljen zdrav temelj koji će služiti zajednici u cjelini.

2.5.1 Usporedba dvaju pristupa





2.5.2 *Instamine* – naš pristup temi

Dash (Darkcoin) predstavlja interesantan slučaj kada se radi o potrebi zaštite od *instaminea*. Naime, 10-15% ukupne količine Dash jedinica je generirano unutar prvih nekoliko dana postojanja valute od strane pojedinih korisnika (Wiecko 2017). Naš pristup *instamineu* je dvostruki: mala subvencija po kojoj je prvih 960 *blockova* (1 dan) linearno povećavano do pune nagrade po *blocku* uz 100% isporuka nagrade po *blocku* rudarima na taj dan. Povijesno gledano, te situacije su dosada rješavane sa niskom nagradom *blocka* na početku i prebacivanje na punu nagradu *blocka* u danom trenutku, no to je često dovodilo do DDoS napada na *poolove* ili do nestabilnosti *poolova* izazvanom naglim priljevom novih rudara. Kada se nagrada linearno podiže, nema smisla pokušavati ometati rad rudara ili *poolova* sa ciljem ostvarivanja prednosti odnosno financijske dobiti.

2.5.3 ICO? Bolje IC-NO!

Činjenica je da smo u trenutku pisanja ovog dokumenta redovito izloženi ICOima. Unatoč njihovoj očitoj ulozi u ekosistemu kriptovaluta, oni često služe stvaranju koncentriranih točaka bogatstva. S obzirom da Bulwark nudi i *masternode* i, kasnije, *proof-of-stake* nagrade, ta koncentracija bogatstva bi mogla imati veliki utjecaj na tržište i ozbiljno usmjeriti kontrolu cijelog ekosistema u korist najranijih (i time najbogatijih) posjednika Bulwarka. Iako su koncentracije bogatstva neizbježne u potpunosti, mi vjerujemo da smo ovim pristupom ostvarili bolje uravnotežen sustav. Kako bi broj točaka bogatstva bio što manji, uveli smo skalirani sistem nagrada *blocka* te poštenu mehaniku dodjeljivanja nagrada sa ciljem prihvaćanja valute od široke publike.

2.6 Brz i funkcionalan

Sa vremenom blocka od 90 sekundi, *masternode* konsenzusnim sistemom poduprtim tehnologijom zamrzavanja transakcija, razumnim planom emisija i sa ekološki svjesnim *stakingom*, Bulwark teži biti vrlo brza odnosno funkcionalna kriptovaluta.

Poglavlje 3

Parametri našeg *blockchaina*

3.1 Pregled specifikacija Bulwarka

Tablica 3.1: Pregled specifikacija Bulwarka

Specifikacija	Vrijednost
Skraćenica	BWK
Algoritam	NIST5
RPC port	52541
P2P port	52543
Razmak *blockova*	90 sekundi
Težinski algoritam	Dark Gravity Wave v3.0
Veličina *blocka*	1MB
Sazrivanje kod rudarenja	67 *blockova* (~100 minuta)
Potvrda	6 *blockova* (~9 minuta)
Jedinica u opticaju (1 godina)	14.505.720 BWK
Jedinica u opticaju (5 godina)	27.668.220 BWK
PoW razdoblje	*nHeight* ≤ 345.600
PoS razdoblje	*nHeight* ≥ 345.601
Podržani protokoli	IPV4, IPV6, TOR
PoS	Blackcoin v3.0 PoS, PIVX SeeSaw nagrade

3.2 Umjeren početak

Naš razuman početak je vidljiv u slijedećim linijama koda (izvorno iz ZCasha):

```
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 je u upotrebi od samog početka kao metoda određivanja PoW težine. Ona koristi jednostavnu matematičku funkciju pomičnog prosjeka, koja može brzo reagirati na velike promjene u računalnoj snazi mreže. Taj pristup rješava tzv. „efekt zaglavljenog *blocka*“, koji je često uzrokovan od strane *multipoolova*, te sprječava pojedince da naglim povećanjem računalne snage u vrlo kratko vrijeme riješe više od nekoliko *blockova*.

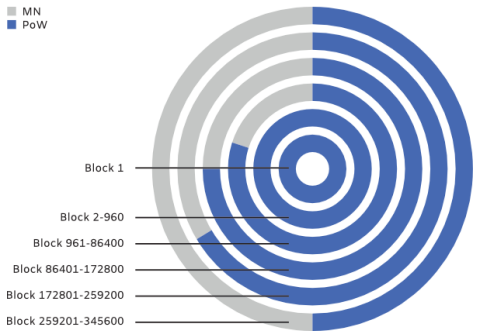
Poglavlje 4

Nagrade *blocka*

4.1 PoW nagrade *blocka*

Tablica: Specifikacije nagrade PoW blocka po periodima

Subvencija	*Block*	PoW	MN	Jed. u opticaju
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



Slika 4.1: Nagrada PoW *blocka* po periodima

4.2 PoS nagrade *blocka*

Tablica 4.2: Specifikacije nagrade PoS blocka po periodima

Subvencija	*Block*	Budžet	PoS/*Masternode*	Period / godina
25.000	345601-432000	10%	SeeSaw	2.
21.875	432001-518400	10%	SeeSaw	2.
18.750	518401-604800	10%	SeeSaw	2.
15.625	604801-691200	10%	SeeSaw	2.
10.250	691201-777600	10%	SeeSaw	3.
10.938	777601-864000	10%	SeeSaw	3.
9.3750	864001-950400	10%	SeeSaw	3.
7.8120	950401-1036800	10%	SeeSaw	3.
6.2500	1036801-1123200	10%	SeeSaw	4.
5.4690	1123201-1209600	10%	SeeSaw	4.
4.6880	1209601-1296000	10%	SeeSaw	4.
3.9060	1296000-1382400	10%	SeeSaw	4.
3.1250	1382401-1468800	10%	SeeSaw	5.
2.7340	1468801-1555200	10%	SeeSaw	5.
2.3440	1555201-1641600	10%	SeeSaw	5.
1.9530	1641601-1728000	10%	SeeSaw	5.
1.6250	1728000+	10%	SeeSaw	Beskonačno

Poglavlje 5

NIST5 *hashing*

5.1 Zašto NIST5

NIST5 *hash* algoritam je upotrebi od svojeg uvođenja od strane TalkCoina u 2014. NIST5 algoritam se može koristiti na mnogim popularnim procesorima, kao i na AMD i NVidia grafičkim karticama. NIST5 nije zaštićen od upotrebe ASICsa kao neki drugi za memorijom gladni algoritmi – mi smatramo da je stabilnost i veća energetska učinkovit u usporedbi sa drugi algoritmima važnija. U slučaju da se razviju ASIC uređaji koji podržavaju NIST5 algoritam prije završetka PoW faze, mi smo spremni zamijeniti NIST5 algoritam nekim drugim - cijela zajednica će moći sudjelovati u odluci koji algoritam će biti korišten. Mi vjerujemo da naša kratka PoW faza i spremnost na promjenu algoritma djeluje odvraćajuće na proizvođače ASIC uređaja i u skladu s time ne očekujemo probleme u tome smislu.

5.2 Pet finalista NIST SHA-3 natječaja

Pet *hashing* algoritma koji čine NIST5 su finalisti NIST *hashing* natječaja (Chang et al. 2012). Ti algoritmi su (po redu izračunavanja *blockova*):

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

5.3 Novi SHA-3 standard

Keccak je algoritam, koji je prošao zadnji krug testova i dobio naziv nove SHA-3 *hashing* funkcije, dok su ostala četiri algoritma (unatoč tome što se smatraju kriptografski gledano sigurnim) izgubila manji broj bodova na sporednim svojstvima. Mi smatramo da je kombinacija novog SHA-3 standarda sa drugim finalistima natječaja odabir koji u cijelosti osigurava brz, siguran i pouzdan *hashing* algoritam.

5.4 Dostupni programi za rudarenje

U trenutku pisanja ovog dokumenta, postoji nekoliko opcija za rudare:

Ime	Platforma	Link
SGMiner-5.0	OpenCL	GitHub
ccminer-2.2.2	CUDA	GitHub
cpuminer-opt	CPU	GitHub

Poglavlje 6

Tehnološka svojstva

6.1 *Masternodeovi*

Masternodovi, pojednostavljeno rečeno, su decentralizirana mreža računala koja služe Bulwark mreži. *Masternodovi* izvode važne mrežne funkcije i primaju dio nagrada *blocka*. Oni služe Bulwarkovom ekosistemu osiguravajući dovoljan broj jedinica valute u opticaju, procesiranjem transakcija i generalno održavaju mrežu sigurnom. Rukovanje *masternodovima* zahtjeva 5000 BWK i umjereno tehničko znanje. Svaki *wallet* sa 5000 BWK može (ali ne mora) preuzeti ulogu *masternoda*.

6.2 Anonimiziranje / miješanje jedinica valute

Bulwark omogućuje upotrebu anonimiziranja, baziranu na višestruko unaprijeđenoj CoinJoin tehnologiji, te provođenu putem miješanja jedinica na decentralizirani način od strane mreže *masternodova*. To uvodi dodatni nivo privatnosti transakcija. Unatoč tome sto se time ne dobiva stopostotna anonimnost, anonimiziranje putem *masternodova* je puno bolje rješenje nego ono u standardnim bitcoin transakcijama, gdje su sve transakcije transparentne. U Bulwarkovoj mreži je potrebno posjedovati preko 50% svih *masternodova* da bi se postigla mogućnost manja od 0.5% da se deanominizira jedna transakcija koja je bila anonimizirana osmostrukim miješanjem (Kiraly 2017b). Ova važna funkcija osigurava visoki nivo anonimnosti za one korisnike Bulwarka, koji se ju odluče koristiti pri provođenju transakcija.

6.3 SwiftTX

SwiftTX tehnologija omogućuje *masternodovima* zaključavanje i konsenzusni autoritet nad transakcijama. Kada se nova transakcija prijavi mreži, grupa *masternodova* će provjeriti tu transakciju. Ako ti *masternodovi* uspiju postići koncensus o valjanosti te transakcije, transakcija će biti zaključana i time pripremljena za uvođenje u *blockchain*, što ubrzava brzinu transakcija

višestruko u usporedbi sa konvencionalnim sistemima, kao što je Bitcoinovo 10-minutno vrijeme *blocka* sa višestrukim potvrdama transakcije. Uz to, SwiftTX omogućava provođenje više transakcija i to prije nego što je *block* mreže sa tim istim ulaznim jedinicama izrudaren. Ovaj sistem se bazira na Dashovom InstantSend sistemu (Kiraly 2017a).

6.4 *Sporks*

Bulwarkova mreža koristi multifazni *fork* mehanizam poznat pod imenom „sporking". To omogućuje uvođenje novih tehnologija u BWK mrežu uz smanjeni rizik od nenamjernog dijeljenja lanca. *Spork* promjene se mogu primijeniti putem mreže i mogu se aktivirati te deaktivirati po potrebi bez softverskih ažuriranja (Strophy 2017). Ova mogućnost je vrlo važna, jer, između ostaloga, omogućuje brzu reakciju na sigurnosne prijetnje.

6.5 TOR & IPV6 *masternodovi*

Bulwark omogućuje korisniku da pusti u rad puni *node* odnosno *masternode* sa *onion* adrese odnosno sa IPV6 adrese. Radili smo na dodavanju punog TOR *nodea* kako bi ojačali TOR mrežu sa jedne i korisničko iskustva korisnika Bulwarka sa druge strane. Unikatna mogućnost TOR *masternoda* je mogućnost konfiguracije *masternoda* kao skrivenog TOR servisa. TOR *nodovi* dozvoljavaju kućnim korisnicama sa stabilnim Internet vezama korištenje *masternodova* bez straha za njihovu privatnost odnosno rizika od potencijalnog napada na njih.

6.6 Važnost zajednice i sistem upravljanja

Za dugoročni uspjeh projekta je Bulwarkova zajednica, i posebno njena mogućnost razumnog utjecaja na razvoj Bulwark valute, najvažniji faktor. S time na umu, na kraju PoW faze planiramo aktivirati proračunske *superblockove* u mreži. Ti *superblockovi*, koji će se isplaćivati mjesečno, će omogućiti zajednici da kontrolira sve aspekte Bulwarkovog razvoja, uključujući razvoj marke i poslove vezane uz samu zajednicu. Odgađanjem aktivacije ovog sistema nam pruža dovoljno vremena da razvijemo dobru korisničku platformu i, istovremeno, da povećamo nagrade *blocka* za rudare i *masternodove*.

Koristit ćemo multifazni proces za stvaranje i podnašanje prijedloga. Svaki korak će se morati potpuno ispuniti – u slučaju da se dolje navedeni koraci ne poštuju, najvjerojatniji je ishod odbijanje prijedloga. Kratki pregled koraka je:

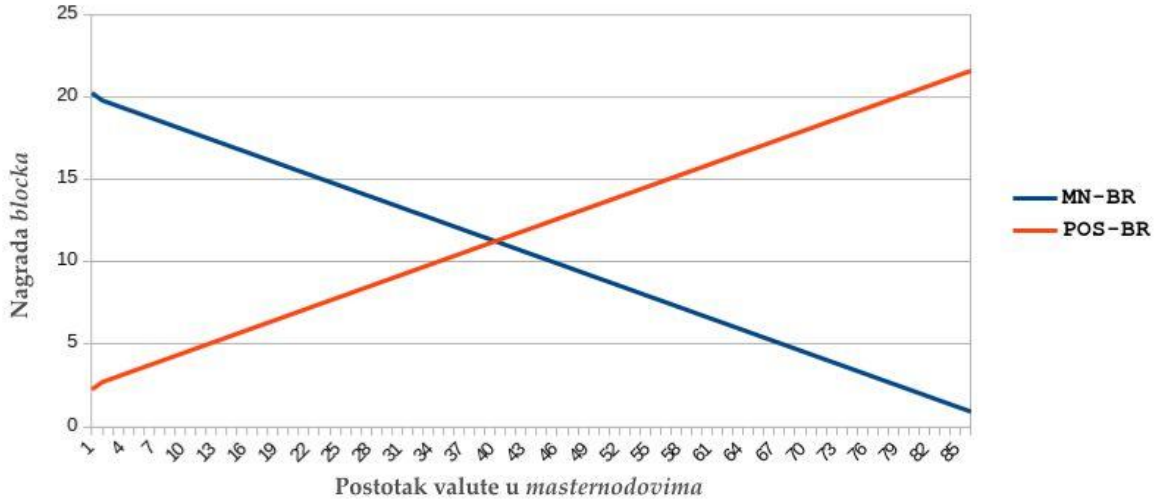
- U Discord *chatu*, razgovaraj sa iskusnim korisnicima. Odmjeri interes tih korisnika za ideju i ako je reakcija pozitivna, prijeđi na slijedeći korak.
- Prezentiraju ideju i diskutiraju ju na drugim socijalnim platformama. Pošto su različiti relevantni dijelovi zajednice Bulwarka prisutni na različitim platformama, trebat će uložiti trud kako bi se dobila reprezentativni reakcija zajednice. Zabilježi reakcije zajednice i priloži ih prijedlogu.
- Budi otvoren prema prijedlozima zajednice i spreman na integraciju drugih ideja i prijedloga u tvoj prijedlog.
- Generiraj formalni predprijedlog na sekciji *Governance -> Pre-Proposal* naše web stranice. Priloži sakupljene citate svih diskusija sakupljenih u prethodnim koracima. Pripremi tvoj predprijedlog pod pretpostavkom da će on kao takav biti poslan na glasanje od strane *blockchaina*.
- Po završetku prethodnih koraka, prijedlog će se trebat podnijeti u *blockchain*. Budi spreman na dvije pristojbe, jednu u trenutku podlaganja prijedloga i drugu, glasačku pristojbu za developera koji će aktivirati tvoj prijedlog u *blockchainu*. Prva pristojba je bespovratna, a druga, glasačka, se samo plaća ako je prijedlog prihvaćen te aktiviran.
- Svatko smije prilagoditi svoj prijedlog tako da se u njemu kompenziraju troškovi navedene dvije pristojbe. U tom slučaju, to se mora spomenuti u prijedlogu.
- Kontaktiraj sve one s kojima si razgovarao o prijedlogu, kako bi te osobe dale svoj glas. Da bi prijedlog bio prihvaćen, 10% registriranih *masternodova* more glasiti „za“ tvoj prijedlog. Sakupljanje 10% glasova je mnogo teže, nego sto se na prvi pogled čini, pa se preporuča da se ostane dosljedan, informativan te uljudan prilikom sakupljanja glasova potrebnih za uspjeh tvog prijedloga.

6.7 Nagrade SeeSaw PoS/*masternodova*

Mi smo odlučili koristiti SeeSaw sistem nagrada, koji je postao popularan uvođenjem PIVXa (Jakiman 2017). SeeSaw nagradni sistem počinje sa omjerom nagradnog *blocka* od 9:1 (u korist *masternodova*) i postepeno prilagođava omjer nagrada između *staking* i *node* operatera dok se otprilike 41.5% jedinica valute ne nalazi zaključano u *masternodovima*. U tom trenutku *staking* nagrade su neznatno veće od *masternode* nagrada gledano po jednoj jedinici valute. Razlog tome leži u našoj želji da se spriječe velike fluktuacije cijene i niska likvidnost, koja se pojavljuje u valutama koje imaju većinu jedinica zaključano u *nodovima*. Ova strategija sprječava probleme pri kupovini valute i čini mrežu robusnijom. S obzirom na naš cilj da se uspostavi dobro podržana i stabilna platforma za anonimno trgovanje, dovoljna količina valute je iznimno važna onima koji koriste i onima koji posjeduju Bulwark.

Slika 3 SeeSaw na visini *blocka* 345601 - 432000

(nakon postotnog proračuna)



Poglavlje 7

Budućnost

7.1 Bulwark kolekcija alata

Planira se ostvarivanje kolekcije dijelova programskog koda, APIja, biblioteka, skripata i generalno informacija, koja će imati tržišni karakter, a gdje bi developerima bilo omogućeno preuzimanje odnosno razmjena znanja, informacija i dijelova programskog koda. Mi smatramo da omogućavanje pristupa developerima takvim alatima je jednako važno kao davanje potrebnih alata, na primjer, stolaru, kako bi on mogao izraditi, na primjer, namještaj.

7.2 Privatnost i razvoj softvera

Mi kontinuirano radimo na novim protokolima, koji unapređuju privatnost korisnika Bulwarka. Trenutno razmatramo nekoliko različitih mogućnosti i planiramo početi sa internim testiranjem u prvoj polovici 2018. Između ostaloga, slijedeća poboljšanja se razmatraju:

- I2P privatna mreža
- Zerocoin protokol ili Stealth adresiranje (nakon što se uvjerimo u zrelost tih tehnologija)
- Usklađivanje našeg osnovnog koda sa onim od bitcoina
- Optimizacija / unaprjeđenje QT *walleta*
- Litbox integracija
- Virtualizacija / kompartmentalizacija Bullwark *walleta* sa ciljem povećanja sigurnosti

7.3 Bulwarkov sigurni osobni *node*

U suradnji sa CAD-specijalistima dizajnirat ćemo osobni, mali i neovisan Bulwarkov *node*. Korisnici će se time moći spojiti na svoje osobne mreže i konfigurirati ga putem web sučelja. Slijedeće funkcije planiramo ugraditi:

- Za one sa stabilnim Internet vezama, mogućnost jednostavnog stavljanja u pogon *masternoda* u potpunom *onion* modu rada korištenjem TOR skrivenih servisa.
- Mogućnost rada u *relay* modu sa ciljem poboljšavanja TOR mreže.
- VPN i/ili *proxy* koji se može koristiti za provođenje osobnog prometa kroz TOR/I2P mrežu.
- Bulwark *staking* putem virtualizacije ili putem dodatnog uređaja.

U smislu decentralizacije, za ispisivanje spremne 3D datoteke i kompletan izvorni kod će biti dostupni zajednici, kako bi se omogućila gradnja i u kućnoj radinosti.

7.4 Razvoj marke Bulwark

Nastavljamo rad na razvoju naše marke i planiramo surađivati sa proizvođačima i trgovcima integriranih hardver sistema, koji sa nama dijele istu strast i ideale. Cilj je unutar pet godina pozicionirati ime "Bulwark" ne samo kao kriptovalutu, nego i kao sinonim za privatnost, sigurnost i poštivanje slobode korisnika. Bulwarkova osnovna svrha je da kroz privatnost pruži slobodu izbora.

7.5 Dizajn i vizualni aspekti

Naš je cilj dizajnerski, vizualno te kvalitativno odvojiti Bulwark od konkurenata na kriptotržištu. Naš dizajnerski tim stremi prema ultimativnom dizajnu koji uključuje najbolje moguće korisničko iskustvo te inovativnu estetiku. Uz kontinuirano praćenje kako trendova i tehnologije, tako i konkurencije, kontinuirano radimo na uvođenju novih i uzbudljivih vizualnih rješenja za korisnike Bulwarka.

Poglavlje 8

Zaključak

8.1 Sažetak

Bulwark je privatnošću orijentirana i zajednicom upravljana valuta sa *masternodovima* i evolvirajućim ekosistemom alata. Projekt je započet na razuman i pravedan način, sa fokusom na široku distribuciju jedinica valute. Polagan početak, podjela nagrade *blocka* i *hashing* algoritam su tako odabrani da vrlo širok krug osoba može sudjelovati u Bulwarkovom ekosistemu. Bulwark se kao valuta od samog početka odlikovao implementacijom različitih tehnologija i principa vezanih za privatnost, čije je usavršavanje i dalje jedna od najvažnijih točaka razvojnog plana Bulwarkovog tima.

8.2 Budućnost

Ekosistem građen oko *masternode* valuta sa naglaskom na privatnost poplavljen je novim valutama koje privlače nove korisnike obećavajući velik povrat uloženih sredstava, razrađene planove pune neispunjivim stavkama i koje se često više bave marketingom nego unapređivanjem ekosistema. Bulwark radi upravo obrnuto: relativno malo primjerenog marketinga, ali zato uporan rad na stvaranju novoga. Sadašnji i svi budući ciljevi projekta će pratiti SMART princip (SMART = *specific, measurable, attainable, relevant* i *time bound*).

Popis literature

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

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

Bitcoin Core Team, T., 2017. Bitcoin developer reference. Dostupan na: 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. Dostupan na: http://nvlpubs.nist.gov/nistpubs/ir/2012/ NIST.IR.7896.pdf.

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., et al., 2015. BlockChain technology. Dostupan na: 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. Dostupan na: 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. Dostupan na: http://www.groestl.info/Groestl.pdf.

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

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

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

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

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

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

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

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