BULWARK

CRYPTOCURRENCY

Cryptocurrency Whitepaper

Bulwark Core Team:

Eatbatterys (Projektkoordination)

Jack (Marketingdirektor)

SerfyWerfy (Blockchain-Entwickler)

Frogman (Kommunikationsleitung)

Patrick (Branding und Design)

Stu (Ökosystem-Entwickler)

Das Bulwark Core-Team

Dezember 2017

Das Bulwark-Team bestätigt hiermit, dass alle in diesem Dokument enthaltenen Informationen von ihm erstellt wurden. Wo Informationen aus anderen Quellen hergeleitet wurden, werden diese Quellen explizit angegeben.

Kurzfassung / Abstract

Bulwark (Ticker: BWK) ist eine an den Bedürfnissen der Community orientierte Kryptowährung, die als Antwort auf die unfairen Praktiken in der Welt der datenschutzorientierten Masternode-Kryptowährungen entwickelt wurde. Unsere wohlüberlegte, faire Markteintrittsstrategie bietet allen Teilnehmerinnen und Teilnehmern die Möglichkeit, an diesem vielversprechenden Projekt von Anfang an teilzuhaben. Wir bieten ein simples Wertversprechen ohne unrealistische Vorankündigungen: Wir erzeugen eine auf Datenschutz ausgelegte Kryptowährung, die heute und in Zukunft funktioniert und auf bewährten Methoden von DASH und PIVX setzt. Statt vollmundigen Versprechen ohne Chance auf Umsetzung bieten wir eine funktionstüchtige Währung mit einer zukunftssicheren Plattform. Jedoch legen wir großen Wert auf Innovation – allerdings setzen wir dabei auf Resultate, nicht auf Hype. Es gibt schon zu viele Währungen, die nur durch Hype befeuert werden und frei von Substanz sind, und wir wollen uns dieser Gruppe, die auf leere Versprechungen setzt, nicht anschließen. Bulwark hat keine ICO, dafür aber eine Soft-Launch-Belohnungsrampe, geringes Pre-Mining und Miner-freundliche Block-belohnungen. Damit bieten wir unseren Anwenderinnen und Anwendern direkten Zugang zu einer durch und durch auf Datenschutz ausgelegten Kryptowährung mit Masternodes, der besten verfügbaren Technologie und einem sinnvollen Entwicklungsplan. Masternodes sind von Anfang an verfügbar und ein fundamentaler Teil von Bulwarks Vision. Sie werden die Zirkulation stabilisieren, das Netzwerk sichern und Funktionalität bereitstellen.

Danksagung

Bulwark wäre ohne die Arbeit der Teams von Bitcoin, Peercoin, Blackcoin, Talkcoin, DASH und PIVX nicht möglich gewesen. Open Source-Software und die Menschen, die dazu beitragen, ebnen ständig den Weg in Richtung neuer und spannender Innovationen. Wenn Information und Wissen frei verfügbar sind, dann profitiert jeder davon. Wir sind unseren Vorgängern für die Möglichkeit, zu diesem wachsenden Ökosystem beizutragen, dankbar.

Inhaltsverzeichnis

Kapitel 1

Einführung in Kryptowährungen

1.1 Vorgeschichte

2009 veröffentlichte Satoshi Nakamoto das Paper *Bitcoin: A Peer-to-Peer Electronic Cash System*, in dem er seine Vision von Finanztransaktionen in der Zukunft darstellte. Nakamoto beschrieb Peer-to-Peer-Währungssysteme auf Basis eines hashbasierenden Proof of Work. Das Netzwerk versieht jede Transaktion mit einem Zeitstempel, indem es sie über eine Hash-Funktion an ein fortlaufendes Wirtschaftsbuch anhängt, welches nachträglich nicht mehr verändert werden kann, es sei denn, man führt den gesamten Proof of Work nochmal durch. Netzwerkknoten folgen dabei der längsten Kette, die vom Pool mit der größten Hashing-Leistung als korrekt betrachtet wird. Solange mehr als 51% der Knoten im Netzwerk keinen Angriff gegen das System planen, werden sie dabei die längste Kette generieren (Nakamoto 2009).

1.2 Der Block

Jeder Block im Netzwerk beginnt mit einem 80 Byte großen Header. Dieser enthält eine Double SHA256-gehashte Kopie vom letzten Blockheader, einen Hash-Baum („Merkle root", ein Double SHA256-Hash einer Ableitung von allen Hashes in diesem Block), den Zeitstempel zu Beginn des Proof of Work, die für diesen Block notwendige Schwierigkeit der Berechnung und ein Nonce - eine Zahlen- oder Buchstabenkombination, die nur ein einziges Mal in diesem Kontext verwendet wird und für das Mining notwendig ist. Durch diese Absicherung wird sichergestellt, dass jeder manipulierte Block durch die Miner des Netzwerks abgelehnt wird (Bitcoin Core Team 2017).

1.3 Die Blockchain

Einzelne Transaktionen werden zu Blöcken zusammengefasst, welche in chronologischer Reihenfolge an eine Kette angehängt werden – so bildet sich die Blockchain. Sie bildet die Geschichte aller Aktivitäten im Netzwerk ab und dient als verteiltes Konsensmodell, durch das jede Transaktion jederzeit verifiziert werden kann (Crosby et al. 2015).

1.4 Arbeitsbeweis („Proof-Of-Work")

Der Proof of Work ist ein Verifizierungsystem. Miner müssen hierbei Ressourcen wie Strom oder Hardware einsetzen, um ein willkürliches, probablilistisches *Worträtsel* zu lösen. Um die Blockchain mit einer unzulässigen Transaktion zu stören, müsste ein Angreifer also alle Proofs of Work bis zum jetzigen Zeitpunkt wiederholen. (Okupski 2016).

Kapitel 2

Bulwark

2.1 Ein solides Fundament

Jedes Haus braucht ein solides Fundament, und bei Bulwark ist es nicht anders. Bulwark basiert auf *PIVX*, welches sich wiederum von der bekannten Kryptowährung *DASH* ableitet. Auch wenn man alle Kryptowährungen bis zum ursprünglichen Satoshi Core zurückverfolgen kann, hat doch jedes Projekt eine spezielle Richtung eingeschlagen, mit eigenen Zielen und Idealen, die die Wünsche der jeweiligen Communities repräsentieren. Wir legen Wert auf den Datenschutz-Ansatz unserer Vorgänger und bauen diesen mit neueren Methoden aus, um die Werkzeuge und Möglichkeiten zu schaffen, die Bulwarks Integration in moderne Technologieplattformen ermöglichen.

2.2 Ein engagiertes, der Community verpflichtetes Team

In manchen Projekten ist die Community nur ein Nebengedanke. Für Bulwark ist sie das zentralste Anliegen. Wir wollen die Kryptowährung für jeden Menschen werden. Wir haben Wettbewerbe und eine lebhafte Diskussionskultur und gehen strikt gegen jede Form von Belästigung gegenüber neuen Mitgliedern vor. Unsere Community erzeugt jetzt schon nützliche Skripte und Ratgeber, die zu einer besseren Benutzererfahrung beitragen.

2.3 Fair und ausgeglichen

Derzeit gibt es einen starken Zustrom an Kryptowährungen, die auf ähnlichen Grundlagen aufbauen. Während es an den zugrundeliegenden Technologien nichts auszusetzen gibt, entdeckt man bei einem genaueren Blick auf die verwendeten Spezifikationen und Parameter oftmals unfaire Praktiken.

2.4 Das Pre-Mining-Problem

2.4.1 FooBarBazCoin: Eine Fallstudie

Momentan beschließen viele Kryptowährungen ein beliebiges Datum in der Zukunft, und definieren ihr Pre-Mining über die dann zirkulierende Menge. Sehen wir uns dazu den FBC (*FooBarBaz Coin*) an, einen fiktiven Fork von *DASH*.

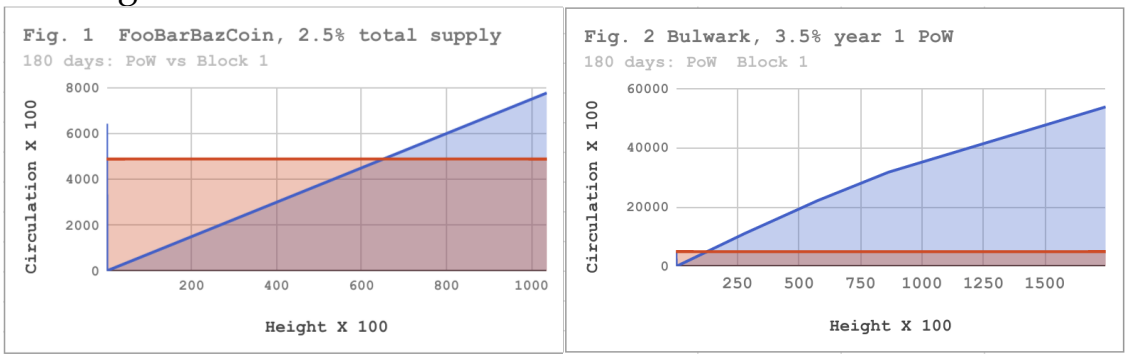
- Block-Belohnung („Block reward”): 15
- Block-Zeit („Block time”) : 2,5 Minuten
- Proof of Work /Masternode - Aufteilung: 50/50%
- Algorithmus der anfänglichen Schwierigkeit: KGW
- Subvention („Subsidy”) sinkt um 12% pro Jahr
- Maximale Menge („Supply”): ~25 Million
- 2,5% Pre-Mining

Die in diesem Beispiel angegebenen 2,5% Pre-Mining stellen ~643.000 der maximal 25 Millionen FBC dar, was auf den ersten Blick vernünftig wirkt. Allerdings würde es etwa 43.000 Blöcke lang dauern, bis Miner durch Proof of Work und Masternodes die gleiche Menge an Coins erstellen können, bei einer Block-Zeit von 2,5 Minuten wären das etwa 75 Tage – sprich, nach diesen 75 Tagen würden die Entwickler immer noch die Hälfte aller existierenden FooBarBazCoins kontrollieren.

2.5 Eine gerechtere Alternative

Das Bulwark-Team erkannte dieses Problem, und entschied sich dafür, offen an die Sache heranzugehen. Unser Pre-Mining von 489.720 Bulwark (3,5%) stellt nur etwas über 12 Tage PoW-Mining dar, oder knapp 10 Tage der gesamten Produktion. Hoffentlich trägt dies dazu bei, unserer Community zu versichern, dass Bulwark nach einer gewissen Zeit nicht mehr durch die vom Team gehaltenen BWK abgewertet werden kann. Wie in Punkt 2.5.1 dargestellt wird, ist der Unterschied zwischen den beiden genannten Modellen bereits nach 180 Tagen klar zu erkennen. Wir hoffen, dass diese offene Herangehensweise Vorbildwirkung hat und der Community zugutekommt.

2.5.1 Vergleich der beiden Modelle



2.5.2 Instamining und unser Ansatz

DASH (Darkcoin) hat aufgezeigt, wie wichtig ein Schutz vor Instamining ist. Zwischen 10% und 15% der gesamten DASH-Menge wurden in den ersten Tagen seiner Existenz durch einige unternehmungslustige Benutzerinnen und Benutzer erzeugt (Wiecko 2017). Wir

haben hierzu zwei Ansätze. Einerseits haben wir eine langsame, linear ansteigende Subvention eingebaut, die die Blockbelohnung während der ersten 960 Blöcke (d.h. während Tag 1) langsam bis zur vollständigen Blockbelohnung steigerte. Andererseits haben wir 100% aller Belohnungen an diesem Tag an die Miner vergeben. Bisher wurde versucht, dieses Problem durch eine sehr kleine Blockbelohnung zu lösen, die dann plötzlich auf den vollen Betrag ansteigt, aber dieser Ansatz führte oft zu durch DDoS-Attacken oder einen plötzlichen Zustrom neuer Miner überlastete Mining Pools. Durch die linear ansteigende Belohnung gibt es keinen Grund, mit der Arbeit von Minern oder Pools zu interferieren, um sich auf diesem Wege zu bereichern.

2.5.3 ICO? Dann doch lieber „IC-NO"!

Ganz ehrlich, im Moment werden wir alle permanent mit ICO-Werbung bombardiert. Diese haben selbstverständlich ihren Platz im Krypto-Ökosstem, oftmals dienen sie aber nur dazu, Wohlstand bei den Betreibern zu generieren. Da Bulwark Masternode-Belohnungen und (in seiner zweiten Phase) auch Proof of Stake anbietet, könnten so starke Marktschwankungen entstehen und es könnte zu einer Machtkonzentration bei den frühesten (und wohlhabendsten) Anwenderinnen und Anwendern kommen. Obwohl Anhäufungen von Wohlstand unvermeidbar sind, sind wir davon überzeugt, dass wir jede Gelegenheit, ein faires und ausgeglichenes System zu schaffen, nützen sollten. Darum haben wir uns für die skalierende Blockbelohnungs-Strategie entschieden, um Bulwark möglichst vielen Menschen zugänglich zu machen und so die Konzentration von Macht und Wohlstand, die bei anderen Projekten vorliegt, zu vermeiden oder zumindest zu verringern.

2.6 Schnell und funktional

Mit einer Blockzeit von 90 Sekunden, Masternode-Konsens und Transaktionssperren („transaction locking"), einem vernünftigen Zeitplan und umweltfreundlichem Staking strebt Bulwark danach, eine wahrhaft schnelle und funktionale Kryptowährung zu sein.

Kapitel 3

Unsere Blockchain-Parameter

3.1 Bulwarks Spezifikationen auf einen Blick

Tabelle 3.1: Bulwarks Spezifikationen auf einen Blick

Spezifikation	Beschreibung
Ticker	BWK
Algorithmus	NIST5
RPC Port	52541
P2P Port	52543
Block-Zeit	90 Sekunden
Schwierigkeits-Algorithmus	Dark Gravity Wave v3.0
Block-Größe	1MB
Mined/Minted-Reife	67 Blöcke (~100 Minuten)
Bestätigung	6 Blöcke (~9 Minuten)
Menge im Umlauf (1 Jahr)	14,505,720 BWK
Menge im Umlauf (5 Jahre)	27,668,220 BWK
PoW-Zeitraum	*nHeight* ≤ 345,600
PoS-Zeitraum	*nHeight* ≥ 345,601
Unterstützte Protokolle	IPV4, IPV6, TOR
PoS	Blackcoin v3.0 PoS, PIVX SeeSaw-Belohnungen

3.2 SlowStart

Unser fairer Start wird durch den folgenden Code gewährleistet (Quelle: *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
} 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 wird von Bulwark verwendet, um die Schwierigkeit des Proof of Work anzupassen. Es verwendet einen gleitenden Durchschnittswert, der auf starke Hash-Veränderungen innerhalb weniger Blöcke reagieren kann. Das lindert den „Stuck Block Effect“ der oftmals durch Multipools hervorgerufen wird und verhindert, dass eine Person, die plötzlich eine große Menge an Rechenleistung in das Netzwerk einbringt, mehr als ein paar Blöcke hintereinander lösen kann.

Kapitel 4

Block-Belohnungen

4.1 Block-Belohungen für Proof of Work

Tabelle 4.1: Block-Belohungen für Proof of Work

Subvention	Block	PoW	MN	Umlauf
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

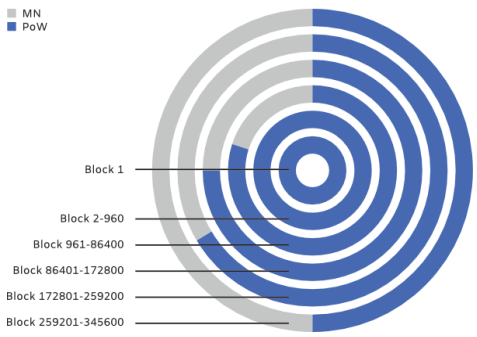


Abbildung 4.1: Blockbelohnungen im PoW-Zeitraum

4.2 Block-Belohnungen für Proof of Stake

Tabelle 4.2 Block-Belohnungen für Proof of Stake

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

Kapitel 5

NIST5 Hashing

5.1 Wieso NIST5?

Seit er 2014 von TalkCoin implementiert wurde, gewann der NIST5- Algorithmus langsam an Popularität. NIST5 funktioniert mit unterschiedlichster Hardware – von CPUs bis hin zu GPUs von NVidia und AMD. Er ist dabei nicht so resistent gegen ASICs wie andere „memory hard"-Algorithmen, dafür aber deutlich stabiler bei geringerem Stromverbrauch. Sollten am Markt verfügbare ASIC-Miner noch vor dem Ablauf des PoW-Zeitraums neue Firmware zum Berechnen von NIST5 erhalten, haben wir einen alternativen Algorithmus. Falls dieser Fall eintritt würden wir eine Abstimmung in der Community durchführen, um zu entscheiden, wie wir darauf reagieren, falls überhaupt. Allerdings glauben wir, dass unsere relativ kurze PoW-Phase und die Bereitschaft, notfalls den Algorithmus zu wechseln, ASIC-Hersteller davon abschrecken sollte, NIST5 zu unterstützen.

5.2 Die fünf Finalisten der NIST SHA-3 Competition

NIST5 besteht aus fünf Hashing- Algorithmen, die alle im Finale der NIST Hashing Competition standen (Chang et al. 2012). Sie sind (in der verwendeten Reihenfolge):

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

5.3 Der neue SHA-3 Standard

Keccak gewann die letzte Runde und wurde so zur neuen Hash-Funktion für SHA3, da die anderen Algorithmen, obwohl sie kryptographisch sicher waren, ein paar Punkte wegen kleinerer technischer Details verloren hatten. Wir sind der Überzeugung, dass die Kombination dieser verschiedenen Systeme einen schnellen, sicheren und vertretbaren Hashing- Algorithmus darstellt.

5.4 Verfügbare Mining-Software

Momentan gibt es drei verschiedene Programme, mit denen man Bulwark minen kann:

Name	Plattform	Link
SGMiner-5.0	OpenCL	GitHub
ccminer-2.2.2	CUDA	GitHub
cpuminer-opt	CPU	GitHub

Kapitel 6

Funktionsumfang

6.1 Masternodes

Grundsätzlich handelt es sich bei Masternodes um ein dezentralisiertes Netz aus Computern, die das Bulwark-Netzwerk unterstützen. Sie führen wichtige Arbeiten durch und erhalten dafür einen Teil der Block-Belohung. Somit stabilisieren Masternodes die Versorgung mit neuen Bulwarks, verarbeiten Transaktionen und sichern das Netzwerk. Masternodes benötigen 5000 BWK und rudimentäres technisches Wissen. Jede Wallet mit 5000 BWK kann ein Masternode einrichten.

6.2 Verschleierung / Coin Mixing

Bulwark unterstützt Verschleierung, basierend auf CoinJoin, allerdings erweitert um verschiedene Verbesserungen gegenüber dem Original. Erreicht wird das durch dezentralisiertes Coin Mixing im Masternode-Netzwerk. So verbessern wir den Datenschutz bei Transaktionen. Obwohl Coin Mixing nicht 100% anonym ist, stellt es doch eine drastische Verbesserung zu Bitcoin-Transaktionen dar. Während bei Bitcoin alle Transaktionen von außen einsehbar sind, bräuchte ein Angreifer bei Bulwark die Kontrolle über die Hälfte aller Masternodes, um auch nur eine Chance von 0,5% zu haben, eine einzelne Transaktion aufzudecken, die 8 Runden lang „gemixt“ wurde (Kiraly 2017b). Diese wichtige Funktion bietet einen hohen Level von Anonymität für alle Bulwark-Benutzerinnen und Benutzer, die ihre Transaktionen verschleiern wollen.

6.3 SwiftTX

SwiftTX gibt Masternodes die Möglichkeit, in Bezug auf Transaktionen einen Konsens zu finden und diese zu verarbeiten. Wenn eine Transaktion an das Netzwerk übermittelt wird, wird diese von einer Gruppe Masternodes validiert. Finden diese Masternodes zu einem Konsens, wird die Gültigkeit der Transaktion vermerkt, damit diese im Anschluss in die Blockchain eingetragen werden kann. Dadurch wird die Transaktionsgeschwindigkeit gegenüber konventionellen Systemen (wie Bitcoins 10-Minuten-Blöcke mit mehreren Bestätigungen) merkbar erhöht. SwiftTX macht es möglich, dass mehrere Transaktionen durchgeführt werden, bevor der zugehörige Block erzeugt wurde. Dieses System basiert auf InstantSend von DASH (Kiraly 2017a).

6.4 Sporks

Das Bulwark-Netzwerk verwendet einen mehrstufigen Fork-Mechanismus, der als „sporking" bezeichnet wird. So wird das Risiko unerwünschter Netzwerk-Forks bei der Implementierung neuer Funktionien minimiert. „Spork"-Änderungen können über das Netzwerk verteilt und bei Bedarf aktiviert oder deaktiviert werden, ohne dass es dafür ein Software-Update der Knoten geben müsste. So kann das Netzwerk schnell auf Sicherheitslücken und andere Probleme reagieren.

6.5 TOR & IPV6 Masternodes

Bulwark erlaubt seinen Benutzerinnen und Benutzern, Masternodes mit einer Onion- oder IPV6-Adresse zu betreiben. Wir arbeiten daran, TOR-Knoten bereitzustellen, um das TOR-Netzwerk zu stärken und Bulwark für Benutzer im TOR-Netz zugänglicher zu machen. Es ist außerdem möglich, ein Masternode als „hidden service" im TOR-Netz laufen zu lassen. So ermöglichen wir Benutzerinnen und Benutzern mit einer stabilen Internetverbindung, ihr Masternode im eigenen Heimnetzwerk zu betreiben, ohne dass sie dadurch ihre Privatsphäre oder Sicherheit gefährden müssen.

6.6 Community und Mitbestimmung

Die Bulwark-Community ist der wichtigste Faktor für den langfristigen Erfolg des Projekts, und ihre Fähigkeit, die Zukunft von Bulwark aktiv mitzubestimmen, steht an erster Stelle. Daher planen wir, am Ende der PoW-Phase Budget-Superblöcke im Netzwerk zu aktivieren. Diese monatlichen Superblöcke erlauben den Anwenderinnen und Anwendern, alle Aspekte von Bulwarks Entwicklung, Präsenz und Community mitzukontrollieren. Die spätere Implementation dieses Systems gibt uns die Zeit, den dafür notwendigen Rahmen zu schaffen, und maximiert die Block-Belohnungen für Miner und Masternodes.

Wir werden einen mehrstufigen Prozess für das Einbringen von Vorschlägen anwenden. Jeder Schritt muss vollständig abgeschlossen werden, anderenfalls wird der Vorschlag höchstwahrscheinlich nicht angenommen. Diese Schritte könnten so aussehen:

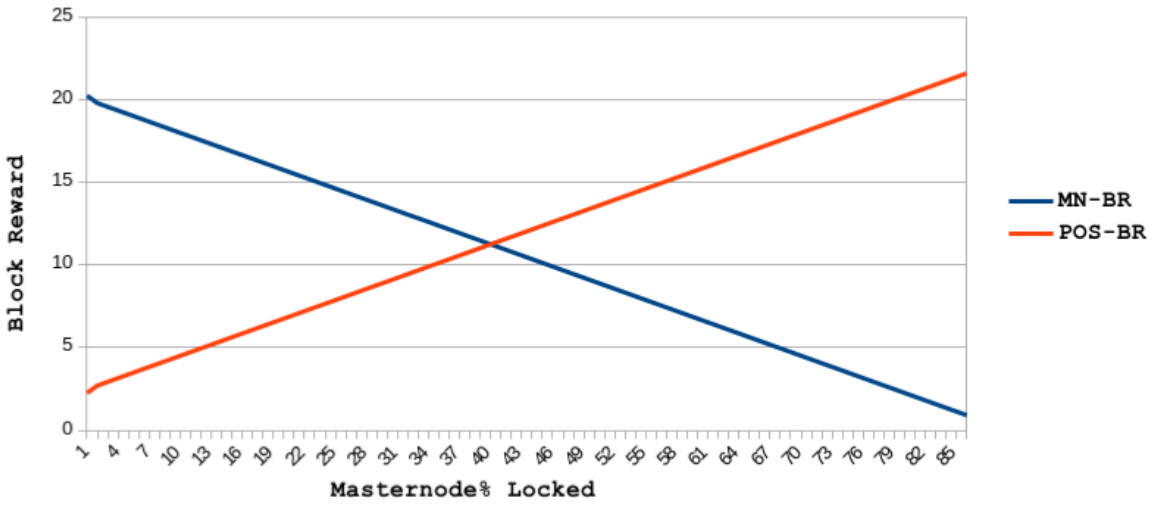
- Zuallererst sollten sie den Vorschlag im Discord-Chat diskutieren. Wird der Vorschlag dort für gut befunden, geht es in die nächste Phase.
- Der Vorschlag wird auf anderen Social Media-Plattformen diskutiert, um Feedback zu sammeln. Da Bulwark eine breite Benutzerbasis hat, kann es etwas aufwändig sein, einen größeren Teil der Anwenderinnen und Anwender zu erreichen. Kommentare aus dieser Diskussion sollten im nächsten Teil zitiert werden.
- Seien sie offen für Vorschläge durch die Community und die Entwickler, und bereit, externe Ideen in ihren Vorschlag einzubinden.
- Erstellen sie einen formellen Vor-Vorschlag im Abschnitt Governance->Pre-Proposal auf der Bulwark-Webseite. Fügen sie Kommentare aus den Schritten eins und zwei hinzu. Verfassen sie den Vorschlag so, als würde er in dieser Form an die Blockchain angehängt und zur Wahl gestellt werden.
- Fügen sie jetzt ihren Vorschlag an die Blockchain an. Dabei fallen zwei Gebühren an, eine für die Einreichung und eine Wahlgebühr, die den Vorschlag auf der Blockchain aktiviert. Die Einreichungsgebühr kann nicht rückerstattet werden, die Wahlgebühr fällt erst an, wenn der Vorschlag aktiviert wird.
- Es ist erlaubt, in dem Vorschlag eine Rückerstattung dieser Gebühren zu beantragen. Dies muss so jedoch im Vorschlag explizit vermerkt werden.
- Kontaktieren sie alle Benutzerinnen und Benutzer, mit denen sie über ihren Vorschlag gesprochen haben, damit sie für diesen Vorschlag abstimmen. Damit ein Vorschlag ausbezahlt wird, müssen 10% der berechtigten Masternodes mit „Ja“ abstimmen. Das kann unter Umständen viel schwieriger sein, als es sich jetzt liest, darum seien sie gewissenhaft, aussagekräftig und respektvoll, wenn sie die für ihren Vorschlag notwendigen Stimmen erwerben wollen.

6.7 SeeSaw PoS/Masternode-Belohnungen

Wir haben uns dazu entschlossen, das von PIVX bekanntgemachte SeeSaw-Belohnungssystem zu verwenden (jakiman 2017). SeeSaw beginnt mit einem Verhältnis von 9:1 zugunsten von Masternodes und passt dieses dann zwischen Stakern und Masternodes an, bis etwa 41,5% aller BWK in Masternodes geparkt sind – ab diesem Zeitpunkt gewinnen Staker einen leichten Vorteil gegenüber Masternodes. Der Grund dafür sind die Probleme – starke Preisvolatilität und geringe Liquidität – die bei Kryptowährungen auftreten, bei denen ein deutlich höherer Anteil in Masternodes steckt. Mit dieser Strategie verhindern wir Frustration bei unseren Benutzerinnen und Benutzern aufgrund geringer Verfügbarkeit und stärken unser Netzwerk. Da es eines unserer erklärten Ziele ist, eine breit unterstützte Plattform für anonymen eCommerce zu werden, ist *Transactability* von höchster Bedeutung für alle, die Bulwark annehmen und besitzen.

Fig 3. SeeSaw @ Height 345601 - 432000

(after budget percentage)



Kapitel 7

Die Zukunft

7.1 Die Bulwark-Werkzeugkiste („Bulwark Tool Chest“)

Die Bulwark-Werkzeugkiste ist eine Sammlung von Codeschnippseln, APIs, Bibliotheken, Scripts und Wissen das ein Bazaar-ähnliches Umfeld erzeugen soll, in dem Entwicklerinnen und Entwickler, die in ihren Projekten Kryptowährungen unterstützen möchten, freien Zugang zu Wissen, Information und Code finden. Wir glauben daran, dass dieses Angebot Menschen die Möglichkeit bietet, spannende und großartige Projekte zu erzeugen, so wie auch ein Zimmermann nur mit den richtigen Werkzeugen Großes vollbringen kann.

7.2 Privatsphäre und Software-Verbesserungen

Wir fühlen uns dazu verpflichtet, neue Protokolle zu übernehmen, die den Datenschutz für unsere Anwenderinnen und Anwender verbessern. Derzeit bewerten wir unterschiedliche Konzepte, welche wir ab der ersten Jahreshälfte 2018 testen und entwickeln möchten. Einige dieser Verbesserungen sind:

- Unterstützung für das I2P-Netzwerk.
- Zerocoin-Protokoll/Stealth addressing (Sobald wir von der Verwendbarkeit dieser Lösungen überzeugt sind).
- Abgleich unserer Codebase mit der Bitcoin-Mainline.
- Verbesserungen QT Wallet.
- Integration von Libtox.
- Virtualisierung beziehungsweise Containerization der Bullwark-Wallet, um eine weitere Sicherheitsebene zu erzeugen.

7.3 Bulwark Secure Home Node

Wir werden mit CAD-Spezialistinnen und Spezialisten zusammenarbeiten, um einen kleinen, in sich geschlossenen Bulwark-Knoten für zu Hause zu entwickeln. Benutzerinnen und Benutzer werden dieses Gerät an ihr Heimnetzwerk anschließen und über ein Web-Interface konfigurieren können. Folgende Funktionen sehen wir vor:

- Ein leicht einzurichtendes Masternode / Full Node hinter einem TOR Hidden Service für Menschen mit einer stabilen Internetverbindung.
- Die Option, das Gerät als Relay zu betreiben, um das TOR-Netzwerk zu stärken.
- VPN und/oder Proxy-Server, um den eigenen Traffic durch TOR oder I2P zu routen.
- Staking von Bulwark durch Virtualisierung oder ein eigenständiges Gerät.

Im Geiste der Dezentralisierung werden die 3D-druckbaren Pläne und der gesamte Quellcode zur Verfügung gestellt, damit alle Benutzerinnen und Benutzer dieses Gerät selbst daheim herstellen können.

7.4 Unsere Marke

Wir werden weiterhin unsere Marke ausdehnen und planen zu diesem Zweck mit Hardware-Herstellern und Systemintegratoren zusammenzuarbeiten, die unsere Leidenschaft und Ideale teilen. In fünf Jahren möchten wir, dass „Bulwark“ nicht nur für Kryptowährung, sondern auch für Privatsphäre, Sicherheit und Respekt vor den Anwenderinnen und Anwendern steht. Unser Hauptanliegen: Wahlfreiheit durch Privatsphäre („freedom of choice through privacy”).

7.5 Design

Wir möchten eine visuelle Sprache entwickeln, die Bulwark von der Konkurrenz abhebt. Unser Design-Team plant mit dem UI/UX und der Marke zu experimentieren, um so hochwertiges Design zu erreichen, das unseren Anwenderinnen und Anwendern die beste Benutzererfahrung in ästhetisch ansprechender Form bietet. Dies wollen wir durch Wettbewerbsforschung, einen aktuell gehaltenen Überblick über technologische Trends und Standards sowie ein stetiges Streben nach innovativen Gestaltungsmöglichkeiten erreichen.

Kapitel 8

Zusammenfassung

8.1 Zusammenfassung

Bulwark ist eine datenschutzorientierte Kryptowährung mit Masternodes, Community-Mitbestimmung und einem stetig wachsenden Set an Werkzeugen. Das Projekt begann mit einem fairen Start und legt den Fokus auf breite Verwendung. Der kontrollierte Anfang, die Verteilung von Belohnungen und der Hashing-Algorithmus wurden bewusst gewählt, um möglichst vielen Menschen eine aktive Teilnahme zu ermöglichen. Bulwark startete mit verschiedenen wichtigen Features für die Wahrung der Privatsphäre seiner Benutzerinnen und Benutzer, und das Entwickler-Team arbeitet hart an der Implementation neuer Funktionen und der Einbringung bewährter Technologien. Bulwark setzt sich für Freiheit durch Privatsphäre ein und wird dafür mit aller Kraft kämpfen.

8.2 Zukünftige Aufgaben

Die Welt der auf Datenschutz ausgelegten Masternode-Kryptowährungen wurde in der letzten Zeit von Projekten überschwemmt, die neue Benutzerinnen und Benutzer mit exorbitanten Gewinnprognosen, meilenlangen Entwicklungsplänen voller unhaltbarer Versprechen und irreführendem Marketing ködern wollen. Bulwark will genau das Gegenteil tun: Wenig Hype, viel Substanz. Jetzige und zukünftige Ziele des Projektes werden dieser Formel folgen: Spezifisch, messbar, erreichbar, relevant und termingebunden.

Verweise

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

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

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

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

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

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

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

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

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

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

Wiecko, R., 2017. Dash instamine issue clarification. Auffindbar bei: https://dashpay.atlassian.net/wiki/spaces/OC/pages/19759164/Dash+Instamine+Issue+Clarification.

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