BULWARK

CRYPTOCURRENCY

Cryptocurrency Whitepaper

Bulwark Core Team:

Eatbatterys (Project Coordinator)

Jack (Marketing Director)

SerfyWerfy (Blockchain Developer)

Frogman (Communications Lead)

Patrick (Brand and Design)

Stu (Ecosystem Developer)

The Bulwark Core Team

December 2017

Мы, основная команда Bulwark, подтверждаем, что работа, представленная в этом документе, является нашей. Если информация была получена из других источников, мы подтверждаем, что это указано в ссылках.

Предисловие

Bulwark (ticker: BWK) - это монета, ориентированная на сообщества, идея которой родилась под впечатлением, как правило, несправедливой политики в отношении приватного окружения masternode. Наша выверенная и честная стратегия запуска позволяет участникам в начале вступить в перспективный проект. Мы предлагаем простое ценное предложение без грандиозного обещания: мы предоставим приватную монету, которая работает сегодня и будет работать в будущем, используя лучшие практики как DASH, так и PIVX. Никаких глянцевых обещаний с туманной перспективой реализации, но рабочая монета на рабочей платформе с поддержкой в будущем. Это не означает, что мы не планируем никаких инноваций, но вместо этого мы будем предоставлять результаты, а не рекламу. Слишком много монет, которые подпитываются шумихой, но полностью лишены сути - мы не хотим вступать в растущий пулл монет, основанный на девизах сверх обещаний но без четкого плана реализации. Без ICO, с вознаграждением за плавный запуск, небольшими премиями и распределением вознаграждений за майнинг, ранние пользователи Bulwark будут иметь полный доступ к начальному выпуску приватной монеты, микс masternod и наилучшую из доступных технологий приватной монеты наряду с проработанной дорожной картой дальнейшей разработки. Masternodes будут доступны и функциональны при запуске и станут основной частью видения этой монеты, будут стабилизировать циркуляцию, обеспечивать безопасность сети и жизненно важную функциональность.

Признательность

Bulwark был бы невозможен без уже проделанной работы команд Bitcoin, Peercoin, Blackcoin, Talkcoin, Dash и PIVX. Программное обеспечение с открытым исходным кодом и его продолжатели постоянно прокладывают путь к новым и захватывающим инновациям. Когда информация и знания свободны для построения нового, общество в целом выигрывает. Мы благодарны нашим предшественникам за возможность внести свой вклад в эту растущую экосистему.

Содержание

Глава 1

Краткое введение в криптовалюту

1.1 Предыстория

В 2009 году Сатоши Накамото выпустил статью под названием A Peer-to-Peer Electronic Cash System, в которой он подробно описал его видение коммерции. В видении Накамото подробно описана peer-to-peer валютная система, поддерживаемая хеш-основанием, подтверждающим работу. Сеть устанавливала время каждой транзакции, шифруя их данные и занося их в общедоступный учет, который не может быть изменен без повторного proof-of-work. Nodes выбирали бы самую длинную цепь как доказательство, подтвержденное самым большим пулом хэширования. До тех пор пока ≥ 51% мощности хеширования сети контролируется узлами, не предназначенными для облегчения атаки, цепочка, которую они создают, останется самой длинной (Nakamoto 2009).

1.2 The Block

Каждому блоку в сети предоставляется 80-байтовый заголовок, содержащий двойную SHA256 хэшированную копию заголовка предыдущего блока, merkle root (двойной SHA256 хэшированный вывод всех хэшей, которые произошли в блоке), фиксируется время в которое начался proof-of-work, сложность, связанная с хешем этого заголовка, должна быть меньшей или равной, а также данное время при котором майнеры достигли данной сложности. Таким образом, любые попытки изменить любую транзакцию в любом блоке приведут к отказу блока от майнерской сети (Bitcoin Core Team 2017).

1.3 Блокчейн

Группы транзакций формируются в блоки, и эти блоки размещаются хронологически в цепочку, образуя блокчейн. Блокчейн создает меняющуюся историю всей деятельности в сети и служит в качестве распределенной модели согласования, где любая транзакция может быть проверена в любое время (Crosby et al., 2015)

1.4 Proof-Of-Work

Proof-of-work - это система верификации, в которой майнеры должны выделять материальные ресурсы (электричество, затраты на оборудование) для решения произвольной вероятности *ошибки*. Для того, чтобы злоумышленник мог испортить блокчейн с помощью мошеннической транзакции, они должны выполнить все proof-of-work до настоящего момента (Okupski 2016).

Глава 2

Представление Bulwark

2.1 Прочный фундамент

Каждому дому нужен прочный фундамент, и Bulwark ничем не отличается. Bulwark построен на PIVX, который сам построен на популярной криптовалюте DASH. В то время как происхождение можно проследить до исходного ядра Сатоши, каждый проект выбрал конкретное направление с целями и идеалами, которые представляют сообщества, которым они служат. Мы будем расширять и придавать особое значение конфиденциальным особенностям монеты наших предшественников изучая новые технологии, и в то же время создавая наборы инструментов и возможностей интеграции Bulwark в современные технологические платформы.

2.2 Команда, посвященная сообществу

Для некоторых проектов сообщества не являются первоочередной целью. Первоочередной же задачей Bulwark является сообщество. С распродажами, конкурсами, оживленной платформой для дискуссий и политикой нулевой терпимости к преследованию новичков, Bulwark стремится быть криптовалютой для всех разновидностей конечных пользователей. Участники нашей пользовательской базы уже вносят полезные пожелания и наставления для дальнейшего улучшения работы пользователей.

2.3 Открытость и сбалансированность

На момент написания этого документа наблюдался наплыв криптовалют которые использовали аналогичную основу. В то время как их базовая технология выглядит надежно, зачастую более глубокое изучение их спецификаций и параметров блокировки выявляет более-чем-несправедливую практику.

2.4 Проблемы в практиках пре-майнинга

2.4.1 Практический пример: FooBarBazCoin

Растущий тренд в пространстве криптовалюты заключается в том, чтобы выбрать произвольную дату в будущем, а затем основывать первичный процент на оборотном запасе на эту дату. Давайте посмотрим на вымышленную FBC (FooBarBaz Coin), DASH-fork.

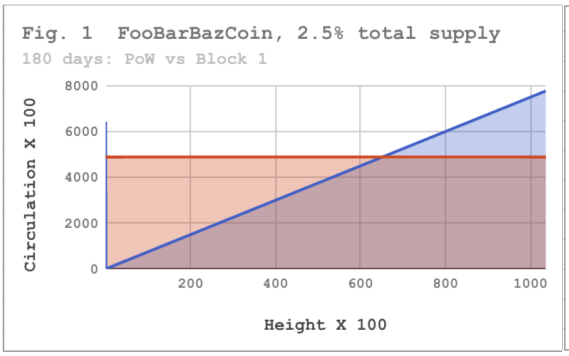
- Вознаграждение блока: 15
- Block Time: 2.5 минуты
- POW/Masternode Split: 50/50%
- Исходная сложность алгоритма: KGW
- Субсидия уменьшается на 12% каждый год
- Максимальное количество монет: ~ 25 миллионов
- 2.5% премайнинга

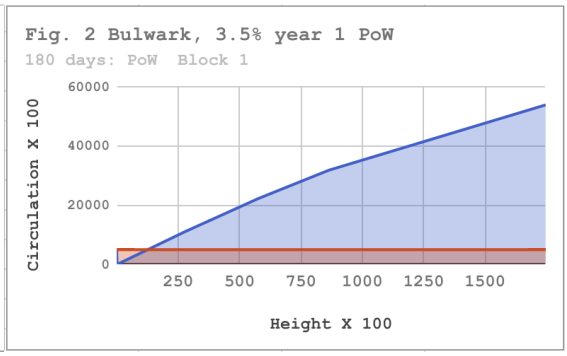
В этом примере рекламируемый 2.5% премайнинг, переводящий до ~ 643 000 монет (из ~ 25 миллионов), кажется разумным для стороннего наблюдателя. Тем не менее, для вознаграждений в рамках программы PoW и Masternode в соответствии с монетами, которыми владеют разработчики, потребуется около 43 000 блоков. При достижении цели в 2,5 минуты на блок, потребуется около 150 дней для майнеров (или 75 дней в целом) для получения такого же количества монет. Через 75 дней разработчики по-прежнему будут контролировать половину существующих монет.

2.5 Более честная альтернатива

Команда Bulwark осознает это и решила упредить проблему. Наш премайн в 489 720 монет (3,5%) представляет собой чуть более чем 12 дней добычи PoW или чуть более 10 дней общего производства. Надеемся, что это послужит успокоением для сообщества, тот факт что после определенного момента рынок не может быть значительно обесценен в результате монетам принадлежащим основной команде. Как вы можете видеть на рисунках ниже, оба из которых представляют 180 дней в каждом сценарии, разница очень ясна. Мы надеемся, что при столь честном подходе к процессам создаст прецедент, который принесет пользу обществу в целом.

2.5.1 Сравнение двух подходов





2.5.2 Instamine и наш подход

Dash (Darkcoin) представляет интересное тематическое исследование о необходимости защиты instamine. Почти 10-15% от общего объема поставок Dash было создано в первые дни существования монеты благодаря некоторым предприимчивым пользователям (Wiecko 2017). Наш подход к проблеме instamine был двухуровневым. Мы использовали медленную субсидию, в которой первые 960 блоков (1 день) линейно увеличивались до полного вознаграждения за блок, при этом 100% вознаграждений за блок также направлялись майнерам в тот же день. Исторически сложилось так, что это привело к очень маленькому вознаграждению в блоке, которое внезапно смещается до полной награды на определенном уровне за блок, однако это часто приводило к тому, что пулы были атакованы DDoSed или перегружены новым трафиком. При линейно увеличивающемся вознаграждении не было бы никакого смысла пытаться вмешиваться в работу майнеров или операторов пула для получения денежной прибыли.

2.5.3 ICO? Скорее IC-NO!

Посмотрим правде в глаза, на момент написания нас постоянно “забрасывают” различными ICO. И хотя у них есть законное место в экосистеме криптовалюты, зачастую они служат только для набивания карманов. Учитывая, что Bulwark предлагает вознаграждения за Masternode и, на втором этапе, proof-of-work вознаграждение, эта концентрация активов может вызвать колоссальные колебания рынка и сильно наклонить систему управления в пользу самых ранних (и самых богатых) последователей. В то время как концентрация активов неизбежны в целом, мы считаем, что любая возможность, которую мы можем предпринять для равной игры должна быть предпринята. Мы начали с масштабной стратегии награды за блок, справедливого механики запуска, чтобы стимулировать широкое распространение Bulwark для многих пользователей, в идеале избегая некоторой концентрации активов, наблюдаемой в других проектах.

2.6 Скорость и функциональность

С 90-секундным block time, консенсусом masternode и блокировкой транзакций, разумным графиком емиссии и ставками дружественными для системы, Bulwark стремится стать действительно быстрой и функциональной криптовалютой.

Глава 3

Параметры нашего blockchain

3.1 Краткие технические характеристики Bulwark

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

Открытость нашего старта предоставляется следующим фрагментом кода (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
} 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 с самого начала используется Bulwark как метод перенацеливания сложности PoW. Он использует простую среднюю переменную, которая может реагировать на значительные nethash увеличения или drop-offs всего за несколько блоков. Это уменьшает эффект «застрявшего блока», часто вызываемый multipools, и не позволяет одному человеку добавить значительный объем вычислительной мощности из мгновенного решения более чем нескольких блоков.

Глава 4

Block Вознаграждения

4.1 PoW Block вознаграждения

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

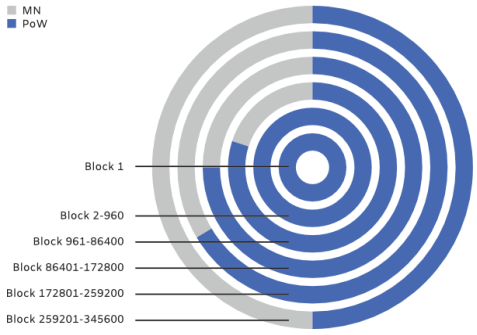


Figure 4.1: PoW Period Block Reward

4.2 PoS Block вознаграждения

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

Глава 5

NIST5 Hashing

5.1 Почему NIST5

Популяризованный TalkCoin в 2014 году, алгоритм хеширования NIST5 испытал скромное использование основного потока. NIST5 можно добывать на широком спектре бытового оборудования, включая процессоры, а также графические процессоры AMD и NVidia. NIST5 не так устойчив к ASIC, как некоторые другие жесткие алгоритмы памяти, но мы считаем, что компромисс приемлем для улучшения стабильности системы и снижения энергопотребления по сравнению с жесткими алгоритмами памяти. В случае, если обновления прошивки, добавляющие поддержку NIST5 для ASIC, возникнут до окончания нашего периода PoW, мы подготовили альтернативный алгоритм в качестве замены. Мы будем призывать к голосованию сообщество в случае необходимости (если возникнет) и реагировать соответственно. Мы считаем, что наш короткий период PoW и готовность к переключению алгоритмов сдерживают производителей ASIC и не предвидем возникновение проблем.

5.2 Пять финалистов (NIST SHA-3 Соревнование)

Пять алгоритмов хэширования, составляющих NIST5, являются финалистами конкурса HIST Hashing Competition (Chang et al., 2012). Это (в порядке хеширования блоков):

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

5.3 Новый SHA-3 стандарт

В конце концов, Keccak прошел последний раунд, чтобы стать новой хэш-функцией SHA-3, в то время как остальные четыре алгоритма (несмотря на то, что они считались криптографически безопасными) потеряли несколько баллов от судей за некоторые незначительные технические тонкости. Мы полагаем, что сочетание нового стандарта SHA-3 наряду с другими вариантами финалистов обеспечивает быстрый, безопасный и установленный алгоритм хэширования

5.4 Доступное программное обеспечение для майнинга

На момент написания статьи, есть несколько вариантов для майнеров:

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

Глава 6

Набор функций

6.1 Masternodes

Masternodes - это, по сути, децентрализованная сеть компьютеров, обслуживающих сеть Bulwark. Masternodes выполняют важные сетевые функции и получают часть вознаграждений за блок. Они обслуживают экосистему Bulwark, стабилизируя поставку монет, обрабатывая транзакции и обеспечивая безопасность сети. Для работы Masternodes требуется 5000 BWK и скромные технические знания. Любой кошелек, контролирующий 5000 BWK, может установить масштаб.

6.2 Obfuscation / Coin Mixing

Bulwark имеет функцию Obfuscation, основанную на CoinJoin, но с различными улучшениями по сравнению с оригиналом и выполненную с помощью микширования монет в децентрализованном стиле, облегченной сетью мастернод. Это обеспечивает дополнительный уровень конфиденциальности в транзакциях. Хотя это не полностью анонимно, Obfuscation посредством смешивания узлов намного лучше, чем стандартная транзакция биткоинов. Например, все транзакции Bitcoin являются прозрачными. Для Bulwark злоумышленник должен был бы контролировать 50% действующих мастернод, чтобы иметь шанс в менее чем 0,5% для де-анонимизации одной единственной транзакции, смешанной с 8 раундами Obfuscation (Kiraly 2017b). Эта важная функция обеспечивает высокий уровень анонимности для пользователей BWK, которые предпочитают не показывать свои транзакции.

6.3 SwiftTX

SwiftTX предоставляет мастерноды с блокировкой и правом консенсуса по транзакциям. Когда транзакция передается в сеть, группа мастернодов проверяет транзакцию. Если эти магистрали достигнут консенсуса относительно действительности транзакции, он будет заблокирован для последующего введения в блок-цепь, что значительно увеличит скорость транзакций по сравнению с обычными системами (например, 10-минутный блок биткоинов с несколькими подтверждениями). SwiftTX позволяет совершать несколько транзакций до того, как блок в сети будет запущен с теми же входами. Эта система основана на InstantSend от Dash (Kiraly 2017a).

6.4 Sporks

В сети Bulwark используется многофазный механизм fork, известный как «sporking». Это позволит сети BWK реализовать новые функции, одновременно минимизируя вероятность непредвиденного сетевого fork-а во время развертывания. Изменения Spork развертываются по сети и могут быть включены и отключены по мере необходимости, не требуя обновлений программного обеспечения узла (strophy 2017). Эта функция чрезвычайно полезна и позволяет сети быстро реагировать на уязвимости безопасности.

6.5 TOR & IPV6 Masternodes

Bulwark позволяет пользователю запускать свой полный node или masternode либо из TOR адреса, либо из IPV6-адреса. Мы работаем над добавлением полных узлов TOR, чтобы как усилить саму сеть TOR, так и опыт пользователя Bulwark, работающий исключительно в режиме TOR. Уникальной особенностью поддержки TOR-masternode является возможность управлять вашим masternode как скрытой службой TOR. Узлы TOR позволяют пользователям со стабильными подключениями к Интернету работать с masternodes всне своей домашней сети без опасений быть выявленными или опасений что их домашняя сеть будет доступна для потенциальной хакерской атаки.

6.6 Значение сообщества и система управления

Сообщество Bulwark является самым важным фактором долгосрочного успеха проекта, и его способность значимо влиять на будущее монеты имеет первостепенное значение. Таким образом, в конце фазы PoW мы намерены активировать бюджетные суперблоки в сети. Эти суперблоки, оплачиваемые ежемесячно, позволят сообществу эффективно осмыслить все аспекты развития Bulwark, присутствие бренда и общественные дела. Отсрочка активации этой системы даст нам время для разработки базовой структуры, необходимой для положительного пользовательского опыта, и максимизации вознаграждений блоков, доступных майнерам и мастеренодам.

Мы будем использовать многофазный процесс для создания и представления предложений. Каждый шаг должен быть полностью завершен. Неспособность выполнить описанные шаги, скорее всего, приведет к тому, что предложение не будет активировано. Основными составляющими этих шагов является следующее:

- Начните наш чат Discord и поговорите с некоторыми из опытных пользователей. Оцените интерес, и если ответ положительный, переходите к следующему этапу.
- Используйте несколько социальных сетей, чтобы все обсудить и получить обратную связь. Помните, что Bulwark имеет разнообразную пользовательскую базу и различные уровни участия в управлении, и для достижения части пользовательской базы часто требуется определенная работа. Примите к сведению эти обсуждения и будьте готовы процитировать их в официальном pre-proposal. Чем больше цитат предоставлено, тем лучше.
- Будьте готовы к предложениям сообщества и разработчиков. Будьте гибкими и готовы включать в свое предложение внешние идеи и предложения.
- Создайте официальное pre-proposal по разделе «Governance->Pre-Proposal» нашего веб-сайта. Укажите цитаты для всех обсуждений, которые произошли с предыдущего шага. Относитесь к своему pre-proposal, как будто это то, что будет представлено на голосование blockchain.
- По завершении этих шагов вы отправите свое предложение в blockchain. Будьте готовы к двум платам, по одному на момент подачи заявки, и к оплате за участие в программе, которая активирует ваше предложение в blockchain. Плата за подачу не подлежит возврату, а плата за участие оплачивается только после утверждения и активации вашего предложения.
- Каждый может скорректировать свое предложения, чтобы включить стоимость возмещения этих двух сборов. Пожалуйста, убедитесь, что в своем

официальном предложении вы заявляете, что добавляете возмещение в запрашиваемую стипендию.

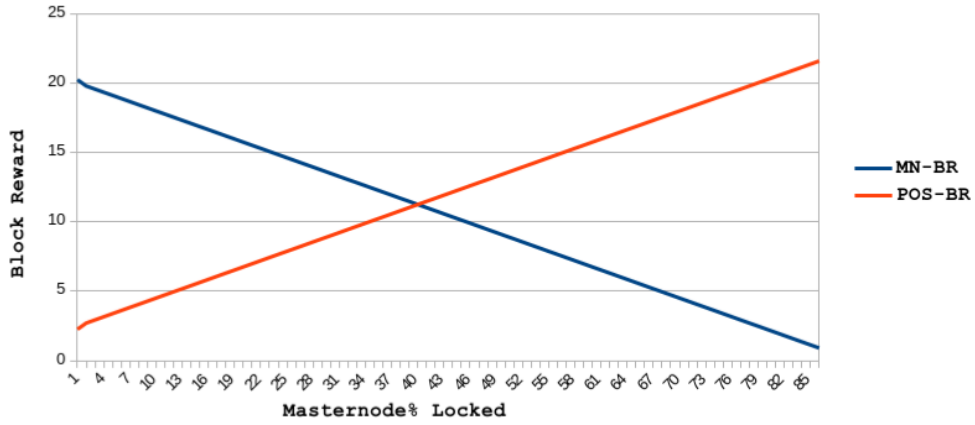
- Обязательно вернитесь на связь со всеми, с кем вы говорили, чтобы ваша идея была проголосована. Для того, чтобы предложение было оплачено, 10% подходящих masternodes должны проголосовать «да» по вашему предложению. Этот процесс получения 10% - ного консенсуса может быть намного сложнее, чем кажется, поэтому будьте внимательны, информативны и уважительны в том, чтобы собирать голоса, необходимые для оплаты вашего предложения.

6.7 SeeSaw PoS/Masternode Rewards

Мы решили использовать систему вознаграждения SeeSaw, популяризированную PIVX (jakiman 2017). Система вознаграждения SeeSaw начинается с коэффициента вознаграждения в размере 9:1 (в пользу мастернод) и плавно корректирует соотношение вознаграждения между операторами stake и masternodes до тех пор, пока около 41,5% монет в обороте не будут заперты в masternodes, тем временем вознаграждения за staking достигают незначительного преимущества над вознаграждениями masternodes на основе coin-by-coin. Причина, по которой SeeSaw отдает незначительное преимущество вознаграждениям за staking, заключается в том, что мы хотим избежать проблем, таких как значительная волатильность цен и низкая ликвидность, - которые влияют на монеты с очень высоким процентом их циркулирующего предложения, заблокированного в nodes. Эта стратегия уменьшит разочарование пользователей в отношении доступа к монетам и поддержит актуальность нашей надежной сети. Одна из наших основных целей является хорошо поддерживаемая платформа для анонимной торговли, что позволяет транзакционной деятельность имеет первостепенное значение для тех, кто принимает Bulwark и тех, кто хранит Bulwark.

Fig 3. SeeSaw @ Height 345601 - 432000

(after budget percentage)



Глава 7

Будущее

7.1 The Bulwark Tool Chest

Коллекция фрагментов кода, API-интерфейсов, библиотек, скриптов и знаний, которые будут способствовать созданию подобной рынку среды, где разработчики, которые могут требовать добавления поддержки криптовалюты в свои проекты, могут свободно обмениваться знаниями, информацией и кодом. Мы считаем, что предоставление разработчикам этих инструментов равносильно предоставлению плотнику инструментов, необходимых ему для создания захватывающих и шедевральных проектов.

7.2 Улучшение конфиденциальности и программного обеспечения

Мы стремимся к принятию новых протоколов, которые повысят конфиденциальность нашей пользовательской базы. В настоящее время мы оцениваем несколько путей и планируем начать внутреннее тестирование и разработку в первой половине 2018 года. Некоторые из этих усовершенствований включают:

- I2P приватную сеть.
- Протокол Zerocoin или адрессирование Stealth (Когда мы будем уверены в зрелости решения).
- Синхронизация нашей кодовой базы ближе к базовой линии биткоина.
- Упорядочивание/Обновление QT кошелька.
- Libtox Интеграция
- Виртуализация / контейнеризация кошелька Bulwark для добавления дополнительного уровня безопасности.

7.3 Bulwark Secure Home Node

Мы будем работать с CAD-специалистами для разработки небольшого автономного узла Home Bulwark. Пользователи смогут подключить это к своей домашней сети и настроить с помощью веб-интерфейса. Функции, которые мы намерены запустить, заключаются в следующем:

- Для тех, у кого есть стабильные подключения к Интернету, легко настроить полностью скрытый masternode (или полный узел) с помощью скрытых служб TOR.
- Возможность работы в качестве реле для улучшения общей сети TOR.
- VPN и / или прокси, которые могут использоваться для маршрутизации домашнего интернет-трафика через сеть TOR / I2P.
- Bulwark staking через виртуализацию либо add-oh устройство

В соответствии с духом децентрализации 3D-файлы для печати и весь исходный код будут доступны сообществу для сборки на дому.

7.4 Развитие нашего бренда

Мы продолжим расширять наш бренд и намерены работать с поставщиками оборудования и системными интеграторами, которые разделяют те же самые страсть и идеалы, которые мы делаем. Через пять лет мы хотим, чтобы имя «Bulwark» было синонимом не только криптовалюты, но и конфиденциальности, безопасности и уважения свободы пользователя. Основная цель Bulwark - обеспечить свободу выбора через конфиденциальность.

7.5 Дизайн и визуализация

Благодаря исследованиям и разработкам мы стремимся создать визуальный дизайн для Bulwark, который отличает его от конкурентов на криптографическом рынке. Наша команда разработчиков планирует внедрить инновации и экспериментировать с текущим UI / UX / Branding, чтобы в конечном итоге достичь превосходства в дизайне найдя золотую середину, которая позволяет наилучшим образом работать с UX, а также эстетически инновационная и красивая. Это будет сделано, исследуя наших конкурентов, сохраняя современные технологические тенденции и стандарты и постоянно применяя новые и захватывающие визуальные эффекты для конечных пользователей.

Глава 8

Заключение

8.1 Итог

Bulwark - это монета, ориентированная на конфиденциальность, с masternodes, управлением и эволюционирующей экосистемой инструментов. Проект начался с честного запуска и сосредоточился на широком распространении монет. Медленный старт, разделение вознаграждения блока и алгоритм хеширования были специально отобраны для создания возможностей для значительного участия сообщества. Bulwark запущен с различными важными функциями конфиденциальности и команда разработчиков усердно работает, чтобы ввести новые функции и строить на основе существующих технологий. Bulwark нацелен на расширение возможностей выбора путем обеспечения конфиденциальности и сосредоточит на этом значительные усилия.

8.2 Будущие работы

Экосистема masternod конфиденциальных монет с недавних пор наводнена монетами, стремящимися привлечь новых пользователей благодаря обещаниям о существенной отдаче от инвестиций, гигантским дорожным картам, наполненным невероятными результатами, и общей направленности на маркетинг чем на фактическое улучшение. Bulwark планирует быть противоположным: низкий уровень создания рекламы и высокий уровень фактического создания. Настоящие и будущие цели проекта будут соответствовать формуле, которая должна быть конкретной, измеримой, достижимой, соответствующей и ограниченной по времени выполнения.

Ссылки

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

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

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

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

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

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

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

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

Okupski, K., 2016. Bitcoin developer reference., pp.3–4. Available at: https://lopp.net/pdf/Bitcoin_Developer_Reference.pdf

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

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

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