SHIELD технический документ версия1.0.0

future-proofing в blockchain

Команда SHIELD

ShieldCoin@protonmail.com

https://ShieldCurrency.com

Аннотация

Протокол SHIELD заменит ECDS на Lamport, Winternitz или BLISS подписи, что позволит адресам быть “quantum-proof ”. SHIELD получит самостоятельный цикл разработки, который позволит продолжить разработку протокола SHIELD и других проектов, описанных в этой статье. SHIELD будет использовать пользовательскую схему PoS (PoS Boo) с помощью Masternodes. These masternodes will also enable features like PrivateSend and InstantSend. Эти Masternodes также позволят использовать такие функции, как PrivateSend и InstantSend.

Ключевые слова: SHIELD, quantum-proof, masternodes, cryptocurrency, blockchain, privacy

1 - Введение

SHIELD - это криптовалюта, основанная на технологии blockchain Satoshi Nakamoto (которую он издал в техническом документе[1] 2009 году), которая с тех пор растет и улучшается. В течение нескольких лет технология blockchain все чаще принимается, но по прежнему существует множество проблем, которые удерживают эту технологию от основного направления. SHIELD стремится решить многие из этих проблем.

2 - Проблемы для решения

Bitcoin был действительно инновационным, когда он был реализован, и значительная часть того, что сделал Satoshi, по-прежнему используется сегодня в основе многих криптовалют. Одним из таких вкладов является блок майнинг, но, более конкретно, блок майнинг с одним алгоритмом. Это привело к разработке специализированных аппаратных средств (ASIC), которые могут хэшировать один алгоритм настолько эффективно, что они делают они делают GPU майнинг устаревшей. Одно из недостатков принятого им решения, как и многие молодые криптоконверсии, стало осознавать тот факт, что майнинг на самом деле не справедлив. Вы можете прочитать об этом в разделе 3, мультиалгоритм майнинг для Proof of Work (PoW).
Квантовые компьютеры становятся все более изощренными и может быть на грани того, чтобы быть доступными для общественности. Будь то для исследователей, правительства, бизнеса и широкой общественности, в конечном итоге мы увидим, что квантовые вычисления станут доступными для состоятельных групп и людей с личными интересами. Хотя это невероятно новая технология, которая может значительно улучшить нашу жизнь, но также есть немало причин для беспокойств об этом развитии. Одним из них является то, что современная криптография может быть эффективно взломана будущими квантовыми компьютерами. Для многих криптоконверсий это может означать сломанный blockchain. Как мы собираемся решить эту проблему, изложен в разделе 4 “*Квантовое Сопротивление*”.
Крупные корпорации, такие как Facebook или Google стали лучше узнавать, кто вы и что вы хотите. Хотя это может и не быть (в настоящее время) слишком актуальным, это будет означать жизнь в мире, где предприятия будут наблюдать за нами; это может быть не так уж плохо, но это не выглядит очень хорошо. Существует множество валют, которые утверждают, что их пользователи анонимны, а что помешало бы этим крупным корпорациям и правительствам отслеживать ваши привычки тратить. Проблема с некоторыми из этих койинов является то, что они не столь эффективны, как они утверждаются. Это означает, что их масштабируемость и практичность очень низкое, что

практически не существует. Немного больше о том, как наши пользователи останутся анонимными, мы раскроем в разделе 5 *“Особенности Конфиденциальности”*. Некоторые альткойны имеют действительно перспективный план; у некоторых даже есть невероятно талантливые разработчики. Но без финансирования это может быть недостаточно, чтобы сохранить койн в живых. Если разработчики не смогут найти какой-то доход от проекта, будет все труднее работать над ним на полную. Мы не хотим, чтобы это произошло, поэтому мы планируем реализовать некоторые функции SHIELD (и некоторые платформы вокруг SHIELD), которые могут помочь нам в финансировании. Вы можете прочитать об этом решении в разделе 6, *“Финансирование”*.

Еще одна проблема с Bitcoin и многими другими валютами заключается в том, что майнеры должны майнить с энергоемкими аппаратными средствами, на разрешения штамповки койнов и подтверждение транзакции. Это было действительно инновационным в то время, и оно по-прежнему отлично работает, но экономические и экологические затраты на продолжение blockchain (то есть только PoW для сетевого консенсуса) очень высока. Это было решено с помощью нашей схемы доказательство доли владения - Proof of Stake (PoS), которую вы можете прочитать в разделе 9 *“PoS Boo”*.

3 Мульти-алгоритм майнинг для PoW

Мы улучшили равномерное распределение вознаграждения и сопротивление на 51%[citation needed] атаки с несколькими алгоритмами PoW. Мульти-алгоритм майнинг - это способ позволяющий несколько типов обрабатывающих устройств для блок майнинга; наш подход включает множество различных устройств, в том числе GPU и ASIC, для совместного майнинга на SHIELD blockchain. Распределение вознаграждений по алгоритму почти всегда одинаковое соотношение общего вознаграждения в течение определенного времени. Например, даже если один алгоритм имеет 300 ГГц/с, а другой - 50 МГц/с, они должны получать одинаковое количество койнов за час. Оно предусмотрена на предотвращения 51% атак, из-за способа распределения блоков; каждый алгоритм следует своему собственному *“*графику*”*, что означает, что для осуществления такой атаки нужно добиться 51% скорости хэширования для каждого алгоритма. Важным аспектом этой системы является то, на сколько сложно отрегулирован каждый алгоритм в отдельности.

Регулировка сложности, управляется схемой «Dark Gravity Wave v3», которая была разработана для Dash, но использовалась в различных других криптовалютах. Она намного лучше управляет спайками и падениями сетевого хеша, чем обычные вычисления

сложности, и затрудняет работу злонамеренных майнеров добыть быстрые койны без обработки транзакций.

4 Квантовое Сопротивление

Протокол SHIELD - это кванто-защищенные транзакции/адресации для определенных адресов. Другие криптовалюты часто не являются кванто-защищенными из-за их использования ECDS (который уязвим для алгоритма Shor[9], обеспечивается с помощью квантовых компьютеров). Чтобы изменить это, мы планируем использовать подписи Lamport или подобные схемы. Цифровые подписи Lamport основаны на хэш-функциях, а хэш-функции не уязвимы для алгоритма Shor. С ECDS, всякий раз, когда отправляется транзакция, адрес отправителя становится уязвимым, так как уязвимая к взлому ECDS подпись отображается. Взлом такой подписи позволит несанкционированный доступ к денежным средствам, связанным с этим адресом. Хэши не уязвимы для алгоритма Shor, таким образом, хешированные цифровые подписи лучше против этой угрозы относительно безопасности пострадавших адресов.

5 Особенности Конфиденциальности

SHIELD’s Project Perdu is one that has recently undergone a change of plan. SHIELD Perdu - это проект который недавно подвергся изменениям в плане.
Изначально мы планировали реализовать протокол Wraith от VergeCurrency[6], но из-за его относительно низких спецификаций мы решили выбрать PrivateSend (разработанный Dash); для нас, это лучше работает так как нам все равно нужно реализовать masternodes. Это изменение дополнительно повысит скорость транзакций по InstantSend. Несмотря на это улучшение, PrivateSend пока не делает транзакции полностью приватными, поэтому Zerocoin[5] или zk-SNARKs[4]/zk-STARK находится на рассмотрении
Подробнее об этом мы поговорим в квартале, в котором оно будет реализовано.

Для физической конфиденциальности мы будем использовать кошельки/узлы Tor[8]/I2P[7], которые скрывают IP-адрес и местоположение конечного пользователя.

6 Финансирование

Самофинансирование SHIELD может работать с использованием процентов от masternode и майнинг блок вознаграждений. Это будет очень небольшой процент, так как нам только нужно держать команду на плаву, а остальное на маркетинг. Мы также будем иметь

некоторые внешние источники поддержки, которые будут сделаны путем создания и присоединения платформ, которые помогают как разработчикам, так и пользователям. Например, мы получили много пожертвований от сообщества, благодаря которым мы можем продожить проект, а также получать поддержку от различных майнинг пулов. Мы надеемся, что это поможет продвинуть наш проект на неопределенный срок. Мы не имели ICO или премайн, как и многие из наших конкурентов в это время; мы считаем, что наличие сильного сообщества является лучшим средством для расширения.

7 Безопасность приложений

SHIELD - это все о безопасности. Мы стараемся улучшить многое в этом отношении с вышеупомянутой кванто-защитой, но мы видели тенденцию во многих уязвимых приложениях, которые взаимодействуют с блокчейном, и заметили, что дыры почти всегда находятся в пользовательских интерфейсах.
Мы думаем, что именно поэтому нам нужно иметь много наших оригинальных проверенных продуктов, это будет сделано с помощью сообщества с открытыми источниками, собирая пентесторов для индивидуального тестирования, и все наши команды разработчиков проверяя код, возможно даже подтверждая каждую фиксацию до распростронения (и не только для официальных обновлений).

Исходя из нашего опыта, используя наш Discord бот, мы наблюдали, что - с безопасным backend - ссылкой на внешний интерфейс которая является одним из самых важных вещей в безопасном приложении.

8 Интеграция

Интеграция новой технологии на новые или существующие платформы может влиять на определение ее конечной пригодности и применимости. Мы будем использовать множество популярных и бесплатных платформ, таких как Discord и Twitter как способ улучшить работу пользователей. Мы сделаем это путем разработки плагинов и ботов для таких платформ, как Discord, Twitter, Facebook (и более). Эта интеграция даст возможность отправлять SHIELD без необходимости запрашивать у получателя адрес кошелёк. Такая интеграция может также включать в себя кошелёк для этих платформ, таким образом, даже не нужен специальный кошелек на компьютере для использования SHIELD.

Интеграция также становится более популярной для общественного потребления. То есть, в сочетании с нетворкингом, очень важная часть расширения нашей аудитории и вариант

использования. Таким образом, для увеличения этих факторов, мы будем контактировать с многими бизнесами в этой сфере. Это позволит сделать наши цены более стабильными и мы будем иметь большую применимость.

9 PoS Boo

SHIELD Boo – это наша собственная схема PoS, основанная на PoS Casper[2]. Схема Casper больше предусмотрена на “POSv3”[3] с введением фактора риска от злонамеренных стакеров. Система прогрессирует в направлениив которая значительно затрудняет выполнение атак, таких как атака 51%; нужны будут большинство из всех минтированных койнов, и можно также столкнутся с потенциальной возможностью потерять их всех при запуске такой атаки[2]. Окончательность в основном определяется факторами стейка и риска, поэтому же может быть трудно выполнить успешную атаку даже с 51% обращением (Рис. 2), ситуация в ином случае была бы очень страшной для такого койна как Bitcoin.

Другая проблема которую решает PoS Casper/Boo так называемая цензура транзакций. С PoW, блок майнер может “выбрать” не майнить блок содержащий определенные адреса, тем самым подвергая цензуре этот адрес из сети. Так как блок создатели выбираются случайным образом и валидаторы являются глобальными с PoS схемой, очень трудно подвергать цензуре адреса из сети (с дополнительным бонусом, если вы попытаетесь заставить, то вы скорее всего потеряете свой стейк).

10 Будущее исследование

Как вы могли заметить, например в разделе 5, мы обсудили некоторые возможные особенности/спецификации, которые не были доработаны. Некоторые особенности отсутствуют в оперативном плане, такие как “sharding” и “smart contracts”. Это связано с тем, что многие SHIELD все еще находится под серьезным развитием и тщательным рассмотрением.

Мы обновим этот технический документ или сделаем новый, в зависимости от того, что мы изменим в будущем. Это не окончательный план развития SHIELD. Кроме того, этот документ будет иметь несколько версий, которые улучшат доступность, читаемость и которые будут предлагать более подробную информацию по вопросам, которые требуют этого.

11 Основные характеристики

Заметка: эти спецификации включают планы на будущее

Мы будем использовать следующие спецификации для ядра SHIELD:

Предмет	Спецификация
Время блока	45 секунд; 240 подтверждений к готовности; SwiftTx/InstantSend
Блок	500 кБ/блок
Блочное вознаграждение	См. Рис. 1
Транзакции/блок	Худший случай[1]: 2777 тр/блок Лучший случай: 14701 тр/блок
Транзакции/секунды	Худший случай: 61 тр/с Лучший случай: 327 тр/с Для графиков см. Рис. 3
Подписи	ECDSA с дополнительным Lamport/Winternitz/BLISS[2] подписями
Штамповка	PoW с помощью x17, blake2s, lyra2rev2, myriad-groestl, и scrypt. PoS Boo с помощью Quark[3] хеш и Slasher схемы
Плата за транзакцию	0.05 XSH за кБ
Особенности конфиденциальности	Tor/I2P nodes, PrivateSend, Zerocoin[4]

Ссылки

[1] Nakamoto, S. (n.d.). *Bitcoin*. Извлечено из https://bitcoin.org/bitcoin.pdf

[2] Buterin, V. (2015). *Understanding Serenity...* Извлечено из https://blog.ethereum.org/2015/12/28/understanding-serenity-part-2-casper/

[3] Vasin, P. (n.d.) *PoSv2* Извлечено из https://bravenewcoin.com/assets/Whitepapers/blackcoin-pos-protocol-v2-whitepaper.pdf

[4] Ben-Sasson, E(2014) *zk-SNARKs* Извлечено из http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf

[1] Наилучший/Худший случай, определяемый количеством входов/выходов в блоке, поскольку входы “тяжелее”, чем выходы

[2] Будет определено позднее

[3] Не окончательный

[4] Не окончательный

[5] cs.jhu.edu, (n.d.) *Zerocoin* Извлечено из http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf

[6] “CryptoRekt”, (2017) *Verge Blackpaper* Извлечено из https://github.com/vergecurrency/Verge-Blackpaper/blob/master/Verge-Anonymity-Centric-CryptoCurrency.pdf

[7] I2P, (n.d.) *I2P tech intro* Извлечено из https://geti2p.net/en/docs/how/tech-intro

[8] Tor, (n.d.) *Tor: The Second-Generation Onion Router Retrieved* from https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf

[9] McAdam, S (n.d.) Shor’s Algorithm Извлечено из https://www.ma.utexas.edu/users/mcadam/monographs/Shor's_algorithms.pdf

Рисунки

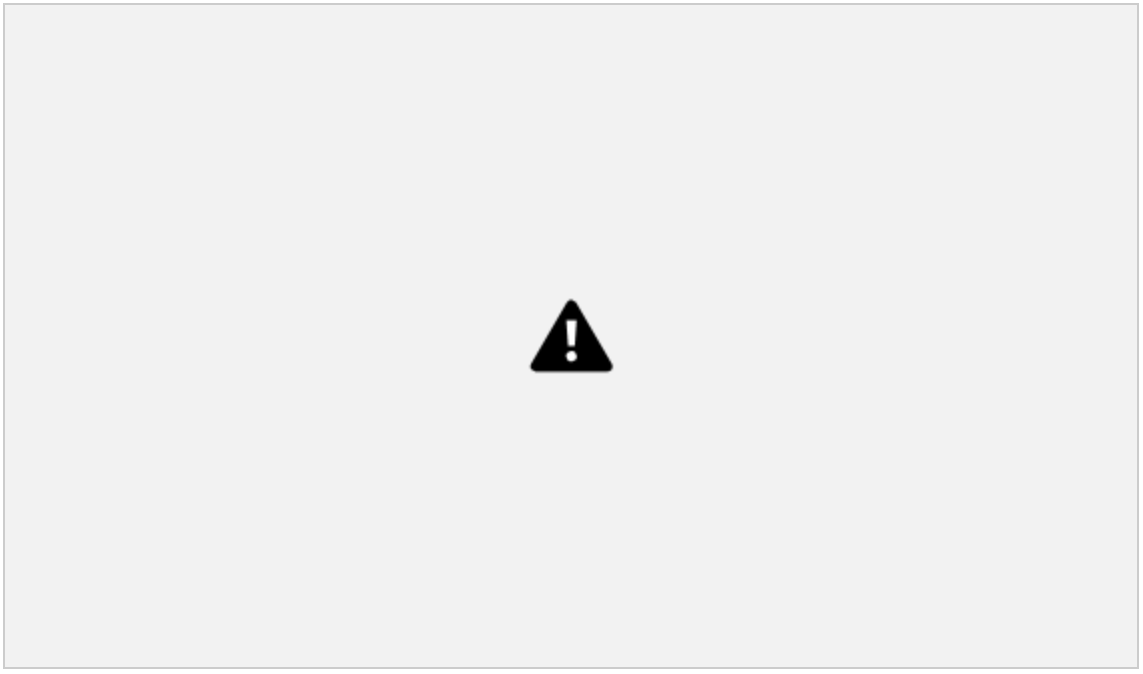

Рис. 1. График койн распределения (y) по блокам (x)

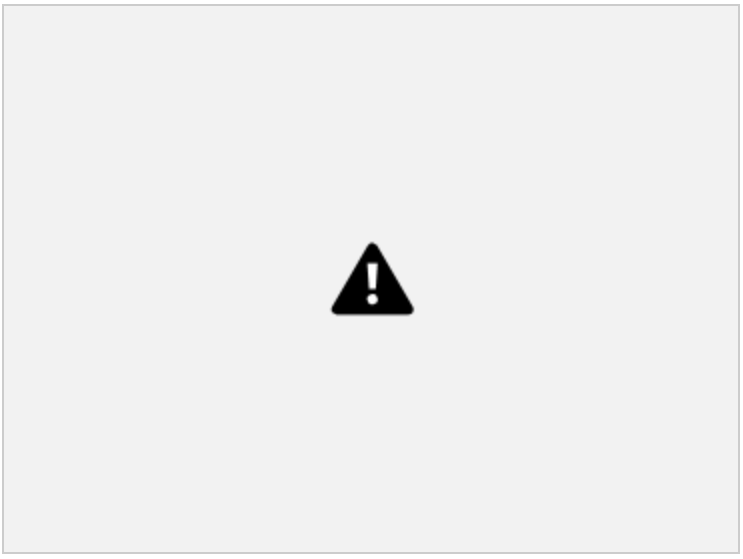

Рис. 2. График потери или выгоды для ставок системы PoS Casper

Рис. 3. 3D-график входов (y) и вывода(x), где z-размер в кБ, худший и лучший случай всегда около Z=500000. Это предполагаемый тип сценария Bitcoin, где блоки должны быть заполнены для обработки как можно большего количества транзакций.