# BOScoin White Paper 2.0

01.11.2018

# Предупреждение

Документ "BOScoin White Paper 2.0" сообщает об основах экосистемы BOScoin и ее планах. Данный документ представляет только планы на будущее с соответствующей информацией, но не гарантирует их выполнение. Любые технические инновации, описанные в данном документе, находятся в стадии разработки и еще не полностью применены, если обратное явно не указано. BlockchainOS не гарантирует успешное развитие и внедрение технических инноваций, а также любой результат деятельности. Информация, представленная в данном документе, получена из надежных источников, однако, гарантия относительно точности, завершенности или адекватности указанной информации не предоставляется.

Команда BlockchainOS (команда BOS) не утверждает и не гарантирует ценность BOScoin. Команда BOS не предоставляет и не гарантирует доход на инвестиции. В максимальной степени, допустимой, действующим законодательством, нормами и правилами, команда BOS, авторы данного документа, советники, и любая третья сторона, вовлеченная в проект BOScoin, не несут ответственность за любые косвенные, прямые, случайные или любые другие виды убытков. Инвесторы несут ответственность за свои инвестиции, связанные с принятием или использованием данного White Paper. Инвестиции должны быть сделаны на основе ваших собственных знаний, исследований, оценок и суждений. Если у вас есть сомнения в отношении действий, которые вы должны предпринять в конкретной ситуации, просим Вас проконсультироваться со своими юридическими, финансовыми советниками, консультантами по налогам или другими профессиональными специалистами.

Информация, содержащаяся в данном документе, может время от времени переводиться на другие языки, использоваться в письменной или устной формах для связи с существующими или потенциальными держателями токенов, партнерами или любыми другими сторонами. В случае возникновения конфликта из- за несоответствия между переведенными версиями и официальной корейской версией, преимущественную силу имеет корейская версия.

Данный White Paper доступен только на сайте компании: https://boscoin.io/. Любая копия или дубликат любой части данного документа без подтверждения компании, могут быть составлены только по предварительному письменному разрешению команды BOS. Данный текст не может быть использован или переписан без предварительного письменного согласия команды BOS. Распространение этого документа может быть ограничено в некоторых странах их законами, регламентами и правилами. Факт владения данным документом является согласием с вышеуказанными условиями.

# Абстракт

Команда BlockchainOS (команда BOS) представляет данный "White Paper" в дополнение к первому White Paper. Расширение бизнеса вокруг блокчейн и рынка криптовалют требуют новых стратегий. Новый проект BOScoin строит глобальную систему финансов. Эта система создания кредитов, управляемая сообществом, планирует изменить существующие экономические парадигмы свежими технологическими и социально - экономическими введениями.

Нынешняя капиталистическая система создала эпоху беспрецедентного богатства за последние 50 лет. Однако, с момента глобального финансового кризиса 2008 года, капитализм, кажется, достиг своих пределов. Как Пикетти (Piketty) лаконично сформулировал в “Капитале в двадцать первом веке" (“Capital in the Twenty -First Century”), усиление экономического неравенства в корпоративной системе, потеря рабочих мест в связи с развитием технологий, снижение потребления, отчуждение финансового суверенитета и т. д. сделают нынешнее общество несостоятельным. Это побудило нас сосредоточиться на трех альтернативах для выхода из существующей экономической системы: крипто экономика, общественное движение и преобразующие инвестиции. Объединив эти три альтернативы с технологией блокчейн, человечество может двигаться вне акционерного капитализма, в котором все богатство находится в руках у нескольких акционеров. Мы хотели бы предложить общественное финансирование (ОФ), которое позволит обществу генерировать кредит и участвовать в демократическом принятии решений. Это эффективный способ использовать ценности, созданные сообществом. Общественное движение смогло выйти за пределы законов о собственности, не отрицая основные принципы капитализма. Аналогичным образом, команда BOS хочет выйти за пределы капитализма самым капиталистическим способом — без отрицания его основных принципов и достоинств. Общественное финансирование — это видение BOScoin; данная модель отличается от других ICO и является основным элементом конкурентоспособной стратегии команды BOS на рынке криптовалют.

Общественное финансирование создает кредит не путем решений, принятых центральным банком или правительством, а через коллективный консенсус лиц, которые пользуются и торгуют реальными кредитами. BOScoin уже ввели систему управления, называемую Конгресс Сети, чтобы дать своим участникам право принимать решение. Сообщество BOScoin может предлагать, просматривать и голосовать за выпуск новых токенов, вступив в сеть Конгресса. Сообщество в целом, а не его избранное меньшинство, обладает финансовым суверенитетом. Эти члены сообщества определяют размер, объем и базовую цену эмиссии, а также условия ее проведения. Решение сообщества исполняются траст контрактами BOScoin. Реальные экономические активы, приобретенные путем эмиссии BOScoins будут

использоваться сообществом в качестве общего достояния, и таким образом общественное финансирование останется "публичным".

Когда в сообществе возникают проблемы, важно, чтобы его члены выражали свое мнение и участвовали. Множество консенсусов, таких как PoS (Proof of Stake) или DpoS (Delegated Proof of Stake), применяемые в некоторых блокчейн проектах, позволяют держателям большего количества монет или акций оказывать большее влияние, доминировать в системе, что, в конечном итоге, приводит к неравенству. Команда BOS стремится реализовать анонимную систему голосования, которая позволяет одному человеку иметь один голос; для осуществления голосования необходимо подтвердить личность.  Команда BOS стремится разработать систему голосования конгрессом на основе технологии гомоморфного шифрования.  Эта технология поможет избежать риски, связанные с захватом ключа и утечкой данных.  Гомоморфное шифрование работает непосредственно на зашифрованных данных без доступа к зашифрованному ключу. Используя это гомоморфное шифрование, команда BOS пытается создать технологию, которая позволяет одному человеку иметь только одну идентичность (singularity) в сообществе, в то же время обеспечивая полностью анонимное голосование внутри сообщества.

Наша цель "взлом капитализма самым капиталистическим путем" позволит преодолеть ограничения существующей капиталистической системы через потенциал крипто экономики и через общественное движение. Общественное финансирование и голосование Конгресса являются важными шагами на пути к достижению этой цели. Содержимое, которое мы не смогли отразить в этом White Paper, крипто - экономическая модель предстоящих планов BOScoin и Generic Trust Third Party (GTTP), будут описаны в следующей редакции.

# Вступление

Мы начали работу над BOScoin White Paper 2.0, чтобы изложить видение BOS команды и BOScoin, не вошедшее в первый White Paper. White Paper 1.0 определил BOScoin в качестве альтернативной модели, чтобы преодолеть ограничения Ethereum. Он представил Конгресс Сети в качестве средства решения технологических проблем и проблем управления траст контрактами. Траст контракты сами по себе решают проблемы безопасности, с которыми сталкиваются смарт контракты и mFBAs (FBAs, которые принимают открытое членство). Экономическая модель под названием Общественный бюджет будет представлена для финансирования экосистемы BOScoin в будущем. Тем не менее, мы заново оценили рынок и развитие нашего бизнеса после ICO и решили, что дополнение к существующей стратегии необходимо. Ядром нашей дополнительной стратегии является Общественное финансирование, в противовес к действующей ICO крипто экономике и голосование Конгресса, реализующее доктрину: один человек - один голос.

Этот White Paper посвящен проблеме, которую команда BOS хочет решить, и наше решение — это “Общественное финансирование”. Как в дальнейшем будет разъяснено в документе, Общественное финансирование будет выполняться путем голосования в Конгрессе Сети. Мы намерены ввести голосование Конгресса на основе разработанного гомоморфного шифрования совместно с Korea Smart Authentication Corp (KoSAC). Мы организуем White Paper 2.0 по этим двум темам. В обновленной версии данного White Paper мы предложим новую концепцию под названием Generic Trust Third Party (GTTP), которая является связующим звеном между BOSNet и внешними данными.

Команда BOS является идейным последователем движения Open Source за открытые источники и его культуры. Мы работаем, веря в то, что технология блокчейн может изменить мир. Работая над последним White Paper, члены команды BOS возрождают наше беспрестанное видение. Какова цель команды BOS? В ответ на этот вопрос, руководитель проекта Yezune сообщил на встречах в Далласе: “В духе Декларации GNU и движения «Создаем общественное», мы хотим взломать капитализм самым капиталистическим способом". Команда BOS не пытается создать платформу для токенов, которая просто использует блокчейн, ни псевдовалюту для конкретной цели. Мы хотим организовать и создать де-факто глобальную систему создания кредитов, которой доверяет мировое сообщество, чтобы успешно заменить существующую капиталистическую систему.

Давайте подробнее рассмотрим проблемы, которые пытается решить команда BOS.

# 1. Введение: Справочная информация

В настоящее время мир переживает самую богатую эпоху с начала цивилизации. Данное изобилие связано с  увеличенем производительности, вызванное не только технологическим развитием, но также созданием кредита капиталистической системой. Эта система способна генерировать кредит на условиях, отличных от тех, что были в прошлом. Конец золотого стандарта 1971 года ввел фиатные деньги, не привязанные к золоту во всем мире, и породил механизм создания кредита.  Преодолев несколько экономических кризисов, которые были представлены как небольшие затруднения, капиталистическая экономическая система стала рассматриваться неуязвимой. Однако эту уверенность сломил мировой финансовый кризис 2008 года.

Нынешняя капиталистическая система не в состоянии распределять богатство. Это указывает на то, что само существование капиталистической системы находится под угрозой, потому что оно продолжает разрушать собственную систему, основанную на потреблении. В то время как перекошенная система распределения вызывает определенные сбои в рыночном механизме, технологическое развитие (особенно информационные технологии) уменьшает потребность в рабочей силе. Это, в свою очередь, снижает трудовые доходы и качество труда. Как капиталистическая система может быть сохранена и поддерживаема, если работники не могут потреблять из-за технологического развития? Если она не может быть сохранена, каковы альтернативы? Это вопросы, которые команда BOS рассмотрит в рамках проекта BOScoin.

В следующем разделе мы подробно рассмотрим проблемы капитализма и проанализируем различные альтернативы, которые пытались преодолеть эти проблемы. Такой анализ альтернатив укажет на новое направление, в котором должен двигаться проект BOScoin. После чего, мы предложим новую крипто экономику для преодоления нынешних экономических проблем.

## 1.1 Понимание текущей экономической модели

### Проблемы распределения, вызванные корпоративными структурами

После промышленной революции капиталистическая система приобрела, несмотря на некоторые трудности, общий опыт, пропорциональный рост доходов и производительность. Это увеличение доходов дало рождение многим потребителям среднего класса с большой покупательной способностью. Экономика продолжала расти, опираясь на процветающий средний класс.  Однако, средний класс в 1980-х и 2000-х испытывал меньший рост доходов, в то время как экономика переживала уверенный рост.  Из-за того, что доход не вырос для рабочего

класса в развитых странах, их потребление поддерживалось за счет введения большего количества низкопроцентных потребительских кредитов. Они смогли покупать все товары и услуги за счет финансирования. Это было названо "финансиализация экономики", тенденция, которая распространилась по всему миру. Благодаря этому механизму, сектор финансовых услуг рос в геометрической прогрессии, и некоторое время экономика казалась быстро развивающейся. За это время сложилась опасная ситуация: капиталисты и люди с деньгами накопили огромные богатства за счет доходов от капитала, в то время как большинство людей попали в долги, чтобы продолжать поддерживать высокую потребительскую активность. Действующий цикл капиталистической системы (так называемый "неолиберализм"), основанный на "финансиализации экономики", создал более фундаментальные проблемы, чем капиталистические системы прошлого. Ипотечный кризис 2008 года был символическим событием, подчеркнувшим все существующие проблемы.

Существует много причин неудачного распределения богатства, но наиболее существенной причиной такого структурного сбоя явился системный упор на максимизацию прибыли акционеров. Корпорация создается и финансируется за счет выпуска акций. Ее основные интересы связаны с распределением прибыли своим акционерам. Именно поэтому большинство корпораций стараются минимизировать производственные затраты и максимизировать цены для потребителей. Они, поэтому стремятся к увеличению производительности на единицу труда; это означает сокращение трудовых затрат. За последние 400 лет — с момента появления первой корпорации — общество, конечно, получило выгоду от инноваций, созданных корпорациями. Однако богатство, генерируемое такими улучшениями производительности, возвращается нескольким акционерам, а не перераспределяется между работниками, которые фактически потребляют произведенные товары и услуги. Корпоративная система не только неудачно распределяет богатство, но также ускоряет экономический спад покупательной способности рабочих. В последние годы, когда информационные технологии стали критически важными, глобальные корпорации переросли в многонациональные корпорации. Эти компании теперь могут сконцентрировать богатство в глобальном масштабе, в отличие от тех, которые ранее ограничивались определенными юрисдикциями (Piketty and Ganser, 2015).

### Централизованное принятие финансовых решений

В капиталистической системе финансы играют решающую роль в создании кредита. Однако, мы признаем невозможность участия в принятии финансовых решений. Учитывая тот факт, что основой финансов является агломерация мелких кредитов от многочисленных простых людей, почему финансовые решения должны принимать несколько финансовых учреждений? Несколько человек контролируют весь процесс принятия всех финансовых решений, а

впоследствии, и прибыль. Проблема этой структуры состоит в том, что в случае сбоев структуры, обычные люди — которые не принимали финансовых решений — несут ответственность. Совокупность решений, которые привели к банкротству Lehman Brothers является прекрасным примером. Решения были сделаны небольшой группой финансистов, но последствия этих решений разделили само общество — что было источником кредита. Другим примером является то, как банки создают кредиты через коммерческие займы; решение об их предоставлении также принимают единичные финансисты. Предложение, выгравированное в первом блоке Bitcoin “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks". (Times, 3 января 2003, Канцлер стоит на грани второго спасения для банков) (Times, 2003, January), точно определило явление, когда общественность лишена финансового суверенитета.

Конечно, любой может участвовать в экономике в качестве акционера корпорации. В нынешней финансовой системе, однако, большинству людей не предоставляется возможность участвовать в качестве акционеров. Возьмем, к примеру, текущую экосистему стартапов, которая создана для того, чтобы быть высоко рискованной, но иметь потенциал к созданию высокой прибыли через M&As и IPO. Стартапы растут за счет венчурных инвестиций. По мере их дальнейшего роста, больше капитала инвестируется через фонды прямых инвестиций и инвестиционные банки.  На основе этих средств стартап может достичь статуса глобальной платформы, как, например, Google и Facebook, и, в конечном итоге, начать торговаться на фондовой бирже. Только тогда публике разрешают получить кусок от пирога.  До размещения на бирже, инвестиции осуществляются исключительно несколькими венчурными капиталистами, менеджерами фондов прямых инвестиций и инвестиционными банкирами. Да, существует высокий инвестиционный риск, но публике запрещен прямой доступ к потенциалу высоко прибыльного капитала.

Как только рынок P2P кредитов и краудфандинга, а также ФинТех в целом, начал расти в 2016 году, основные страны, такие как США, установили индивидуальные инвестиционные лимиты для P2P-кредитов и краудфандинга. Возможность для индивидуалов принять риск инвестирования и получать высокие проценты на инвестиции забрали во имя "защиты инвесторов". С одной стороны, государство обязано защищать людей, с другой стороны, это необоснованное регулирование финансовых решений, принятых обществом. Существуют различные инструменты для стимулирования широко освещаемых инвестиций и, по-прежнему, присутствуют возможности. Например, Россия недавно установила максимальную сумму в долларах для участия в ICO широкой общественности и требует, чтобы физические лица прошли курс обучения в признанном учреждении для получения права увеличивать суммы инвестиций за пределами максимума. Даже на рынке ICO есть похожие попытки, например, потолок индивидуальных инвестиций для предотвращения участия общественности.  Таким образом,

можно утверждать, что при любом капиталистическом и либеральном экономическом порядке рядовой работник и гражданин не имеет “финансовой независимости”.

### Развитие информационных технологий снижает потребность в рабочей силе

В индустриальную эпоху ключевыми факторами производства были земля, капитал и труд. По мере развития индустриализации, управление и технология росли даже более значительно, и сегодня они стали ключевыми факторами производства. Изменения во время 1980-х и 2000-х были значительны, из-за огромных достижений в технологии. В отличие от прошлого, когда технологии дополняли и повышали производительность труда (Brynjolfsson and Saunder, 2009), автоматизация сегодня заменяет рабочие места во всей экономике; такое замещение работников технологиями может усугубить разрыв между доходами капитала и доходами труда. (Brynjolfsson, and McAffee, 2014).

Как показали котировки акций современных глобальных платформенных корпораций (таких как Amazon, Google, Facebook, Uber, Airbnb и т. д.), индустрия информационных товаров и технологий, которая использует информацию как ключевой фактор производства, становится все более влиятельной (Cusumano, 2017_1; Cusumano 2017_2). Компании, которые производят физические продукты, также используют информационную технологию для того, чтобы совершенствовать товары широкого потребления. Например, Nike улучшает свою продукцию, представляя товар с данными по состоянию здоровья. По прогнозам, эта тенденция сохранится. Корпорации будут использовать такие технологии для увеличения капитала акционеров и замены рабочей силы. Кроме того, корпорация, которая не поступит подобным образом, останется позади всех.

Посреднические ИТ корпорации на платформах масштабируются от эффекта положительных внешних факторов, т.н. информационных товаров. Например, когда пользователь на веб-сайте Amazon покупает цифровую камеру, одежду или книги его выбор записывается и используется для помощи в выборе другим пользователям Amazon. В экономике акционерного капитала, большинство богатства, созданного с помощью таких информационных товаров, забирается предприятием и впоследствии его немногочисленными акционерами. В то же время, эти ИТ инновации разрушают ранее существовавшие отрасли и рабочие места. Уничтожение Amazon розничной торговли в США было настолько эффективно, что вызвало банкротство многих небольших независимых розничных торговцев. За это время Amazon создал лишь несколько высококвалифицированных ИТ-рабочих мест. Парадоксально, но потребители, которые способствовали росту Amazon, теряют работу из-за него. Новые технологии, связанные с искусственным интеллектом и большими объемами данных, только ускоряют эту тенденцию, этот тренд сохраняется.

В целом, информационные товары и технологии стали гораздо более важными факторами производства, чем традиционные факторы, такие как земля, капитал и труд. Информационные товары и технологии легко копируются и имеют минимальные затраты в производственном процессе. Из-за этих атрибутов информационные технологии продолжают повышать производительность и снижают потребность в рабочей силе. Информационная технология имеет тенденцию к замещению человеческого труда для ускорения окупаемости инвестиций. Рабочие места остаются в областях с низко окупаемыми инвестициями — часто это самая низкооплачиваемая работа. Более того, как только информационная технология все более глубоко развивается и способствует быстрой окупаемости инвестиций, процесс повторяется и в низкооплачиваемых работах. ИТ компании на платформах предоставляют услуги для улучшения опыта пользователей, но такие инновации уменьшают потребность в рабочей силе и уничтожают существующие индустрии. Эта перспектива предлагает совершенно новый масштаб экономических кризисов, с которыми мы столкнулись.

### Три проблемы и направление новой экономической системы

Мы считаем, что “новая экономическая система” должна быть способна решить три вышеуказанные проблемы. Другими словами, необходимо не только использовать силу кредитной генерации капитала, но и 1) преодолеть проблемы акционерного капитализма и предоставить возможность каждому участвовать на рынке, 2) позволить тем, кто обеспечивает кредит для экономики, участвовать в принятии финансовых решений, и 3) определить систему производства как общественный ресурс, если производство требует или использует потребительскую активность, но не приносит пользы потребителям.

Ученые предложили введение международного стандарта налогообложения капитала и базового дохода для решения фундаментальных проблем капитализма. Эти предложения требуют смелого и прагматичного политического принятия решения. Однако, другие подходы — альтернативы, не требующие политических решений — уже здесь. Давайте взглянем на эти подходы.

## 1.2 Альтернативы нынешней экономической системе

Существует много альтернатив современной экономической системе, но мы здесь рассмотрели те, которые вдохновили нас на создание нового видения: криптовалюта, общественное движение и преобразующие инвестиции.

### Криптовалюта

В 2017 году, интерес к рынку криптовалют распространился по всему миру. Экономическая система, основанная на криптографии, названная криптовалютой, частично становится альтернативной экономической системой. Большинство крипто проектов являются 1) децентрализованными через технологию блокчейн, 2) организованными для вознаграждения участникам экосистемы через криптовалюты (экономика токенов) и 3) в отличие от существующих инвестиционных схем; ICO (Первоначальное предложение монет) предоставляют легкую возможность любому стать инвестором. Данные черты могут потенциально преодолеть проблемы акционерного капитализма, поэтому криптовалюты становятся альтернативой корпоративной системе. Эти три характеристики соответствуют нашим условиям “новой экономической системы", рассмотренной выше — низкий барьер для участия, коллективное принятие решений и совместное использование средств производства. С должным оптимизмом криптовалютный рынок значительно вырос в 2017 году. В прошлом, стартапы возникали в рамках инвестирования венчурного капитала (ВК). На данный момент существует много стартапов, которые запустили ICO, и многие венчурные капиталисты предпочитают инвестировать в эти проводящие ICO стартапы.

BOScoin представляет Конгресс Сети для усиления силы участников по принятию решений, но ни BOScoin, ни большинство криптовалют в достаточной мере не удовлетворяют трем условиям “новой экономической системы”. Вопрос о совместном использовании средств производства зачастую даже не рассматривался. Есть движение, однако, которое поддерживает, что система производства, созданная глобальным сообществом, является общественным ресурсом и должна предоставлять доступ каждому. Это называется Общественное движение.

### Общественное движение

Бюджет, представленный в White Paper 1.0 BOScoin, является общественным бюджетом, а не общим бюджетом. Общественный бюджет еще не имеет четкого определения и стратегии действия, но он был создан в духе общественного движения. Общественное относится к культурным и природным ресурсам, доступным для всех членов общества, включая природные элементы, такие как воздух, вода и земля. Эти ресурсы не частные, а находящиеся в совместной собственности, и общественное управляется сообществом для личного и коллективного интереса. Среди этих движений, были попытки организовать информационные товары и технологии как общественную собственность коллективного общества. Знаменитые примеры таких движений это GNU и Creative Commons.

Если информационные товары и технологии составляют значительную часть добавленной стоимости продукта, то следует рассмотреть следующие два вопроса. Во-первых, должны ли

компании монополизировать информационные товары и технологии пока накапливают богатства, создаваемые благодаря им? Более того, когда значение ИТ к добавленной стоимости растет, отсутствие рабочих мест разрушает потребительский рынок, и вся экономика находится в депрессии, должна ли добавленная стоимость, создаваемая за счет информационных товаров и технологий, использоваться совместно с сообществом? Общественное движение, которое толкует информационные технологии и производственные системы, как "общественные", может быть важным шагом на пути к рабочей общественной системе, использующей совместную собственность.

Если сообщество соглашается с тем, что определенный ресурс является общественным, доход, полученный от использования общественного ресурса, должен совместно использоваться сообществом. Это фундаментальная и эффективная альтернатива порочного круга умирающей потребительской базы и падения трудовых доходов.  Мы проанализируем Общественное движение в пункте 1.3 и представим наше предложение, чтобы сделать эту философию успешной.

**Преобразующие инвестиции (импакт – инвестиции)**

"Преобразующие инвестиции" предоставляют собой такие инвестиции, которые не только приносят доход, но и социальную ценность. Пока обычные инвестиции фокусируются на экономических и финансовых показателях, импакт - инвестиции относятся к инвестициям, выходящим за рамки и учитывающим социальные и экологические последствия. Это попытка решить социальные проблемы через бизнес — признавая, что сложно решить социальные проблемы только за счет государственных бюджетов. Например, в 2012 году Goldman Sachs инвестировал $ 9,6 млн. в проект по снижению уровня рецидивов среди молодежи в Нью-Йорке. Есть и другие активные инвестиции в подобные проекты. Преобразующие инвестиции также является формирующимся трендом в Корее. Например, фирмы венчурного капитала, такие как Korean Social Investment и Yellow Dog активно участвуют в импакт - инвестировании. Есть также компании девелоперы и управляющие компании, такие как 00Ground, чья миссия состоит в том, чтобы превратить свои здания в независимые платформы для решения социальных проблем, создавая ценности и прибыль.

Импакт - инвестирование является хорошим способом для сообщества обеспечить общественное достояние, но, если оно осуществляется избранным меньшинством, это, безусловно, не самое эффективное решение проблем современной экономической системы. Однако, ясно, что преобразующее инвестирование может увеличить социальные показатели.

## 1.3 Анализ альтернатив и новое направление

Мы увидели, что криптовалюта и общественное движение представляют решения для новой экономической системы. В разделе 1.3 мы проанализируем ограничения современного общественного движения и крипто экономики и обсудим, как совместить преимущества этих двух альтернатив.

### Деньги и коммерция как общественное движение

Благие намерения и практическая польза являются двумя независимыми величинами. Общественное движение стремится расширить общественный P2P метод производства; но может ли этот подход достичь идеалов общественного движения?

Если общественное движение хочет быть больше, чем государство и рынок, то общественное движение должно конкурировать на рынке в государственном или в глобальном масштабе. Например, предположим коллективная платформа была создана для решения проблем, вызванных Uber. Сможет ли эта платформа пережить конкуренцию с Uber? Смогут ли P2P системы производства конкурировать с продуктами, созданными роботами? Мы осмеливаемся сказать, что это не будет легко. Мелкомасштабным производителям будет трудно наверстать упущенное и влиять на экономику.

Конечно, коллективное P2P производство является эффективным в определенных сферах. Есть две известных истории успеха общественного движения: GNU и Wikipedia. У этих двух проектов были общие черты: 1) оба проекта с самого начала имели четко определенных участников и энергичных вкладчиков, 2) эти проекты были невозможны без крупномасштабного сотрудничества, и 3) они были структурированы для того чтобы дать вкладчикам не только репутацию — изначальный стимул — но и экономические стимулы, основанные на этой репутации. Это привело к появлению продукции с качеством, сопоставимым с качеством обычных капиталистических компаний. Так как эти сходства способствовали успеху? Первое сходство — иметь четко определенных участников и вкладчиков — это условие, а не метод для достижения успеха. Третье сходство — это то, что использование репутации в качестве экономического стимула также является недостаточно большим мотивом для участников. Мы считаем, что основополагающим механизмом, с помощью которого эти два проекта увенчались успехом, было то, что они мобилизовали крупномасштабное сотрудничество, которое существующие капиталистические компании не смогли воспроизвести. Это означает, что залогом успеха общественного движения является сотрудничество между большим и более разнообразным числом лиц, чем это могут сделать существующие капиталистические предприятия. Вряд ли все сферы жизни общества смогут стать предметом общественного

движения (по крайней мере, пока общественное движение не сможет занять доминирующее положение в обществе). Причина этому в том, что не все области подходят для крупномасштабного сотрудничества. Также необходимо иметь надежные, стабильные инструменты, чтобы гарантировать участие каждого человека.

Итак, мы задаемся вопросом - решая проблемы капитализма, в каких областях общественное движение может быть наиболее эффективным? Мы рассматриваем финансы как идеального кандидата для общественного движения. Как уже освещалось раннее, если мы не сможем решить основополагающие вопросы капитализма и финансов, стабильное поддержание современного уровня достатка невозможно. Исторически, особенно для совместного кредитования в финансовом секторе существовало крупномасштабное сотрудничество среди простых граждан. Однако отсутствие технологии затруднило организацию глобального широкомасштабного сотрудничества, такого как GNU и Wikipedia. Тем не менее, блокчейн и крипто экономика смогут построить доверие среди граждан, способствующее глобальному широкомасштабному сотрудничеству. Таким образом, мы можем генерировать больше кредитов, чем финансовые институты. Кроме того, мы считаем, что можно будет создать кредит в больших масштабах на основе крипто экономики и сделать общественными эти средства производства. BOScoin уже создал Общественную концепцию путем введения Общественного бюджета. Однако, мы считаем, что методология, представленная в White Paper 1.0, была недостаточной для изложения этой цели. Сейчас мы обсудим и дополним этот пробел обзором текущего состояния крипто экономики.

### Современные проблемы крипто экономики и наше предложение

Ограничения современной крипто экономики с точки зрения технологий очевидны: медленная скорость обработки транзакций, небезопасная среда разработки смарт-контрактов, которая приводит к частым случаям взлома, программный код, который оставляет контракты недоступными публике и т.д. Однако, предполагается, что технические проблемы криптовалют будут решены в обозримом будущем. В первом White Paper мы представили альтернативу этим техническим ограничениям через mFBA и траст контракты. Мы верим, что техническая стратегия White Paper 1.0 остается в силе, она находится в разработке. Таким образом, в этом White Paper будут рассмотрены стратегии и политика современного рынка криптовалют с социально - экономической точки зрения больше, чем со стороны технических и аналитических проблем.

1) ***Волатильность цены*** *из-за установленного лимита выпуска.* Большая волатильность цены криптовалюты частично зависит от роста рынка, но больше от ожидаемой нехватки криптовалюты из-за установленного лимита выпуска. После финансового кризиса 2008 года центральные банки безрассудно печатали фиатные деньги (количественное смягчение) и Bitcoin

стал ответом на снижение стоимости фиатных валют. Bitcoin был разработан с предопределенным общим количеством выпуска монет и децентрализованной денежной системой. Он стал альтернативой существующим фиатным валютам, валютой в крипто сообществе. Криптовалюта стала привлекать внимание благодаря одному конкретному механизму: дефицит увеличивает стоимость криптовалюты, участники увеличиваются с увеличением стоимости, и цикл повторяется ("механизм дефицита"). Кроме того, Ethereum расширил масштаб применения приложений на блокчейн в 2016 году, следовательно, количество и капитализация криптовалютных проектов во всем мире значительно возросло. Механизм дефицита работает как инвестиция, стимулирующая участие в экосистеме криптовалют, но вызывает большие колебания цен на криптовалюту. Волатильность криптовалют является барьером для выполнения денежных функций. Если цена пойдет вверх, одна сторона захочет сохранить криптовалюту и, если цена идет вниз, другая сторона будет неохотно принимать ее. Для того, чтобы решить эту проблему, различные попытки — например, создание стабильного по стоимости токена, привязанного к фиатной валюте — были сделаны, но они не нашли фундаментальных решений. Волатильность усложняет экономические экосистемы даже с одной криптовалютой, проблема становится более комплексной, когда несколько криптовалют используются одновременно. Давайте рассмотрим эту проблему через Dapp - ICO стратегию платформ криптовалют.

2. *Разделение денежного пространства ICO.* Когда Ethereum предоставил возможность выпуска токенов для Dapps (децентрализованных приложений), были запущены многочисленные ICO на основе токенов ERC20. Кроме того, Ethereum недавно представил DAICO, чтобы решить проблемы, возникшие из-за взлома DAO. Стратегия Ethereum - позиционировать себя как платформу для выпуска токенов. Другие платформы, даже те, которые пытаются превзойти Ethereum, используют похожие стратегии Dapp. Данная стратегия подходит для первоначального роста платформы. Большинство платформ на основе консенсуса имеют ограниченные возможности, но они эффективны для начального привлечения капитала. BOScoin также однажды согласился с этой стратегией и применил ее в White Paper 1.0.

Однако, мы считаем, что стратегия Dapp - ICO, скорее всего, сократит денежное пространство крипто платформ путем разделения пользователей и продавцов. Деньги концептуально похожи на платформу тем, что они приобретают ценность только тогда, когда они широко используются — покупателями, держателями и инвесторами. В настоящее время, стратегия Dapp - ICO разделяет денежное пространство, даже если использует один и тот же ресурс крипто сети. Несмотря на удобство инвесторов использовать биржу, покупателям очень неудобно пользоваться различными криптовалютами в повседневной жизни. В настоящее время большинство держателей криптовалют не станут жаловаться на появление различных

криптовалют, потому что им свойственно рассматривать криптовалюту как цифровой актив. В будущем, однако, мы предвидим, что разделение денежного пространства, вызванное стратегией Dapp - ICO, станет основным препятствием для подъема криптовалют до статуса фиатных денег. Стратегия Dapp - ICO кажется благоприятной в краткосрочной перспективе, но она не сопоставима со статусом фиатной валюты.

3. ***Разделенная система создания кредитов.*** В целях предотвращения разделения денежного пространства, BOScoin предложил развитие Dapp через общественный бюджет. После общения с многими потенциальными партнерами, мы обнаружили, что партнеры больше заинтересованы в создании кредита через ICO, нежели в использовании самой платформы BOScoin. Мы также выяснили, что платформа может быть вторичным компонентом для некоторых индустрий. Кроме того, размер кредита, который им был нужен, был слишком большим, чтобы соответствовать общественному бюджету. (Детали общественного бюджета и его использования будут описаны позже в следующей версии White Paper 2.0). Существующие законные валюты выпускаются Центральным банком, а кредит создается совместным банковским резервом коммерческих банков. Таким образом, коммерческие банки имеют масштабированный механизм создания кредита, который создает добавочный кредит, основанный на созданных кредитах. Эта система создания кредитов на основе фиатных средств является ядром финансового капитализма. В настоящее время крипто экономика не имеет такой системы создания кредита; ICO сначала создают кредит, но нет непрерывного цикла. Также сложно для платформ на основе консенсуса отправлять кредит, созданный одним Dapp - ICO другому Dapp - ICO. Другими словами, крипто экономика не в состоянии превзойти капиталистическую систему создания кредита. Для расширения крипто экономики и обгона существующей капиталистической кредитной системы, необходимо заменить стратегию Dapp - ICO.

4. ***Проблема централизации.*** Большинство криптовалют объединены в сеть экономическими стимулами. Вначале Bitcoin славился своей децентрализацией, но вся сеть находится под контролем тех, у кого больше мощностей хеша. Сделки с низкой комиссией постоянно помещались в ситуацию, когда подтверждения были нестабильными и узлам приходилось платить высокую комиссию за своевременную обработку транзакции. Возникла ситуация, полностью отличающаяся от ожиданий крипто экспертов, которые утверждали, что операционные издержки будут снижены с децентрализацией. Ожидается, что методы PoS или DPoS также вызовут проблемы централизации, аналогичные PoW. Проект EOS, к сожалению, подтвердил это предположение. Сеть начинает становиться централизованной, как только процесс консенсуса зависит от экономических стимулов. Это не то, что мы хотим видеть в экономике криптовалют. Кроме того, криптовалюта без системы управления сталкивается с

очень сложной ситуацией в решении проблемы централизации. Проблема централизации – это то, что даже компания BOScoin, которая имеет структуру управления, должна эффективно преодолеть. (Решение этой проблемы будет рассмотрено в следующей версии White Paper 2.0).

# 2. Предложение

Кратко суммируем содержание введения. В современной капиталистической системе важное значение имеют информационные товары и технологии. Трудовые доходы уменьшаются, а богатства не распределяются. Это разрушает потребительскую базу, от которой зависит капитализм. Нам нужна система для решения проблемы распределения и действующая крипто экономика является наиболее подходящим решением для этой проблемы. Тем не менее, одна из стратегий крипто экономики, под названием Dapp - ICO скорее всего приведет к разделению системы создания кредита, и в итоге не сможет решить капиталистическую проблему, которую намерена решить команда BOS.

*Общественное финансирование.* Для решения проблемы разделенной системы создания кредитов, вызванной стратегией Dapp – ICO, мы предлагаем общественное финансирование (ОФ). ОФ позволит людям, которые используют и торгуют реальным кредитом принимать коллективные решения по созданию кредита. В отличие от навязываемых решений Центрального банка или Правительства, сообщество создает свой собственный кредит. В отличие от других крипто платформ, BOScoin может предложить ОФ, потому что он имеет систему управления, называемую Конгресс Сети. В капитализме институциональная финансовая система содержит основной капитал и основные полномочия по принятию решений; большинство членов системы покорно следуют решениям, принятым другими. Также сложно выйти из системы. С другой стороны, многие криптовалюты, включая BOScoin, являются валютами сообщества. Если валюта не отражает голосов своих членов, сообщество завянет и умрет. Криптовалюта может вырасти в деньги сообщества, если мотивирована консенсусом сообщества. Таким образом, криптовалюта должна иметь возможность предложить структуру управления, подходящую большинству сообщества. Конгресс Сети, предложенный в White Paper 1.0, разрешал тем, у кого много узлов — больше средств — иметь больше влияние на принятие решений. Чтобы решить эту проблему мы внедряем систему один человек - один голос. Система один человек - один голос может быть не лучшим методом решения проблемы плутократии, но она является наиболее подходящей системой управления на данный момент. Принцип один человек – один голос невозможно применить без идентификации личности, что в свою очередь, ставит под угрозу принцип конфиденциальности и свободы волеизъявления. На момент написания White Paper 1.0 мы не смогли найти решение этой проблемы и процесс принятия решения Конгрессом сети остался без ответа. Мы проанализировали эту проблему с KoSAC и рассмотрели возможность создания форм голосования Конгресса с использованием гомоморфного шифрования. Это подробно описано в разделе 2.2.

## 2.1. Общественное финансирование

### Предпосылки

До сих пор мы описывали предпосылки для введения ОФ.  В резюме, мы оценили, что крипто экономика является, среди множества альтернатив современной экономической системе, наиболее эффективной в использовании механизмов создания кредита и решении проблем распределения. Тем не менее, стратегия Dapp - ICO современной экономики криптографических токенов не является подходящей альтернативой капиталистической системе, потому что она изолирует и разделяет денежное пространство.

### Определение и значение

ОФ означает сообщество BOScoin, выпускающее дополнительные BOScoins в качестве средства создания кредита для приобретения различных активов реального сектора экономики. Кредит создается сообществом, а не инвестируется третьей стороной за пределами сообщества. Само сообщество предлагает, рассматривает и голосует за дополнительный выпуск токенов через Конгресс сети. Это решение реализуется через траст контракты BOScoin. Мы определяем этот процесс как Общественное финансирование (ОФ).  Активы и доходы от их использования, полученные сообществом благодаря ОФ, не будут распределяться между членами сообщества. Сообщество использует и управляет активами и доходами от них путем решений, принятых Конгрессом Сети.

Отличие от раннего предложения с общественным бюджетом: Во-первых, в дополнение к предопределенному плану выпуска, сообщество выпускает дополнительные монеты через коллективное принятие решения. Во-вторых, если общественный бюджет концептуально аналогичен затратам, то ОФ следует рассматривать как аналогию инвестициям. В-третьих, когда BOScoin выпускается для инвестиций в ОФ, общественные активы BOScoin (the commons) увеличиваются в стоимости, чтобы соответствовать выпущенному объему. Наконец, Общественный Бюджет был моделью, которая не предусматривала использование активов, а основная цель ОФ - использование активов, и это использование должно быть разумным. Потому что без планирования будущей прибыли члены не заинтересованы в внедрении ОФ внутри BOSnet.

Термин "общественное финансирование" был создан в противоположность проектному финансированию — вершине финансового капитализма — и финансирование является "общественным" в двух отношениях.

Во-первых, члены сообщества имеют силу — финансовый суверенитет — принимать финансовые решения. Здесь слово "общественный" означает не просто проинвестированный в общественные товары, но ближе к деньгам, созданные общественным консенсусом. В отличие от проектного финансирования, которое осуществляется традиционными финансовыми институтами, воля сообщества и его решения создают кредит для общественного финансирования. Это решает долгосрочную проблему "финансового суверенитета", которая рассматривалась во введении. Общественный консенсус возможен, потому что BOScoin имеет систему управления, названную Конгрессом сети.

Во-вторых, богатство, производимое через приобретение реальных экономических активов — общественные товары— будет рассматриваться, как общественный ресурс с экономической точки зрения. Общественное финансирование является "общественным", потому что общественные товары приобретенные посредством ОФ и богатства, созданные этими общественными товарами, будут использоваться для сообщества BOScoin. Мы считаем, что это может решить фундаментальную проблему, как капитал и технологии вытесняют трудовой доход.

Предложение ОФ, представленное сообществу Конгрессом сети, вероятно, будет включать цель и ожидания проекта, размер и условия выпуска монет, методы использования, а также планы реинвестирования для устойчивой экономической системы. Каждое предложение ОФ опишет конкретный инвестиционный план; однако, план не должен включать в себя займ денег или что-то аналогичное займу. Если заявители, которые будут включены в Сеть BOScoin, нуждаются в финансовой поддержке по мере необходимости, поддержка должна быть беспроцентной. ОФ является видением BOScoin, идентичностью и конкурентной стратегией на крипто рынке. ОФ также является механизмом построения экосистемы для Generic Trust Third Party (GTTP), участника сети BOScoin, который будет представлен в следующей версии White Paper 2.0.

Чтобы получить реальный опыт ОФ, мы планируем пилотный проект ОФ в разумных масштабах и создание реалистичного плана. Пилотный проект предоставит сообществу подробный процесс, а также данные для улучшения качества принятия решения перед запуском процесса голосования Конгресса сети. Пилотный проект выполняется как реверсивная партнерская программа ICO (RIPP)

### Реверсивная партнерская программа ICO

ОФ можно разделить на несколько категорий в соответствии с его назначением: ОФ МСП (малых и средних предприятий) для инвестирования, поощрительное ОФ для вознаграждения сообщества, инфраструктурное & системное ОФ для строительства BOScoin инфраструктуры.

Среди этих категорий ОФ МСП необходимо проводить на основе проверки бизнес-модели (BM) компании, цели, потенциала и способности объединиться с BOScoin. Мы разработали реверсивную партнерскую программу ICO (RIPP) для осуществления верификации. RIPP будет включать реверсивный ICO процесс, в котором можно проверить целевую компетентность компаний. В зависимости от результата реверсивного ICO, компания может быть включена в сообщество BOScoin путем голосования Конгресса.

## 2.2. Голосование Конгресса

**Предпосылки**

Блокчейн является технологией протокола, построенной, чтобы быть децентрализованной, неизменной, бесперспективной и беспартийной. Таким образом, блокчейн был отмечен как “управление через инфраструктуру” (Sclavounis O. 2017). Но даже в блокчейн проектах предусмотрена роль человека. Создание и управление системой осуществляется различными заинтересованными сторонами в сообществе, которые можно рассматривать в качестве «управления инфраструктурой» (De Filippi, P. & Loveluck, Б., 2016). Способность BOScoin само развиваться управляется “человеком”; здесь, “само развитие” состоит из коллективного обсуждения и принятия решений.

Каждое блокчейн сообщество имеет два уровня управления (Myungsan Jun, 2018). Консенсус в реестре блокчейн работает по принципу прямой демократии. Все узлы могут участвовать в равной степени, подтверждать и одобрять транзакцию. Будет ли соглашение заключено 51% или 67% - дело вкуса. Ключевая идея заключается в том, что все участвующие узлы получают равные права и возможности для достижения консенсуса. На втором уровне управления, однако, ранние крипто проекты либо не имели, либо имели слабо проработанный процесс принятия решений. Если процесс существовал, механизмы главным образом были предусмотрены вне сети блокчейн. Блокчейн имеет свои основы в логике принятия решений (вычислительная "хеш-мощность"). С момента того, как майнинг, как бизнес стал масштабироваться, естественная логика вычислительной монополии неизбежно привела к тому, что крупные майнинг операторы захватили наибольшую мощность и прибыль (Ehrsam F., 2017). Другие члены, такие как пользователи и разработчики, были исключены из распределения благ.

Проблема заключается не только в централизации. Когда система ухудшает качество или уменьшает преимущества для своих членов, членам не остается выбора, кроме как покинуть сеть (либо путем перехода к другому проекту или проведением хардфорка), что ведет к снижению эффективности сети (Albert O. Hirschman. 1970). Если у всех участников есть канал для участия и внесения изменений для увеличения своей прибыли, сообщество сохранит больше членов. Это

также полезно для развития сообщества, чтобы лучше понять проблему и предоставить больше возможностей для решения проблем. Эффективная система управления может лучше включать и увеличивать голоса участников своей сети (Duncan L., 2017).

Крипто проекты признали это и стали внедрять различные механизмы, такие как голосование мастер узла, DGBB (децентрализованное управление бюджетом блокчейн) (Wiecko Robert., 2018) и системы голосования, основанные на равноправии. Это усилие добавило дополнительный децентрализованный уровень к “управлению инфраструктурой”. Однако, такая система является плутократией, в которой те, кто обладает ресурсами, оказывают большее политическое влияние. Так как несколько богатых человек доминируют в системе, сообщество, вероятно, сместиться к модели, в которой все больше благ распределяется в пользу богатых. Это создаст само-укрепляющуюся систему с растущим материальным неравенством и приведет к тому, что рядовые члены станут все больше отдаляться от создаваемых ими ценностей.

Если мы считаем, что все участники сети должны быть одинаково представлены, то сеть должна определить каждого человека. Без этого процесса, сеть уязвима для атаки Сибиллы. Атака Сибиллы являются атаками, которые создают несколько фальшивых личностей, чтобы оказывать чрезмерное влияние на P2P сеть. Однако, сбор личной идентификационной информации нарушает конфиденциальность пользователя. Если нет решения, которое может подтвердить существование и личность пользователя без ущерба его конфиденциальности и свободы при «управлении инфраструктурой», невозможно окончательно решить все существующие проблемы блокчейна.

### Определение

Децентрализованное и демократическое "управление инфраструктурой" BOSnet будет осуществляться через платформу так называемым Конгрессом сети. Конгресс сети будет полнофункциональным органом BOSnet для демократического принятия решения. Сеть введет современное решение для шифрования, которое идентифицирует участников, обеспечивает полную анонимность и предотвращает атаки Сибиллы. Сеть имеет несколько уровневую систему принятия решений, созданную для того, чтобы максимизировать мудрость толпы (Surowiecki J., 2005) и представить ее наиболее законным способом, наилучшим образом, отражающим разнообразие и независимость суждений. Децентрализация произойдет на всех уровнях формирования расписания, представления предложений, содействия обсуждению и голосования. Во время осуществления голосования Конгресса в BOSnet, персональные данные будут обрабатываться как описано в этом документе и в соответствии с применимыми законами “О защите данных”.

### Гомоморфное шифрование

Полное гомоморфное шифрование, или гомоморфное шифрование, является формой шифрования, первоначально созданной Rivest, Adleman и Dertouzos в 1978 году и впервые примененной Craig Gentry в 2009 году. Гомоморфное шифрование отличается от обычных методов шифрования тем, что может работать непосредственно с зашифрованными данными, не требуя доступа к закрытому ключу. (Homomorphic Encryption Standardization homepage, 2018). С другой стороны, существующие методы шифрования требуют, чтобы секретные ключи хранились на сервере, где выполняются вычисления, или чтобы данные преобразовывались из зашифрованных в текстовые. Это может привести к потере ключа или простой утечке текстовых данных.

Асимметричный шифр

E= (KeyGen, Encrypt, Decrypt)

Можно считать гомоморфным, если возможны следующие операции:

Запуск “+” арифметических операций в сообщении (возможны и другие операции, такие как умножение)

Вывод нового шифро текста “s”, запустив “+” алгоритмы на открытом ключе “pk” и шифро текстах “c1” и “c2”

Это верно, когда все сообщения "m1", " m2” дают "d = m1 + m2".

(pk, sk) ← KeyGen(); c1←Encrypt(pk, m1); c2 ← Encrypt(pk, m2);

f(c1, m2)= Encrypt{f(m1, m2)}(Bernhard D., Warinschi B., 2014)

### Членство

Для того, чтобы принять участие в Конгрессе сети, необходимо сначала получить членство в Конгрессе. Любой желающий может стать членом конгресса. Национальность и пол не имеет значение. Любой в сообществе BOScoin может убедиться, что внести вклад в BOSnet очень просто.  Кроме того, идентификации каждого участвующего в процессе управления помогает предотвратить атаку Сибиллы. Но, это не означает, что необходимо знать полную идентификацию личности каждого, кто участвует в системе.  Все, что нам нужно знать, это то, что личность принадлежит реальному человеку, который является единственным, уникальным членом сети. Наша цель - минимизировать требования к персональной информации — максимизировать конфиденциальность — и в то же время обеспечить уникальность личности. Идентификационный счет будет сформирован на блокчейн, и пользователь получит токен, чтобы доказать, что владелец является уникальным членом Конгресса сети. Счету присваивается публичное имя, названное $ID_A$.

В краткосрочной перспективе будут использоваться документы, удостоверяющие личность, такие как паспорта, но в долгосрочной перспективе члены смогут удостоверить свое физические присутствие и уникальность путем использования биометрических технологий, таких как сканирование радужной оболочки глаза. Самое большое преимущество этого заключается в том, что можно сопоставить данные "от 1 до n" без использования личной информации, такой как имена, государственные регистрационные номера и адреса (B. Thiyaneswaran, S. padma., 2012). Данные идентификационной верификации записываются в хранилище биометрической информации доверенной третьей стороны (TTP) и гомоморфный алгоритм хеширования применяется для того, чтобы сделать невозможным отслеживание личности в хранилище. Все новые данные идентификации личности можно затем сравнить с существующей базой данных, чтобы исключить все одинаковые и слишком похожие данные. Если в результате запроса обнаруживается совпадение с существующими данными, запрос отклоняется. Идентификационная информация хранится в базе данных вне блокчейн и будет использоваться как централизованная облачная служба. Хотя это требует определенной степени доверия к третьей стороне, существует преимущество масштабируемости и безопасности, так как все данные хранятся зашифрованными. Кроме того, сторонняя служба хранения биометрической информации сама не участвует в блокчейн транзакциях или в процессе принятия решений, таким образом, BOSnet или Конгресс Сети не зависят от TTP (Zyskind, Nathan, Pentland, 2016). Вышеупомянутая личная информация не будет храниться в блокчейн и не будет использоваться в комбинации с информацией счета.

### Голосование

Для осуществления голосования на повестке дня создана программа голосования (открытый адрес $ID_V$). Каждый член ($ID_A$) имеет право одного голоса по данному вопросу ($ID_V$) и выпускается единый бюллетень.

### Требования:

1. Правомочность: система должна быть в состоянии видеть, что избиратель имеет полномочие участвовать в голосовании.
2. Конфиденциальность: анонимность голосующих. Невозможность связать результат с голосующим.
3. Честность: невозможность подделать бюллетени, результаты или изменить расписание.
4. Отсутствие принуждения: невозможность принужденного голосования и покупки голоса.
5. Уникальность: один человек имеет один голос. Если в период голосования допускается изменение голоса, учитывается только последний голос.
6. Полнота: необходимость подсчитывать действительные бюллетени. Недействительные бюллетени не учитываются. Результаты должны быть точно табулированы.

7. Справедливость: голосование не должно зависеть от голосов других людей. Другими словами, частичные подсчеты не должны влиять на весь процесс.
8. Проверяемость: избиратели должны иметь возможность убедиться, что их голоса правильно отражены в результатах и что все голоса были отданы справедливо (Fujioka A., Okamoto T., Ohta K., 1993), (Çetinkaya O., Doganaksoy A., 2007)

### Подготовка к голосованию: получение бюллетеня для голосования

После процесса регистрации, участники получают индивидуальный кошелек, связанный с модулем счета и программой голосования (1. Правомочность гарантируется). Личные кошельки генерируют одноразовый PKI ключ. $ID_A$ подтверждает правомочность голосующего, подтвержденную во время регистрации.

Затем члены могут подать заявку на получение бюллетеня голосования. Во время подачи заявки, случайное значение посылается голосующему. Затем голосующий гомоморфно шифрует это значение с помощью закрытого ключа и отправляет его в программу голосования. Программа голосования формирует бюллетень голосования на основе шифрования Encrypt (RE) с использованием гомоморфных вычислений.

Encrypt (Ballot Stamp) = f{$ID_A$, $ID_V$, Encrypt($R_E$), $R_A$}

Этот бюллетень создается в заслуживающей доверия среде, и, кроме того, программа голосования, которая создает его значение, не может ни прочитать данные, ни связать их с конкретным человеком (2. Конфиденциальность гарантируется.) Бюллетень создается на общественном домене, но только избиратель, имеющий закрытый ключ, может использовать его.

Дополнительные процессы устраняют время ожидания между запросом на создание бюллетеня и голосованием — создавая еще большую конфиденциальность для избирателя.

### Решающий голос

Когда бюллетень доставляется члену, член использует свой закрытый ключ для расшифровки бюллетеня, принимает решение и возвращает бюллетень с решением по зашифрованным каналам в программу голосования. Так как текстовые данные бюллетеня известны только члену, член может произвольно создавать несколько бюллетеней и голосовать несколько раз, и программа голосования не сможет увидеть разницу. Во избежание этого, и чтобы проверить, что хозяин ключа подписал бюллетень, программа голосования посылает бюллетень в виде значения тега.

Tag =f{sk, Encrypt(BallotStamp)}

Значение "sk" известно только программе голосования, и только те, у кого есть ключ для "шифрования (BallotStamp)" могут выяснить секретное значение. “XOR” операции или метод "слепой подписи" могут быть использованы для значения "f", которое является публичным. Поскольку это гомоморфная операция, следующие примеры также возможны.

Encrypt (BallotStamp)*sk1+sk2 = Encrypt (BallotStamp * sk1 +sk2)

Член вычисляет значение "sk" и направляет его в программу голосования вместе с бюллетенем для голосования и решением. Если значение "sk" является правильным, программа голосования сохраняет “бюллетень голосования”, решение участника, и значение "sk" для будущей верификации (3. Честность гарантируется). Значение "sk " может быть проверено по хэшу перед тем, как он вычисляется при помощи "Бюллетеня голосования". Это подтвердит полноту программы голосования на будущее.

Участники могут подать заявку на “Бюллетень голосования” несколько раз, но система создает "Бюллетень голосования” с тем же значением каждый раз. Другими словами, пользователь может проголосовать несколько раз с тем же Бюллетенем голосования в течение периода голосования; по мере поступления новой информации во время голосования избиратели могут свободно менять свои решения. Это также ограничивает возможность принуждения, которое может иметь место в удаленном голосовании. (4. Отсутствие принуждения гарантируется).

### Подсчет голосов

В конце периода голосования система сохраняет результаты голосования. Дата и время каждого голосования сохраняются, и, если один и тот же бюллетень дублируется, только последний голос считается окончательным результатом (5. Уникальность гарантируется). Этот процесс и результаты можно проверить; результаты записаны на блокчейн и никакие действительные голоса не теряются. (6. Полнота гарантируется). Как только подсчет сделан после завершения голосования, частичные подсчеты, которые могут повлиять на голосование, не разглашаются. (7. Справедливость гарантируется).

Когда результаты суммируются, они хранятся в блокчейн. Поскольку участники знают текстовые данные своих бюллетеней, голосующие могут подтвердить, что их голоса были приняты во внимание. (8. Проверяемость гарантируется).

Благодаря этому процессу наш протокол отвечает всем требованиям, описанным выше.

# 3. Заключение

Знаменитый экономист John Maynard Keynes однажды сказал: "трудность заключается не столько в развитии новых идей, сколько в освобождении от старых."

Насколько сложно изменить представление о том, что только центральные банки и существующие финансовые институты могут генерировать кредит? Что если крипто платформа имеет лучшую систему создания кредита, чем настоящая финансовая капиталистическая система? Криптовалюта была подвергнута критике, за то что она не является "настоящими деньгами", на основе того, что она не является подходящим средством обмена, методом платежа или средством сохранения стоимости (из-за ее волатильности). Кроме того, существующие криптовалюты не так хорошо генерируют кредит, как фиатные валюты. Чтобы преодолеть это, BOScoin намеревается ввести систему генерации кредитов, называемую системой Общественного финансирования (ОФ), вооруженную структурой управления, называемой сетью Конгресс; отходя от текущей модели ICO.

В дополнении, реальные экономические активы (богатство), приобретенные кредитом, созданным через ОФ, будут рассматриваться в качестве общественного достояния и использоваться в соответствии с консенсусом. Мы верим, что ОФ сможет решить основную проблему капитализма.

Чтобы обеспечить успех ОФ, Конгресс сети должен идентифицировать людей. Для того, чтобы предотвратить нарушения конфиденциальности процесса индивидуальной идентификации, мы планируем использовать гомоморфное шифрование для голосования в Конгрессе. Это также остановит фальшивые идентификации для создания чрезмерного влияния на голосование и предотвращения атаки Сибилла. Процесс позволяет одному человеку иметь один голос вместо голосования, пропорционального количеству активов в собственности. Это значит, что сообщество, в целом, может участвовать с душевным спокойствием и активно обмениваться разнообразными знаниями и мнениями. Конгресс Сети действует как децентрализованный, демократический орган принятия решений.

В следующей версии мы будем объяснять концепции, не рассматриваемые в этом White Paper. Они будут включать экономическую модель BOScoin, включая концепцию GTTP, которая связана BOSNet с внешними данными. Мы отойдем от старых идей и предложим новые, которые взламывают капитализм самым капиталистическим способом. Мы признаем, что каждое историческое достижение являлось “невыполнимой мечтой”, пока оно не было достигнуто. Маркс, чей 200 день рождения отмечался в 2018 году, может показаться анахронизмом. Тем не

менее, его мысли постоянно пересматриваются по мере выявления различных критических недостатков капиталистической системы. Хотя развитие капитализма принесло значительные экономические богатства, он не смог решить проблемы неравенства, разделения труда и распределения.

Проект BOScoin, который заложит основу для новой крипто экономики, будет способствовать инновациям, которые кардинально изменят мир. Цель этого проекта построить систему социального доверия, соединив технологические инновации с социальными инновациями. Некоторые глобальные тенденции могут быть приостановлены, но являются необратимыми. Одним из таких трендов является блокчейн и крипто экономика. Мы присоединяемся к этому движению, чтобы участвовать в революционизации общества так, как мы ее знаем.

# Ссылки


- Piketty, T. Capital in the Twenty - First Century. Belknap Press, 2017.
- Brynjolfsson, E., and McAffee, A. The Second Machine Age: Work Progress, and Prosperity in a Time of Brilliant Technologies. W.W. Norton and Company, 2014.
- Brynjolfsson, E., and Saunders, A. Wired for Innovation: How Information Technology is Reshaping the Economy. The MIT Press, 2009.
- Cusumano, M.A. "The sharing economy meets reality," Communications of the ACM, 61 (1): 26-28, 2017.
- Cusumano, M.A. "Amazon and whole foods; follow the strategy (and the money)," Communications of the ACM, 60 (10): 24-26, 2017.

Голосование Конгресса

- Myungsan Jun (2018) Blockchain Government: A next form of infrastructure for the twenty- first century. CreateSpace Independent Publishing Platform June 15, 2018 (https://boscoin.io/blockchain-government-free-download/)
- Sclavounis O. (2017) Understanding Public Blockchain Governance. Oxford Internet Institute. Retrieved March 18, 2018 from https://www.oii.ox.ac.uk/blog/understanding-public-blockchain-governance/
- De Filippi, P. & Loveluck, B. (2016) The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. Internet Policy Review, 5(3). Retrieved March 18, 2018 from https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infratructure
- Ehrsam F. (2017) Blockchain Governance: Programming our future. Retrieved March 18, 2018 from https://medium.com/@FEhrsam/blockchain-governance-programming-our-uture-c3bfe30f2d74
- Albert O. Hirschman. 1970. Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States.Cambridge, MA: Harvard University Press. Retrieved March 18, 2018
- Duncan L. (2017) Thoughts on Governance and Network Effects. Medium. Retrieved March 18, 2018 from https://blog.aragon.one/thoughts-on-governance-and-network-effects-f40fda3e3f98
- Wiecko Robert. (2018) Understanding the Governance and Budget System. Dash Official Documentation. Retrieved March 18, 2018 from https://dashpay.atlassian.net/wiki/spaces/DOC/pages/8585240/Understanding+the+Governance+and+Budget+System
- Surowiecki J. (2005) The Wisdom of Crowds: Why the many are smarter than the few and how collective wisdom shapes business, economies, societies, and nations. Anchor. Retrieved March 18, 2018
- Homomorphic Encryption Standardization homepage, Retrieved March 18, 2018 from http://homomorphicencryption.org/introduction/
- Bernhard D., Warinschi B. (2014) Cryptographic Voting — A Gentle Introduction. In: Aldini A., Lopez., Martinelli F. (eds) Foundations of Security Analysis and Design VII. Lecture Notes in Computer Science, vol 8604. Springer, Cham, Retrieved March 18, 2018 from https://link.springer.com/chapter/10.1007/978-3-319-10082-1_7 [10] B. Thiyanesw aran, S. padma. (2012) Iris Recognition Using left and right Iris feature of the Human Eye for Bio-metric Security system.
- IJCA, vol 50 No.152. Retrieved March 18, 2018 from http://www.gjimt.ac.in/wp-content/uploads/2017/11/Vijay-Kumar-Sinha_Enhancing-Iris-Security-by-Detection-of-Fake-

Iris_Paper.pdf [11] Zyskind, Nathan, Pentland (2016) Decentralizing Privacy: Using Blockchain to Protect Personal Data. Retrieved March 18, 2018 from https://enigma.co/ZNP15.pdf

- Fujioka A., Okamoto T., Ohta K. (1993) A practical secret voting scheme for large scale elections. In: Seberry J., Zheng Y. (eds) Advances in Cryptology — AUSCRYPT '92. AUSCRYPT 1992. Lecture Notes in Computer Science, vol 718. Springer, Berlin, Heidelberg. Retri eved March 18, 2018 from https://link.springer.com/chapter/10.1007/3-540-57220-1_66
- Çetinkaya O., Doganaksoy A. (2007) A Practical Verifiable e-Voting Protocol for Large Scale Elections over a Network, Availability Reliability and Security 2007. ARES 2007. The Second International Conference on, pp. 432-442, 10–13 April 2007. Retrieved March 18, 2018 from https://ieeexplore.ieee.org/document/4159833

# Авторы, советники и инвесторы BOScoin White Paper 2.0

**Авторы**

**Jonghyun Kim:** Вопросы безопасности в BlockchainOS / главный редактор WP2.0 / создатель концепции и автор публичной финансовой части

**Myungsan Jun:** Директор по развитию в BlockchainOS / автор части голосование Конгресса

**Kibong Moon:** директор KoSAC / автор голосования Конгресса

**Hawon Han:** разработчик KoSAC / автор голосования Конгресса

**Советники**

**Yezune Choi:** директор BlockchainOS / Консультативный комитет по WP2.0

**Minhyo Bae:** технический директор BlockchainOS / Консультативный комитет по WP2.0

**Joonkoo Kang:** технический директор KoSAC / Консультативный комитет по голосованию Конгресса

**Kibae Kim:** разработчик в ARIST (научно-исследовательский центр BlockchainOS) / Консультативный комитет по Общественному финансированию

**Инвесторы**

**Soonkuk Kang:** разработчик BlockchainOS / Консультативный комитет по WP2.0

**Joonseouk Lee:** бывший разработчик BlockchainOS / Консультативный комитет по WP2.0

**Taekwon Jung:** бывший разработчик в ARIST (научно-исследовательский центр BlockchainOS) / Консультативный комитет по WP2.0

**Jaeoh Kim:** менеджер Общественного финансирования BlockchainOS / редактор WP2.0

**Hojung Park:** менеджер Общественного финансирования BlockchainOS / редактор WP2.0 (английский)

**Gyucheol Cho:** менеджер Общественного финансирования BlockchainOS / редактор WP2.0

**Корейский редактор**

Joonsoo Kim Lee

**Английский перевод**

Seungwook Yeo

**Английский редактор**

Scott Matheina: комьюнити-менеджер BlockchainOS

**Русский перевод**

Солдатова Лилия