Proof of Stake vs. Proof of Work

White Paper

(перевод на русский)

BitFury Group

21 сентября 2015 (Версия 1.0-ru)

Аннотация

Подтверждение доли (англ. proof of stake) — механизм согласования для электронных валют, альтернативный механизму доказательства работы (англ. proof of work), используемому в Биткойне. Основными заявленными преимуществами подходов, использующих подтверждение доли, являются отсутствие дорогих вычислений и, соответственно, более низкий входной барьер для получения вознаграждений за генерацию блока. В этой работе исследуются аргументы за и против обоих механизмов согласования и показывается, что существующие реализации подтверждения доли являются уязвимыми для атак, которые крайне маловероятны для Биткойна и других подходов, использующих доказательство работы.

История версий

Версия	Дата	Описание изменений
1.0	13 сен. 2015	Начальная версия (англ.)
1.0-ru	21 сен. 2015	Начальная версия (перевод на русский)

В основе структуры для хранения транзакций в Биткойне и других криптовалютах лежит распределенная база данных — блокчейн, в которой хранится вся история транзакций. Блокчейн (англ. blockchain, цепочка блоков) получил свое название потому, что транзакции собираются в блоки; каждый блок (кроме самого первого, то есть генезис блока) ссылается на предыдущий. Каждый узел, участвующий в сети Биткойн, имеет свою копию блокчейна[1]. Узлы синхронизируются между собой с помощью пиринговой (P2P) сети. Любая реализация криптовалюты должна быть способна защитить свой блокчейн от возможных атак. Например, атакующий может потратить определенную сумму денег, а затем обратить транзакцию путем распространения своей собственной версии блокчейна, которая не включает эту транзакцию. Так как безопасность блокчейна не полагается на единый центр, пользователи не знают априори, какая версия базы данных является действительной.

В Биткойне безопасность сети полагается на алгоритм доказательства работы (PoW) в форме майнинга блоков. Каждый узел, желающий принимать участие в майнинге, должен решить вычислительно сложную задачу, чтобы гарантировать действительность нового блока; награда за решение выплачивается в виде новых биткойнов. Протокол является честным в том смысле, что майнер с долей общей вычислительной мощности, равной p, может создать блок и получить награду с вероятностью p. Атакующий должен решать те же задачи, что и оставшаяся часть сети, то есть атака будет успешной, только если атакующий сможет привлечь значительные вычислительные ресурсы.

Функционирование протокола Биткойн таково, что безопасность сети поддерживается физически редкими ресурсами:

- специализированное оборудование для проведения вычислений;
- электричество, необходимое для работы оборудования.

Это делает Биткойн неэффективным с точки зрения потребления ресурсов. Для увеличения своей доли вознаграждения, майнеры в сети Биткойн вынуждены участвовать в «гонке вооружений», то есть использовать всё больше ресурсов для майнинга. С одной стороны, это делает стоимость атаки на Биткойн непомерно высокой. С другой, экологическое недружелюбие Биткойна привело к возникновению предложений построить подобные системы, которые требуют намного меньше ресурсов.

Одна из возможных реализаций распределенной базы данных, не опирающихся не дорогие вычисления, основана на алгоритмах *подтверждения доли* (PoS). Идея подтверждения доли проста: вместо вычислительной мощности, вероятность создать новый блок и получить соответствующее вознаграждение пропорциональна доле владения пользователя в системе. Отдельно взятый держатель валюты, имеющий долю p от общего числа монет в обороте, создает новый блок с вероятностью p.

[1] Строго говоря, существуют узлы в сети Биткойн, которые не хранят блокчейн целиком, а используют упрощенную проверку платежей (SPV) [1]. В дальнейших рассуждениях мы не рассматриваем эти узлы, так как они не добавляют безопасности к сети.

Логическое обоснование состоятельности алгоритма подтверждения доли заключается в следующем: пользователи с наибольшими долями в системе имеют наибольший интерес в поддержании безопасности сети, так как они больше всего пострадают в случае, если репутация и стоимость криптовалюты упадет в результате атак. Чтобы провести успешную атаку, злоумышленник должен приобрести большую часть валюты, а это будет непомерно дорого, если система будет достаточно популярной.

В последующих разделах работы изучается, является ли согласование в виде подтверждения доли более чувствительным по отношению к атакам, чем доказательство работы, в следующих разделах.

1. Теория

В системах, основанных на криптовалюте, таких, как Биткойн, содержится информация (состояние системы), позволяющая пользователям получать баланс своего счета. Для Биткойна состояние системы — это набор неиспользованных выходов транзакций (англ. unspent transaction outputs, UTXO). Каждый выход криптографически заблокирован и требует от пользователя предоставить доказательство владения, чтобы его потратить. Вместо того, чтобы явно хранить балансы счетов, Биткойн и другие криптовалюты сохраняют полную историю транзакций пользователей, из которой можно получить текущее состояние системы, а также все предыдущие.

Транзакции представляют атомарные изменения состояния системы. Транзакции группируются в блоки; блоки формируют упорядоченный набор, называющийся *блокчейном*. Чтобы организовать блокчейн, то есть цепочку блоков, каждый блок содержит ссылку на предыдущий. Первый блок в цепи — это *генезис блок*; у него нет предыдущего блока и обычно он напрямую прописывается в протокол. Новые блоки формируются и находятся в соответствии с определенными правилами, установленными в пртоколе криптовалюты. Важной функцией этих правил является защита против атак на блокчейн, а также достижение согласия в случае появления нескольких версий блокчейна. Доказательство работы и подтверждение доли отвечают двум типам ограничений на действительные блоки и влекут за собой различные механизмы согласия.

Определение 1. Пользователь работает над блоком B, если он пытается открыть блок, который ссылается на B как на предыдущий.

Заметим, что B однозначно определяет весь блокчейн, поэтому можно обозначить блокчейн его последним блоком B и говорить, что блоки строятся над блокчейном B.

Система криптовалюты может рассматриваться как распределенная база данных, с копиями базы, принадлежащими провайдерам инфраструктуры для валюты, которые общаются между собой с помощью пирингового интернет-протокола. В терминах CAP-теоремы (англ.

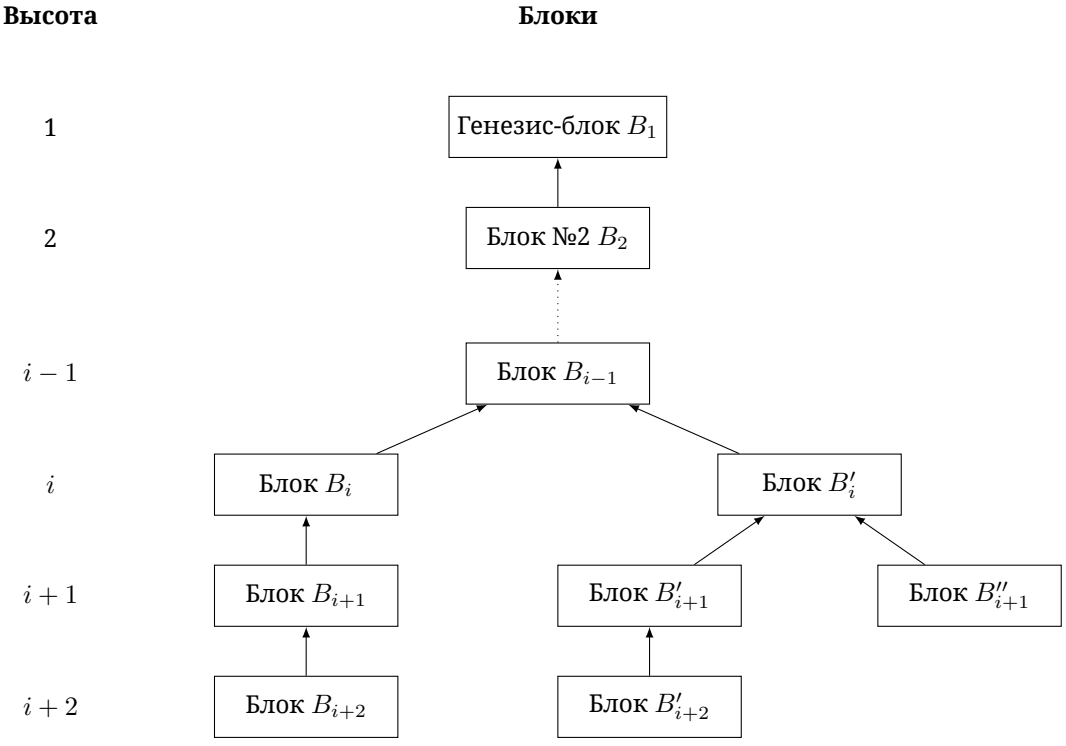

Рис. 1. Несколько блокчейнов в системе криптовалюты. В «хорошем» протоколе согласования рациональные пользователи дожны работать над B_{i+2} или B'_{i+2}

consistency, availability, partition-tolerance) [2], системы криптовалют обладают свойствами доступности (любой запрос завершается корректным откликом) и устойчивости к разделению (сервис продолжает работать, даже если некоторые узлы выходят из строя), но не обладают согласованностью данных. Время от времени, различные пользователи видят различные состояния системы как текущие. В некоторых случаях несогласованность отвечает ситуации, когда обнаружен новый блок, но еще не был передан всем пользователям системы. Чтобы добиться согласованности в конечном итоге (англ. eventual consistency [3]), адекватный консенсус-протокол должен накладывать следующее ограничение:

Условие 1. Пользователь, который обнаружил новый блок, должен быть заинтересован в том, чтобы распространить его по сети немедленно, а не удерживать для себя.

В других случаях, несогласованность в системе обусловлена расщеплением блокчейна на несколько веток (рис. 1). Существует несколько причин расщепления блокчейна (*форкинга*):

- два пользователя обнаруживают блок в одно и то же время;
- злоумышленник пытается обратить ранее осуществленную транзакцию с помощью форкинга.

Чтобы избежать преднамеренного ветвления, в адекватный консенсус-протокол должно быть включено следующее требование:

Условие 2. Пользователи не должны пытаться открывать блоки над промежуточными цепями. А именно, если есть известный блок B', который ссылается на блок B, у пользователя не должно быть причин работать над B.

В ситуации, изображенной на рис. 1, в соответствии с условиями 1–2, только три блока могут быть использованы в качестве базы для продолжения блокчейна: B_{i+2}, B''_{i+1} и B'_{i+2}. Существуют дальнейшие ограничения на действительные блокчейны; в большинстве случаев, эти ограничения сводятся к выбору цепи максимальной длины (что исключает B''_{i+1} из множества блоков, над которыми рациональный пользователь может работать). Целью консенсус-правил является обеспечение выбора единой цепи; тем не менее, обычно некоторые правила зависят от пользователя. Например, если в сети Биткойн есть несколько блокчейнов одинаковой длины, пользователи должны выбирать тот, который они получили первым. Таким образом, нет способа обеспечить выбор одной и той же цепи всеми пользователями (так как очень сложно или даже невозможно гарантировать выполнение правил, специальных для пользователей).

Чтобы система была целостной в конечном итоге, ее консенсус протокол должен удовлетворять третьему условию:

Условие 3. Правила согласования должны быть так, чтобы приводить к разрешению ветвлений блокчейна, то есть одна из соревнующихся веток должна опередить все остальные за разумное время.

Мы будем использовать отдельные термины для открытия блоков с использованием алгоритмов доказательства работы и подтверждения доли:

Определение 2. Процесс решения вычислительной задачи, поставленной протоколом доказательства работы, называется *майнингом* (англ. mining, добыча) блоков.

Определение 3. Процесс решения вычислительной задачи, поставленной протоколом подтверждения доли, называется *минтингом* (англ. minting, чеканка) блоков.

1.1. Доказательство работы

Рассмотрим Биткойн в качестве примера системы криптовалюты, использующей для безопасности алгоритм доказательства работы. Каждый блок в Биткойне состоит из двух частей:

- заголовок блока с ключевыми параметрами, включая время создания блока, ссылку на предыдущий блок и корень дерева Меркла [4] блока транзакций;
- список транзакций.

Чтобы ссылаться на конкретный блок, его заголовок хешируется дважды с помощью функции SHA-256 [5]; итоговое целое число принадлежит отрезку $[0, 2^{256} - 1]$. Чтобы учесть разные возможные реализации, мы будем использовать общую хеш-функцию $\mathrm{hash}(\cdot)$ с различным

числом аргументов и областью значений $[0, M]$. Например, аргументы функции могут рассматриваться как бинарные строки, которые соединяются вместе, формируя один аргумент, который может быть передан в SHA-256 хеш-функцию.

Ссылка на блок используется в протоколе, использующем доказательство работы; чтобы блок считался действительным, его ссылка должна не превышать определенный порог:

$$\text{hash}(B) \leqslant M/D, \tag{1}$$

где $D \in [1, M]$ — целевая сложность. Не существует известного способа найти B, удовлетворяющее неравенству (1), кроме последовательного перебора по всем возможным значениям заголовка блока. Чем больше величина D, тем больше итераций необходимо произвести, чтобы найти действующий блок; ожидаемое число операций равняется D.

Время $T(r)$, которое требуется майнеру с оборудованием, способным выполнять r операций в секунду, чтобы найти действительный блок, имеет экспоненциальное распределение с параметром r/D (см. приложение А):

$$P\{T(r) \leqslant t\} = 1 - \exp(-rt/D).$$

Рассмотрим n майнеров Биткойна с долями хеширующей мощности r_1, r_2, ..., r_n. Время T, чтобы найти блок, равняется минимуму из значений случайных величин $T(r_i)$ в предположении, что майнер сразу же отправляет найденный блок и он достигает других майнеров немедленно[2]. Согласно свойствам экспоненциального распределения, T также распределено экспоненциально:

$$P\{T \stackrel{\text{def}}{=} \min(T_1, \ldots, T_n) \leqslant t\} = 1 - \exp\Big(-\frac{t}{D}\sum_{i=1}^{n} r_i\Big);$$

$$P\{T = T_i\} = \frac{r_i}{\sum_{j=1}^{n} r_j}.$$

Последнее равенство показывает, что майнинг — честный процесс: майнер с долей вычислительной мощности p имеет ту же вероятность p открыть блок раньше других майнеров. Можно показать, что доказательство работы в том виде, в котором оно используется в Биткойне, удовлетворяет условиям 1–3.

1.2. Подтверждение доли

В алгоритмах подтверждения доли неравенство (1) модифицируется таким образом, чтобы оно зависело от количества конкретной криптовалюты, принадлежащего пользователю, а не от свойств блока. Рассмотрим пользователя с адресом A и балансом $\text{bal}(A)$. Обычно в алгоритмах подтверждения доли используется условие, аналогичное

$$\text{hash}(\text{hash}(B_{prev}), A, t) \leqslant \text{bal}(A)M/D, \tag{2}$$

где

[2] Существует теоретическая возможность атаки [6], которая основана на отправке блоков с задержкой. Здесь мы ее не рассматриваем и предполагаем, что все майнеры действуют честно.

- B_{prev} обозначает блок, над которым пользователь работает;
- t — текущее время (UTC).

По различным причинам, некоторые криптовалюты используют модифицированные версии (2), которые обсуждаются в соответствующих разделах.

В отличие от (1), единственная переменная, которую пользователь может менять, это время t в левой части неравенства (2). Баланс адреса блокируется протоколом; например, протокол может считать баланс, исходя из средств, которые не двигались в течение дня. В качестве альтернативы, PoS-криптовалюта может использовать неиспользованные выходы транзакций, как это делается в Биткойне; в таком случае, баланс закрыт естественным образом. Протокол с подтверждением доли ставит ограничения на возможные значения t. Например, если t не может отличаться от UTC-времени узлов сети больше, чем на час, то пользователь может попробовать не более 7200 значений t. Таким образом, в подтверждение доли не вовлечены дорогие вычисления.

Вместе в адресом A и временем t, удовлетворяющими (2), пользователь должен предоставить доказательство владения адресом. Чтобы этого добиться, пользователь может подписать новый блок с помощью своей цифровой подписи; чтобы создать действительную подпись, необходимо обладать секретным ключом, соответствующим адресу A.

Время, необходимое, чтобы найти блок для адреса A, распределено экспоненциально с параметром $\text{bal}(A)/D$ (см. приложение A). Следовательно, реализация (2) подтверждения доли является честной: вероятность сгенерировать блок равна отношению баланса адреса к общему объему валюты в обороте. Время, которое требуется всей сети, чтобы найти блок, распределено экспоненциально с параметром $\sum_a \text{bal}(a)/D$. Таким образом, если денежная масса валюты $\sum_a \text{bal}(a)$ фиксирована или растет с предсказуемой скоростью, сложность D должна быть известна заранее:

$$D = \frac{1}{T_{ex}} \sum_a \text{bal}(a),$$

где T_{ex} обозначает ожидаемое время между блоками. На практике, однако, сложность D должна настраиваться на основании недавних блоков, потому что не все обладатели валюты принимают участие в минтинге.

1.3. Делегированное подтверждение доли

Делегированное подтверждение доли (англ. delegated proof of stake, DPoS) — общий термин, описывающий эволюцию базовых консенсус-протоколов на основе подтверждения доли. DPoS используется в BitShares (раздел 2.5), а также в предложенных алгоритмах, таких как Slasher и Tendermint (раздел 4). В этих протоколах, блоки порождаются предопределенным множеством пользователей системы (*делегатами*), которые получают вознаграждение за свою обязанность и наказываются за злонамеренное поведение (такое как участие в двойном расходовании средств). В DPoS-алгоритмах, делегаты участвуют в двух раздельных процессах:

- построение блока транзакций;
- верификация действительности сгенерированного блока с помощью электронной подписи.

В то время как блок создается отдельным пользователем, чтобы считаться действительным, он обычно должен быть подписан более чем одним делегатом.

Список пользователей, подходящих для подписывания блоков, периодически изменяется в соответствии с определенными правилами; например, в Slasher делегаты избираются исходя из их доли и истории блокчейна. Множество делегатов для каждого блока обычно мало; заметным исключением является Tendermint, в котором каждый блок может быть подписан любым пользователем системы. В некоторых версиях DPoS, делегат должен подтвердить обязательство с помощью депонирования своих средств на гарантийный счет, где средства временно блокируются в целях безопасности (и конфискуются в случае вредоносного поведения); эта версия DPoS обычно называется *подтверждение доли, основанное на депозите* (англ. deposit-based proof of stake).

Делегированное подтверждение доли не использует условий (2). Доля учитывается в DPoS одним из следующих способов:

- Делегаты могут выбираться на основании их долей в системе.
- Делегаты могут получать голоса от всех пользователей, сила голоса зависит от доли валюты у голосующего.
- Голоса делегатов за действительные блоки могут иметь вес, пропорциональный их гарантийному депозиту.

В целом, делегированное подтверждение доли менее стандартизировано, чем базовая версия PoS; существующие реализации описываются более подробно в соответствующих разделах.

1.4. Объективность протоколов согласования

Одна из задач протокола согласования состоит в том, чтобы вновь прибывшие пользователи могли определить состояние системы исходя из информации, полученной от одноранговых узлов (пиров). Эта задача нетривиальна, так как некоторые узлы могут принадлежать стороне, осуществляющей атаку Сибиллы [7].

Определение 4 ([8]). Протокол согласования является *объективным*, если новый узел может независимо прийти к тому же текущему состоянию, что и оставшаяся часть сети, основываясь только на правилах протокола (таких, как определение генезис-блока) и сообщениях, передаваемых по системе (например, множество всех действительных блоков).

Консенсус в виде доказательства работы является примером объективного протокола; если новый узел сети имеет подключение хотя бы к одному "честному" пользователю, он выберет

действительный блокчейн, так как тот имеет большую суммарную вычислительную сложность. Подтверждение доли, с другой стороны, не является объективным. В самом деле, рассмотрим злоумышленника со значительной вычислительной мощностью. В том случае, если ветка злоумышленника достаточно длинна, сложность внутри нее отрегулирована, чтобы отражать ситуацию, в которой только счета, контролируемые злоумышленником, активны; это позволяет злоумышленнику построить цепочку, длиннее, чем действительный блокчейн. В то время как долгосрочные ветвления отвергаются существующими пользователями системы (например, введением правила, которое ограничивает длину возможного ветвления), новички без предварительных сведений о текущем состоянии выберут блокчейн злоумышленника.

Определение 5. Протокол согласования является *слабо субъективным*, если узлу нужно недавнее состояние в дополнение к правилам протокола и сообщениям, распространяемым по системе, чтобы независимо определить текущее состояние системы.

В случае подтверждения доли, если есть правило, которое запрещает ветвления длины более N, то есть после точки ветвления не может быть больше N блоков, то достаточно считать содержимое блока глубины N или меньше, чтобы надежно определить текущее состояние системы. Вновь прибывший пользователь может получить доступ к блоку от доверенного источника (например, вебсайт, посвященный рассматриваемой валюте). В то время как этот метод может подорвать безопасность и децентрализацию системы подтверждения доли, в *Proof of stake: How I learned to love weak subjectivity* [8] утверждается, что слабая субъективность — это хороший способ объединить безопасность, контролируемую компьютером с социально управляемой.

2. Реализации

В настоящее время существует несколько примечательных криптовалют, основанных на согласовании путем подтверждения доли (табл. 1):

- Peercoin, или PPCoin (peercoin.net);
- Nxt (nxt.org);
- BlackCoin (blackcoin.co);
- Novacoin (novacoin.org).

Делегированное подтверждение доли используется в BitShares, платформе для электронных активов (bitshares.org). Разработчики Ethereum (ethereum.org) планируют изменить согласование на делегированное подтверждение доли в будущем; сейчас Ethereum опираются исключительно на доказательство работы.

Таблица 1. Статистика рынка PoS криптовалют. Для капитализации и суточного объема торгов использованы медианные значения, взятые за месячный период (с 24 июля по 23 августа 2015 года) из CoinMarketCap [9].

Название	Общий запас, млн.	Капитализация, млн. $	Суточный объем, тыс. $	Замечания
Peercoin (PPCoin)	22,6	10,8	83	гибрид PoW / PoS
NXT	1 000	10,7	27	
BlackCoin	75,0	2,2	15	гибрид PoW / PoS
Novacoin	1,14	1,4	20	гибрид PoW / PoS
BitShares	2 511	11,7	55	делегированный PoS

2.1. Peercoin

Peercoin, или PPCoin — криптовалюта, основанная в 2012 году анонимным разработчиком Sunny King. Peercoin использует комбинацию доказательства работы и подтверждения доли [10]:

- Доказательство работы используется для распределения новых монет.
- Подтверждение доли используется для защиты транзакций, то есть в качестве основного средства для генерации блоков транзакций.

Структура блокчейна в Peercoin очень похожа на Биткойн: также, как и Биткойн, Peercoin оперирует неиспользованными выходами транзакций (UTXO). Новые блоки находятся в среднем каждые 10 минут; транзакции состоят из входов, ссылающихся на UTXO и выходов.

Peercoin использует тот же алгоритм доказательства работы, основанный на хеш-функции SHA-256, что и Биткойн; однако награда за майнинг зависит не от высоты блока, а от целевой сложности. Когда сложность растет, вознаграждение падает; шестнадцатикратный рост сложности влечет за собой снижение награды в два раза. Пока награда за майнинг стремится к нулю, стимул использовать PoW становится меньше в сравнении с PoS. С этой точки зрения, Peercoin является энергоэффективным в долгосрочной перспективе.

Подтверждение доли в Peercoin основывается на понятии *возраста монет* (англ. coin age). Возраст монет используется в Биткойне для определения приоритета транзакций [11].

Определение 6. *Возраст монет* неиспользованного выхода транзакции — это его величина, умноженная на период времени, который прошел с момента его создания. Транзакция, расходующая ранее не использованный выход, *потребляет*, или *уничтожает*, его возраст монет.

Возраст монет используется в Peercoin и с другой целью: чтобы определить действительный блокчейн. Это блокчейн с наибольшим суммарным уничтоженным возрастом монет всех транзакций во всех блоках (ср. с механизмом, использующим полную ожидаемую работу, потраченную на строительство блокчейна в Биткойне).

Возможность создать блок, используя неиспользованный выход U в Peercoin определяется условием

$$\text{hash}(\text{hash}(B_{prev}), U, t) \leqslant \text{bal}(U)\,\text{age}(U)M/D, \tag{3}$$

где $\text{age}(U)$ обозначает время, прошедшее с момента создания U. Версия PoS (3) подразумевает, что вместо суммарного количества валюты, вероятность создать блок пропорциональна суммарному возрасту монет всех UTXO, принадлежащих пользователю.

Первая транзакция в новом блоке — это специальная coinstake транзакция, которая доказывает, что выигравший UTXO принадлежит пользователю, который открыл блок. Первый вход coinstake транзакции должен совпадать с непотраченным выходом U, удовлетворяющим (3); в большинстве случаев, пользователь тратит U, отсылая самому себе.

Декларируемая причина, стоящая за реализацией PoS (3) — более равномерное распределение владельцев решенных блоков. Действительно, добыча блока уменьшает вероятность для того же пользователя добыть следующий блок, так как суммарный возраст монет его UTXO уменьшается. В результате пользователи с малыми долями валюты тоже могут обнаружить блок, если будут ждать достаточно долго.

Чтобы обеспечить стабильность блокчейна, Peercoin использует периодически рассылаемые точки сохранения. Этот метод распространения вводит точку централизации. В то время как точки сохранения присутствуют в протоколе Биткойна [12], они могут быть выключены; помимо этого, они закодированы в протокол, а не распространяются. Соответственно, механизм точек сохранения в Биткойне не предполагает риска централизации.

2.2. Nxt

Nxt — криптовалюта, основанная в 2013 году и использующая только подтверждение доли. В отличие от Peercoin, Nxt не использует доказательство работы, чтобы создавать новые монеты; весь доступный запас монет, 1 миллиард NXT, присутствует в системе с самого начала, с генезис блока. Таким образом, единственным стимулом открывать блоки является сбор комиссий за транзакции.

Транзакции в Nxt рабикально отличаются от транзакций в Биткойне, что, в свою очередь, приводит к следующим отличиям протоколов [13]:

- Транзакции в Nxt не имеют запирающих и отпирающих скриптов. Вместо них для задания отправителя и получателя транзакции протокол Nxt использует явно заданные профили пользователей. Это ограничивает возможности системы обращаться со смарт-контрактами в сравнении с Биткойном.
- Существуют различные типы транзакций, например, специальные транзакции для сообщений, цветных монет, электронных товаров и т. д.
- Существует ограничение на количество транзакций в блоке: не более 255. С другой стороны, среднее время между блоками равно одной минуте.

- Все транзакции имеют срок годности (по умолчанию 24 часа). Транзакции, не включенные в блок, удаляются из пула по истечении срока годности и должны быть отправлены заново.

Nxt использует модифицированную версию согласования путем подтверждения доли. Вместо (2), для пользовательского профиля A, чтобы он мог создать блок, должно выполняться неравенство

$$\text{hash}(\text{hash}(B_{prev}), A) \leqslant t\,\text{bal}(A)M/D. \tag{4}$$

В (4) B_{prev} — блок, над которым пользователь работает, t — время, прошедшее с момента создания B_{prev}. Таким образом, изначально после того, как новый блок распространяется по сети, возможность удовлетворить условию PoS низка для каждого пользователя; эта вероятность растет со временем. Хеш-функция в (4) считается следующим образом:

1. берется специальное поле (подпись генерации, англ. generation signature) в B_{prev};
2. подпись генерации подписывается с помощью публичного ключа пользователя;
3. выбираются первые 8 байтов полученной подписи.

Так как публичные ключи, соответствующие профилям, публично известны, кто угодно может проверить, выполняется ли (4) для любого пользовательского профиля A. Как и в Биткойне, действительный блокчейн в Nxt определяется как цепь с максимальной ожидаемой сложностью D.

Отметим, что в отличие от (2), (4) не содержит *никаких* переменных, которые пользователь A мог бы изменить. Таким образом, PoS в Nxt обладает следующим интересным свойством: возможно предсказать с разумной точностью, кто откроет следующий блок. Чтобы сделать это, нужно лишь найти

$$\hat{A} = \arg\min_{A} \frac{\text{hash}(\text{hash}(B_{prev}), A)}{\text{bal}(A)}$$

для всех пользовательских профилей. Nxt имеет отличную от Биткойн лежащую в основе вероятностную модель. Она благоприятна для крупных игроков: если у пользователя есть существенная доля валюты, вероятность открыть блок для него выше, чем его доля [14] (см. приложение B).

2.3. Novacoin

Novacoin — гибридная PoW/PoS криптовалюта, похожая по принципу на Peercoin. Основные отличия:

- Novacoin использует более консервативную формулу для наград за минтинг: вознаграждение уменьшается в два раза, как только сложность возрастает в 64 раза [15] (ср. с увеличением в 16 раз в Peercoin).

- В подтверждении доли используется немного модифицированный метод, основанный на *весе монето-дней* (англ. coin day weight) вместо возраста монет (3). Кроме того, coinstake-награда за PoS-блок зависит от использованного возраста монет и от сложности PoS [16].

Вес монето-дней в Novacoin считается аналогично возрасту монет, но со сдвигом в 30 дней и ограничением в 90 монето-дней. Например, вес монето-дней UTXO величиной в 1 Novacoin изменяется во времени следующим образом:

Возраст, дни	1	10	30	60	90	120	200
Вес монето-дней	0	0	0	30	60	90	90

2.4. BlackCoin

Blackcoin — гибридная криптовалюта, использовавшая доказательство работы для начального распределения валюты. Сейчас используется только подтверждение доли. BlackCoin — единственная из рассматриваемых криптовалют, которая использует изначальную версию подхода подтверждения доли (2), согласно которой доля пользователя определяется как его доля общего количества монет [17]. Новые блоки открываются в среднем каждые 64 секунды; создатели блоков получают 1% годовых (означая, что BlackCoin является инфляционной валютой).

2.5. BitShares

BitShares — полиморфный электронный актив, который может быть использован для создания взаимозаменяемых активов, привязанных к конкретным рынкам (например, доллары США). Он похож на систему цветных монет, где BitShares выступает в качестве внутренней валюты (как XCP в Counterparty). Одним из инновационных свойств BitShares является алгоритм согласования в виде делегированного подтверждения доли. Создатели BitShares сейчас разрабатывают BitShares 2.0, финансовую платформу для смарт контрактов корпоративного класса, использующую некоторые технологии из BiShares, включая DPoS.

Делегированное подтверждение доли в системе BitShares основывается на понятии *свидетелей*. Держатели BitShares могут выбрать произвольное количество свидетелей, которые создают блоки транзакций. У каждого держателя валюты есть количество голосов, равное количеству BitShares, которыми он обладает; голоса могут быть распределены между свидетелями произвольно. Кроме свидетелей, пользователь также выбирает количество свидетелей, которое он считает достаточным для децентрализации. Естественно, пользователь не может голосовать за большее количество свидетелей, чем он считает нужным.

После того как результаты голосов просуммированы, выбираются N свидетелей, получившие наибольшее количество голосов. N определяется как наименьшее число, удовлетворяющее голосам не менее половины пользователей. Выбранные свидетели по очереди производят

блоки каждые две секунды. После того, как каждый из N свидетелей создал свой блок, список свидетелей перемешивается, поэтому порядок создателей блоков постоянно меняется.

Аналогично свидетелям, пользователи системы выбирают *делегатов*, которые имеют возможность менять параметры сети, включая комиссии за транзакции, размер блоков и интервалы между ними, а также вознаграждения свидетелям. Чтобы осуществить изменения в протокол сети, делегаты вместе подписывают специальный пользовательский профиль (так называемый генезис-профиль). После того, как большинство делегатов подтвердили предложенное изменение, у владельцев валюты есть две недели, в течение которых они могут отозвать своих делегатов и отменить изменения. В отличие от свидетелей, делегаты не получают награды за свои усилия.

3. Атаки и проблемы

Этот раздел описывает атаки, которые возможны в каждой из PoS-систем, а также некоторые атаки, специфические для конкретных реализаций протокола. Некоторые описания атак взяты из *Cryptocurrencies without proof of work* [19].

Большинство проблем с PoS-протоколами возникают из-за того, что протоколу не известно ничего, кроме соответствующего блокчейна [20]. В системах доказательства работы присутствует внешний фактор, а именно количество вычислительной работы, которое требуется, чтобы найти решение (1). В системах с подтверждением доли отсутствуют факторы, закрепляющие блокчейн в физическом мире; поэтому интуитивно видно, что согласование на основе PoS допускает больше видов атак.

3.1. Проблема «ничего на кону»

Наивные алгоритмы подтверждения доли, опирающийся только на (2), имеют серьезную проблему: если произошло ветвление блокчейна (неважно, случайное или умышленное), рациональное поведение для всех пользователей — минтить блоки на обоих ветках. С алгоритмом доказательства работы, такое поведение иррационально. Разделяя ресурсы на различные ветки, майнер уменьшает вероятность найти блок на каждой из них; оптимальная стратегия в PoW системе — всегда работать над одной веткой. В алгоритме подтверждении доли, в отличие от PoW, вероятность найти блок не убывает, если пользователь пытается работать над несколькими ветками блокчейна. Поэтому, рациональное поведение в PoS-системе — работать над всеми ветками, о которых пользователь знает. Хуже того, наивное подтверждение доли не удовлетворяет условию 2: в некоторых условиях, подходящей стратегией может оказаться работа над промежуточным блокчейном (см. раздел 3.4).

Эта проблема облегчает задачу двойного расходования или других видов атак, опирающихся на ветвление блокчейна. Если пользователи верят, что атака может удаться, они будут поддерживать ее, работая над блокчейном злоумышленника. В то время как пользователи с боль-

шими объемами валюты будут противостоять атакам, проводимым путем ветвления, так как они боятся потерять свои деньги, атака имеет хорошие шансы быть успешной, если валюта распределена равномерно между многими пользователями.

Есть несколько предложенных решений к проблеме «ничего на кону»; они описаны в разделе 4. Алгоритмы делегированного PoS обычно не подвержены этой проблеме, так как на кону средства минтеров блоков; эти средства будут конфискованы, если минтер примет участие в атаке на систему.

3.2. Проблема начального распределения

В системах, использующих PoS, всегда существует угроза, что начальные держатели монет не будут заинтересованы в том, чтобы тратить свои монеты, так как их баланс прямо способствует увеличению их благосостояния. В Биткойне и других PoW-системах ранние последователи технологии находятся в тех же условиях, что и остальные пользователи: чтобы майнить монеты, им нужно постоянно улучшать свое оборудование и оптимизировать потребление ресурсов. В PoS-системе пользователь, который приобрел 10 % от общего числа монет, когда система только запустилась (например, за 1 000 $) имеет преимущество по сравнению с пользователями, имеющими те же средства в момент, когда система набрала популярность и 1 000 $ эквивалетно 0,01 % всех монет.

Чтобы предотвратить эту ситуацию, реализации PoS используют дополнительные алгоритмы для начального распределения валюты; например, Peercoin и Ethereum используют доказательство работы для создания новых монет (см. раздел 4).

3.3. Атака издалека

В системе с PoS-согласованием, злоумышленник, обладающий достаточной вычислительной мощностью, может попробовать построить альтернативный блокчейн, начиная с самого первого блока. В PoW-системе, этой атака препятствует огромная вычислительная мощность, необходимая, чтобы построить блокчейн с нуля; в то же время, эту задачу реально решить в PoS-системе. Так как злоумышленник может перемещать монеты свободно в блокчейне, который он строит, у него намного большая размерность пространства поиска; таким образом, этот тип атаки может быть предпочтительнее для построения альтернативного блокчейна с недавней точкой ветвления. Возможность атаки сохраняется в делегированном подтверждении доли, где она может быть осуществлена большинством делегатов.

Чтобы предотвратить атаку издалека, протокол может установить максимальную разрешенную глубину точки ветвления. Например, в Nxt пользователь не может принимать альтернативный блокчейн, если он отличается от существующего более чем в последних 720 блоках (что соответствует 12 часам). Тем не менее, это ограничение не решает проблему новых пользователей. Когда пользователь присоединяется к сети, он видит несколько блокчейнов, не имея предварительных сведений об их подлинности. Если блокчейн атакующего предпо-

чтительнее действительного в рамках протокола, новые пользователи примут его. Один из способов узнать, какой блокчейн правильный — загрузить его из доверенного источника; в то же время, это делает систему несколько централизованной и вносит фактор доверия. Тем не менее, загрузки блокчейна из доверенных источников используются фактически во всех существующих PoS-системах.

3.4. Атака взятками

В этой атаке, злоумышленник пытается дважды израсходовать свои средства следующим образом:

1. купить какие-либо товары или услуги;
2. подождать, пока транзакция, содержащая платеж, будет считаться подтвержденной продавцом;
3. Объявить вознаграждение за строительство на основе усеченного блокчейна, не включающего рассматриваемый платеж. Например, если продавец ждет шести подтверждений, злоумышленник начнет с блокчейна без последних шести блоков. Злоумышленник может предложить большую награду пользователям, которые работают только над блокчейном атакующего без этого, блокчейном злоумышленника никогда не догонит правильный).
4. Атакующий может продолжать платить взятки, даже когда его блокчейн и правильный будут иметь одинаковую длину, чтобы получить поддержку большинства держателей криптовалюты.

Пользователи, принимающие участие в атаке, ничего не теряют, если атака терпит неудачу; для атакующего атака будет прибыльной, если общее число выплаченных взяток меньше стоимости товара. Для сравнения, в PoW-системе подобная атака требуют от злоумышленника подкупа большинства майнеров. К тому же, в этом случае майнеры теряют ресурсы, потраченные на вычисления, если атака не удается, значит, сумма взяток, скорее всего, будет высокой. Атака не выполнима в системе с делегированным PoS по причинам, описанным в разделе 3.1.

3.5. Атака накоплением возраста монет

Эта атака относится к Peercoin и другим системам, использующим возраст монет вместо богатства в качестве меры пользовательской доли.

В первых версиях Peercoin, возраст монет не был ограничен. Это означало, что злоумышленник, достаточно долго подождав, может накопить достаточно монет, чтобы фактически овладеть сетью. Например, злоумышленник, обладающий пятью процентами всех монет, может разделить свои деньги на несколько выходов и подождать, пока возраст его UTXO станет в 10 раз выше среднего. После этого, злоумышленник может открыть несколько блоков подряд

с большой вероятностью (если его UTXO малы по отдельности), чтобы осуществить двойное расходование или другое вредоносное действие. Если было несколько пользователей, пытающихся осуществить эту атаку, это бы привело к серьезному ухудшению качества сети.

В более поздних версиях протокола Peercoin, возраст UTXO ограничен 90 днями. Аналогично, возраст монет ограничен в Novacoin и BlackCoin. Хоть ограничение и делает накопительную атаку намного менее вероятной, оно значительно уменьшает преимущества использования возраста монет перед долей в (3).

3.6. Атака предвычислением

Пусть A — минтер некоторого блока B_h высоты h; то есть A удовлетворяет (2) с параметрами, соответствующими B_h. Если A обладает существенной вычислительной мощностью, он может повлиять на хеш блока B_h, чтобы иметь возможность решить следующий блок B_{h+1}, например, добавляя новую транзакцию в B_h. Чтобы зарезервировать B_{h+1} для себя, A просматривает все профили пользователей и проверяет, выполняется ли условие (2) для каждого из разрешенных значений времени t. Если хеш B_h «плохой», то есть вычисления показывают, что следующий блок будет решен другим пользователем, злоумышленник изменяет параметры вставленной транзакции и пробует снова. Атакующий может построить длинную цепочку блоков, чтобы собрать больше комиссий и попытаться провести двойное расходование (строя свою цепь в секрете и выпуская затем все блоки сразу, чтобы обогнать правильный блокчейн с транзакцией, которую атакующий хочет обратить).

Эффективность предвычислительной атаки зависит от доли злоумышленника, а также от общего числа пользователей или UTXO в системе. В PoW-системе, эта атака фактически невозможна, так как сгенерировать блок с «хорошим» хешем намного сложнее, чем просто корректный блок. Аналогично, в системе с делегированным PoS последовательность лиц, подписывающих блоки, не зависит от свойств самого последнего блока; таким образом, DPoS-согласование является устойчивым к предвычислительным атакам.

3.7. Сравнение с доказательством работы

Основанные на PoW криптовалюты в некоторой степени подвержены двойному расходованию; тем не менее, возможность успешного двойного расходования постепенно уменьшается по мере роста количества подтверждений транзакции и сильно зависит от количества майнинговых мощностей, которыми обладает атакующий [21]. Чтобы уменьшить риск двойного расходования, продавцы обычно ждут определенного количества подтверждений (например, 6). В дополнение, существуют механизмы уменьшения рисков в быстрых платежах [22].

Типы атак, общие для для PoW и PoS — это отказ в обслуживании (англ. denial of service, DoS) и атака Сибиллы (англ. Sybil attack). DoS-атака направлена на то, чтобы прервать нормальное функционирование сети путем переполнения узлов. Например, злоумышленник может наполнить сеть транзакциями низкой стоимости, как это произошло при масштабной флуд-

атаке на сеть Биткойн в июле 2015 года [23]. В случае атаки Сибиллы злоумышленник подрывает функционирование сети, создавая значительное число некорректно ведущих себя узлов. Степень подверженности сети DoS-атакам и атакам Сибиллы зависит не только от типа согласования, используемого в сети, но и от деталей протокола сети. Не существует внутренних свойств, которые бы сделали PoS менее чувствительным к этим атакам, чем PoW.

Один из немногих векторов атаки, особенных для согласования доказательством работы, является эгоистичный майнинг (англ. selfish mining) [6]. При эгоистичном майнинге злоумышленник выборочно публикует блоки, чтобы вычислительные ресурсы других майнеров были потрачены впустую. Так как в случае PoS согласования дорогие ресурсы не вовлечены в создание блоков, эта атака не эффективна для PoS криптовалют. С другой стороны, нет никаких доказательств, что эгоистический майнинг был когда-либо успешно использован в Биткойне [24]; некоторые исследования утверждают, что описание атаки основано на некорректных предположениях [25].

В таблице 2 приведено сравнение доказательства работы и подтверждения доли по отношению к уязвимостям. Для согласования с использованием PoW степень подверженности атакам может быть предсказана, основываясь на суммарной хеширующей мощности системы. В случае PoS-систем, нет эквивалентной меры «состояния здоровья» сети:

- если валюта системы равномерно распределено между пользователями, система подвержена атакам, основанным на разветвлении блокчейна;
- если есть пользователи с большими долями, они могут подорвать работу сети (например, применяя к транзакциям цензуру).

Таблица 2. Уязвимость доказательства работы и подтверждения доли для различных векторов атаки

	Уязвимость		
Тип атаки	PoW	PoS	DPoS
Краткосрочная атака (например, взятка)	−	+	−
Атака издалека	−	+	+[3]
Атака накоплением возраста монет	−	возможно[4]	−
Атака предвычислением	−	+	−
Отказ в обслуживании, DoS	+	+	+
Атака Сибиллы	+	+	+
Эгоистичный майнинг	возможно[5]	−	−

[3] Может быть предотвращена с использованием социально-ориентированной безопасности

[4] Зависит от типа PoS-условия для корректных блоков

[5] Неясно, осуществим ли эгоистичный майнинг на практике

3.8. Стоимость атаки

3.8.1. Атака взятками

Рассмотрим следующий сценарий двойного расходования:

1. Злоумышленник расходует средства в транзакции, которую собирается позже обратить.
2. Сразу после транзакции, атакующий начинает строить альтернативную цепь, основываясь на блоке, предшествующем тому, в котором содержится эта транзакция. Построение альтернативной цепи происходит в тайне.
3. После того, как транзакция получает достаточное число подтверждений (например, 6) и цепь злоумышленника становится длиннее, чем действительная цепь, атакующий публикует ее полностью. Цепь атакующего принимается за новый действительный блокчейн, и транзакция становится обращенной, то есть недействительной.

Чтобы провести успешную атаку со стопроцентной вероятностью, злоумышленнику нужно контролировать более 50% ресурсов, используемых для защиты системы (вычислительная мощность в случае PoW, ликвидный капитал в случае PoS) на время атаки. Таким образом, в случае подтверждения доли атакующему не нужно обладать более чем половиной валюты — ему лишь нужно получить доступ к более чем половине валюты в обороте на несколько часов, например, заплатив взятки, как это описано в разделе 3.4. Сумма взяток пропорциональна вознаграждению, которое принимающие пользователи теряют за строительство не над действительным блокчейном (если подкупленные пользователи будут работать над обоими блокчейнами, блокчейн злоумышленника никогда не догонит действительный). Предположим, что:

- награды за минтинг осуществляются из комиссий за транзакции;
- количество транзакций в день — 100 000 (примерно равно количеству транзакций в день в Биткойн);
- комиссия за транзакцию — 0,10 $ (выше чем сейчас в Биткойн).

Тогда ежедневная награда за минтинг будет 10 000 $; если атака длится час, злоумышленнику понадобится заплатить взяток менее чем на 500 $.

Сравним это со стоимостью атаки в Биткойн. Награда за решение блока составляет 25 биткойнов, или около 5 000 $. В случае экономического равновесия, стоимость майнинга одного блока близка к этому числу; предположим, она равна 4 000 $. Если атака должна длиться 6 блоков, атакующему понадобится заплатить не менее чем за 7 блоков, чтобы обогнать действительный блокчейн (сумма составляет 28 000 $). Это более чем в 50 раз превосходит сумму взяток в случае подтверждения доли. Существует другое соображение, которое делает атаку на доказательство работы менее надежной и более дорогостоящей. Атака становится очевидной, как только блокчейн атакующего опубликован, потому что реорганизация последних шести блоков — статистически крайне редкое событие. Так как в экосистеме Биткойна довольно

немного крупных майнеров, участие в атаке отрицательно повлияет на их репутацию. В случае системы PoS фактор репутации играет второстепенную роль, так как большинство держателей валюты, скорее всего, анонимны.

PoS-системы могут представлять немного инфляционную экономику для вознаграждения минтеров. Рассмотрим систему с капитализацией 3 миллиарда $ (немного меньше, чем в Биткойн) и инфляцией 1 %. Ежедневная награда за минтинг в системе составляет

$$3 \cdot 10^9 \text{ \$} \cdot 0.01/365 \approx 82 \cdot 10^3 \text{ \$}.$$

Это число означает, что стоимость атаки продолжительностью 1 час близка к 3 400 $ — снова намного меньше, чем для Биткойна.

Чтобы атака была прибыльной, атакующему понадобится дважды израсходовать большую сумму денег. Соответственно, контрагент может запросить больше подтверждений для транзакции злоумышленника. Как в PoW, так и в PoS, прямая стоимость атаки растет линейно с необходимым количеством подтверждений; значит, отношение стоимостей должно быть примерно тем же. Тем не менее, в ходе атаки на PoW-систему, она становится всё более очевидной для участников системы, потому что атака сильно уменьшает хешрейт действительного блокчейна. Если в системе относительно немного майнеров (как в случае Биткойна), пользователи могут идентифицировать майнеров, принимающих участие в атаке, даже до того, как она закончится; если атакующие представляют собой майнинг пулы, их участники будут иметь стимул присоединиться к другим пулам или временно приостановить свою деятельность. В случае, если атака на PoS-криптовалюту проводится несколько раз, курс обмена этой валюты падает; в итоге злоумышленнику становится проще собрать ресурсы для последующих атак. Последнее не верно для PoW-криптовалют, так как расходы на майнинг (электричество, оборудование и т. д.) не зависят от курса обмена рассматриваемой валюты.

3.8.2. Атака накоплением

Рассмотрим атаку накоплением возраста монет, описанную в разделе 3.5. Этот тип атаки невозможен в PoW-системах; он возможен только в PoS-системах, где полный уничтоженный возраст монет определяет действительный блокчейн. Мы рассмотрим Peercoin как пример системы, уязвимой для атаки накоплением.

Предположим, атакующий хочет обратить транзакцию. Чтобы сделать это, он создает разветвленный блокчейн, для чего он уничтожает весь доступный ему возраст монет, перемещая свои средства на новые выходы (по-прежнему принадлежащие злоумышленнику). Блокчейн атакующего может перевесить действительный блокчейн в терминах уничтоженного возраста монет, если атака атака была произведена достаточно быстро и атакующий имеет достаточно возраста монет в своем распоряжении. Предположим у атакующего есть доля x от общего возраста монет в системе; наша цель — определить такое x, при котором атака будет успешной с вероятностью p. Пусть r_d — скорость уничтожения возраста монет в системе, то есть скорость,

с которой возраст монет уничтожается в транзакциях. (например, транзакции в Биткойн уничтожают ≈5 миллионов биткойн-дней каждый день[26], что означает $r_d \approx 5 \cdot 10^6$ биткойнов. Блок атакующего должен удовлетворять условию подтверждения доли (3); атакующему необходимо потратить некоторое время T, генерируя такой блок. T имеет экспоненциальное распределение с параметром t_0/x, где t_0 — ожидаемое время между блоками (в Peercoin, $t_0 = 10$ минут). Чтобы цепь атакующего победила с вероятностью p, возраст монет, уничтоженный честной частью сети (Tr_d) должен быть меньше, чем возраст монет, уничтоженный атакующим:

$$P\{Tr_d < xS\} = p.$$

Учитывая функцию распределения экспоненциальной случайной величины, получаем

$$\begin{aligned} 1 - \exp\Big(-\frac{x}{t_0} \cdot \frac{xS}{r_d}\Big) &= p; \\ x &= \sqrt{-\log(1-p)\frac{t_0 r_d}{S}}. \end{aligned} \tag{5}$$

Для того, чтобы получить численное значение доли атакующего x, необходимо выяснить отношение между скоростью уничтожения r_d и накопленным возрастом монет системы S. Если предположить, что накопленный возраст монет растет со временем, $r_d < B$, где B — общее количество валюты в обращении. Это неравенство справедливо для Peercoin, где $r_d \approx 10^7$ монет и $B \approx 2.3 \cdot 10^7$ монет [27]. Будем предполагать, что $r_d \approx B$. Возраст монет в Peercoin ограничен 90 днями. Таким образом, эффективный возраст монет для произвольного непотраченного выхода транзакции в условии (3) не может превысить 90 дней; соответственно, $S \leqslant B \cdot 90$ дней. Будем использовать значение, близкое к максимуму, — $S \approx B \cdot 60$ дней. Эта оценка подтверждается низкой интенсивностью транзакций в сети Peercoin [28].

Полученные оценки для r_d and S дают

$$x = \sqrt{-\log(1-p)\frac{10 \text{ минут} \cdot B}{B \cdot 60 \text{ дней}}} = \sqrt{-\log(1-p)\frac{1}{144 \cdot 60}}. \tag{6}$$

Чтобы атака состоялась с вероятностью $p = 0.5$, атакующему требуется $x \approx 0.9\%$ общего возраста монет; для значения $p = 0.9$ формула (6) дает $x \approx 1.6\%$.

Как и в других типах атак, атакующему не требуется *владеть* долей x от суммарного возраста монет в системе; он может подкупить других пользователей, чтобы те участвовали в атаке. Так как такие пользователи получает уменьшенную вероятность собирать комиссию за транзакции до тех пор пока их возраст монет не восстановится (т.е. на протяжении приблизительно 60 дней), общее количество взяток сравнимо с

$$x \cdot \langle \text{дневная награда за минтинг} \rangle \cdot 60 \text{ дней}/2.$$

Для системы с ежедневной наградой в 10 000 $ и $x = 1.6\%$ размер взяток составляет около 4 800 $. При этих предположениях возможно перезаписать блокчейн вглубь на $xS/r_d \approx 1$ день.

3.8.3. Атака издалека

Краткосрочные атаки, описанные ранее в этом разделе, становятся чересчур затратными в случае делегированного подтверждения доли, так что необходимо рассмотреть стоимость атак издалека. Для систем, использующих доказательство работы, затраты на атаку издалека запретительно велики. Например, атака на Биткойн длительностью в 1 000 блоков потребует по крайней мере 4 млн. $ (и, в отличие от краткосрочной атаки, она будет легко обнаружима, так как наблюдаемая хеширующая мощность сети упадет в два раза в течение длительного промежутка времени).

В ранних версиях подтверждения доли, стоимость атаки издалека намного ниже; как было показано выше, стоимость атаки длительностью в один день может составлять порядка 5 000 $ в случае, когда корректный блокчейн выбирается на основе общего уничтоженного возраста монет. В делегированном PoS атака в общем случае требует сговора 2/3 делегатов; ее стоимость сложно оценить, так как протоколы DPoS используют существенно различные методы для выбора, вознаграждения и наказания делегатов.

4. Модификации и гипотетические алгоритмы

4.1. Ссылки на блоки в транзакциях

В некоторых PoS-системах (напр., в BitShares, протоколе Chains of Activity, предложенном в *Cryptocurrencies without proof of work* [19], а также в алгоритме *Transactions as Proof of Stake* [29]), каждая транзакция может (но не обязана) включать хеш недавнего блока, известного создателю транзакции. Эта модификация деалает невозможным включение транзакции в блокчейн, который не содержит блока, на который ссылается транзакция. Таким образом, атакующий, создающий альтернативный блокчейн и пользователи системы, которые его поддерживают, создавая блоки поверх цепи блоков атакующего, не могут собрать комиссию за большинство транзакций.

Усовершенствование полагается на несколько оптимистичное допущение, что пользователи системы могут при любых условиях определить, какой блокчейн является корректным; оно не эффективно, если награда за создание блоков не определяется комиссией за транзакции.

4.2. Гибридное согласование PoW / PoS

Некоторые криптовалюты, использующие подтверждение доли, решают проблему начального распределения средств (раздел 3.2), применяя ограниченную версию доказательства работы для увеличения монетарной массы; примерами таких валют являются Peercoin и Novacoin. Гибридное согласование работает за счет создания двух типов корректных блоков:

- PoW-блоки, удовлетворяющие (1);
- PoS-блоки, удовлетворяющие (2) или схожему условию.

Основная альтернатива гибридному согласованию — полностью заранее созданный запас валюты (как в Nxt). Решение с PoW- и PoS-блоками, разделенными во времени, используется в Ethereum. В настоящее время Ethereum использует исключительно доказательство работы; введение PoS-согласование запланировано на будущее, когда система станет более зрелой.

Гибридное PoW / PoS-согласование устойчиво против атак издалека при условии, что безопасность системы обеспечивается достаточными хеширующими мощностями. Включение PoW-блоков в блокчейн также помогает защитить систему против других видов атак, описанных в разделе 3. Однако, так как подтверждение доли обычно вводится как альтернатива доказательству работы, комбинированные системы со временем отказываются от PoW полностью либо во всяком случае снижают его роль в системе.

4.3. Tendermint

Tendermint [30] — предложенная концепция блокчейна, в котором безопасность обеспечивается модифицированным протоколом согласования на основе подтверждения доли. В Tendermint каждый блок должен быть криптографически подписан *валидаторами*. Валидатор — это пользователь системы, который подтверждает свою заинтересованность в обеспечении безопасности, замыкая свои средства с помощью *залоговой транзакции* (англ. bonding transaction); вес мнения каждого валидатора пропорционально объему замкнутых средств. После окончания службы в качестве валидатора, пользователь получает доступ к замкнутым средствам за счет *возвращения залога* (англ. unbonding transaction); средства отпираются с определенной задержкой (англ. unbonding period).

Блок считается корректным, если он подписан валидаторами, которые в сумме имеют не менее $2/3$ общего веса голосов. Таким образом, форк блокчейна возможен только в случае, если существует группа валидаторов с не менее чем $1/3$ весом голосов, которая подписывает блоки в обоих конкурирующих блокчейнах. В случае форка валидаторов, подписывающие несколько блокчейнов, можно наказать за счет публикации произвольным пользователем транзакции-свидетельства (англ. evidence transaction), содержащей доказательство их злого умысла, например, их цифровых подписей блоков одинаковой высоты из обеих цепей. Транзакция-свидетельство уничтожает все заложенные средства валидаторов, действующих вне протокола. Эта логика предотвращает кратковременные атаки (такие как атаки взятками, описанные в разделе 3.4). В то же время, атаки издалека все еще возможны: валидаторы с $2/3$ общего веса голосов могут сговориться и опубликовать форк блокчейна после того, как их средства разблокированы. Для предотвращение долгосрочных атак можно использовать механизм, запрещающий длинные форки блокчейна (как в Nxt).

4.4. Slasher

Slasher — гибридный PoS / PoW-алгоритм согласования, описанный Виталиком Бутериным (Vitalik Buterin), одним из архитекторов Ethereum [31]. В отличие от других гибридных алго-

ритмов, для генерации блоков в Slasher используется исключительно доказательство работы; но при этом каждый блок валидируется как PoW, так и PoS.

Блоки создаются при помощи доказательства работы (1). Вместо того, чтобы включать coinbase-транзакцию для получения вознаграждения за решенный блок, майнер включает в блок число $\text{hash}(n)$ для некоторого большого натурального числа n. Это число служит доказательством майнинга; майнер может забрать положенную ему награду за блок, создав специальную транзакцию, открывающую n. Награда за майнинг замкнута на 100 блоков и ограничена во времени: награду за блок на высоте h можно получить за счет транзакции, записанной в одном из блоков с высотой $h + 100$, $h + 101$, ..., $h + 900$. Среднее время между созданием блоков равно 30 секундам.

Чтобы создать корректный блок, он должен быть криптографически подписан. Подписывающие пользователи выбираются случайным образом с использованием условия, похожего на (2):

$$\text{Signers}(h) = \{A : \text{hash}(n(h-2000), n(h-1999), ..., n(h-1901), A) \leqslant 64M\,\text{bal}(A)/B\}, \qquad (7)$$

где $B = \sum_a \text{bal}(a)$ — общее количество монет в обращении, а $n(i)$ — доказательство майнинга, использованное в блоке i. Уравнение (7) означает, что в среднем каждый блок могут подписать 64 пользователя, а вероятность стать подписчиком пропорциональна объему средств, которыми владеет пользователь. Для определения корректного блокчейна при форке используется суммарное количество подписей. Подписав блок, пользователь получает награду, замкнутую в течение следующих 1 000 блоков. Награда за подпись выше, чем награда за майнинг, с целью предотвратить гонку вооружений среди майнеров.

Для борьбы с форками блокчейна Slasher использует механизм, аналогичный Tendermint. Если пользователь системы видит несколько блоков одинаковой высоты, подписанные одним и тем же валидатором, пользователь может опубликовать транзакцию с этими двумя подписями. Если эта транзакция будет включена в блок прежде чем награда за блок станет доступна для использования недобросовестным валидатором, 33 % награды выплачивается пользователю, обнаружившему отступление от протокола, а остальные средства уничтожаются.

Имплементация подтверждения доли, используемая в Slasher, в большой степени предотвращает краткосрочные форки блокчейна. В самом деле, уязвимость PoS к краткосрочным атакам проистекает из следующего наблюдения. В модели PoS (2), вероятности создать блок для каждой из конкурирующих цепей независимы друг от друга, так как они зависят от хеша последнего блока цепи. Для пользователей системы имеет смысл пытаться создать блоки на основе каждой из цепей, так как это увеличивает ожидаемое вознаграждение. С другой стороны, в Slasher вероятность стать валидатором блока определяется с большим временным интервалом и одинакова для всех цепей, если они относительно малы. Таким образом, у пользователей нет оснований поддерживать форк блокчейна, так как они заранее знают, будут ли они подписывать блоки в будущем. Для пользователей не имеет поддерживать несколько ветвей блокчейна, если у них нет уверенности, что форк просуществует более 2 000 блоков.

Так как Slasher использует доказательство работы для создания блоков, атаки издалека требует существенных вычислительных мощностей. Это дает Slasher существенно преимущество по сравнению с моделями делегированного PoS, которые не используют доказательство работы (например, BitShares).

4.5. Casper

Casper — концептуальный алгоритм подтверждения доли, предложенный разработчиком Ethereum Vlad Zamfir [32]. По аналогии с Tendermint, в Casper использует понятие валидаторов блоков. Валидатор ставит на блоки, присваивая каждому из них вероятность; сумма вероятностей для блоков на одинаковой высоте должна равняться единице. Для того чтобы выбрать единственный блок с конкретной высотой, валидаторам, возможно, требуется несколько раундов голосования, пока по крайней мере $2/3$ валидаторов не сделают ставку на один и тот же блок с высокой вероятностью (например, 99 %). Чтобы противостоять атакам большинства валидаторов, Casper наказывает отклонения от протокола за счет уничтожения наград за создание блоков и заложенных средств валидаторов.

5. Заключение

На настоящий момент существуют несколько цифровых валют, в которых в той или иной мере реализовано подтверждение доли; примеры таких валют — Peercoin, Nxt, Novacoin, BlackCoin и BitShares. Однако походы, использующие подтверждение доли в чистом виде, подвержены серьезным угрозам безопасности, которые невозможно воспроизвести в валютах, использующих доказательство работы (включая Биткойн). Эти проблемы внутренне присущи PoS-алгоритмам, так как согласование на основе подтверждения доли не укреплено в физическом мире (ср. с оборудованием для решения блоков в рамках доказательства работы).

Поэтому практически все валюты, полагающиеся на подтверждение доли, используют дополнительные средства защиты для обеспечения безопасности. Например, проблема начального распределения средств может быть решена за счет использования ограниченной во времени версии доказательства работы; атаки повторного расходования можно предотвратить, включив информацию о недавних блоках в транзакции. Тем не менее, эти модификации можно рассматривать как спонтанные и неполные. В отличие от PoW, согласование на основе подтверждения доли не является объективным; новые пользователи не могут точно определить состояние PoS-системы на основе исключительно правил протокола и данных, полученных от узлов системы. Для того чтобы исключить возможность длинных форков блокчейна, PoS-система должна быть слабо субъективной, дополняя правила протокола безопасностью, обеспечиваемой социально. Социальная компонента систем, использующих подтверждение доли, ослабляет их децентрализацию и математическую обоснованность. Как отмечено в [20], «Все “чистые” PoS-системы по сути содержат постоянную знать; конечное слово в таких системах

всегда остается за держателями средств в генезис-блоке. Не важно, что произойдет через миллион блоков; участники генезис-блока всегда могут собраться, запустить форк с альтернативной историей транзакций и обеспечить победу этого форка» (перевод наш).

Относительно недавнее развитие идеи подтверждения доли — делегированные системы. Хотя такие системы решают несколько значительных проблем, присущих прямолинейным реализациям PoS, они еще не слишком распространены, что усложняет задачу оценки их безопасности. Тем не менее, делегированное подтверждение доли решает проблему «ничего на кону» и предотвращает краткосрочные атаки на систему.

Приложение A. Распределение времени создания блока

Предположим, что все действительные блоки в блокчейн-протоколе удовлетворяют условию

$$U \leqslant \theta \leqslant 1, \tag{8}$$

где $U \sim [0,1]$ — равномерно распределенная случайная величина, сгенерированная путем хеширования определенных данных и нормализации полученной величины. Согласно свойствам хеш-функций, доказательство работы (1) и подтверждение доли являются частными случаями (8):

- в случае PoW, $\theta = 1/D$;
- в случае PoS, $\theta = \text{bal}(A)/D$, где $\text{bal}(A)$ означает долю пользователя в системе.

Чтобы сгенерировать блок, пользователь должен найти данные, которым соответствует U, удовлетворяющее (8). Пусть N обозначает количество вариантов данных, которые пользователь должен проверить, прежде чем найти подходящее значение. В доказательстве работы пространство поиска велико, поэтому пользователь может пробовать r комбинаций в секунду, где r определяется майнинговым оборудованием и теоретически ничем не ограничено. В случае доказательства работы (2) пространство поиска мало, поэтому мы можем считать $r = 1$. Время T, необходимое для нахождения блока, связано с N как $T = N/r$. Рассмотрим функцию распределения

$$P\{T \leqslant t\} = P\{N \leqslant rt\} = 1 - P\{N > rt\} = 1 - (1-\theta)^{rt} = 1 - \exp(\log(1-\theta)rt).$$

В предположении $\theta \ll 1$ (а это обычно имеет место),

$$\log(1-\theta) \approx -\theta; \quad P\{T \leqslant t\} \approx 1 - \exp(-\theta rt).$$

Итак, T имеет экспоненциальное распределение с параметром θr. В случае PoW, параметр равен r/D, в случае PoS он равен $\text{bal}(A)/D$.

Приложение B. Распределение создателей блоков в Nxt

Как было сказано в разделе 2.2, Nxt описывается вероятностной моделью, фундаментально отличающейся от других криптовалют. Это можно интуитивно увидеть из PoS-неравенства (4), используемого в Nxt: оно использует параметр времени другим способ, чем PoW (1) или общий PoS (2). Анализ (4), проведенный в белой книге Nxt [14] недостаточно убедителен, поэтому было решено провести собственное исследование на эту тему.

Предположим, есть n пользователей Nxt с относительными балансами

$$b_1 \geqslant b_2 \geqslant \ldots \geqslant b_n > 0, \quad \sum_{i=1}^{n} b_i = 1.$$

Подтверждение доли (4) приписывает каждому пользователю равномерно распределенную случайную величину $U_i \sim [0, 1/b_i]$. Пользователь создает следующий блок, если значение его величины меньше значений остальных величин. Значит, вероятность открыть блок для пользователя i, равна

$$p_i = P\{U_i = \min_j U_j\}.$$

Интегрируя по вероятностному пространству, мы получаем

$$p_i = \prod_{j=1}^{n} \frac{1}{b_j} \int_0^{1/b_i} dx_i \underbrace{\int_{x_i}^{1/b_1} dx_1 \int_{x_i}^{1/b_2} dx_2 \ldots \int_{x_i}^{1/b_n} dx_n}_{n-1 \text{ интегралов по } x_j, j \neq i}.$$

После простых преобразований,

$$p_i = b_i \int_0^{1/b_1} \prod_{j \neq i} (1 - b_j x)\, dx,$$

или, раскрывая произведение

$$p_i = b_i \sum_{j=0}^{n-1} \frac{(-1)^j B_j^{(i)}}{(j+1) b_1^{j+1}}, \tag{9}$$

где $B_j^{(i)}$ — сумма по произведениям наборов из j элементов из множества балансов b, которые не включают b_i. (Например, если $n = 4$,

$$\begin{aligned} B_1^{(0)} &= 1; \\ B_1^{(1)} &= b_2 + b_3 + b_4; \\ B_1^{(2)} &= b_2 b_3 + b_2 b_4 + b_3 b_4; \\ B_1^{(3)} &= b_2 b_3 b_4, \end{aligned}$$

и так далее.) Выражение (9) не поддается анализу в общем случае; мы рассмотрим несколько важных случаев.

Равные доли. Предположим $b_i = 1/n$. В этом случае,

$$p_i = \frac{1}{n} \int_0^n \Big(1 - \frac{x}{n}\Big)^{n-1} dx = \frac{1}{n} \Big(1 - \frac{x}{n}\Big)^n \Big|_n^0 = \frac{1}{n},$$

то есть распределение честное.

Одна большая доля. Предположим

$$b_1 = a; \quad \forall i = 2, \ldots, n \quad b_i = b = \frac{1-a}{n-1}.$$

то есть существует пользователь с большой долей a, и много пользователей с малыми равными долями b.

$$p_1 = a \int_0^{1/a} (1 - bx)^{n-1}\, dx = a \frac{1 - (1 - b/a)^n}{nb}.$$

Соответственно, разность между фактической и честной вероятностями обнаружить блок для пользователя с большой долей равняется

$$p_1 - a = \frac{a}{nb}(1 - nb - (1 - b/a)^n).$$

Вспомним, что b можно выразить через a и n:

$$p_1 - a = \frac{n-1}{n} \frac{a}{1-a} \left[1 - \frac{n(1-a)}{n-1} - \Big(1 - \frac{1-a}{a(n-1)}\Big)^n\right].$$

Когда пользователей много,

$$\lim_{n\to\infty} p_1 = a + \frac{a}{1-a}\big[a - e^{(a-1)/a}\big].$$

Это означает, что пользователь с большой долей имеет преимущество: процент его блоков строго больше его доли в системе (см. рис. 2). Таким образом, Nxt не является честной системой.

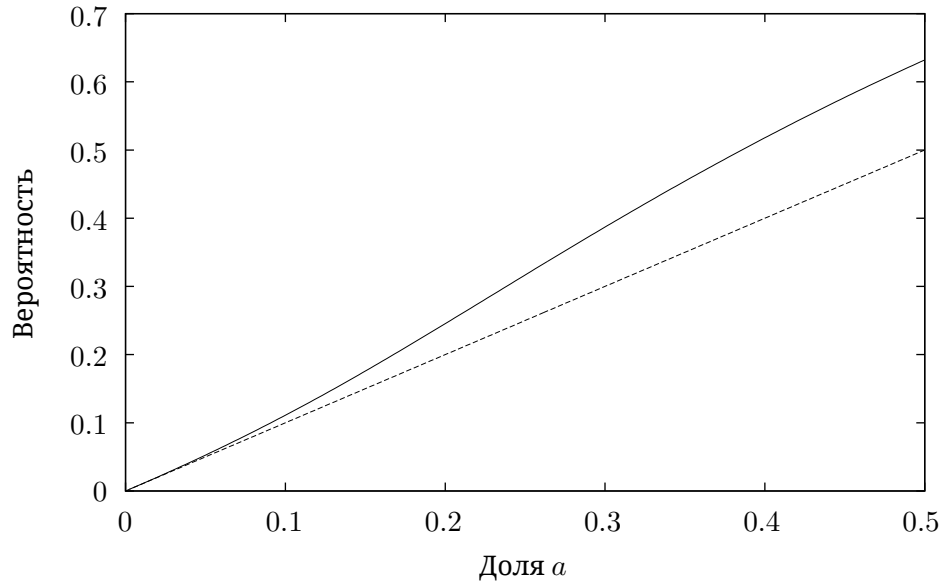

Рис. 2. Вероятность создать блок в Nxt в зависимости от доли в системе

Чтобы сделать Nxt честным, белая книга [14] предлагает простую модификацию, основанную на следующем наблюдении: если $U \sim [0, 1]$, то $-\log U/b$ — экспоненциально распределенная случайная величина с параметром b. Таким образом, если изменить подтверждение доли (4) на

$$\log M - \log \mathrm{hash}(\mathrm{hash}(B_{prev}), A) \leqslant t\, \mathrm{bal}(A)/D,$$

вероятности открыть блок будут честными. Тем не менее, предложение остается нереализованным.

Список литературы

[1] Thin client security // Bitcoin Wiki.
URL: https://en.bitcoin.it/wiki/Thin_Client_Security

[2] *Seth Gilbert, Nancy Lynch*. Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services // ACM SIGACT News. — 2002. — № 33 (2). — pp. 51–59.

[3] *Werner Vogels*. Eventually consistent - revisited. — 2008.
URL: http://www.allthingsdistributed.com/2008/12/eventually_consistent.html

[4] Merkle tree // English Wikipedia.
URL: https://en.wikipedia.org/wiki/Merkle_tree

[5] SHA-2 // English Wikipedia.
URL: https://en.wikipedia.org/wiki/SHA-2

[6] *Ittay Eyal, Emil Gün Sirer*. Majority is not enough: Bitcoin mining is vulnerable. — 2013.
URL: http://arxiv.org/pdf/1311.0243v5

[7] Sybil attack // English Wikipedia.
URL: https://en.wikipedia.org/wiki/Sybil_attack

[8] *Vitalik Buterin*. Proof of stake: How I learned to love weak subjectivity // Ethereum Blog. — 2014.
URL: https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/

[9] Crypto-currency market capitalizations
URL: http://coinmarketcap.com/

[10] *Sunny King, Scott Nadal*. PPCoin: peer-to-peer crypto-currency with proof-of-stake. — 2012.
URL: http://www.peercoin.net/assets/paper/peercoin-paper.pdf

[11] Transaction fees // Bitcoin Wiki.
URL: https://en.bitcoin.it/wiki/Transaction_fees

[12] Checkpoint lock-in // Bitcoin Wiki.
URL: https://en.bitcoin.it/wiki/Checkpoint_Lockin

[13] Nxt whitepaper // Nxt Wiki.
URL: https://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt

[14] *mthcl*. The math of Nxt forging. — 2014.
URL: http://www.docdroid.net/e29h/forging0-5-1.pdf.html

[15] Proof of work // Novacoin Project Wiki.
URL: https://github.com/novacoin-project/novacoin/wiki/Proof-of-work

[16] Proof of stake // Novacoin Project Wiki.
URL: https://github.com/novacoin-project/novacoin/wiki/Proof-of-stake

[17] *Pavel Vasin*. BlackCoin's proof-of-stake protocol v2. — 2014.
URL: http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

[18] *Daniel Larimer, Charles Hoskinson, Stan Larimer*. BitShares: a peer-to-peer polymorphic digital asset exchange. — 2014.
URL: http://scribd.com/doc/173481633/BitShares-White-Paper

[19] *Iddo Bentov, Ariel Gabizon, Alex Mizrahi*. Cryptocurrencies without proof of work. — 2013.
URL: http://www.cs.technion.ac.il/~idddo/CoA.pdf

[20] *Vitalik Buterin*. On stake // Ethereum Blog. — 2014.
URL: https://blog.ethereum.org/2014/07/05/stake/

[21] *Meni Rosenfeld*. Analysis of hashrate-based double-spending. — 2012.
URL: https://bitcoil.co.il/Doublespend.pdf

[22] *Ghassan O. Karame, Elli Androulaki, Srdjan Capkun*. Two bitcoins at the price of one? Double-spending attacks on fast payments in Bitcoin. — 2012.
URL: http://eprint.iacr.org/2012/248.pdf

[23] July 2015 flood attack // Bitcoin Wiki.
URL: https://en.bitcoin.it/wiki/July_2015_flood_attack

[24] *Matt Springer*. Is Bitcoin currently experiencing a selfish miner attack? // ScienceBlogs. — 2014.
URL: http://scienceblogs.com/builtonfacts/2014/01/11/is-bitcoin-currently-experiencing-a-selfish-miner-attack/

[25] *Ed Felten*. Game theory and Bitcoin // Freedom to Tinker. — 2013.
URL: https://freedom-to-tinker.com/blog/felten/game-theory-and-bitcoin/

[26] Bitcoin days destroyed // Blockchain.info.
URL: https://blockchain.info/charts/bitcoin-days-destroyed

[27] Peercoin charts live // blockr.io (получено 07 сен. 2015).
URL: http://ppc.blockr.io/charts

[28] Peercoin block explorer // blockr.io (получено 07 сен. 2015).
URL: http://ppc.blockr.io/

[29] *Daniel Larimer*. Transactions as proof-of-stake. — 2013.
URL: http://bravenewcoin.com/assets/Uploads/TransactionsAsProofOfStake10.pdf

[30] *Jae Kwon*. Tendermint: consensus without mining. — 2015.
URL: http://tendermint.com/docs/tendermint.pdf

[31] *Vitalik Buterin*. Slasher: a punitive proof-of-stake algorithm // Ethereum Blog. — 2014.
URL: https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/

[32] *Vlad Zamfir*. Introducing Casper “the friendly ghost” // Ethereum Blog. — 2015.
URL: https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/