Coda: Экономика и Монетарная Политика

Бред Кон, Эван Шариро и Эмре Текизалп

O(1) Labs

16 Января 2020

Предисловие

Поскольку криптовалюты становятся все более популярными и широко используемыми, стоимость проверки блокчейна растет пропорционально общей пропускной способности транзакций и быстро становится недоступной для большинства реальных пользователей. Таким образом, криптовалюты могут в конечном итоге стать жертвами собственного успеха, становясь все более недоступными для своих пользователей, которым в свою очередь приходится доверять посредникам. Протокол Coda решает эту проблему, заменяя блокчейн легко проверяемым доказательством. Такой протокол требует тщательного разделения ролей, структуры стимулов и разумной денежно-кредитной политики, чтобы функционировать должным образом и противостоять атакам.

1 Введение

Комбинируя криптографические методы с экономическими стимулами, Биткойн[Nak09] стал первым децентрализованным протоколом одноранговых платежей. Критическим аспектом дизайна Биткойна является степень, в которой различные компоненты усиливают и укрепляют друг друга. Например, POW (доказательство выполнения работы) накладывает стоимость на производство блоков, что не позволяет злоумышленникам подменять транзакции. Однако это резко увеличивает требование на хранение истории транзакций в блокчейне, потому что любая подмена транзакций сразу видна для всем пирам в сети с недорогим оборудованием. Этот метод, делающий атаки дорогостоящими и защиту дешевыми, является краеугольным камнем современной криптографии и отличительной чертой хорошо разработанного крипто- экономического протокола.

Тем не менее, дизайн Биткойна имеет некоторые ограничения. Хотя блокчейны обеспечивают быстрое обнаружение несанкционированного доступа, они не обеспечивают быстрого подтверждения правильности. Фактически, каждый раз, когда новый участник присоединяется к сети, он должен проверять каждую транзакцию с самого начала сети(генезис), чтобы проверить корректность истории транзакций. Это требование растет линейно с общей пропускной способностью транзакций и быстро становится недоступным для большинства реальных пользователей на устройствах с ограниченными ресурсами, таких как смартфоны. Таким образом, по мере того, как криптовалюты становятся все более популярными и широко используемыми, они становятся заложниками собственного успеха и становятся все более недоступными для своих пользователей, которым, в свою очередь, приходится доверять посредникам.

Рекурсивные zk-SNARK обеспечивают решение этой дилеммы. Подобно тому, как блокчейн обеспечивает постоянный контроль несанкционированного изменения истории транзакций, рекурсивные zk-SNARK позволяют проверять неизменность истории транзакций. Вместо того, чтобы каждый участник в сети проверял историю транзакций для себя, сеть сотрудничает, чтобы сгенерировать доказательства правильности транзакций (zk-SNARK), а затем делится ими в сети. Таким образом, вместо того, чтобы конечные пользователи доверяли посредникам в предоставлении точной информации о состоянии истории транзакций, им предоставляется состояние вместе с zk-SNARK, который криптографически гарантирует, что это состояние является подлинным. Протокол Coda заменяет блокчейн легко проверяемым доказательством. Для получения дополнительной информации о технической реализации этого протокола см. Технический документ [MRS19].

Такой протокол требует тщательного разделения ролей, структуры стимулов и разумной денежно- кредитной политики, чтобы функционировать должным образом и противостоять атакам. Рассмотрим ниже основные концепции дизайна.

2 Сетевые роли и стимулы

В сетях большинства криптовалютных протоколов есть как минимум две роли: 1) те, кто проверяет каждую транзакцию в сети, часто называемые полными узлами(нодами), стейкерами(POS) или майнерами(POW) 2) те, кто доверяет третьим сторонам проверять транзакции для них, такие как легкие клиенты(полные ноды, предоставляющие услуги). По мере распространения и использования этих протоколов, проверка блокчейна становится все более дорогостоящей, поэтому все больше участников выходят из первой группы и переходят во вторую. Например, хотя исторически сложилось так, что биткойн в среднем имеет менее 1,5 транзакций в секунду, новый участник сети должен проверить около 500 000 000 транзакций, чтобы обеспечить полную безопасность узла. Эта проблема усугубляется тем, что некоторые протоколы утверждают, что имеют пропускную способность большую чем Биткойн в 10– 100 000 раз и теоретически могут генерировать гигабайты или терабайты данных каждую неделю при пиковых нагрузках.

Coda, напротив, имеет постоянные требования к ресурсам: независимо от того, сколько транзакций обработала сеть, пользователи могут полностью проверить текущее состояние с помощью небольшого zk-SNARK. Чтобы поддерживать это, у Coda есть три роли в сети, каждая из которых стимулируется к участию различными механизмами.

2.1 Верификаторы

Мы ожидаем, что подавляющее большинство участников сети будут способны верифицировать текущие состояния. Поскольку Coda использует рекурсивные zk-SNARK для непрерывного подтверждения достоверности состояния, полная безопасность узла достигается простой загрузкой zk-SNARK, которая примерно составляет нескольких сотен байтов и для проверки требуется несколько миллисекунд вычислений. zk-SNARK сертифицирует информацию консенсуса и корень Merkle до актуального состояния блокчейна. На этом этапе верификаторы могут запрашивать пути Merkle к соответствующим частям состояния. Проверяя путь Merkle, верификаторы гарантируют, что части состояния, о которых они заботятся (например, об остатках на балансах), действительно содержатся в том же блокчейне, который сертифицирован zk- SNARK.

2.2 Производители блоков

Производители блоков похожи на майнеров или стейкеров в других протоколах. Они стимулируются в форме вознаграждений за блок в виде коинбейз транзакций, а также комиссиями в сети, выплачиваемыми пользователями за их транзакции. Важно отметить, что производители блоков не заинтересованы в «угрозе урезания», поскольку Coda использует Ouroboros[DGKR17]. В дополнение обычному стейкингу, отдельные лица могут делегировать свою долю другому производителю блоков. Это позволяет делегату стейкать - но не отправлять транзакции от другого имени.

Как правило, производители блоков выбирают, какие транзакции включать в следующий блок. Очевидно, они заинтересованы включать транзакции с самой высокой комиссией. Однако, чтобы блокчейн оставался сжатым, производители блоков несут дополнительную ответственность: для каждой транзакции, которую они добавляют в блок, они должны создать снарк для эквивалентного количества ранее добавленных транзакций. Если они этого не сделают, их блок не будет соответствовать правилам консенсуса и будет отклонен другими узлами. Этот факт удобно представить как очередь транзакций, например, производитель блока хочет добавить 10 транзакций в конец очереди (они могут требовать комиссионные за транзакции), он должен создать снарк 10-ти транзакций в начале очереди. Они могут сами производить эти SNARK'и или выбрать их на маркетплейсе, которому способствуют другие специализированные участники сети, Снаркеры(Снарк воркеры), которые мы обсудим ниже.

2.3 Снаркеры

Снаркеры, описанные в техническом whitepaper Coda[MRS19], являются участниками сети, которые создают zk-SNARK, проверяющие транзакции. Они компенсируют свою работу размещением комиссий, называемые заявками в маркетплейсе и, если их SNARK'и используются в блоке, то производитель блока выплачивает эти комиссии из общей суммы комиссий за транзакции в блоке.

Учитывая тот факт, что многие Снаркеры могут размещать комиссии за одну и ту жетуже транзакцию, производители блоков заинтересованы в том, чтобы минимизировать комиссии, которые они платят за созданный SNARK, это естественно формирует рынок, где участники соревнуются в создании наиболее дешевых доказательств zk-SNARK. Для удобства мы можем обозначить это как Snarketplace. Ниже мы рассмотрим некоторые из его экономических показателей.

Во-первых, до тех пор, пока в сети имеется некоторое количество скрытых вычислений - почти наверняка обеспеченных сетью производителей блоков Snarketplace не будет влиять на жизнеспособность или устойчивость протокола, поскольку всегда будет предложение производить SNARK'и по какой-либо цене.

Чтобы убедиться в этом, рассмотрим стимул участника сети, у которого есть свободные вычислительные мощности и который наблюдает за ростом комиссий SNARK в сети из-за отсутствия предложений произведенных SNARK. Когда комиссии SNARK превышают предельные издержки производства SNARK для этого участника, если они являются экономически рациональными, они начинают предлагать заявки выше своей цены производства и ниже рыночной цены, чтобы получить прибыль, следовательно, стабилизируя комиссии SNARK. Производители блоков могут просто передать эти комиссии тем, кто совершает транзакции. На практике стоимость вычислений для генерации SNARK должна быть чрезвычайно низкой, примерно меньше цента за транзакцию при текущих ценах облачных вычислений.

Во-вторых, учитывая эффект масштаба, возможно, что некоторые операции SNARK со временем станут более доминирующими, как некоторые операции майнинга с биткойнами. Однако любая концентрация производства SNARK не будет иметь никакого отношения к централизации или жизнеспособности протокола. Это потому, что любой сможет производить SNARK'и по какой-то цене. Таким образом, даже если бы был какой-нибудь производитель SNARK, который мог бы предложить более дешевые SNARK'и, и если бы они отказались обрабатывать определенные транзакции, любой другой пользователь в сети мог бы предоставить SNARK за чуть более высокую плату, и производители блоков все равно были бы заинтересованы в том, чтобы включить его в реестр. В-третьих, механизм добровольной координации, который предотвращает двойное доказательство, вероятно, уменьшит комиссии SNARK и бесполезные вычисления в сети, хотя такой механизм не нужен для обеспечения безопасности или жизнеспособности.

2.3.1 Устойчивость к цензуре

Возможно, стоит немного уделить внимание и поддержать идею сопротивления цензуре. Несмотря на то, что существует ряд вероятных атак на сопротивление цензуре биткойнов[NBF16], оказывается, что вы можете быть включены в блок, если вы просто заплатите достаточно высокую комиссию или будете ждать достаточно долго. Coda очень похожа на биткойн, с дополнительным усложнением, что вам нужно, чтобы ваша транзакция была сжата в какой-то момент после ее включения в блок.

Таким образом, чтобы Coda не была устойчивой к цензуре, транзакция должна быть включена в блок, а затем никто не должен предложить для нее Snark. Это потребовало бы сговора между всеми Снаркерами (которые отказались бы от этой транзакции) или всеми производителями блоков (которые решили бы не включать Snarked-транзакцию в обновления реестра). Исходя из предположений Ouroboros, мы можем предположить, что сеть децентрализована, и поэтому производители блоков не вступают в сговор.

Теперь давайте посмотрим на Снаркеров. Поскольку вычислительные затраты на Snarking для транзакции чрезвычайно низки и доступны любому, у кого есть компьютер, заставить всех Снаркеров вступить в сговор гораздо сложнее, чем заставить всех производителей блоков вступить в сговор. Существующие Снаркеры не могут помешать новому Снаркеру войти в рынок. Если кто-то заметит, что транзакция не была сжата, он мог бы легко и выгодно предложить ее SNARK, и даже при очень низкой плате за транзакцию производитель блоков мог бы выгодно включить Snarked транзакцию в обновление реестра.

Время жизни транзакции Coda

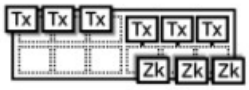
- Верификатор выполняет транзакцию
- Она приходит в мемпул
- Она растространяется в сети

Тем временем…

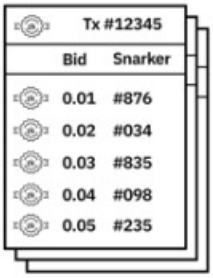
Снарк воркеры создают доказательства для несжатых (unsnarked) транзакций

Дальше выбирается производитель блоков (ПБ)

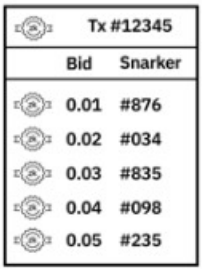
ПБ смотрит в свой мемпул и выбирает самые выгодные транзакции чтобы добавить в следующий блок



ПБ должен добавить в блок столько снарков сколько транзакций он добавил

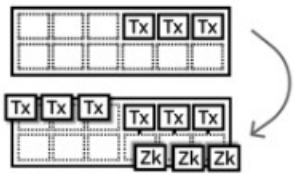


ПБ смотрит в список предложений снарков для каждой транзакции и покупает самые дешевые



Каждая недавно добавленная транзакция имеет свой собственный список предложений снарков и каждаый соревнуется за лучшую цену

Эти снарки должны соответствовать несжатым (unsnarked) транзакциям добавленным в очередь

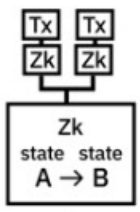


ПБ добавляет новые транзакции и снарки(из ранее добавленных транзакций) в очередь

ПБ добавляет новый блок в блокчейн Coda

Очередь состояния обновляется для поддержания постоянного размера (новые добавленные и сжатые транзакции удаляются)

Новые блоки распространяются и валидируются



ПБ обновляет zk snark для блокчейна

Экономика Coda

3 Терминология и обозначения

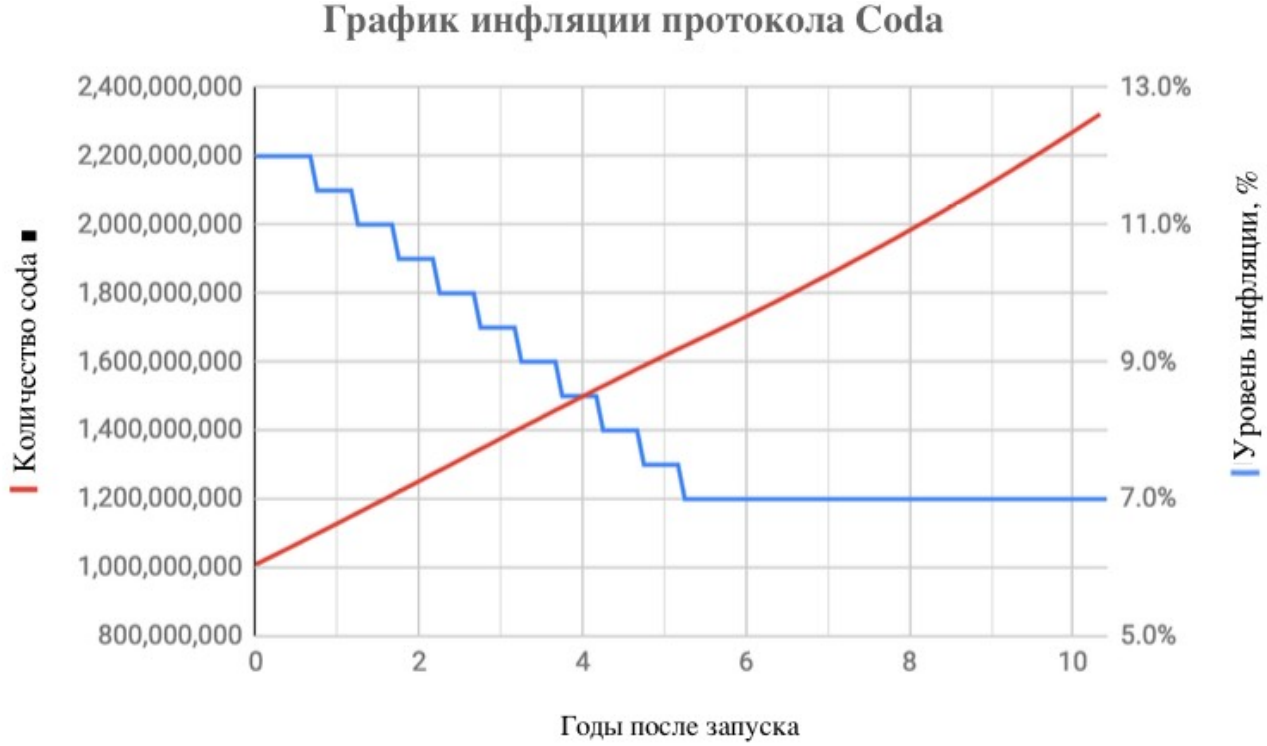
Отдельные единицы валюты называются coda и обозначаются символом валюты: ◼ (UTF-16: U+25FC). Начальное количество Coda составляет ◼1,000,000,000 (1 миллиард). Каждая coda делится на 1 миллиард единиц (нанокода). Промежуточные наименования валюты используют стандартные префиксы метрик:

1. ◼1 = 1 кода
2. ◼0.01 = 1 центикода
3. ◼1^-6 = 1 микрокода

4 Денежная политика

Поскольку Coda использует вариант Ouroboros Proof of Stake[DGKR17][MRS19], вознаграждения за блоки и сборы распределяются приблизительно пропорционально текущим владением, пока все в сети делают стейкинг. Следовательно, если участников стейкинга становится больше, любая номинальная инфляция в протоколе аннулируется номинальной доходностью, выраженной в протоколе, гарантируя, что пропорциональное владение аккаунтов остается постоянным.

Однако участники, которые не будут участвовать в стейкинге или делегировать, будут испытывать размывание своих кода по сравнению с теми, кто стекает. Чтобы мотивировать участников начать делать стейкинг, номинальная инфляция Coda начнется с 12%, затем в течение первых пяти лет, уровень инфляции снизится до 7%, а после этого по умолчанию останется на уровне 7%, но может измениться в результате управления сетью.



Важно отметить, что протокол спроектирован так, что уровень инфляции не будет зависеть от уровня участия в стейкинге. Это означает, что вознаграждение за блок будет динамически ски меняться, чтобы соответствовать этому уровню инфляции. Например, если стекеров 50%, тогда награда за блок удвоится. Это связано с тем, что в расчете на Ouroboros число блоков, произведенных за эпоху, будет пропорционально коэффициенту стейкинга. Это естественно будет, побуждать все больше людей стейкать.

[1] Документ управления сетью в разработке

Основным соображением при снижении уровня инфляции будет определение того, будут ли вознаграждения выше, чем это необходимо, чтобы у производителей блоков был достаточный стимул для проверки без необходимости значительного увеличения комиссий.

Также важно понять, как денежная политика обеспечивает постоянное развитие децентрализованной сети Coda. Инфляция в форме награды за блок используется для защиты блокчейна от атак путем стимулирования проверки со стороны производителей блоков. Однако безопасность - не единственное требование для новой сети. А именно, долгосрочное поддержание и улучшение протокола также потребует финансирования. Мы предлагаем наиболее подходящий механизм для этого - создание специальных наград за блоки, назначаемых получателям в соответствии с определением руководства сети.

Ссылки

[DGKR17] Bernardo David, Peter Gaži, Aggelos Kiayias, and Alexander Russell. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake protocol. Cryptology ePrint Archive, Report 2017/573, 2017. https://eprint.iacr.org/2017/573.

[MRS19] Izaak Meckler, Vanishree Rao, and Evan Shapiro. *Coda: Decentralized Cryptocurrency at Scale, 2019.*

[Nak09] Satoshi Nakamoto. Bitcoin: *A peer-to-peer electronic cash system, 2009.*

[NBF+16] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction,* 2016. Feather Forking.