

Децентрализованная репутационная сеть: Основа для естественной организации общества

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

Чувство справедливости—убеждённости в том, что несправедливость исправляется, а заслуги вознаграждаются,—является сильнейшей связующей силой общества. Когда централизованные институты управления не способны обеспечить это чувство, поскольку издержки на защиту права превышают ценность самого права, социальная сплочённость размывается. Нынешние институциональные структуры не справляются со значительным классом споров ровно так же, как централизованное планирование не справляется с распределением ресурсов: через информационную асимметрию, отсутствие обратных связей и оторванность лиц, принимающих решения, от последствий этих решений. В настоящей работе представлена репутационная социальная сеть (RSN): децентрализованный, неподкупный и устойчивый к цензуре коммуникационный уровень, построенный на децентрализованных идентификаторах (DID), который позволяет псевдонимным участникам публиковать, проверять и потреблять репутационную информацию о поведении в реальном мире. Основной механизм опирается на три принципа проектирования: (1) асимметричную структуру издержек, при которой чтение репутационных данных обходится дешево, а запись требует проверяемых усилий; (2) недетерминированный протокол выбора верификаторов на основе консистентного хеширования, который назначает цену радикальным утверждениям через нарастающие издержки итераций; и (3) рыночную модель репутационных авторитетов, в которой частные верификаторы ставят на кон свою накопленную репутацию, ручаясь за достоверность утверждений, которые они заверяют. Получающаяся архитектура порождает эмерджентную меритократию без центральной координации и обеспечивает постепенный,

обратимый путь миграции от существующих государственно управляемых систем.

1 Введение

1.1 Проблема централизованного доверия

Современное управление опирается на фундаментальное допущение: что централизованные институты способны опосредовать доверие между незнакомцами в масштабе. Суды разрешают споры. Реестры удостоверяют собственность. Регуляторные органы обеспечивают соблюдение стандартов. Эти институты создавались в эпоху, когда информация была дефицитной, коммуникация—медленной, а делегирование полномочий центральному органу было единственным осуществимым механизмом координации. Централизованное управление, однако, терпит неудачу по тем же структурным причинам, что и централизованное планирование: информационная асимметрия, отсутствие обратных связей и оторванность лиц, принимающих решения, от последствий этих решений.

Это допущение не выдерживает, например, когда издержки институционального посредничества превышают ценность спора. Рассмотрим арендатора, который обнаруживает, что в его съёмной квартире отсутствует юридически обязательный сертификат электробезопасности—условие, создающее непосредственную угрозу жизни. Законное право арендатора расторгнуть договор бесспорно. Однако издержки на защиту этого права через судебную систему превышают денежную стоимость залога и причитающихся убытков, даже с учётом возможной установленной законом компенсации [1]. Рациональный ответ—смириться с потерей и уйти.

Это не патологический пограничный случай.

Это положение по умолчанию для значительного класса споров, в которых вред реален, но денежные ставки падают ниже порога, при котором институциональное принуждение становится экономически рациональным. Результатом является система, которая структурно благоволит недобросовестным акторам: те, кто причиняет вред другим в объёмах ниже этого порога, могут действовать безнаказанно, поскольку издержки на достижение справедливости ложатся на пострадавшую сторону.

Приведённый выше пример взят из правовой среды автора—чешской системы гражданского права. В других правовых традициях—прецедентном общем праве, обычном праве, смешанных системах—справедливость терпит неудачу по-разному и в разной степени в зависимости от культурных и процедурных особенностей юрисдикции. Читатели, вероятно, узнают эквивалентные примеры из собственного контекста. Структурно универсальной является закономерность: споры, чья ценность падает ниже порога экономически рационального принуждения, заканчиваются тем, что потеря поглощается пострадавшей стороной. RSN не обещает совершенной справедливости—она лишь снижает структурное преимущество, которым пользуются недобросовестные акторы, когда институциональное принуждение неэкономично.

1.2 Почему существующие решения недостаточны

Фреймворки децентрализованной идентичности (DID) [2] предоставляют криптографические механизмы для самосуверенного управления идентичностью, но сосредоточены прежде всего на верификации идентичности, не затрагивая более широкий вопрос поведенческой репутации.

Soulbound-токены (SBT) [3] улавливают идею, что репутация непередаваема, но полагаются на блокчейн-инфраструктуру с ограничениями масштабируемости и не затрагивают экономические стимулы, регулирующие ввод информации. Смежные концепции, такие как токены заслуг (например, *Liberland*), разделяют схожую философию, но остаются привязанными к конкретным юрисдикционным рамкам.

Децентрализованные автономные организации (DAO) [4] реализуют управление через смарт-контракты, но воспроизводят плутократическую динамику, где влияние

пропорционально капиталу. Квадратичное голосование [5] частично смягчает это, но ограничивает практическое внедрение. DAO также сталкиваются с фундаментальной *проблемой оракула*: смарт-контракты не способны надёжно проверять состояния реального мира без доверенного внешнего источника, и эта проблема не имеет общего решения в рамках блокчейн-архитектуры.

Ни одна существующая система не сочетает децентрализацию, устойчивость к цензуре, псевдонимность, проверяемую стоимость входа и эмерджентный консенсус.

1.3 Вклад работы

Настоящая работа вносит следующий вклад:

1. Определение **репутационной социальной сети (RSN)**, децентрализованного протокола, расширяющего фреймворк DID для поддержки двустороннего обмена репутацией.
2. **Недетерминированный протокол выбора верификаторов** на основе консистентного хеширования [6].
3. **Принцип дорогого радикализма**, назначающий цену утверждениям в зависимости от их удалённости от консенсуса сети через три взаимоусиливающих канала издержек.
4. Модель **репутационного авторитета** с асимметричными стимулами, при которой ложное заверение обходится катастрофически дороже, чем законные комиссии.
5. **Постепенный путь миграции** через параллельную фискальную инфраструктуру.

2 Принципы проектирования

Архитектура RSN ограничена пятью неотъемлемыми принципами проектирования.

Непрерывность и эволюция. Система сосуществует с существующими институтами в течение переходного периода неопределённой длительности. Переход должен быть обратимым на каждом этапе.

Добровольность и ответственность. Участие добровольно, но добровольность сопряжена с ответственностью: участник, берущий на себя контроль над институциональной функцией, одновременно принимает и сопутствующие обязательства.

Разнообразие и культурная нейтральность. Консенсус возникает из двусторонних взаимодействий, а не из заранее заданных правил, навязанных проектировщиками системы.

Устойчивость и сопротивление цензуре. Издержки цензурирования сети должны превышать издержки её терпения. Только полный тоталитаризм—ценой разорительных политических и экономических издержек—способен подавить систему.

Консенсус и принуждение. Система включает человеческие склонности к мелочности, злопамятству и удовлетворению от возмездия как несущие функциональные элементы. Проступок не запрещается; ему назначается цена.

3 Обзор системы

3.1 Репутационная социальная сеть

RSN—это децентрализованный одноранговый коммуникационный уровень, в котором участники обмениваются проверяемой информацией о поведении в реальном мире. Её определяющие свойства таковы: децентрализованная и нецензурируемая инфраструктура; псевдонимное участие через DID; асимметричная структура издержек (чтение дёшево, запись дорого); криптографическая проверяемость; и **поддержка стандартов**—машиночитаемые форматы для информации, распространяемой через сеть, для услуг, предлагаемых авторитетами (составление утверждений, заверение, услуга свидетеля), и для формата политики, включая правила оценки репутации контрагента и оценки риска несоответствия политики (между заявленным и фактическим поведением).

3.2 Архитектурные компоненты

RSN состоит из четырёх основных компонентов (рис. 1):

1. **Уровень DID.** Идентичности участников с заявленными правилами, репутационными метаданными и сетевой маршрутизацией.
2. **Протокол утверждений.** Структурированный формат для публикации утверждений о событиях реального мира.
3. **Сеть верификации.** Децентрализованный протокол назначения верификаторов с использованием консистентного хеширования.

4. **Уровень агрегации репутации.** Услуги, порождающие человекочитаемые сводки репутации.

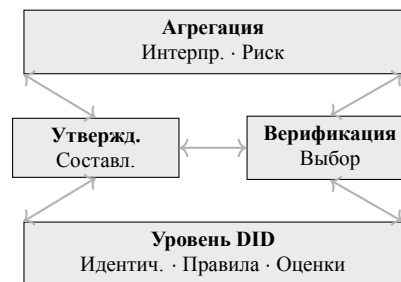


Figure 1: Четырёхуровневая архитектура RSN.

3.3 Роли участников

Транзакция верификации задействует до шести различных ролей DID (рис. 2): **Эмитент** (DID_I , создаёт и подаёт утверждение), **Субъект** (DID_S , DID, о котором идёт утверждение—может совпадать с Эмитентом), **Авторитет** (DID_A , заверяет утверждение за плату; может также предлагать услуги свидетеля—*опционально*), **Свидетель** ($DID_{W_{1..n}}$, инкогнито-наблюдатель за честностью верификатора через коды-вызовы—*опционально*), **Верификатор** (DID_V , алгоритмически выбранный для публикации утверждения) и **RSN** (сеть, где публикуются проверенные утверждения). Любая роль может быть делегирована другому DID (раздел 7.4). Авторитет обычно совмещает заверение с услугами свидетеля, но эти две функции логически независимы.

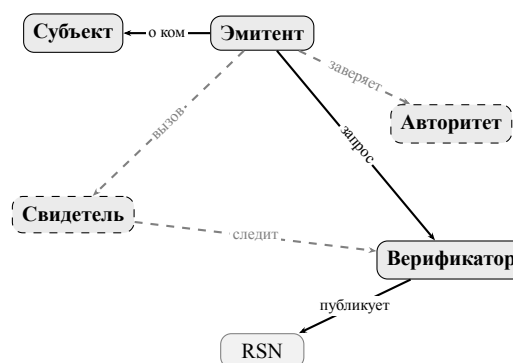


Figure 2: Роли DID в транзакции верификации. Пунктир = опционально (Авторитет, Свидетель).

3.4 Неподкупность: четыре силы

Неподкупность RSN проистекает не из единственного механизма, а из четырёх

одновременно действующих сил. Ни одна из них не достаточна сама по себе; лишь их сочетание делает попытку подкупа экономически нерациональной.

Непредсказуемая цель. Верификатор для каждого утверждения выбирается недетерминированно через консистентное хеширование (раздел 5.3). Атакующий не может заранее нацелиться на конкретного верификатора для подкупа, поскольку идентичность верификатора является функцией содержимого утверждения и предыдущих итераций, а не выбора эмитента.

Репутационный рычаг—медленно вверх, быстро вниз. Репутацию можно приобретать лишь постепенно, через устойчивое последовательное поведение. Однако её можно катастрофически утратить одним мошенническим заверением (раздел 6.2). Эта асимметрия означает, что годы накопленной репутации могут быть уничтожены одним нечестным заверением; оптимальной стратегией остаётся отклонение подозрительных утверждений.

Публичное обещание. Каждый Держатель DID публично заявляет свою политику—машиночитаемый набор правил, которым он обязуется следовать. Расхождение между заявлением и фактическим поведением обнаружимо и оценивается как репутационное нарушение более тяжкое, чем само исходное нарушение (раздел 7.3). Лицемерие поэтому обходится дороже прямой нечестности.

Асимметрия стоимости атаки на сетку. Издержки цензурирования или дестабилизации сети растут нелинейно с размером и плотностью сети, тогда как издержки её терпения остаются постоянными. Чтобы цензура окупилась, централизованному актору пришлось бы применить её ко всей сети—что требует мер, несоразмерных любой мыслимой выгоде (раздел 10).

4 Модель децентрализованной идентичности

4.1 DID с особыми свойствами

RSN расширяет спецификацию W3C DID Core [2] следующим: **Заявленные правила** (машиночитаемые поведенческие обязательства), **Репутационные метаданные** (агрегированная поведенческая оценка) и **Сетевая**

маршрутизация (изменяемый onion-шлюз, отдельный от стабильной позиции в кольце).

4.2 Жизненный цикл утверждения

Утверждение проходит шесть стадий (рис. 3): составление, опциональное заверение авторитетом, выбор верификатора через консистентное хеширование, решение о верификации (принять или отклонить с итерацией), публикация и обновление репутации для всех сторон.

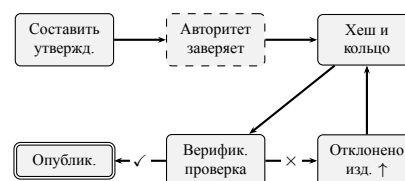


Figure 3: Жизненный цикл утверждения с циклом итераций.

4.3 Отношение к W3C DID Core

Модель идентичности RSN является собственным надмножеством спецификации W3C DID Core [2]. Все DID сети RSN являются валидными W3C DID. Специфичные для RSN расширения кодируются как свойства DID-документа, определённые в отдельной спецификации DID-метода, совместимой с существующей инфраструктурой, такой как ION [7] и Ceramic [8].

5 Верификация и распространение информации

5.1 Стоимость ввода информации

Ключевой экономический принцип RSN—асимметрия между чтением и записью. Чтение репутационных данных приближается к нулевой предельной стоимости для участников, которые входят в сеть DID и имеют доступ, соразмерный их репутации—новичкам приходится постепенно зарабатывать более широкий доступ (см. анти-паразитирование). Запись—понимаемая как долговременная материализация репутации в сеть, а не как разовый технический акт—требует проверяемых накопленных вложений по трём измерениям: **время** (годы жизни, потраченные на последовательное поведение, выполненные обязательства и выстроенные

отношения), **энергия** (усилия, вложенные в честное ведение дел, заботу о партнёрствах и долгосрочную надёжность) и **деньги** (вложения в собственное имя—профессиональное развитие, качество своей работы, возмещение причинённого вреда). Репутацию нельзя купить мгновенно—она является результатом пожизненного накопления, которое система лишь делает видимым и переносимым между контекстами. Разовые технические издержки протокола (криптографические подписи, комиссии верификаторов) незначительны по сравнению с этими базовыми вложениями.

5.2 Социальный граф и глубина контактов

RSN по своей сути является социальной сетью: каждый DID добавляет контакты (другие DID), которые разрешают соединение. У этих контактов есть свои контакты, и так далее. Алгоритмический поиск верификатора действует в пределах настраиваемой глубины h связанных контактов (например, $h = 3$: собственные прямые контакты, их контакты и контакты контактов). Эта архитектура не требует единого глобального блокчейна—она естественно благоприятствует возникновению сообществ/кластеров с пересечениями в другие сообщества. Каждый участник DID обязан иметь опубликованную **политику**—машиночитаемый набор правил, регулирующих то, как оцениваются входящие запросы. Нарушения политики фиксируются в сети как негативные артефакты.

5.3 Алгоритмический выбор верификатора

Протокол верификации использует консистентное хеширование [6] (рис. 4). Верификация—платная услуга: верификаторы работают за плату, создавая рынок, где конкуренция определяет цену, скорость и надёжность.

Шаг 1. Документ утверждения объединяется с результатом хеша предыдущей итерации (или $\emptyset$ на первой итерации) и хешируется:

$$\text{pos} = f_h(\text{claim} \parallel \text{prev_hash}) \quad (1)$$

Алгоритм должен включать *полный путь* всех предыдущих запросов и ответов—а не просто хеш предыдущей итерации. Полный ответ каждого верификатора (принятие, отклонение,

назначенная цена, причина) добавляется к растущему документу, проверяемому через криптографические подписи на каждом шаге.

Шаг 2. Хеш отображается на N позиций на кольце консистентного хеша, равномерно распределённых (например, для $N = 4$: $+0^\circ, +90^\circ, +180^\circ, +270^\circ$). Из каждой позиции поиск по часовой стрелке выбирает ближайший DID как кандидата в верификаторы (рис. 5). N —переменный параметр, который может зависеть от процента активных в данный момент DID, времени суток или исторической отзывчивости сети.

Шаг 3. Верификатор принимает (публикует, ставя на кон репутацию) или отклоняет (возвращаясь к Шагу 1 с хешем отклонения). Когда узел не отвечает, несмотря на заявленный онлайн-статус, следующий запрос должен включать все ответы от всех N предыдущих кандидатов в верификаторы.

Анти-паразитирование. Целевые DID могут устанавливать плату или ограничения доступа для запросов от новых DID с малой репутацией. Этот градуированный механизм (не бинарный) вынуждает новичков наращивать репутацию через подлинную активность, прежде чем свободно потреблять данные других.

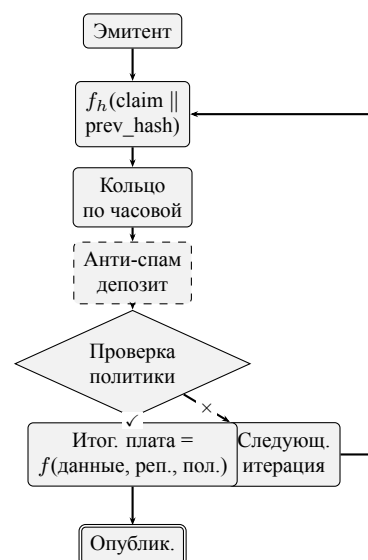


Figure 4: Протокол выбора верификатора. Анти-спам депозит опционален и может быть возвратным. Итоговая плата взимается только при принятии.

Каждое отклонение добавляет полный ответ верификатора (включая причины и условия) к документу утверждения, расширяя его содержимое. Из расширенного документа

недетерминированно вычисляется новый хеш, отображающийся на другую позицию кольца и выбирающий другого верификатора. Документирование полного пути обязательно—эмитент не может предсказать или повлиять на следующего верификатора. Если верификатор игнорирует запрос, несмотря на совместимую заявленную политику, свидетели (если они есть) фиксируют это, и эмитент может приложить свидетельские доказательства при итоговой публикации.

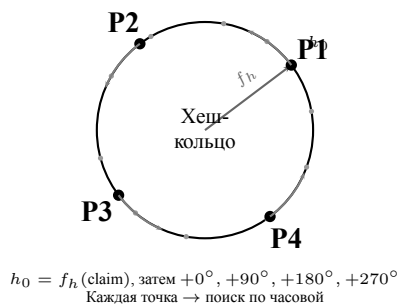


Figure 5: Многоточечный выбор ($N=4$). Хеш h_0 задаёт смещение; 4 точки равномерно распределены от h_0 .

5.4 Протокол свидетеля

Роль **Свидетеля** обеспечивает инкогнито-подотчётность честности верификатора через криптографический протокол кодов-вызовов:

Шаг W1. Запрашивающий подписывает запрос на верификацию и отправляет его N_w свидетелям—контактам из социальной сети запрашивающего или специализированным поставщикам услуг свидетеля, работающим за плату.

Шаг W2. Каждый свидетель w_i подписывает весь подписанный запрос, сохраняет исходную подпись σ_i и вычисляет код-вызов $c_i = h(\sigma_i)$. Код-вызов добавляется к запросу.

Шаг W3. Запрос, несущий теперь N_w кодов-вызовов, отправляется верификатору. Верификатор наблюдает коды, но *не может определить*, кто свидетели и соответствуют ли коды реальным подписям.

Шаг W4 (честный верификатор). Если верификатор отвечает согласно своей заявленной политике, коды-вызовы остаются непрозрачными. Свидетели никогда не раскрываются. Никакие дополнительные данные не публикуются.

Шаг W5 (нарушение политики). Если

верификатор нарушает свою политику (игнорирует запрос, отвечает непоследовательно), запрашивающий держит исходные подписи свидетелей σ_i . Их можно опубликовать как сопутствующие данные: любой может проверить $c_i = h(\sigma_i)$, доказав, что свидетель присутствовал. Запрашивающий может опубликовать независимо—верификатор уже подписал коды-вызовы в своём ответе.

Свойство блефа. Запрашивающий может подставить случайные значения вместо некоторых или всех кодов-вызовов. Верификатор не может отличить подлинные коды (подкреплённые высокорепутационными авторитетами) от шума. Эта *неопределённость* и есть механизм принуждения: каждый запрос несёт риск того, что уважаемый авторитет наблюдает инкогнито. Издержки поддержания этого давления близки к нулю (генерация случайных чисел), тогда как потенциальные издержки нечестности для верификатора катастрофичны. Честное поведение стимулируется даже при отсутствии реальных свидетелей.

Авторитет как свидетель. Авторитет, заверяющий утверждение, может совмещать услуги свидетеля: “Я заверяю ваше утверждение и служу инкогнито-свидетелем во время верификации”. Это естественная бизнес-модель—у авторитета уже есть контекст. Однако эти две роли логически независимы.

5.5 Принцип дорогого радикализма

Три канала издержек усиливают друг друга одновременно (рис. 6):

Канал 1: Издержки итераций. Каждое отклонение вынуждает новую итерацию, потребляющую время и ресурсы. Линейный рост.

Канал 2: Разбухание документа. Каждая итерация добавляет полный ответ верификатора к документу утверждения. Рост линеен, но с базовым смещением: исходная нагрузка (содержимое утверждения, заверение авторитетом, криптографические подписи) уже имеет нетривиальный размер B_0 . Общий размер после k итераций: $S(k) = B_0 + k \cdot \Delta$, где Δ —средний размер ответа.

Канал 3: Премия за риск верификатора. Риск субъективен. Верификатор оценивает, конфликтуют ли заявленные политики запрашивающего DID с собственными

коммерческими, социальными или политическими интересами верификатора. Премия может нарастать экспоненциально с воспринимаемой удалённостью от “идеала” верификатора: $P(d) = \alpha \cdot e^{\beta d}$, где d —субъективная метрика удалённости верификатора. За пределами личной границы “не входить” верификатор может отказать полностью.

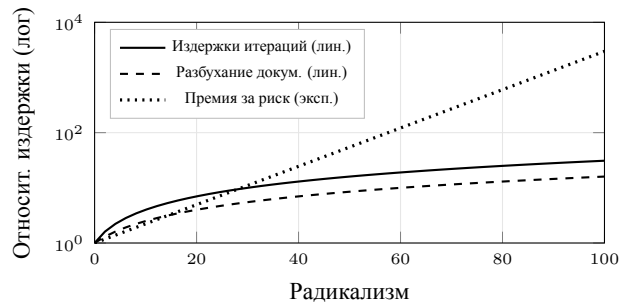


Figure 6: Нарастание издержек по трём каналам. Премия за риск доминирует при высоком радикализме.

Что критически важно, это не цензура. Ни одно утверждение не запрещается. Система назначает цену риску (табл. 1).

Table 1: Сравнение издержек по типам утверждений.

Тип	Итер.	Докум.	Плата	Итого
Достоверное	$k_{\min}$	B_0	$P_{\min}$	Низкие
Спорное	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Умеренные
Радикальное	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Очень высокие
Мошенническое	$\rightarrow \infty$	—	—	Непубликуемо

6 Репутация и оценка риска

6.1 Модель накопления репутации

Репутация обладает тремя свойствами: **медленное накопление** (постепенный рост через последовательное поведение), **быстрое разрушение** (одно мошенничество может катастрофически снизить оценку) и **индивидуальная оценка** (каждая потребляющая сторона может применять собственную функцию агрегации).

6.2 Репутационные авторитеты

Репутационный авторитет рассматривает утверждения и, если удовлетворён, соподписывает

их—ставя на кон собственную репутацию (рис. 7). Асимметрия заложена намеренно: приобретение репутации медленно (постепенное $+\delta$ за честное заверение), тогда как её утрата катастрофична ($-\Delta \gg \delta$ за ложное заверение; для иллюстрации, например, $+2\%$ против -70%). Оптимальной стратегией всегда является отклонение подозрительных утверждений. Конкретные значения δ и Δ —системные параметры.

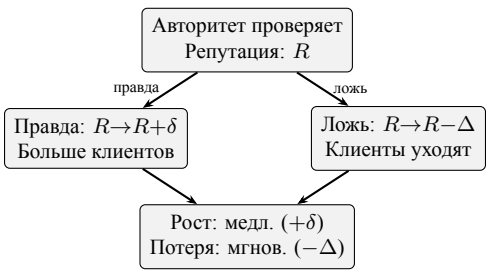


Figure 7: Репутационный авторитет—асимметричные стимулы.

6.3 Многомерная репутация

Репутация—не скаляр, а вектор во множестве измерений: финансовая надёжность, личная порядочность, профессиональная компетентность, гражданская вовлечённость и другие (рис. 8). Разные поставщики оценки проецируют тот вектор по-разному в зависимости от контекста—кредитор отдаёт приоритет финансовой надёжности, работодатель—профессиональной компетентности, сосед—гражданскому поведению. Не существует единой “правильной” оценки репутации; есть лишь перспективы.



Figure 8: Многомерные векторы репутации. Разные DID демонстрируют разные профили по измерениям.

6.4 Демократизированная оценка риска

RSN демократизирует систематическую оценку риска—способность, ныне сосредоточенную в финансовых институтах, но применимую далеко за пределами банковского дела. Промышленные конгломераты, оценивающие надёжность поставщиков, страховые компании, назначающие цену поведенческому риску, комплексная проверка при слияниях и поглощениях, оценка срока службы оборудования в производстве—езде, где риск контрагента требует оценки, RSN предоставляет децентрализованную, рыночную альтернативу. Рынок услуг интерпретации переводит сырые многомерные данные репутации в действенные сводки, делая оценку контрагента доступной любому участнику по предельной стоимости.

7 Консенсус и разрешение споров

7.1 Модель децентрализованной справедливости

RSN переосмысливает справедливость как задачу двусторонних переговоров. Угроза постоянного, проверяемого репутационного ущерба является более действенным сдерживающим фактором, чем судебное разбирательство, которое пострадавшая сторона не может себе позволить.

7.2 Эмерджентный консенсус

Каждый участник поддерживает личный порог удовлетворённости. Совокупный консенсус сети возникает как статистическое среднее тысяч двусторонних переговоров (рис. 9). Реакция, значительно превышающая консенсус (варварская), дорога в публикации. Реакция вблизи консенсуса (соразмерная) дешева. Консенсус—не правило, а ценовой сигнал.

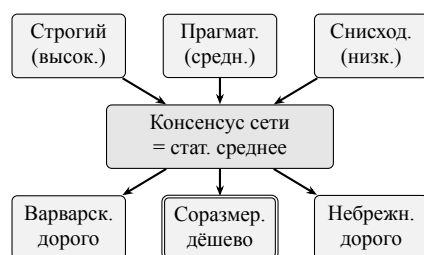


Figure 9: Эмерджентный консенсус из индивидуальных порогов удовлетворённости.

7.3 Калибровка наказания

Каждый Держатель DID публично заявляет реакции на конкретные категории проступков. Непропорционально суровые или мягкие заявления притягивают негативные репутационные сигналы. Соразмерные заявления принимаются без трения—самокалибрующаяся система наказания.

Заявления о консенсусе сами подлежат обнаружению лицемерия: декларативная приверженность консенсусной позиции при непоследовательном поведении составляет репутационное нарушение более тяжкое, чем само отклонение, поскольку демонстрирует умышленный обман.

7.4 Делегирование

Все действия в рамках DID—за одним исключением—могут быть делегированы другому DID. Роль Субъекта—DID, о чьём поведении идёт утверждение,—не может быть делегирована; она непередаваемо привязана к держателю идентичности, к которому относится утверждение. Другие активные роли—Эмитент, Авторитет, Свидетель, Верификатор—могут быть переданы назначенному делегатскому DID, будь то для верификации, подачи утверждений, участия в консенсусе или разрешения споров. Делегирование отзывается в любой момент. Это позволяет специализацию (например, профессиональные услуги верификации), при этом Держатель сохраняет окончательный контроль и ответственность. Делегирование применяется во всей системе и существенно для масштабируемости.

7.5 От индивидуальной морали к эмерджентному общественному договору

Заявленная политика каждого DID представляет формализацию индивидуальной морали: что Держатель считает приемлемым, как он реагирует на конкретное поведение, что он требует от контрагентов. Эти политики не навязываются проектировщиком системы—они выбираются каждым участником и выражаются в машиночитаемой форме.

Эта формализация обеспечивает трёхстадийное возникновение. Во-первых, индивидуальная мораль кодируется как **политика**—набор

заявленных правил, порогов и функций реакции, которым DID обязуется следовать. Во-вторых, совокупность всех политик в сети порождает **эмерджентную этику**—статистически наблюдаемые нормы, которые не спроектировал ни один отдельный участник, но которые возникают из взаимодействия тысяч индивидуальных моральных позиций [9]. В-третьих, эта эмерджентная этика, выраженная как разделяемые поведенческие нормы, обеспечиваемые через двусторонние ценовые сигналы, составляет **измеримый общественный договор**—не теоретическую конструкцию, которую никто не подписывал [10], а эмпирически наблюдаемый набор правил, подкреплённый фактическим поведением.

Этот процесс отражает выводы теории моральных оснований [11]: человеческая мораль интуитивна, плюралистична и культурно изменчива. RSN не требует морального консенсуса на входе; она производит поведенческий консенсус на выходе. Получающийся общественный договор не статичен—он эволюционирует по мере того, как участники присоединяются, уходят и корректируют свои политики в ответ на обратную связь сети. В отличие от классической теории общественного договора, этот договор отзываем, наблюдаем и обеспечим без суверена.

8 Экономическая модель

Предыдущие разделы описывали инструмент—механизмы верификации RSN, структуру издержек и эмерджентный консенсус. В этом разделе описывается методология применения этого инструмента к фискальному и управленческому переходу. Инструмент универсален; изложенная ниже методология—одно из возможных применений.

8.1 Структура стимулов

Репутация как капитал создаёт прямые стимулы к честному поведению. При нормальной работе участники наращивают репутацию естественно через повседневные транзакции и выполненные обязательства. Основные расходы приходятся на *негативные* утверждения—фиксацию вреда, причинённого другими. Эта асимметрия стимулирует полезное, надёжное поведение: быть честным не стоит ничего дополнительного, тогда как быть вредоносным

создаёт документированный след, который другие заплатят за сохранение. Лицемерие—заявление правил без следования им—является самым дорогим режимом отказа, поскольку демонстрирует умышленный обман.

8.2 Параллельная фискальная система

Три компонента обеспечивают конкурентное давление: (1) **Простой налог**—единая пропорциональная ставка без исключений, изначально незначительно ниже существующей эффективной ставки; (2) **Электронная регистрация расходов (ESR)**—инвертирование чешской модели ЕЕТ, чтобы граждане надзирали за государственными расходами; (3) **Направляемое гражданами распределение налогов**—начиная с нескольких процентов в первый год и достигая через десятилетие любой величины от нижних двузначных значений до полной миграции к системе, направляемой гражданами, в зависимости от темпа внедрения. Фактический темп зависит от скорости, с которой возникают свободнорыночные альтернативы государственным услугам, и от готовности государства сотрудничать с переходом; функция времени не обязана быть линейной, и нет причин задавать верхнюю границу того, к чему внедрение может в итоге прийти.

9 Путь миграции

Миграция проходит через три фазы (рис. 10): **Фаза 1: Наложение** (RSN как информационный уровень, государство—единственный поставщик), **Фаза 2: Конкуренция** (RSN предоставляет функциональные альтернативы, использование двойной системы) и **Фаза 3: Переход** (RSN превосходит государственные эквиваленты, добровольная миграция). Переход обратим на каждом этапе.



Figure 10: Трёхфазная миграция—обратимая на каждом этапе.

Основной механизм давления фискален: когда условные налогоплательщики достигают “экономически значимого меньшинства

X —группы, достаточно большой, чтобы репрессии против неё причиняли нетривиальный экономический ущерб, а гражданское неповиновение становилось правдоподобной угрозой,—государство вступает в переговоры. Для иллюстрации мы используем $X \approx 15\%$ ВВП, но фактический порог зависит от конкретной экономики.

10 Анализ безопасности

Мы рассматриваем пять категорий противников: отдельные недобросовестные акторы, организованные группы, корпоративные противники, противники государственного уровня и противники уровня протокола.

Сопrotивление атаке Сивиллы [12]. Нарастание репутации требует устойчивого, проверяемого взаимодействия. Издержки успешной атаки Сивиллы масштабируются линейно с числом фальшивых идентичностей и квадратично с целевым уровнем репутации. Параллельное управление несколькими DID возможно, но дорого по замыслу—каждая идентичность должна независимо накапливать репутацию через подлинную активность. В свободных обществах эти издержки сдерживают случайное злоупотребление; в диктатурах параллельные DID становятся инструментом выживания, обеспечивающим сегментированное сопротивление, подпольную координацию и более безопасную навигацию по чёрному рынку.

Защита от сговора. Паттерны взаимного заверения среди закрытых групп обнаруживаются через анализ социального графа. Функции агрегации репутации дисконтируют утверждения из плотно сгруппированных источников.

Противник государственного уровня. Оптимизация маршрутизации, отсутствие централизованной инфраструктуры и распределение ролей Верификатора по базе участников обеспечивают, что подавление требует мер, несоизмеримых любой выгоде.

Приватность против подотчётности. Псевдонимность—промежуточное положение между анонимностью и раскрытием идентичности—позволяет DID накапливать значимую репутацию без раскрытия реальной идентичности Держателя.

11 Соображения приватности

Модель приватности RSN построена на псевдонимности. Держатель контролирует раскрытие идентичности: минимальное (чистый псевдоним), выборочное (связаны конкретные удостоверения) или полное (ассоциирована юридическая идентичность). Опубликованные утверждения постоянны—система поддерживает контекстную коррекцию, но не стирание. Держатель может отказаться от скомпрометированного DID и начать заново, утратив накопленную репутацию.

12 Смежные работы

Спецификация W3C DID Core [2] и сеть Ceramic [8] предоставляют основу идентичности. EigenTrust [13] продемонстрировал распределённую агрегацию репутации без центрального авторитета. SBT [3] ввели непередаваемые социальные токены. RSN отличается акцентом на экономических издержках как фильтре качества и своим механизмом назначения цены радикализму.

DAO [4] и квадратичное голосование [5] продемонстрировали осуществимость децентрализованного управления. RSN выводит консенсус из двусторонних ценовых переговоров, а не из голосования.

Предложение опирается на анархо-капиталистическую теорию [14, 15] в части частного предоставления услуг, но отходит от неё в двух критических отношениях: оно проектируется под злопамятство и импульсы возмездия, а не предполагает рациональность, и предлагает постепенный переход, а не революцию. Концепция эмерджентных общественных договоров имеет предшественников в теории спонтанного порядка Хайека [16].

Анархо-агоризм. RSN разделяет значительную общую почву с агористской контр-экономикой [17]—в особенности акцент на построении параллельных институтов и добровольном обмене. Однако агоризм склонен предполагать рациональный своекорыстный интерес как достаточный механизм координации и зачастую лишён конкретного пути миграции от существующих государственных структур. RSN явно включает нерациональные поведенческие склонности и предоставляет механизм фискального давления для постепенного перехода.

Меритократия. RSN может представлять

первое функциональное описание того, как меритократия [18] способна возникнуть как системное свойство, а не лозунг. Традиционные меритократические системы терпят неудачу, потому что требуют центрального авторитета для определения и обеспечения “заслуги”. В RSN заслуга возникает из двусторонних оценок: те, кто приносит ценность, накапливают репутацию; никакой комитет не решает, у кого есть заслуга.

Собственность как привилегия. RSN фундаментально отходит от трактовок прав собственности как естественных и абсолютных в анархо-капитализме и австрийской школе. В рамках RSN собственность является *привилегией*— социальным признанием, которое в крайних случаях может быть отозвано сообществом, когда участник фундаментально нарушает разделяемые нормы (предательство, отказ защищать сообщество в экзистенциальном кризисе, систематическая эксплуатация). Это не государственная экспроприация, а отзыв социального признания сетью двусторонних отношений.

13 Обсуждение и ограничения

Холодный старт. Ценность RSN зависит от сетевых эффектов; ранние последователи сталкиваются с ограниченной ценностью, пока участие не достигнет порога. Однако даже на ранних стадиях сеть DID служит полезным вспомогательным источником информации. Ожидается, что ранняя оценка репутации и оценка авторитетов будут развиваться постепенно с ростом изошрённости.

Анти-паразитирование и контроль доступа. Целевые DID могут налагать градуированную плату и ограничения доступа на запросы от низкорепутационных DID. Это не бинарно, а непрерывная шкала: чем меньше репутации у запрашивающего DID, тем меньше информации он получает, тем дольше ждёт и тем больше платит. Этот механизм стимулирует подлинное участие вместо пассивного потребления.

Неравенство доступа. Издержки публикации утверждений могут отфильтровывать законные претензии экономически неблагополучных участников. Смягчение: каждый участник одновременно служит потенциальным верификатором (или делегирует эту роль) и зарабатывает комиссии верификации. На достаточном временном горизонте нерадикальный

участник должен приближаться к финансовой нейтральности—доход от верификации примерно компенсирует издержки публикации. Это статистическое ожидание, а не гарантия.

Неравенство репутации. Ранние последователи накапливают преимущества, которые могут создавать барьеры для опоздавших. Однако оценка репутации выполняется сторонними поставщиками, которые могут решить смягчить преимущество первопроходца через свои алгоритмы агрегации. Быть первым с хорошей репутацией—законное сравнительное экономическое преимущество, и это заложено по замыслу.

Открытые вопросы. Оптимальные функции издержек, стандарты агрегации, управление протоколом и взаимодействие с синтетическими репутационными данными, сгенерированными ИИ, остаются областями для будущей работы.

Настоящая работа не утверждает, что RSN приведёт к оптимальным результатам во всех обстоятельствах. Она утверждает, что RSN представляет *осуществимую* альтернативу—технически реализуемую, экономически самокупаемую и социально совместимую с человеческими поведенческими склонностями такими, каковы они на самом деле.

14 Заключение

В настоящей работе представлена репутационная социальная сеть—децентрализованный протокол, обеспечивающий псевдонимный, проверяемый обмен репутацией. Принцип дорогого радикализма гарантирует, что мошеннические утверждения вытесняются ценой без цензуры. Предложенный путь миграции обеспечивает постепенный, обратимый переход от существующих институтов. Замысел включает человеческую природу такой, какова она есть—включая мелочность, злопамятство и желание удовлетворения от возмездия,—а не требует идеологической трансформации. Результат—не утопия, а система, где справедливость доступна, репутация заслуживается, а издержки проступка несёт сторона, которая его причинила.

References

- [1] Czech Republic, “Act no. 549/1991 coll., on court fees, as amended,” 1991, fee schedule for

- court proceedings; cost rules per Act No. 99/1963 Coll. (Code of Civil Procedure) and Decree No. 177/1996 Coll. (Attorney Tariff).
- [2] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen, “Decentralized identifiers (DIDs) v1.0,” W3C Recommendation, Jul. 2022.
 - [3] E. G. Weyl, P. Ohlhaver, and V. Buterin, “Decentralized society: Finding Web3’s soul,” *SSRN Electronic Journal*, May 2022.
 - [4] V. Buterin, “DAOs, DACs, DAs and more: An incomplete terminology guide,” Ethereum Blog, May 2014.
 - [5] V. Buterin, Z. Hitzig, and E. G. Weyl, “A flexible design for funding public goods,” *Management Science*, vol. 65, no. 11, pp. 5171–5187, 2019.
 - [6] D. Karger, E. Lehman, T. Leighton, R. Panigrahy, M. Levine, and D. Lewin, “Consistent hashing and random trees: Distributed caching protocols for relieving hot spots on the World Wide Web,” in *Proc. 29th ACM STOC*, 1997, pp. 654–663.
 - [7] D. Buchner, “ION — a scalable DID method based on Bitcoin,” Microsoft, 2021.
 - [8] Ceramic Network, “Ceramic protocol specification,” GitHub, 2023. [Online]. Available: <https://github.com/ceramicnetwork>
 - [9] É. Durkheim, *The Division of Labor in Society*. Free Press, 1893, english translation 1984.
 - [10] J. Rawls, *A Theory of Justice*. Harvard University Press, 1971.
 - [11] J. Haidt, *The Righteous Mind: Why Good People Are Divided by Politics and Religion*. Vintage Books, 2012.
 - [12] J. R. Douceur, “The Sybil attack,” in *Proc. 1st International Workshop on Peer-to-Peer Systems (IPTPS)*, 2002, pp. 251–260.
 - [13] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, “The EigenTrust algorithm for reputation management in P2P networks,” in *Proc. 12th International Conference on World Wide Web*, 2003, pp. 640–651.
 - [14] M. N. Rothbard, *For a New Liberty: The Libertarian Manifesto*. Macmillan, 1973.
 - [15] H.-H. Hoppe, *Democracy: The God That Failed*. Transaction Publishers, 2001.
 - [16] F. A. Hayek, *Law, Legislation and Liberty*. University of Chicago Press, 1973.
 - [17] S. E. I. Konkin, *An Agorist Primer*. KoPubCo, 2006.
 - [18] M. Young, *The Rise of the Meritocracy*. Thames and Hudson, 1958.