Proof of Time: Одноранговая система временного консенсуса

Алехандро Монтана
alejandromontana@tutamail.com
25 декабря 2025

Аннотация

Чисто одноранговая система консенсуса позволяет достичь распределённого согласия без зависимости от капитала или вычислительных ресурсов. Существующие решения — Proof of Work и Proof of Stake — масштабируют влияние через покупаемые ресурсы, неизбежно концентрируя власть в руках владельцев капитала. Мы предлагаем решение на основе верифицируемых функций задержки (VDF), где влияние накапливается через присутствие во времени, а не через расход ресурсов. Сеть создаёт временные метки блоков через последовательные вычисления, которые невозможно распараллелить или ускорить. Узлы конкурируют за 21 миллион минут временного актива, распределяемого в течение 131 года. Система требует всего 3 активных узла и остаётся безопасной, пока честные участники контролируют большинство взвешенного влияния. Время нельзя купить, произвести или передать — его можно только потратить.

1. Введение

Все распределённые системы консенсуса сталкиваются с одной фундаментальной проблемой: как достичь согласия между недоверяющими сторонами без центрального арбитра?

Bitcoin решил эту проблему через Proof of Work — механизм, где право создать блок определяется вычислительной мощностью. Ethereum перешёл на Proof of Stake — право определяется количеством заблокированных монет. Оба механизма работают. Оба механизма справедливы в своих правилах.

Но оба механизма несправедливы в своей сути.

Proof of Work требует специализированного оборудования. Участник с капиталом покупает ASIC-майнеры и контролирует хэшрейт пропорционально инвестициям. Proof of Stake делает это явным — застейкал монеты, получил влияние. В обоих случаях ресурс, определяющий власть, можно купить.

Что если построить консенсус на ресурсе, который нельзя купить?

Время — единственный такой ресурс. Узел, работающий 180 дней, накапливает одинаковое влияние независимо от того, принадлежит он миллиардеру или студенту. Это время необратимо. Его нельзя купить на бирже. Нельзя арендовать в облаке. Можно только потратить — существуя.

2. Проблема плутократии

Все существующие механизмы консенсуса страдают от одной фундаментальной слабости: зависимость от ресурсов создаёт плутократический захват.

В Proof of Work хэшрейт покупается. Инцидент с GHash.io в 2014 году показал, что один майнинг-пул может приблизиться к 51% хэшрейта Bitcoin. Сегодня майнинг сконцентрирован в промышленных операциях в регионах с дешёвым электричеством. Барьер для значимого участия превышает ресурсы обычных людей.

В Proof of Stake проблема структурна. Требования к стейкингу создают минимальные пороги богатства для валидации. Награды за стейкинг увеличивают существующие накопления. Богатые становятся богаче — по дизайну.

Делегированные системы (DPoS) лишь добавляют посредников. Ликвидный стейкинг создаёт деривативы, которые переконцентрируют власть. Каждая вариация сохраняет суть проблемы: те, у кого капитал, контролируют консенсус.

Решение не в том, чтобы перераспределить ресурсы справедливее внутри этих систем. Решение — построить консенсус на ресурсе, который невозможно неравномерно распределить.

Время течёт для всех с одинаковой скоростью. Одна секунда для государства равна одной секунде для индивида. Это не политика. Это физика.

3. Верифицируемые функции задержки

Верифицируемая функция задержки (VDF) — это функция, требующая определённого числа последовательных операций для вычисления, но результат которой можно эффективно проверить. Ключевое свойство: вычисление невозможно распараллелить.

Для VDF с параметром сложности t: • Вычисление требует O(t) последовательных шагов • Верификация требует O(log t) шагов • Никакое количество параллельных процессоров не сокращает время вычисления

Это создаёт криптографическое доказательство того, что время прошло. Каждое доказательство зависит от хэша предыдущего блока: VDF(h_prev, t) → π. Предвычисление невозможно, поскольку h_prev неизвестен до финализации предыдущего блока.

Сеть использует VDF-конструкцию Веселовски, которая обеспечивает: • Эффективную верификацию (логарифмическую от сложности) • Компактные доказательства (постоянный размер независимо от сложности) • Безопасность при стандартных криптографических предположениях

Когда узел производит валидный VDF-пруф, он математически демонстрирует, что t последовательных операций выполнено. Это доказательство времени.

4. Архитектура сети

Сеть работает через взвешенный выбор лидера. Каждые 10 минут один узел выбирается для создания блока. Вероятность выбора зависит от трёх факторов:

Формула вероятности узла: P_i = (w_time · f_time(t_i) + w_space · f_space(s_i) + w_rep · f_rep(r_i)) / Z

Где Z нормализует вероятности к сумме 1, целевые веса: • w_time = 0.60 (присутствие во времени) • w_space = 0.20 (хранение цепи) • w_rep = 0.20 (репутация)

Функции насыщения: • f_time(t) = min(t / 180 дней, 1) • f_space(s) = min(s / 0.80 × история_цепи, 1) • f_rep(r) = min(r / 2016 блоков, 1)

Критическое свойство: все компоненты насыщаются. Узел достигает максимального влияния за 180 дней. После насыщения дополнительное время не даёт преимущества. Новые участники могут достичь паритета с ранними.

Сеть требует минимум 3 активных узла для консенсуса. Выбор лидера использует VRF (верифицируемую случайную функцию) на основе хэша предыдущего блока. Если выбранный лидер не создаёт блок в течение 12 минут, лидерство переходит к следующему кандидату.

Упорядочивание транзакций внутри блоков использует Proof of History (последовательное SHA-256 хэширование), аналогично Solana, но без требований к оборудованию Solana. Консенсус остаётся VDF-основанным.

5. График эмиссии

Общее предложение: 21 000 000 минут (1 260 000 000 секунд)

Это 40 лет временного актива, распределяемого в течение 131.7 лет календарного времени.

Награды за блок: • Блоки 1–210 000: 50 минут за блок • Блоки 210 001–420 000: 25 минут за блок • Блоки 420 001–630 000: 12.5 минут за блок • (Халвинг продолжается каждые 210 000 блоков)

Временная компрессия: В начальную эпоху сеть производит временной актив в соотношении 5:1 (50 минут награды за 10 минут реального времени). Это соотношение уменьшается с каждым халвингом, асимптотически приближаясь к 1:1.

Общая эмиссия следует геометрической прогрессии: Σ E(e) = 210 000 × 3 000 × (1 + 1/2 + 1/4 + ...) = 1 260 000 000 секунд

Комиссии за транзакции: минимум 1 секунда. После завершения эмиссии комиссии поддерживают сеть.

Символ: ɬ (инвертированное t со знаком равенства) Базовая единица: 1ɬ = 1 секунда

6. Анализ безопасности

Устойчивость к Sybil-атакам: Создание N Sybil-узлов не даёт преимущества. Каждый новый узел начинает с: • Нулевого присутствия во времени (требуется 180 дней для насыщения) • Нулевого хранения цепи (нужна синхронизация полной истории) • Нулевой репутации (нужно подписать 2016 блоков)

Вероятность нормализуется по всем узлам. Разделение идентичности на множество узлов пропорционально делит влияние — общее влияние не меняется.

Если скорость подключения новых узлов превышает 2× медианную историческую, новые узлы входят в 180-дневный испытательный срок с 90% снижением вероятности.

Стоимость атаки 51%: Для контроля большинства взвешенного влияния атакующий должен: • Запустить N узлов × 180 дней каждый (временная компонента) • Хранить N × 80% истории цепи (пространственная компонента) • Подписать N × 2016 блоков без эквивокации (репутация)

В отличие от PoW/PoS атак, которые можно выполнить мгновенно при достаточном капитале, временные атаки требуют... времени. Атака, запланированная сегодня, не может быть выполнена раньше чем через 6 месяцев.

Штраф за эквивокацию: Попытка подписать конфликтующие блоки вызывает немедленный слэшинг: • Сброс репутации до нуля • 180-дневный карантин (вероятность выбора = 0) • Потеря всего накопленного присутствия во времени

Единственный путь атакующего — перезапустить 180-дневный процесс накопления.

Анализ разорения игрока: Для атакующего с вероятностью q, пытающегося догнать честную цепь с вероятностью p > q с отставанием в z блоков:

P(догнать) = (q/p)^z при p > q

Для одного атакующего узла среди N честных узлов при максимальном насыщении: q = 1/N. Вероятность атаки падает экспоненциально с глубиной цепи.

7. Приватность

Все транзакции используют кольцевые подписи (LSAG) и стелс-адреса по умолчанию. Приватность не опциональна — она обязательна для всех участников.

Кольцевые подписи: Каждый вход транзакции ссылается на множество возможных выходов. Криптографически невозможно определить, какой выход был реально потрачен. Правдоподобное отрицание структурно встроено.

Стелс-адреса: Каждая транзакция генерирует уникальный одноразовый адрес. Множественные платежи одному получателю невозможно связать через анализ адресов.

RingCT (кольцевые конфиденциальные транзакции): Суммы транзакций скрыты через обязательства Педерсена: C = aG + bH

Где a — сумма, b — фактор маскировки. Доказательства диапазона гарантируют a > 0 без раскрытия a. Валидаторы подтверждают валидность транзакции, не узнавая значений.

Традиционная банковская модель достигает приватности через контроль доступа — ограничивая, кто может видеть реестр. Proof of Time достигает приватности через криптографию — реестр публичен, но его содержимое непрозрачно.

8. Сравнение

Proof of Time против Proof of Work: • PoW: Влияние = f(инвестиции в оборудование) • PoT: Влияние = f(присутствие во времени) • PoW: Барьеры растут с конкуренцией • PoT: Барьеры фиксированы — максимум 180 дней

Proof of Time против Proof of Stake: • PoS: Влияние = f(капитал) • PoT: Влияние = f(присутствие во времени) • PoS: Богатые богатеют (сложный процент от стейкинга) • PoT: Все насыщаются одинаково

Proof of Time против Solana (PoH): • Solana: PoH для консенсуса, требует мощного оборудования ($5000+) • PoT: PoH только для упорядочивания, VDF для консенсуса, минимальное оборудование • Solana: ~1500 валидаторов • PoT: Теоретически неограниченное число участников

Компромиссы: Proof of Time жертвует пропускной способностью ради децентрализации. Время блока — 10 минут (против 400мс у Solana). Расчётный TPS — ~10 000 (против 50 000+ у Solana). Система оптимизирована для равенства участия, а не скорости транзакций.

9. Философское основание

Proof of Time не просто технический протокол. Это ответ на вопрос, который человечество задаёт тысячелетиями: как создать справедливую систему координации?

Все предыдущие системы — от феодализма до капитализма, от золотого стандарта до фиатных валют — основывались на ресурсах, которые можно накопить неравномерно. Земля. Золото. Капитал. Вычислительная мощность.

Время — единственный ресурс, распределённый абсолютно равномерно. Секунда президента равна секунде бездомного. Это не идеология. Это факт реальности.

Консенсус очевидности: В Bitcoin 51% хэшрейта = истина. В Ethereum 51% стейка = истина. PoT работает иначе. Истина не голосуется. Она обнаруживается.

Когда все согласились, что 1ℏ = 1 секунда земного времени — ценность перестала требовать внешней привязки. Она стала привязкой.

Layer -1: PoT — это Layer -1. Ниже инфраструктуры. Ниже консенсуса. Ниже кода. Время было до блокчейна. До интернета. До электричества. До языка.

TCP/IP — протокол передачи данных. PoT — протокол передачи доверия через время.

10. Заключение

Мы предложили механизм консенсуса, удаляющий капитал как основу влияния. Система использует время — единственный истинно дефицитный и равномерно распределённый ресурс — как фундамент для распределённого согласия.

Proof of Time не требует доверия к институтам, корпорациям или богатым индивидам. Он требует лишь того, чтобы честные участники коллективно инвестировали больше времени, чем атакующие. Поскольку время нельзя купить, произвести или сконцентрировать, система противостоит плутократическому захвату, поражающему все ресурсо-зависимые механизмы консенсуса.

Сеть устойчива в своей простоте. Узлы не требуют идентификации. Сообщения требуют лишь доставки по мере возможности. Участники могут уходить и возвращаться свободно, принимая самую длинную валидную цепь как каноническую историю.

Во времени все равны.

Это было очевидно с самого начала. Но не было способа это доказать.

Теперь есть.

Литература

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] D. Boneh, J. Bonneau, B. Bünz, B. Fisch, "Verifiable Delay Functions," CRYPTO 2018.

[3] B. Wesolowski, "Efficient Verifiable Delay Functions," EUROCRYPT 2019.

[4] A. Yakovenko, "Solana: A new architecture for a high performance blockchain," 2018.

[5] S. Noether, "Ring Signature Confidential Transactions for Monero," Ledger, 2016.

[6] N. van Saberhagen, "CryptoNote v2.0," 2013.

[7] W. Feller, "An Introduction to Probability Theory and Its Applications," Wiley, 1957.

[8] M. Bellare, P. Rogaway, "Random Oracles are Practical," ACM CCS, 1993.