АУДИТ ТОКЕНА · 09.26

$ZEC

z.cash

ИТОГОВЫЙ РЕЙТИНГ — BBB

66/100

Zcash — блокчейн Layer-1 с криптографией нулевого разглашения. Работает с 2016 года, первым вывел zk-SNARK в промышленную эксплуатацию. Здесь монета и есть продукт: приватная транзакция без владения ZEC невозможна. Максимальная эмиссия 21 млн, выпущено 80,3%.

FDV	MC	ЭКРАНИРОВАНО	ЭМИССИЯ В ГОД	ДОЛЯ ЭКРАНИРОВАННОГО
$8,38 млрд	$8,38 млрд	$2,17 млрд	$326 млн	25,9%

ВЫПУЩЕНО

80,3%

Эта монета незаменима: без ZEC нет приватной транзакции, но у модели нет ни одного механизма поглощения эмиссии, а разработку оплачивает держатель

Связь монеты с продуктом: монету невозможно обойти — без ZEC нет приватной транзакции. Потолок 21 млн, вестинга и разблокировок нет.

Устойчивость токеномики: разработку оплачивает разводнение 3,89% в год; механизмов поглощения эмиссии нет.

Краткое резюме Аудита Монеты ZEC

- **Монета здесь и есть продукт.** ZEC — расчётная единица сети: приватная транзакция без владения коином невозможна в принципе. По шкале методологии это категория unavoidable — максимальная оценка необходимости коина, редкая для рынка.
- **Но платят держатели, а не выручка.** Комиссии сети ничтожны и достаются майнерам; выкупа, сжигания и распределения выручки не существует. Разработка и гранты финансируются разводнением: 20% каждой блок-награды уходит организациям экосистемы, держатель размывается на **3,89% в год**.
- **2026 год определила уязвимость Orchard.** Дефект схемы, существовавший с 2022 года, теоретически допускал недетектируемую подделку ZEC. Свидетельств эксплуатации не найдено, средства не потеряны. Устранение заняло **5 дней**, полная замена пула — **60 дней**: 28 июля 2026 года активирован Ironwood с механизмом turnstile, ограничивающим вывод объёмом верифицируемо внесённых средств.
- **Сообщество ответило деньгами.** За 16 дней после активации из запечатанного Orchard в Ironwood перешло **2,79 млн ZEC из 3,66 млн — 73%**. Совокупно экранировано 4,37 млн ZEC, или **25,92% предложения** ($2,17 млрд).
- **Локбокс оказался отложенной выплатой, а не блокировкой.** Расчёт сходится до затоши: за 420 000 блоков накопилось ровно 78 750 ZEC, и вся сумма выплачена при обновлении NU6.1 на мультиподпись трёх организаций. Считать 12% эмиссии выведенными из обращения нельзя.
- **Структура предложения исключительно чистая:** максимум жёстко ограничен 21 млн, выпущено 80,3%, вестинга, клиффов и разблокировок не существует, венчурного навеса нет, Founders' Reward завершился в 2020 году.

Рейтинг: 66 / 100, BBB

Zcash — противоположность типичной проблеме крипторынка. Обычно продукт растёт, а монета остаётся в стороне; здесь коин встроен в продукт настолько плотно, насколько это вообще возможно. Ограничивает оценку другое: против ежегодной эмиссии в 657 000 ZEC у модели нет ни одного механизма поглощения, а развитие сети оплачивается не выручкой, а разводнением держателей. Zcash решил задачу «зачем нужна монета» и не решил задачу «за счёт чего она дорожает, кроме спроса на приватность».

1. Вступительная часть

Аудит не несет коммерческой цели, а выводы не являются инвестиционной рекомендацией. Аудит предназначен для широкого круга лиц, а его разработка ставит перед собой цель выявить слабые места монеты $ZEC и показать их как самому проекту, так и всем держателям монеты $ZEC. При проведении аудита используются только открытые данные из сети Интернет.

Zcash — блокчейн Layer-1, запущенный 28 октября 2016 года как форк кодовой базы Bitcoin с добавлением криптографии с нулевым разглашением. Проект первым вывел доказательства zk-SNARK в промышленную эксплуатацию и остаётся основным активом нарратива приватности.

Основные отличительные функции:

- Два типа адресов: прозрачные (как в Bitcoin) и экранированные, где сумма, отправитель и получатель скрыты криптографически.
- Консенсус Proof-of-Work на алгоритме Equihash; стейкинга в сети нет.
- Максимальная эмиссия 21 млн ZEC с халвингом раз в четыре года — денежная политика унаследована от Bitcoin.

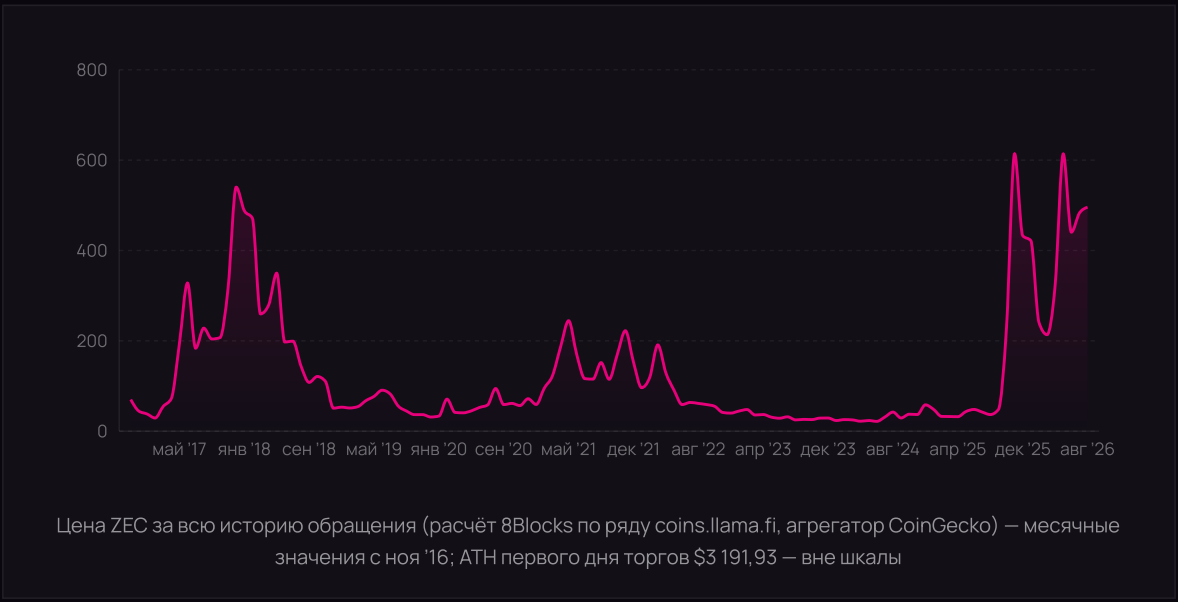
- Разработку ведут Electric Coin Company и Zcash Foundation, изменения принимаются через публичный процесс предложений ZIP.

В обращении находится 16 872 342 ZEC — 80,3% максимальной эмиссии. Монета используется для хранения, перевода и оплаты внутри сети; иных функций у неё нет.

Сайт: z.cash

2. Цена монеты

2.1 Анализ цены монеты



Цена ZEC за всю историю обращения (расчёт 8Blocks по ряду coins.llama.fi, агрегатор CoinGecko) — месячные значения с ноя '16; ATH первого дня торгов $3 191,93 — вне шкалы

- Текущая цена: $495,79 на 13 августа 2026 года;
- All-Time High (ATH): $3 191,93, зафиксирован 28 октября 2016 года — в первый день торгов;
- All-Time Low (ATL): $16,08, зафиксирован 4 июля 2024 года;
- Капитализация: $8,38 млрд, 15-е место по капитализации;
- Дневной объём торгов: $212,6 млн — около 2,5% от капитализации.

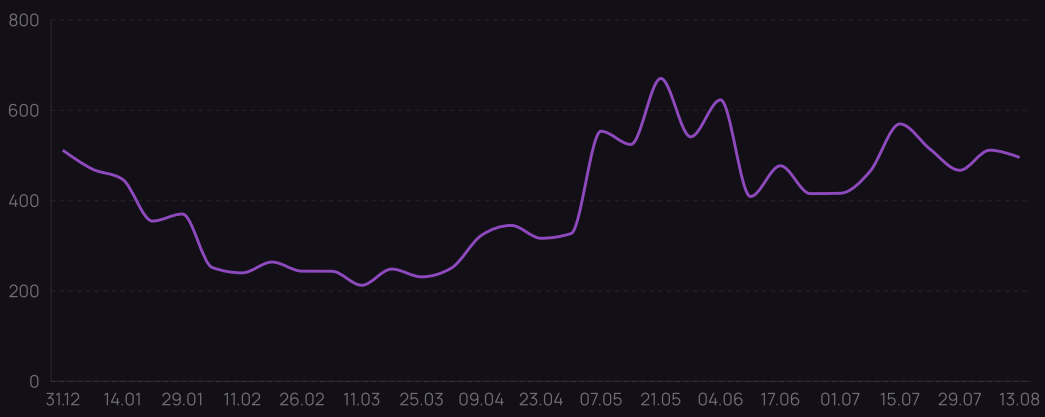
История цены распадается на четыре фазы.

Первая — запуск в октябре 2016 года: из-за нулевого предложения в первые часы торгов цена достигла $3 191,93, а уже к концу декабря того же года опустилась до $44 — этот максимум не превзойдён до сих пор.

Вторая — восемь лет затухающих циклов: пики $540 в декабре 2017 года и $244 в мае 2021 года, между ними и после них — снижение до исторического минимума $16,08 в июле 2024 года.

Третья — взрывной рост осени 2025 года: с $47,91 в середине сентября до $614 к 10 ноября, то есть примерно в тринадцать раз за два месяца.

Четвёртая — волатильный 2026 год: откат до $213 к марту, второй пик $671 к 21 мая, падение после раскрытия уязвимости Orchard и восстановление к ~$490 в августе.



Цена ZEC в 2026 году: пик, раскрытие уязвимости и восстановление (расчёт 8Blocks по ряду coins.llama.fi)

Важно

недельный ряд показывает механику падения точно: пик $671 зафиксирован 21 мая, к 4 июня цена снизилась до $623, а к 11 июня — до $409. Это минус 34,3% за неделю, на которую пришлись экстренный софт-форк 2 июня и хард-форк 3 июня. По данным KuCoin Research основное движение уложилось в одни сутки, а распродажу усилил публичный выход крупного участника рынка. К августу цена вернулась к уровням около $490 — то есть выше, чем была до пика мая.

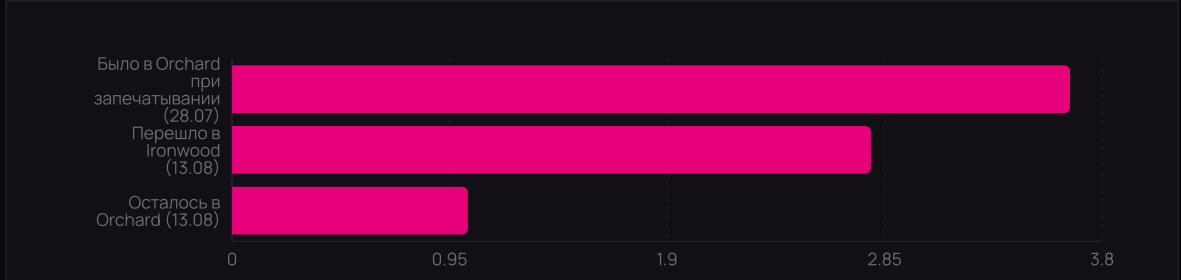
Оборот в 2,5% от капитализации при 15-м месте в рейтинге говорит о достаточной, но не выдающейся ликвидности. Отдельный структурный фактор — регуляторный: приватные активы периодически исключаются с площадок отдельных юрисдикций, и часть бирж Азии и Ближнего Востока вернула торговые пары лишь в начале 2026 года.

Важно

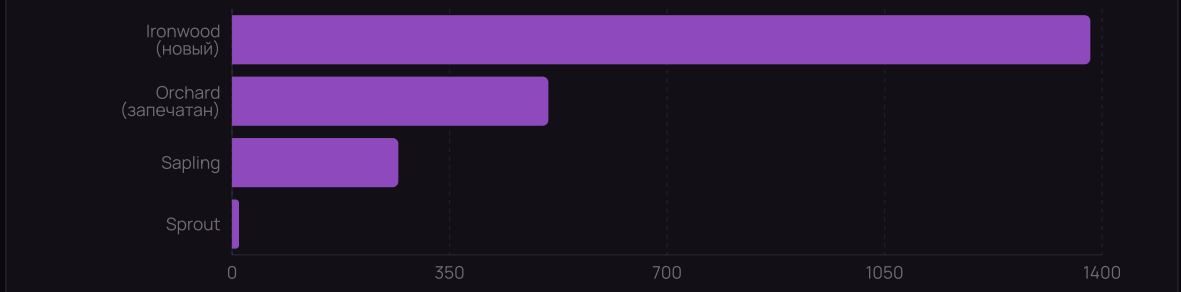
совпадение событий во времени не является доказательством причинности. Перечисленные выше события совпали с фазами движения цены, но количественно измерить их вклад по открытым данным невозможно.

2.2 Анализ экранированного пула (аналог TVL)

У Zcash нет DeFi-слоя и, соответственно, показателя TVL. Функциональный аналог — объём средств в экранированных пулах: он показывает, какая часть предложения реально используется ради приватности, то есть ради того, зачем существует сам продукт.



Миграция средств из запечатанного Orchard в Ironwood (расчёт 8Blocks по данным CoinDesk и zkp.baby) — млн ZEC



Состав экранированного пула на момент написания документа (расчёт 8Blocks по данным zkp.baby) — $ млн

Совокупно экранировано 4 374 320 ZEC — 25,92% предложения, около $2,17 млрд. Распределение по пулам:

Пул	Объём, ZEC	Стоимость	Статус
Ironwood	2 785 354	$1,38 млрд	активный, запущен 28.07.2026
Orchard	1 026 678	$0,51 млрд	запечатан, только вывод
Sapling	539 667	$0,27 млрд	активный, с 2018 года
Sprout	22 621	$0,01 млрд	устаревший

> **Важно**
>
> за 16 дней после активации Ironwood из запечатанного Orchard перешло 73% средств — 2,79 млн ZEC из 3,66 млн. Миграция полностью добровольная и требует действия от каждого владельца. Такая скорость при отсутствии дедлайна — сильный сигнал вовлечённости держателей: это не пассивные балансы, а активно управляемые средства.

Доля экранированного предложения — ключевая метрика продукта. Она означает, что четверть всех ZEC используется по прямому назначению, а не просто лежит на биржах. Накопительно по сети проведено 3,29 млн экранированных транзакций (Sapling и Orchard), из них около 2,87 млн после отсеивания спама.

2.3 Выводы относительно цены монеты

ПОЗИТИВНЫЕ ФАКТОРЫ И ФАКТОРЫ РИСКА

- ✓ Цена выросла примерно в тридцать раз от исторического минимума июля 2024 года, при этом рост совпал с проверяемыми институциональными событиями, а не только с рыночным циклом.
- ✓ Рынок быстро восстановился после раскрытия уязвимости: падение на 30–37% отыграно за два месяца.
- ✓ 15-е место по капитализации и оборот 2,5% обеспечивают ликвидность, достаточную для институционального участия.
- - Цена крайне чувствительна к сообщениям о криптографии: один отчёт об уязвимости стоил трети капитализации за сутки.
- - Регуляторный риск структурен для категории: делистинги приватных активов происходили и могут повториться.
- - Максимум 2016 года не превзойдён за десять лет, что ограничивает историческую базу для оценки потолка.

Цена ZEC определяется спросом на приватность и доверием к криптографии сети. Продуктовая метрика — доля экранированного предложения — растёт, и это единственный измеримый канал связи между использованием сети и спросом на монету. Экономических механизмов, преобразующих активность в покупательское давление, у модели нет.

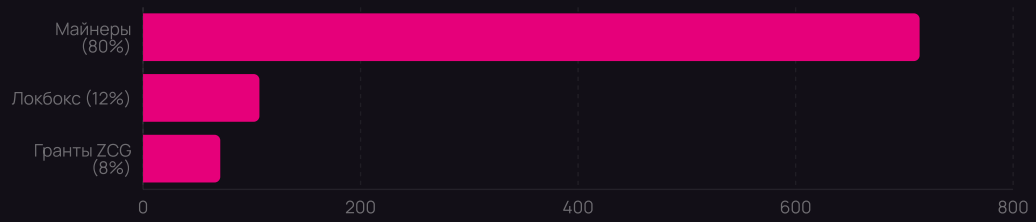
3. Распределение монет

Максимальная эмиссия ограничена 21 млн ZEC, выпущено 16 872 342 — 80,3%. Денежная политика унаследована от Bitcoin: награда за блок уменьшается вдвое примерно раз в четыре года, последний халвинг прошёл в ноябре 2024 года (награда снизилась с 3,125 до 1,5625 ZEC), следующий ожидается 23 ноября 2028 года.

> **Важно**
>
> у ZEC нет ни вестинга, ни клиффов, ни разблокировок — этих понятий не существует в модели в принципе. Всё новое предложение поступает единственным способом: через награду за блок. Венчурных аллокаций с дисконтом нет; Founders' Reward, действовавший первые четыре года, завершился в 2020 году.

3.1 Как распределены монеты, клифы и разморозки

Единственный источник нового предложения — блок-награда. Она делится по правилам ZIP-1015, продлённым ZIP-271:



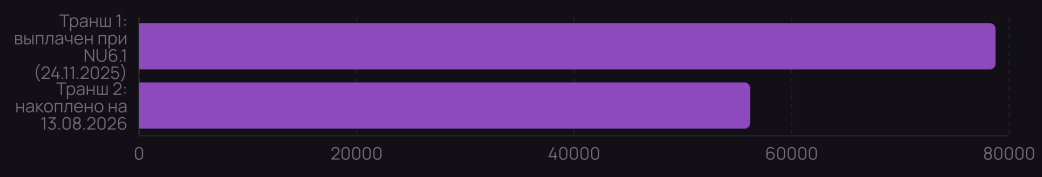
Распределение дневной эмиссии (расчёт 8Blocks по данным z.cash/network и zkp.baby) — $ тыс. в сутки

Получатель	Доля	ZEC в сутки	В долларах в сутки
Майнеры	80%	1 440	$713 938
Локбокс (отложенный фонд)	12%	216	$107 091
Гранты сообщества ZCG	8%	144	$71 394
Итого	100%	1 800	$892 422

Расчёт: 1 152 блока в сутки × 1,5625 ZEC × $495,79. В годовом выражении эмиссия составляет 657 000 ZEC, или $325,7 млн — **3,89% от текущего обращения**.

Локбокс требует отдельного разбора, поскольку его часто трактуют как механизм вывода монет из обращения. Это не так. Проверка арифметикой:

- ZIP-1015 направлял 12% блок-награды в локбокс с блока 2 726 400 по блок 3 146 400 — это 420 000 блоков;
- 420 000 × 1,5625 × 12% = **78 750 ZEC** — ровно та сумма, которую ZIP-271 предписал выплатить разово;
- выплата произведена при обновлении NU6.1 24 ноября 2025 года на адрес мультиподписи 2 из 3, ключи у Zcash Foundation, Electric Coin Company и Shielded Labs;
- с NU6.1 по 13 августа 2026 года накоплено 56 187,56 ZEC, что совпадает с расчётом по 299 666 блокам.



Локбокс: накопление и выплата первого транша (расчёт 8Blocks по ZIP-1015, ZIP-271 и балансу локбокса) — ZEC

> **Важно**
>
> локбокс является механизмом отложенной выплаты, а не блокировки. Первый транш был полностью выплачен на двенадцатый месяц накопления. Считать 12% эмиссии выведенными из обращения нельзя: это отложенное предложение, которое поступит на рынок по решению трёх организаций. Порядок распоряжения вторым траншем на момент написания документа не утверждён — ZIP-1016, описывающий голосование коинхолдеров с кворумом 420 000 ZEC, имеет статус предложения.

3.2 Выводы относительно распределения монет

ПОЗИТИВНЫЕ ФАКТОРЫ И ФАКТОРЫ РИСКА

- ✓ Максимальная эмиссия жёстко ограничена 21 млн ZEC на уровне протокола; выпущено уже 80,3%, а темп выпуска снижается вдвое каждые четыре года.
- ✓ Вестинга, клиффов и разблокировок не существует — календарного навеса предложения нет ни в какой форме.

- ✓ Нет венчурного навеса и монет, купленных с дисконтом: Founders' Reward завершился шесть лет назад.
- ✓ График эмиссии проверяется поблочно и сходится с фактическими балансами до затоши.
- - 20% всей новой эмиссии направляется организациям, а не участникам сети: держатель финансирует разработку разводнением своей доли.
- - Порядок распоряжения локбоксом определяется постфактум — на момент начала накопления механизм выплаты не был установлен, а модель голосования коинхолдеров до сих пор не активирована.
- - Правила финансирования менялись четырежды за историю проекта, а ZIP-234 предполагает замену схемы халвингов на плавную кривую целиком.
- - Фактическая концентрация держателей структурно неизмерима: экранирование делает классификацию адресов невозможной по устройству сети.

Структура предложения ZEC — одна из самых чистых на рынке: без премайна в обращении, без инвесторского навеса, без календарных разблокировок, с жёстким потолком. Единственный спорный элемент — 20% эмиссии, уходящие организациям, и неопределённость с распоряжением локбоксом. Это не скрытый риск, а осознанный компромисс: проект без выручки финансирует разработку единственным доступным способом.

4. Стейкинг и фарминг

4.1 Анализ инструментов

Стейкинга в сети Zcash не существует. Консенсус построен на Proof-of-Work, и новые монеты получают майнеры за вычислительную работу, а не держатели за блокировку средств. Ликвидного стейкинга, фарминга и программ вознаграждения за предоставление ликвидности проект не предлагает.

> Важно
>
> отсутствие стейкинга означает, что у держателя нет ни одного протокольного способа получить доход от владения монетой и ни одного повода выводить её из свободного обращения. Экранирование средств — не блокировка: монеты выводятся из пула в любой момент.

В разработке находится **Zcash Trailing Finality Layer** (проект Crosslink) — гибридная модель, добавляющая слой финальности на основе доказательства доли к существующему Proof-of-Work. По открытым данным ориентировочный срок — 2026–2027 годы.

> Важно
>
> если Trailing Finality Layer будет запущен со стейкингом ZEC, у монеты впервые появится механизм связывания предложения и доходность, обеспеченная работой сети. На момент написания документа это разрабатываемое предложение, а не действующий механизм, и оценивать его как работающий нельзя.

4.2 Анализ формул

Формула эмиссии унаследована от Bitcoin и задана в протоколе:

- Награда за блок после халвинга ноября 2024 года: **1,5625 ZEC**;
- Целевое время блока: 75 секунд, то есть **1 152 блока в сутки**;
- Дневная эмиссия: 1 152 × 1,5625 = **1 800 ZEC**;
- Годовая эмиссия: 657 000 ZEC, или **3,89% текущего обращения**;
- Следующий халвинг: **23 ноября 2028 года**, после которого награда снизится до 0,78125 ZEC за блок.

Предложение ZIP-234 предполагает замену дискретных халвингов плавной логарифмической кривой: доля от остатка денежного резерва в каждом блоке (BLOCK_SUBSIDY_FRACTION = 0,0000004126), что за четыре года даёт примерно тот же результат, но без ступенчатых обрывов. Статус предложения — черновик, активация запланирована вместе с Network Upgrade 7.

> Важно
>
> у ZIP-234 есть неочевидное следствие: плавная кривая допускает повторное вовлечение изъятых из обращения ZEC в будущие блок-награды. Это меняет трактовку потолка в 21 млн — он остаётся, но становится асимптотическим.

Вместе с ZIP-234 к Network Upgrade 7 рассматриваются ещё два предложения того же пакета Network Sustainability Mechanism. **ZIP-233** вводит в протокол саму возможность безвозвратно выводить средства из обращения. **ZIP-235** применяет её к комиссиям: 60% каждой комиссии перестают доставаться майнеру и уничтожаются. Оба имеют статус черновика и на мейннете не действуют. При сегодняшнем объёме комиссий эффект ZIP-235 был бы символическим — заведомо менее 0,1% годовой эмиссии, — но это был бы первый в истории проекта механизм поглощения предложения, а его вклад рос бы вместе с числом транзакций.

4.3 Анализ денежных потоков

Приток на рынок (эмиссия):

- Майнеры: 1 440 ZEC в сутки (~$713 938) — продаются для покрытия затрат на электроэнергию и оборудование;
- Локбокс: 216 ZEC в сутки (~$107 091) — отложенное предложение, выходит траншами по решению организаций;
- Гранты ZCG: 144 ZEC в сутки (~$71 394) — распределяются командам экосистемы.

Вывод из обращения:

- Механизмы вывода отсутствуют: сжигания нет, выкупа нет, протокольных блокировок нет.

> Важно
>
> баланс односторонний: 657 000 ZEC в год поступает на рынок, ноль выводится. Комиссии сети, которые в других сетях служат источником сжигания, здесь минимальны по объёму и целиком достаются майнерам. Проект финансирует своё развитие из кармана держателя — это работоспособная модель для денежного

актива, но она означает, что цена должна расти минимум на 3,89% в год только для сохранения доли держателя.

Объём комиссий поддаётся точному расчёту. Ставка задана ZIP-317: 5 000 затоши за логическое действие при минимуме в два действия, то есть **0,0001 ZEC** за типовую транзакцию. Накопительно по сети проведено 3,29 млн экранированных транзакций — это **329 ZEC** комиссий, около $163 тыс. по цене снимка. Против годовой эмиссии в 657 000 ZEC это **0,05% одного года**. Чтобы комиссии достигли хотя бы одного процента годовой эмиссии, сети потребовалось бы 180 000 транзакций в сутки при историческом темпе порядка тысячи. При этом комиссии не выводятся из обращения: они входят в coinbase-выход блока и целиком принадлежат майнеру, а распределение 80 / 12 / 8 к ним не применяется — оно действует только для блок-субсидии. Отдельного адреса или фонда, где комиссии накапливались бы, в протоколе не существует.

Отдельно стоит зафиксировать источник финансирования разработки. У Zcash нет протокольной выручки: комиссии за транзакции ничтожны, платящих клиентов у сети нет. Electric Coin Company, Zcash Foundation и грантополучатели финансируются исключительно долей в блок-награде. Это принципиально отличается от проектов, где разработка оплачивается выручкой продукта.

4.4 Выводы

- Стейкинга нет; протокольной доходности у держателя нет; предложение не связывается ни на какой срок.
- Источник новых монет — исключительно блок-награда, потолок жёстко ограничен 21 млн, темп снижается вдвое каждые четыре года.
- 20% эмиссии финансирует развитие проекта за счёт разводнения держателей — прямой, но честно раскрытый компромисс.
- Trailing Finality Layer способен изменить эту картину, но пока остаётся разработкой.

Раздел, который у большинства проектов описывает механику удержания токена, у Zcash описывает денежную политику. Это последовательная позиция для актива, претендующего на роль частных денег: у наличных тоже нет доходности. Риск в другом — денежный актив без доходности требует, чтобы спрос на его основную функцию рос быстрее эмиссии.

5. Утилизация монет

5.1 Сценарии использования

- **Приватный перевод** — основная и, по сути, единственная функция: экранированная транзакция скрывает сумму, отправителя и получателя. Без владения ZEC она невозможна.
- **Прозрачный перевод и хранение** — функциональность уровня Bitcoin.
- **Оплата комиссий сети** — любая транзакция требует ZEC.
- **Обеспечение безопасности сети** — через майнинг, но это функция вычислительной мощности, а не владения монетой.

Важно

на ключевую проверку методологии — можно ли пользоваться продуктом, не владея монетой — ответ однозначный: нельзя. ZEC не надстройка над продуктом,

а сам продукт. Это высшая категория необходимости монеты, и по этому показателю Zcash получает максимальную оценку.

Оборотная сторона той же медали: у монеты нет ни одной дополнительной функции. Governance-прав она не даёт — решения принимаются через процесс ZIP операторами узлов, а не голосованием держателей; предложенная модель голосования коинхолдеров ZIP-1016 не активирована. Доходности монета не приносит. Расширять утилиту некуда без изменения природы актива.

5.2 Инструменты и сервисы

- **Zashi** — официальный кошелёк Electric Coin Company с поддержкой экранированных адресов и обменом через Near Intents;
- **Gemini** — экранированные выводы ZEC, первый подобный случай среди крупных бирж (ноябрь 2025);
- **Coinbase Custody и BitGo** — институциональное хранение с поддержкой экранированных балансов (конец 2025). Это первый случай, когда регулируемый кастодиан США официально поддержал экранирование;
- **Grayscale Zcash Trust** — инвестиционный траст с активами около $190 млн;
- **Zcash Shielded Assets (ZSA)** — предложение о выпуске сторонних активов в экранированном виде, находится в разработке.

> Важно
>
> подключение регулируемых кастодианов к экранированным балансам — важнейшее событие для категории. Оно снимает главное практическое возражение против приватных активов: невозможность институционального хранения в правовом периметре.

5.3 Выводы

- Монета незаменима для основной функции продукта — это максимальная оценка по шкале необходимости.
- Утилита единственная и не расширяется: ни governance, ни доходности, ни применения за пределами сети.
- Экосистема сервисов вокруг монеты за 2025–2026 годы заметно окрепла: институциональное хранение, экранированные выводы на биржах, инвестиционный траст.

На вопрос методологии «Кто и зачем будет покупать эту монету?» Zcash отвечает прямее большинства проектов: покупает тот, кому нужна финансовая приватность, и покупает потому, что без ZEC её не получить. Слабость ответа не в самом механизме, а в размере рынка: он определяется спросом на приватность, а не масштабом какого-либо бизнеса.

6. Обращение монет

6.1 Как двигаются монеты

1. Приток в обращение:

- Блок-награда — единственный источник: 1 800 ZEC в сутки, из них 1 440 майнерам, 216 в локбокс, 144 в гранты;
- Транши локбокса — отложенное предложение, выходящее на рынок по решению организаций (первый транш 78 750 ZEC выплачен в ноябре 2025 года).

2. Вывод из обращения:

- Протокольных механизмов вывода нет: сжигания, выкупа и блокировок не предусмотрено.
- Экранирование средств не является выводом: 4,37 млн ZEC в пулах могут быть перемещены владельцами в любой момент.

> Важно
>
> особый случай — запечатанный пул Orchard. С 28 июля 2026 года из него возможен только вывод через turnstile: правило на границе пула ограничивает суммарный вывод объёмом верифицируемо внесённых средств. Это не блокировка капитала, а защита от вывода потенциально поддельных монет; 73% средств уже перешли в Ironwood. Оставшиеся 1,03 млн ZEC выводятся без ограничения по времени.

Обращение ZEC устроено как у Bitcoin: майнеры продают часть добытого для покрытия издержек, остальное перераспределяется рынком. Treasury-контура накопления и повторного использования монет у проекта нет — локбокс выполняет роль фонда развития, а не механизма поддержки цены.

6.2 Риски

- Полное отсутствие механизмов поглощения при эмиссии 657 000 ZEC в год: всё новое предложение должно быть выкуплено органическим спросом.
- Финансирование разработки разводнением: если спрос на приватность стагнирует, 20% эмиссии становятся чистым давлением на цену без компенсирующего эффекта.
- Неопределённость с локбоксом: порядок распоряжения вторым траншем не утверждён, объём растёт на 216 ZEC в сутки.
- Регуляторный риск категории: делистинг приватных активов на отдельных площадках сокращает ликвидность и доступность.
- Риск криптографии: дефекты схем экранирования по природе недетектируемы, а рынок реагирует на них падением на треть за сутки.

> Важно
>
> главный баланс, за которым нужно следить, — темп роста экранированного предложения против темпа эмиссии. Экранированный пул растёт быстрее 3,89% в год, значит спрос на основную функцию опережает разводнение. Разворот этого соотношения будет первым признаком того, что модель перестала работать.

7. Критические замечания

- **Развитие оплачивает держатель, а не выручка.** Комиссии сети ничтожны, платящих клиентов нет, поэтому 20% каждой блок-награды уходит организациям. Модель работоспособна, но она означает, что качество разработки напрямую зависит от цены монеты, а держатель несёт эти расходы через разводнение на 3,89% в год.
- **Против эмиссии нет ни одного механизма поглощения.** Сжигания, выкупа, стейкинга и залоговых блокировок не существует. Единственный источник спроса — желание владеть приватными деньгами. Для денежного актива это допустимо, но лишает модель какой-либо встроенной поддержки в периоды падения спроса.
- **Уязвимость Orchard четыре года оставалась незамеченной.** Дефект схемы, допускавший недетектируемую подделку, существовал с 2022 года и был найден исследователем, а не аудитом. Свидетельств эксплуатации не найдено и потерь нет, но сам факт означает: в системе, где предложение непроверяемо по устройству, целостность обеспечивается только качеством криптографии и механизмом turnstile.
- **Локбокс не является стоком.** Трактовка 12% эмиссии как выведенных из обращения средств неверна: первый транш был полностью выплачен трём организациям через двенадцать месяцев после начала накопления. Порядок распоряжения вторым траншем до сих пор не утверждён.
- **Правила финансирования нестабильны.** За историю проекта модель менялась четырежды, а ZIP-234 предполагает замену схемы халвингов целиком, что сделает потолок в 21 млн асимптотическим. Для актива, чья ценность строится на предсказуемости денежной политики, частота изменений — самостоятельный риск.

При этом ответ проекта на инцидент 2026 года заслуживает отдельного признания. Пять дней от раскрытия до исправления, шестьдесят дней до полной замены пула, механизм turnstile, ограничивший возможный ущерб объёмом верифицируемо внесённых средств, формальная верификация новой схемы и ноль потерь у пользователей — это лучший из возможных сценариев для уязвимости такого класса.

8. Итоговое заключение

Zcash решает задачу, на которой спотыкается большинство токенов: связь между продуктом и монетой. Здесь её не нужно выстраивать — она встроена в саму природу актива. Приватная транзакция невозможна без ZEC, обойти монету нельзя, заменить её нечем. По шкале необходимости монеты это высшая категория, и она встречается редко.

Ограничивает оценку экономика. У сети нет выручки: комиссии минимальны и достаются майнерам, платящих клиентов нет, а разработка финансируется двадцатью процентами эмиссии — то есть разводнением держателей на 3,89% в год. Против этого потока не стоит ни один механизм поглощения: сжигания нет, выкупа нет, стейкинга нет, а локбокс, который часто принимают за сток, оказался отложенной выплатой — его первый транш в 78 750 ZEC был полностью выплачен трём организациям.

Структура предложения при этом исключительно чистая. Потолок жёстко ограничен, выпущено 80,3%, вестинга и разблокировок не существует, венчурного навеса нет. Проекту не нужно оправдываться за инсайдерские аллокации — их просто нет. Это редкое сочетание: слабая экономика передачи ценности при безупречной механике предложения.

2026 год стал для сети проверкой на прочность. Уязвимость, четыре года просуществовавшая незамеченной в главном пуле, могла закончиться катастрофой для актива, чья ценность целиком построена на доверии к криптографии. Не закончилась: потерь нет, исправление заняло пять дней, замена пула — шестьдесят, а держатели за шестнадцать дней добровольно перевели 73% средств в новый пул. Последняя цифра говорит о проекте больше, чем любые заявления: у сети есть сообщество, которое действует.

Ключевой вопрос для Zcash — станет ли спрос на приватность расти быстрее, чем сеть печатает новые монеты. Сегодня доля экранированного предложения растёт быстрее эмиссии, и это единственное, что удерживает модель в равновесии. Появление Trailing Finality Layer со стейкингом или любого механизма поглощения предложения изменило бы картину принципиально.

8.1 Рекомендации для проекта

1 Утвердить порядок распоряжения локбоксом до того, как второй транш достигнет размера первого.

Сегодня 216 ZEC в сутки накапливаются без утверждённого механизма выплаты, а модель голосования коинхолдеров ZIP-1016 остаётся предложением. Неопределённость по 12% эмиссии — устранимый риск, который проект создаёт себе сам.

2 Довести до запуска Trailing Finality Layer со стейкингом ZEC.

Это единственный обсуждаемый механизм, способный одновременно связать предложение и дать держателю доходность, обеспеченную работой сети. Сегодня у монеты нет ни того, ни другого.

3 Создать источник протокольной выручки, не зависящий от эмиссии.

Zcash Shielded Assets — выпуск сторонних активов в экранированном виде — потенциально даёт сети платящих клиентов. Комиссия за такой выпуск стала бы первым в истории проекта доходом, не являющимся разводнением держателей.

4 Зафиксировать долгосрочность денежной политики.

Правила финансирования менялись четырежды, ZIP-234 меняет схему халвингов целиком. Для актива, продающего предсказуемость, стоит установить процедуру, повышающую порог изменения денежных параметров по сравнению с обычными ZIP.

5 Распространить формальную верификацию, применённую в Ironwood, на все действующие пулы и опубликовать регулярный отчёт о состоянии проверок.

Инцидент 2026 года показал, что четырёх лет обычного аудита недостаточно для схем такого класса.

6 Публиковать в открытом виде отчётность о расходовании средств локбокса и грантов ZCG.

Держатели финансируют разработку разводнением и должны видеть, на что уходят их деньги.

8.2 Важные замечания для инвесторов

1 Главная метрика для отслеживания — доля экранированного предложения.

Она показывает, растёт ли спрос на основную функцию сети. Сегодня 25,92%; устойчивый рост означает, что спрос опережает эмиссию в 3,89% годовых, снижение — обратное.

2 Держатель размывается на 3,89% в год, и механизма компенсации не существует.

Для сохранения доли нет способа: стейкинга нет, доходности нет. Цена должна расти минимум на эту величину только для сохранения позиции.

3 Локбокс — отложенное предложение, а не изъятые из обращения средства.

Второй транш растёт на 216 ZEC в сутки, и порядок его выплаты не утверждён. Решение по нему будет событием, влияющим на предложение.

4 Риск криптографии для приватного актива является главным, а не второстепенным.

Инцидент мая 2026 года стоил трети капитализации за сутки при том, что потерь не было вовсе. Позицию стоит оценивать с учётом того, что подобное может повториться.

5 Второй индикатор — статус Trailing Finality Layer.

Запуск стейкинга изменит экономику монеты принципиально; до официальной активации рассматривать это как факт нельзя.

6 Регуляторный риск структурен для категории приватных активов и не устраняется действиями проекта.

Закрытие проверки SEC в январе 2026 года — позитивный прецедент, но не гарантия для других юрисдикций.

Рейтинг $ZEC по методологии 8Blocks

Итоговый рейтинг: 66 / 100. Буквенный рейтинг: BBB.

Блок	Вес	Оценка (0–5)	Оценка (0–100)	Вклад в итог
Token Product Linkage	40%	2,78	55,6	22,24
Tokenomics Sustainability	20%	3,19	63,7	12,74
Fundamentals	15%	3,19	63,9	9,58
Governance / Control	10%	3,68	73,6	7,36
Security	10%	3,58	71,5	7,15
Market Layer	5%	4,08	81,6	4,08
Базовая оценка	100%			63,15
Бонусы				+3,00
Итого				66,15

Интерпретация. Token Product Linkage 2,78 — категория Moderate Linkage. Внутри блока крайние значения расходятся сильнее, чем у любого другого проекта: необходимость монеты оценена в 5,0 из 5,0 (максимум — монета незаменима), а передача ценности и механизмы поглощения предложения — в 1,5 и 1,2. Zcash не имеет проблемы «продукт растёт без монеты»; он имеет проблему «нет механизма, конвертирующего рост в стоимость».

Ограничитель рейтинга. При TPL в диапазоне 2,5–2,99 действует потолок 70 баллов. Базовая оценка 63,15 с бонусами даёт 66,15 — потолок не сработал, но запас составляет менее четырёх баллов. Повышение TPL выше 3,0 подняло бы потолок до 80 и стало бы наиболее результативным изменением.

Бонусы применены на +3: прохождение спадов 2018 и 2022 годов без остановки сети и изменения обязательств (+2) и качество реакции на инцидент 2026 года — пять дней до исправления, шестьдесят до замены пула, ноль потерь (+1). **Штраф за major exploit не применён**: методология требует значимых финансовых потерь, неполного восстановления и актуальности ущерба для текущей версии — ни одно из условий не выполняется.

Сильные стороны: необходимость монеты (максимальная оценка), чистота структуры предложения (нет вестинга, разблокировок и венчурного навеса при жёстком потолке), отсутствие админ-ключей и возможности изъятия средств, ликвидность 15-го актива рынка.

Что должно измениться для повышения рейтинга. Наибольший эффект даст появление любого механизма поглощения предложения — стейкинга через Trailing Finality Layer либо сжигания части комиссий по ZIP-235: это подняло бы Supply Sinks и Coverage, а с ними и TPL выше порога 3,0. Второй по значимости фактор — источник протокольной выручки, не связанный с эмиссией (ZSA), который снял бы зависимость разработки от разводнения. Третий — утверждение порядка распоряжения локбоксом.

Уверенность оценки: 82 / 100 (High). Расчёты эмиссии и локбокса сверены с фактическими балансами до затоши, все ключевые параметры зафиксированы в открытых спецификациях ZIP. Основное ограничение — концентрация держателей структурно неизмерима из-за экранирования. Сценарный диапазон: консервативный 61, базовый 66, оптимистичный 69 — разброс 8 пунктов, буквенная категория BBB устойчива во всех сценариях.

Дата снимка данных: 13 августа 2026 года.

Приложение. Источники данных

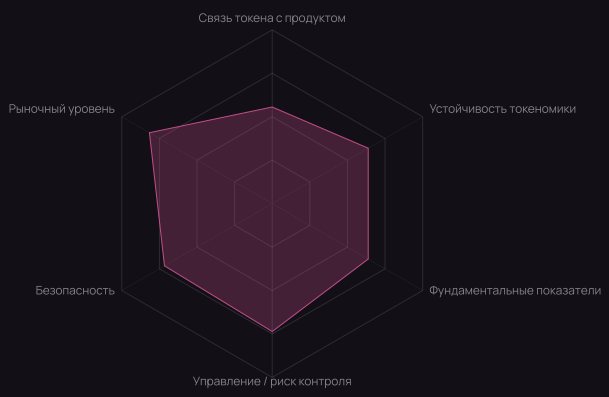
Данные	Источник	Дата
Описание продукта, организации, экосистема	z.cash (официальный сайт)	13.08.2026
Распределение блок-награды, халвинг, обращение	z.cash/network (официальный)	13.08.2026
Правила локбокса и грантов	ZIP-1015, ZIP-271, ZIP-1016 (zips.z.cash)	13.08.2026
Схема плавной эмиссии	ZIP-234 (черновик, zips.z.cash)	13.08.2026
Активация NU6.1 и высота блока	z.cash/upgrade/nu6-1	24.11.2025
Обновления кошелька, кастодианы, дорожная карта	electriccoin.co/blog	2025–2026
Цена, MC, FDV, supply, ATH/ATL, объём	CoinGecko	13.08.2026
Ряды цены (месячный и недельный)	coins.llama.fi (агрегатор CoinGecko)	13.08.2026
Экранированный пул по пулам, локбокс, высота блока	Дашборд zkp.baby	13.08.2026
Уязвимость Orchard, обновление Ironwood	The Block, CoinDesk	28–29.07.2026
Реакция рынка на раскрытие уязвимости	KuCoin Research	06.2026
Институциональное хранение, траст Grayscale, SEC	CryptoSlate	12.08.2026
Накопительное число экранированных транзакций	Coinpedia	12.08.2026
Ставка комиссии, механизмы вывода из обращения	ZIP-317, ZIP-233, ZIP-235 (zips.z.cash)	02.09.2026

Расхождения источников. Доля экранированного предложения: дашборд zkp.baby даёт 25,92% (4 374 320 ZEC), отдельные обзоры со ссылкой на CoinGecko приводят «более 30%» — в аудите используется дашборд как источник с поблочной детализацией по пулам. FDV: CoinGecko рассчитывает показатель от общего предложения 16,874 млн ($8,384 млрд), а не от максимальных 21 млн (что дало бы около $10,4 млрд); в аудите приведено значение источника. Объём Orchard на момент запечатывания: The Block указывает 3,6 млн ZEC, CoinDesk — 3,66 млн ZEC; расхождение в пределах округления и на выводы не влияет. Согласно политике источников 8Blocks первичной является документация проекта: параметры эмиссии и распределения взяты из спецификаций ZIP и сверены расчётом с фактическими балансами.

Ограничения аудита. Первое: графики цены построены по прореженному ряду (месячный шаг для всей истории, недельный для 2026 года), поэтому точные внутридневные экстремумы в них не попадают — значения ATH и ATL в тексте приведены по CoinGecko отдельно. Второе: исторической динамики экранированного пула в открытых API получить не удалось, поэтому пул показан текущим составом и сопоставлением «до и после» запечатывания Orchard. Третье: классификация адресов и анализ концентрации держателей не проводились и в случае Zcash невозможны по устройству сети. Четвёртое: значения по разделу 4.2 относительно ZIP-233, ZIP-234 и ZIP-235 отражают статус черновика и подлежат пересмотру при активации Network Upgrade 7.

Итоговый рейтинг

ПРОФИЛЬ ПО БЛОКАМ



ДЕТАЛИЗАЦИЯ (0–100)

Связь токена с продуктом	**55.6**
Устойчивость токеномики	**63.8**
Фундаментальные показатели	**63.8**
Управление / риск контроля	**73.6**
Безопасность	**71.6**
Рыночный уровень	**81.6**

ИТОГОВОЕ ЗАКЛЮЧЕНИЕ

Zcash решил задачу «зачем нужна монета»: приватная транзакция без ZEC невозможна, потолок 21 млн, вестинга и разблокировок нет. Но комиссии ничтожны и уходят майнерам, а разработка оплачивается разводнением держателей на 3,89% в год без единого механизма поглощения эмиссии: рейтинг BBB, 66/100.

Аудит не является инвестиционной рекомендацией. Используйте его как часть собственного анализа.

ИТОГОВЫЙ РЕЙТИНГ

66 /100

РЕЙТИНГ BBB

Главный эксперт
Тони Эфрен in
Co-founder, 8Blocks

Блок	Вес	Оценка (0–5)	Оценка (0–100)	Вклад
Связь токена с продуктом	40%	2.78	55.6	**22.2**
Устойчивость токеномики	20%	3.19	63.8	**12.8**
Фундаментальные показатели	15%	3.19	63.8	**9.6**
Управление / риск контроля	10%	3.68	73.6	**7.4**
Безопасность	10%	3.58	71.6	**7.2**
Рыночный уровень	5%	4.08	81.6	**4.1**
Итого	**100%**	**3.2**	**63**	**63.3**