TOKEN AUDIT · 09.26

$ZEC

z.cash

FINAL RATING — BBB

66 /100

Zcash is a Layer-1 blockchain with zero-knowledge cryptography. Live since 2016, it was the first to bring zk-SNARKs into production.
Here the coin is the product: a shielded transaction is impossible without holding ZEC. Maximum supply 21m, 80.3% issued.

FDV	MC	SHIELDED	ANNUAL EMISSION	SHIELDED SHARE
$8.38bn	$8.38bn	$2.17bn	$326m	25.9%

ISSUED

80.3%

This coin is irreplaceable: no ZEC, no shielded transaction — but the model has not a single absorption mechanism against emission, and holders pay for development

Coin product linkage: the coin cannot be bypassed — without ZEC there is no shielded transaction. A 21m cap, no vesting and no unlocks.

Tokenomics sustainability: development is paid for by 3.89% annual dilution; there are no supply-absorption mechanisms.

Executive Summary of the ZEC Coin Audit

- **Here the coin is the product.** ZEC is the network's unit of account: a shielded transaction is impossible in principle without holding the coin. On the methodology's scale this is the unavoidable category — the maximum score for coin necessity, and a rare one on this market.
- **But it is holders who pay, not revenue.** Network fees are negligible and go to miners; there is no buyback, no burn and no revenue sharing. Development and grants are funded by dilution: 20% of every block reward goes to ecosystem organisations, and the holder is diluted by **3.89% a year**.
- **2026 was defined by the Orchard vulnerability.** A flaw in the scheme that had existed since 2022 theoretically allowed undetectable counterfeiting of ZEC. No evidence of exploitation was found and no funds were lost. The fix took **5 days** and the full replacement of the pool **60 days**: on 28 July 2026 Ironwood was activated with a turnstile mechanism that caps withdrawals at the volume of verifiably deposited funds.
- **The community answered with its money.** Within 16 days of activation, **2.79m ZEC out of 3.66m — 73%** moved from the sealed Orchard into Ironwood. In total 4.37m ZEC are shielded, or **25.92% of the supply** ($2.17bn).
- **The lockbox turned out to be a deferred payout, not a lock-up.** The arithmetic matches to the zatoshi: over 420,000 blocks exactly 78,750 ZEC accumulated, and the entire amount was paid out at the NU6.1 upgrade to a multisig held by three organisations. The 12% of emission cannot be treated as withdrawn from circulation.
- **The supply structure is exceptionally clean:** the maximum is hard-capped at 21m, 80.3% has been issued, vesting, cliffs and unlocks do not exist, there is no venture overhang, and the Founders' Reward ended in 2020.

Rating: 66 / 100, BBB

Zcash is the opposite of the typical problem on the crypto market. Usually the product grows while the coin stays on the sidelines; here the coin is built into the product as tightly as it is possible to be. What limits the score is something else: against annual emission of 657,000 ZEC the model has not a single absorption mechanism, and the network's development is paid for not by revenue but by diluting holders. Zcash has solved the question of "why the coin is needed" and has not solved the question of "what makes it appreciate, other than demand for privacy".

1. Introduction

This audit has no commercial purpose and its conclusions are not investment advice. The audit is intended for a broad audience; its aim is to identify the weak points of the $ZEC coin and to show them both to the project itself and to every $ZEC holder. Only public data from the internet is used in the audit.

Zcash is a Layer-1 blockchain launched on 28 October 2016 as a fork of the Bitcoin codebase with zero-knowledge cryptography added. The project was the first to bring zk-SNARK proofs into production use and remains the flagship asset of the privacy narrative.

Key distinguishing features:

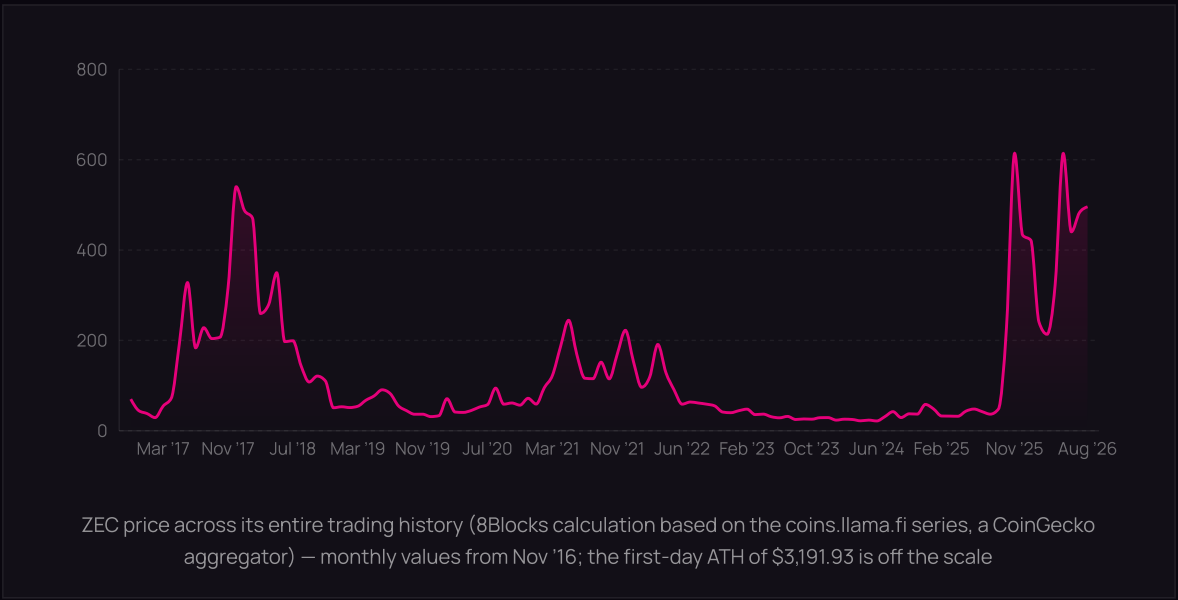
- Two types of address: transparent (as in Bitcoin) and shielded, where the amount, the sender and the recipient are hidden cryptographically.
- Proof-of-Work consensus on the Equihash algorithm; there is no staking in the network.
- A maximum supply of 21m ZEC with a halving every four years — the monetary policy is inherited from Bitcoin.
- Development is led by Electric Coin Company and the Zcash Foundation, and changes are adopted through the public ZIP proposal process.

16,872,342 ZEC are in circulation — 80.3% of the maximum supply. The coin is used for storing, transferring and paying inside the network; it has no other functions.

Website: z.cash

2. Coin price

2.1 Coin price analysis



ZEC price across its entire trading history (8Blocks calculation based on the coins.llama.fi series, a CoinGecko aggregator) — monthly values from Nov '16; the first-day ATH of $3,191.93 is off the scale

- Current price: $495.79 as of 13 August 2026;
- All-Time High (ATH): $3,191.93, recorded on 28 October 2016 — the first day of trading;
- All-Time Low (ATL): $16.08, recorded on 4 July 2024;
- Capitalisation: $8.38bn, 15th by market capitalisation;
- Daily trading volume: $212.6m — around 2.5% of capitalisation.

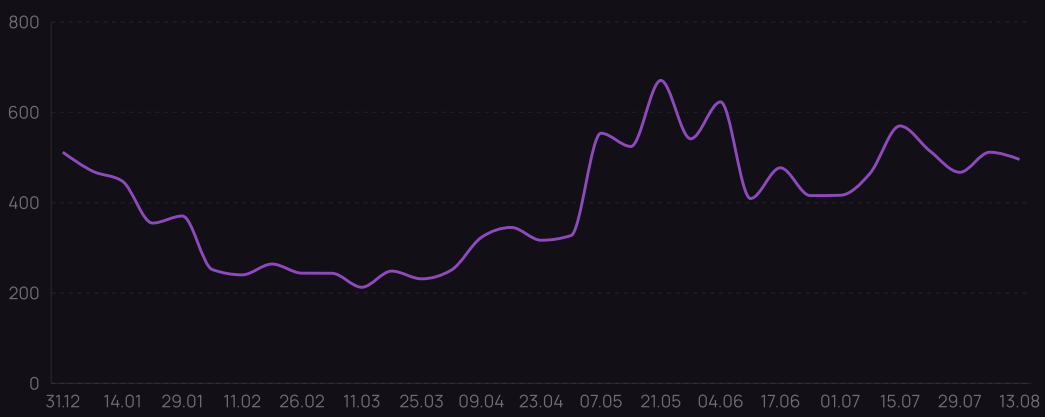
The price history falls into four phases.

The first is the launch in October 2016: with supply at zero in the first hours of trading the price reached $3,191.93, and by the end of December of the same year it had fallen to $44 — that high has still not been surpassed.

The second is eight years of fading cycles: peaks of $540 in December 2017 and $244 in May 2021, with a decline between and after them down to the all-time low of $16.08 in July 2024.

The third is the explosive growth of autumn 2025: from $47.91 in mid-September to $614 by 10 November, roughly a thirteen-fold rise in two months.

The fourth is the volatile year 2026: a pullback to $213 by March, a second peak of $671 by 21 May, a fall after the disclosure of the Orchard vulnerability and a recovery to around $490 in August.



ZEC price in 2026: the peak, the vulnerability disclosure and the recovery (8Blocks calculation based on the coins.llama.fi series)

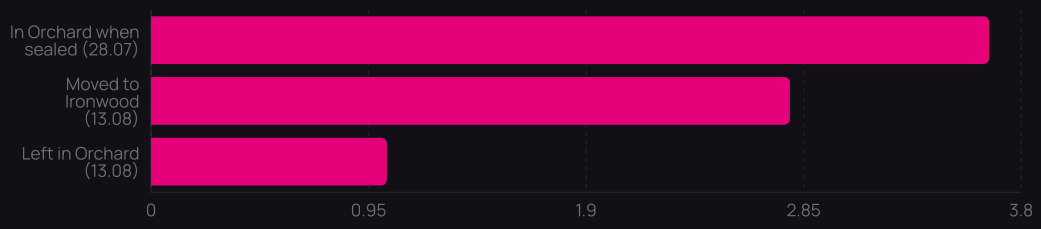
> Important
>
> the weekly series shows the mechanics of the fall precisely: the peak of $671 was recorded on 21 May, by 4 June the price had fallen to $623 and by 11 June to $409. That is minus 34.3% over a week that contained the emergency soft fork of 2 June and the hard fork of 3 June. According to KuCoin Research the bulk of the move fitted into a single day, and the sell-off was amplified by the public exit of a large market participant. By August the price had returned to levels around $490 — that is, higher than it stood before the May peak.

Turnover of 2.5% of capitalisation at 15th place in the ranking indicates adequate but not outstanding liquidity. A separate structural factor is regulatory: privacy assets are periodically delisted from venues in individual jurisdictions, and some exchanges in Asia and the Middle East only restored their trading pairs at the beginning of 2026.

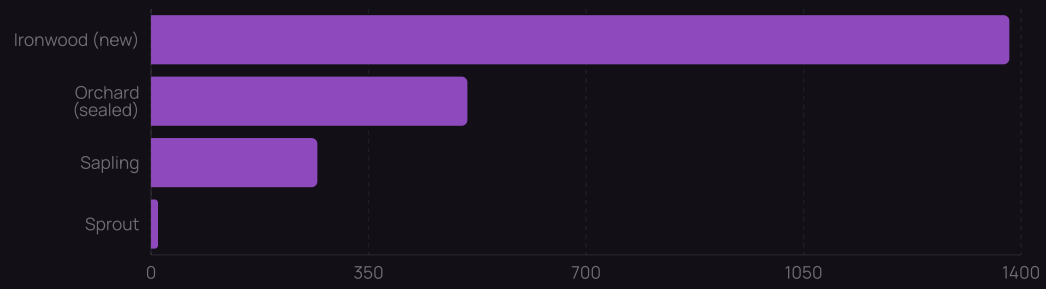
> Important
>
> a coincidence of events in time is not proof of causality. The events listed above coincided with phases of the price movement, but their contribution cannot be measured quantitatively from public data.

2.2 Shielded pool analysis (the TVL equivalent)

Zcash has no DeFi layer and therefore no TVL metric. The functional equivalent is the volume of funds held in the shielded pools: it shows what share of the supply is actually used for privacy — that is, for the very reason the product exists.



Migration of funds from the sealed Orchard into Ironwood (8Blocks calculation based on CoinDesk and zkp.baby data) — m ZEC



Composition of the shielded pool at the time of writing (8Blocks calculation based on zkp.baby data) — $m

In total 4,374,320 ZEC are shielded — 25.92% of the supply, around $2.17bn. The breakdown by pool:

Pool	Volume, ZEC	Value	Status
Ironwood	2,785,354	$1.38bn	active, launched 28.07.2026
Orchard	1,026,678	$0.51bn	sealed, withdrawals only
Sapling	539,667	$0.27bn	active, since 2018
Sprout	22,621	$0.01bn	deprecated

> **Important**
>
> within 16 days of the Ironwood activation, 73% of the funds moved out of the sealed Orchard — 2.79m ZEC out of 3.66m. The migration is entirely voluntary and requires action from every owner. Such speed in the absence of any deadline is a strong signal of holder engagement: these are not passive balances but actively managed funds.

The shielded share of supply is the product's key metric. It means that a quarter of all ZEC is used for its intended purpose rather than simply sitting on exchanges. Cumulatively the network has processed 3.29m shielded transactions (Sapling and Orchard), of which around 2.87m remain once spam is filtered out.

2.3 Conclusions on the coin price

POSITIVE FACTORS AND RISK FACTORS

- ✓ The price has risen roughly thirty-fold from the all-time low of July 2024, and that growth coincided with verifiable institutional events, not merely with the market cycle.
- ✓ The market recovered quickly after the vulnerability disclosure: a fall of 30–37% was recouped in two months.
- ✓ 15th place by capitalisation and turnover of 2.5% provide liquidity sufficient for institutional participation.
- - The price is extremely sensitive to news about cryptography: a single vulnerability report cost a third of the capitalisation in one day.
- - Regulatory risk is structural for the category: delistings of privacy assets have happened before and may happen again.
- - The 2016 high has not been surpassed in ten years, which limits the historical basis for estimating a ceiling.

The ZEC price is set by demand for privacy and by trust in the network's cryptography. The product metric — the shielded share of supply — is growing, and it is the only measurable channel linking use of the network to demand for the coin. The model has no economic mechanisms that convert activity into buying pressure.

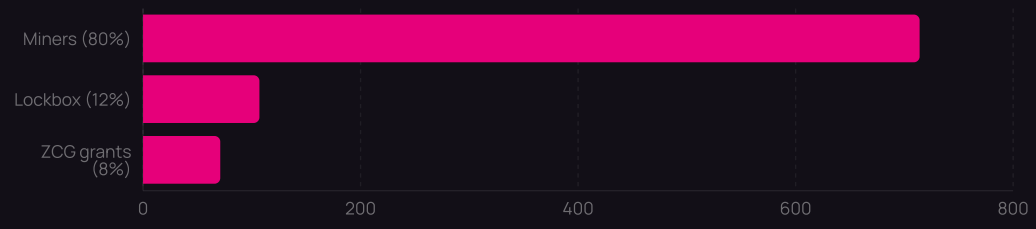
3. Coin distribution

The maximum supply is capped at 21m ZEC, of which 16,872,342 — 80.3% — has been issued. The monetary policy is inherited from Bitcoin: the block reward halves roughly every four years, the last halving took place in November 2024 (the reward fell from 3.125 to 1.5625 ZEC), and the next is expected on 23 November 2028.

> **Important**
>
> ZEC has no vesting, no cliffs and no unlocks — these concepts do not exist in the model at all. All new supply arrives in a single way: through the block reward. There are no discounted venture allocations; the Founders' Reward, which ran for the first four years, ended in 2020.

3.1 How coins are distributed, cliffs and unlocks

The only source of new supply is the block reward. It is split according to the rules of ZIP-1015, extended by ZIP-271:



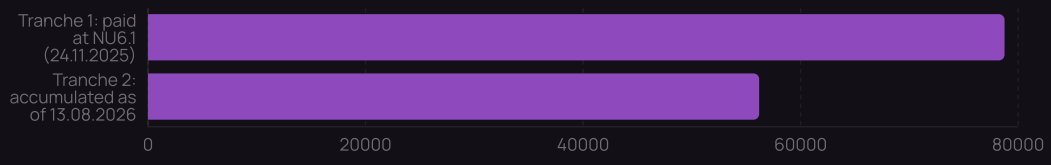
Distribution of daily emission (8Blocks calculation based on z.cash/network and zkp.baby data) — $k per day

Recipient	Share	ZEC per day	US dollars per day
Miners	80%	1,440	$713,938
Lockbox (deferred fund)	12%	216	$107,091
ZCG community grants	8%	144	$71,394
Total	100%	1,800	$892,422

The calculation: 1,152 blocks per day × 1.5625 ZEC × $495.79. On an annualised basis emission comes to 657,000 ZEC, or $325.7m — **3.89% of the current circulating supply**.

The lockbox deserves a separate examination, because it is often read as a mechanism that withdraws coins from circulation. It is not. A check with arithmetic:

- ZIP-1015 directed 12% of the block reward into the lockbox from block 2,726,400 to block 3,146,400 — that is 420,000 blocks;
- 420,000 × 1.5625 × 12% = **78,750 ZEC** — exactly the amount that ZIP-271 mandated to be paid out in a single tranche;
- the payout was made at the NU6.1 upgrade on 24 November 2025 to a 2-of-3 multisig address, with the keys held by the Zcash Foundation, Electric Coin Company and Shielded Labs;
- from NU6.1 to 13 August 2026, 56,187.56 ZEC has accumulated, which matches the calculation across 299,666 blocks.



The lockbox: accumulation and payout of the first tranche (8Blocks calculation based on ZIP-1015, ZIP-271 and the lockbox balance) — ZEC

> Important
>
> the lockbox is a deferred-payout mechanism, not a lock-up. The first tranche was paid out in full in the twelfth month of accumulation. The 12% of emission cannot be counted as withdrawn from circulation: it is deferred supply that will reach the market at the decision of three organisations. The procedure for handling the second tranche has not been approved as of the time of writing — ZIP-1016, which describes a coinholder vote with a quorum of 420,000 ZEC, has the status of a proposal.

3.2 Conclusions on coin distribution

POSITIVE FACTORS AND RISK FACTORS

- ✓ The maximum supply is hard-capped at 21m ZEC at the protocol level; 80.3% has already been issued, and the issuance rate halves every four years.
- ✓ Vesting, cliffs and unlocks do not exist — there is no calendar supply overhang in any form.

- ✓ There is no venture overhang and no coins bought at a discount: the Founders' Reward ended six years ago.
- ✓ The emission schedule can be verified block by block and matches the actual balances to the zatoshi.
- - 20% of all new emission goes to organisations rather than to network participants: the holder funds development by diluting their own share.
- - The procedure for handling the lockbox is decided after the fact — when accumulation began no payout mechanism had been established, and the coinholder voting model has still not been activated.
- - The funding rules have changed four times over the project's history, and ZIP-234 proposes replacing the halving scheme with a smooth curve entirely.
- - The actual concentration of holders is structurally unmeasurable: shielding makes address classification impossible by the very design of the network.

The ZEC supply structure is one of the cleanest on the market: no premine in circulation, no investor overhang, no calendar unlocks, and a hard cap. The only contentious element is the 20% of emission that goes to organisations, together with the uncertainty over how the lockbox will be handled. This is not a hidden risk but a deliberate trade-off: a project without revenue funds its development in the only way available to it.

4. Staking and farming

4.1 Analysis of the instruments

There is no staking in the Zcash network. Consensus is built on Proof-of-Work, and new coins go to miners for computational work rather than to holders for locking up funds. The project offers no liquid staking, no farming and no reward programmes for providing liquidity.

> Important
>
> the absence of staking means the holder has no protocol-level way to earn income from holding the coin and no reason to take it out of free circulation. Shielding funds is not a lock-up: coins can be moved out of a pool at any moment.

Under development is the **Zcash Trailing Finality Layer** (the Crosslink project) — a hybrid model that adds a proof-of-stake finality layer on top of the existing Proof-of-Work. According to public sources the indicative timeline is 2026–2027.

> Important
>
> if the Trailing Finality Layer launches with ZEC staking, the coin will for the first time have a supply-locking mechanism and a yield backed by the work of the network. At the time of writing this is a proposal under development, not a working mechanism, and it cannot be assessed as though it were live.

4.2 Analysis of the formulas

The emission formula is inherited from Bitcoin and is set in the protocol:

- Block reward after the November 2024 halving: **1.5625 ZEC**;
- Target block time: 75 seconds, that is **1,152 blocks per day**;
- Daily emission: 1,152 × 1.5625 = **1,800 ZEC**;
- Annual emission: 657,000 ZEC, or **3.89% of the current circulating supply**;
- Next halving: **23 November 2028**, after which the reward falls to 0.78125 ZEC per block.

The ZIP-234 proposal would replace the discrete halvings with a smooth logarithmic curve: a fraction of the remaining money reserve in every block (BLOCK_SUBSIDY_FRACTION = 0.0000004126), which over four years produces roughly the same result but without step changes. The proposal has draft status, and activation is planned together with Network Upgrade 7.

> Important
>
> ZIP-234 has a non-obvious consequence: a smooth curve allows ZEC withdrawn from circulation to be drawn back into future block rewards. That changes how the 21m cap should be read — it remains, but it becomes asymptotic.

Alongside ZIP-234, two further proposals from the same Network Sustainability Mechanism package are under consideration for Network Upgrade 7. **ZIP-233** introduces into the protocol the very ability to remove funds from circulation irreversibly. **ZIP-235** applies that ability to fees: 60% of every fee stops going to the miner and is destroyed. Both have draft status and are not live on mainnet. At today's fee volume the effect of ZIP-235 would be symbolic — well under 0.1% of annual emission — but it would be the first supply-absorption mechanism in the project's history, and its contribution would grow with the number of transactions.

4.3 Analysis of cash flows

Inflow to the market (emission):

- Miners: 1,440 ZEC per day (~$713,938) — sold to cover the cost of electricity and equipment;
- Lockbox: 216 ZEC per day (~$107,091) — deferred supply, released in tranches at the decision of the organisations;
- ZCG grants: 144 ZEC per day (~$71,394) — distributed to ecosystem teams.

Withdrawal from circulation:

- There are no withdrawal mechanisms: no burn, no buyback and no protocol-level lock-ups.

> Important
>
> the balance is one-sided: 657,000 ZEC a year enters the market and zero leaves it. Network fees, which in other networks serve as a source of burn, are minimal in volume here and go entirely to miners. The project funds its development out of the holder's pocket — a workable model for a monetary asset, but one that means the price has to rise by at least 3.89% a year simply for the holder to keep their share.

The volume of fees can be calculated exactly. The rate is set by ZIP-317: 5,000 zatoshi per logical action with a minimum of two actions, that is **0.0001 ZEC** for a typical transaction. Cumulatively the network has processed 3.29m shielded transactions — that is **329 ZEC** in fees, around $163k at the snapshot price. Against annual emission of 657,000 ZEC that is **0.05% of a single year**. For fees to reach even one per cent of annual emission the network would need 180,000 transactions a day, against a historical rate of roughly a thousand. Nor are fees removed from circulation: they enter the block's coinbase output and belong entirely to the miner, and the 80 / 12 / 8 split does not apply to them — it governs the block subsidy alone. No separate address or fund in which fees would accumulate exists in the protocol.

It is worth recording separately where the funding for development comes from. Zcash has no protocol revenue: transaction fees are negligible and the network has no paying customers. Electric Coin Company, the Zcash Foundation and the grant recipients are funded exclusively by their share of the block reward. This differs fundamentally from projects where development is paid for out of product revenue.

4.4 Conclusions

- There is no staking; the holder has no protocol yield; supply is not locked for any period.
- The sole source of new coins is the block reward, the cap is hard-set at 21m, and the rate halves every four years.
- 20% of emission funds the project's development at the expense of diluting holders — a direct trade-off, but an honestly disclosed one.
- The Trailing Finality Layer could change this picture, but for now it remains under development.

The section that for most projects describes the mechanics of holding a token describes monetary policy in the case of Zcash. That is a consistent position for an asset claiming the role of private money: cash pays no yield either. The risk lies elsewhere — a monetary asset without yield requires demand for its core function to grow faster than emission.

5. Coin utility

5.1 Use cases

- **A private transfer** — the main and, in essence, the only function: a shielded transaction hides the amount, the sender and the recipient. It is impossible without holding ZEC.
- **Transparent transfer and storage** — Bitcoin-level functionality.
- **Paying network fees** — every transaction requires ZEC.
- **Securing the network** — through mining, but that is a function of computing power, not of holding the coin.

> Important
>
> to the methodology's key test — can the product be used without holding the coin — the answer is unambiguous: it cannot. ZEC is not a layer on top of the product; it is the product itself. This is the highest category of coin necessity, and on this measure Zcash receives the maximum score.

The other side of the same coin: it has not a single additional function. It confers no governance rights — decisions are taken through the ZIP process by node operators, not by a holder vote, and the proposed ZIP-1016 coinholder voting model has not been activated. It pays no yield. There is nowhere to extend the utility without changing the nature of the asset.

5.2 Tools and services

- **Zashi** — the official Electric Coin Company wallet, supporting shielded addresses and swaps via Near Intents;
- **Gemini** — shielded ZEC withdrawals, the first such case among major exchanges (November 2025);
- **Coinbase Custody and BitGo** — institutional custody with support for shielded balances (end of 2025). This is the first time a regulated US custodian has officially supported shielding;
- **Grayscale Zcash Trust** — an investment trust with around $190m in assets;
- **Zcash Shielded Assets (ZSA)** — a proposal to issue third-party assets in shielded form, currently under development.

> Important
>
> connecting regulated custodians to shielded balances is the most significant development for the category. It removes the main practical objection to privacy assets: the impossibility of institutional custody within a legal perimeter.

5.3 Conclusions

- The coin is irreplaceable for the product's core function — the maximum score on the necessity scale.
- The utility is singular and does not expand: no governance, no yield, no use beyond the network.
- The ecosystem of services around the coin strengthened markedly over 2025–2026: institutional custody, shielded withdrawals on exchanges, an investment trust.

To the methodology's question "who will buy this coin, and why?" Zcash gives a more direct answer than most projects: the buyer is whoever needs financial privacy, and they buy because there is no way to obtain it without ZEC. The weakness of that answer is not in the mechanism itself but in the size of the market: it is set by demand for privacy, not by the scale of any business.

6. Coin circulation

6.1 How coins move

1. Inflow into circulation:

- The block reward is the only source: 1,800 ZEC per day, of which 1,440 goes to miners, 216 to the lockbox and 144 to grants;
- Lockbox tranches — deferred supply that reaches the market at the decision of the organisations (the first tranche of 78,750 ZEC was paid out in November 2025).

2. Withdrawal from circulation:

- There are no protocol-level withdrawal mechanisms: no burn, no buyback and no lock-ups are provided for.
- Shielding funds is not a withdrawal: the 4.37m ZEC in the pools can be moved by their owners at any moment.

> Important

the sealed Orchard pool is a special case. Since 28 July 2026 only withdrawal through the turnstile is possible from it: a rule at the pool boundary caps total withdrawals at the volume of verifiably deposited funds. This is not a lock-up of capital but a defence against withdrawing potentially counterfeit coins; 73% of the funds have already moved into Ironwood. The remaining 1.03m ZEC can be withdrawn with no time limit.

ZEC circulation works as it does in Bitcoin: miners sell part of what they mine to cover their costs, and the rest is redistributed by the market. The project has no treasury loop that accumulates and reuses coins — the lockbox acts as a development fund, not as a price-support mechanism.

6.2 Risks

- The complete absence of absorption mechanisms against emission of 657,000 ZEC a year: all new supply has to be bought up by organic demand.
- Development funded by dilution: if demand for privacy stagnates, 20% of emission becomes pure pressure on the price with no offsetting effect.
- Uncertainty over the lockbox: the procedure for handling the second tranche has not been approved, and the balance grows by 216 ZEC a day.
- The category's regulatory risk: delisting of privacy assets on individual venues reduces liquidity and availability.
- Cryptographic risk: flaws in shielding schemes are by their nature undetectable, and the market reacts to them with a one-third fall in a single day.

Important

the key balance to watch is the growth rate of shielded supply against the rate of emission. The shielded pool is growing faster than 3.89% a year, which means demand for the core function is outpacing dilution. A reversal of that ratio would be the first sign that the model has stopped working.

7. Critical remarks

- **Development is paid for by the holder, not by revenue.** Network fees are negligible and there are no paying customers, which is why 20% of every block reward goes to organisations. The model works, but it means the quality of development depends directly on the coin price, and the holder bears that cost through 3.89% annual dilution.
- **There is not a single absorption mechanism against emission.** Burns, buybacks, staking and collateral lock-ups do not exist. The only source of demand is the wish to hold private money. For a monetary asset that is acceptable, but it leaves the model without any built-in support during periods of falling demand.
- **The Orchard vulnerability went unnoticed for four years.** A flaw in the scheme that permitted undetectable counterfeiting had existed since 2022 and was found by a researcher, not by an audit. No evidence of exploitation was found and there were no losses, but the fact itself means that in a system where supply is unverifiable by design, integrity rests solely on the quality of the cryptography and on the turnstile mechanism.
- **The lockbox is not a sink.** Reading the 12% of emission as funds withdrawn from circulation is wrong: the first tranche was paid out in full to three organisations twelve months after accumulation began. The procedure for handling the second tranche has still not been approved.

- **The funding rules are unstable.** Over the project's history the model has changed four times, and ZIP-234 proposes replacing the halving scheme entirely, which would make the 21m cap asymptotic. For an asset whose value is built on the predictability of its monetary policy, the frequency of change is a risk in its own right.

That said, the project's response to the 2026 incident deserves separate recognition. Five days from disclosure to fix, sixty days to a full replacement of the pool, a turnstile mechanism that capped the possible damage at the volume of verifiably deposited funds, formal verification of the new scheme and zero user losses — this is the best possible outcome for a vulnerability of this class.

8. Final conclusion

Zcash solves the problem most tokens stumble over: the link between the product and the coin. Here it does not have to be built — it is embedded in the very nature of the asset. A shielded transaction is impossible without ZEC, the coin cannot be bypassed and there is nothing to replace it with. On the coin-necessity scale this is the highest category, and it is rarely seen.

What limits the score is the economics. The network has no revenue: fees are minimal and go to miners, there are no paying customers, and development is funded by twenty per cent of emission — that is, by diluting holders 3.89% a year. Not a single absorption mechanism stands against that flow: there is no burn, no buyback and no staking, and the lockbox, often mistaken for a sink, turned out to be a deferred payout — its first tranche of 78,750 ZEC was paid out in full to three organisations.

The supply structure, by contrast, is exceptionally clean. The cap is hard-set, 80.3% has been issued, vesting and unlocks do not exist and there is no venture overhang. The project has no insider allocations to justify — there simply are none. It is a rare combination: weak value-transfer economics alongside impeccable supply mechanics.

2026 was a stress test for the network. A vulnerability that had gone unnoticed in the main pool for four years could have ended in catastrophe for an asset whose value rests entirely on trust in cryptography. It did not: there were no losses, the fix took five days, the pool replacement sixty, and holders voluntarily moved 73% of the funds into the new pool within sixteen days. That last figure says more about the project than any statement could: the network has a community that acts.

The key question for Zcash is whether demand for privacy will grow faster than the network prints new coins. Today the shielded share of supply is growing faster than emission, and that is the only thing holding the model in balance. The arrival of the Trailing Finality Layer with staking, or of any supply-absorption mechanism, would change the picture fundamentally.

8.1 Recommendations for the project

1 Approve the procedure for handling the lockbox before the second tranche reaches the size of the first.

Today 216 ZEC a day accumulate with no approved payout mechanism, and the ZIP-1016 coinholder voting model remains a proposal. Uncertainty over 12% of emission is an avoidable risk that the project creates for itself.

2 Take the Trailing Finality Layer with ZEC staking through to launch.

It is the only mechanism under discussion capable of locking supply and at the same time giving the holder a yield backed by the work of the network. Today the coin has neither.

3 Create a source of protocol revenue that does not depend on emission.

Zcash Shielded Assets — the issuance of third-party assets in shielded form — could give the network paying customers. A fee on such issuance would be the first income in the project's history that is not dilution of holders.

4 Fix the monetary policy for the long term.

The funding rules have changed four times, and ZIP-234 changes the halving scheme entirely. For an asset that sells predictability, it is worth establishing a procedure that raises the threshold for changing monetary parameters above that of an ordinary ZIP.

5 Extend the formal verification applied in Ironwood to all active pools and publish a regular report on the state of those checks.

The 2026 incident showed that four years of ordinary auditing is not enough for schemes of this class.

6 Publish open reporting on how the lockbox funds and the ZCG grants are spent.

Holders fund development through dilution and should be able to see where their money goes.

8.2 Important notes for investors

1 The main metric to track is the shielded share of supply.

It shows whether demand for the network's core function is growing. Today it stands at 25.92%; sustained growth means demand is outpacing the 3.89% annual emission, and a decline means the opposite.

2 The holder is diluted by 3.89% a year and there is no compensating mechanism.

There is no way to preserve one's share: there is no staking and no yield. The price has to rise by at least that much simply for a position to hold its ground.

3 The lockbox is deferred supply, not funds withdrawn from circulation.

The second tranche grows by 216 ZEC a day and the procedure for paying it out has not been approved. The decision on it will be an event that affects supply.

4 For a privacy asset, cryptographic risk is the principal risk, not a secondary one.

The incident of May 2026 cost a third of the capitalisation in a single day even though there were no losses at all. A position should be assessed on the basis that this can happen again.

5 The second indicator is the status of the Trailing Finality Layer.

The launch of staking would change the coin's economics fundamentally; until official activation it cannot be treated as fact.

6 Regulatory risk is structural for the privacy-asset category and cannot be removed by anything the project does.

The closure of the SEC review in January 2026 is a positive precedent but not a guarantee for other jurisdictions.

$ZEC Rating under the 8Blocks methodology

Final rating: 66 / 100. Letter rating: BBB.

Block	Weight	Score (0–5)	Score (0–100)	Contribution
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
Base score	100%			63.15
Bonuses				+3.00
Total				66.15

Interpretation. Token Product Linkage of 2.78 falls into the Moderate Linkage category. Within the block the extremes diverge more widely than for any other project: coin necessity is scored 5.0 out of 5.0 (the maximum — the coin is irreplaceable), while value transfer and supply-absorption mechanisms score 1.5 and 1.2. Zcash does not have the problem of "the product grows without the coin"; it has the problem of "there is no mechanism converting growth into value".

The rating cap. With TPL in the 2.5–2.99 range a ceiling of 70 points applies. A base score of 63.15 plus bonuses gives 66.15 — the ceiling did not bind, but the headroom is under four points. Raising TPL above 3.0 would lift the ceiling to 80 and would be the single most effective change.

Bonuses of +3 have been applied: coming through the 2018 and 2022 downturns without halting the network or changing its commitments (+2), and the quality of the response to the 2026 incident — five days to the fix, sixty to the pool replacement, zero losses (+1). **No major-exploit penalty has been applied**: the methodology requires material financial losses, incomplete recovery and damage still relevant to the current version — none of these conditions is met.

Strengths: coin necessity (the maximum score), the cleanliness of the supply structure (no vesting, no unlocks and no venture overhang, under a hard cap), the absence of admin keys and of any ability to seize funds, and the liquidity of the market's 15th-largest asset.

What would have to change for the rating to rise. The largest effect would come from the appearance of any supply-absorption mechanism — staking via the Trailing Finality Layer, or the burning of part of the fees under ZIP-235: that would lift Supply Sinks and Coverage, and with them TPL above the 3.0 threshold. The second most significant factor is a source of protocol revenue unconnected to emission (ZSA), which would end development's dependence on dilution. The third is approval of the procedure for handling the lockbox.

Assessment confidence: 82 / 100 (High). The emission and lockbox calculations have been reconciled with actual balances to the zatoshi, and all key parameters are fixed in the public ZIP specifications. The main limitation is that holder concentration is structurally unmeasurable because of shielding. Scenario range: conservative 61, base case 66, optimistic 69 — a spread of 8 points, with the BBB letter category stable in every scenario.

Data snapshot date: 13 August 2026.

Appendix. Data sources

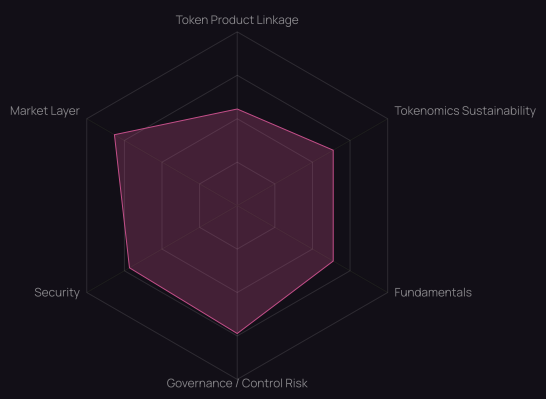
Data	Source	Date
Product description, organisations, ecosystem	z.cash (official website)	13.08.2026
Block reward distribution, halving, circulation	z.cash/network (official)	13.08.2026
Lockbox and grant rules	ZIP-1015, ZIP-271, ZIP-1016 (zips.z.cash)	13.08.2026
Smooth emission scheme	ZIP-234 (draft, zips.z.cash)	13.08.2026
NU6.1 activation and block height	z.cash/upgrade/nu6-1	24.11.2025
Wallet updates, custodians, roadmap	electriccoin.co/blog	2025–2026
Price, MC, FDV, supply, ATH/ATL, volume	CoinGecko	13.08.2026
Price series (monthly and weekly)	coins.llama.fi (CoinGecko aggregator)	13.08.2026
Shielded pool by pool, lockbox, block height	zkp.baby dashboard	13.08.2026
Orchard vulnerability, Ironwood upgrade	The Block, CoinDesk	28–29.07.2026
Market reaction to the vulnerability disclosure	KuCoin Research	06.2026
Institutional custody, Grayscale trust, SEC	CryptoSlate	12.08.2026
Cumulative number of shielded transactions	Coinpedia	12.08.2026
Fee rate, mechanisms for removal from circulation	ZIP-317, ZIP-233, ZIP-235 (zips.z.cash)	02.09.2026

Discrepancies between sources. The shielded share of supply: the zkp.baby dashboard gives 25.92% (4,374,320 ZEC), while some reviews citing CoinGecko quote “more than 30%” — the audit uses the dashboard as the source that breaks the figure down pool by pool. FDV: CoinGecko calculates the metric from a total supply of 16.874m ($8.384bn) rather than from the maximum of 21m (which would give around $10.4bn); the audit quotes the source’s figure. The volume of Orchard at the moment of sealing: The Block gives 3.6m ZEC and CoinDesk 3.66m ZEC; the discrepancy is within rounding and does not affect the conclusions. Under the 8Blocks sourcing policy the project’s own documentation is primary: the emission and distribution parameters are taken from the ZIP specifications and reconciled by calculation against actual balances.

Limitations of the audit. First: the price charts are built on a downsampled series (a monthly step for the full history, weekly for 2026), so exact intraday extremes do not appear in them — the ATH and ATL values are quoted separately in the text from CoinGecko. Second: the historical dynamics of the shielded pool could not be obtained from public APIs, so the pool is shown by its current composition and by a “before and after” comparison of the Orchard sealing. Third: address classification and holder-concentration analysis were not carried out and, in the case of Zcash, are impossible by the design of the network. Fourth: the figures in section 4.2 relating to ZIP-233, ZIP-234 and ZIP-235 reflect draft status and are subject to revision when Network Upgrade 7 activates.

Final rating

BLOCK PROFILE



BREAKDOWN (0–100)

Token Product Linkage	**55.6**
Tokenomics Sustainability	**63.8**
Fundamentals	**63.8**
Governance / Control Risk	**73.6**
Security	**71.6**
Market Layer	**81.6**

SUMMARY

Zcash has answered “why the coin is needed”: a shielded transaction is impossible without ZEC, the cap is 21m, and there is no vesting or unlocks. But fees are negligible and go to miners, while development is paid for by diluting holders 3.89% a year with no absorption mechanism whatsoever: rating BBB, 66/100.

This audit is not investment advice. Use it as part of your own analysis.

FINAL RATING

66 /100

RATING BBB

Lead expert

Toni Efren in

Co-founder, 8Blocks

Block	Weight	Score (0–5)	Score (0–100)	Contribution
Token Product Linkage	40%	2.78	55.6	**22.2**
Tokenomics Sustainability	20%	3.19	63.8	**12.8**
Fundamentals	15%	3.19	63.8	**9.6**
Governance / Control Risk	10%	3.68	73.6	**7.4**
Security	10%	3.58	71.6	**7.2**
Market Layer	5%	4.08	81.6	**4.1**
Total	**100%**	**3.2**	**63**	**63.3**