Keystead Whitepaper

Your keys, your ground. Draft, October 2026
SC1E Network: the first Self-Custody, One-Ecosystem Layer-1 currency.

Preface: why I'm building Keystead

Bitcoin promised money that belongs to the people who hold it. Somewhere along the way, most of that promise was handed back to exchanges, apps and companies. I'm building Keystead to take it back, and to make that easy enough for anyone.

- **Money is meant to be spent.** A currency should pay for coffee, rent and a friend's half of the bill, not just sit on a chart. Keystead is built for everyday use, with a wallet, payment requests and a point-of-sale app for businesses.
- **You hold full control.** Your keys live on your device. No company can freeze, lose or lend out your coins, and you can take them to any other wallet whenever you like.
- **Fewer logins and websites.** One app holds your coins, trades them, stakes them, mines and lets you chat. No more six accounts, seven tabs and a password for each.
- **Simple for beginners, powerful for experts.** Keystead is designed for someone with limited technical knowledge, but it still gives a technical user every tool they could want or need in Advanced mode. Most other cryptocurrencies copy the same hard-to-use, confusing setup: separate wallet software, outside mining programs, extra logins, and more points of failure at every step. Keystead puts it all in one app that works out of the box.
- **Your data stays yours.** No account to sign up for, no ID to upload just to hold your own money, and no company collecting your history to sell, leak or lose in a breach.
- **Fair from the first block.** No premine, no presale, nothing set aside for insiders. Everyone starts from the same place, me included.

Keystead won't promise anyone riches. It's meant to be useful: money you control, in an app you can trust, built in the open so anyone can check it.

About the developer

I found Bitcoin in early 2009, about a month after Satoshi Nakamoto released it to the public. Back then an ordinary home computer could mine it, and I mined hundreds of bitcoin. When that hard drive failed, I threw it in the garbage, and the coins went with it.

Losing them never changed what I believed. Bitcoin's original vision was money that governments and corporations can't devalue or dilute, money that belongs to the person who holds it. I created Keystead to get back to that principle.

That lost drive is also why Keystead makes every new user back up and confirm their recovery phrase before they can receive a single coin. I know first-hand what one failed drive can cost.

Abstract

Keystead (KSTD) is a new Layer-1 cryptocurrency with no premine, a 21,000,000 coin cap, and a hybrid security model: proof-of-work blocks that proof-of-stake holders must approve. Mining runs on four algorithms, three of them merge-mined with Bitcoin, Litecoin/Dogecoin and Monero, so existing miners can secure Keystead at no extra energy cost.

Keystead calls this an **SC1E network: Self-Custody, One Ecosystem.** *Self-custody* means every user holds their own keys: nobody can freeze, lend out or lose their coins. *One ecosystem* means a single app and a single chain cover what usually takes half a dozen accounts and services: holding, sending, staking, mining, trading and private messaging. Other projects offer self-custody, or an all-in-one app, but usually not both. Keystead is built to be both from its first block, on its own Layer-1 chain.

The first product is a desktop wallet that replaces the usual stack of apps: self-custody for KSTD, BTC, ETH, XMR, LTC, DOGE and USDC; staking; a built-in miner; an exchange with liquidity pools; encrypted chat; and a block explorer. It is designed so someone who has never used crypto can use it safely, with Advanced mode for everyone else.

This paper is a draft. Values marked *proposed* are not final until the genesis parameters are locked.

The problem

Bitcoin set out to remove the need to trust a third party with your money. In practice, most people now hand their coins back to one, because self-custody is hard and the tools are scattered.

- **Custody risk.** Coins held on an exchange can be frozen, lost to a hack, or lost when the exchange fails. The user holds a balance on a screen, not the coins.
- **Too many apps.** A typical holder juggles a separate wallet per coin, an exchange account, a staking service, a mining dashboard, a block explorer and a chat app. Each one is another password, another fee and another place to make a mistake.
- **Unfair launches.** Many new coins start with a premine or presale that hands insiders a large share before the public can take part. The result is often a fast rise and an engineered collapse.

Keystead's answer is a coin with a provably fair start, and one app that makes self-custody as easy as an exchange account.

Design principles

1. **Your keys, your ground.** Keys are created and kept on the user's own device. Nothing leaves the wallet unless the user chooses to trade.
2. **No premine, no presale.** The genesis block pays nothing to anyone. Every coin is mined or earned through staking.
3. **Security from two independent sources.** An attacker needs a majority of hashrate and a majority of stake at the same time.
4. **Use existing hardware.** Merged mining lets Bitcoin, Litecoin, Dogecoin and Monero miners secure Keystead without spending more energy. Home CPUs and GPUs compete only against their own hardware class.
5. **Plain language first.** Simple mode explains every action in one sentence and puts a clear confirmation before anything irreversible.
6. **Honest about trade-offs.** Where something is custodial or carries risk, the app says so in plain words.
7. **Never roll our own crypto.** Keystead uses audited, widely used cryptographic libraries and published standards.

Consensus overview

Every Keystead block is mined with proof-of-work, then approved or rejected by a small committee of stakers. On top of that, every staker votes on a checkpoint every 20 blocks, and once two-thirds of the stake agree, the chain becomes final and can never be rewritten past that point.

- **Block time:** 60 seconds target.
- **Proof-of-work:** four algorithms, each targeting 25% of blocks with its own difficulty (next section).
- **Proof-of-stake voting:** stakers approve each mined block in the next block, in the style of Decred.
- **Finality:** every 20-block epoch, every active staker signs one vote. Two-thirds of the stake justifies a checkpoint, and the next justified checkpoint makes it final. Nodes never reorganize past a final checkpoint.
- **Determinism:** all consensus math uses integers or fixed-point values. No floating point, no system time beyond block timestamp rules, no randomness.

The result is that a large merge-mining pool cannot rewrite history on its own. It would also need most of the stake, and even then only back to the last checkpoint.

Mining: four lanes

Keystead splits mining into four lanes so that each kind of hardware competes only with its own kind, and no single mining industry can dominate the chain.

Lane	Hardware	How it is mined	Target share
SHA-256	Bitcoin ASICs	Merge-mined with Bitcoin (AuxPoW)	25%
Scrypt	Litecoin/Dogecoin ASICs	Merge-mined with Litecoin and Dogecoin (AuxPoW)	25%
RandomX	CPUs	Built-in miner, pools, or merge-mined with Monero	25%
KawPow	GPUs	Built-in miner or pools	25%

- **Merged mining** lets a miner work on Bitcoin, Litecoin, Dogecoin or Monero and Keystead at the same time with the same hashes. Keystead uses the Namecoin/Dogecoin-compatible AuxPoW format, with a fixed chain-ID slot so one proof can never back more than one Keystead block. Monero merged mining uses a seed-validity rule computed from the Keystead chain alone.
- **Per-lane difficulty** retargets every block (LWMA), so each lane settles near 25% of blocks.
- **Anti-domination cap:** no lane may produce more than 40% of the last 100 blocks. The cap switches on only once at least three lanes are active, so the chain cannot stall in its early days.
- **Mining is always opt-in.** The wallet never starts mining on its own and always shows a clear on/off state. The official mining software takes no developer fee.
- **Pool fee:** the official pool takes 1% of each block it finds, including the Bitcoin, Litecoin, Dogecoin and Monero rewards it earns through merged mining, split 0.5% to the dev fund and 0.5% to the LP fund. Solo mining and other pools pay no pool fee to Keystead.

Staker voting and finality

A mined block only stands if stakers approve it in the next block, and every staker helps make the chain final about every 20 minutes.

Per-block votes

1. For each block, a committee of 5 stakes is drawn from the previous block's hash, weighted by stake. The draw is public, so anyone can recompute it. If committee members are slow, backup stakes become eligible one at a time, one more for every 30 seconds without a block.

2. Each drawn staker signs *approve* or *reject*. The next block must carry at least 3 of these votes and carries at most 5. Only committee votes are paid; backups earn nothing.
3. If 3 or more committee members reject, the block's transactions and its reward are cancelled, and the transactions return to the mempool. The dev and LP outputs still apply. Backup votes can never cancel a block.
4. If stakers stay silent for an hour, blocks may carry fewer than 3 votes so the chain never halts, but those blocks add no weight when nodes choose between competing chains.

Stakers reject blocks that are invalid, withheld, or built on a minority fork.

Finality

- Keystead uses Casper FFG, the finality design Ethereum uses, on top of proof-of-work.
- Every 20 blocks (an epoch, about 20 minutes), every active staker signs one vote with a BLS key. Votes are combined into compact aggregate signatures inside blocks, so finality doesn't bloat the chain.
- When stakers holding two-thirds of the stake vote for a checkpoint, it is *justified*. When the next checkpoint is justified on top of it, it becomes *final*. In normal conditions a payment is final within about an hour.
- No node ever reorganizes past its final checkpoint. KSTD deposits to the Keystead market are credited only once they are final.
- Finality switches on by itself once at least 16 stakers and 100,000 KSTD of stake have been active for 8 epochs in a row. Before that, blocks are protected by proof-of-work and the per-block votes.
- If many stakers go offline, an inactivity rule gradually lowers the absent stakers' voting weight (never their coins) until the rest can finalize again.
- A wallet that has been offline for more than about 10 days warns its user to make sure it is following the real network before it trusts old checkpoints.

The one penalty: double-signing

Coins are never taken for being offline or missing votes; an absent staker simply earns less. The only thing that destroys coins is signing two conflicting finality votes, which is what an attacker would do to try to finalize two different histories. If a staker's key does that, all of that key's stake is burned, including coins that are still unstaking. Burned coins are gone for good and never reissued, and nobody is paid for reporting it.

The wallet protects honest users from this. It records every vote it signs and refuses to sign anything that conflicts. After every start or restore, it watches the network for two epochs to make sure the same key isn't already signing somewhere else. **Run only one staking wallet per recovery phrase.**

Staking start

Per-block voting switches on at block 20,160, about two weeks after genesis. Before it, blocks need no votes. This gives miners time to earn coins and stake them, so no premine is needed to start staking. A stake counts once it holds at least 10 KSTD and is about a day old (1,440 blocks). Unstaking takes about a week.

Monetary policy

KSTD has a hard cap of 21,000,000 coins, enforced in consensus, with half of all coins issued in the first four years and the rate halving every four years after that.

Parameter	Value
Maximum supply	21,000,000 KSTD
Decimals	8 (1 KSTD = 100,000,000 base units)
Block time	60 seconds (525,600 blocks a year)
Initial block subsidy	about 4.994 KSTD, set so total issuance never exceeds the cap
Halving interval	every 2,102,400 blocks (4 years)
Subsidy split	70% proof-of-work reward, 30% staking budget
Premine	none

Period	Subsidy per block	Issued by end of period	Share of cap
Years 0–4	~4.994 KSTD	10,500,000	50%
Years 4–8	~2.497 KSTD	15,750,000	75%
Years 8–12	~1.249 KSTD	18,375,000	87.5%
Years 12–16	~0.624 KSTD	19,687,500	93.75%

The subsidy keeps halving until it rounds to zero, roughly 116 years after launch. After that, miners and stakers earn transaction fees only.

Staking yield

The staking rate adjusts itself from on-chain data only, with no price oracle. It is recomputed every epoch of 1,440 blocks (about a day).

- `raw rate = staking budget per year ÷ eligible staked supply`, clamped between **1% and 35% a year**.
- Few stakers means a high rate; many stakers means a low one. The rate balances itself.

- If the raw rate is above 35%, stakers receive 35% and the rest goes to an unissued **Staking Reserve**, which still counts against the 21M cap.
- If it falls below 1%, the reserve tops it up to 1% while the reserve lasts.
- 35% is the most a staked coin can earn, not the inflation rate of the whole supply.
- Eligible stake needs at least 10 KSTD and must be at least 1,440 blocks (about a day) old, which discourages churn and splitting stake into many small pieces.

Fees, dev fund and LP fund

Every reward Keystead pays sends 1% to two public funds, 0.5% to a development fund and 0.5% to a liquidity fund, and the rest goes to whoever did the work. Market swaps fund them differently: a separate 0.10% protocol fee on top of the 0.30% that goes to pool depositors.

Source	To the miner, staker or depositor	Dev fund	LP fund	Enforced by
Block reward	99%	0.5%	0.5%	Consensus
Transaction fees	99%	0.5%	0.5%	Consensus
Staking rewards (solo and delegated)	99%	0.5%	0.5%	Consensus
Official mining pool	99%	0.5%	0.5%	Pool software
Market swaps (0.40% of the trade in total)	0.30% of the trade	0.05% of the trade	0.05% of the trade	Market software

- **Enforced on-chain.** A block whose coinbase does not pay the dev and LP outputs exactly is invalid. Staking cuts are added to those same two outputs, so every block still has one dev output and one LP output.
- **Multisig, not single keys.** Both funds are held by multisig scripts fixed in consensus. Signers and thresholds will be published before launch.
- **Fully visible.** Every payment into and out of both funds appears on the explorer's network page, with a public note for each outgoing payment.
- **The LP fund** deposits into the Keystead market's KSTD pools as protocol-owned liquidity, in small scheduled amounts. Its share of non-KSTD swap fees (BTC, DOGE, LTC and others) is paired with KSTD and added to those pools. Funds held on other chains sit at the fund's own published addresses and are included in the proof of reserves.
- **The dev fund** pays for development, audits, infrastructure and legal work. It never touches pool liquidity.

- **Scale:** 0.5% is small. In year one each fund receives about 13,000 KSTD from block rewards, so early development is funded by the founder, not by users.

Service nodes and delegation

Service nodes are always-online staking nodes that vote for people who cannot stay online, and run network services for light wallets and chat. Delegators lend them voting rights only. Their coins never leave their own wallets.

Rule	Value
Minimum self-stake	0.05% of all KSTD minted so far, never below 100 KSTD or above 10,000 KSTD, recomputed each epoch, with a 2-epoch grace period to top up when it rises
Maximum commission	10% of delegators' rewards, enforced in consensus
Commission changes	take effect after a delay, so delegators can leave first
Concentration cap	no node may hold more than max(5%, 200% ÷ number of nodes) of eligible stake
Delegation	voting rights only, signed with the stake's own vote key; revocable any time, and the change reaches votes about a day after it is mined
Rewards	paid per vote, directly in the block: the delegator receives their share and the node its commission, with at most 5 votes paid per block
Penalties	a node whose votes stop arriving earns no commission, and after 3 such epochs its delegations return to their owners; a node can never get a delegator's coins burned, because it never signs finality for them

- **Why not masternodes.** A separate collateral class would favour large holders, add a third reward split under a fixed cap, and duplicate the staking system Keystead already has.
- **Services.** Nodes can offer vote delegation, compact block filters for light wallets, and relays for chat and calls. Each is an advertised flag.
- **Founder nodes.** At launch the founder may run a few service nodes so blocks keep getting votes while the network is small. Each will be publicly listed and labelled, follows the same rules as everyone else, and is never ranked above independent nodes in the wallet. The founder's share of stake will be published regularly.

The Keystead wallet

The wallet is one app that does what most holders use six or seven for, with every key kept on the user's own device.

Feature	What it does
Self-custody	Holds KSTD, BTC, ETH, XMR, LTC, DOGE and USDC from one 12-word recovery phrase, using each chain's standard derivation so coins can be restored in other wallets
Send and receive	Coin-aware addresses, QR codes, an address book, payment links, and a review screen that states exactly what will happen
Staking	Named stakes, delegation to service nodes, and a live view of the current rate
Mining	A built-in CPU and GPU miner with one Start/Stop button, plus a local proxy for the user's own Scrypt and SHA-256 ASICs
Market	Swaps between all supported coins, limit and stop orders, and liquidity pools
Chat	End-to-end encrypted direct messages, groups, official signed channels, and payment requests
Explorer	A built-in block explorer that verifies what it shows where it can
Taxes	One export of income, trades and transfers with values at the time

Built for people new to crypto

- **Simple mode by default:** every core task in three steps or fewer, plain words, and the fiat value next to every amount. Advanced mode adds fee control, coin control, charts and the RPC console. Both modes allow exactly the same actions.
- **Backup before money:** a new wallet cannot receive funds until the user has confirmed their recovery phrase.
- **Spending safety:** a daily sending limit, and a 24-hour wait on large sends to new addresses that the user can cancel. Loosening either setting takes 24 hours to apply.
- **Family recovery:** an optional backup split among trusted contacts, any two of three of whom can help restore it.
- **Scam warnings** for money requests from strangers and for look-alike addresses.

The desktop app comes first. A phone app and a lightweight point-of-sale app for businesses (KeyPay) are in design.

Market and liquidity pools

The Keystead market is a custodial automated market maker: users trade against shared pools, and people who deposit into those pools earn the trading fees. It is the one part of Keystead where coins leave the user's own keys, and the app says so wherever it matters.

How it works

- Every pair of supported coins has its own pool, 21 pools for 7 coins. Prices follow the constant-product rule ($x \times y = k$).
- A router compares the direct pool with two-step routes and picks the best result. The quote always shows the route, fee and price impact.
- Each swap pays 0.40% in total: 0.30% to that pool's depositors, plus a 0.10% protocol fee split 0.05% to the dev fund and 0.05% to the LP fund. The protocol fee can never exceed 0.15%, and any change is announced in advance. Depositors who trade get a discount on the 0.30% part only.
- Limit and stop orders wait on the ledger and fill against the pool when its price reaches them.
- Trades settle instantly on the market's ledger. Real coins move on-chain only for deposits and withdrawals.

For depositors

- Fees build up inside the pool, so shares grow without anything to claim.
- Committing shares for 30, 90 or 180 days raises their share of fees to 1.25×, 1.5× or 2×. Leaving early is always allowed and only drops the boost.
- New shares start earning after 24 hours, which stops people from jumping in just before a large trade.
- The app tracks impermanent loss: how a pool position compares with simply holding the same coins.
- No extra KSTD rewards are paid on deposits. That feature is switched off until a legal review.

Safeguards

- Withdrawals are always allowed. They are paid in batches at unpredictable times from a small hot wallet, while most coins stay in offline multisig cold storage.
- KSTD deposits are credited only after a finality checkpoint covers them.
- A circuit breaker pauses swaps on any pool whose price strays too far from major exchanges.
- **Proof of reserves and liabilities:** pool addresses on every chain are public, and a Merkle sum tree of all balances is posted on the Keystead chain so each user's wallet can check its own balance is included.

- No margin, leverage, futures or lending, ever.

Keystead never claims the pools support the KSTD price. Deposits belong to the depositors.

Why spot only

Every trade on the Keystead market is paid for with coins the trader actually holds. There is no borrowing, no margin, no futures or perpetual contracts, and no lending feature, and there won't be. The market's ledger can never go negative, and an order larger than the trader's balance is refused.

Leverage didn't invent crypto crashes: Bitcoin fell more than 90% in 2011, long before leveraged trading was common. What leverage changed is how crashes happen. A dip forces leveraged positions to be sold automatically, which pushes the price lower, which forces more selling. A normal decline becomes a cascade measured in minutes, and traders can trigger it on purpose by hunting other people's liquidation levels. On October 10, 2025, one such cascade wiped out roughly $19 billion of leveraged positions in about a day.

Keystead is built for money people own and spend, not for betting with borrowed money. So:

- **No leverage on Keystead's own market,** including Meme Markets and any future prediction markets.
- **No outside price feed sets the KSTD pools' price.** It moves only when someone trades in them, so a sudden liquidation crash on another exchange doesn't reach Keystead until someone actually moves coins.
- **KSTD deposits wait for finality,** and the circuit breaker pauses a pool on sudden moves. A brief crash elsewhere is often over before it can carry across.
- **No official wrapped KSTD and no derivatives partnerships.**

Keystead can't stop other exchanges from offering KSTD futures; nobody can control what others build on an open network. Spot only also doesn't mean the price only goes up. KSTD will still have cycles. It means Keystead's own market won't amplify them.

Messaging and privacy

Keystead chat is end-to-end encrypted, built on an established protocol rather than a custom design, and kept separate from the user's money.

- **Separate identity.** A user's chat identity comes from its own key, not from a wallet key, so a chat name cannot be linked to funds.
- **Payments in chat.** Users can send money or a payment request in a conversation. Paying always goes through the normal review screen and safety rules; nothing is ever paid automatically.

- **Signed messages.** A payment can carry a private note sent through encrypted chat, and users can sign or verify a message with an address using each chain's own standard.
- **Official channels** from the team are signed and verified, and the team will never ask for a recovery phrase.
- **Light-wallet privacy.** Light wallets check their own balances with compact block filters fetched from several service nodes, so no single server learns which addresses a user cares about.
- **Optional Tor** routing, and the option to run a full node.

Planned: friends lists, community rooms and voice calls. Live chat and calls will be peer-to-peer and free. Messages for someone who is offline will be held by service nodes, encrypted, and paid for with small prepaid stamps that cannot be traced back to the buyer. Messages between friends stay free up to a daily allowance.

Security model

Keystead is built so that no single failure, whether a mining pool, a server, a stolen laptop or a rushed user, can quietly cost people their money.

Threat	Defence
A large merge-mining pool tries to rewrite history	Needs a majority of stake as well as hashrate, and cannot go behind a finality checkpoint
One mining lane takes over	Per-lane difficulty, and a 40% cap per lane over the last 100 blocks
Stakers grind their way onto committees	A public, stake-weighted draw from the previous block's hash. A miner can only change it by throwing away blocks it found, which costs real hashrate
Double-spend against the market	KSTD deposits credited only after finality
Market hot wallet is hacked	Small hot float; most coins in offline multisig; no code path can use a cold key
Ledger and coins drift apart	Reconciliation after every withdrawal batch; withdrawals halt on any mismatch
Stolen or infected computer	Keys encrypted at rest with Argon2; signing happens in Rust and keys never reach the interface; daily limit and 24-hour wait
Scam calls and fake support	Plain warnings, signed official channels, and no feature that ever asks for a recovery phrase
Malicious network data	All peer-to-peer input treated as hostile, with size limits and fuzz-tested parsers
Fake light-wallet data	Headers, Merkle proofs and filters verified; anything unverifiable is labelled as such

Engineering rules

- Audited cryptography only: secp256k1, ed25519, ChaCha20-Poly1305, Argon2, BIP39/BIP32 and the established Monero and messaging libraries.
- Consensus code uses integer math only, ships with test vectors and property tests, and is reviewed separately from the person who wrote it.
- Releases are code-signed and reproducible, so anyone can check that a binary matches the published source.
- External security audits before mainnet. A bug bounty is planned.

Fair launch

Nobody, including the founder, starts with any KSTD. Every coin is mined or earned in public, and the launch is set up so anyone can check that.

- **No premine, no presale, no private sale, no airdrop to insiders.** The genesis block pays nothing, and that rule is part of consensus.
- **Published before launch:** the genesis timestamp, reproducible builds and signed binaries, so anyone can rebuild the software and verify there is no hidden allocation.
- **Founder holdings disclosed.** The founder's mining equipment, payout addresses, service nodes, and any plan to sell will be published before launch. The founder's share of stake will be reported regularly.
- **Mining first, trading later.** For the first period after genesis there is only mining. The market opens only after staking and finality checkpoints are running.
- **Planned opening deposit window:** before trading opens, miners deposit KSTD and others deposit other coins into the opening pools. When the window closes, the opening price is simply the ratio of the totals, so no single person sets it. Running totals are shown live, and the final 24 hours are frozen so the price cannot be swung at the last moment.
- **No price talk.** Keystead's official channels discuss the software and the network, never the price, and never promise returns.

Governance and open questions

Consensus rules change only through a published proposal, open review, and a software release that node operators choose to run. No one can change the rules from a server.

- **Proposals** are written up in public with their reasoning and test results before any release.
- **Community input** comes through the in-app Suggestions channel, where everyone can vote on ideas, and a separate channel for requesting new coins.
- **Fund spending** from the dev and LP multisigs is recorded publicly, with a note for every payment.

Still open before genesis

- Signers and threshold for the dev fund and LP fund multisigs
- Minimum stake and exact minimum stake age
- Final staking start height
- Which coins the market supports first, and in what order
- Signers for the market's cold-storage multisig
- Whether Keystead adds an on-chain data output for public payment notes and time-locked scripts for inheritance plans

Roadmap

Everything is built and tested on a test network first, and mainnet launches only after external audits and a legal review of the market.

Three stages and one gate: build and test everything on a test network; pass external audits and a legal review of the market; then launch mainnet and add the rest of the ecosystem.

No dates are promised. Each stage starts when the one before it is finished and tested.

Risks and disclaimers

KSTD is new, experimental software. Its value can go to zero, and nothing in this paper is a promise of any return.

- **Price risk.** KSTD has no guaranteed value. Early prices will swing sharply because pools start small. Only use what you can afford to lose.
- **Software risk.** Despite testing and audits, bugs can exist in consensus, wallet or market code.
- **Early-network risk.** Before staking and checkpoints are running, the chain is secured by mining alone and recent blocks can be reorganized.
- **Custody risk in the market.** Coins deposited to the market are held by Keystead until withdrawn. Proof of reserves reduces this risk but does not remove it.
- **Pool risk.** Depositors can end up with less value than if they had simply held their coins (impermanent loss).
- **Third-party coins.** Bitcoin, Ethereum, Monero, Litecoin, Dogecoin and USD Coin follow their own networks' rules. USD Coin's issuer can freeze addresses.
- **Regulatory risk.** Laws on digital assets, custody and money transmission differ by country and are changing. Some features may be limited or unavailable in some places, and the market is subject to legal review before launch.

- **Key risk.** In self-custody, anyone with the recovery phrase controls the coins, and a lost phrase cannot be recovered by Keystead.

This document describes software under development. It is not an offer to sell, a solicitation to buy, or financial, legal or tax advice. Details will change before launch.