



Could Redbelly connect to Quant Overledger?

A feasibility report on interoperability between Redbelly Network and Quant's Overledger.



Feasibility research only. Redbelly and Quant have no announced partnership or talks [S1](#), and nothing in this report suggests otherwise. Redbelly has not published an official position on bridging [S1](#), so any question that no public source answers is marked Unknown.

38 SOURCES 96 QUOTED FACTS WEB VERSION OVERLEDGER.TEST-HUB.XYZ

00 SHORT ANSWER

Key findings

01

● ANALYSIS

Could Overledger's Gateway reach Redbelly today, for reading data and sending signed transactions?

Possibly

Possibly, but unconfirmed. Redbelly is EVM compatible and its RPC fits Overledger's self-serve tests, but Overledger describes self-serve as for public permissionless networks, and writing to Redbelly needs a credential. Nobody has shown it working. [S2](#) [S3](#) [S4](#) [S5](#)

02

● ANALYSIS

Can Redbelly join the Fusion Rollup, Overledger's shared layer for deposits, unified token balances and cross-chain messages?

Not yet

Not possible yet, as far as public sources show. Redbelly is not among the networks documented at testnet launch, and the docs describe no self-serve way to add one. [S6](#) [S7](#)

03

● ANALYSIS

Would Receptor credentials and Tokeniser rules travel with an asset to another chain?

No

No, not by themselves. Redbelly's access credential and Proof by Query checks run on Redbelly, and Tokeniser enforces its rules at the point of transfer. A copy on another chain follows only that chain's own rules. [S5](#) [S8](#) [S9](#)

04

● CONFIRMED

Is there any agreement between Redbelly and Quant?

None

None has been announced. [S1](#)

HOW TO READ THE LABELS

● CONFIRMED

Stated in a public source. The source is linked and quoted in the source list.

● TESTED

We ran the call ourselves on 15 October 2026. The full log is in evidence/tests.

● ANALYSIS

Our reasoning from the confirmed facts it cites. Not a statement by Redbelly, Tokeniser or Quant.

● UNKNOWN

Not answered by any public source we found. Treat as open.

01 CONTEXT

Why this question comes up now

● CONFIRMED

On 24 September 2026 The Clearing House said it selected Quant to power its On-Chain Money Initiative, a payments network for clearing and settling tokenised deposits between financial institutions [S10](#). Quant's technology is to provide the network's interoperability, orchestration and transaction management layer [S10](#), with connectivity to existing payment systems such as RTP and CHIPS [S10](#). Quant's own release says The Clearing House will use Quant's technology to bring on-chain capabilities to its tokenised deposit network [S11](#).

● CONFIRMED

The network is expected to be available to participating institutions in the first half of 2027, and details on participation and use cases are still to be announced [S10](#).

● UNKNOWN

Neither announcement names any blockchain the network will use or connect to, and neither mentions Redbelly. No public source we found says whether it will connect to Redbelly or to any other specific chain [S10](#) .

— 02 OVERLEDGER

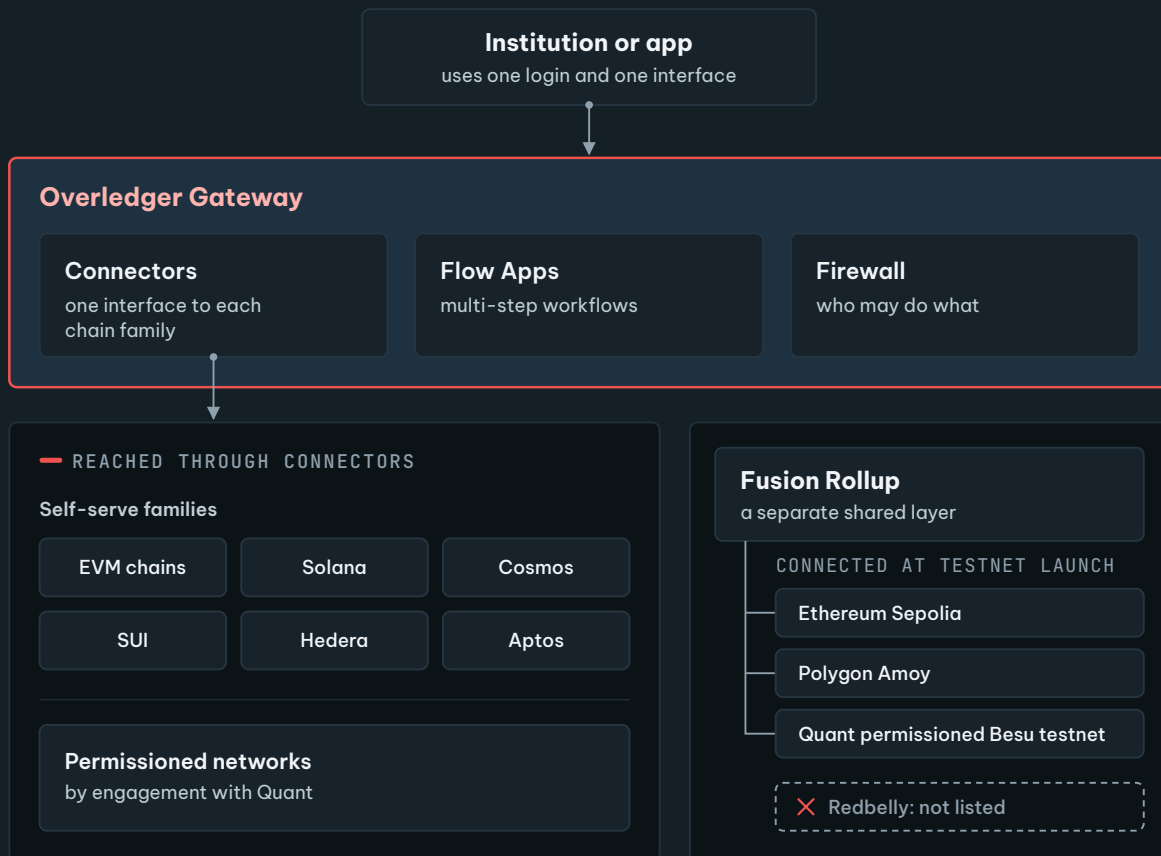
What Overledger is

● CONFIRMED

Overledger is Quant's platform for building applications that span more than one blockchain [S12](#) . It has three foundations: a Gateway that authenticates clients and routes requests [S13](#) ; Connectors that put each chain's own RPC protocol behind one common interface [S13](#) ; and the Fusion Rollup, a shared layer that anchors to several chains at once and supports deposits, withdrawals and cross-chain messages between them [S13](#) .

FIGURE 1

Overledger in one picture



The Gateway, Connectors and Flow Apps are the switchboard [S12](#) [S13](#). The Fusion Rollup is a separate layer whose deposits, withdrawals and cross-chain messages run with the networks connected to it [S13](#), and Redbelly is not among the networks documented at testnet launch [S6](#).

● ANALYSIS

In plain terms, the Gateway and Connectors are a switchboard: one login and one interface to talk to many chains [S13](#). The Fusion Rollup is different. It is a separate EVM-compatible layer: tokens deposited from the chains connected to it appear as balances on the rollup and can be withdrawn back to those chains [S13](#). The rollup connects to only a subset of the networks the Gateway reaches [S13](#), so a chain can be reachable through the switchboard without being connected to the Fusion Rollup.

● CONFIRMED

Multi-step workflows such as signing or deploying a contract run as Flow Apps [S12](#). Signing can be done with the user's own keys [S14](#), and the client never sees private key material [S14](#).

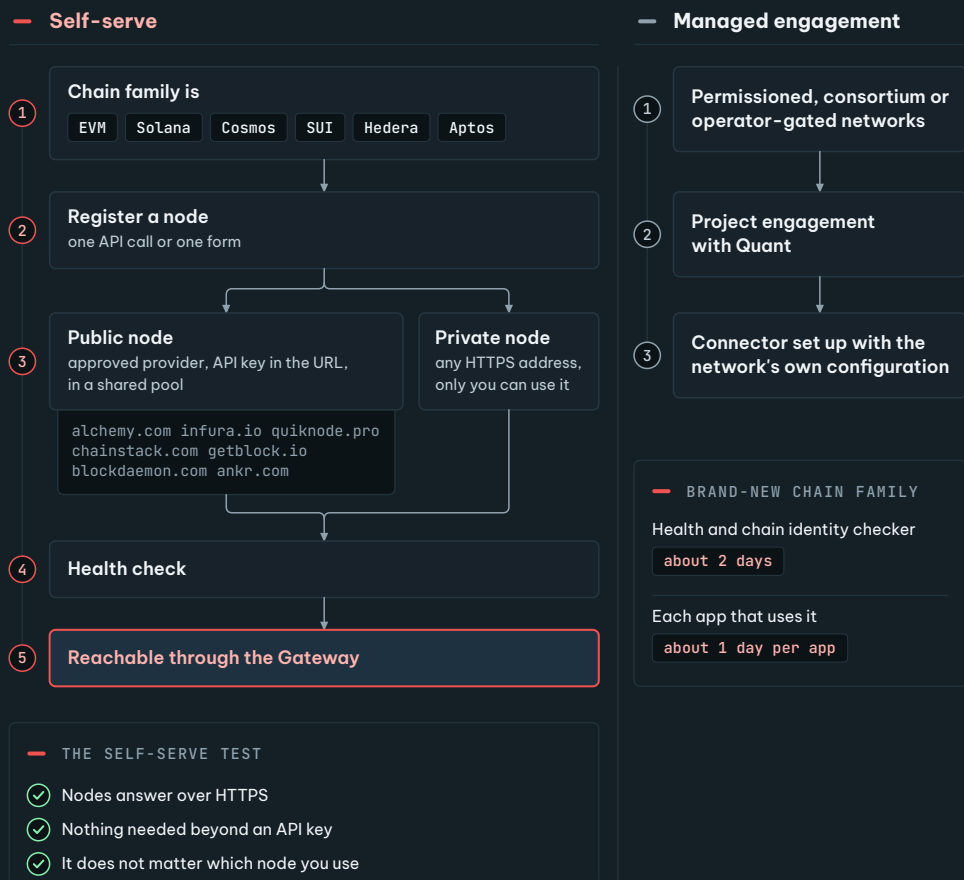
How chains connect to Overledger today

● CONFIRMED

There are two routes. The self-serve route covers six chain families, including EVM, where an account can register a node and use the network without talking to Quant's account team [S3](#). The self-serve EVM family is described as covering every EVM-compatible chain [S3](#), but self-serve Connectors are for public, permissionless chain families [S3](#), and permissioned EVM networks such as permissioned Hyperledger Besu are on the engagement route [S3](#). The managed engagement route is for private or consortium networks, and for chain families Quant does not support yet [S13](#).

FIGURE 2

Two ways a chain reaches Overledger



Self-serve covers six chain families and needs no talk with Quant's account team: one API call or form registers a node and, for a new network, the network itself [S3](#). Networks where node identity matters, and new chain families, go through an engagement [S3](#) [S13](#).

● CONFIRMED

A chain family qualifies for self-serve when its nodes offer an interface over HTTPS, need nothing beyond an API key, and it does not matter which node a client uses [S3](#). Networks where node identity matters, such as permissioned consortium chains and operator-gated public chains, are not self-serve today [S3](#).

● CONFIRMED

A chain that is not listed yet, but belongs to one of the six self-serve families, is added with the same registration call that adds a node [S3](#). The first registration creates the network, and it then becomes available to other Overledger users [S3](#).

● CONFIRMED

Each node is registered as public or private. A public node must come from an approved provider and joins the shared pool for that network [S3](#), while a private node can be at any address but is scoped to the account that added it [S3](#). The approved providers are Alchemy, Infura, QuickNode, Chainstack, GetBlock, Blockdaemon and Ankr [S3](#), and a public node URL must carry the provider's API key [S3](#). A private node can be any reachable HTTPS address [S3](#). Every node must pass a health check before it is used [S3](#).

● CONFIRMED

When a brand-new chain family is needed, the documented effort is about 2 days for a health and chain identity checker, plus about 1 day for each app that needs to use it [S3](#).

04 REDBELLY

The Redbelly facts that matter here

● CONFIRMED

Redbelly is a layer 1 blockchain built for real world asset tokenisation [S15](#). It is compatible with the Ethereum Virtual Machine and runs smart contracts written for it [S2](#). Mainnet is chain ID 151 with a public RPC address [S16](#), and Redbelly lists Ankr as a third-party public RPC provider for mainnet [S16](#). Testnet is chain ID 153 [S16](#).

● TESTED

On 15 October 2026 the official mainnet RPC and the Ankr RPC both answered with chain ID 151 (0x97) [S4](#), and the official mainnet RPC returned the latest block [S4](#). The method `net_version`, which gives a network ID to wallets and tools that predate `eth_chainId` [S6](#), returned "the method `net_version` does not exist/is not available" [S4](#).

● CONFIRMED

Writing to Redbelly is gated by identity. Every user must claim an access credential from an accredited issuer before their account can write to the network [S5](#) , and all participants must prove who they are before gaining access [S17](#) . Accredited issuers are listed in an on-chain registry [S18](#) . Businesses can also be verified as incorporated entities [S17](#) [S19](#) , and even node operators need network access for their accounts [S20](#) .

FIGURE 3

Reading Redbelly is open, writing needs an access credential

— READ ● TESTED

Public RPC

- `governors.mainnet.redbelly.network`
- `rpc.ankr.com/redbelly_mainnet`



Chain ID 151
answered on 15 Oct 2026

✗ `net_version`
not supported

— WRITE ● CONFIRMED

Wallet

Accredited issuer

listed in an
on-chain registry

Access credential

claimed by the user

Write access

account self-enables it
through a network contract

— BRIDGE ROUTES LISTED BY REDBELLY

— Celer cBridge

— LayerZero with Stargate

— Lucid Labs

Every account must claim an access credential from an accredited issuer before it can write [S5](#) [S18](#) . Reading through the public RPC needs no key, and both RPC addresses answered with chain ID 151 in our test [S4](#) [S16](#) . Redbelly's developer portal lists three bridge routes [S21](#) [S22](#) [S23](#) .

● CONFIRMED

Receptor is Redbelly's identity and verifiable credential protocol [S24](#) , built on the W3C verifiable credential data model [S24](#) . It supports two methods [S25](#) . Proof by Query uses a zero knowledge verifier smart contract [S8](#) and publishes identity state to the chain [S8](#) . Selective Disclosure uses BBS+ signatures [S26](#) , reveals chosen details to a verifier, and can only be used off-chain [S26](#) . The documented issuer identifiers for Redbelly environments take the form `did:receptor:redbelly` [S27](#) , and apps can use eligibility checks to control who may call their contract functions [S28](#) .

● CONFIRMED

Tokeniser runs on Redbelly [S9](#) and enforces eligibility, identity and target market rules at the point of transfer, every time [S9](#). Before any trade proceeds, identity, eligibility and limits are checked [S29](#); transfers are recorded on the register in real time [S30](#); and pledged units stay locked until a loan is repaid [S31](#). Redbelly settles a transaction in a single round [S9](#).

● CONFIRMED

Redbelly already has token bridges. Its developer portal lists three routes: Celer cBridge [S21](#), LayerZero with Stargate [S22](#) and Lucid Labs [S23](#). Celer uses a pegged bridge method [S32](#), and its RBNT route goes out from Redbelly but not back [S21](#). Redbelly announced Wrapped RBNT on Ethereum with the contract 0xb45f...bf13 [S33](#), which the portal lists under Lucid Labs [S23](#). The portal lists a different Ethereum contract for the Celer route [S21](#).

● CONFIRMED

Community research for TASK-08 found LayerZero live on Redbelly mainnet [S34](#). A second TASK-08 entry found that, when it was written, no major interoperability protocol had deployed core messaging infrastructure to Redbelly testnet [S35](#), and the selected entry built a lock-and-mint testnet bridge [S34](#). The TASK-16 playbook says the bridges it calls official, Reddex and Lucid, then supported only bridging USDC and USDT from BNB Chain [S36](#).

05 THE ANSWER

Can Redbelly connect now, and what is missing?

A connection can mean three different things. Each has a different answer.

FIGURE 4

Three meanings of 'connect', three answers

1 LEVEL Gateway access read data, send self-signed transactions • POSSIBLY, UNTESTED	IN PLACE ✓ Redbelly is EVM compatible ✓ Ankr, an approved provider, runs a Redbelly RPC ✓ RPC answers chain ID 151	MISSING OR OPEN ○ Self-serve status not confirmed ○ Health check method not documented ○ net_version not supported on Redbelly ○ Keyed Ankr endpoint not confirmed ○ Live network lists need an API key
2 LEVEL Flow Apps Quant workflows such as signing • UNKNOWN	OPEN ○ App catalogue not published ○ Every shipped app is built by Quant	
3 LEVEL Fusion Rollup deposits, unified balances, cross-chain messages • NOT POSSIBLE YET	IN PLACE — Nothing documented for Redbelly	MISSING ✗ Not in the documented list ✗ Bridge and dispute contracts on Redbelly ✗ Rollup state roots posted to Redbelly from accounts with Redbelly access ✗ Each token added by Quant governance

Level 1 rests on Redbelly's EVM compatibility and Overledger's self-serve EVM route [S2](#) [S3](#), with open points: whether self-serve applies to a network where writing needs a credential, the health check, a keyed provider endpoint and the live lists [S3](#) [S4](#) [S7](#) [S13](#). Level 2 cannot be checked from public sources [S14](#). Level 3 is not possible yet as far as public sources show [S5](#) [S6](#) [S37](#).

● ANALYSIS **Level 1: reaching Redbelly through the Overledger Gateway. Possibly, unconfirmed.**

Redbelly is EVM compatible [S2](#), and Overledger's self-serve EVM family is described as covering EVM-compatible chains [S3](#). An unlisted network in a self-serve family can be added by the first node registration [S3](#). At the RPC level Redbelly appears to fit the self-serve tests [S3](#): its RPC works over HTTPS and answered without a key, two different endpoints returned the same chain [S4](#), and its write rule is attached to accounts [S5](#), not to the node a client uses. Ankr, an approved provider [S3](#), runs a Redbelly mainnet endpoint [S16](#), and the official RPC could be added as a private node [S3](#).

● ANALYSIS

If it works, this level would give an institution one interface to read Redbelly data and send transactions it has signed itself. After its own access checks, the Gateway forwards the payload to a Redbelly node and passes back the native response unchanged [S3](#), so Redbelly's own rules still apply. A transaction sent this way only succeeds if the sending account has Redbelly write access [S5](#).

● UNKNOWN

Four points are open. First, how Overledger would classify Redbelly. Self-serve is written for public, permissionless networks [S3](#), Overledger's own glossary calls a network where anyone can read but only allowlisted parties can write "public permissioned" [S13](#), and permissioned EVM networks are on the engagement route [S3](#). Writing to Redbelly needs an access credential [S5](#), so Redbelly could be treated as an engagement network; the docs do not say. Second, the docs say only that the health check uses the chain's standard validation [S3](#) and that a checker does a chain identifier lookup [S3](#), not which call the EVM check uses. If it relies on net_version, Redbelly's answer [S4](#) could fail it. Third, a public node URL must carry a provider API key [S3](#), and we did not confirm that Ankr's keyed service covers Redbelly. Fourth, Overledger's live network list [S3](#) and the Fusion Rollup's list [S38](#) both answered "Missing authorization header" without an API key [S7](#), so we could not see whether Redbelly is already listed.

● ANALYSIS

Level 2: Overledger Flow Apps on Redbelly. Unknown.

Flow Apps are multi-step workflows run through the Gateway [S12](#), and customers and partners can also host their own [S13](#). The catalogue is not published [S14](#) and every shipped app is built by Quant [S14](#), so whether a given app accepts a self-serve EVM network such as Redbelly cannot be checked from public sources. The docs give an effort of about a day per app only for adding a brand-new chain family [S3](#); they give no figure for a new network inside a family Overledger already supports.

● CONFIRMED

Level 3: joining the Fusion Rollup.

The networks documented as connected at testnet launch are Ethereum Sepolia, Polygon Amoy and Quant's permissioned Besu testnet [S6](#). Each connected chain carries the rollup's bridge and dispute contracts [S6](#) and receives the rollup's state roots [S6](#). Token entries on the bridge are controlled by Quant's governance signers [S37](#).

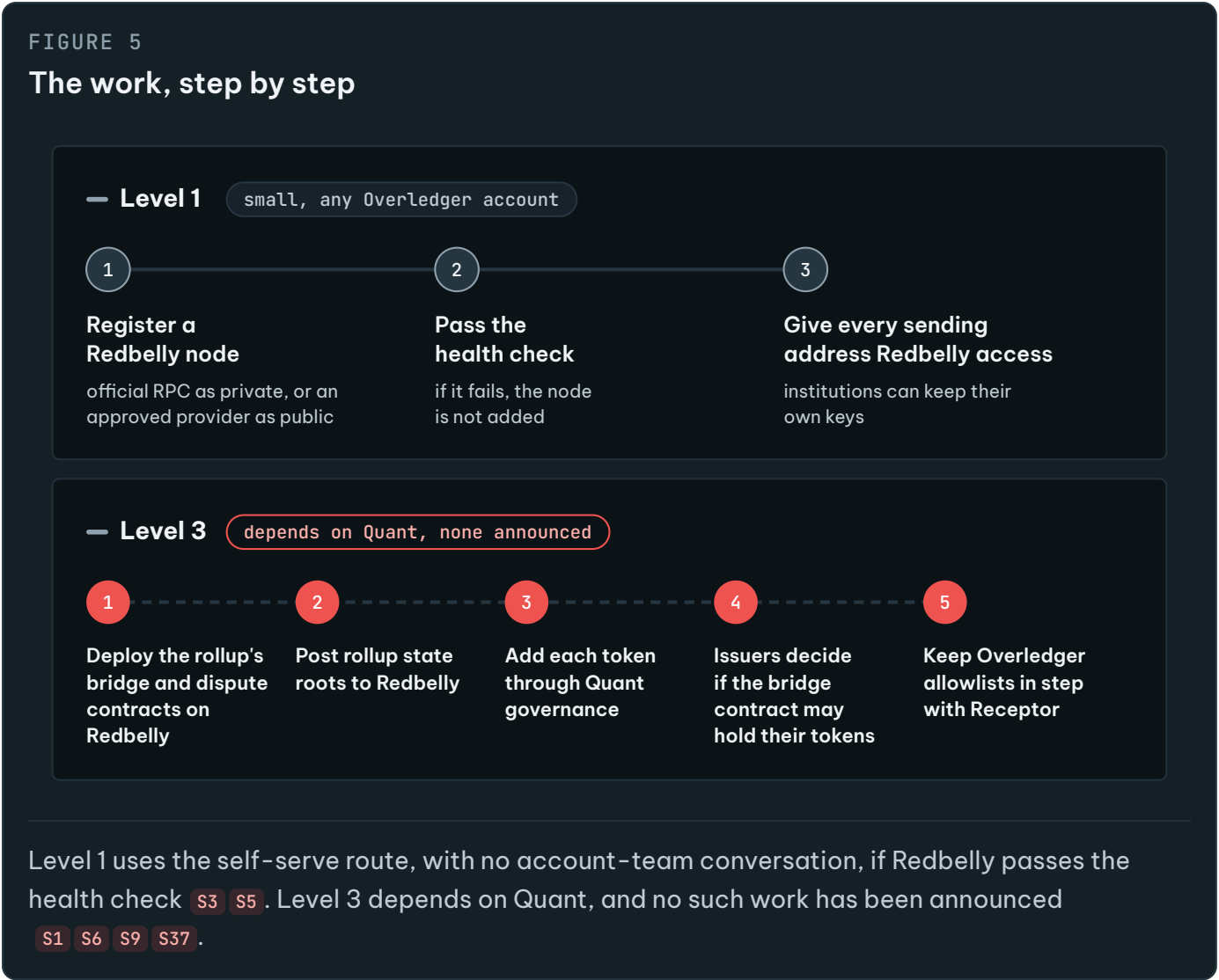
● ANALYSIS

Not possible yet, as far as public sources show.

Redbelly is not in the documented list, the live list could not be read without an API key [S7](#), and the documentation we read describes no self-serve way to add a chain to the Fusion Rollup. Joining would also have a Redbelly side: every account that writes needs an access credential [S5](#), so the accounts that deploy the rollup's contracts and post its state roots would each need Redbelly network access. No such work has been announced [S1](#).

The technical work a connection would need

Written for a non engineer. Steps marked Level 1 are small. Steps marked Level 3 depend on Quant, because Redbelly is not among the documented Fusion Rollup networks S6 and bridge tokens are added by Quant's governance S37 ; the accounts involved would also need Redbelly access S5 . No such work has been announced S1 .



● ANALYSIS

1

LEVEL 1, STEP 1

Someone with an Overledger account registers a Redbelly node: the official RPC as a private node [S3](#) or, if an approved provider's keyed service covers Redbelly (not confirmed), that provider's endpoint as a public node [S3](#). The first registration also adds the network [S3](#). This is one form or one API call [S3](#).

2

LEVEL 1, STEP 2

The node has to pass Overledger's health check [S3](#). If the check fails, the node is not added, and the docs do not say what would happen next. For scale, a checker for a brand-new chain family is documented at about 2 days [S3](#).

3

LEVEL 1, STEP 3

Every address an institution sends from needs Redbelly write access, which its user enables after claiming an access credential from an accredited issuer [S5](#). The organisation can also be verified as a business [S19](#). They can sign with their own keys [S14](#).

1

LEVEL 3, STEP 1

The rollup's standard bridge and dispute contracts are deployed on Redbelly [S6](#), from accounts that hold Redbelly access [S5](#).

2

LEVEL 3, STEP 2

The rollup's services start posting rollup state roots to Redbelly for settlement [S6](#).

3

LEVEL 3, STEP 3

Each token that should move is added to the bridge token list by Quant's governance [S37](#).

4

LEVEL 3, STEP 4

Issuers decide whether their asset contracts may hold or release tokens to the bridge contract, because Tokeniser checks eligibility on every transfer [S9](#).

5

LEVEL 3, STEP 5

Someone would have to keep Overledger's own allowlists [S37](#) in step with Receptor credentials [S5](#), because neither system's documentation describes a link to the other.

● ANALYSIS

Registering a node is a technical action any Overledger account can take [S3](#). It would not by itself mean any agreement between Redbelly and Quant.

What a connection could offer institutions

● ANALYSIS

- One interface. An institution that already reaches other chains through Overledger [S12](#) could read Redbelly and send its own signed transactions through the same Gateway and firewall checks [S13](#), without managing its own Redbelly RPC providers or node failover [S12](#), once a Redbelly node is registered [S3](#).
- Rules stay on Redbelly. At Level 1 the Gateway passes each payload to a Redbelly node and passes back the native response unchanged [S3](#), so Redbelly's access credential still applies to every sending account [S5](#), and Tokeniser's eligibility checks still apply to every transfer of a Tokeniser asset [S9](#).
- Key control. Institutions can keep and use their own keys in Overledger's model [S14](#).
- Unified balances, only at Level 3. The Fusion Rollup can merge copies of the same token from several chains into one balance [S6](#). Redbelly is not among the documented connected networks [S6](#), so as far as public sources show this is not available to Redbelly.
- No known route to tokenised deposit networks yet. The Clearing House network will use Quant's technology for its interoperability layer [S10](#), but the announcements do not say which chains it will use. Whether it will ever reach Redbelly, or any public chain, is unknown [S10](#).

● ANALYSIS

Limits to weigh. Redbelly's developer portal already lists bridge routes through Celer, LayerZero and Lucid Labs [S21](#) [S22](#) [S23](#), and Tokeniser points to EVM compatibility as its link to other networks [S9](#). Overledger would add an institutional access layer rather than a first route out. Level 3 would also put Quant's governance signers in the path, since they control which tokens may cross the Fusion bridge [S37](#), and withdrawals from the rollup wait for a dispute window [S6](#), unlike Redbelly's single round settlement [S9](#).

Receptor credentials and Tokeniser assets across chains

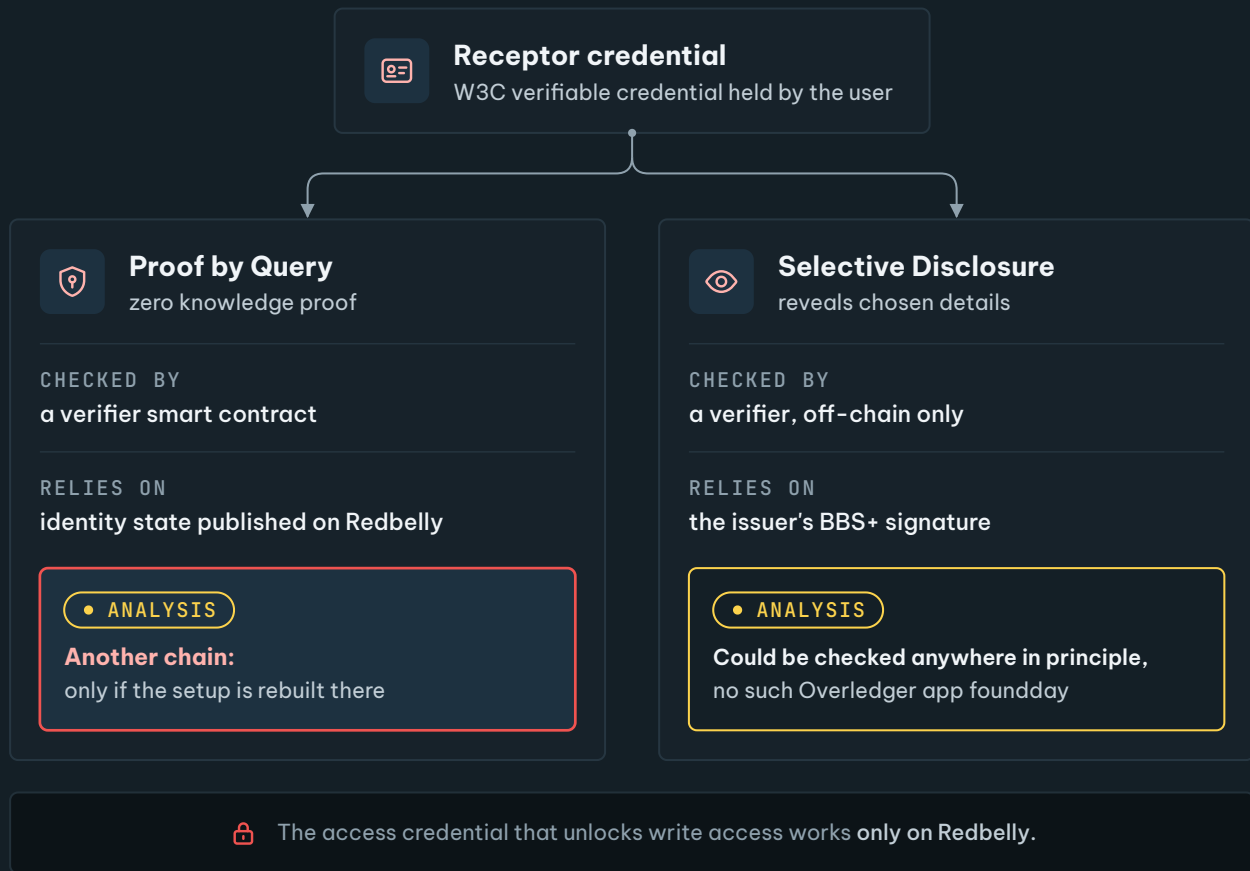
● ANALYSIS

How Receptor credentials would behave

A Receptor credential is a W3C verifiable credential held by the user [S24](#). Its two methods travel differently. A Selective Disclosure proof is checked off-chain [S26](#), so in principle any verifier could check it, including an externally hosted Overledger Flow App [S13](#); we found no such app, and every shipped app is built by Quant [S14](#). A Proof by Query check runs in a verifier contract against identity state published on Redbelly [S8](#), so another chain cannot run the same check unless that setup is rebuilt there. The access credential that unlocks write access applies to Redbelly only [S5](#).

FIGURE 6

Which Receptor checks could work off Redbelly

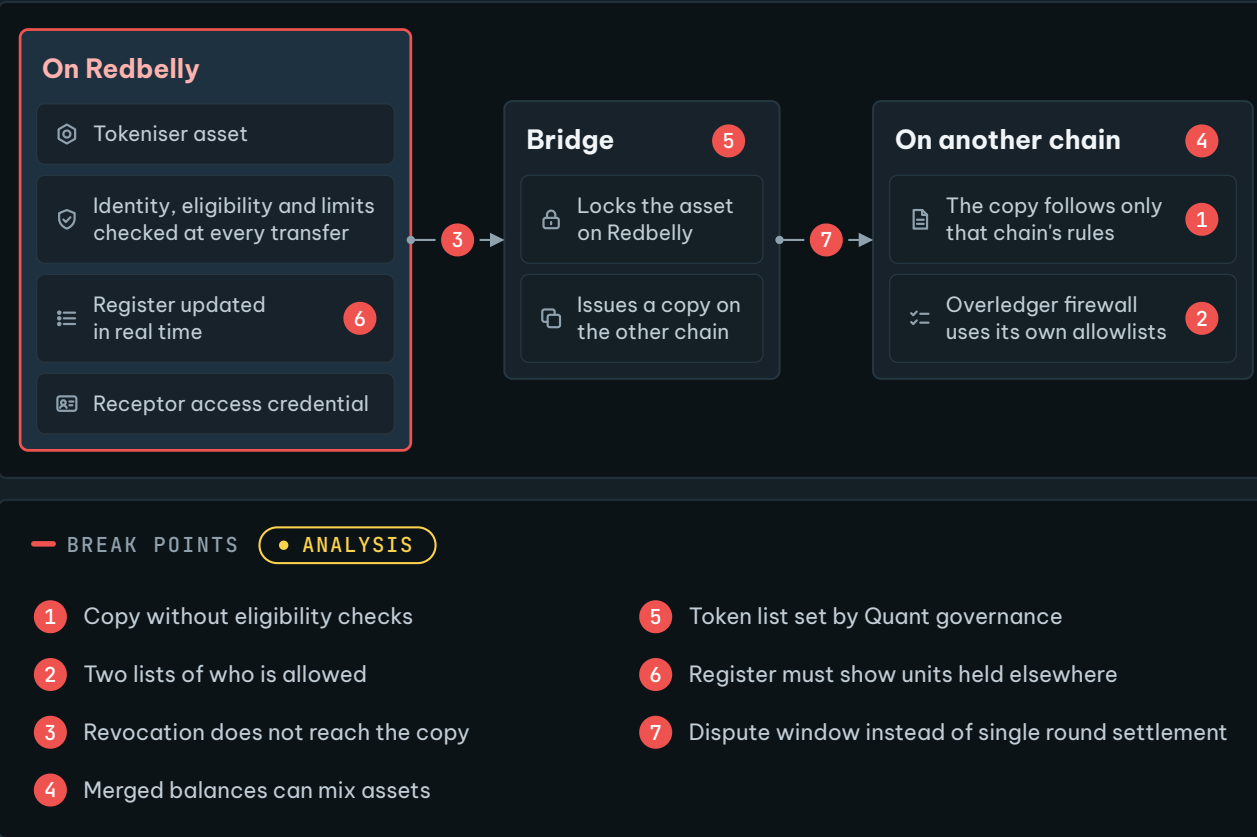


Receptor has two methods [S25](#). Proof by Query runs in a verifier contract against identity state on Redbelly [S8](#). Selective Disclosure uses BBS+ signatures and is checked off-chain [S26](#), so in principle it could be checked anywhere, but we found no Overledger app that does this; every shipped app is built by Quant [S13](#) [S14](#). The access credential applies to Redbelly only [S5](#).

ANALYSIS How Tokeniser assets would behave

Tokeniser enforces a Tokeniser asset's rules on Redbelly at every transfer [S9](#) [S29](#). A lock-and-mint bridge, the pattern of the TASK-08 testnet bridge [S34](#), locks the asset on one chain and issues a copy on the other. The copy obeys only the rules of the contracts and policies on the other chain. Overledger's firewall decides access from its own list of users and their addresses [S37](#), not from Receptor credentials.

FIGURE 7
Where compliance could break



Tokeniser enforces its rules on Redbelly at every transfer [S9](#) [S29](#) . A bridge locks the asset and issues a copy elsewhere [S34](#) , and the copy follows only the rules on that chain [S37](#) . The numbers match the list below [S6](#) [S9](#) [S30](#) [S31](#) [S37](#) .

● ANALYSIS

Where compliance could break

- 1 A copy on another chain without eligibility checks could be passed to someone who never proved eligibility on Redbelly [S9](#).
- 2 Two lists of who is allowed: Receptor credentials on Redbelly [S5](#) and Overledger's allowlists [S37](#). If they drift apart, one system allows what the other refuses.
- 3 A revoked credential on Redbelly [S5](#) does not reach a copy held elsewhere unless someone updates the other list [S37](#).
- 4 Merged balances [S6](#) could mix a restricted asset with an unrestricted copy of the same asset.
- 5 The list of tokens that may cross the Fusion bridge is set by Quant's governance [S37](#), not by the issuer.
- 6 The register is kept on Redbelly in real time [S30](#). Units held on another chain, or locked in a bridge [S31](#), need clear treatment in that register.
- 7 Settlement timing changes: rollup withdrawals wait for a dispute window [S6](#), while Redbelly is final in one round [S9](#).

● ANALYSIS

The lowest risk pattern is for regulated assets to stay on Redbelly and for Overledger to carry only instructions and data at Level 1, so that every transfer still meets Redbelly's checks [S3](#) [S5](#) [S9](#).

09 OPEN QUESTIONS

Not possible yet, and unknown

QUESTION	ANSWER TODAY
Joining the Fusion Rollup	● NOT POSSIBLE YET As far as public sources show S6 S7
Receptor credentials recognised by Overledger's firewall	● NOT POSSIBLE YET No documented link S5 S37
Tokeniser rules enforced on copies held on other chains	● NOT POSSIBLE YET Only the destination's rules apply S9 S34

QUESTION	ANSWER TODAY
Whether Overledger treats Redbelly as self-serve or engagement	● UNKNOWN Writing to Redbelly needs a credential S3 S5 S13
Whether Redbelly passes Overledger's EVM health check	● UNKNOWN Needs a test with an account S3 S4
Whether Redbelly is already in Overledger's live network list	● UNKNOWN The lists need an API key S7
Whether Flow Apps work with Redbelly	● UNKNOWN Catalogue not public S14
Which chains The Clearing House network will reach	● UNKNOWN S10
Redbelly's position on bridging or on Overledger	● UNKNOWN Nothing published S1
Any plan by Redbelly or Quant to connect	● NONE ANNOUNCED S1

10 METHOD

How this report was made and how to check it

● HOW IT WAS DONE

Every source page was saved as a text snapshot on 15 October 2026, with its address, capture time and SHA-256 hash in evidence/manifest.json. Each factual claim cites a fact, and each fact quotes its source word for word. The script scripts/check.py confirms that every quote is in its snapshot, that every Confirmed paragraph cites a source, and that the text has no partnership wording, no investment language, no dashes and no emoji. We ran the RPC and API calls ourselves, and kept the full output in evidence/tests. We did not create an Overledger account, so nothing here was tested inside Overledger.

Community summary

Plain language, ready for the DAO to share. Copy the paragraphs, a single post, or the whole thread.

A few paragraphs

Could Redbelly connect to Quant's Overledger? We looked only at public documents. Redbelly and Quant have not announced any partnership or talks, and this research does not suggest any.

Overledger is Quant's platform for reaching many blockchains through one interface. Its self-serve route covers EVM chains, and Redbelly is EVM compatible, so a basic connection, reading Redbelly and sending transactions the sender has signed, looks possible. It is untested, and Overledger describes self-serve as for public permissionless networks, while writing to Redbelly needs a credential. Every Redbelly rule would still apply.

Overledger's Fusion Rollup, its shared layer for moving tokens between chains, does not list Redbelly among its connected networks, and the docs describe no self-serve way to add a chain. As far as public sources show, that part is not possible today.

Receptor credentials and Tokeniser's eligibility rules are enforced on Redbelly. They do not travel with a token to another chain. Keeping regulated assets on Redbelly avoids that gap.

Open questions: whether Overledger would treat Redbelly as self-serve, whether Redbelly passes its network check, which chains The Clearing House network will reach, and Redbelly's own position on bridging. The full report and every source are linked below.

As an X thread, 6 posts

Post 1 of 6

239 / 280

1/ The Clearing House picked Quant to power its tokenised deposit network, so people are asking: could Redbelly connect to Quant's Overledger? We read the public docs. No partnership or talks between Redbelly and Quant have been announced.

Post 2 of 6

232 / 280

2/ Overledger reaches many chains through one interface. Its self-serve route covers EVM chains, and Redbelly is EVM compatible. A basic connection for reading data and sending signed transactions looks possible, but it is untested.

Post 3 of 6

173 / 280

3/ Redbelly's rules still apply on that route. Every account that sends a transaction needs a Redbelly access credential, and Tokeniser checks eligibility on every transfer.

Post 4 of 6

206 / 280

4/ Overledger's Fusion Rollup, which moves tokens between connected chains, does not list Redbelly, and the docs describe no self-serve way to add a chain. As far as public sources show, not possible today.

Post 5 of 6

191 / 280

5/ Receptor credentials and Tokeniser rules do not travel with a token to another chain. A copy elsewhere follows only that chain's rules. Keeping regulated assets on Redbelly avoids the gap.

Post 6 of 6

250 / 280

6/ Still unknown: whether Overledger would treat Redbelly as self-serve, since writing needs a credential, which chains The Clearing House network will reach, and Redbelly's position on bridging. Full report with every source: <https://overledger.test-hub.xyz>

Source list

Each source with the exact words this report relies on. Page copies with SHA-256 hashes are in the project repository.

S1 Redbelly DAO Task Board: TASK-29 brief: Quant Overledger and Redbelly Interoperability Research

<https://taskboard.redbellydao.network/tasks/TASK-29>

- o “This is feasibility research only. Redbelly and Quant have no announced partnership or talks”
- o “Redbelly has not published an official position on bridging”

S2 Vine, Redbelly Network developer portal: EVM compatibility and version details

<https://vine.redbelly.network/consensus/evm-compatibility/>

- o “Redbelly is compatible with the Ethereum Virtual Machine (EVM) and can execute smart contracts written for the EVM.”

S3 Quant, Overledger documentation: Chapter 5: Connectors

<https://docs.overledger.dev/docs/connectors>

- o “Six DLT families are available for self-serve onboarding today, you can register a node and call the network without an account-team conversation”
- o “Covers every EVM-compatible chain”
- o “A DLT family is considered eligible for self-serve if (a) its nodes expose RPC or REST over HTTPS, (b) the RPC requires no security factor beyond an API key, and (c) node identity does not matter to other tenants (so a pool of equivalent nodes can be load-balanced safely).”
- o “New network within a supported DLT family, the network is not yet listed by Overledger, but its DLT family is one Overledger already supports for self-serve (EVM, Solana, Cosmos, SUI, Hedera, Aptos). The first POST /nodes call registers both the network and your node for it. This new network will then be available for Overledger users.”
- o “If public is selected then the user can only add nodes from whitelisted providers. If private is selected then the user can add nodes from any domain.”
- o “alchemy.com, infura.io, quiknode.pro, chainstack.com, getblock.io, blockdaemon.com, ankr.com”
- o “Required, embedded in the URL path (the Gateway forwards the URL as-is), not a header.”
- o “Any reachable HTTPS URL, self-hosted, custom-provider, on your own infrastructure, anywhere.”
- o “The Gateway runs a health check using the DLT’s standard validation from section 5.1 and, on success, adds the node to the network’s load-balancing pool.”
- o “For networks where node identity matters, typically permissioned DLTs used by regulated consortia and operator-gated public chains, Overledger does not self-serve currently.”
- o “Implement a DLT checker (health validation + chain identifier lookup) ~2 days”
- o “Add per-DLT handling in any apps that need to consume it ~1 day per app”
- o “Forwards the payload, returns the native response unchanged.”
- o “Self-serve Connectors for public, permissionless DLT families.”
- o “For networks where it does not matter which node a client connects to, i.e. public permissionless networks”
- o “Hyperledger Besu (permissioned) Permissioned EVM Used in regulated EVM deployments.”
- o “Run GET /networks to retrieve the live list.”
- o “Overledger lets you register a managed-provider node URL via a single API call. The network then becomes immediately reachable through the Overledger Gateway.”
- o “Any tenant with access to the network, the node joins the shared load-balancing pool for that network.”
- o “the node is scoped to your user identity”

S4 Test run for this report: JSON-RPC calls to Redbelly mainnet and testnet endpoints, 15 October 2026

<evidence/tests/rpc-check.txt> (project repository)

- o “https://governors.mainnet.redbelly.network eth_chainId -> {“jsonrpc”:“2.0”,“id”:1,“result”:“0x97”}”
- o “https://rpc.ankr.com/redbelly_mainnet eth_chainId -> {“id”:1,“jsonrpc”:“2.0”,“result”:“0x97”}”
- o “https://governors.mainnet.redbelly.network net_version -> {“jsonrpc”:“2.0”,“id”:1,“error”:{“code”:−32601,“message”:“the method net_version does not exist/is not available”}}”
- o “eth_getBlockByNumber -> {“jsonrpc”:“2.0”,“id”:1,“result”:{“

S5 Vine, Redbelly Network developer portal: User access

<https://vine.redbelly.network/identity/user-access/>

- “Before being granted access to Redbelly Network, each user must claim their access credential from a network accredited issuer before they self enable their account with write access to the network through a specific network smart contract.”

S6 Quant, Overledger documentation: Chapter 8: Fusion Rollup

<https://docs.overledger.dev/docs/fusion-rollup>

- “Connected DLT networks on testnet launch are: Ethereum Sepolia, Polygon Amoy, Quant’s permissioned Besu testnet. The full live list comes from GET /networks/fusion.”
- “The bridge and dispute contracts deployed on each connected DLT network. Standard OP Stack contracts, one deployment per chain.”
- “Compute Fusion Rollup state roots and post them to all connected DLT networks for settlement”
- “Because Fusion is an optimistic rollup, a withdrawal is not immediately final, there is a dispute window during which a challenger can prove the Fusion Rollup state root invalid.”
- “Fusion can map several token contracts to a single rollup-side ERC-20, so deposits from any of those source chains land in one unified balance.”
- “Network ID. Exposed for wallets and tools that predate eth_chainId.”

S7 Test run for this report: Calls to the public Overledger server API without an account, 15 October 2026

[evidence/tests/overledger-api-check.txt](#) (project repository)

- “GET https://fusion-rollup.quant.dev/networks/fusion -> HTTP 401 {“status”:401,“error”:“Missing authorization header.”}”
- “GET https://fusion-rollup.quant.dev/networks -> HTTP 401 {“status”:401,“error”:“Missing authorization header.”}”

S8 Redbelly Network technical documentation: Proof by Query

<https://docs.redbelly.network/pages/methods/proof-by-query/>

- “a zero knowledge proof based verifier smart contract”
- “State verification and transition, with subsequent publication to the blockchain.”

S9 Tokeniser: Technology

<https://tokeniser.com/technology>

- “Eligibility, identity and your target market determination are enforced at the point of transfer, every time.”
- “Deterministic finality settles a transaction in a single round, final the moment it completes.”
- “full EVM compatibility connects you to more than 150 networks out of the box”
- “Underneath it runs Redbelly Network”

S10 The Clearing House: The Clearing House Partners with Quant to Advance the On-Chain Money Initiative (24 September 2026)

<https://www.theclearinghouse.org/payment-systems/Articles/2026/09/The-Clearing-House-Partners-with-Quant-to-Advance-the-On-Chain-Money-Initiative>

- “The Clearing House announced the selection of Quant, a leading provider of programmable money infrastructure, to power its On-Chain Money Initiative, a new interoperable payments network that will enable financial institutions of all sizes to clear and settle tokenized deposit transactions.”
- “Quant’s technology will enable the network’s interoperability, orchestration, and transaction-management layer that coordinates the clearing and settlement of tokenized deposit transactions”
- “providing connectivity to existing fiat payment systems that financial institutions and their customers use every day, including the RTP® and CHIPS® networks”
- “The network is expected to become available to participating institutions in the first half of 2027, with additional details on participation and use cases to be announced as development progresses.”

S11 Quant: Press release: The Clearing House Partners with Quant to Advance the On-Chain Money Initiative

<https://quant.network/press-releases/the-clearing-house-partners-with-quant-to-advance-the-on-chain-money-initiative/>

- “The Clearing House will use Quant’s technology to bring on-chain capabilities to its tokenised deposit clearing and settlement network for financial institutions.”

S12 Quant, Overledger documentation: Start Here

<https://docs.overledger.dev/docs/start-here>

- “Overledger is Quant’s multi-DLT platform for building applications that span more than one blockchain”
- “Flow Applications turn multi-step business logic (signing, smart-contract deployment, compliance check, payment”
- “You don’t manage RPC providers, node failover, or chain-specific clients.”

S13 Quant, Overledger documentation: Chapter 1: Overview

<https://docs.overledger.dev/docs/overview>

- “A Gateway that authenticates clients, routes requests, and orchestrates higher-level workflows.”
- “A set of Connectors that abstract individual DLT RPC protocols behind a common interface.”
- “A Multi-ledger rollup (the Fusion Rollup) that anchors to multiple blockchains simultaneously, providing one EVM-compatible execution environment with deposits, withdrawals, and cross-chain messaging across every connected L1.”
- “Customers and partners can host their own Flow Apps externally, stand up an HTTPS service that implements the Flow App contract, register its URL with the Gateway, and your bespoke regulated workflow becomes a first-class app in Overledger.”
- “Managed engagement: you work with Quant’s team to onboard a private / consortium network (e.g. Corda, Canton, Fabric) or to add a brand-new DLT family Quant doesn’t yet support.”
- “A network with controlled write access; “public permissioned” means anyone can read but only allowlisted parties can write.”
- “The Rollup connects to a subset of these networks.”
- “It applies to every public or permissioned DLT network that the Gateway reaches”

S14 Quant, Overledger documentation: Chapter 6: Flow Apps

<https://docs.overledger.dev/docs/flow-apps>

- “today every shipped app is internal”
- “The Flow App catalogue is intentionally not enumerated in these docs”
- “Three phases between Client, Gateway, Flow App, and Signer Flow App. The Sign phase hands off via a sub-flow; the Client never sees private-key material.”
- “You hold the keys (BYO signing, see chapter 7.2).”

S15 Redbelly Network technical documentation: Home

<https://docs.redbelly.network>

- “The Redbelly Network is a layer 1 blockchain, built and optimised for real world asset tokenisation.”

S16 Vine, Redbelly Network developer portal: Redbelly Network environments

<https://vine.redbelly.network/environments/>

- “Network name: Redbelly Network Mainnet RPC URL: <https://governors.mainnet.redbelly.network> Chain ID: 151”
- “Ankr https://rpc.ankr.com/redbelly_mainnet”
- “RPC URL: <https://governors.testnet.redbelly.network> Chain ID: 153”

S17 Vine, Redbelly Network developer portal: Identity and participation on the network

<https://vine.redbelly.network/identity/>

- “all network participants MUST prove they are who they say they are before gaining access”
- “business verification is also available on the network”

S18 Vine, Redbelly Network developer portal: Accredited issuers

<https://vine.redbelly.network/identity/accredited-issuers/>

- “All accredited issuers are listed in an on chain registry.”

S19 Vine, Redbelly Network developer portal: Business verification

<https://vine.redbelly.network/business-verification/>

- “To be verified, businesses need to prove they are an incorporated entity to a network accredited issuer.”

S20 Vine, Redbelly Network developer portal: Becoming a node operator

<https://vine.redbelly.network/nodes/become-operator/>

- “Node operators MUST have network access for 2 accounts and provide their public address when applying to run a node.”

S21 Vine, Redbelly Network developer portal: Bridged tokens: Celer cBridge

<https://vine.redbelly.network/bridged-tokens/celer/>

- “RBNT bridges out from Redbelly to Ethereum and BNB Chain, not back.”
- “Ethereum 0x063a1D5BFEAb213c9c12f47b704fccf81D60983e wRBNT Wrapped RBNT 18”

S22 Vine, Redbelly Network developer portal: Bridged tokens: LayerZero

<https://vine.redbelly.network/bridged-tokens/layerzero/>

- “Tokens on Redbelly Network that can be bridged to other chains via LayerZero, using Stargate, and vice versa.”

S23 Vine, Redbelly Network developer portal: Bridged tokens: Lucid Labs

<https://vine.redbelly.network/bridged-tokens/lucidlabs/>

- “Tokens on Redbelly Network that can be bridged to other chains via Lucid Labs, and vice versa. Powered by Polymer and LayerZero.”
- “Ethereum 0xb45fB51984d626Ee758b336C61Cf20990c6bF13 WRBNT Wrapped RBNT 18”

S24 Redbelly Network technical documentation: Receptor overview

<https://docs.redbelly.network/pages/receptor/>

- “Receptor is Redbelly’s native digital identity and verifiable credential protocol.”
- “Receptor is built on the W3C verifiable credential data model, providing a standardised and interoperable foundation for identity verification and eligibility criteria assurance.”

S25 Vine, Redbelly Network developer portal: Eligibility

<https://vine.redbelly.network/identity/eligibility/>

- “Redbelly supports two distinct credential types, or methods, that can be used to perform eligibility criteria checks:”

S26 Redbelly Network technical documentation: Selective Disclosure

<https://docs.redbelly.network/pages/methods/selective-disclosure/>

- “As selective disclosure involves disclosing information to the Verifier, it can only be used off-chain.”
- “Selective Disclosure involves using credentials that implement BBS+ signatures.”

S27 Redbelly Network technical documentation: Eligibility SDK for Redbelly Network

<https://docs.redbelly.network/pages/eligibility-sdk/eligibility-sdk/>

- “Redbelly Mainnet did:receptor:redbelly:mainnet:31AAH8sSaGd6fPnG1TcB6yQ4UZnNeyHzTk5aM2P7rjv”

S28 Vine, Redbelly Network developer portal: Eligibility checks (smart contracts)

<https://vine.redbelly.network/smart-contracts/eligibility-checks/>

- “Eligibility checks can be used to control access to your dApp or smart contract’s functions or when specific smart contract functions are called to help meet your compliance requirements.”

S29 Tokeniser: Automated compliance

<https://tokeniser.com/product/superpowers/automated-compliance>

- “Before any trade proceeds, the investor’s identity, eligibility (including wholesale or sophisticated status where required) and your limits are verified automatically.”

S30 Tokeniser: Secondary transfer

<https://tokeniser.com/product/superpowers/secondary-transfer>

- “every transfer is recorded on your register in real time”

S31 Tokeniser: Collateral mobility

<https://tokeniser.com/product/superpowers/collateral-mobility>

- “Investors pledge units as security, and the units remain locked until the loan is repaid.”

S32 Celer Network blog: Celer Announces cBridge Support for Redbelly (1 August 2025)

<https://blog.celer.network/2025/08/01/celer-announces-cbridge-support-for-redbelly/>

- “Celer is supporting asset and token bridging initially via a pegged bridge method”

S33 Redbelly Network on X: Wrapped RBNT Token is now live on Ethereum Mainnet (14 February 2025)

<https://x.com/RedbellyNetwork/status/1890340030197166112>

- “Wrapped RBNT Token is now live on Ethereum Mainnet.”
- “0xb45ffb51984d626ee758b336c61cf20990c6bF13”

S34 Redbelly DAO Community Task Board: TASK-08 bridge integration guide (selected entry)

<https://github.com/Redbelly-DAO-Community-Taskboard/TASK-08-bridge-integration-guide>

- “Redbridge is a lock-and-mint bridge”
- “Yes, on Mainnet dedicated “Redbelly Mainnet” deployment”

S35 TASK-08 entry, public repository: Bridging Ethereum Sepolia to Redbelly Testnet: technical guide

https://github.com/tycayomide/redbelly-testnet-bridge/blob/main/TECHNICAL_GUIDE.md

- “no major interoperability protocol has deployed core messaging infrastructure (endpoints, gateways, or guardian sets) to”

S36 Redbelly DAO Community Task Board: TASK-16 Cross-Chain Recovery Playbook (selected entry, PDF)

<https://github.com/Redbelly-DAO-Community-Taskboard/TASK-16-cross-chain-recovery-playbook/blob/main/deliverable/Redbelly-task-16-revised.pdf>

- “Because the official Redbelly bridges (Reddex and Lucid) currently only support bridging USDC and USDT from BNB Chain”

S37 Quant, Overledger documentation: Chapter 9: Overledger Firewall

<https://docs.overledger.dev/docs/overledger-firewall>

- “Overledger maintains the binding between each user and their authorised on-chain address(es) off-chain, so policies expressed against a user translate into on-chain address allowlists at the contracts that enforce them.”
- “Token allowlist entries are governance-controlled (Quant Safe signers), not per-deployer, they apply to all users of the bridge.”

S38 Quant, Overledger API reference: Overledger Server API reference

<https://docs.overledger.dev/reference>

- “List Fusion Rollup connected networks”