bisik.

Indonesian for *whisper*. You whisper quotes. The market hears nothing.

A confidential multi-dealer RFQ desk for OTC block trades — native on Canton.

Live on Canton Devnet | Private DeFi & Capital Markets | TradeFi & Tokenized Assets | Agentic Commerce

Build on Canton Hackathon · Encode Club × Canton Foundation

THE PROBLEM

You cannot trade size in the open.

- Post a $4M block on a public venue and the order — plus every competing bid — leaks.
- Front-running, market impact, alpha gone the moment it touches a mempool.
- Today's workaround: OTC desks and chat rooms. Trust a middleman, keep no clean audit trail.
- **$30B+ a month still trades this way.**

THE BIND

Fair price discovery *requires* sealed bids.

A transparent ledger makes sealed bids impossible — unless you bolt on a cryptography stack.

WHY THIS BUILD IS DIFFERENT

We built this exact product four times, on four chains.

Each time, most of the work was fighting the chain's transparency.

PROJECT	CHAIN	PRIVACY MACHINERY WE HAD TO BUILD
Diam	Arbitrum (iExec)	TEE confidential compute, encrypted handles
Segel	Stellar (Soroban)	Two Circom/Groth16 ZK circuits, hand-rolled Poseidon
Sealed Pair	Sui	Walrus blob commitments + Seal threshold encryption
Samar	Ethereum (Zama fhEVM)	FHE, branchless `FHE.select` settlement
Bisik	**Canton**	**None. Sub-transaction privacy is the ledger model.**

On Canton, “Dealer B cannot see Dealer A's quote” is not a cryptographic achievement. It is a `signatory` / `observer` declaration.

WHAT BISIK IS

A sealed-bid RFQ desk where the guarantees are code, not a middleman.

- A buyer requests quotes from a chosen dealer panel. The market never sees the RFQ.
- Each dealer answers with a sealed quote — rival dealers never *receive* it.
- The dealer's asset locks into escrow: it cannot be double-sold mid-auction.
- The buyer awards: cheapest ask wins, paid the second-cheapest price (reverse Vickrey).
- Settlement is atomic DvP — cash and asset move together or not at all.
- A regulator observes executed trades — *and only executed trades*.

WHY VICKREY

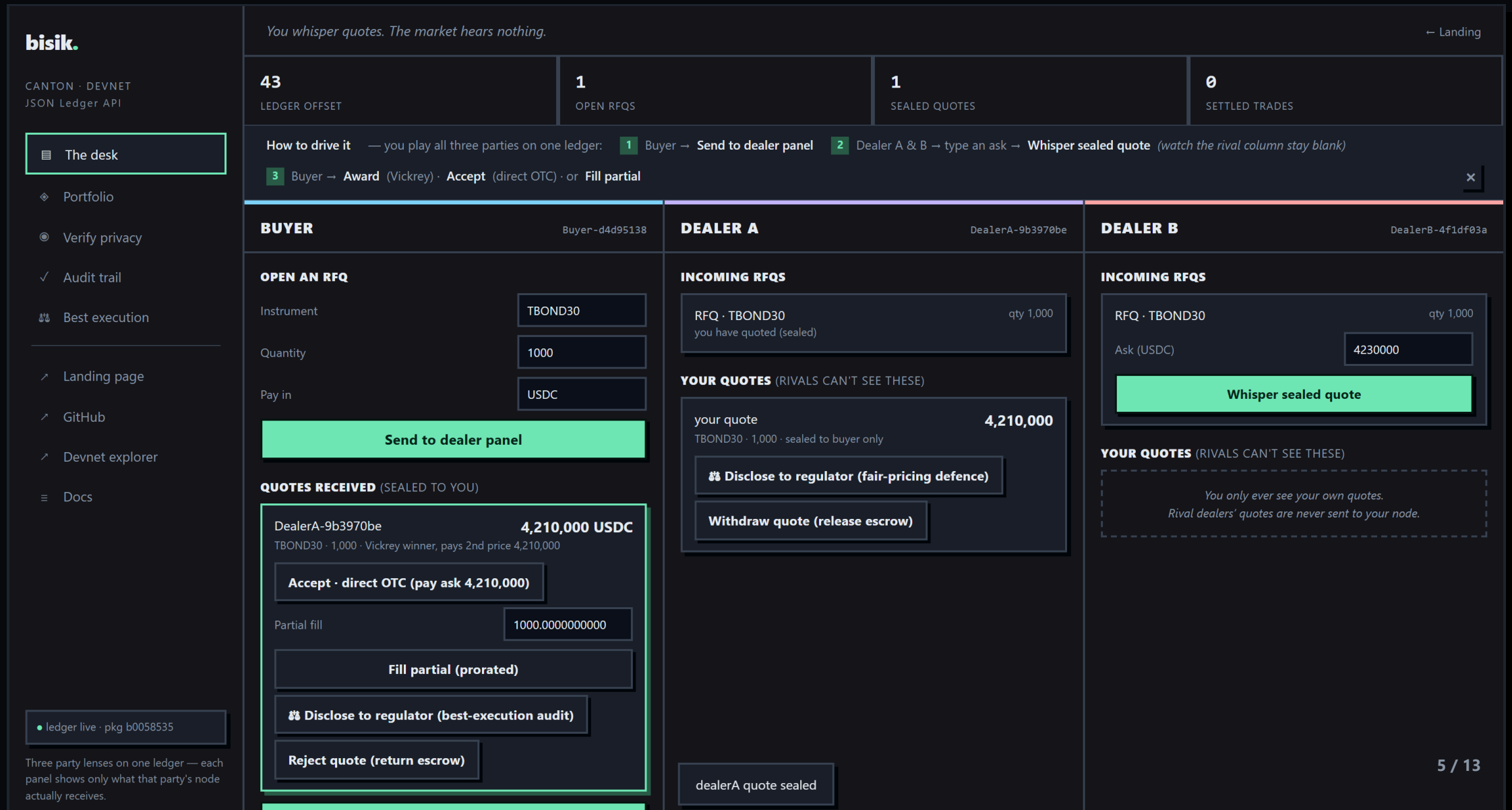
Winner is paid the runner-up's price, so dealers can quote their true reserve without shading.

On a transparent chain this needs ZK or FHE. Here it is ~40 lines of Daml.

THREE SETTLEMENT RAILS

Competitive Vickrey · direct bilateral OTC · partial fills on both. Plus multi-instrument baskets, atomically.

Dealer A has quoted. Dealer B's column stays empty.



THE WHOLE PRIVACY LAYER

This is the entire mechanism.

```
template RFQ             signatory buyer, observer invitedDealers
                         — the market never sees it

choice   SubmitQuote     dealer locks the asset into escrow + seals a quote

template Quote           signatory dealer, buyer — NO other observers
                         — rivals never RECEIVE it (physically, not by policy)

template EscrowedHolding signatory issuer+dealer, observer buyer
                         — dealer cannot double-sell or pull it back alone

choice   Award           cheapest ask wins, paid the SECOND price (Vickrey);
                         atomic DvP in one transaction; losers archived unrevealed

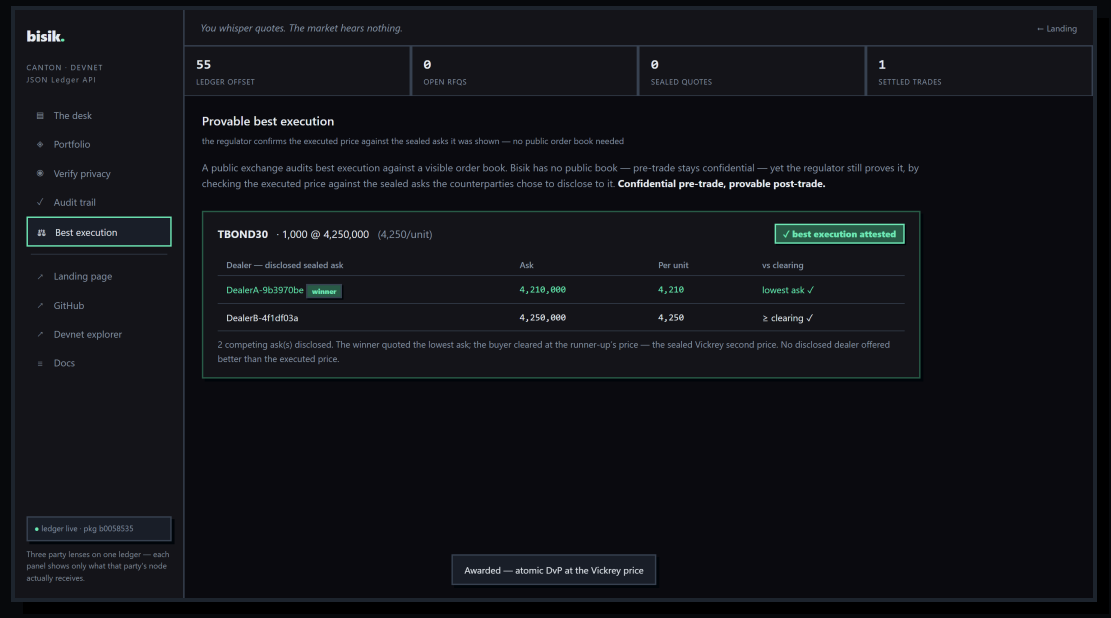
template TradeReport     observer regulator — post-trade only
```

No circuits. No ceremony. No trusted hardware. The privacy is the data model.

THE INSTITUTIONAL PAYOFF

Provable best execution — with no public order book.

- Counterparties selectively disclose their sealed asks to the regulator — buyer *and* dealer can each reveal.
- The regulator recomputes: did the executed price beat every competing ask?
- **Confidential pre-trade. Provable post-trade.** Both, at once.
- This is the compliance obligation (MiFID-style best execution) that normally forces a transparent venue.



16 attestations live on Devnet | **Vickrey · direct-OTC · partial**

AGENTIC COMMERCE, FOR REAL

Two software agents negotiated and settled a live trade.

```
$ npm run agent:demo

· two market-maker agents quote blind
    MarketMaker A  4,233,600  (+0.80%)  — won
    MarketMaker B  4,258,800  (+1.40%)  — runner-up
· each agent's node holds only its OWN quote ✓
· buyer-agent awards; the ledger clears at
  the SECOND price — 4,258,800
· TradeReport settled on Canton Devnet ✓
```

- No human sets the clearing price — the `Award` choice does, on-ledger.
- Each dealer-agent is structurally blind to its rival: it cannot peek, because the data never reaches it.
- An **MCP server** exposes the desk to AI agents — five read tools plus `post_rfq`, which posts a real RFQ on Devnet.
- An agent can verify Canton's privacy model *for itself* rather than take it on faith.

TOKENIZED ASSETS

A CIP-0056-shaped token standard, live on Devnet.

`Holding`

A standard, viewable position — with a real lock, so reserved state is visible to tooling.

`TransferInstruction`

Two-step transfer: propose → accept / reject / withdraw, with an expiry. Funds are never stranded.

`Allocation → DvP`

Reserve a leg, then settle two legs in *one* transaction. Neither side can claim unilaterally.

Deployed as its own package, verified on-ledger: a two-step transfer instruction and an atomic delivery-versus-payment swap, both executed live on Canton Devnet.

Honest scope: this is the standard's on-ledger *shape*, native. Full external-wallet registry interop (the Splice factory DARs) is the next step.

NOT A MOCK-UP

Live on Canton Devnet — with a real book behind it.

41	5	16
SETTLED TRADES	ATOMIC BASKETS	BEST-EXEC ATTESTATIONS

Sovereigns (US, UK, Germany, Japan, France, Canada, Australia, Netherlands, Switzerland, Korea, Singapore), supranationals (World Bank, EIB, KfW), corporates (Apple, Microsoft, Nvidia, Goldman) and EM (Mexico, Brazil, India, Indonesia) — settled against tokenized cash, issuer-bound, atomic DvP.

```
desk       bisik-otc v0.6.0   b0058535…   parties bisik-v6-*
token      bisik-token        d969c045…   transfer + atomic DvP verified
regulator  {"TradeReport":41,"BasketTradeReport":5,"QuoteDisclosure":32}
dealerB    sees only its own quotes  ✓ privacy verified on-ledger
```

ENGINEERING RIGOR

The tests found real bugs. That is the point of having them.

36	143	3
DAML SCRIPTS	AUTOMATED CHECKS	BROWSER ENGINES

Playwright drives the real UI, the live hosted build, and the MCP server over real JSON-RPC. CI gates a four-package Daml workspace on every push.

CAUGHT BY ADVERSARIAL QA

- Escrow was **unilaterally revocable** — a dealer could pull collateral while its quote stayed live.
- No issuer binding — a dealer could quote a **self-issued counterfeit** bond.
- DvP was not atomic: a receiver could **take a leg without delivering** theirs.
- Each one is now a named regression test.

HONEST SCOPE

What is guaranteed, and what is not.

ENFORCED ON-LEDGER

- Rivals never receive each other's quotes.
- A dealer is never paid below its own ask.
- Both legs move, or neither does.
- Escrow cannot be pulled back unilaterally.
- A quote settles the RFQ it was made against — no other.
- Issuers are checked; counterfeits are rejected.

LEFT TO THE AUCTIONEER

Only the buyer sees every sealed quote, so only the buyer can run the auction. It can curate the awarded set and clear at the winner's own ask — *suppressing the Vickrey uplift*, though never underpaying a dealer.

Forcing the true second price needs a trusted auctioneer or MPC — and MPC re-introduces exactly the cryptography Canton lets us skip. We would rather state the limit than overclaim.

The confidential OTC desk that finally didn't need a cryptography stack —

because Canton already is one.

```
live desk   bisik-eight.vercel.app/app
repository  github.com/PugarHuda/bisik
network     Canton Devnet · JSON Ledger API
```

bisik. — you whisper quotes. The market hears nothing.