HUMAN RIGHTS FOUNDATION · BITCOIN DEVELOPMENT FUND · APPLICATION PENDING

PACT

Quantum-sunset protection for Bitcoin holders who cannot move their coins without revealing who they are.

40%

of the proposed scope is already delivered, built before any funding decision.

216

automated tests and conformance cases, all passing, all runnable with no setup.

51

conformance cases pinning both formats, so an independent implementation can be checked against the reference.

The problem. About 35 percent of unspent Bitcoin, a measured band of 34.911 to 35.005 percent at block 959,800, sits at addresses whose public keys are already visible on the chain. If a future protocol change disables spending from them, a holder must have recorded in advance that they controlled the address. Recording it afterwards is exactly what the change prevents.

The constraint. The obvious way to record it is to move the coins, which is public. For a holder whose safety depends on nobody knowing what they hold, that defeats the purpose. The people most exposed are the ones least able to act.

What PACT does. It creates a timestamped record that a holder controlled an address, without revealing which address, how much it holds, or who they are, and without any transaction attributable to them. Open source, MIT licensed.

VERIFIED ON THE BITCOIN BLOCKCHAIN

The pooling service's first live submission is anchored in block 974,627, six minutes after it was sent, routed over Tor. The batch held only padding and no member data, so the submission itself disclosed nothing — which is the property the design exists to provide. The OP_RETURN carries the timestamping calendar's aggregated root, with the batch root inside it.

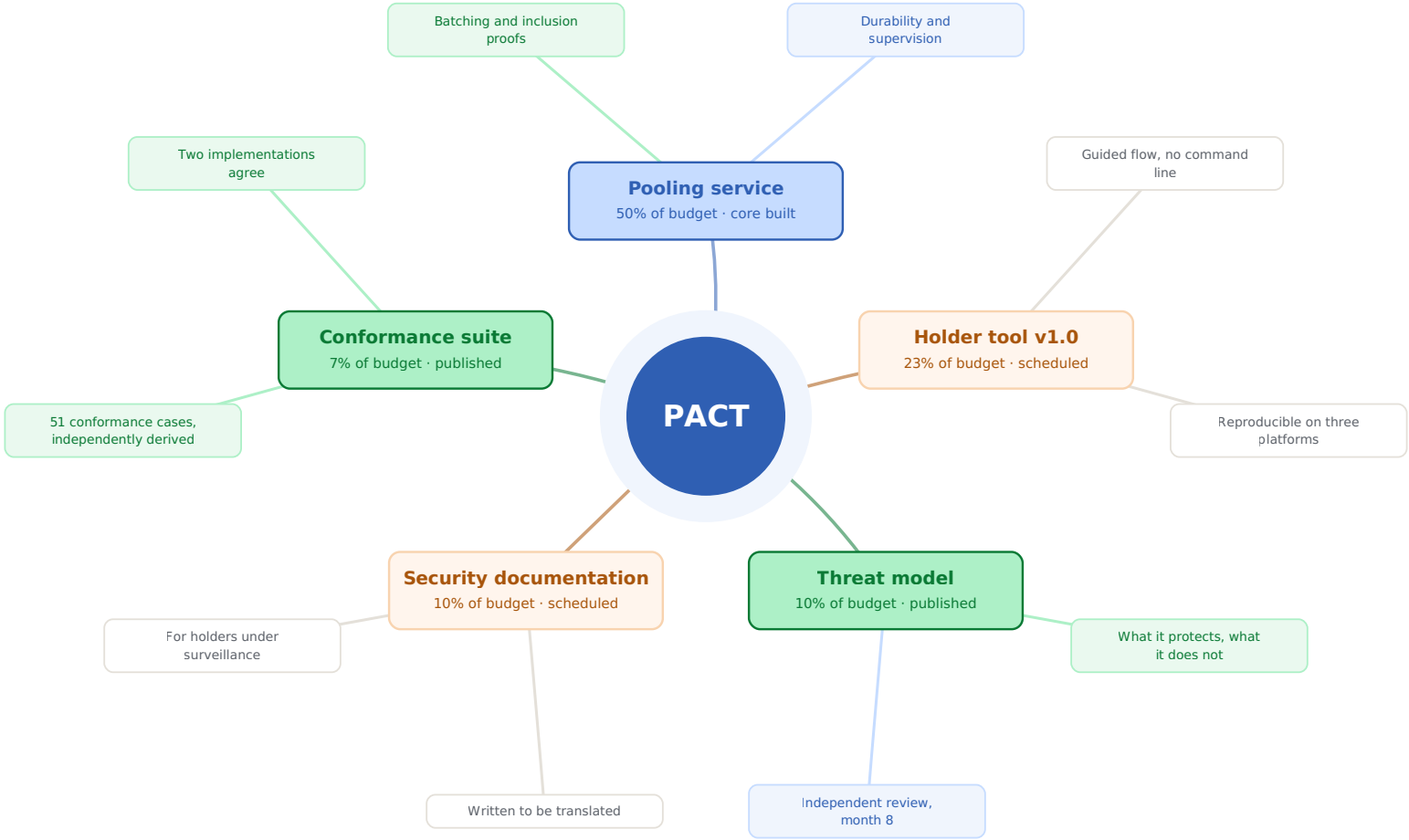
`tx 3b0498b9de5573db3ae48efdaab52b0bc335b9082be2890d579f6b26aa273948 · 2026-11-05 04:56:22 UTC`

Status reported against artefacts and tests. Months counted from grant start.

THE PROGRAMME

Five proposed deliverables

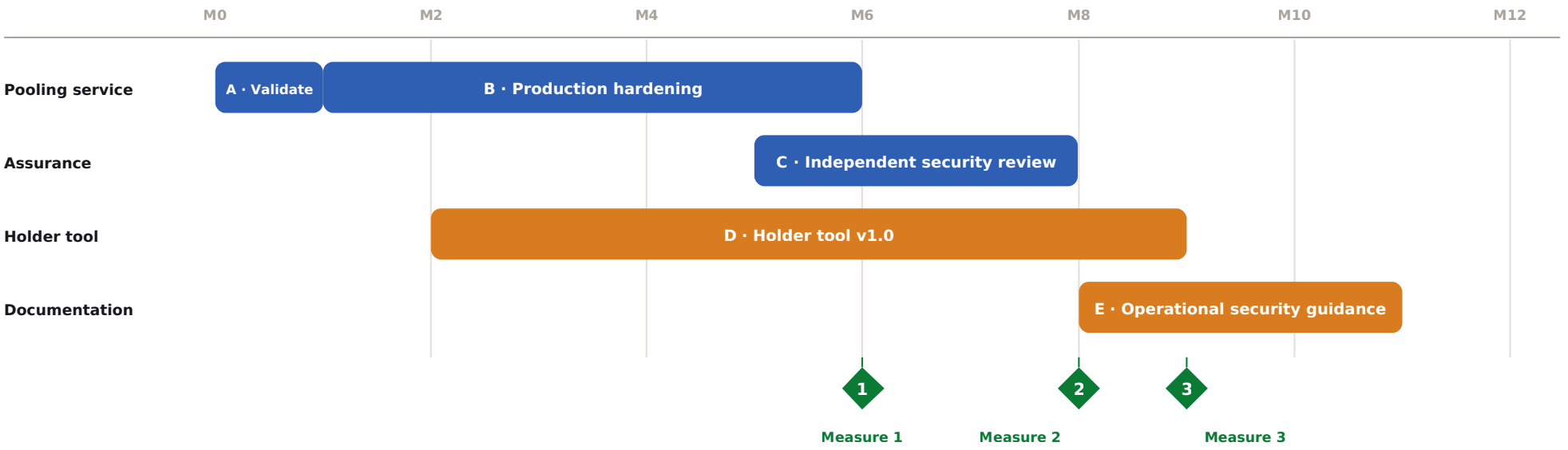
Three are complete or materially under way. The pooling service carries half the proposed budget and half of it is built. Percentages are the budget weights submitted on the application form.



DELIVERY

Timeline and committed measures

Months run from grant start. The two build tracks run in parallel; assurance follows the work it reviews. Diamonds mark the three success measures committed to on the application.



MEASURE 1 · MONTH 6

Pooling service published, running, and reproducible from source by an independent party

Three conditions. Published is a release. Running means an unbroken sequence of sealed intervals a reader can inspect. Independently reproducible means someone who is not the author rebuilds from source and obtains the same artefact.

MEASURE 2 · MONTH 8

Threat model published and reviewed by at least two outside reviewers with relevant security expertise

The document is written and published. The measure's weight sits in the review: a threat model is an argument rather than a measurement, so it cannot be self-certified and the author is the last person able to judge whether it is complete.

MEASURE 3 · AT RELEASE

Holder tool v1.0 released after usability testing with at least five non-technical testers

With the failure modes found and fixed documented. The record has to show what testers got wrong and what changed because of it, which is what makes the result useful to anyone building something similar.

METHOD

How progress is verified

A grant is a claim about the future, so the thing worth offering is a record of how claims get checked. Three practices the work is held to.

01

Corrections are written down in public

When something turns out to be wrong, the correction is recorded where the mistake was, not quietly overwritten. The conformance suite's own notes explain why its passing result is weaker evidence than it looks. The scheduling code opens by recording that an earlier plan cited the wrong source. The threat model states on its own face that nobody outside the project has reviewed it.

Published in the repositories, not just claimed

02

Specification before implementation

The commitment format is pinned by conformance vectors derived independently of the code that implements it, so an outside developer can check their own build against the reference rather than taking it on trust.

51 cases · two implementations agree

03

Independent review before release

Finished components are handed to an independent reviewer briefed to test them rather than confirm them. Nothing is released until every finding is closed and covered by a regression test that holds it closed.

Every finding closed and regression-tested

Where your network multiplies the grant

Four steps need people from outside the project rather than engineering time, and three of them are written into the success measures. Nobody is being hired and no budget is set aside for them: these are unpaid contributions, and the work is specified and open so that an afternoon is enough.

MEASURE 2 · MONTH 8

Two security reviewers

Relevant expertise, outside the project.

MEASURE 1 · MONTH 6

One independent engineer

To rebuild from source and confirm the artefact.

MEASURE 3 · AT RELEASE

Five non-technical holders

For observed usability testing of the holder tool.

DELIVERABLE 4

One field practitioner

Who supports users living under surveillance.