Name: Crossing bridges with confidence explainer

Category: Security

Paper title: *'Crossing with Confidence: Formal Analysis and Model Checking of Blockchain Bridges'*

Authors: Pyrros Chaidos, Pooya Farshim, Denis Firsov, Dimitar Jetchev, Aggelos Kiayias, Markulf Kohlweiss, and Anca Nitulescu

Paper: https://eprint.iacr.org/2026/292.pdf

Published:

Crossing bridges with confidence explainer

Major blockchain networks, worth a combined value of $3tn, cannot talk to each other directly. Instead, they rely on blockchain bridges: protocols that transfer information, such as asset ownership or smart contract state, between separate ledgers. Several high-profile bridges have relied on a small, fixed committee to determine the state of the sending chain, an arrangement that has led to serious breaches, including the Ronin attack ($625M stolen), the Poly Network attack ($611M stolen), and the compromise of Solana's Wormhole bridge ($325M in assets affected). Even sound trust assumptions have suffered subtle, but costly and technically sophisticated attacks proving that that security has to carry through from design into implementation.

A formal security treatment for bridges

Research by the Input Output Research (IOR) team, alongside collaborators from the University of Edinburgh and Microsoft Azure AI Platform, introduces the first formal, code-based security treatment for blockchain bridges. The work defines explicit security properties for bridges and applies them to five architectures already used in practice: direct observation, fixed committee, consensus certificate, zero-knowledge (ZK), and a new advanced threshold signature (ATS) design. Each is backed by a pen-and-paper security proof.

The ATS design lets bridge committees rotate every epoch, drawn fresh from the sending chain each time, the way block-production committees already do. Unlike older threshold-signature setups, each signer generates their own key rather than going through a shared key-generation ceremony, removing a step that has historically been a target for attackers.

The research goes a step further by automatically checking these definitions and protocols for logical flaws using Quint, a specification language and model checker closely related to TLA+. This is the first systematic application of model checking to bridge protocols expressed in the Universal Composability (UC) framework, and it uncovered bugs, some subtle, in nearly all of the initial functionality definitions the team checked, even ones that looked correct on inspection.

Why cross-chain security matters

This research has practical benefits for blockchain ecosystems that rely on moving assets and information between chains:

Stronger guarantees before deployment: catching design flaws through automated checking, rather than after a bridge goes live, reduces the risk of the kind of exploits that have already cost the ecosystem over $1.5bn.

A path beyond fixed committees: the ATS bridge lets bridge committees rotate the way block-production committees already do, removing the single point of failure that fixed committees represent.

Broader applicability: because the proofs don't rely on assumptions specific to any one blockchain's design, the results can be applied to a wider range of blockchains than prior bridge analyses.

The bridge protocols are generic with respect to their underlying chains, and can be used to connect a wide range of blockchains, as long as the receiver chain supports smart contracts. (IOR is developing a Bitcoin bridge as complementary work to support this concept.)

How the ATS bridge works

The advanced threshold signature (ATS) design replaces a fixed, static committee with one that rotates and refreshes itself over time:

- **Committee selection**: At the start of each epoch, a new committee is drawn fresh from the sending chain's own validator set — the same way block-production committees are chosen. No committee sits in place indefinitely.
- **Key generation**: Rather than running a shared key-generation ceremony (where the committee jointly produces one combined key), each signer generates their own key independently.
- **Signing**: When a cross-chain transfer needs to be certified, the rotating committee produces a threshold signature attesting to the state of the sending chain, which the receiving chain can verify.
- **Rotation**: At the next epoch boundary, the process repeats with a freshly drawn committee, so no single group of signers retains long-term control over the bridge.

Learn more

For a deep cryptographic dive into the details and design of this protocol, read the 'Crossing with Confidence: Formal Analysis and Model Checking of Blockchain Bridges' paper by Pyrros Chaidos, Pooya Farshim, Denis Firsov, Dimitar Jetchev, Aggelos Kiayias, Markulf Kohlweiss, and Anca Nitulescu.