galois

Helping the Interchain Foundation demonstrate the resilience of the Tendermint protocol

Guaranteeing you can trust the protocol that secures $75B+ in assets

At Galois we offer mathematically rigorous security analysis for companies looking to increase trust in their most critical software. The organizations we help have some of the most demanding security requirements in the world. They include the largest global cloud providers and United States intelligence agencies.

> *Galois's proofs of the Tendermint protocol in Ivy gives us assurance in the protocol correctness that is much higher than standard English specifications, code simulations, or model checking. In addition to the thorough correctness assurance, we're inspired by Galois's approach to make formal verification more developer friendly which we continue to build upon at Informal Systems.*
>
> **Zarko Milosevic,**
> Chief Scientist at Informal Systems

Company name
Interchain Foundation

Industry
Information Technology

Website
Interchain.io

Tendermint: Trusted consensus protocol

Trust is imperative and there is no room for error when it comes to the Tendermint protocol. Tendermint is the core protocol that guarantees the integrity of blockchains built on the Tendermint SDK — including the Binance DEX and many blockchains in the COSMOS Network. COSMOS is supported by the Interchain Foundation, a non-profit that researches and develops decentralized networks.

The Tendermint protocol secures an estimated $75B+ in digital tokens, and there are 200+ projects in Tendermint's blockchain ecosystem. Businesses rely upon the Tendermint protocol and their viability depends on whether their customers trust this technology to secure their assets.

Challenge

1. The Tendermint protocol allows untrusting parties to agree on the state of a financial ledger — a role traditionally fulfilled by a bank — and secures about $75B+ in digital tokens.
2. Tendermint's Fork Accountability mechanism detects when some parties are attempting to commit fraud. How can businesses trust the Tendermint protocol is grounded in solid evidence?

Solution

1. Galois's formal verification methods are designed to find errors. We build a mathematical model of the protocol and then use logical reasoning to prove something works for all possible scenarios.
2. In the Tendermint case, Galois created a proof *guaranteeing* that attackers will be detected and punished — regardless of how many parties collaborate or how clever they are.
3. Galois provided the highest level of assurance for this critical part of Tendermint's architecture.

Challenge: Detect and defend against attacks in an open, untrusted environment

The Tendermint protocol is a set of communication rules enabling untrusting parties to agree on the state of a financial ledger, i.e. who owns what, and update the ledger with new financial transactions. Maintaining a ledger for third parties is traditionally done by a bank. With Tendermint, there is no need for a trusted bank; instead, the protocol guarantees that, as long as at least two-thirds of the parties are honest and responsive, the ledger functions correctly.

Tendermint also detects when some of the parties sharing the ledger deviate from the protocol to try to defraud other parties. This is Tendermint's Fork-Accountability mechanism. By confiscating the deposits of the offending parties, the Fork-Accountability mechanism creates a strong incentive against attacking the protocol and allows parties to trust that their assets are secure. In this situation, any mistakes in the protocol could result in financially devastating security breaches. How can businesses within the Tendermint ecosystem trust that the Tendermint protocol is grounded in solid evidence?

Solution: Use formal verification to mathematically prove that, in all possible attack scenarios, the Fork-Accountability mechanism works as intended

Because trust in the Tendermint consensus protocol is essential to the development of the Tendermint ecosystem, the Interchain Foundation asked Galois to work with the Tendermit experts at Informal Systems to ensure that it contains no mistakes.

Galois relies on a mathematical technique called formal verification to find errors. Instead of relying on human intuition or testing of inputs, our team of computer scientists builds a mathematical model of the protocol and then uses logical reasoning to prove that the desirable properties hold once-and-for-all, in all possible scenarios.

Galois scientists employ user-friendly, yet machine-checkable languages to help communicate their work to the Tendermint community while enabling automated proof-checking to rule out any errors. Additionally, our mathematical models are executable, which allows engineers to run them and check that the model's behavior corresponds to their understanding of the protocol.

In the case of Tendermint, our proof demonstrated that any bad behavior by parties trying to subvert the financial ledger is inevitably punished — in other words, regardless of how many parties collaborate and how clever the attackers are, we *guarantee* the attackers will be detected and punished. This provides the highest level of assurance for a critical part of Tendermint's architecture.

Iron-clad verification that your solution works as intended

Formal verification provides dramatically more confidence and trust than audits based on human examination or testing. We used what's known as a *mechanically-checked proof* — a proof written in a machine-readable language that is checked by a program for any logical flaws. In this case, Galois's audit allowed the Interchain Foundation to bolster trust in the Tendermint protocol.

How can we help?

From U.S. defense and intelligence agencies to global technology companies working on the edge of what is technologically possible, we work to ensure that you don't have to blindly trust the software everything relies on.

Do you have software that you must rely on without compromise?

We'd love to learn about your business and see if we can help.

Portland, OR
Arlington, VA
Dayton, OH

contact@galois.com
Tele. 503.626.6616
Fax 503.350.0833