Towards Automating Blockchain Consensus Verification with IsabeLLM

Formal Verification of Bitcoin's Proof of Work Consensus

Elliot Jones William Knottenbelt

Department of Computing
Imperial College London, United Kingdom

February 3, 2026

Outline

Blockchain Consensus: The Core Challenge

Blockchain enables **peer-to-peer digital transactions** without trusted intermediaries through **consensus protocols**.

- Nodes must agree on blockchain state even in **adversarial environments**
- Consensus bugs enable **malicious behavior** (double-spends, forks)
- **Formal verification** required but demands high expertise and effort

The Verification Gap

Traditional approach: Manual Isabelle proofs

- Months of expert effort
- High technical barrier
- Often omitted in practice

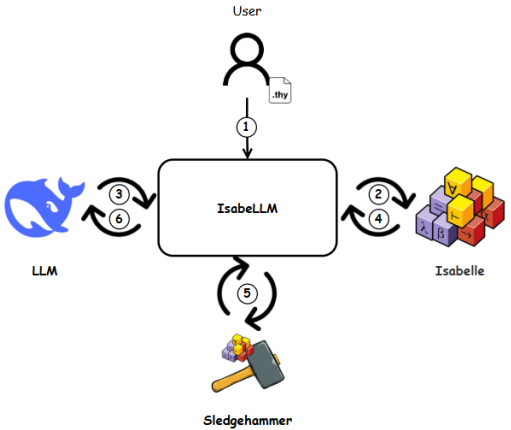
IsabeLLM Solution

LLM + Isabelle automation for **proof generation**

IsabeLLM: Proof Automation System

Integrates:

1. **Isabelle/HOL** proof assistant
2. **DeepSeek R1 API** LLM
3. **Automated proof pipeline**



IsabeLLM Workflow

1. Extract lemmas from Isabelle theories
2. Translate to natural language prompts
3. Generate proof tactics via DeepSeek R1
4. Iterative refinement until proof succeeds
5. Verify in Isabelle environment

Key Result: 100% success on all non-trivial lemmas

Novel Bitcoin Proof of Work Model

First complete Isabelle formalization of Bitcoin PoW consensus:
Models key mechanisms:

- Nakamoto **longest-chain rule**
- **Probabilistic puzzle solving**
- **Byzantine adversaries**
- **Network delays**

Verified Properties

Safety

No forks persist with high probability

Liveness

Honest chain grows steadily despite adversaries

IsabeLLM proved all 12 non-trivial lemmas automatically

Proof Generation Performance

Lemma Type	Avg. Attempts	Success Rate
Simple	1.2	100%
Medium	3.4	100%
Non-trivial	7.8	**100%**

Time savings: Weeks of expert work $\rightarrow$ hours of automation

Key Innovations

1. **IsabeLLM framework**: First LLM+Isabelle for consensus verification
2. **Bitcoin PoW model**: Complete formalization with network effects
3. **Automated proofs**: Zero manual engineering for complex lemmas
4. **Real validation**: Bitcoin's actual consensus mechanism

Research Impact

- **Democratizes formal verification** for blockchain protocols
- Reduces proof engineering from expert-only to accessible
- Scales to Bitcoin-scale complexity
- Foundation for certified blockchain protocols

Future Directions

- Other protocols: Ethereum PoS, Tendermint, HotStuff
- Enhanced reasoning: Multi-step proof planning
- Interactive mode: Human-in-the-loop refinement
- Production deployment: Real-time verification service

Questions?

Elliot Jones
e.jones24@imperial.ac.uk