# Towards Automating Blockchain Consensus Verification with IsabeLLM

## Formal Verification of Bitcoin's Proof of Work

Elliot Jones  William Knottenbelt

Department of Computing
Imperial College London, United Kingdom

February 3, 2026

# Outline

# What is Blockchain?

- Blockchain enables **peer-to-peer digital transactions** without trusted intermediaries
- Relies on **consensus protocols** for agreement between nodes
- Must work correctly even in **adversarial environments**

**Key Challenge**

Consensus must be designed and implemented correctly to prevent malicious behavior

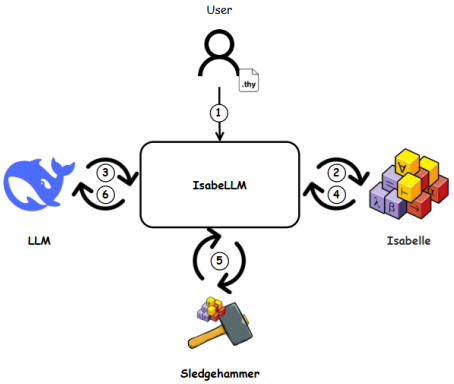
# The Problem with Consensus Verification

- Consensus bugs can lead to catastrophic failures
- **Formal verification** ensures correctness
- Requires high expertise and significant effort
- Often omitted during development

# Introducing IsabeLLM

**IsabeLLM** integrates:

- **Isabelle** proof assistant
- **Large Language Model** (DeepSeek R1 API)



# IsabeLLM Key Features

- **Automates proof generation**
- **Assists human experts**
- Generates correct proofs for non-trivial lemmas
- Reduces formal verification barrier to entry

# Bitcoin's Proof of Work Consensus

- Nodes compete to solve computational puzzles
- Longest valid chain wins
- Probabilistic finality (no absolute guarantees)
- Novel formal model developed using IsabeLLM

# Verification Results

## Key Achievement

IsabeLLM generated **correct proofs** for **all non-trivial lemmas** in the Bitcoin PoW verification

- Verified liveness properties
- Verified safety properties
- Handled complex adversarial scenarios

# Key Contributions

1. **IsabeLLM**: Novel LLM+Isabelle integration for proof automation
2. **Novel Bitcoin PoW model** with full formal verification
3. Demonstrated effectiveness on complex real-world protocol
4. Generated correct proofs for all non-trivial lemmas

# Future Work

- Extend to other consensus protocols (Ethereum, Tendermint)
- Improve LLM reasoning capabilities
- Develop interactive proof assistance interface
- Scale to larger protocol models

# Thank You

## Questions?

Elliot Jones
e.jones24@imperial.ac.uk