Professor Bogdan Warinschi
School of Computer Science
Merchant Venturers Building
Woodland Road, Clifton
Bristol BS8 1UB, United Kingdom
csxbw@bristol.ac.uk

Professor Andrzej Tarlecki
Chair, Academic Council of
Computer and Information Sciences
University of Warsaw

20 September 2026

Report on the doctoral thesis of Grzegorz Fabiański

An Analysis of Security of Blockchain Protocols and the Role of Formal Methods

Supervisor: Professor Stefan Dziembowski
University of Warsaw, April 2026

The thesis contains substantial original research on blockchain security and formal methods and provides a sufficient basis for the award of a PhD. My comments concern the presentation and several local corrections; they do not alter this positive assessment.

Research contributions

Chapter 3 establishes a communication lower bound for a class of Plasma protocols. Its information-theoretic proof explains how unavailable data can force costly on-chain communication, identifying a limitation that protocol design must confront.

Chapter 4 verifies funds security and bounded recovery for a simplified two-party Lightning channel in Why3. Its small participant interface usefully separates implementation details from the general security argument. The model handles adversarial scheduling and unbounded histories, while omitting HTLCs, multi-hop payments, fees and a full refinement to Bitcoin. These are reasonable limits; the result does not establish payment liveness or verify a production client.

Chapter 5 formalizes symbolic cryptography in Lean, proves a conditional computational soundness theorem and applies it to garbled circuits. The reusable separation of symbolic reasoning from cryptographic reductions is a strength. The paper “Computationally Sound Symbolic Cryptography in Lean” received the CSF 2026 Distinguished Paper Award, complementing the recognition represented by the other publications at ITCS and Financial Cryptography.

For these coauthored papers, the contribution statement on page 17 identifies substantial personal work: the main Plasma lower-bound proof, leadership of the Lightning verification project and its interface abstraction, and approximately half of the Lean formalization, including the pseudo-fixpoint technique. This demonstrates the breadth and technical maturity expected of doctoral research.

My examination of the formal developments did not include an independent replay of the complete Lean and Why3 proofs.

Presentation and synthesis

The thesis has a credible common theme, but its presentation remains close to a collection of papers. The main opportunity for improvement is to explain more clearly what the results collectively establish. The introduction devotes too much space to general background and illustrative examples; a more focused account of the research questions and their connections would be more useful. A short concluding discussion could compare the chapters' assumptions and guarantees, particularly the congestion problem motivating the Plasma work and the bounded ledger delivery assumed in the Lightning verification. It would also help to explain more directly how Chapter 5's general cryptographic framework contributes to the thesis's broader argument. This is a weakness of synthesis, not of the underlying research.

Specific corrections and clarifications

The summary on page 11 should describe the Plasma theorem in terms of aggregate on-chain communication or the communication cost of an individual exit, subject to the locality and collateral assumptions. A bound on transcript length does not establish that a constant fraction of users must communicate, or that communication grows linearly with the monetary value withdrawn. It would also be useful for the discussion of collateral to indicate when the bound becomes uninformative.

There is a minor bug in the definition of forced on-chain action on page 34: "did not receive any order" should read "did not receive any exit order". Adding "exit" agrees with the explanation below the definition and with transcript T2, whose users received payment orders but no exit orders.

Two related passages would benefit from clarification. The discussion following Theorem 1 on page 34 excludes "uniquely attributable" forced on-chain actions, although the theorem's first alternative concerns actions without uniquely attributable faults. Please clarify which class of protocols is intended and why that alternative is excluded. In the proof of Lemma 1 on page 36, security is invoked to rule out attributing faults to corrupt parties. Please clarify how protection against falsely accusing honest parties, together with equality of transcript distributions, establishes the conclusion. These appear to be issues of exposition.

In Chapter 5, the normalization rules on page 74 should use Boolean constants rather than VarB 0 and VarB 1, and follow the code's swap convention. The pseudo-fixpoint argument on page 80 needs the restriction to the appropriate key universe. The final version should also identify immutable artifact versions and provide reproducible build instructions.

Recommendation

I give a positive assessment of the thesis and recommend that the candidate address these comments in the final version. On scientific grounds alone, the thesis is a strong candidate for an honorary distinction, a judgment reinforced by the CSF Distinguished Paper Award. My hesitation in recommending that distinction reflects the standards of thesis presentation to which I am accustomed in the UK, where I would expect a substantially more unified account of the research. I therefore defer to reviewers more familiar with Polish academic standards on how these presentational reservations should weigh in the decision on distinction.

Professor Bogdan Warinschi
Professor of Computer Science
University of Bristol

