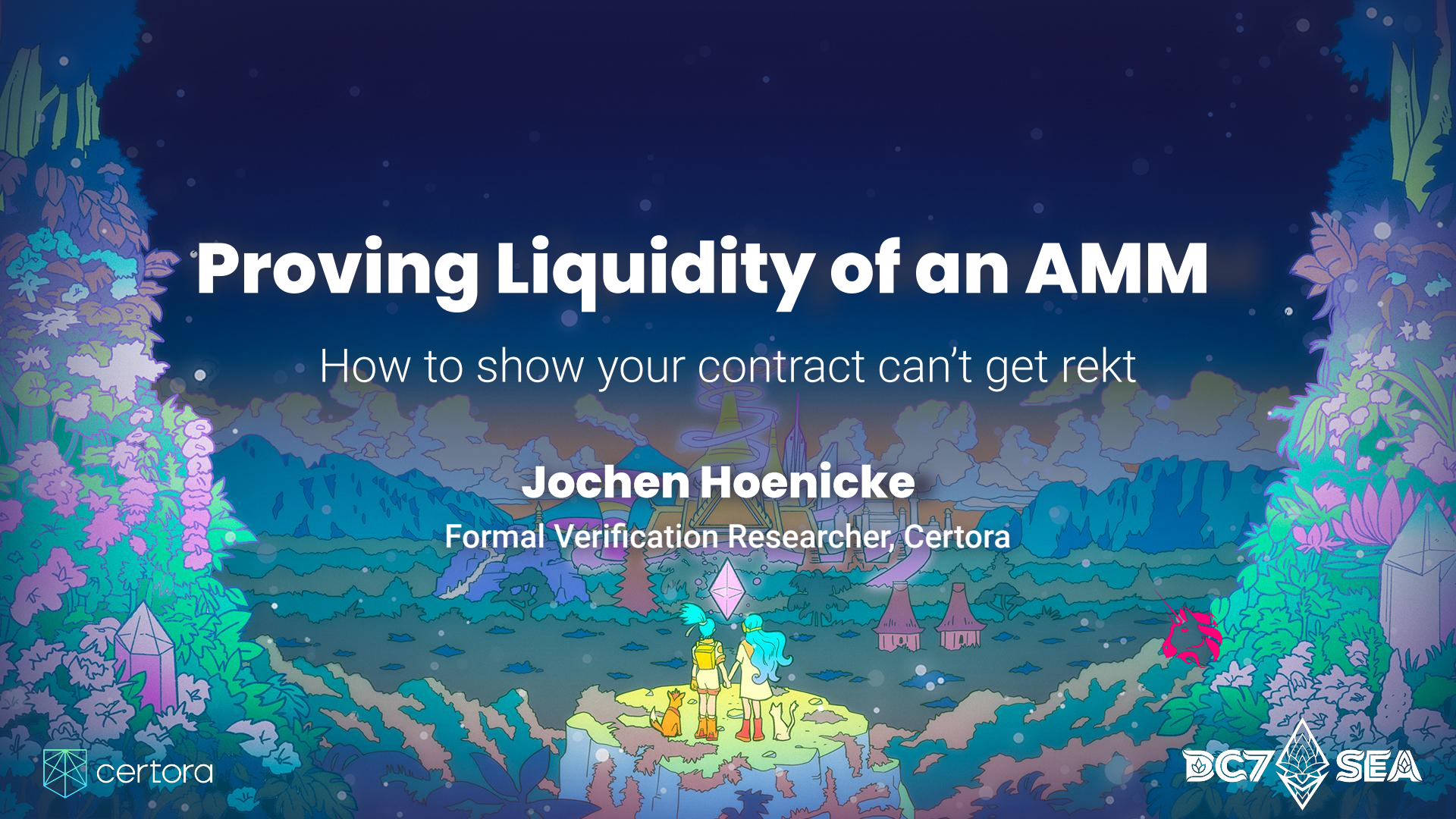
Proving Liquidity of an AMM

How to show your contract can't get rekt

Jochen Hoenicke

Formal Verification Researcher, Certora



certora

DC7 SEA

Section 1

AMM and Liquidity

Automated Market Maker(AMM)

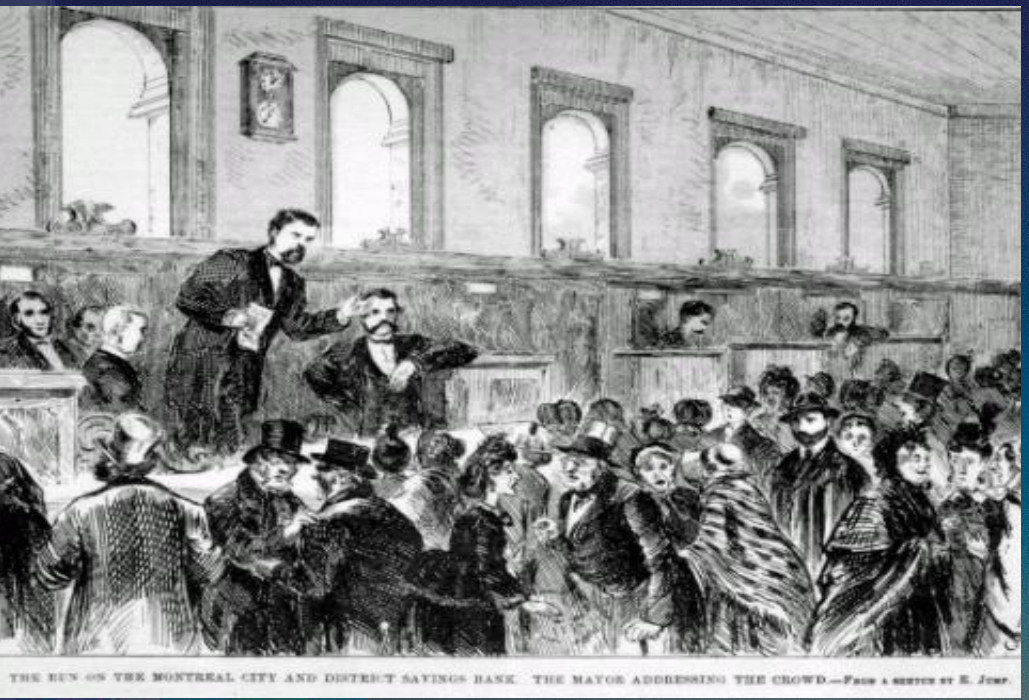
An AMM is a decentralized exchange having two major actors.

- **Traders**
- **Liquidity Providers**

Liquidity Providers are the most vulnerable

- The AMM smart contract has custody over their funds.
- Their tokens are automatically traded by the contract.
  - We ignore “impermanent losses” from trading, though.
- Bugs in contract can be catastrophic for liquidity providers.

Desired Property: Contract is always liquid



THE RUN ON THE MONTREAL CITY AND DISTRICT SAVINGS BANK. THE MAYOR ADDRESSING THE CROWD.—From a sketch by E. Jump.

Liquid means: Money can always be withdrawn

Even during a bank run, liquidity providers can withdraw their fair share.

1. Contract has enough funds
2. Withdraw never reverts

certora

Formal Verification for Uniswap v4

Uniswap v4 has “scary” features

- Permissionless: everybody can add a new pool.
- All tokens of all pools are kept in a single contract.
- Hooks provide a mechanism to customize pools.

Attack Vectors from Unknown Code

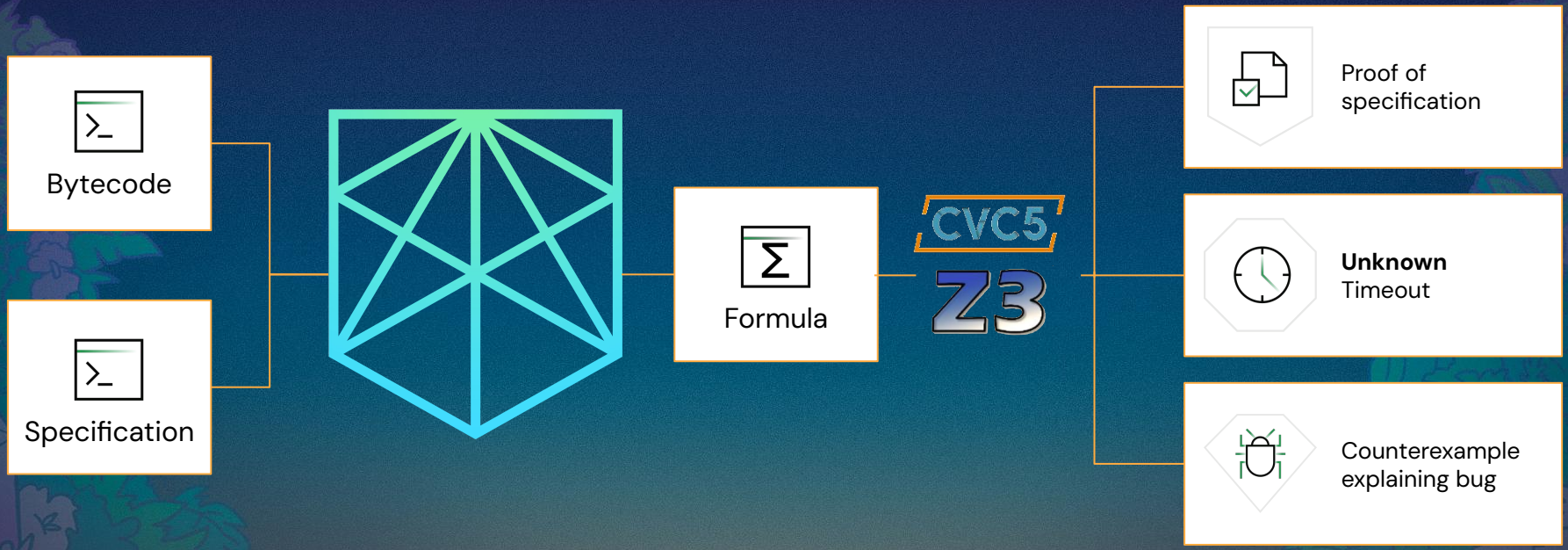
- Malicious ERC-20 token,
- Malicious Custom Hooks.

Section 2

Formal Verification

certora

Static Code Analysis



certora

Assumptions for Unknown Code

ERC-20

- Balance only changed by transfer/mint/burn
- Only owner and approved accounts can transfer/burn
- Only receiver pays fees (if any)
- Transfer succeeds if balance sufficient
- Balance doesn’t change when transferring other tokens.

Hook

- For liquidity: no withdraw hook.

Proof Method: Inductive Invariants

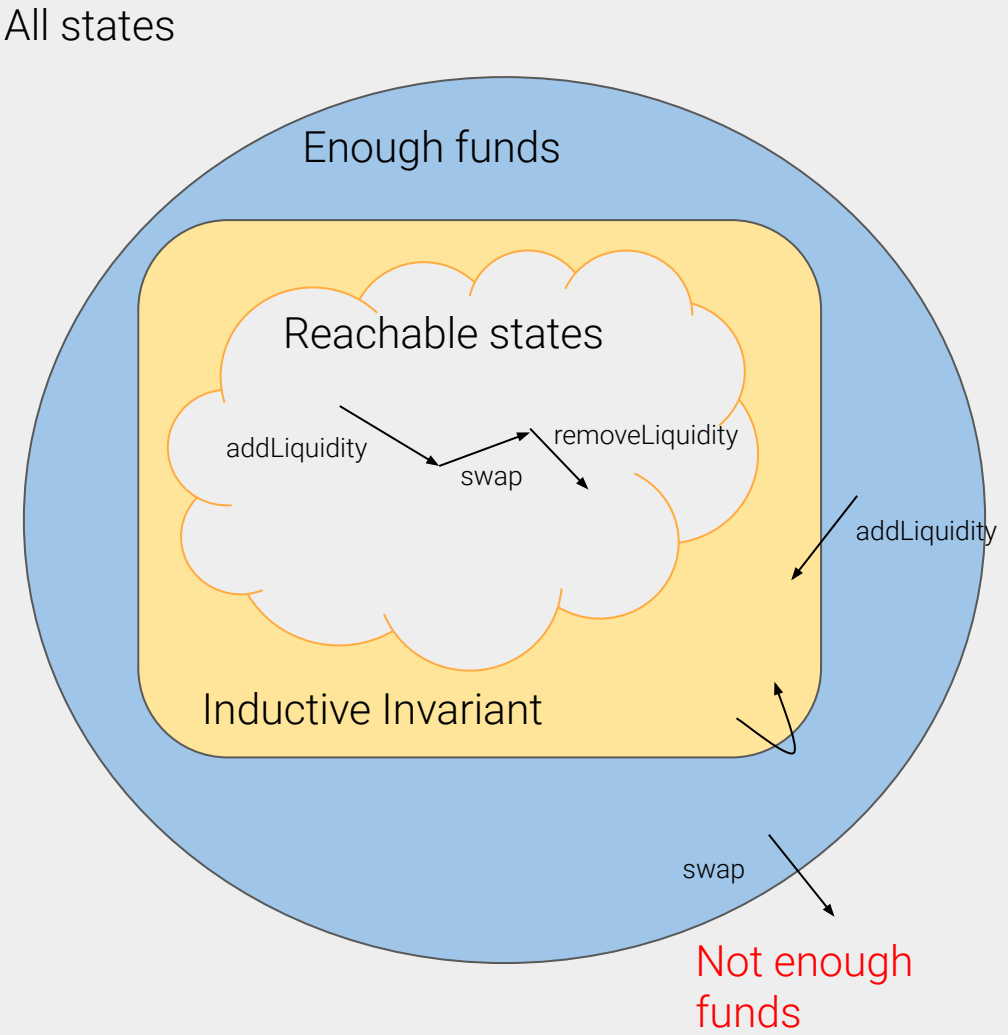
Desired Property:

Contract has enough funds

Inductive invariant:

enough funds + consistent accounting

certora



Challenges when Proving Uniswap v4

Problems

- Rounding errors break invariant
- Need to reason about sums

$$\sum_{\text{Pos } p} \sum_{\text{Tick } t} \mathsf{a}(p, sp, t) = \sum_{\text{Tick } t} \sum_{\text{Pos } p} \mathsf{a}(p, sp, t)$$

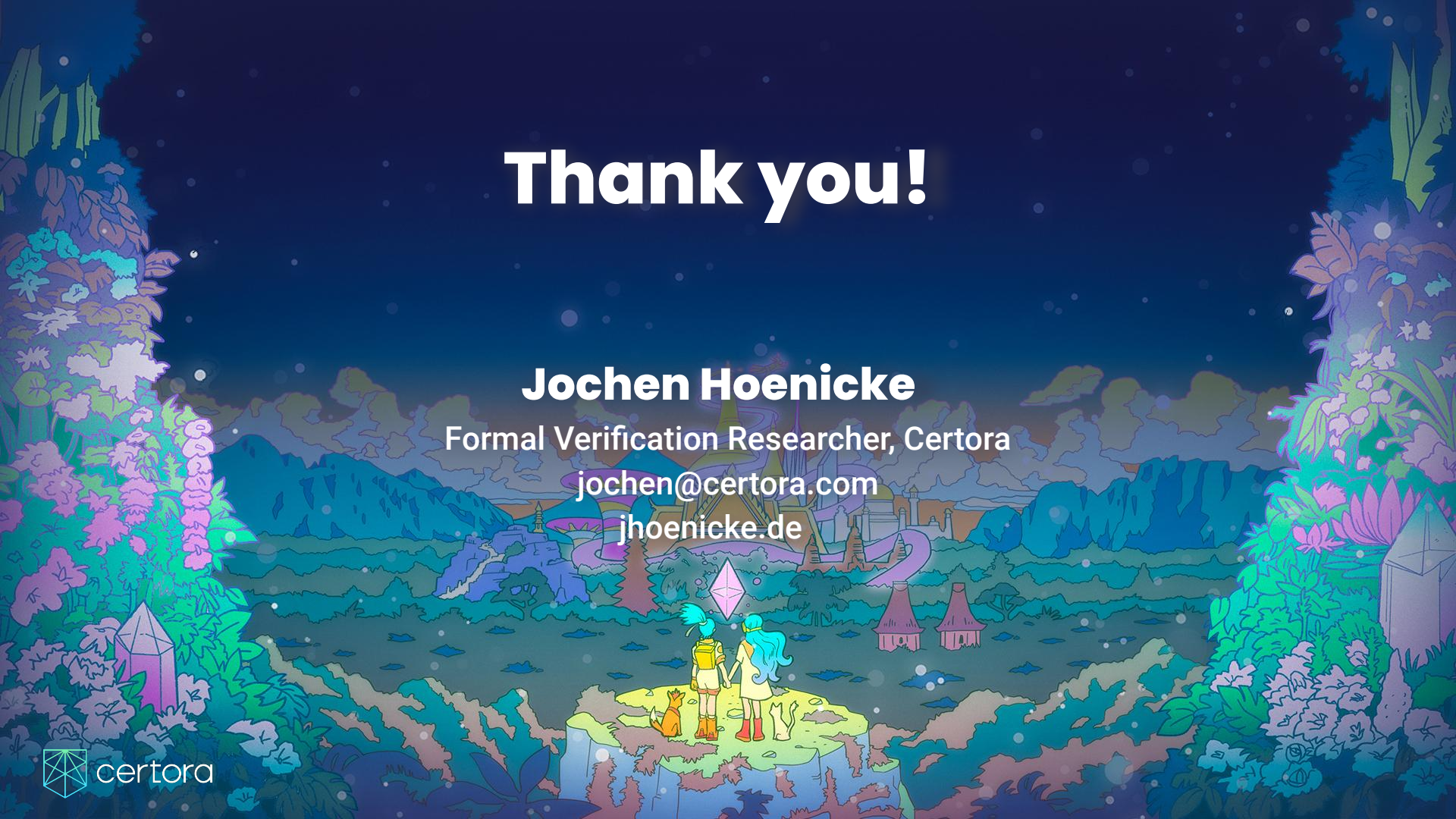
- Undecidable non-linear math:
  `amount_delta, tick2sqrtprice`
- Calls to external hooks
  with potential callbacks

Solutions

- Spec uses high-precision fixed point
  $\forall i < 2^{256} : \text{PRECISION} \bmod i = 0$
- Use arrays to store partial sums,
  update when a position is changed.
- Abstract with uninterpreted functions.
  + axioms for monotonicity
- Strong invariants (preserved by hooks).
  Start with arbitrary state after hook.

certora

Enough Funds + Consistent Accounting is an inductive invariant


Thank you!
Jochen Hoenicke
Formal Verification Researcher, Certora
jochen@certora.com
jhoenicke.de
certora