The Blockchain Bridge That You Dream About

Martin Derka, Ph.D.
Head of New Initiatives, Quantstamp
What Is A Bridge?
Assets are being custodied on the main chain, and a form of debt token is issued to the user on the target chain.
What Is A Bridge (Withdrawal)

The user burns the debt token on the other chain and the communicator tells the custodian that funds can now be released.
Section 2

The Menu
The Menu

- **Speed**
  Bridging should happen quickly

- **Finality**
  Once bridging happens, it will not be rolled back

- **Atomicity**
  Everything happens at once on both chains - wouldn’t it be cool?

- **Security**
  Losing funds is never fun
The Menu

- Censorship Resistance
  Everyone should be able to use the bridge
- Availability
  We should be able to send transactions to the bridge whenever
- Liveness
  All transactions should eventually get processed
- Pausability
  If one chain has troubles, we would like to pause the bridge
The Menu

- **Liquidity**
  We would like to be able to bridge arbitrary amounts

- **Expressive Power**
  We would like to be able to bridge arbitrary assets (ERC20, ERC721)

- **Cost Efficiency**
  Bridging should be cheap

- **Privacy**
  Bridging should be private

- **Transparency and Auditability**
  Everyone should be able to monitor the bridge activity
Section 3

Why Is This Hard?
Trade Offs

- **Speed vs. Finality**
  Finality has to be reached on two chains, so it is unlikely to be fast

- **Availability vs. Pausing**
  Paused bridge is not available

- **Security vs. Liquidity**
  Limiting liquidity often serves as an additional security measure
Thank you!

Martin Derka, Ph.D.
Head of New Initiatives, Quantstamp
martin@quantstamp.com

@quantstamp