TRAIL OF BITS

# ARDC - Trail of Bits



# Who are we?

- **Since 2012, Trail of Bits provides technical security assessment and advisory services to some of the world's most targeted organizations**
  - Blockchain: Aave, Algorand, Balancer, Bitcoin SV, Curve, Chainlink, Compound, Offchain Labs, Optimism, Solana, Starknet, Yearn, …
    - 300+ blockchain security reviews
    - Worth 30+ years of security engineer efforts
  - Non blockchain: Epic Games, Google, HashiCorp, Kubernetes, Microsoft, Zoom, …
- **Leading in highly specialized technology**
  - Appsec, Blockchain, Cryptography, Machine learning, Program analysis

# Our goal

- **Ensuring greater security of the Arbitrum ecosystem, by leveraging**
  - Dedicated expertise
  - Open source tools
  - Extensive security research

# Our proposal

- **Review of code updates proposals**
  - Identifying flaws on upgrades
- **Invariants development**
  - Be proactive in providing long term security
- **Tooling**
  - Enable developers with static analysis, visualization tools, governance helpers, ..
- **Educational material**
  - Public content (blogpost, videos, ....)
- **Additional services, based on the ARDC needs**
  - Design review, threat modeling, appsec/crypto review, guidance on incident response plan

# Why Trail of Bits?

- **Unique technical expertise on Arbitrum**
  - Since 2021, 180+ engineer weeks on Arbitrum
  - All included, ArbOS, Nitro, Stylus, …
  - Core protocol, not just deployed projects
- **Unique tooling and open source experience**
  - We've developed industry-leading security tools, all open source
  - Not just one time effort, but continuous maintenance, ex:
    - Slither: 4.9k stars on github (since 2018)
    - Echidna: 2.5k stars on github (since 2018)
- **Educational material**
  - Secure-contracts.com, 10+ hours of fuzzing workshop, 50+ technical blogposts & academic papers, 40+ industrial presentations

# Conclusion

- **Proposal**
  - Code update reviews, tooling & educational materials
- **Why Trail of Bits?**
  - Unique Arbitrum expertise & demonstrated open source achievements
- **By partnering with Trail of Bits, the ARDC will not secure its ecosystem but set a new standard in the blockchain security**

***I would love your feedback: @montyly (twitter/telegram)***