Understanding Crypto Markets Security

Dan Guido - CEO, Trail of Bits

Trail of Bits

- We help solve the hardest challenges in software security
- Unmatched expertise: 140 research engineers w/ 20 in blockchain security
- Worked with DARPA, DoD, tech, and entire blockchain industry
- Have secured internal operations and blockchain code
- CEO: Product of NSF SFS/CyberCorps, dedicated to getting software right

Things are not what they seem

Perception

- Everyone is getting hacked and losing millions
- The industry is awash in scams and schemes
- Security is mostly an afterthought

Reality

- Very difficult for orgs to keep up
- Industry is dominated by awful marketing
- Some of our clients are the most mature and security-conscious companies we work with

The field moves fast

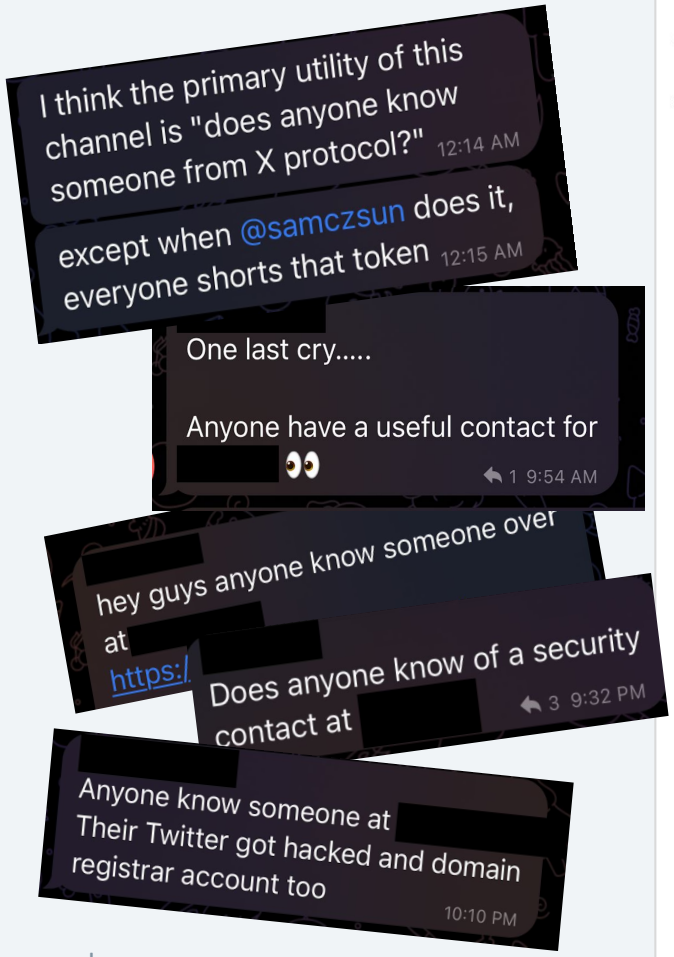
- A firm six months behind the curve on security is already woefully behind, we ourselves can barely keep up
- Standards in other industries - NIST CSF, SOC-2, PCI - don’t and won't work here
- Today looks nothing like ICOs of 2017: bridges, L2s, DeFi, composability
- Criminals have also become more resourceful and sophisticated: composability bugs, flash loans, price oracle manipulation

The problems we’re solving today didn’t exist 5 years ago

Before ~2020	After ~2020
• Arithmetic overflow • Lack of access controls • Reentrancy	• Price Oracle Manipulation • Slippage • Cross contract reentrancy • Third party integrations

Information is public and platforms are shared

- Breaches on public on social media before orgs can react; Twitter, Discord, Telegram will know instantly
- Inverted view on what is ‘secret’ - all contracts and transactions are inspectable by anyone, by design
- Opportunity to learn – you can walk-through blockchain attacks step-by-step
- Every code change is critical: safe today doesn’t mean safe tomorrow

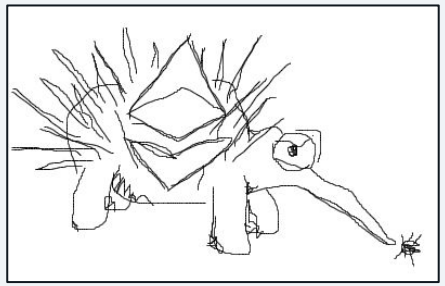


rekt

1. **Ronin Network - REKT** *Unaudited*
   $624,000,000 | 03/23/2022
2. **Poly Network - REKT** *Unaudited*
   $611,000,000 | 08/10/2021
3. **BNB Bridge - REKT** *Unaudited*
   $586,000,000 | 10/06/2022
4. **SBF - MASK OFF** *N/A*
   $477,000,000 | 11/12/22
5. **Wormhole - REKT** *Neodyme*
   $326,000,000 | 02/02/2022
6. **Euler Finance - REKT** *Sherlock*
   $197,000,000 | 03/13/2023
7. **BitMart - REKT** *N/A*
   $196,000,000 | 12/04/2021
8. **Nomad Bridge - REKT** *N/A*
   $190,000,000 | 08/01/2022
9. **Beanstalk - REKT** *Unaudited*
   $181,000,000 | 04/17/2022
10. **Wintermute - REKT 2** *N/A*
    $162,300,000 | 09/20/2022

The bar is higher for blockchain

- Current blockchain tools are rudimentary,, yet…
- Blockchain code requires rocket-level safety assurances
- Every code change is critical – safe today doesn’t mean safe tomorrow
- AI isn’t going to save blockchain security; need a scalpel, not a paintbrush
- Existing best practices are necessary but insufficient: we need more research



SLITHER

MANTICORE

Summary

Key takeaways

- Blockchain companies are motivated to fix security issues and many are very security-conscious
- Blockchain's security foundation shifts incredibly fast and requires holistic understanding of financial and technological concepts
- Public nature of blockchain presents enormous learning opportunity
- Improved tooling and continuous testing is deeply needed; motivation and desire is not enough

… So how do we have a conversation about improving controls?

Does your protocol pass The Rekt Test?

Our checklist allows protocols to examine their own procedures and create best practices.

- ❑ Have you documented all actors, their roles, and their privileges?
- ❑ Does your key management system require multiple humans and physical steps?
- ❑ Do you have a written and tested incident response plan?
- ❑ Have all employees undergone positive identification and background checks?
- ❑ Does someone on your team have security defined in their role?
- ❑ Does access to production systems require hardware security keys?
- ❑ Do you use the best automated tools for discovering security issues in your code?
- ❑ Have you defined key invariants for your system and do you test them on every commit?
- ❑ Have you received an external audit and do you run a vulnerability disclosure or bug bounty program?
- ❑ Have you documented all the external services, contracts, and oracles you rely on?
- ❑ Have you documented the best ways to attack your own system?
- ❑ Have you considered and mitigated avenues for abusing users of your system?

Resources

The Rekt Test

Are blockchains decentralized?

246 findings from audits

65 open source tools

Smart contract best practices

Contact

@dguido

dan@trailofbits.com

trailofbits.com