Private TREAT

Devere Anthony Weaver

COSC670 – Cryptocurrencies and Blockchain

Agenda

- Background
- Article Summary
- Importance
- Industry and Future
- Companies
- Tech Landscape
- Long-term Impact
- Riff
- Q&A

Main Players

- Shiba Inu
  - Decentralized cryptocurrency created in August 2020
  - Ryoshi – founder and lead developer
  - Goal: "altruistic…give an opportunity for fair distribution and ownership from day 1" - [ADD CITATION]
  - Tokens
    - SHIB
    - BONE
    - LEASH
  - NFTs
    - SHIBOSHIS
    - SHEBOSHI
  - Shibarium
    - Layer 2 blockchain built on top of Ethereum to settle transactions

Main Players

- Zama
  - "open source cryptography company building state-of-the-art Fully Homomorphic Encryption (FHE) solutions for blockchain and AI." - [ADD CITATION]
  - HQ in Paris, France
  - Zama Concrete ML – privacy-reserving ML
  - Zama's fhEVM - confidential smart contracts

Main Players

- Fully Homomorphic Encryption (FHE)
  - Traditional end-to-end encryption not sufficient
  - Why?
    - Enables processing data without decrypting it
    - Companies can process user data without ever seeing the user's data
    - True end-to-end encryption?
  - Why not?
    - Poor performance on large computation
    - Still under research

The Article

- Title: "Shiba Inu Adopts Tech to Bring More Privacy to SHIB Token Holders"
  - Author: Shaurya Malwa (CoinDesk)

- Supporting Articles
  - "SHIB Lead Breaks Silence on Shiba Inu New Mega Deal: Details"
    - Anon??? @ Trading View
  - "Shiba Inu Lead Developer Praises This New Partner"
    - Thecryptobasic.com @ Crypto News
  - "Shiba Inu Team to Pin Another Security Layer to Improve Network Privacy: Details"
    - R. Parashar, S. Suvarna @ Gadgets360

The Article

- Primary article summary
  - Shiba Inu developers have partnered with a cryptography company Zama to develop a new privacy-focused network to add privacy layer for their layer-2 blockchain Shibarium
  - Privacy will be implemented using Zama's FHE solutions for use with Shiba Inu's TREAT token.
    - Not further implementation details
- Why?
  - "Attempt to future-proof Shiba Inu ecosystem against emergeing threast, fostering innovation through access to top-tier privacy tools, and empowering developers to create the next generation of secure, privacy-centric applications." [ADD IN-TEXT CITATION

Importance to Crypto

- Shiba Inu
  - Enhances the value proposition of SHIB tokens
  - Will SHIB become a big player?
- Most important: This could set precedent for other L2 blockchain to adopt similar methods and add privacy layers to their networks
- New security protocol in general
  - New stuff is always cool

Affect on Industry

- Cryptocurrency – Currently no
  - The FHE isn't fully implemented in the Shiba Inu ecosystem yet
  - Currently computationally expensive with numerical errors

- Future?
  - It's possible that this may be a move that give SHIB a legit use case for those users wishing for more privacy in their transactions
  - However, should be noted that since we haven't be given the implementation details, we're not sure if this will impact untraceability and unlinkability
    - These two are properties of CryptoNote protocol (Monero) that are already implemented
      - randomized derivations for public keys for unlinkability
      - one-time ring signatures for untraceability

Companies does this impact? How?

- No idea, don't know of any legitamate companies that are confirmed to work with Shiba Inu

Greater Landscape

- Privacy option as standard in L2 blockchains?
  - "It's a beacon for the entire crypto community, signaling a shift toward a more secure, private, and innovative blockchain future. Here's to the next chapter in the Shib saga — one that promises not just growth and expansion, but a steadfast commitment to privacy and security at the cutting edge of technology."
- Internet
  - Potential for HTTPZ to become the internet standard
  - Internet is private by default

Personal

- While I do believe in supporting and creating new privacy preserving protocols and algorithms, it must be done, I'm not a fan of Shiba Inu backing it
  - Shiba Inu isn't the most credible of organizations, started as a meme coin
  - Zama is credible (recognized by crypto community at RSA Conference contests, have tangible products you can implement into your web2 and web3 applications)

References

- Slide 2
  - https://assets-global.website-files.com/6424006598e25f12a6360e93/6425c40b662f5690cb62e831_Ryoshi_Article.pdf
- Slide 3
  - https://www.zama.ai/about
- Slide 7
  - https://news.shib.io/article/65dd609ce7793300013d4c0d

Q&A

Questions, comments, concerns, hates, detbates?..