web3
foundation

Trust-less and Efficient Bridges via Random Sampling

Bhargav Bhatt
Web3 Foundation


web3
foundation
Less Trust
More Truth

web3 foundation

What are Bridges?

- Infra for interoperability b/w ***independent***, ***technically diverse*** chains
- Chains can fetch and believe the state of the other
- Interesting Applications can be built upon this basic functionality

web3 foundation

Bridges via Trusted Intermediaries

Trusted Intermediary:
Usually a Multisig

Cons:

- Extra trust assumptions
- Centralised (SPoF):
  - Safety
  - Liveness
  - Censorship

So far, NOT so good ...

$80M lost in first hack of 2024

South Korea's Orbit bridge lost $80 million in a hack involving a recurrent theme:

BY BESSIE LIU / JANUARY 2, 2024 08:30 AM

Eric Golden
@ericgoldenx · Follow

You cannot make this up

Hacker steals $600MM in ETH from Ronin blockchain the one underlying Axie

Hacker then goes short Ronin & AXS (Axie token) knowing as soon as news breaks that tokens will plummet

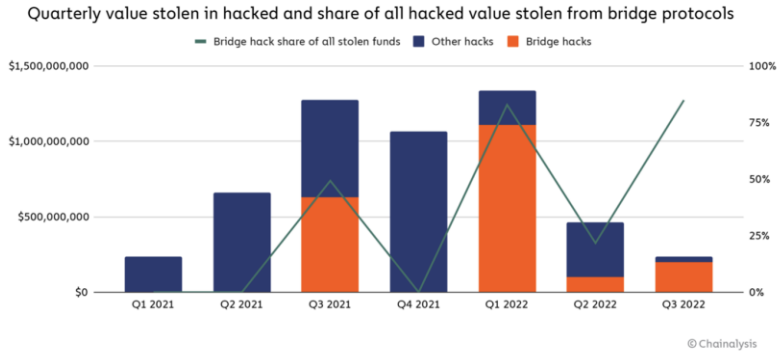
But NO ONE notices and they get liquidated on short before news breaks

X Post

6:32 PM · Mar 29, 2022

Harmony
@harmonyprotocol · Follow

1/ The Harmony team has identified a theft occurring this morning on the Horizon bridge amounting to approx. $100MM. We have begun working with national authorities and forensic specialists to identify the culprit and retrieve the stolen funds.



web3 foundation

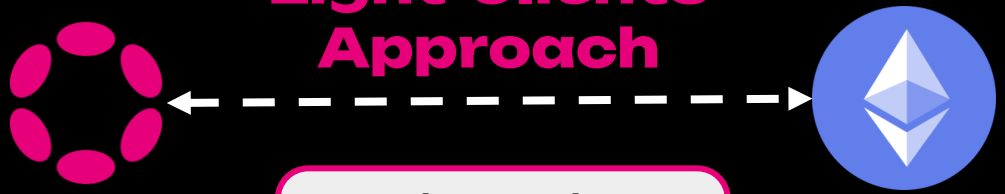
web3 foundation

Trustless Bridges

Definition:
No *additional trust assumptions* on intermediaries/relayers for *safety* of bridge

Requirements:
- Anyone can run a relayer (no stake)
- Any misbehaviour traceable to validators
- Do not shoot the messenger!

Light-Clients Approach



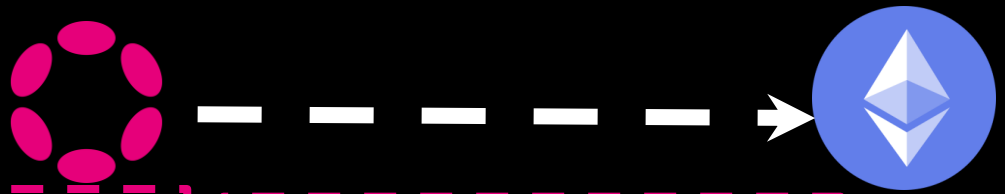
❖ ETH Light Client running as a parachain
❖ Listens to Finality on ethereum via ***Altair*** (sync-committees)

Trust-less Relayers:
Relay messages & collect fees

❖ Polkadot Light Client run on a Smart Contract on Ethereum
❖ Listens to finality on Polkadot, via ***BEEFY***

Polkadot → Ethereum

web3 foundation



Polkadot Light Client as Smart Contract; listens to Finality

BEEFY Finality
Easier for **on-chain** light clients to follow.

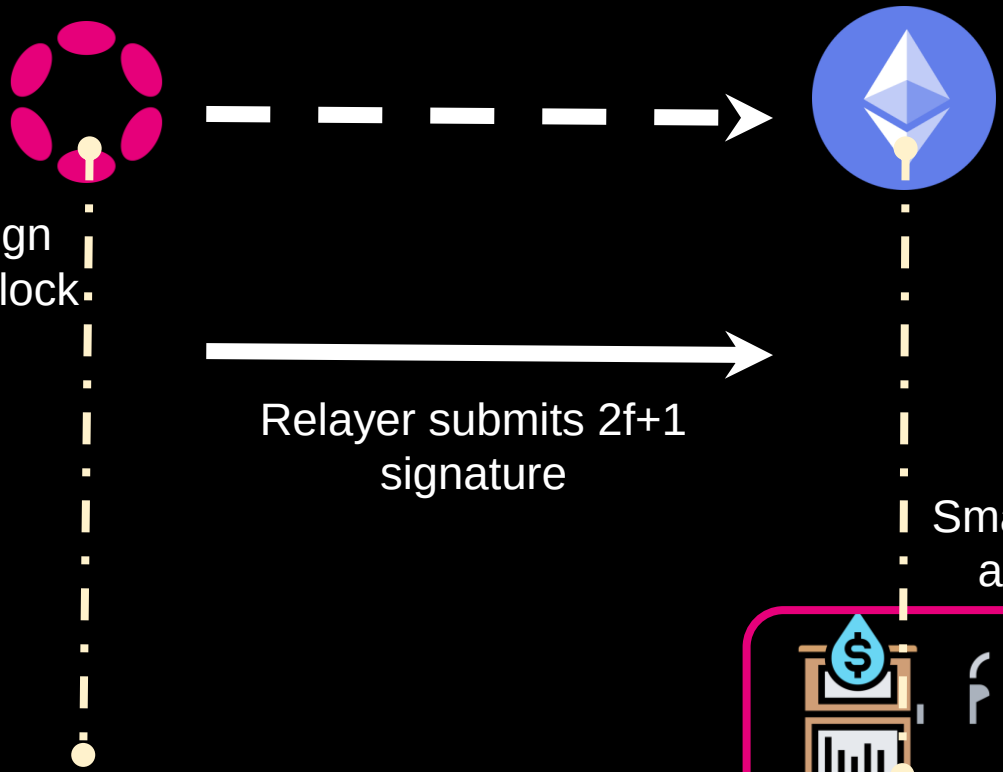
Random Sampling
Interactive protocol which reduces costs while retaining security

BEEFY

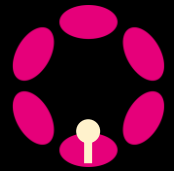
Challenge: Running a Light Client Smart Contract is **expensive.** How to efficiently listen to finality on Polkadot?

Strawman Protocol

web3 foundation



Interactive Random Sampling



Light Client

2f+1 validators sign BEEFY finalised block

Relayer **claims** to have 2f+1 signatures & Sig_V

Uses **RANDAO** to randomly sample ***m*** signatures

Gathers and sends the *m* signatures

Verifies *m* signatures

m is the security parameter!
Probability of light client being duped is $1/2^m$

web3 foundation

Security Analysis

- *m* (# signature checks) regulates trade-off between **security** and **efficiency**
- **Crypto-Economic** argument**:**

  Exp_Val = p*(MarketCap) + (1-p)*(-Slash) < 0

  - **p:** probability of successful attack = $1/2^m$.
  - **Slash:** slash value for signing invalid BEEFY blocks.
    Note: we only slash the validators and not relayers.
  - **MarketCap:** attack value bounded by total DOT market cap

Hang on ....

web3 foundation

Limitations of Strawman Protocol

We assumed that the protocol is one-shot but it is interactive.

1. **Concurrency can be exploited to increase probability of successful attacks**

1. **RANDAO Randomness is biasable**

web3 foundation

Concurrency Issue

Relayer-1

Signs Malicious **B**

Relayer-2

Signs Malicious **B**

Relayer-n

Signs Malicious **B**

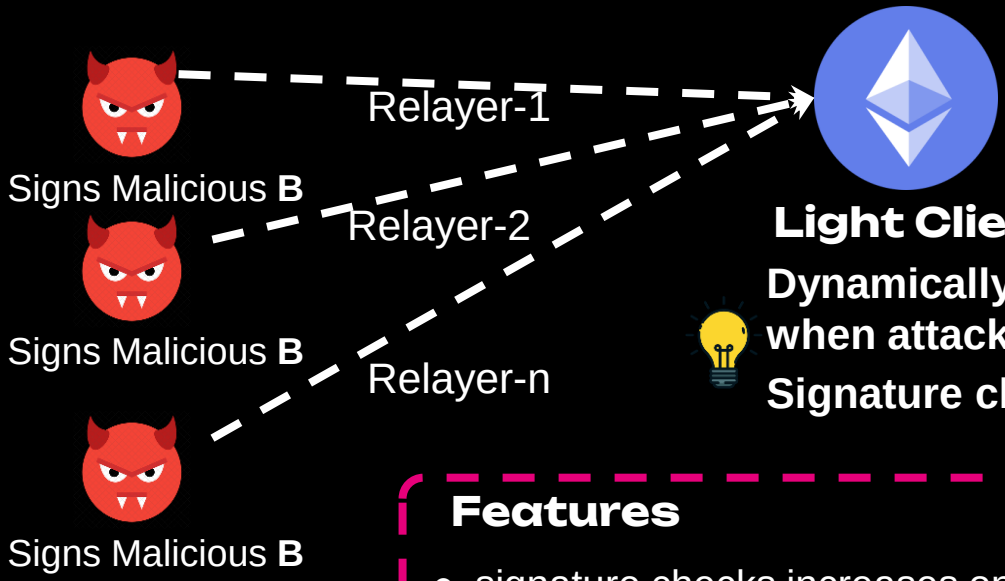
Light Client

- **Only Validators get slashed**
- **It takes a delay D to slash malicious behaviour**

Concrete Attack:

- **Spawn multiple relayers using same malicious sigs.**
- **Slashable stake doesn't increase**
- **Multiple roll of dice (RANDAO) without incurring repercussions**

Solution: Dynamic Sampling



Light Client

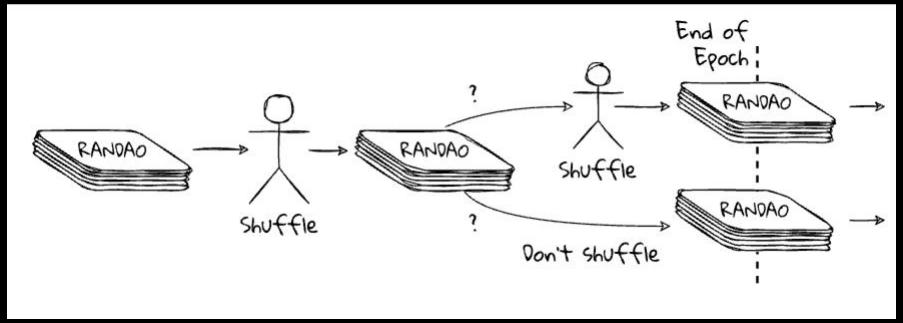
Dynamically increase security parameter when attack is detected.

Signature checks = m + $2*\log_2(n)+1$

Features

- signature checks increases only when attack is launched
- No limit on # of relayers and no trust assumptions
- Can Relayers start spamming just to increase the security parameter? **NO, such griefing attacks are too expensive**

2nd Issue: RANDAO Biasibility



Shorter Tail of Malicious Producers

Longer Tail of Malicious Producers

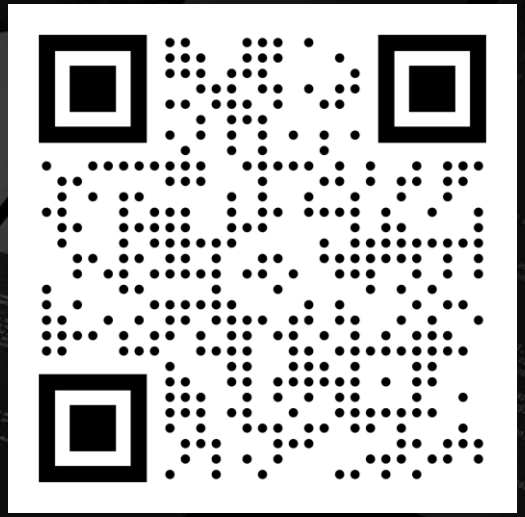
- **Last-revealer Attack:** block producer skips authoring to bias 1-bit
- Performed **Markov Chain analysis** to quantify the bias.
- **Solution:** Add extra signature checks to negate the bias. ~10 extra sig checks assuming 67% honesty on Ethereum.

web3 foundation

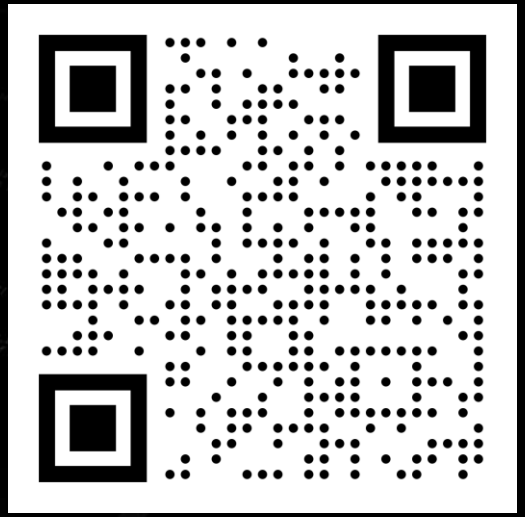
Status

- Snowbridge, an implementation which uses random sampling is scheduled to go live soon.
- Saves around $5M/year in gas costs for running the light-client smart contract on ethereum.
- Developing a SNARK-based accountable light client protocol using aggregate signatures to reduce latency.

W3F Grants



JUST Grants



web3
foundation

Accountable Light Client Systems for PoS Blockchains

Oana Ciobotaru[1], Fatemeh Shirazi[2], Alistair Stewart[1], and Sergey Vasilyev[1]

[1]Web3 Foundation
[2]Independent Researcher

January 12, 2023

Abstract

A major challenge for blockchain interoperability is having an on-chain light client protocol that is both efficient and secure. We present a protocol that provides short proofs about the state of a decentralised consensus protocol while being able to detect misbehaving parties. To do this naively, a verifier would need to maintain an updated list of all participants' public keys which makes the corresponding proofs long. In general, existing solutions either lack accountability or are not efficient. We define and design a committee key scheme with short proofs that do not include any of the individual participants' public keys in plain. Our committee key scheme, in turn, uses a custom designed SNARK which has a fast prover time. Our committee key scheme can be used in an accountable light client system as the main cryptographic core for building bridges between proof of stake blockchains. Finally, we implement a prototype of our custom SNARK for which we provide benchmarks.

web3 foundation

We fund research and development teams who are building the foundation of the decentralized web.

Our mission is delivering a decentralized and fair network where users control their own data, identity and destiny.