grincon1
2019.11.22 // c-base berlin

Grin Open Research Problems

“Let’s hire a cryptographer"

@quentinlesceller

Q T U M

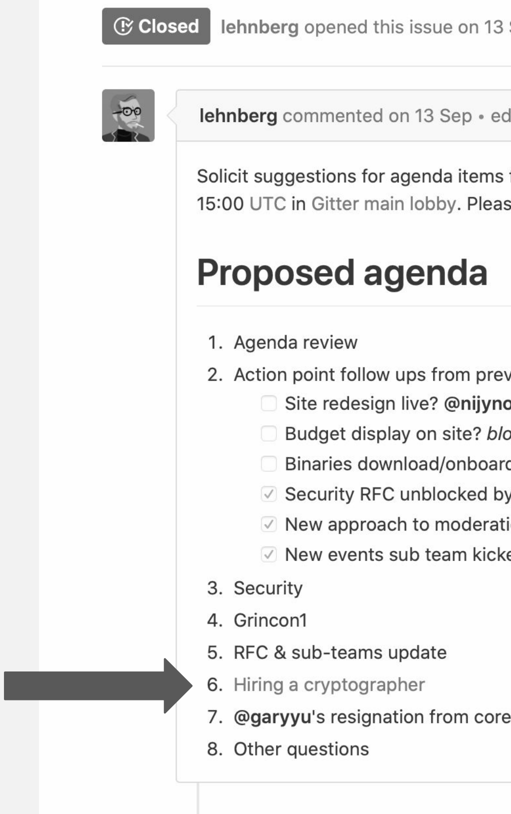
SPARK POOL

“Let's hire a cryptographer”

Ok. but ...

- Lot of talks about hiring a cryptographer on Grin
- Many questions:
  - Who?
  - Which subject?
  - Timelines?
  - Funding?

First: Define the Research Problems



Closed lehnberg opened this issue on 13

lehnberg commented on 13 Sep • ed

Solicit suggestions for agenda items
15:00 UTC in Gitter main lobby. Pleas

Proposed agenda

1. Agenda review
2. Action point follow ups from prev
   - □ Site redesign live? @nijyno
   - □ Budget display on site? *blo*
   - □ Binaries download/onboard
   - ☑ Security RFC unblocked by
   - ☑ New approach to moderati
   - ☑ New events sub team kicke
3. Security
4. Grincon1
5. RFC & sub-teams update
6. Hiring a cryptographer
7. **@garyyu**'s resignation from core
8. Other questions

Research Problems

Types of Research Problems

Privacy Enhancement

Optimization

Implementation

Abstract Cryptographic Problems

Current Research Problems

- BLS Signatures
- Accumulator
- Kernel Aggregation
- Scriptless Scripts
- Flyclient
- Asynchronous Transaction Building
- Reducing Linkability of Outputs On Chain
- Erlay Transaction Relaying
- Payment Channel Hubs
- Research on ZKPs Recent Advances

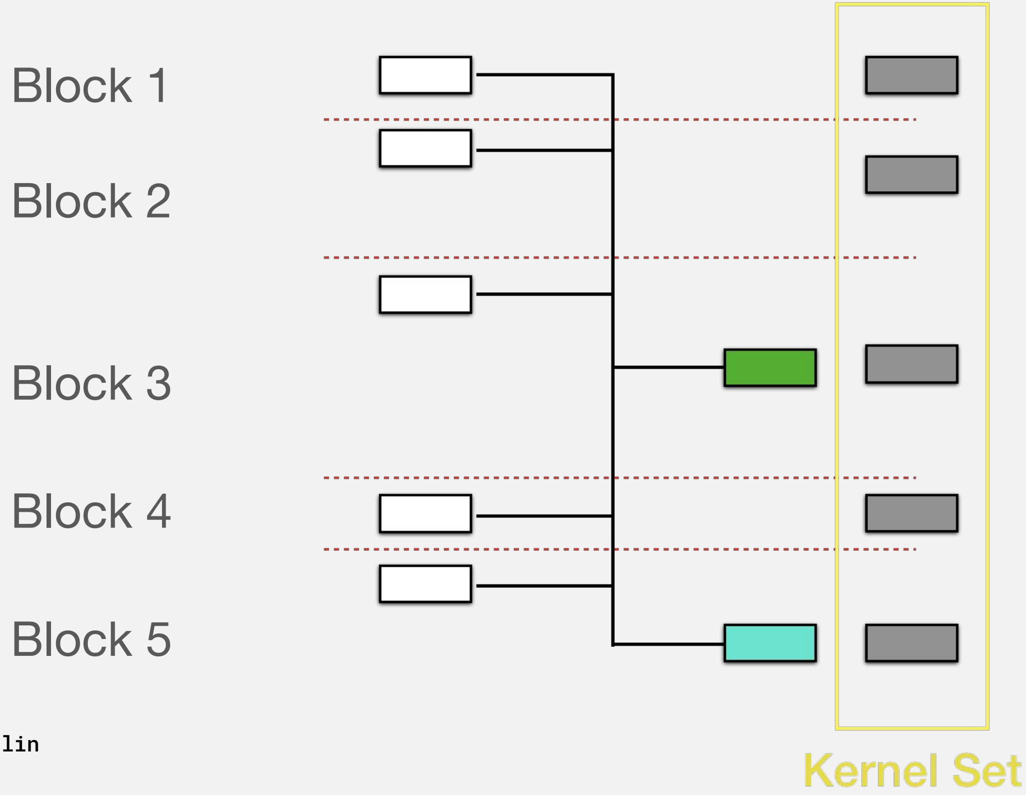
https://github.com/mimblewimble/docs/wiki/Grin-Open-Research-Problems

Current Research Problems

- BLS Signatures
- Accumulator
- Kernel Aggregation
- Scriptless Scripts
- Flyclient
- Asynchronous Transaction Building
- Reducing Linkability of Outputs On Chain
- Erlay Transaction Relaying
- Payment Channel Hubs
- Research on ZKPs Recent Advances

https://github.com/mimblewimble/docs/wiki/Grin-Open-Research-Problems

Kernel Aggregation



Block 1

Block 2

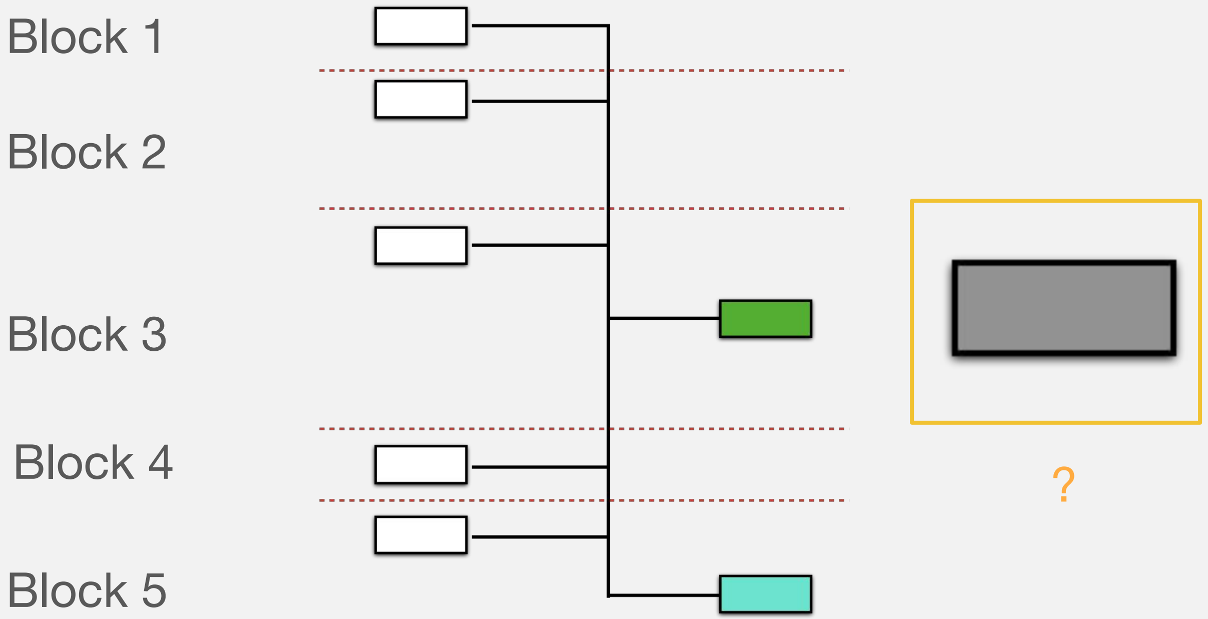
Block 3

Block 4

Block 5

Kernel Set

Kernel Aggregation



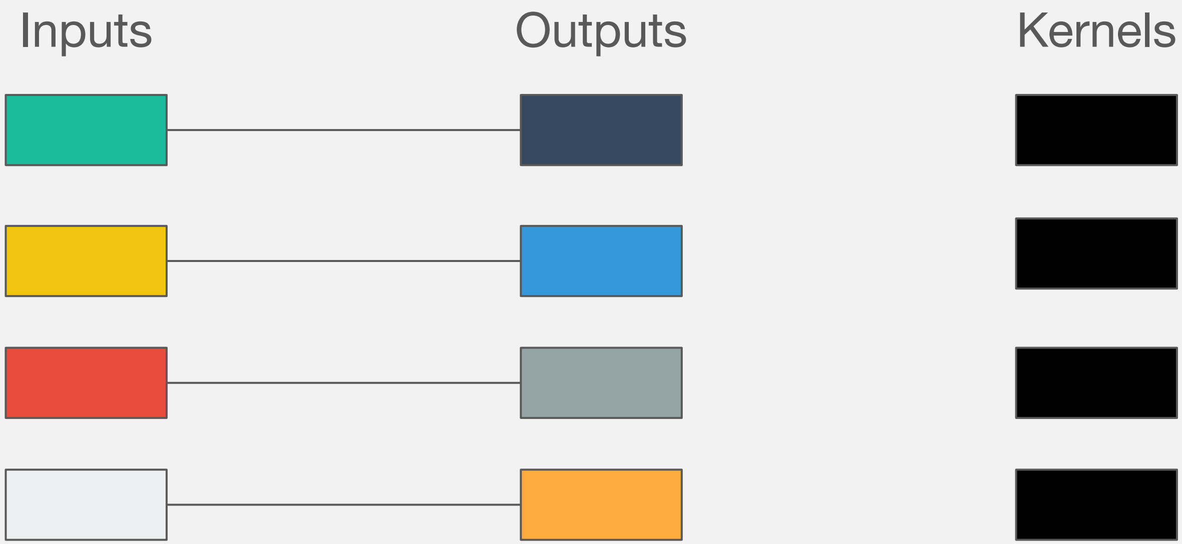
Kernel Aggregation

- **Current Situation:** While inputs/outputs can be thrown away once spent, there is another piece of data called the kernel that must stay.
  For each transaction a kernel is created, this piece of information cannot currently be aggregated or discarded.

- **Goal:** Identify potential ways to aggregate transaction kernels and/or possibly discard them if not needed.

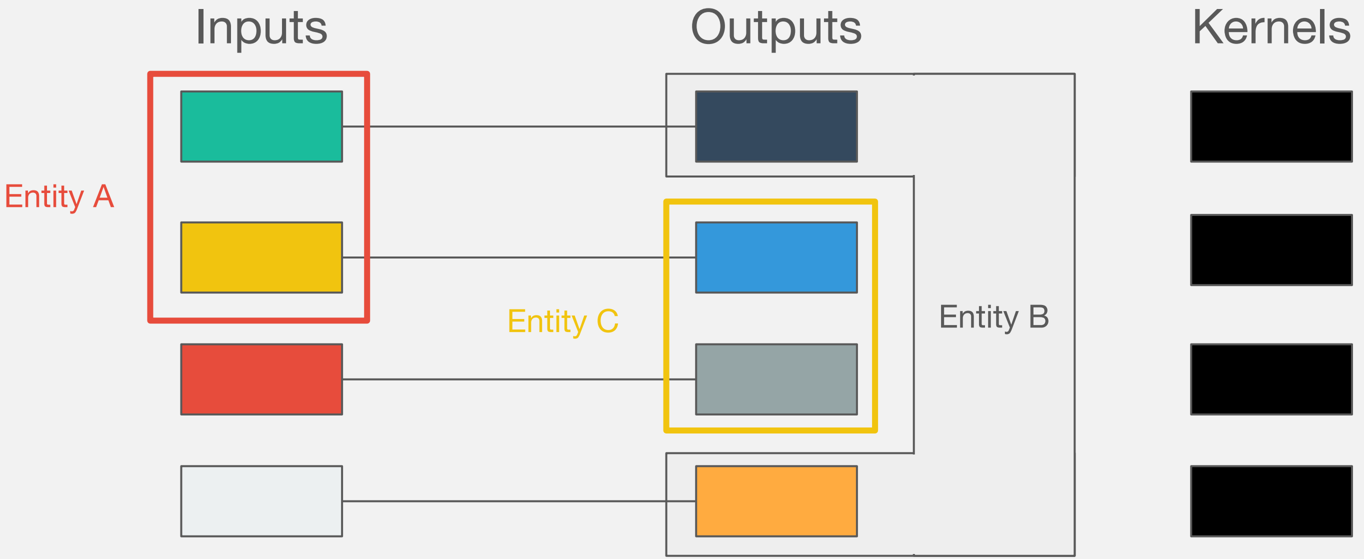
Reducing Linkability of Outputs On Chain

On the network



Reducing Linkability of Outputs On Chain

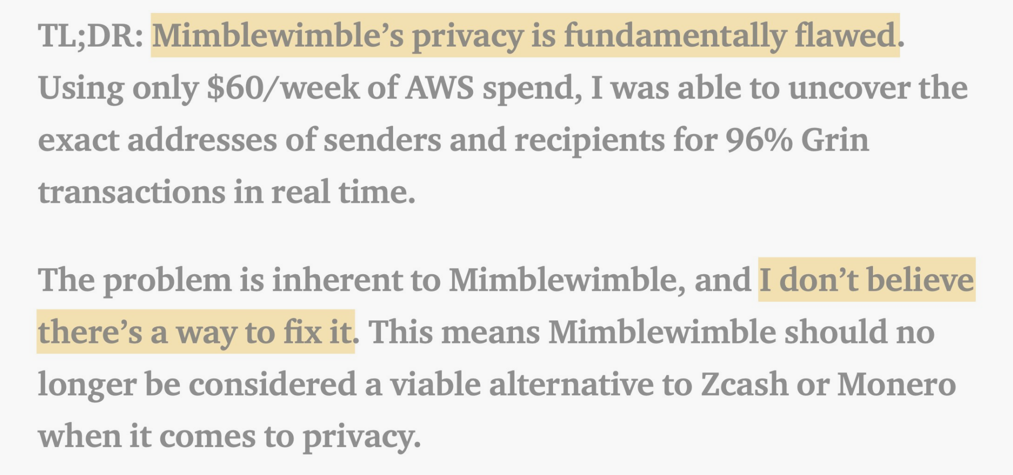
After Analysis



for illustration purposes only...

Reducing Linkability of Outputs On Chain

- **Current situation:** not great.
- **Goal:** the title of this slide.

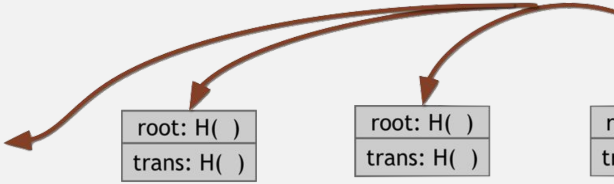


TL;DR: Mimblewimble's privacy is fundamentally flawed. Using only $60/week of AWS spend, I was able to uncover the exact addresses of senders and recipients for 96% Grin transactions in real time.

The problem is inherent to Mimblewimble, and I don't believe there's a way to fix it. This means Mimblewimble should no longer be considered a viable alternative to Zcash or Monero when it comes to privacy.

Flyclient

- Created by Loi Luu, Benedikt Bünz, Mahdi Zamani (Scaling Bitcoin 2017)
- Store the Header MMR root in the block header to quickly check blockchain validity



- Two uses cases for Grin (#1555)
  - Light Clients
  - Quickly identify longest chain for full node (with near certainty). Download block headers in the background after.

Flyclient

- **Current Situation:** We already have the MMR roots stored.

- **Goal:** Investigate the necessaries prerequisites for the introduction of a FlyClient in Grin and implement it on Grin.

Asynchronous Transaction Building

- **Current Situation:** Mimblewimble type blockchain requires a round trip between the payer and payee to construct a valid transaction.
- Several research attempts have been made in that direction: relying on federated relays or Beam shared bulletin board system.
- **Goal:** Investigate and develop an asynchronous, robust, and privacy preserving method of building Grin transactions.

Grin Draft RFC - Asynchronous Transacting via Relays by David Burkett

Targets?
$?

Targets

- Anyone especially:
  - PhD
  - Independent researchers
  - Expert cryptographers
  - Developers
  - You?

Funding

- Funding available from the Grin General Fund
- Reasonable requirements:
    - Track record
    - Clear objectives
    - Time constraint
    - Clear plan
- Feel free to join us on Keybase: http://keybase.io/team/grincoin

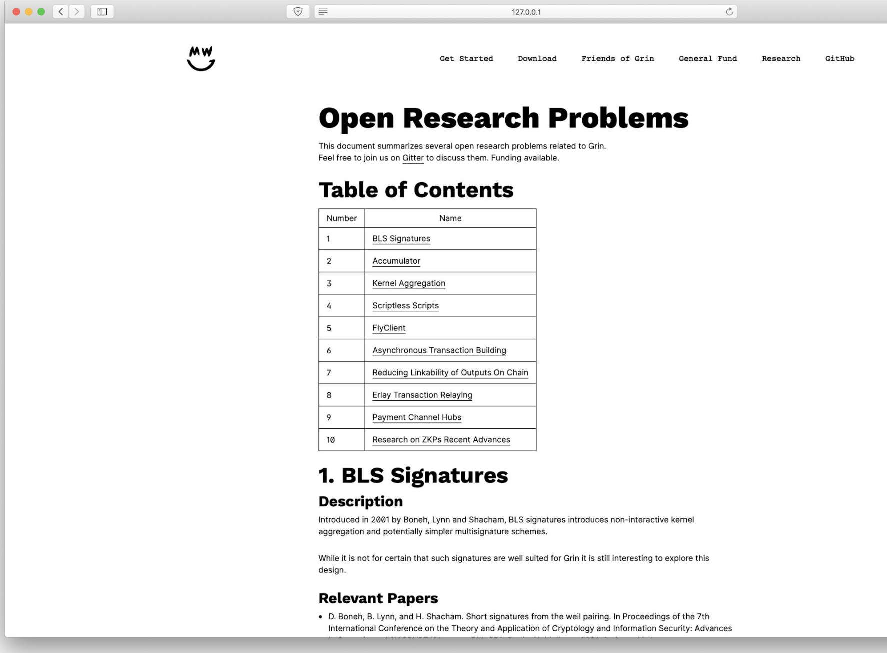
Or talk to us after :)

What’s Next?

Increase Visibility

- New page on grin.mw
- Bounty? Monero like?
- Let’s hear your suggestions

https://github.com/mimblewimble/site/issues/166



Open Research Problems

This document summarizes several open research problems related to Grin.
Feel free to join us on Gitter to discuss them. Funding available.

Table of Contents

1. BLS Signatures

Description

Introduced in 2001 by Boneh, Lynn and Shacham, BLS signatures introduces non-interactive kernel aggregation and potentially simpler multisignature schemes.

While it is not for certain that such signatures are well suited for Grin it is still interesting to explore this design.

Relevant Papers

- D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. In Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances

Thank you