



Grin London Meetup
08.01.2019 // London

Grin intro

@lehnberg

Contents

- Protocol
- Project
- Implementation
- Proof of work
- Launch
- Community projects
- Contributing
- Q&A with @yeastplume



Protocol

Mimblewimble

- Proposed by Jedusor (2016), improved by Poelstra (2016).
- New blockchain design, utilising Confidential Transactions (Maxwell 2016).
- No amounts, no scripts, no addresses, no non-confidentiality, in a simple protocol that leaves little room for information leakage.
- Ownership proved via single-use key.



Wait what?

No addresses?



Interactive transaction building

1. Sender **creates** a slate. Sends to recipient.
2. Recipient **processes** slate. Returns to sender.
3. Sender **finalizes** slate. Broadcasts to peers.



Also possible in reverse (invoicing)

1. Receiver **creates** a slate. Sends to sender.
2. Sender **processes** slate. Returns to Receiver.
3. Receiver **finalizes** slate. Broadcasts to peers.



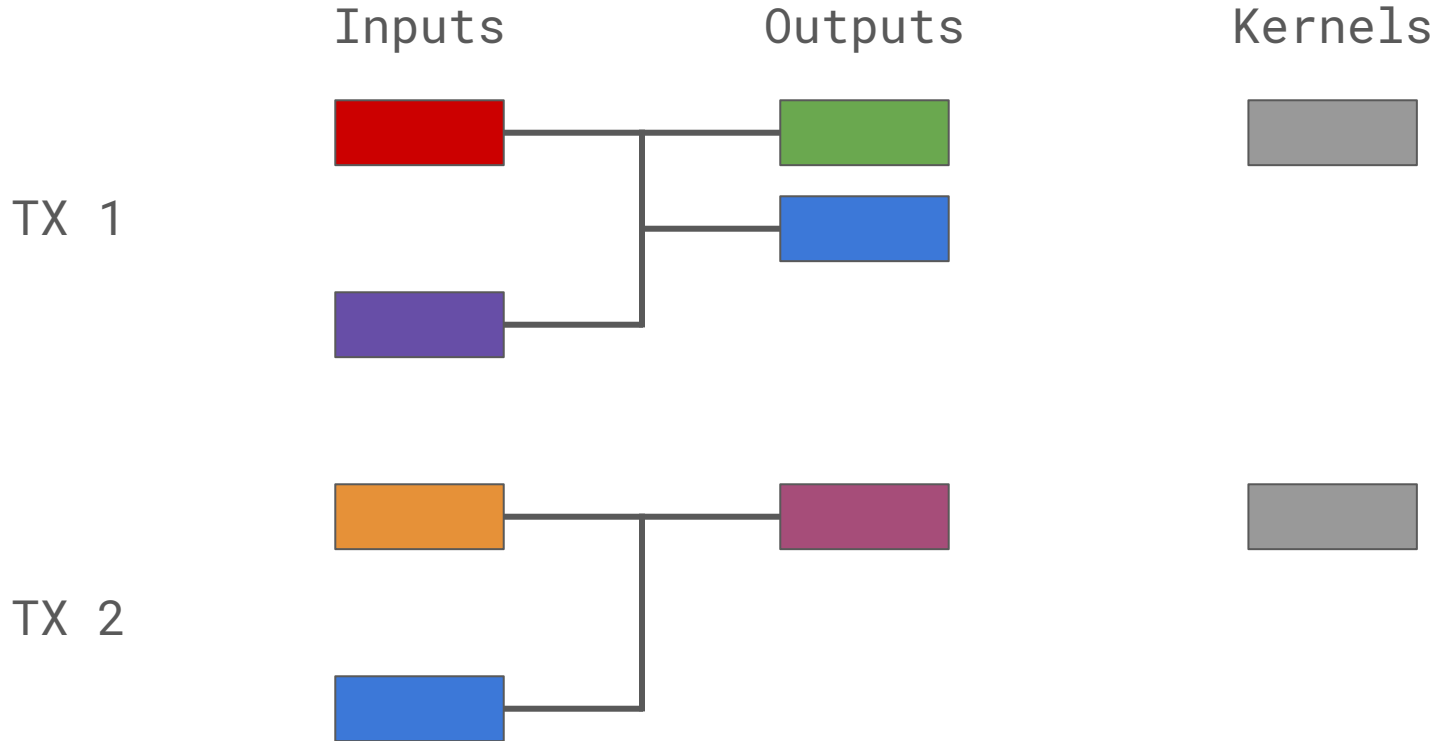
Transaction structure

- Inputs: reference old unspent outputs
- Outputs: new commitments
- Kernels: excess and a signature

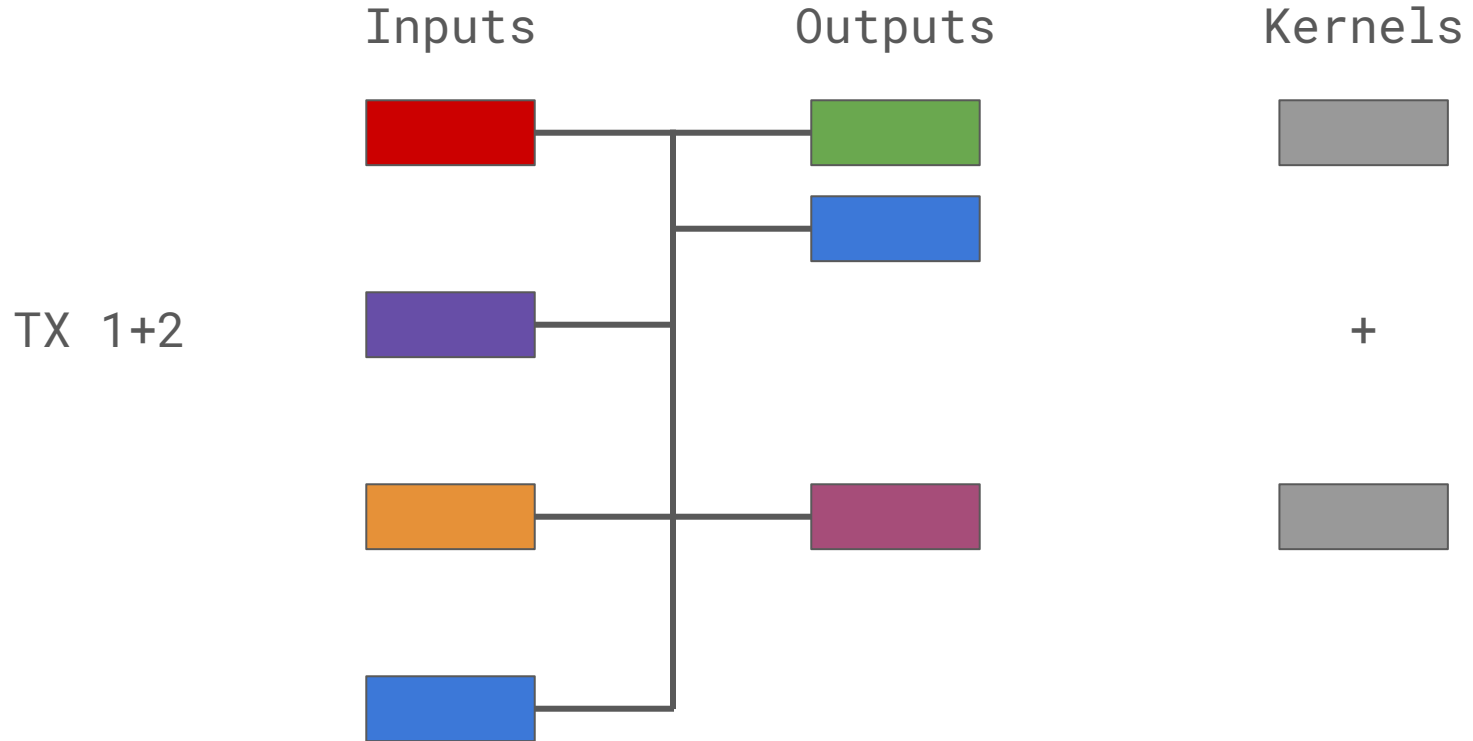
sum outputs - sum inputs == sum excess



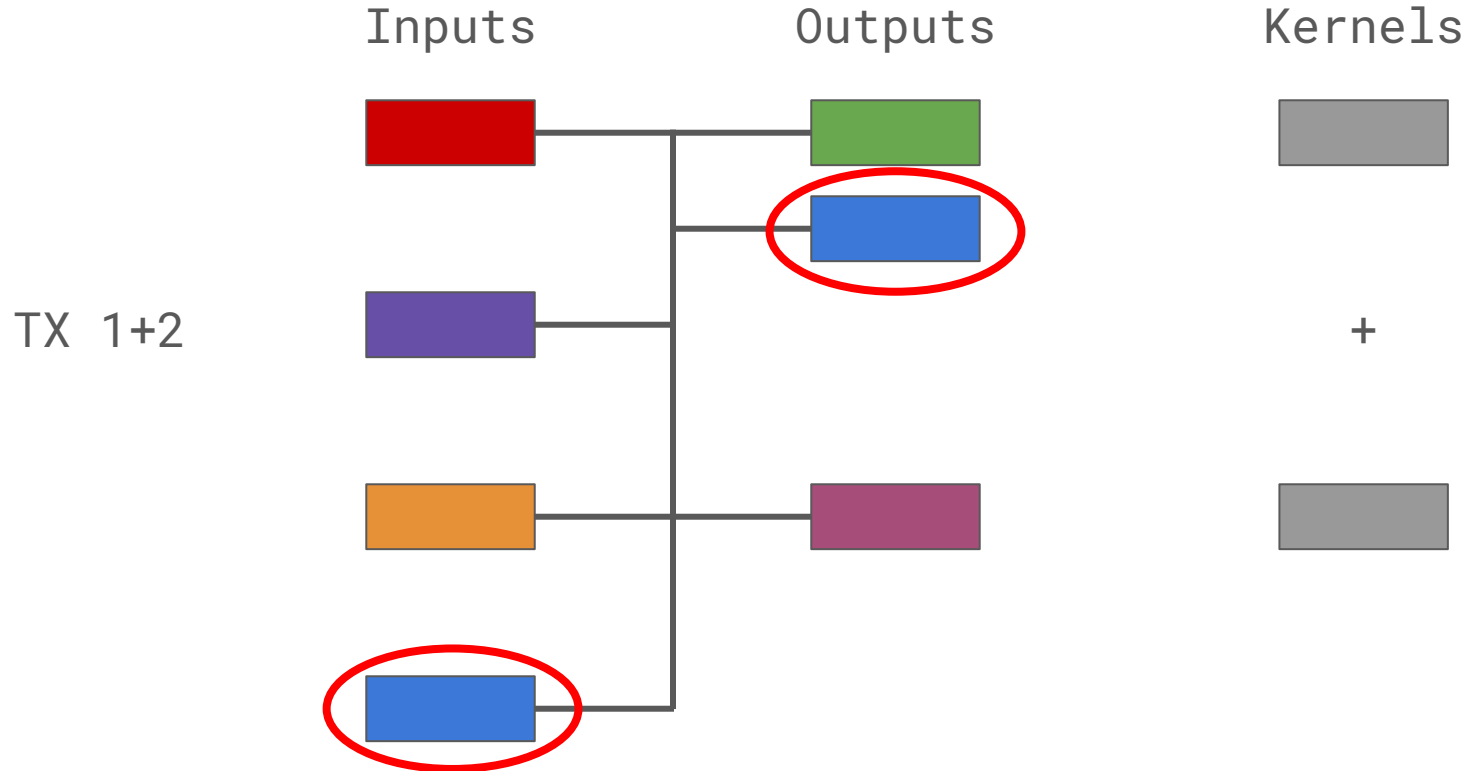
Transactions...



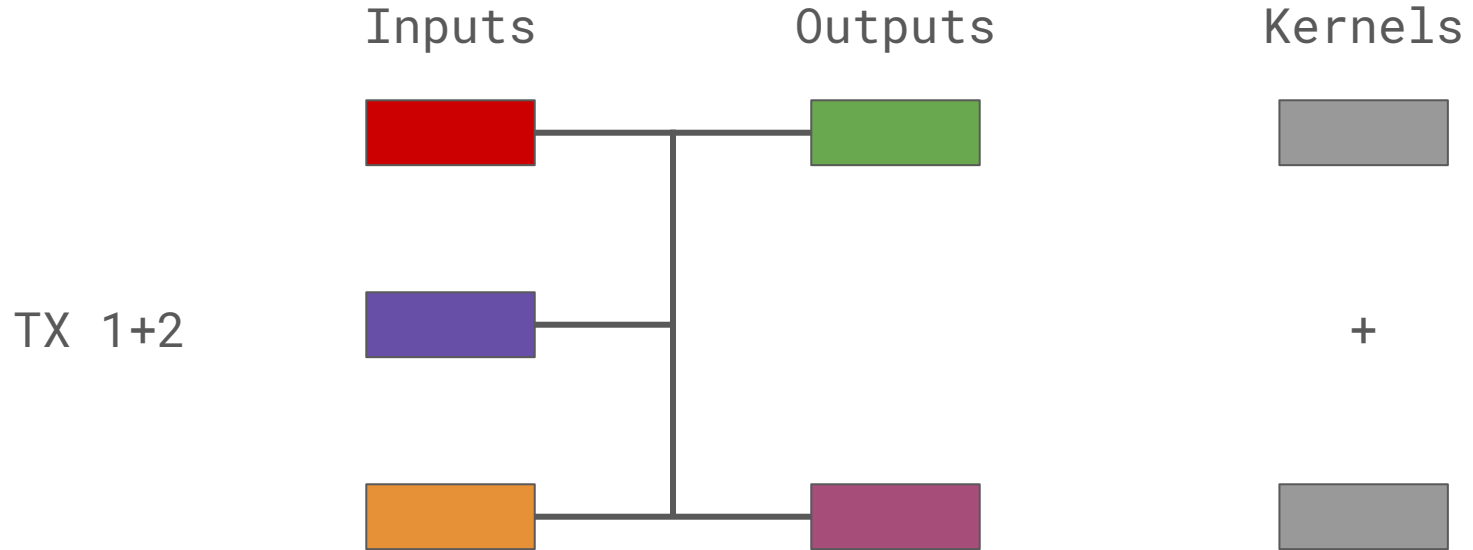
...can be joined together.



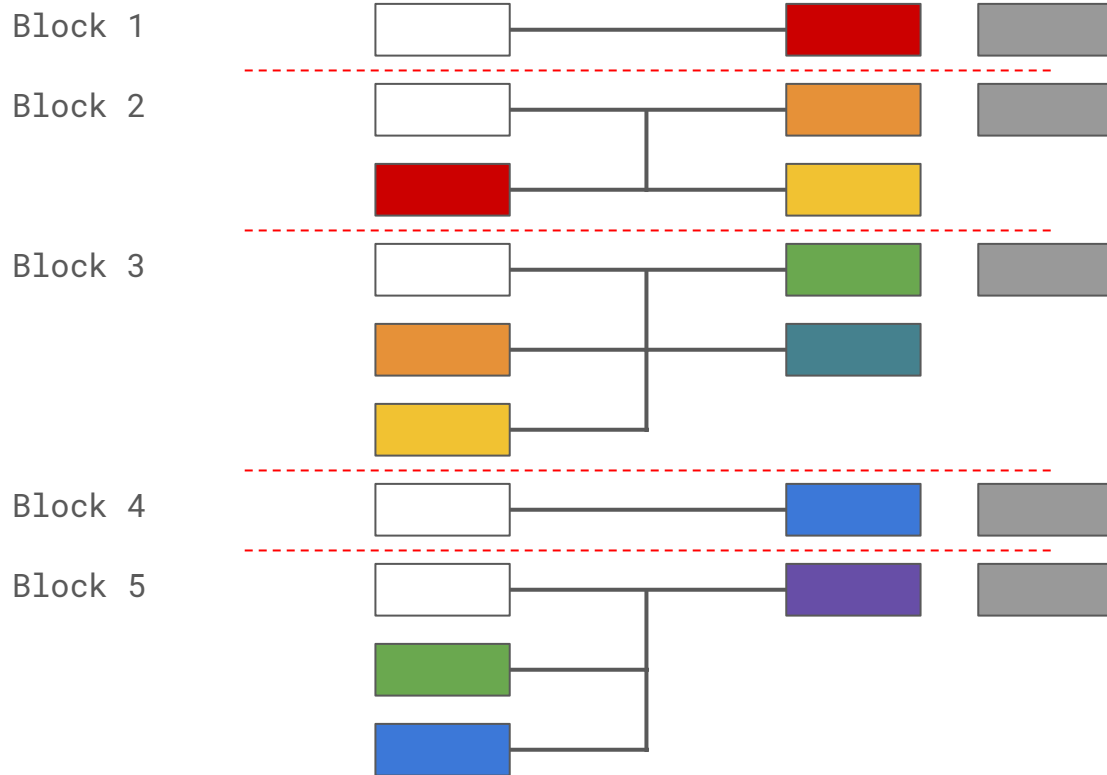
And outputs later used as inputs...



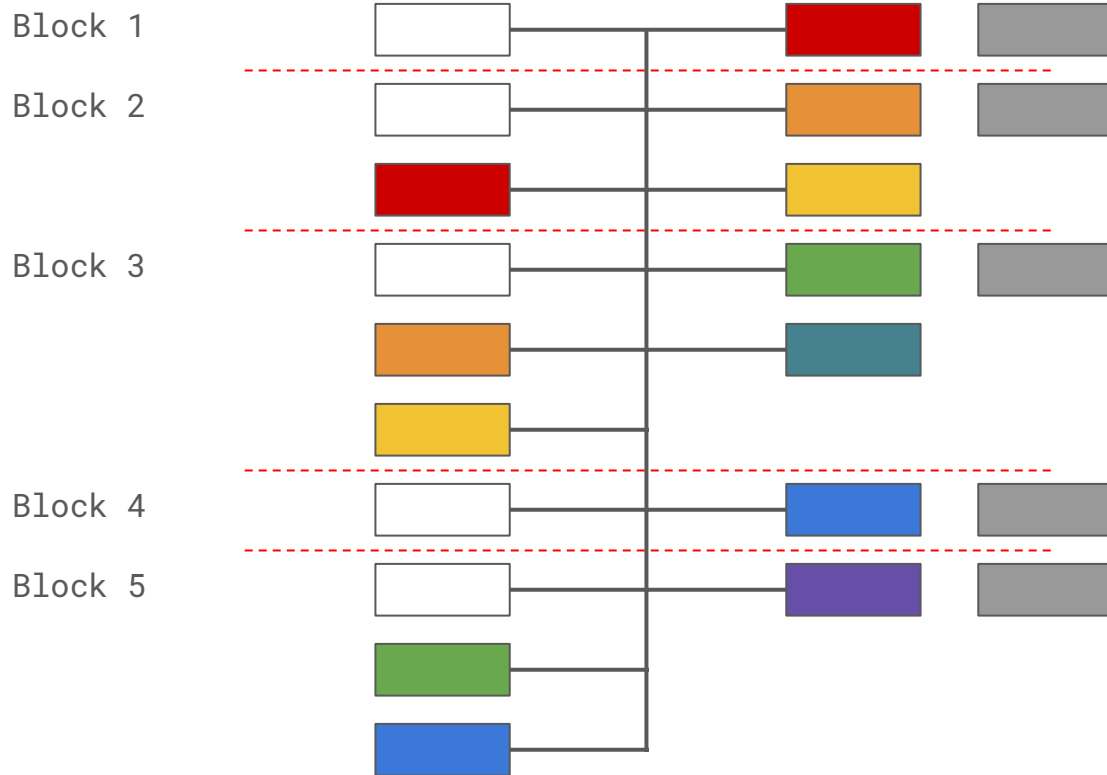
...can be discarded.



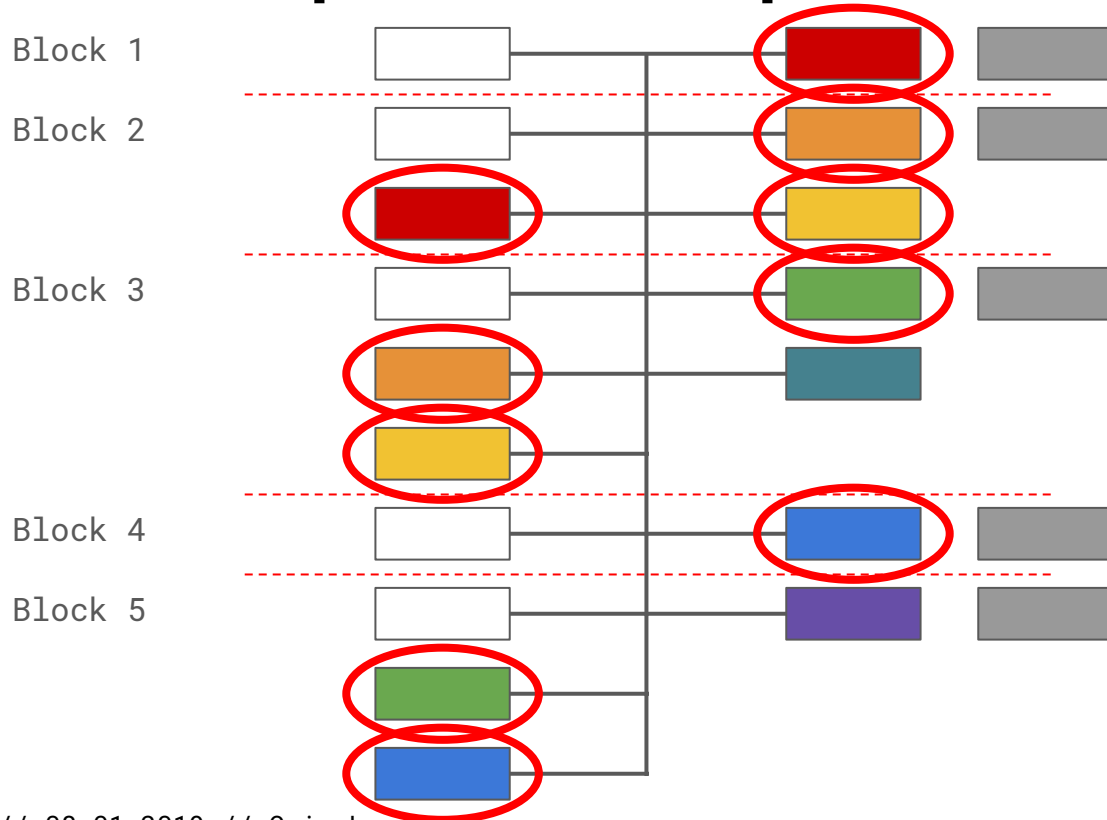
Similarly, the blockchain...



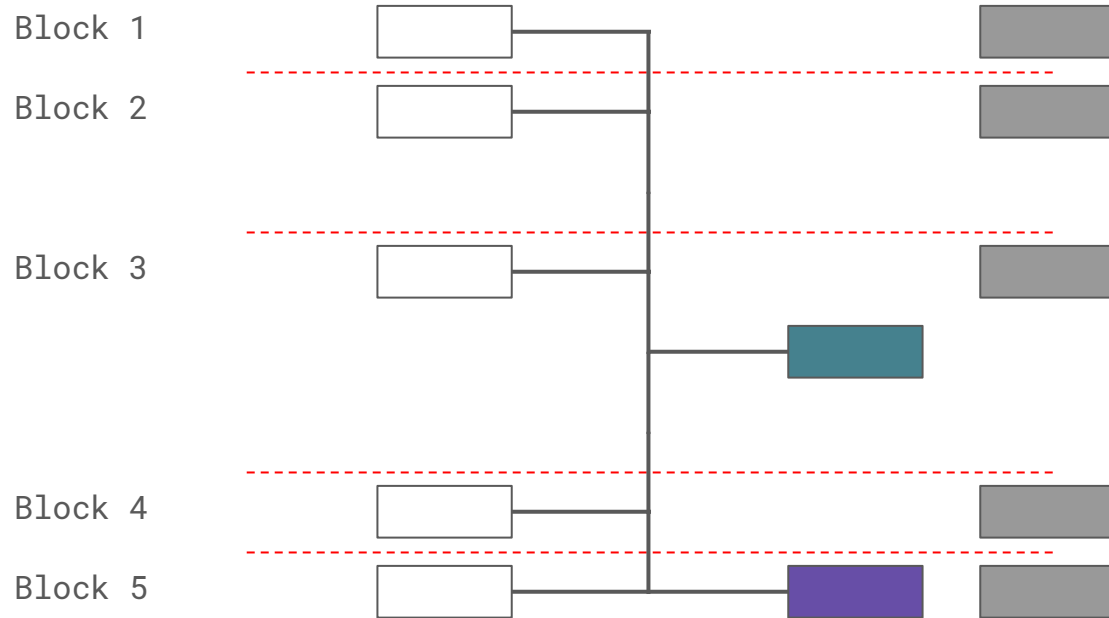
...can be joined.



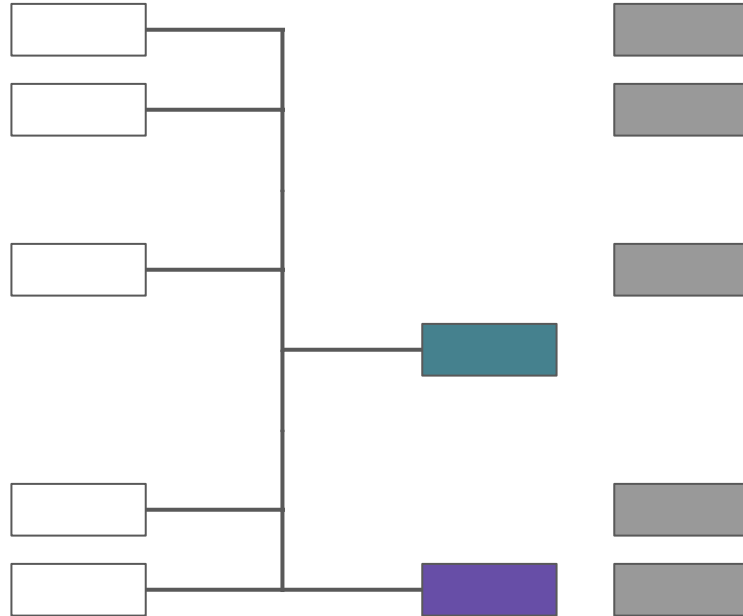
And when outputs are spent...



...they can be removed.



Initial sync



Block headers



Initial sync

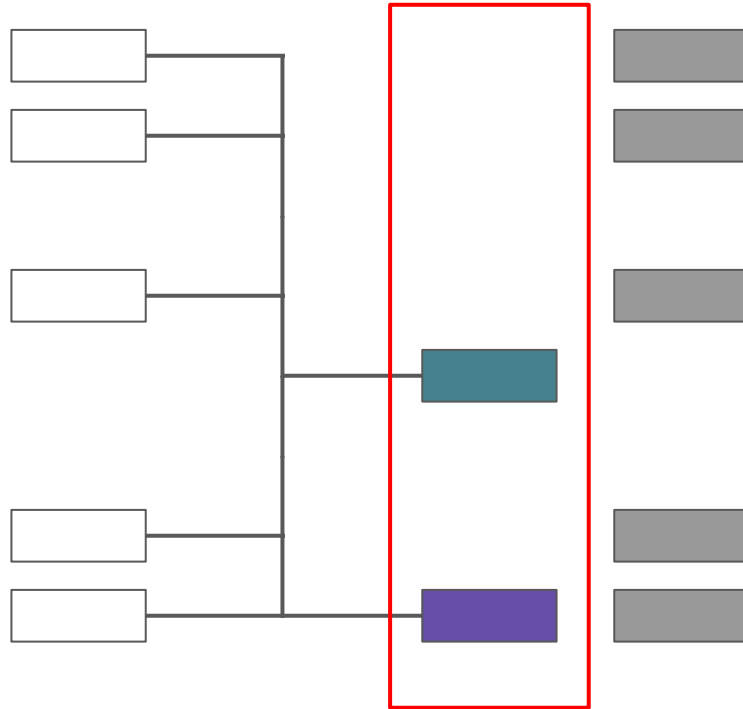
Block 1

Block 2

Block 3

Block 4

Block 5



UTXO set



Initial sync

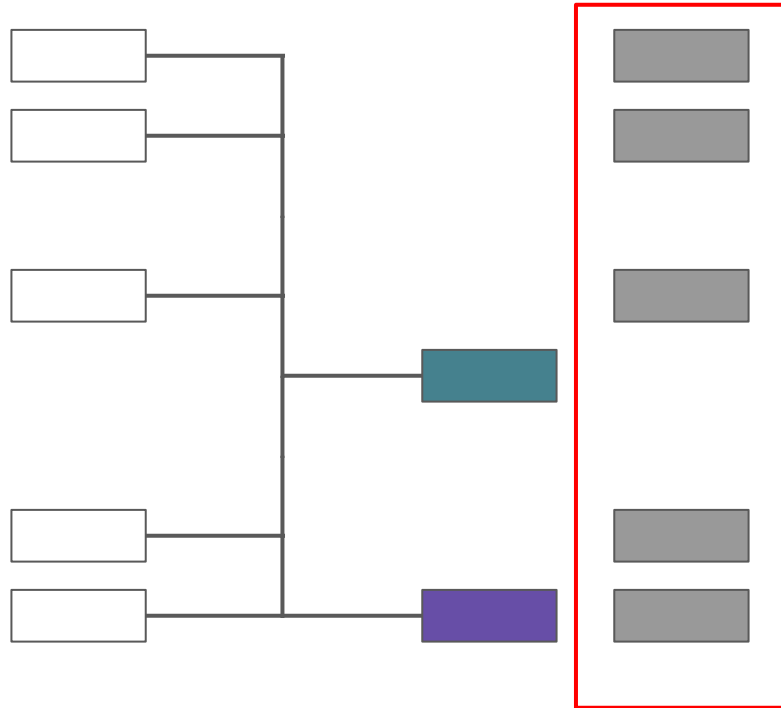
Block 1

Block 2

Block 3

Block 4

Block 5



Kernel set



Mimblewimble pros/cons

Pros:

- + No amounts
- + No addresses
- + Improved scaling

Cons:

- Interactive transactions
- Some output linking still possible
- No scripting (but scriptless scripts)



Project

Grin

Announced October 20th, 2016 by “Ignotus Peverell”

First Mimbalewimble implementation

Written in Rust

Open source, 100% community driven

Funded by donations

No: ICO, CEO, DevCo, advisors, investors, founder rewards, premines, pre-allocation, pre...



Why bother?

MW tech is worth experimenting with

Bitcoin is very conservative

Sidechains are/were a mythical beast

Some MW-native concepts are impossible in Bitcoin

Can implement many state-of-the-art technologies



Philosophy

Grin likes itself small and easy on the eyes. It wants to be inclusive and welcoming for all walks of life, without judgement. Grin is terribly ambitious, but not at the detriment of others, rather to further us all. It may have strong opinions to stay in line with its objectives, which doesn't mean disrespect of others' ideas.

We believe in pull requests, data and scientific research. We do not believe in unfounded beliefs.



Words I use to describe the project

- Open
- Fair
- Honest
- Minimal
- Rational
- Transparent



Governance

KISS

No foundation

Technocratic council

Constantly evolving work in progress

Decisions taken in the open in bi-weekly development and governance meetings where possible



Implementation

Technologies used (sub-set)

Schnorr Signatures. Smaller sigs, better security, enables mu-sig and scriptless scripts, and certifiable transactions.

Bulletproofs. Smaller range proofs required for CT.

Scriptless scripts. Enables atomic swaps in Grin and some other scripting behavior.

Dandelion. Privacy-preserving transaction propagation and aggregation.



Future areas of research (maybe)

FlyClient

Lightning network

Confidential assets

Universal accumulators

BLS signatures



Emission

1 Grin/s forever.

Proof of work mined.

One minute block time.

60 grin constant coinbase reward.

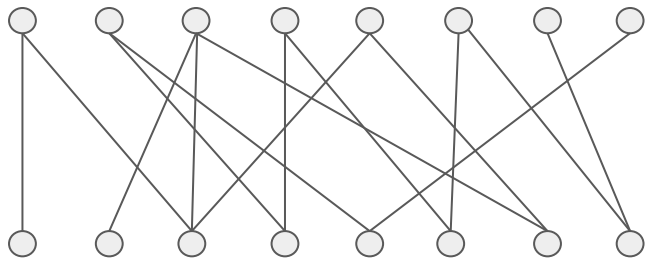
Simple. Incentivises spending. Discourages unfair advantage for early adopters for the benefit of improved longer term adoption.



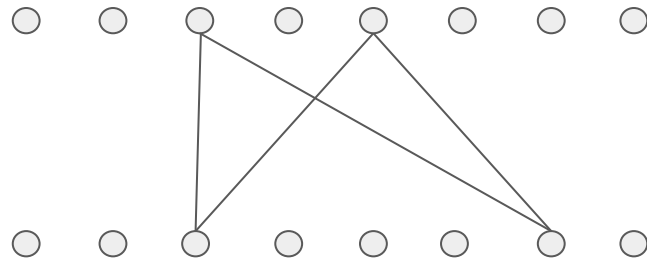
Proof of Work

Cuckoo Cycle family

Finding 42-cycles in random bipartite graphs with billions of nodes. Creator: John Tromp



Begin with a mess



End up with a cycle



Grin Mainnet PoWs

- For GPUs: **Cuckaroo29** - 2^{29} edges
 - Variant of Cuckoo that enforces Mean mining
 - Minimum 5.5 GB of memory (less with slowdown)
 - Tweaked to maintain ASIC resistance for 2 years
 - 90% of rewards at launch, linearly decreasing to 0 in 2 years
- For ASICs: **Cuckatoo31+** - 2^{31} edges or more
 - Variant of Cuckoo that simplifies ASIC design
 - Takes 512 MB of memory, with random single-bit accesses to half
 - Can be mined on 11GB GPU initially
 - Takes 2^k GB after $2^{(1+k)}$ years, by phasing out smaller sizes
 - 10% of rewards at launch, linearly increasing to 100% in 2 years



Best GPU for mainnet

Nvidia RTX 2080 Ti*

* Unless ASICs make Cuckatoo mining with it infeasible.
If so, then GTX 1080 Ti.

** With what we know today.

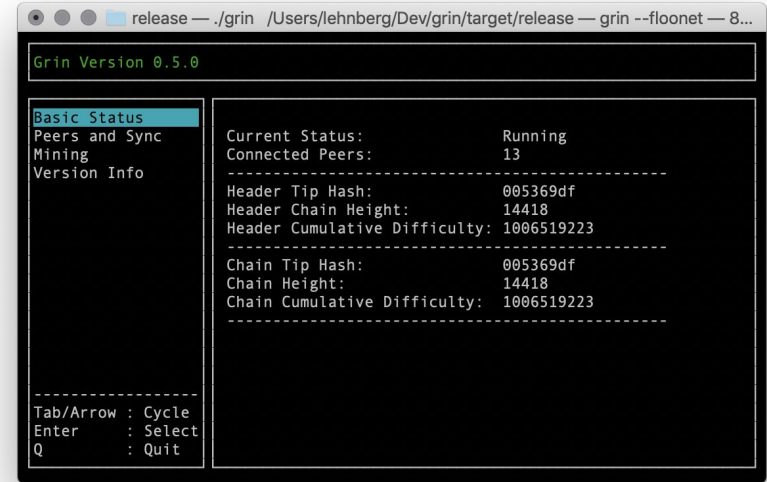


Launch

Next week
Jan 15, 2019

What's in the box?

- **Node.** Stratum protocol.
- **Wallet.** Basic commands.
Transactions via file,
keybase, http(s)
- **Miner.** CUDA and OpenCL
plugins for both algos.



```
release — ./grin /Users/lehnberg/Dev/grin/target/release — grin --floonet — 8...
Grin Version 0.5.0

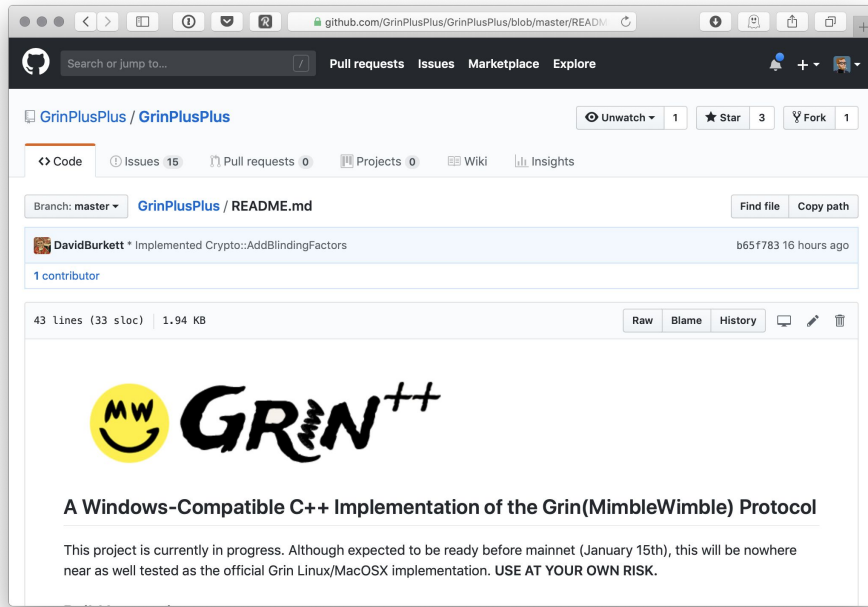
Basic Status
Peers and Sync
Mining
Version Info

Current Status: Running
Connected Peers: 13
-----
Header Tip Hash: 005369df
Header Chain Height: 14418
Header Cumulative Difficulty: 1006519223
-----
Chain Tip Hash: 005369df
Chain Height: 14418
Chain Cumulative Difficulty: 1006519223
-----

-----
Tab/Arrow : Cycle
Enter      : Select
Q          : Quit
```



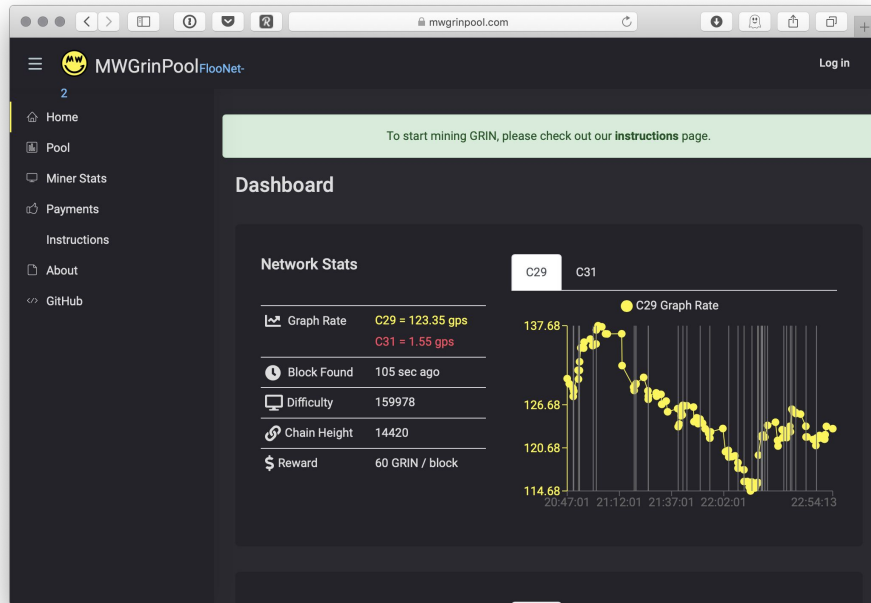
Selected community projects



<https://github.com/GrinPlusPlus/GrinPlusPlus>

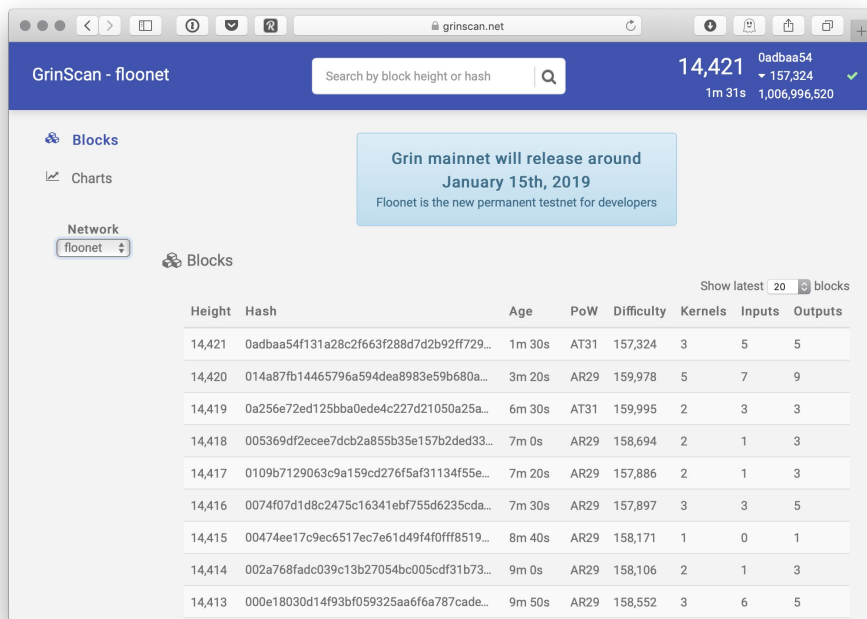


Grin intro // 08.01.2019 // Grin London

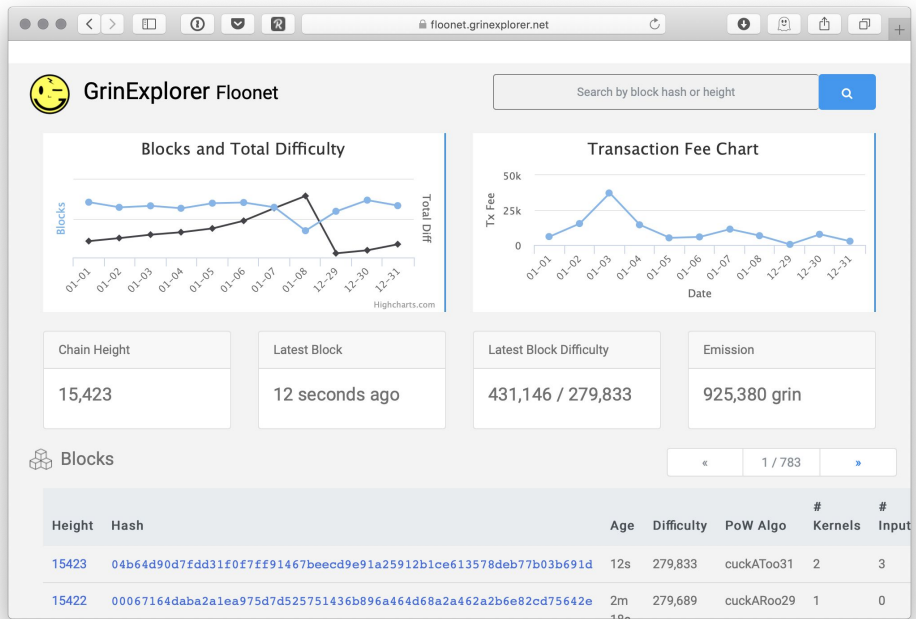


<https://github.com/grin-pool/grin-pool>





<https://grinscan.net>



<https://floonet.grinexplorer.net>



Grin intro // 08.01.2019 // Grin London



Hats (6)



Shirts (24)



Sweaters (15)



Accessories (16)



Books (1)



Holiday (5)

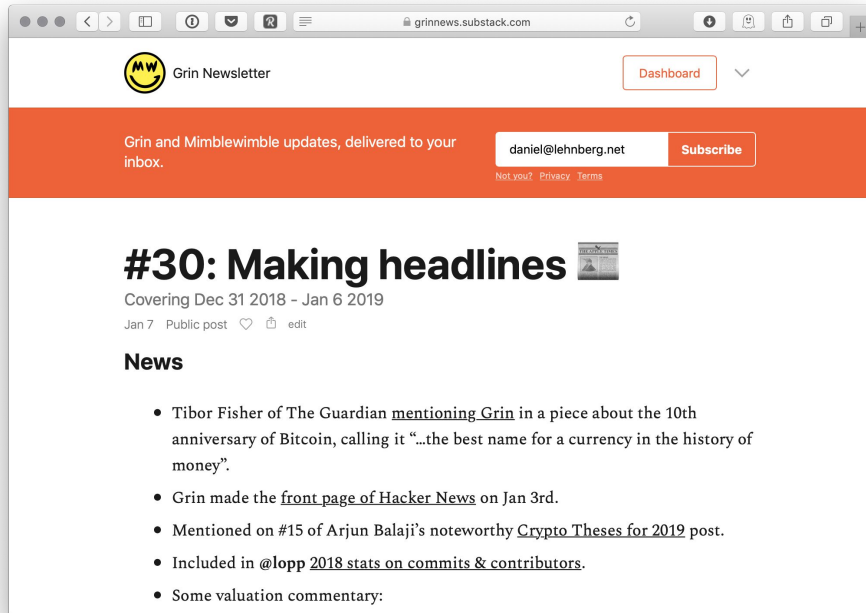
<https://tmgox.com>





<https://grin-hub.org>





<https://grinnews.substack.com>



Contributing

“JUST DO IT.”

– @hashmap



We need you!

Rust developers

Researchers

Frontend developers

UI/UX specialists

Graphic designers

Technical writers

Community members



Get involved

- Don't ask for permission, the project is open source.
- Be excessively polite and nice.

<https://github.com/mimblewimble/grin>

<https://grin-tech.org>



Fund @yeastplume

To work full time on Grin, March - Aug 2019

Goal: Crypto equivalent of €55,000

Good way to protect your Grin investment.

<https://www.grin-forum.org/t/funding-campaign-yeastplume-march-to-aug-2019/1697>



Take a technical crash course

<https://grincon.org>

What is Grin

Contributing

Dandelion

Wallet

Atomic Swaps

Proof of Work

Panel



Questions?



telegram/gitter/keybase/twitter: @lehnberg