grincon<US>(0)
19.01.28 // hero city, san mateo (CA)

A layperson’s intro to Grin

@lehnberg

Value prop?

1.

“Good design is as little design as possible”

- Dieter Rams

2.

“The worst enemy of life, freedom and the common decencies is total anarchy; their second worst enemy is total efficiency”

- Aldous Huxley

3.

“Don’t take out a wallet full of cash when you pay in a bar”

- Vasilios Nerantzidis (grandpa)

Contents

- Protocol
- Project
- Implementation
- Proof of work
- Status
- Community projects
- Contributing
- Value prop
- Questions

Protocol

Mimblewimble

- Proposed by Jedusor (2016), improved by Poelstra (2016).
- New blockchain design, relying on concepts in Confidential Transactions (Maxwell 2016), CoinJoin (Maxwell 2013), and OWAS (Mouton 2013).
- 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?

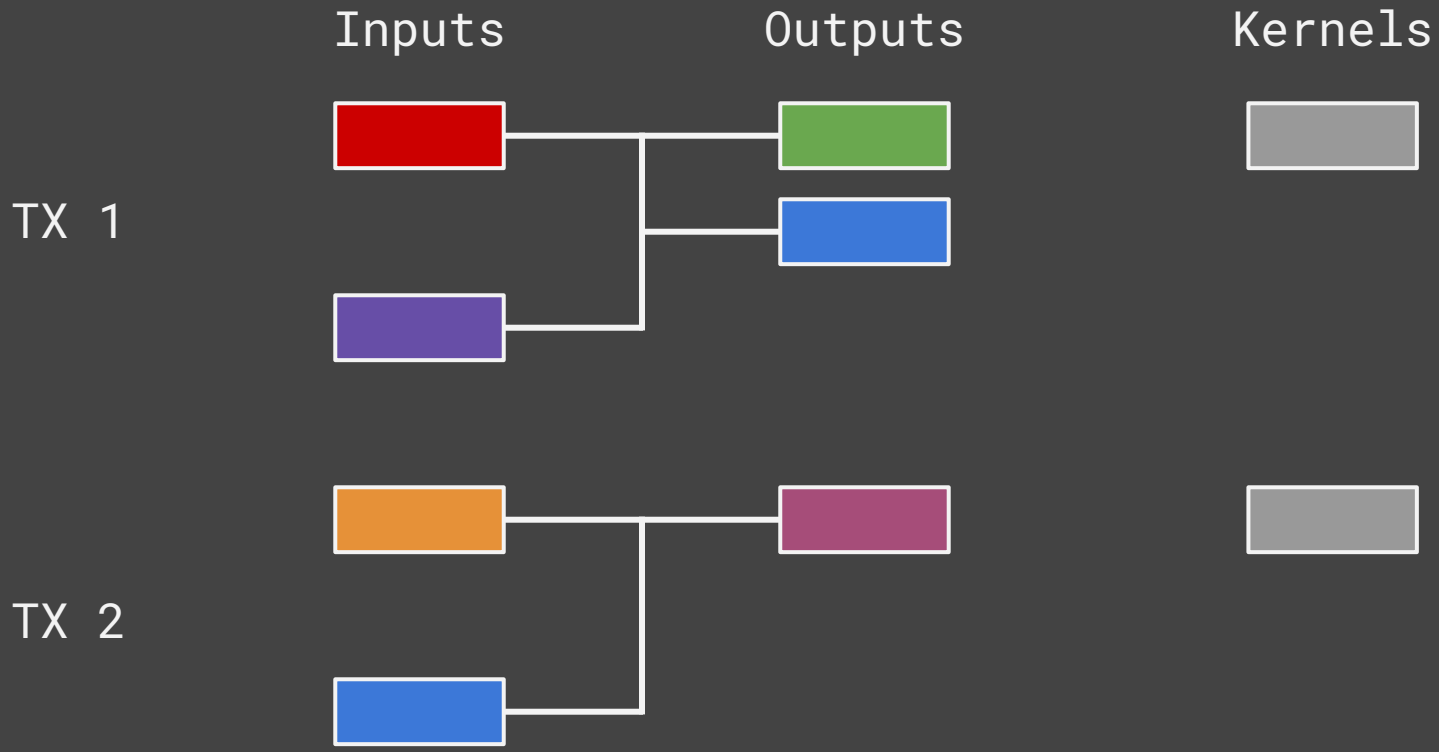
Interactive transaction building

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

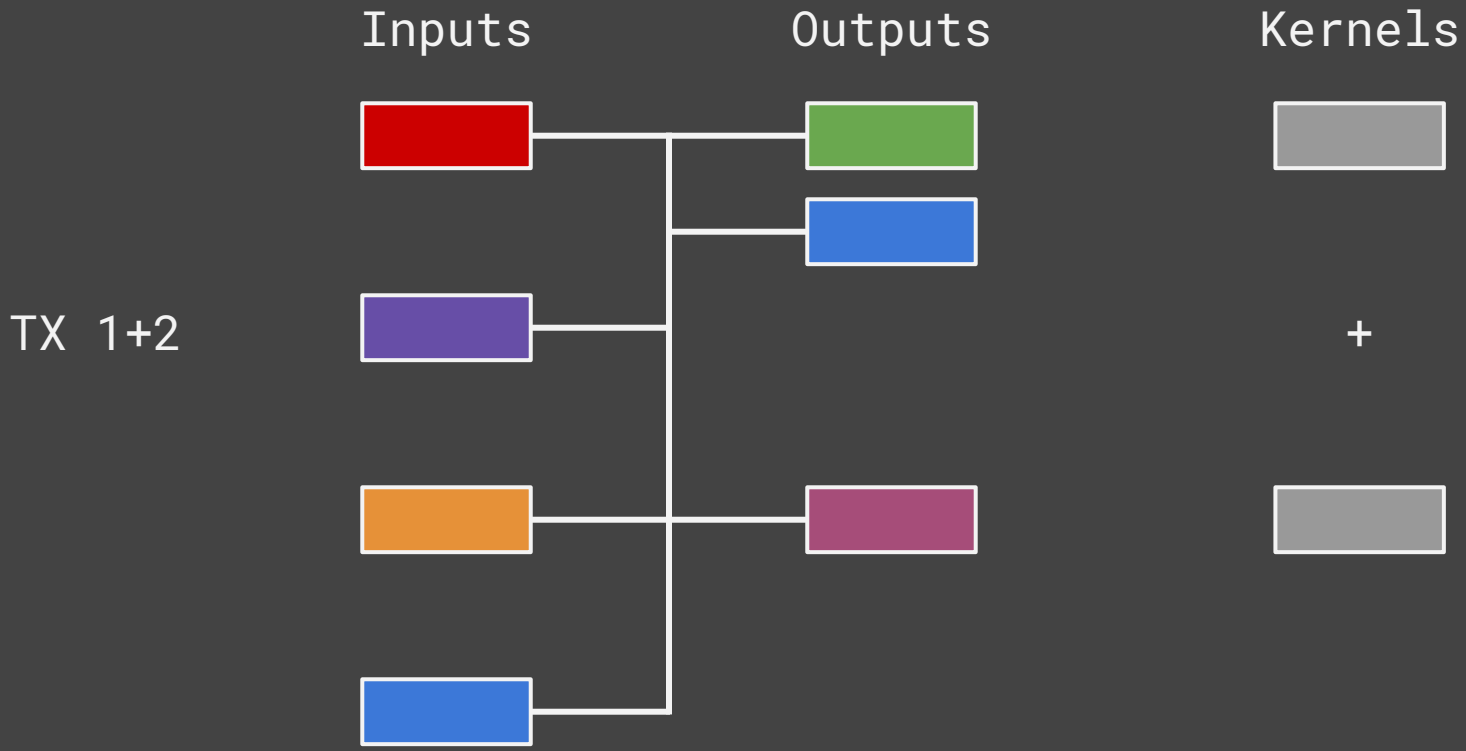
Also possible in reverse (invoicing)

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

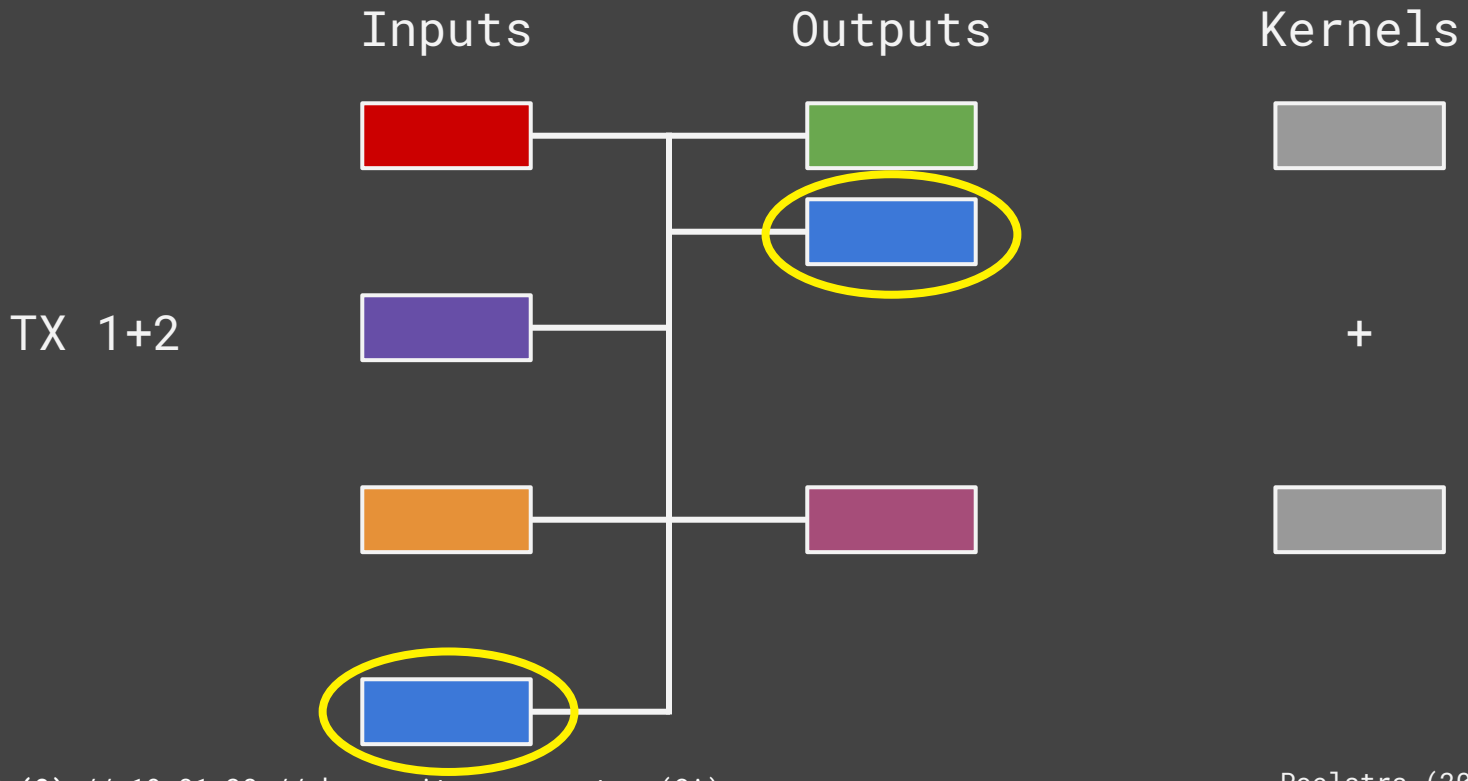
Transactions...



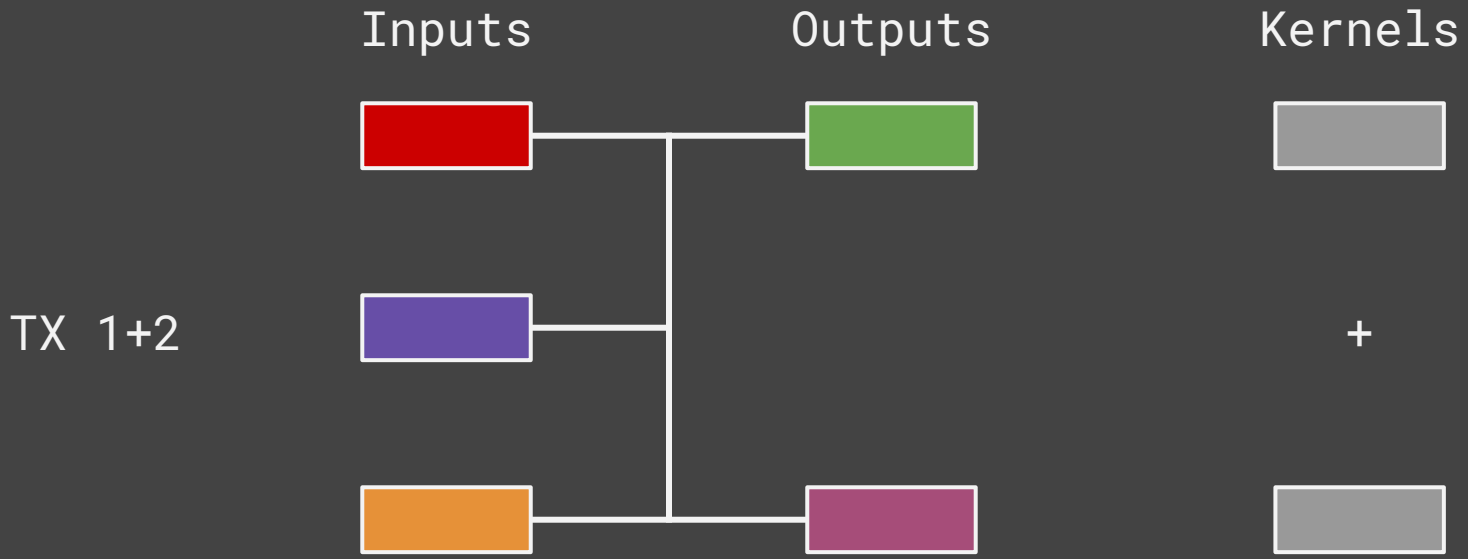
...can be joined together.



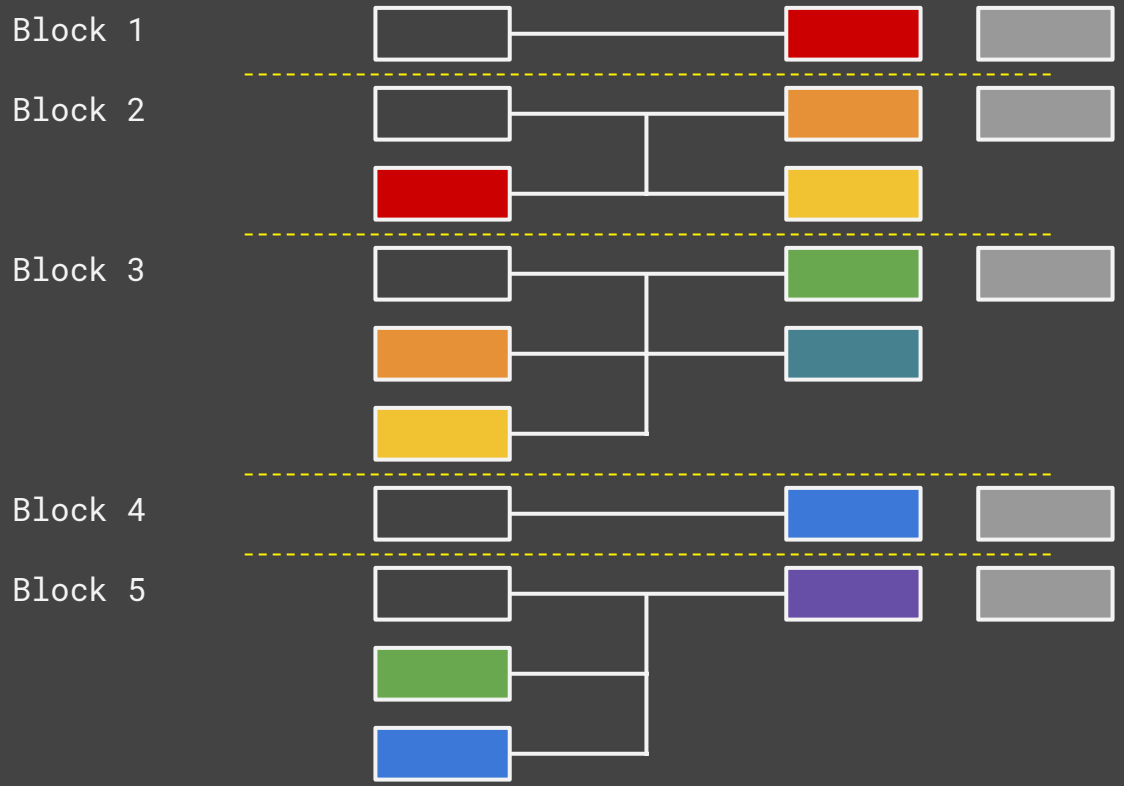
And outputs later used as inputs...



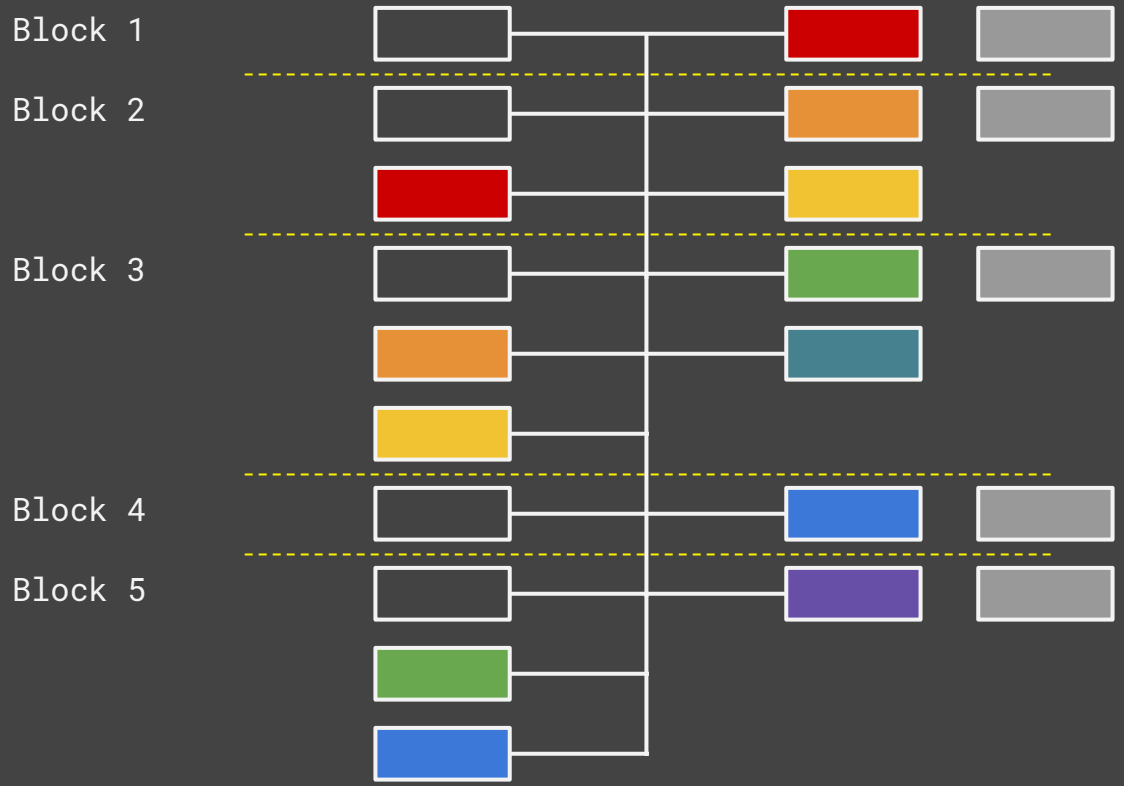
...can be discarded.



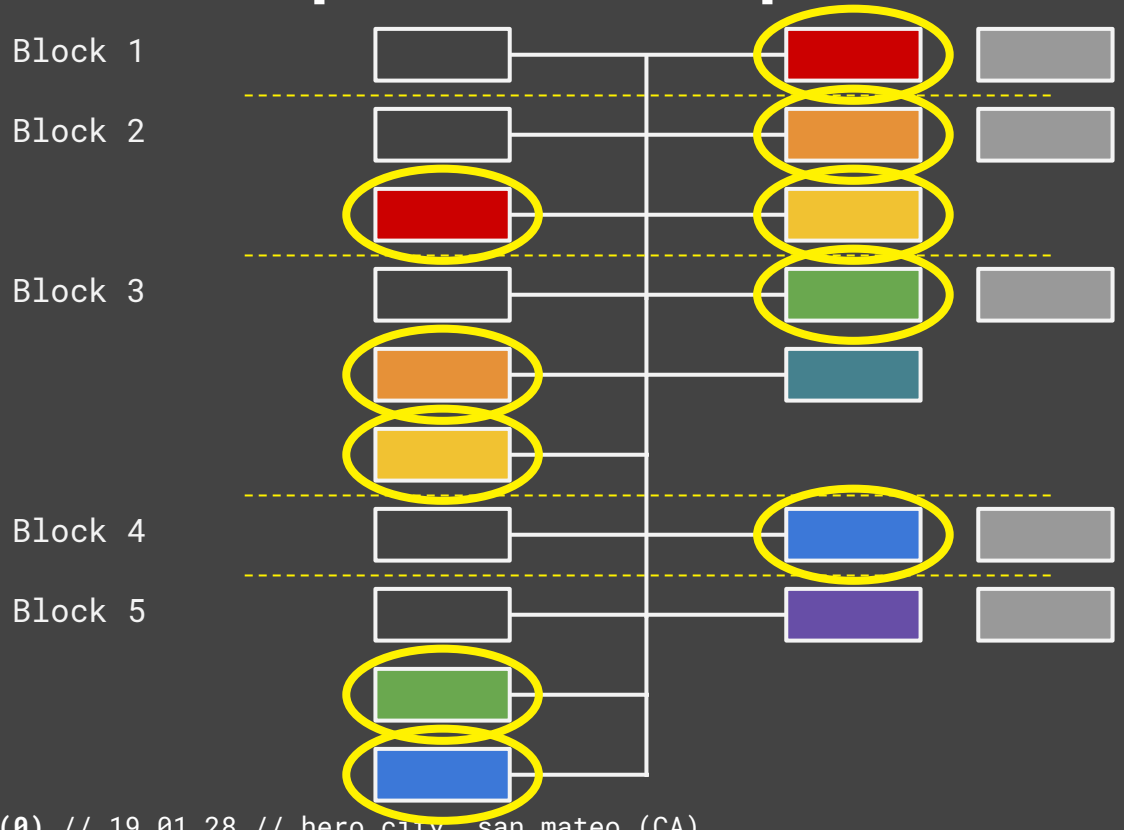
Similarly, the blockchain...



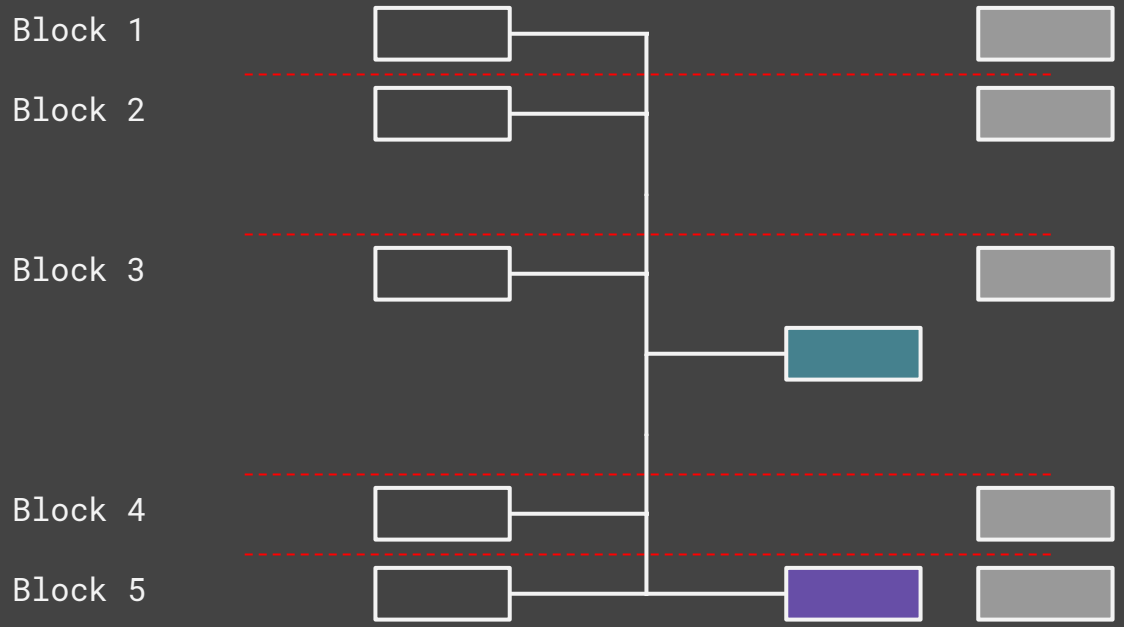
...can be joined.



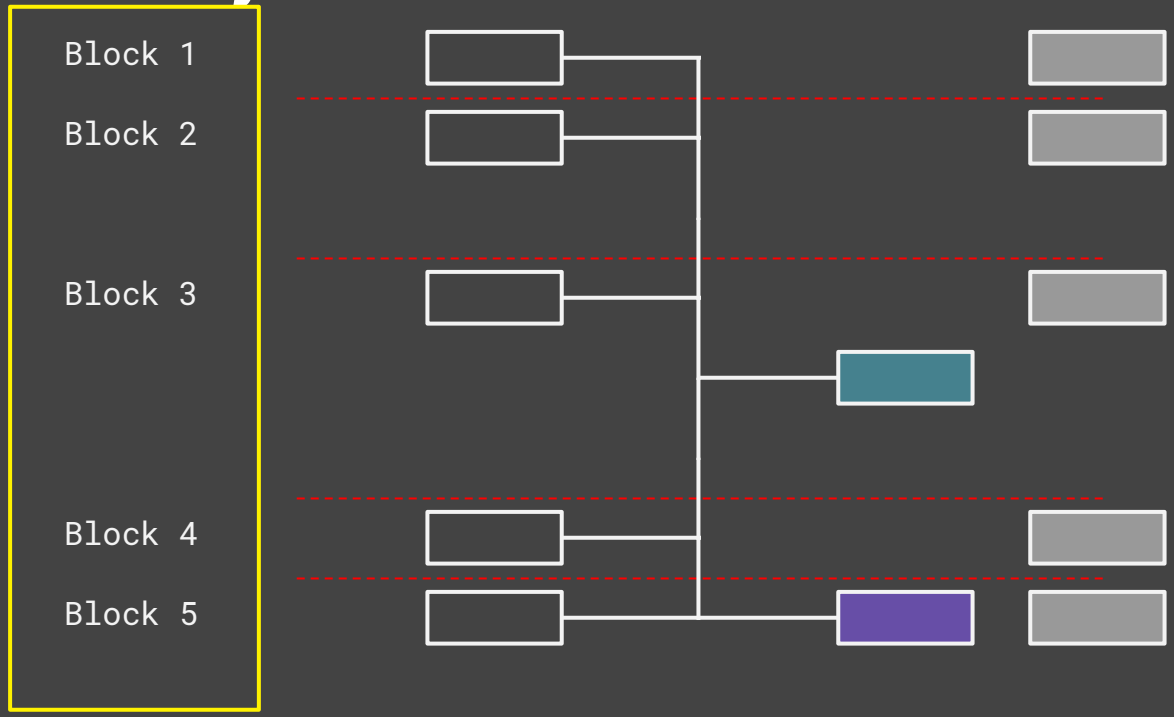
And when outputs are spent...



...they can be removed.

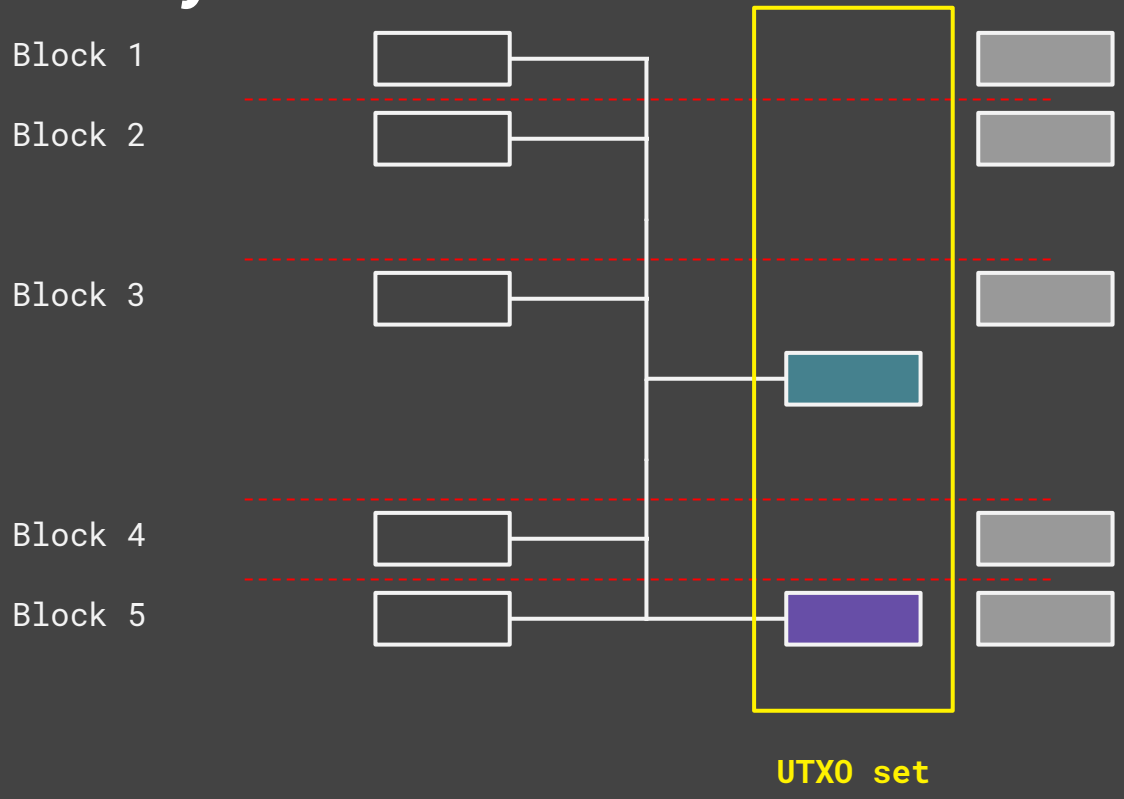


Initial sync

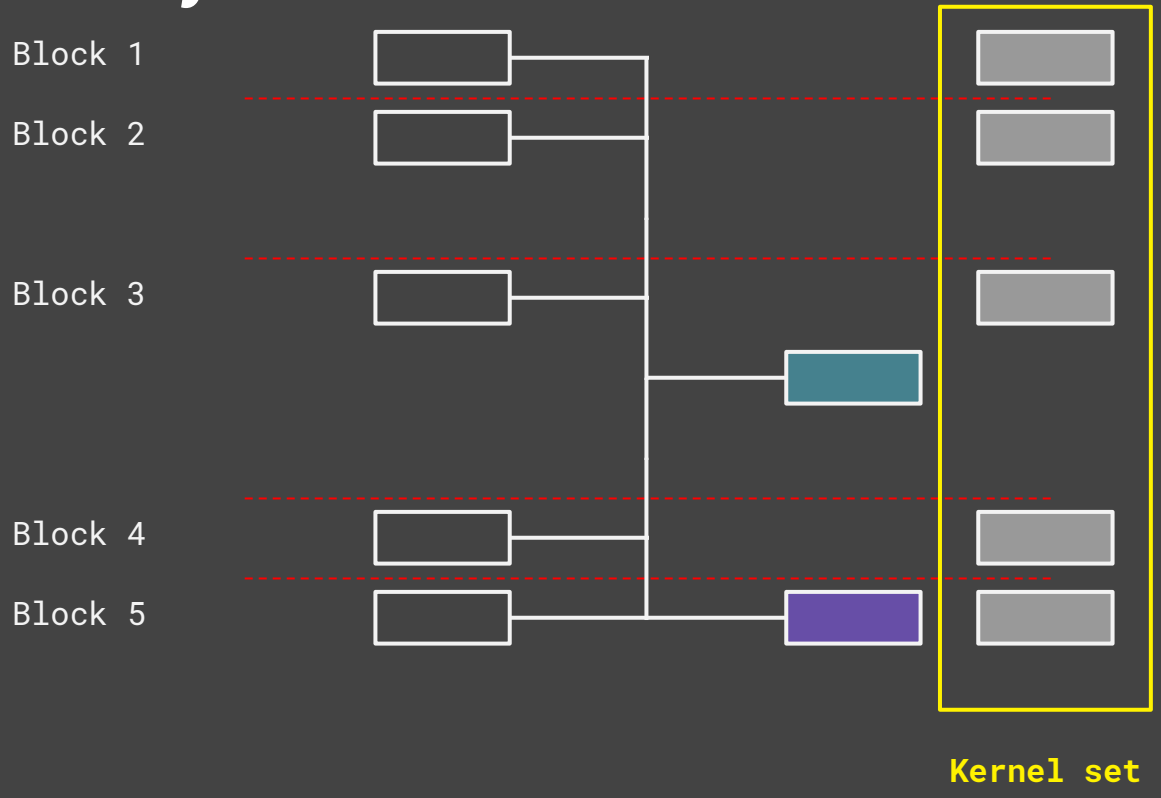


Block headers

Initial sync



Initial sync



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 Mimblewimble 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

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.

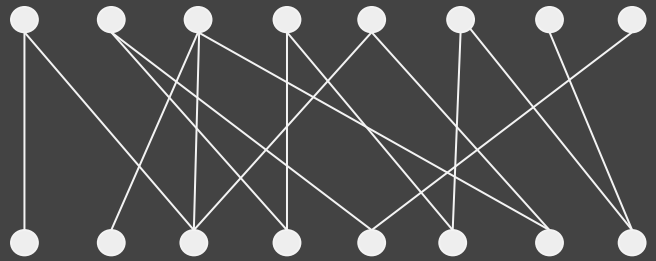
Proof of work mined.
One minute block time.
60 grin constant coinbase reward.

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

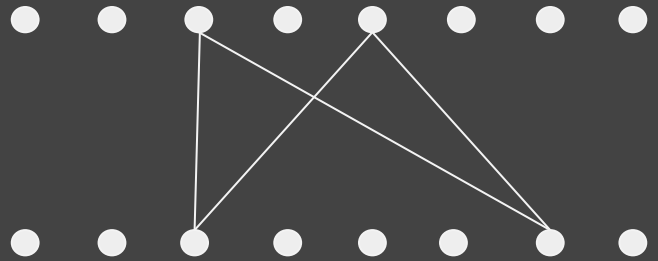
Proof of Work

Cuckoo Cycle family

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



Begin with a mess

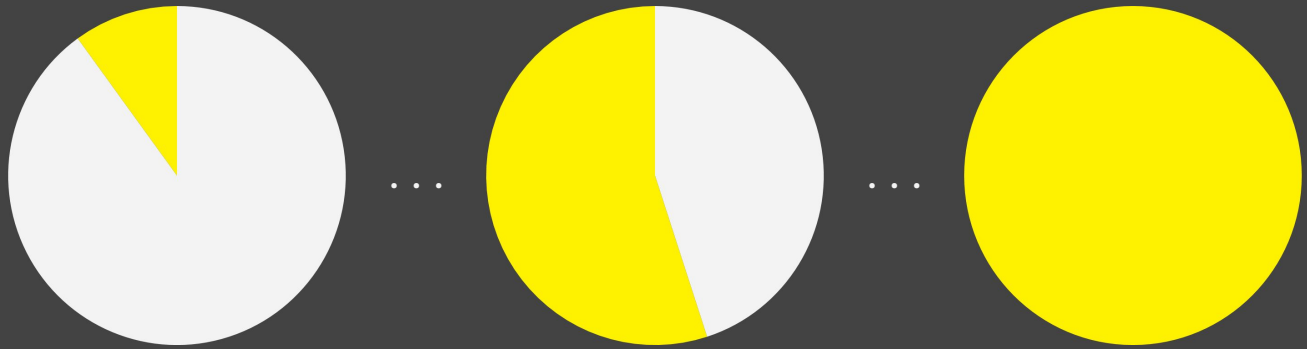


End up with a cycle

Grin Mainnet PoWs

For GPUs: **CuckARoo29**

For ASICs: **CuckATOO31+**



Launch:
10% AT
90% AR

Year 1:
55% AT
45% AR

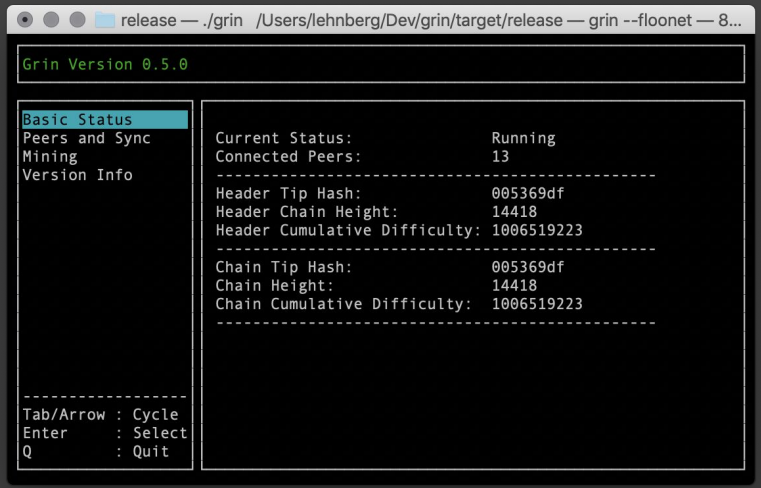
Year 2:
100% AT
0% AR

Status

Launched
Jan 15 2019

What's in the box?

- **Node.** Mining protocol.
- **Wallet.** Basic commands. Transactions via file, keybase, http(s)
- **Miner.** Nvidia and AMD plugins for both algos.



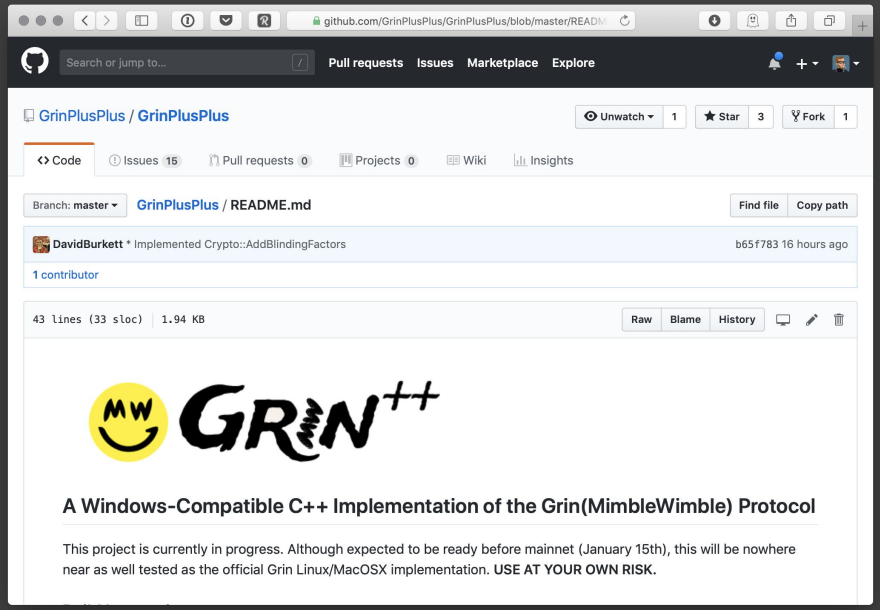
What's next?

- Quality of life
- Security
- Stability
- Performance
- Documentation
- Ecosystem support

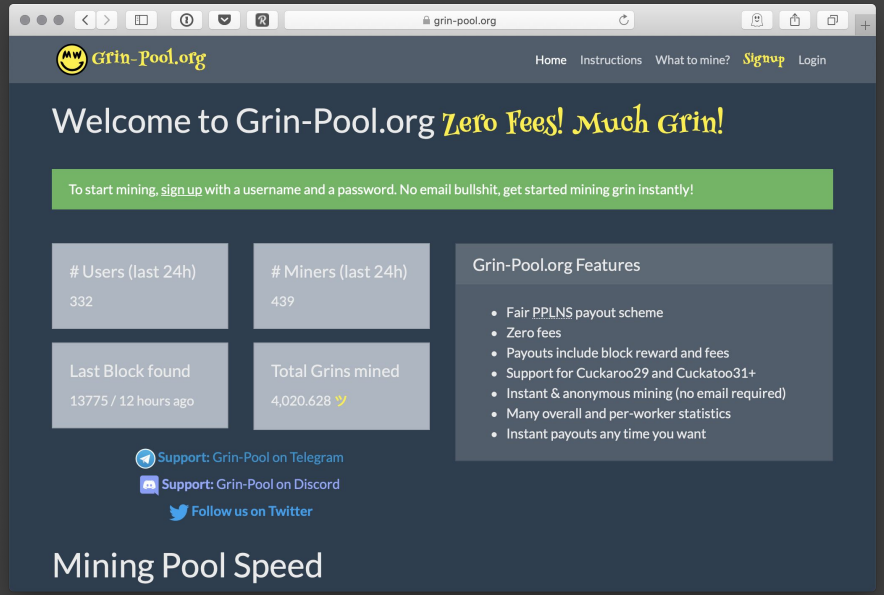
Exchange integrations

- We don’t do applications.
- We don’t do NDAs.(There is no legal entity.)
- We don’t pay listing fees. We’re broke.
- We do try to be helpful.
- We do welcome integrations,
  (...and contributions to the dev fund).

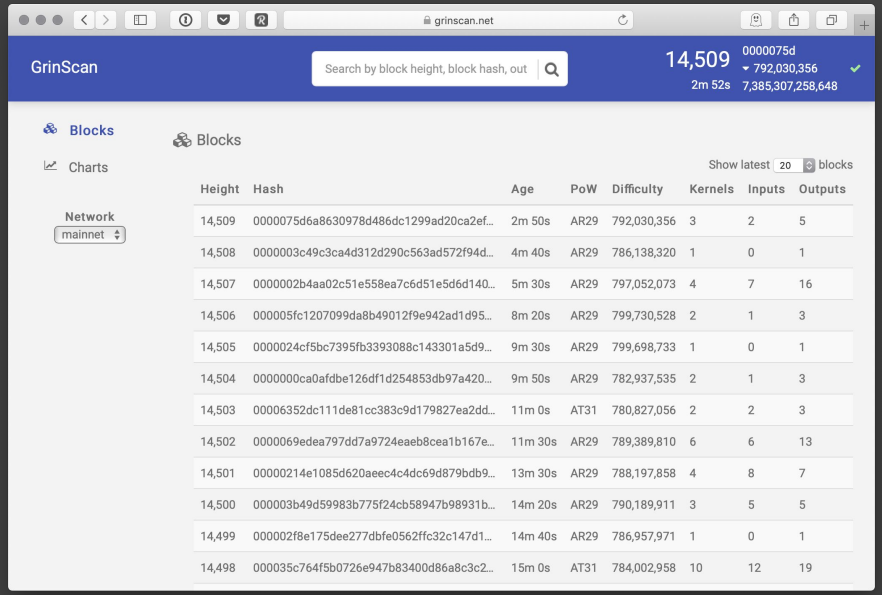
Selected community projects



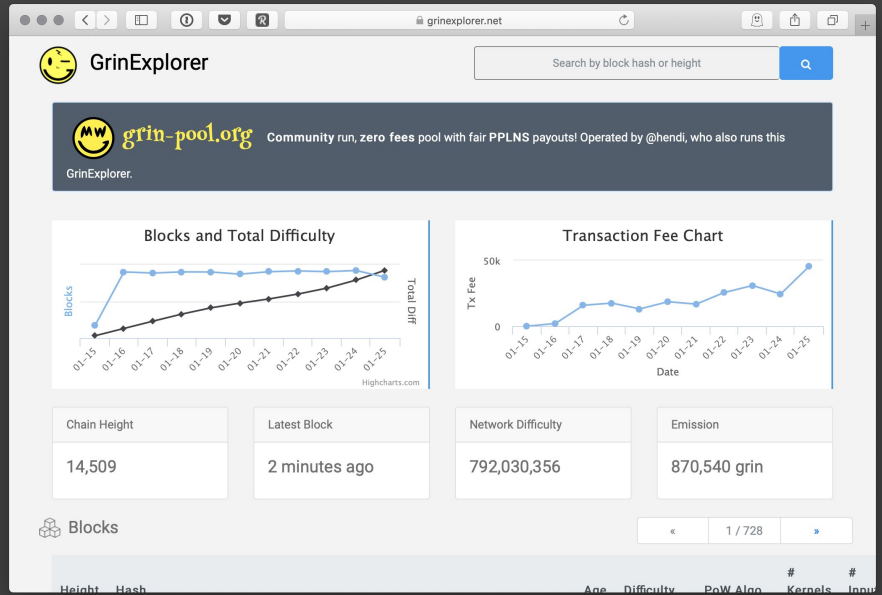
https://github.com/GrinPlusPlus/GrinPlusPlus



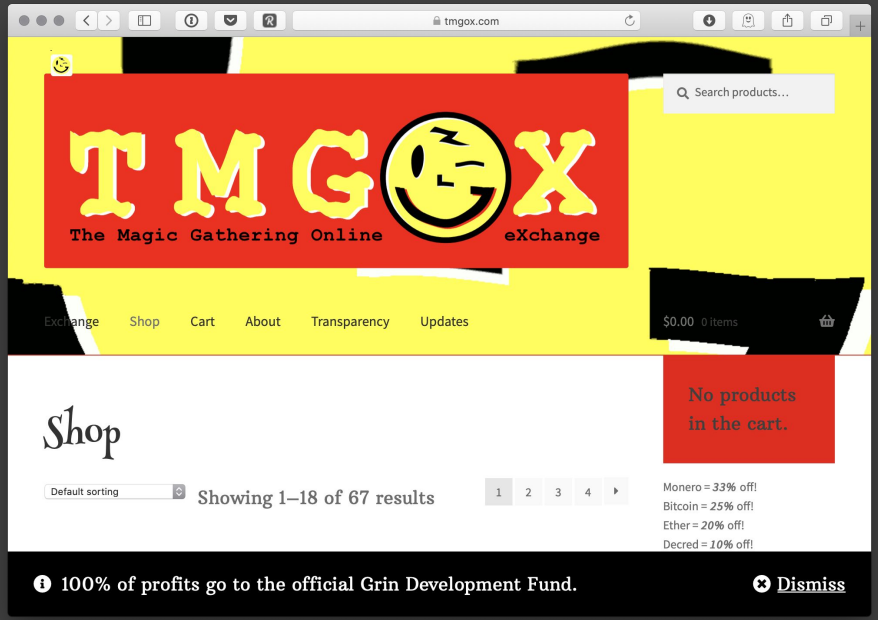
https://grin-pool.org



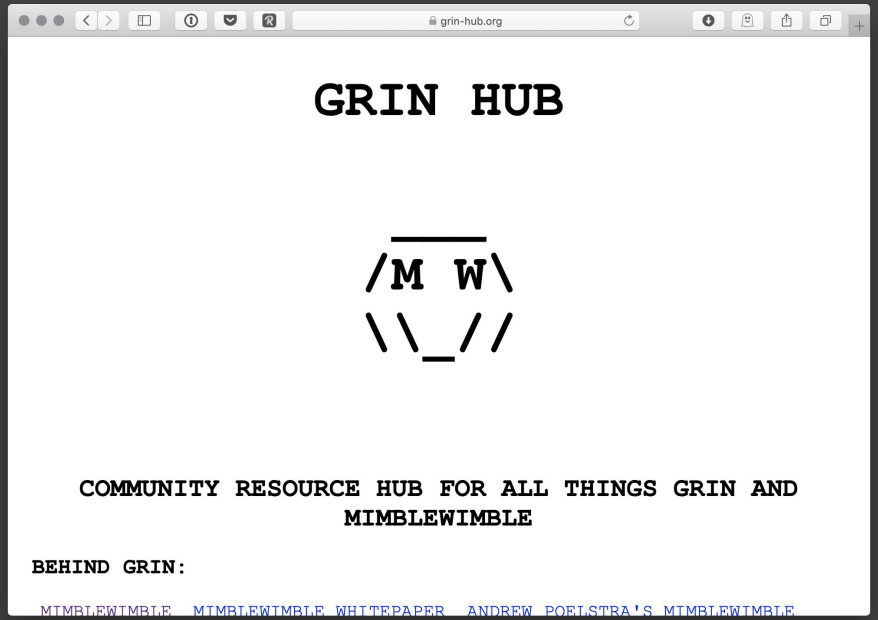
https://grinscan.net



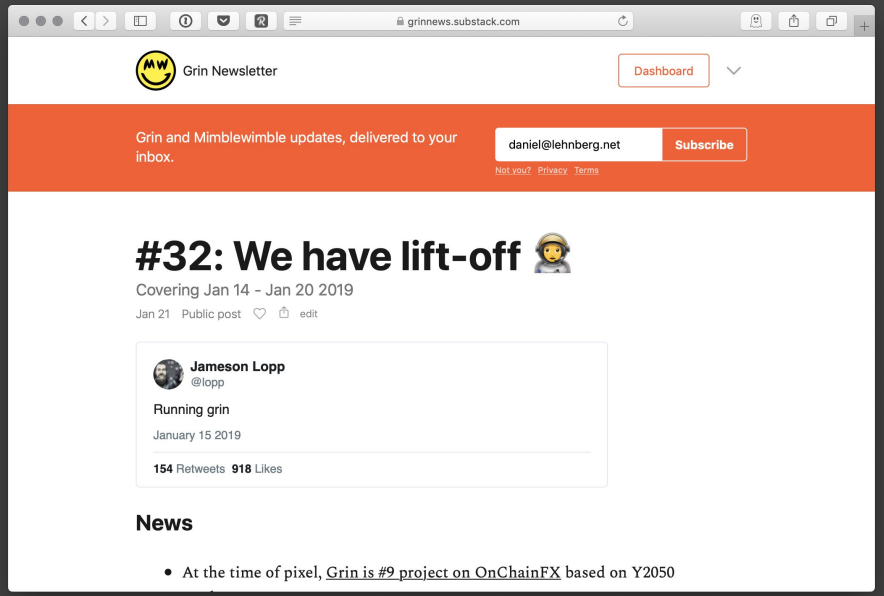
https://grinexplorer.net



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

Value proposition

Value proposition

Grin is not perfectly private. Yet.
But it does the job quite well.

It’s minimal in design. That’s hard.
And very attractive.

Grin does not like centrality or hierarchies.
This helps sustainability in the long term.

Value proposition (cont'd)

Privacy is turned on by default.
And can only selectively be turned off.

Being community driven is a core strength.
Not a weakness.

The fair launch and emission schedule
align interests and protect integrity.

Questions?

telegram/gitter/keybase/twitter: **@lehnberg**