



Grin Amsterdam

26.03.2019 // Amsterdam

Grin update

@lehnberg

Contents

- Grin tl;dr
- Development
- Governance
- Security
- Ecosystem
- Contributing
- Quick Q&A



Grin t1;dr

Grin: Better money ツ

A lightweight implementation of a cryptocurrency that aims to be privacy preserving, scalable, and fair.

- First implementation of Mimblewimble.
- No amounts, no scripts, no addresses, no opt-in privacy, in a simple protocol.
- Sender and Receiver interact to build transactions.
- Written in Rust by an open source community.
- Fairly launched, fairly mined, funded by donations.
- 1 grin/s emission, forever.



Development

Dev snapshot

Join the next meeting:
Apr 2 @ 3PM UTC on Gitter

Effort	Release	Includes
v1.0.0	Jan 15	Baseline node, wallet, miner
v1.0.1	Feb 01	Bug fixes, wallet perf, mining perf
v1.0.2	Feb 25	Critical vulnerability patch, bug fixes and perf
v1.0.3	This week	Bug fixes and performance improvements
v1.1.0	w/c Apr 8	Win support, standalone wallet, dandelion++, hooks
Research	Ongoing	i2p, verifiable transactions, variable size MMRs



Governance

Governance

Join the next meeting:

Apr 9 @ 3PM UTC on Gitter

Decision on Security Auditing firm

Income and spending logs now public on /grin-pm

Q12019 transparency report due in April

Friends of Grin includes Hall of Fame section

Ignotus Peverell is funded for three months

Antioch Peverell secured funding from an unnamed company



Security

Security

libsecp fork audited by JP Aumasson before launch

Coinspect working on audit of crates, report due Apr 20

Critical vulnerability CVE-2019-9195 discovered, patch released within 72 hours

Additional findings from audit are being patched on ongoing basis

We are reviewing our vulnerability disclosure and security processes, please participate

Mainnet is <70 days old. Grin is *highly* experimental software.



Ecosystem

Ecosystem

Join the next meeting:

Apr 9 @ 5PM UTC on Gitter

5+ mining pools, more to be announced

5+ different mining software providers

10+ exchanges added Grin voluntarily so far

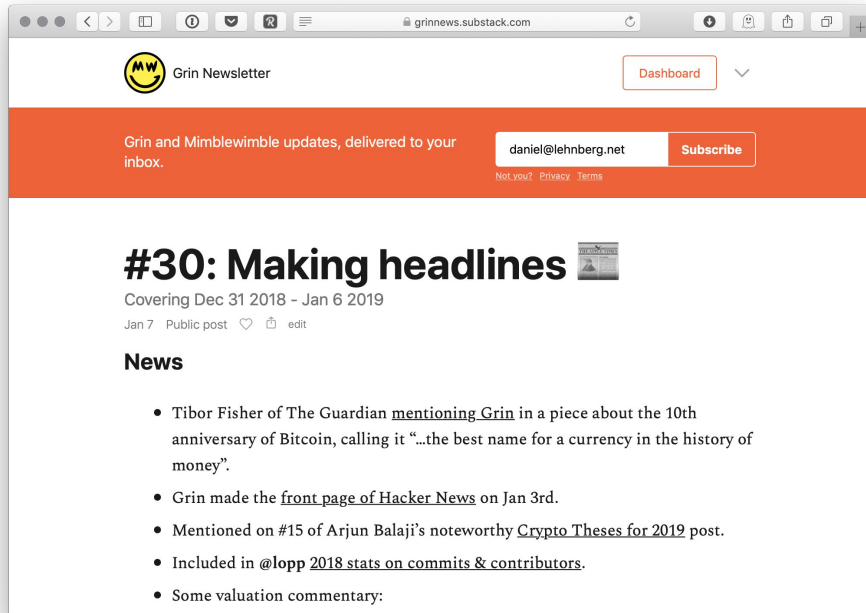
3+ ASICs announced, some details of Obelisk GRN1 released

Grin++: a C++ implementation of node + wallet

cycle42: Team building mobile wallet & merchant processor

vault713: Team building wallet713 & grinbox transaction protocol





<https://grinnews.substack.com>



Contributing

Get involved

Don't ask for permission, the project is open source.

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

Fund the project

A good way to protect your grins and the integrity of mankind.

<https://grin-tech.org/funding>

“JUST DO IT.”

– @hashmap



Take a technical crash course

<https://github.com/mimblewimble/grin-pm#presentations>

grincon0, Berlin

What is Grin

Contributing

Dandelion

Wallet

Atomic Swaps

Proof of Work

Panel

grincon.US, San Mateo CA

Grin value proposition

Security audit

Scriptless scripts

How to mine

Privacy & scalability

RSA Accumulators

...and more



Questions?



telegram/gitter/keybase/twitter: @lehnberg