

Grin:
as little as possible

@hashmap
Web3 Summit 2019





“Good design is as little design as possible”
Dieter Rams

Source: https://en.wikipedia.org/wiki/Dieter_Rams#/media/File:Braun_T1000CD.jpg

What is Grin?

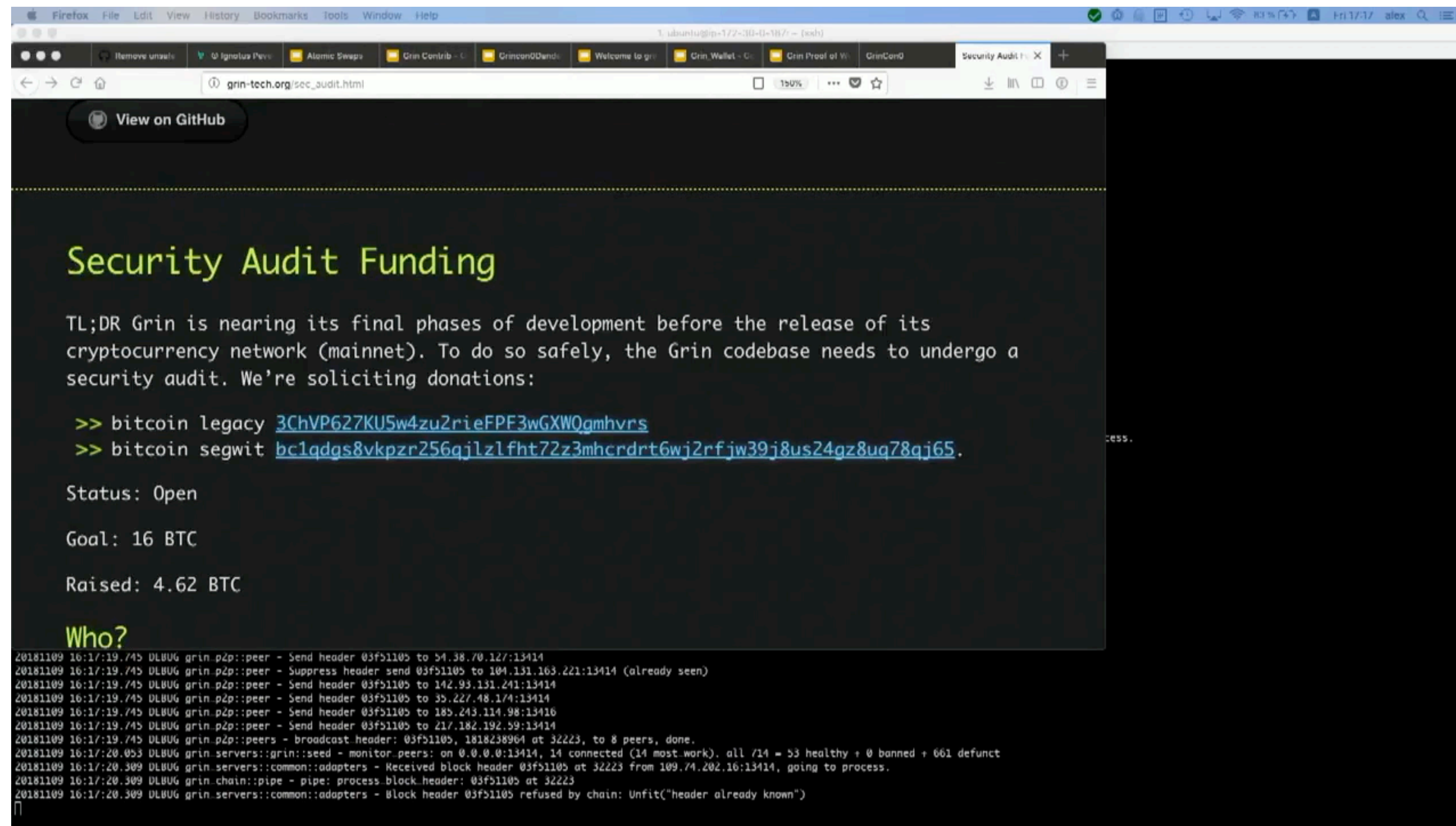
Better money ツ

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

Ignotus Peverell

(text-to-speech over SSH)

Grincon0, Berlin, November 9th 2018



Firefox File Edit View History Bookmarks Tools Window Help

grin-tech.org/sec_audit.html

View on GitHub

Security Audit Funding

TL;DR Grin is nearing its final phases of development before the release of its cryptocurrency network (mainnet). To do so safely, the Grin codebase needs to undergo a security audit. We're soliciting donations:

- >> bitcoin legacy [3ChVP627KU5w4zu2rieFPF3wGXWQgmhvrs](#)
- >> bitcoin segwit [bc1qdqs8vcpzr256qjlz1fht72z3mhcrdrt6wj2rfjw39j8us24gz8uq78qj65.](#)

Status: Open

Goal: 16 BTC

Raised: 4.62 BTC

Who?

```
20181109 16:17:19.745 DLBUUG grin.p2p::peer - Send header 03fb1105 to 54.38.70.127:13414
20181109 16:17:19.745 DLBUUG grin.p2p::peer - Suppress header send 03fb1105 to 104.131.163.221:13414 (already seen)
20181109 16:17:19.745 DLBUUG grin.p2p::peer - Send header 03fb1105 to 142.93.131.241:13414
20181109 16:17:19.745 DLBUUG grin.p2p::peer - Send header 03fb1105 to 35.227.48.174:13414
20181109 16:17:19.745 DLBUUG grin.p2p::peer - Send header 03fb1105 to 185.243.114.98:13416
20181109 16:17:19.745 DLBUUG grin.p2p::peer - Send header 03fb1105 to 217.182.192.59:13414
20181109 16:17:19.745 DLBUUG grin.p2p::peers - broadcast header: 03fb1105, 1818238964 at 32223, to 8 peers, done.
20181109 16:17:20.053 DLBUUG grin.servers::grin::seed - monitor.peers: on 0.0.0.0:13414, 14 connected (14 most work), all /14 = 53 healthy + 0 banned + 661 defunct
20181109 16:17:20.309 DLBUUG grin.servers::common::adapters - Received block header 03fb1105 at 32223 from 109.74.202.16:13414, going to process.
20181109 16:17:20.309 DLBUUG grin.chain::pipe - pipe: process block header: 03fb1105 at 32223
20181109 16:17:20.309 DLBUUG grin.servers::common::adapters - Block header 03fb1105 refused by chain: Unfit("header already known")
[]
```

Lightweight / minimal Fair

 [mimblewimble](#) / [grin](#)

 Code

 Issues **113**

 Pull requests **18**

 Projects

Minimal implementation of the MimbleWimble protocol.

**Minimal and fair:
Grin coin**

Mimblewimble properties

- Scalable: Little data required for full sync.
- Fungible: No amounts, no scripts, no addresses.
- Proven math (Elliptic Curves Cryptography).
- Easy to understand.

Grin Block

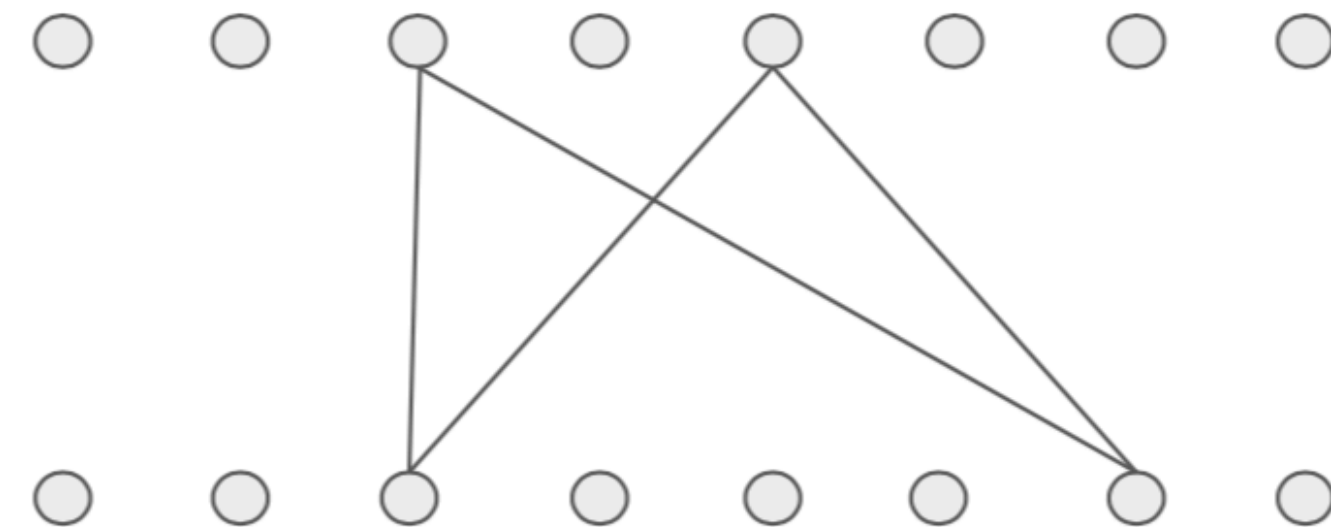
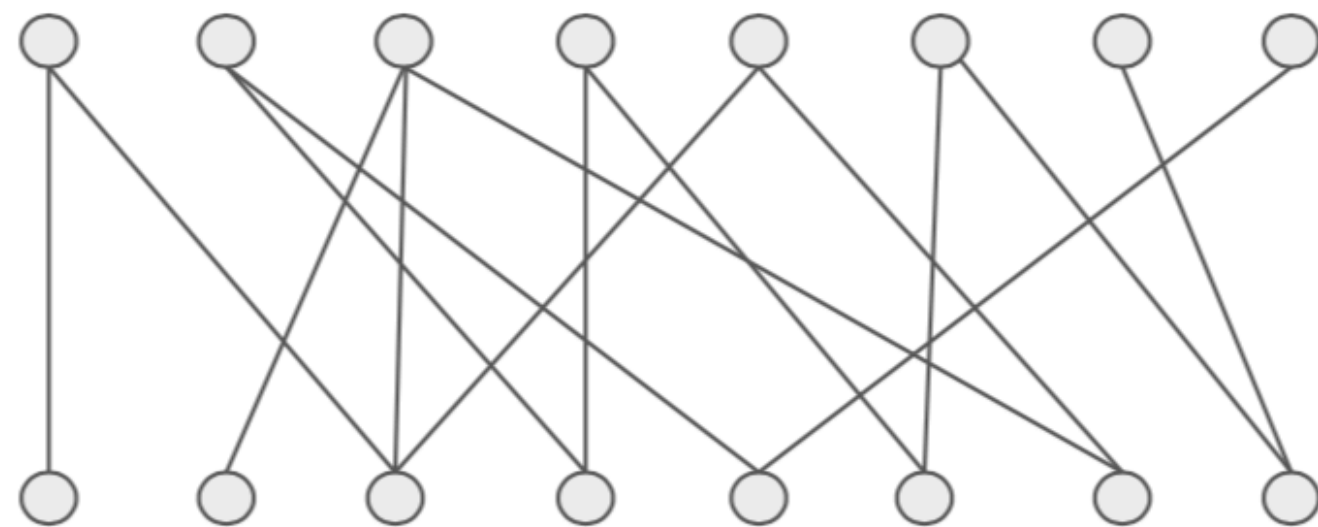
Reward	60 + 0.024 Grin							
Kernels (4)	#	Type	Excess				Fee	Lock height
	0	Height locked	0910f06c5bf7d169721dbd990df9483a9e996769ca003d316542ab7e6cadf42852				0.008	252,046
	1	Coinbase	08551fa43bd4b2eb04a2b8f35cf75ef20312d037df28874651c99c3970ae6941a8					
	2	Height locked	08686fe9bd56d8a71640054326edb8f06bba690f4d2c874a9c3912cef5172a3f90				0.008	252,046
	3	Height locked	083eebac49b1eaa557909669173a9d6b35377bf9bd23cb2b92cd9f00343ae39660				0.008	252,046
Inputs (3)	#	Type	Maturity	Commit				
	0		128	089f117f4a36c155fd64cd281b8bcd20713961e1ed21e4c9a5522638bbc0b7018e				
	1		128	081de02e4bd57d7fd259a3e08cc5615956cef7b3dc1f853417cccec83e90895e66				
	2		128	09101115fe29dffe9a24e17d741e25569f4ee63337cf3d01f2fa37a449ad3a967b				
Outputs (7)	#	Type	Commit					
	0		09d4a7f37e6706104d88aea243cd0315254984a8ba3721bef0d1cae6641fffe4c1					
	1	Coinbase	0856b2f1e7213f770adf98795890ec5418fe18659530ed83738525461add9e722a					
	2		085926e445d87ef7a93336e5d3baf0c847ba0e13fdbd34c4a2c003caf028d6b197					
	3		09a1d8289f0ad8dce00da68ed174fbbf3b757560e646bfda68c908329dc2745755					

Turtles all the way down

- Transaction (kernel(s), inputs, outputs)
- Block (kernels, inputs, outputs)
- Chain (kernels, inputs, outputs)

Proof of work

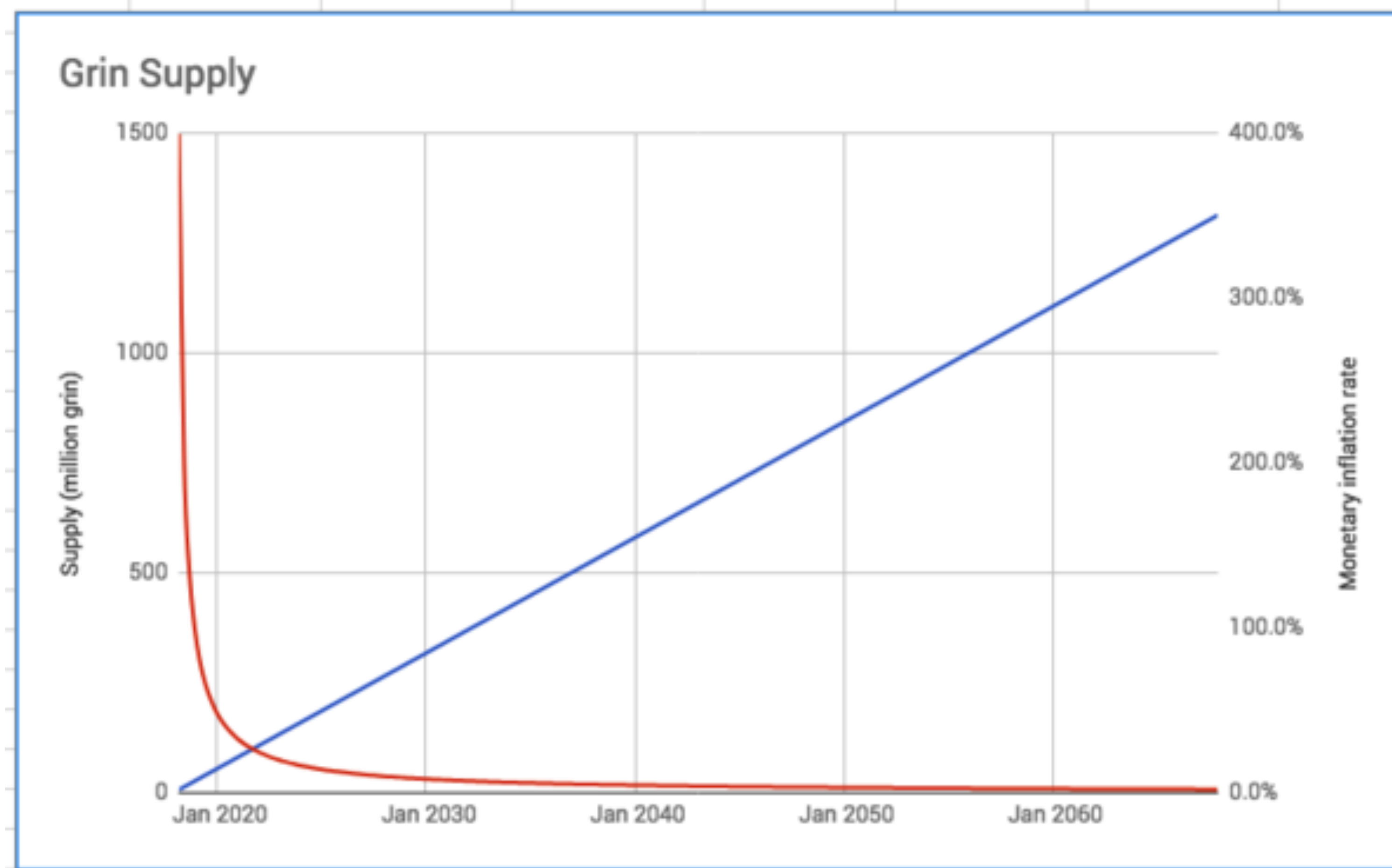
- Finding 42-cycles in random bipartite graphs with billions of nodes
- Simplest known PoW
(the spec is 42 lines of code)



Linear emission

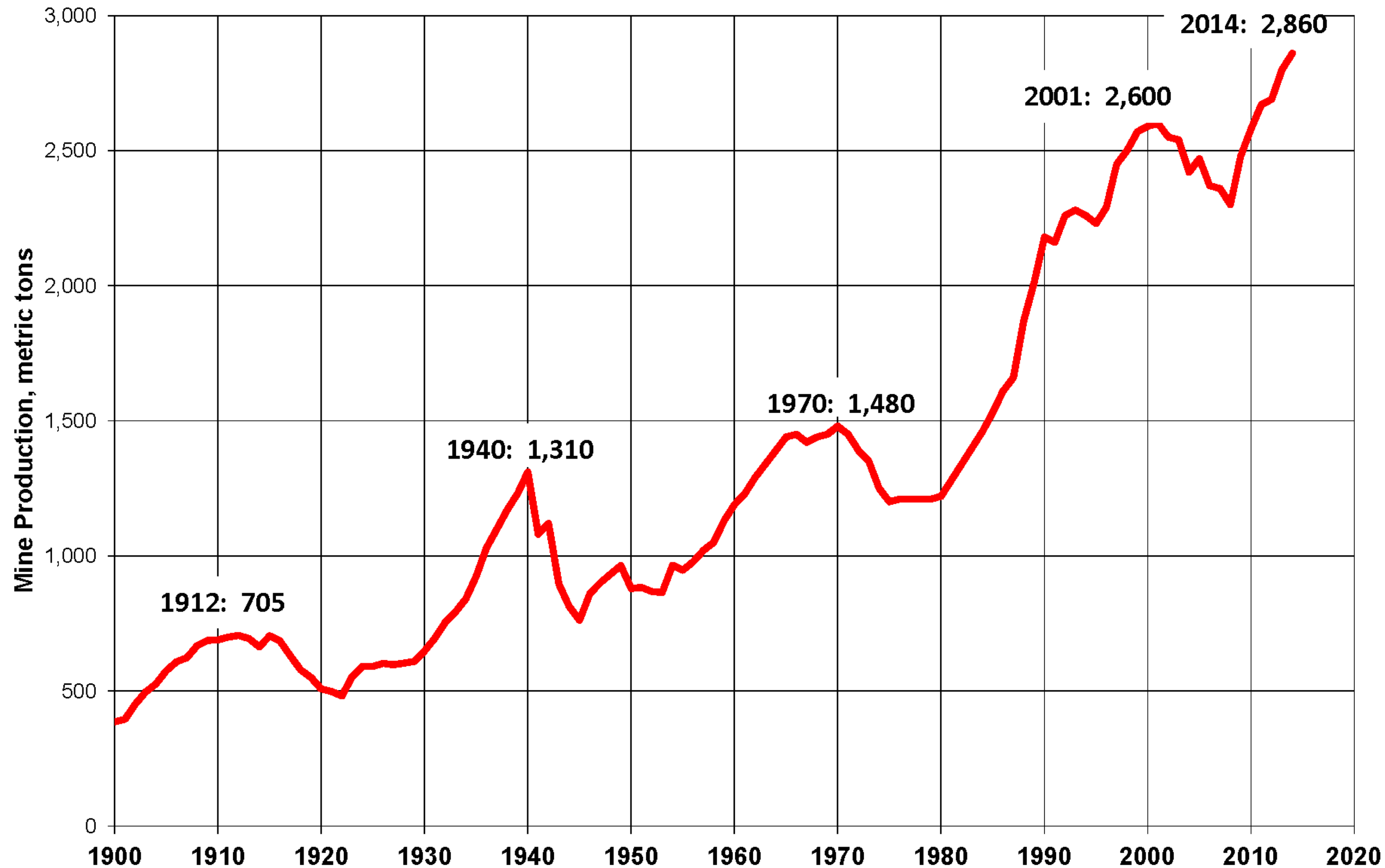
- 1 grin / second
- Forever
- Simple and fair

Grin supply and inflation



Source: <https://www.getrevue.co/profile/zpx/issues/grin-finally-bares-itself-155455>

Annual world mined gold production, 1900-2014



Source: https://en.wikipedia.org/wiki/Gold_mining#/media/File:World_Gold_Production_1900-2014.png

Fair launch

- No ICO, premine, dev tax
- Open launch in the Gitter chat
- ~ 100 000 GPUs at day 1

**Minimal and fair:
Grin development**

Codebase size (node)

Language	files	blank	comment	code
Rust	189	5634	8414	35219
Markdown	63	3548	0	8014
TOML	15	49	5	457
YAML	6	5	13	268
Bourne Again Shell	2	12	33	42
Dockerfile	1	16	5	28
Bourne Shell	1	7	1	26
SUM:	277	9271	8471	44054

Growing Grin

- When XXX? When ready
- Add a feature only if it's really needed
- Remove a feature if it's hard to maintain
- Grin is like a tree (it doesn't grow, then it's bigger than you, then 50 years later you gone and your grandchildren play in the shades of tree)
- Collaboration, not competition

Switch commitments

- Quantum Armageddon insurance
- Implemented
- Removed
- Reimplemented

Git log

Switch commitments #179

Merged ignopeverell merged 11 commits into `mimblewimble:master` from `yeastplume:switch_commitments` on Oct 16, 2017

Removed all switch commitment usages, including restore #841

Merged ignopeverell merged 4 commits into `mimblewimble:master` from `unknown repository` on Mar 22, 2018

Conversation 4 Commits 4 Checks 0 Files changed 18



ignopeverell commented on Mar 21, 2018 • edited

Member



Reviewe

[Floonet] Switch commitments #2157

Merged yeastplume merged 1 commit into `mimblewimble:floonet` from `jaspervdm:switch_commitment_fix` on Dec 18, 2018

Conversation 2 Commits 1 Checks 0 Files changed 11



jaspervdm commented on Dec 14, 2018 • edited

Member



Reviewers

No reviews

Switch commitments removal



ignopeverell commented on Mar 21, 2018

Author

Member



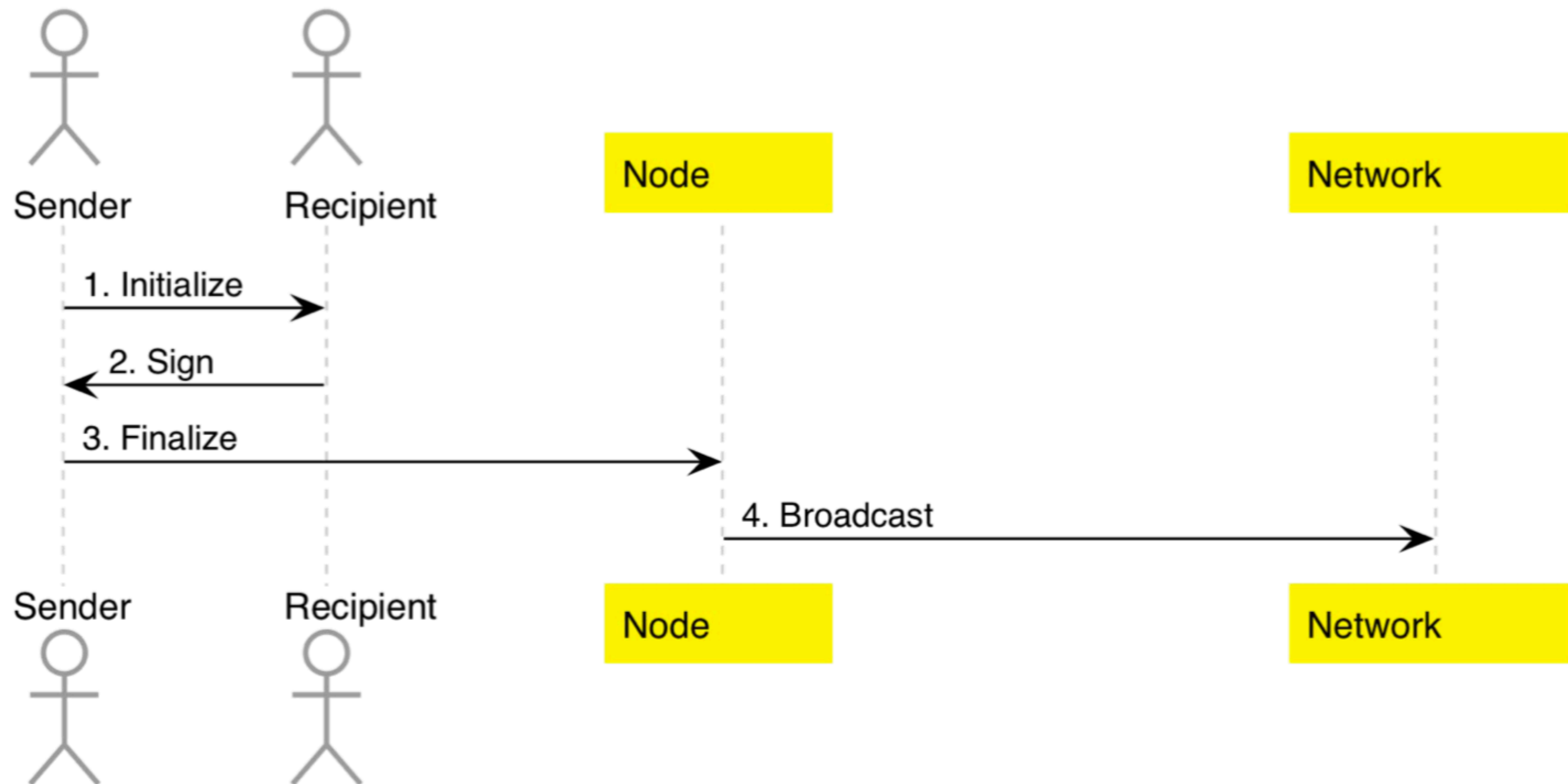
For reference, switch commitments were found to:

- add a lot of complexity and assumptions
- take additional space for little benefit right now
- allow the inclusion of arbitrary data, potentially for the worst
- provide little to no advantage in case of quantamageddon (as range proofs are still a weakness)

P2P connection limit

- Drop an incoming connection?
- Drop an existing connection?
- Accept new one and later one drop a connection? Which one?
- “Fair” was mentioned many times


Interactive transaction building





Transaction building relay

- Grin transaction are interactive
- Counter-party may be offline, intermediate storage?
- Use existing p2p network and node storage?
- Spam attack / resource abuse threat for the entire network and a particular node
- Multiple ad-hoc workarounds?
- Not simple, not fair
- Grinbox: a community project

Grin web wallet

WALLET

SEND

RECEIVE

GRIN

141300

Chain Height

Spendable: (Validated 0 Blocks Ago)

2539.9990

(0.0000 Unconfirmed or Immature)

[Wallet](#) / [Info](#)

Wallet Summary Info

Show Outputs

Last Validated at Block 141300 (0 Blocks Ago)

Total	2539.9990000000
Awaiting Confirmation	0.0000000000
Immature Coinbase	0.0000000000
Currently Spendable	2539.9990000000

(46.0900000000 is locked pending transaction confirmations)

Update and Validate against Node

Most Recent Transactions

Show All Transactions

16/10/2018, 19:35:34	Sent	-700.0010000000	Confirmed
16/10/2018, 19:35:32	Coinbase	60.0000000000	Confirmed
16/10/2018, 19:35:32	Coinbase	60.0000000000	Confirmed
16/10/2018, 19:35:32	Coinbase	60.0000000000	Confirmed
16/10/2018, 19:35:32	Coinbase	60.0000000000	Confirmed
16/10/2018, 19:35:32	Coinbase	60.0000000000	Confirmed
16/10/2018, 19:35:32	Coinbase	60.0000000000	Confirmed
16/10/2018, 19:35:32	Coinbase	60.0000000000	Confirmed


<https://github.com/mimblewimble/grin-web-wallet>

Grin web wallet tech stack

- JavaScript / Angular
- HTML / CSS

Guess what happened

This repository has been archived by the owner. It is now read-only.

 [mimblewimble](#) / [grin-web-wallet](#) Archived

Watch ▾13

★ Star37

🍴 Fork17

<> Code

⚠ Issues 5

🔗 Pull requests 2

📁 Projects 0

📖 Wiki

🛡 Security

📊 Insights

Grin WebUI Wallet

wallet

webapp

grin

cryptocurrency

🔄 30 commits

🌿 1 branch

🏷 3 releases

👤 3 contributors

No “official” GUI wallet

- What?! Even Satoshi created Bitcoin-QT!
- Exactly
- We rely on the community

Wallets

- [Wallet 713](#) is a command line wallet that integrates with [Grinbox](#) and Keybase for easily sending transactions if you can't or don't want to expose your IP-address publicly. It also supports generating proofs that prove you sent a transaction or amount.
- [Ironbelly](#) iOS/Android wallet for Grin. Open sourced at [cyclefortytwo/ironbelly](#)
- [Niffler](#) Open Sourced Grin GUI Wallet; support mac/linux/windows; support English\简体中文\русский.
- [Vite Grin Mobile Wallet](#) A open-sourced multi-crypto HD mobile wallet supporting GRIN! In addition to all native GRIN transactions (transaction file, HTTP address), Vite Grin Mobile Wallet supports a unique way of transferring through VITE address where the receiver is not required online at all. At the time being, Vite Grin Mobile Wallet iOS version is formally released while Android will come soon. Source code can be found at [here](#). Telegram support link [click me](#)
- [Grin++](#), Open source, easy-to-use GUI powered by an ultra-fast, custom C++ node and wallet backend. Supports sending/receiving via file, http(s), and grinbox. Supports Windows, MacOS, and Linux.
- [Diagon Alley](#) is an Electron wallet for Grin
- [Wimble](#) is a wallet designed specifically for Grin, supports MacOS only at the moment. Beta

Obsolete

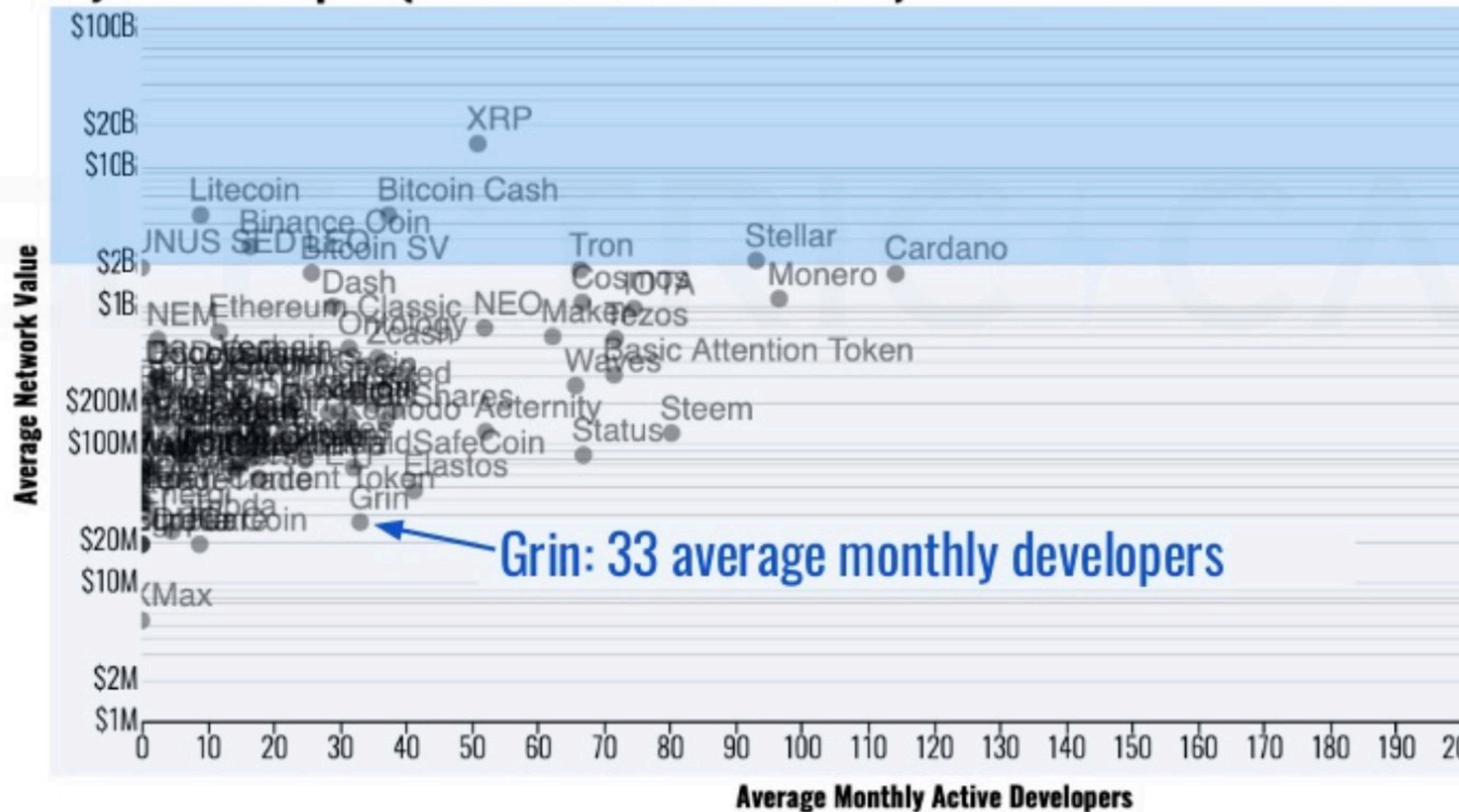
- ~~[Grin Vault](#) Android Wallet. Currently open beta with support only for Floonet.~~
- ~~[Grin Purse](#) Grin Purse is the first GRIN GUI wallet that redefines GRIN's transfer method and uses a bitcoin-like address for transfer, just as simple as using a Bitcoin wallet.~~
- ~~[SuperGrin](#) is a GUI Grin wallet for Mac. Open Source.~~
- ~~[smirk](#) is a user friendly Grin wallet, built using Electron.~~
- ~~[Superlinear](#) is a native Grin wallet for Mac, Windows, and Linux.~~

Source: <https://github.com/mimblewimble/docs/wiki/Community-projects#wallets>

Grin dev ecosystem size

Grin has the most developers for ecosystems under \$50M

Ecosystem Developers (01/01/2019 to 06/30/2019)



**Minimal and fair:
Grin governance**

Grin is a social experiment

- It relies on donations
- Greed and self-interest is a safer choice
- It has been mocked for being too naive
- It doesn't discriminate late adopters
- It doesn't encourage early adoption

Growing Grin

- Decentralization - everyone has equal rights to influence the projects
- With different results
- Any governance structure is an attack vector
- Added only if needed
- Low maintenance

Grin governance 0.1 (testnet 1-2)

- No legal entity, no foundation
- The founder, a small team of developers

Grin governance 0.2 (testnet 3-4)

- No legal entity, no foundation
- The founder, a small team of developers
- Grin council

Grin governance 0.3 (mainnet)

- No legal entity, no foundation
- The founder, a small team of developers
- Grin council
- RFC process
- Subteams (node, wallet, ecosystem etc)

We do not

- Apply for exchange listing
- Sign NDA
- Establish partnership (Remember these? "TCP/IP & Netscape announce partnership to make internet accessible" Me neither. @RyanSAdams)
- Tell you what to do / not do with Grin

Independent communities

- Grin discord server
- 5-10 Telegram groups
- Facebook page
- @GrinMW twitter account
- Grin subreddit
- Grin News newsletter
- WeChat groups
- Meetups: London, Berlin, Moscow, Bay Area, Seoul

Grin clones (forks)

- ~ 5 blockchains (?)
- 2013: it's fashionable to fork Bitcoin
- 2019: it's fashionable to fork Grin

Community projects

Explorers

- Grin Explorer [GitHub](#)
 - [GrinExplorer.net](#) by [@hendi](#) (*floonet*)
 - [GrinMint.com/explorer](#) by [BlockCypher](#)
 - [Grin-Fans.org](#) (English\chinese 简体中文 version) by [xiaojay@gmail.com](#)
- [GrinScan](#) maintained by [@jaspervdm](#) (*floonet*)
- [Blockscan](#) by the same team behind *Etherscan*
- Grin Blockchain Explorer [MinerGate](#)

Community projects

Nodes

- [Grin++](#), Grin node and wallet implementation in C++ for Windows, MacOS & Linux
- ~~[grin-dotnet](#), Grin node implementation in C# (Inactive)~~
- ~~[gringo](#), Grin node implementation in Go (Inactive)~~

Community projects

Other services

- [Grinbox](#), a transaction building service for Grin (for "offline" txs)
- [Knockturn Allee](#) Grin payment processor which supports integration with existing e-commerce platforms in a few clicks
- ~~[Installation Script](#) by JackRack (Inactive)~~

Miners

- grin-miner
- bminer
- ePIC Boost Miner
- GrinGoldMiner
- MinerBabe
- lolminer
- Gminer
- TeamRedMiner
- nbminer
- AIOMiner
- nanominer

Mining Pools

- BTC.com
- CuckooMine
- F2Pool
- GrinCoin
- GrinMint
- GrinPool.co
- Grin-Pool
- LeafPool
- Luxor
- mwgrinpool, open-sourced at [grin-pool/grin-pool](https://github.com/grin-pool/grin-pool)
- Sparkpool
- Uupool
- 666pool
- 2Miners
- MinerGate
- TheGrinPool

Exchanges

- Hotbit
- BitMesh
- BHex
- ChainRift
- Kaiserex
- Poloniex
- BigONE
- TradeOgre
- Kucoin
- A1 Exchange
- Bgogo
- Bittrex
- BitForex
- Deex.Exchange
- Gate.io
- GrinPay
- HitBTC
- qTrade

Grin resources

- Web site <http://grin-tech.org/>
- Forum <http://grin-forum.org/>
- Github <https://github.com/mimblewimble>
- Gitter chat https://gitter.im/grin_community/Lobby

