



grincon<US>(0)

19.01.28 // hero city, san mateo (CA)

The Future of Grin

@yeastplume

Overview

1. Brief Roadmap
2. Project Goals
3. Where we are
4. Current Focus + Approach
5. Future Core Tech
6. Community Support
7. Council / Governance
8. Hit you up for money



Roadmap



Project Goals

Project Goals (Overall)

- Provide open, scalable privacy for all
- Further MW Research, Development and Testing
- Ensure Grin/MW is accessible and usable for all needs



Private



Scalable



Open



Project Goals (More Immediate)

- Not going to compete with Visa at present
- Make Grin a compelling option in settings where cryptocurrencies are already accepted (alongside Bitcoin, Monero, etc)



Where We Are

Where we are (Core)

- We launched a blockchain
 - MimbleWimble
 - Fast Sync
 - Schnorr Sigs
 - Certifiable Transactions
 - Cuckoo Cycle
 - Bullet Proofs (+ MultiSig BP extensions)
 - Merkle Mountain Ranges
 - Compact Blocks
 - Atomic Swaps
 - Dandelion



Where we are (Community)

- Community Projects
 - Block Explorers
 - Wallets
 - Mining Pools
 - Exchange Support
 - Alternate Mining
 - Large and involved community

GrinScan - mainnet

Search by block height, block hash or output

11,330 00000575
1m 21s 451,798,940
5,243,056,834,893

Try out wallet713, an easy-to-use Grin wallet
No node required / No compiling required / Grinbox addresses

Network: mainnet

Blocks

Show latest 20 blocks

Height	Hash	Age	PoW	Difficulty	Kernels	Inputs	Outputs
11,330	00000575539f7c4066dfd861dc35e4d7f4835cf354db6e51ae9de5d443ee1517	1m 20s	AR29	451,798,940	4	34	7
11,329	00000c1ef036205728258ae8d5d4686a814d99c33c3131afa81c2bd3cd2fba02	2m 0s	AR29	449,408,656	2	1	3
11,328	000116ac622eeeb24a1442a01fce24bbeb5d724ed5f445cd56e73f1a068cf3aa	3m 0s	AT31	445,656,052	1	0	1

```
wallet713> info
___ Wallet Summary Info - Account 'default' as of height 11284 ___

Total | 0.000000000
Awaiting Confirmation (< 10) | 0.000000000
Locked by previous transaction | 0.000000000
-----|-----
Currently Spendable | 0.000000000

wallet713> info
___ Wallet Summary Info - Account 'default' as of height 11284 ___

Total | 0.000000000
Awaiting Confirmation (< 10) | 0.000000000
Locked by previous transaction | 0.000000000
-----|-----
Currently Spendable | 0.000000000

wallet713>
```



Where we are (Audits)

- Security Audits
 - Libsecp256k lib changes (Aggsig/Bulletproofs) Complete
 - grin-core, grin_keychain, grin_chain underway soon
 - grin-wallet beyond that
 - Rest of code



Current Focus + Approach

Areas of Focus



Ignotus Peverell @ignopeverell

Jan 22 16:17

the great majority of what we're going to be doing now are:

1. perf, stability and security improvements
2. actual functionalities (a few)
3. support an ecosystem

all the discussion about wallet integration for example fits in 3, so there's definitely going to be a lot of attention there makes sense?



Yeastplume @yeastplume

Jan 22 16:18



Antioch Peverell @antiochp

Jan 22 16:18



What Igno Said

- Ongoing improvements to what's there
 - Bugs/Issues
 - Security Enhancements
 - Results of Audits
 - Maybe support Windows one day soon
- Calm and measured introduction of New Features
- Enhancements and extensions to support the community
 - E.g. Wallet and transaction APIs



General Approach

- Improvements and fixes as needed
- Enhancements/community features as identified
- New technologies as and when they're ready
- No set roadmap



Future Core Tech

Future Tech (Nearish)

- Atomic Swaps
 - Successfully performed against ETH and BTC testchains
- Relative Locks
 - Will be looked at for 1.1.0
- FlyClient
 - Very excited about
- Dandelion++



Future Tech (Further Awayish)

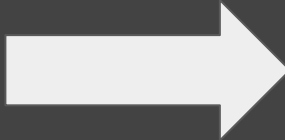
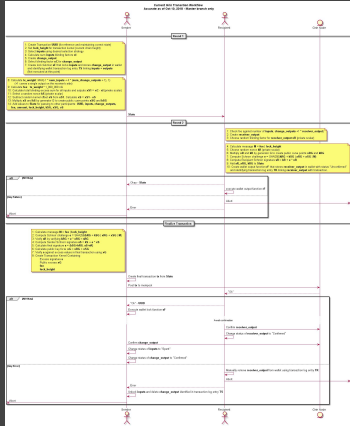
- Vaults/Covenants
 - Improved attack security
- Relative Locks
 - Will be looked at for 1.1.0
- RSA Accumulators
 - Remove a lot of data while enhancing privacy
 - Exciting, but still theoretical
- Scriptless Scripts
 - Leverage Aggsig to emulate smart contracts
- 2nd Tier Enablement
 - Lightning



Community Support

Enabling the Ecosystem

- Non-Prescriptive Approach
- Provide the core tools to enable creative solutions to existing problems



API Fever

- Transaction building APIs
 - Wallet APIs
 - Keychain APIs
 - Node APIs
-
- Mobile/Web/Native/Cloud etc



Continued Support

- Documentation
- Wikis
- Developer Support



Council and Governance

Current Council

- Seems to work (for now)
- Small, Core of developers
- Would prefer more diversity
- How/when/why do we expand it?



Future of Funding

Funding Grin

- No ICO/Premine/Pre-allocation/Mining Tax etc
- General Fund
- Specific Campaign (e.g. Audits)
- Developer Campaigns
- Community Pledges
 - Grinmint, Grinpool, others
 - Miners (GrinGoldMiner)



Funding Me

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





<https://grin-tech.org>

For more presentations like this
and updates on Grin, sign up here