grincon0
18.11.09 // c-base berlin

Grin:

The state of it
@yeastplume

All about Grin

- Grin: the Idea
- Grin: the Project
- Grin: the Community
- Grin: the Technology
- Grin: the Future
- Grin: the T-Shirt

The name of the bank in Harry Potter is ‘Gringotts’

Grin: the Idea

How much Grin can I jam into 30 minutes? Let’s see.

Mimblewimble

- A potentially transformative insight

MIMBLEWIMBLE
Tom Elvis Jedusor
19 July, 2016

****/
Introduction
/****\

Bitcoin is the first widely used financial system for which all the necessary data to validate the system status can be cryptographically verified by anyone. However, it accomplishes this feat by storing all transactions in a public database called "the blockchain" and someone who genuinely wishes to check this state must download the whole thing and basically replay each transaction, check each one as they go. Meanwhile, most of these transactions have not affected the actual final state (they create outputs that are destroyed a transaction later).

Tom Malvolio Riddle -> I am Lord Voldemort
Tom Elvis Jedusor -> Je suis Voldemort
Tom Vorlost Riddle -> Ist Lord Voldemort

Grin

- ‘A minimal implementation of MimbleWimble’

47 < igno_peverell> I have a minimal implementation of MimbleWimble available. It's very far from complete but has the basics, included the summing of pedersen commitments:
47 < igno_peverell> https://github.com/ignopeverell/grin
47 < igno_peverell> Any feedback or review is greatly appreciated. Thanks!
48 < qpm> tx:<Jeremy_Rand> igno_peverell: nice username. :)

Ignotus Peverell -> evil Lego punters

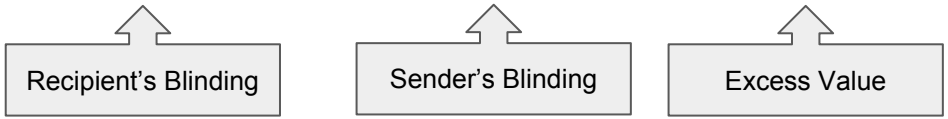
What's a Mimblewimble?

Confidential Transactions

- Pedersen Commit to hide amounts (Blinding + Value)
- C = b*G + v*H
- CIn1 + CIn2 + CIn3 - COut1 - COut2 - COut3 == 0

Key Mimblewimble Insight

- Interactively choose blinding factors to prove ownership
- (113*G + 3*H) - (28*G + 3*H) = 85*G + 0*H



Mimblewimble prevents your opponent from accurately casting their next spell. Usually comes in handy for your daily commute.

Grin: the Project

You know what this world really needs? Another Cryptocurrency. MY Cryptocurrency!

Why a new Coin?

- There is some consensus around the idea that MW is worth experimenting with.
- Bitcoin is hard to change.
- BTC Sidechains not necessarily supported then and now
- MW concepts like Fast-Sync/Cut-through nearly impossible in BTC
- Mimblewimble needed and still needs a LOT of experimentation.

YOU try getting a PR to support your experimental technology accepted into Bitcoin core, then tell me again how MW should be a sidechain.

Grin wants to ...

- build a usable MW implementation.
- focus on staying as simple and minimal as possible.
- research and advance Mimblewimble tech.
- work toward better privacy for all.
- work toward prohibiting censorship and control.
- work toward decentralisation.
- be open and fair to all its users.
- maintain a level playing field at launch and beyond.

… channel the resources of entire US Military-Industrial complex into Grin ASIC production.

Grin does not want to …

- be the one true MW Implementation.
- be the gatekeepers of the word of Voldemort.
- unfairly reward a small group of people.

Moneycat thinks Grin should ICO at a valuation of $90 Billion. Naughty Moneycat!

Grin's Approach

- The Upside
  - No ICO
  - No 'Founder's Reward'
  - No Premine
  - No Pre-allocation
  - No Pre-Anything
  - Better for openness, fairness, decentralisation

My kid's school needed money to fix the gym's roof, so they thought they'd try an ICO instead of a bake sale this year. They raised $947 million.

Grin's Approach

- The Downside
  - No ICO
  - No 'Founder's Reward'
  - No Premine
  - No Pre-allocation
  - No Pre-Anything
  - We're Poor

The roof is still leaking.

Grin: the Community

We might be poor, but we're rich in community spirit!
I guess that can be a thing.

Grin's Community

- Grin's Best Asset
- Can't be bought
- Direct result of Grin's Principles

I can't meme later than 2005.
This is why I don't meme.

Grin's Community

- Technocratic Council
- Contributing Developers
- Forum Frequenters
- Mailing List Watchers
- Mining / Hardware Community

Satoshi also likes to turn up in once in a while to troll us about the emission curve. (I'm like 99% sure it's him.)

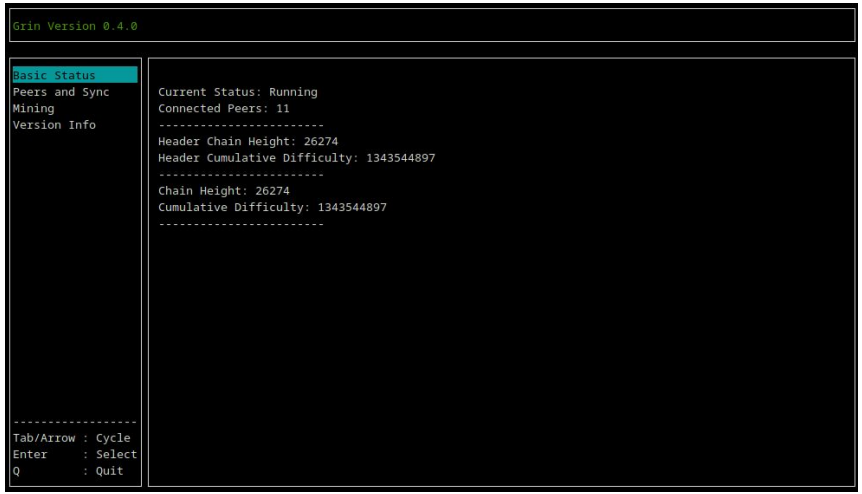
Community Funding

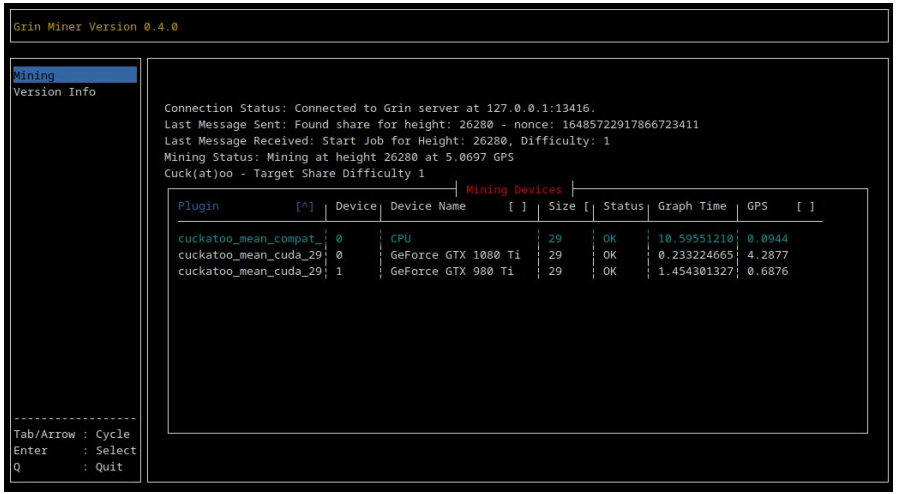
- Challenging, but results VERY encouraging
- 3 Yeast Campaigns
- 1 Security Audit Campaign
- Many future needs

Grin: the Technology

Rust is like your really annoying friend who's always right about everything. Except you can't take Rust out for the day then come back and tell everyone it died in a tragic accident.

Grin - 4th Testnet





Actually, Rust is more like Columbo. Everything is file, all seems to be compiling, errors seem to be gone. Then the borrow checker turns up and says ‘oh, just one more thing’ and you’re fooked.

Current Grin Technology

- https://github.com/mimblewimble/grin
- Working MW Chain, w. fast-sync
- Transaction Aggregation
- Dandelion
- Bulletproofs
- Secure Aggsig (Schnorr) Tx Creation Protocol
- ‘Cuckoo’ family PoW (AR + AF)
- ‘Official’ Miner + solvers
- Wallet + Supporting Wallet Libs
- Infrastructure (TUI, Logging, Builds)
- Continually out-of-date documentation

Why didn’t you do it in C?!??! I’m a master at C++ and if you’d only decided to build Grin in C then I’d have been able to contribute. Well you didn’t. So now you’ve lost out on my CONSIDERABLE talents.

Grin: the Future

Grin aims to be the currency of choice after ‘The Event’, and will support the ever-mutating needs of the post-apocalyptic community. Remain Indoors.

Launch Plans

- When Grin?
- Soon Grin.

Pictured: Front page illustration of every ICO prospectus ever.

First …, then Grin

- Many core features done-ish
- Security Audit
- Much testing, many bug fixes
- Usable Web Wallet
- PoW Finalisation
- User Experience

If mainnet were live, 1320 new Grins would have been added to the world in the time I've spent yammering here. I wouldn't own any of them.

Then More Grin

- Post-Launch Mayhem
- Flyclient
- RSA Accumulators (Research)
- Much atomic swapping
- Vaults
- Confidential Assets
- Ongoing work...

Benedikt Bünz is like, 14 and he's already contributed more to the world than you or I ever will. Prick.

Beyond Grin

- fork grin, make forkgrin monetary policy similar to bitcoin or monero
- Mitigate shittiness of grin supply 1coin/1second always
- 100% funded by gogoxmr

Actually better thought-out than most Crypto-twitter arguments.

Grin: the T-Shirt

Seriously, why doesn't everyone do this to fund their blockchain?

Specs

- 100% combed and ring-spun cotton
  - Heather colors contain polyester
- Fabric weight:
  - 142 g/m2 (4.2 oz)
- Shoulder to shoulder taping
- Side seamed
- Many designs available
- 100% of profits to Grin Project
- Available from:

  https://tmgox.com/

Pretty much the only funding option anyone will have left after the SEC is done regulating ICOs.

Grin: The Brief QA Session

Grin: The ‘Thank You’ Slide

Thank you for not throwing anything at me during this presentation. It means a lot.

https://grin-tech.org